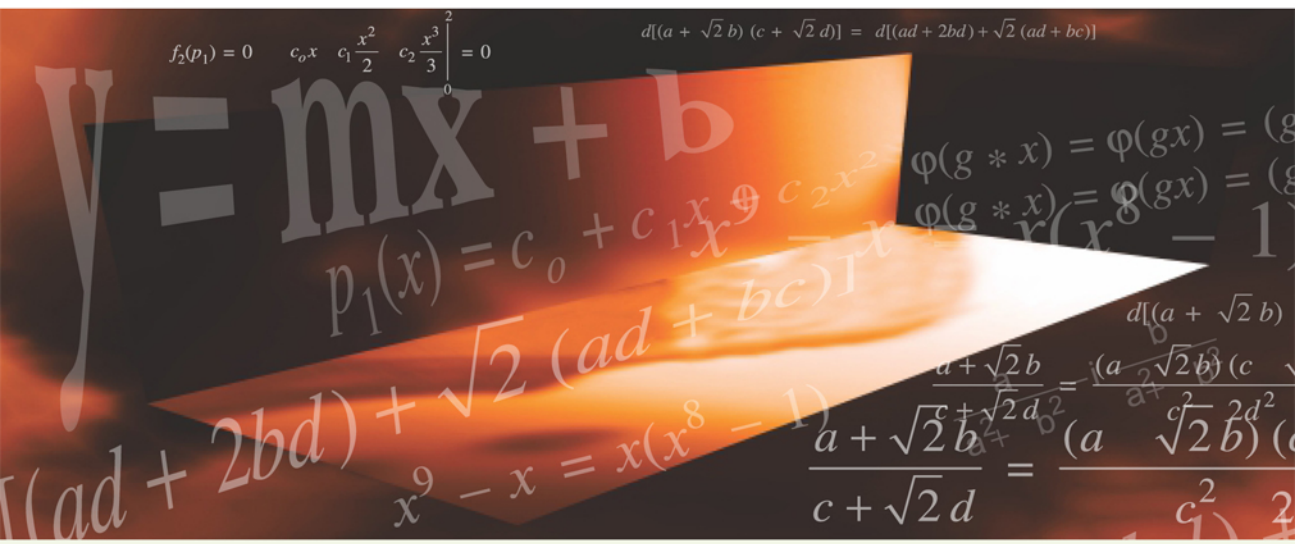
VIKAS®

A COURSE IN ABSTRACT ALGEBRA

FOURTH EDITION



Vijay K Khanna • S K Bhambri

A COURSE IN
ABSTRACT ALGEBRA

Fourth Edition

A COURSE IN
ABSTRACT ALGEBRA

Fourth Edition

VIJAY K KHANNA
S K BHAMBRI

Formerly
Associate Professors
Department of Mathematics
Kirori Mal College
University of Delhi

VIKAS® PUBLISHING HOUSE PVT LTD

VIKAS® PUBLISHING HOUSE PVT LTD
E-28, Sector-8, **Noida**-201301 (UP) India
Phone: +91-120-4078900 • Fax: +91-120-4078999
Registered Office: 576, Masjid Road, Jangpura, **New Delhi**-110014. India
E-mail: ***helpline@vikaspublishing.com*** • Website: ***www.vikaspublishing.com***

- **Ahmedabad :** 305, Grand Monarch, 100 ft Shyamal Road, Near Seema Hall, Ahmedabad-380051 • Ph. +91-79-65254204, +91-9898294208
- **Bengaluru :** First Floor, N S Bhawan, 4th Cross, 4th Main, Gandhi Nagar, Bengaluru-560009 • Ph. +91-80-22281254, 22204639
- **Chennai :** E-12, Nelson Chambers, 115, Nelson Manickam Road, Aminjikarai, Chennai-600029 • Ph. +91-44-23744547, 23746090
- **Hyderabad :** Aashray Mansion, Flat-G (G.F.), 3-6-361/8, Street No. 20, Himayath Nagar, Hyderabad-500029 • Ph. +91-40-23269992 • Fax. +91-40-23269993
- **Kolkata :** 82, Park Street, Kolkata-700017 • Ph. +91-33-22837880
- **Mumbai :** 67/68, 3rd Floor, Aditya Industrial Estate, Chincholi Bunder, Behind Balaji International School & Evershine Mall, Malad (West), Mumbai-400064 • Ph. +91-22-28772545, 28768301
- **Patna :** Flat No. 101, Sri Ram Tower, Beside Chiraiyatand Over Bridge, Kankarbagh Main Rd., Kankarbagh, Patna-800020 • Ph. +91-612-2351147

A Course in Abstract Algebra
ISBN: 978-93259-6900-1

Third Edition 2008
Reprinted several times
Fourth Edition 2013

Preface to the Fourth Edition

Today, when we look back, it is more than twenty years since the first edition of the book was published. Over the years, it has been subjected to a lot of changes (improvements, if we dare say) keeping in mind the requirements of the readers for whom it was intended. The present volume goes on to do the same and we have tried to further improve upon the contents. Almost all the chapters have undergone revision and a fairly large number of new examples and worked out problems have been added to make the theory easier to grasp. The portion on Fields may seem to be taking the back seat, but then it has had its share of revision in the previous editions. At places, new/alternate proofs have been added and some reshuffling has also been done to move certain results to better-suited places.

The subject matter has been planned so as not to remain constrained by the syllabus of a particular course. It is meant for anyone and everyone pursuing a serious course in Abstract Algebra. The book also comes to you in a bigger and better looking format, designed to make reading more focused.

While thanking all those readers who have been advising us for improvements, a word of thanks to that vast majority of silent admirers cannot be overlooked and we do feel indebted to them for making the book a success that it is.

Utmost care has been taken to keep the misprints out and we hope we have been successful in our effort. Since there is always room for improvement, it goes without saying that any suggestions, howsoever trivial, would be highly welcome.

Vijay K Khanna
S K Bhambri

Preface to the First Edition

The present volume has grown out of our association with the teaching of Algebra to the honours and postgraduate classes for the last several years and our exposure to the problems faced by the students in grasping the abstract nature of the subject. This experience is the foundation and, we hope, the strength of the text. Earnest efforts have been exerted to present the subject matter in a well-knit manner so as not only to stimulate the interest of the student but also to provide with an insight into the complexities of a subject of great intrinsic beauty.

The book is intended to serve as a text for undergraduate students especially those opting for an honours course in Mathematics. However, postgraduate students will find it equally useful.

The first chapter on Preliminaries is a curtain-raiser to the main contents of the book. It gives a rather terse summary of the results from Set Theory (some of which we presume the reader would already be familiar with). A few results from Number Theory are incorporated in the later half of this chapter. We debated between ourselves whether or not to give a 'full chapter status' to Number Theory results, and after a careful thought decided to keep these as only a part of the first chapter since we feared that a full chapter on these might impair the balance of the book.

The main text can be divided into four sections on Groups, Rings, Vector spaces (Linear Algebra) and Fields. Fairly sufficient ground has been covered in the first three sections. It is only in the last section on Fields that we can possibly be accused of being stingy. But then there are constraints and it was paucity of space and time (and not of ideas) that finally made us keep Galois Theory out. Maybe in a subsequent edition it would find its way in.

Different concepts have been explained with the help of examples. A large number of problems with solutions have been provided to assist one get a firm grip on the ideas developed. There is plenty of scope (in the form of exercises) for the reader to try and solve problems on his own. In all, a substantial variety of challenges (and rewards) is assured.

We are deeply indebted to all those authors whose books (research papers) on Algebra influenced our learning of the subject and take this opportunity to express our sincere gratitude to them. We are also thankful to those friends and colleagues with whom we had fruitful discussions from time to time.

It is our earnest belief that no 'work' is ever complete till it has had its share of criticism and hence we'll be only too glad to receive comments and suggestions for the betterment of the book.

Vijay K Khanna
S K Bhambri

Contents

Glossary of Symbols

$\in$	:	Belongs to
$\notin$	:	Does not belong to
$\exists$	:	There exists
$\Rightarrow$	:	Implies
$\Leftrightarrow$	:	Implies and is implied by
iff	:	If and only if
$a \mid b$	:	a divides b or b is a multiple of a
$a \nmid b$	:	a does not divide b
φ	:	Empty set
$H \leq G$	:	H is a subgroup of G
$H < G$	:	H is a proper subgroup of G
$H \trianglelefteq G$	:	H is a normal subgroup of G
$i_G(H)$	:	Index of H in G
$[G:H]$	:	In groups, index of H in G. In fields, degree of G over H
N	:	Set of natural numbers
Z	:	Set of integers
Q	:	Set of rational numbers
R	:	Set of real numbers
C	:	Set of complex numbers
$Z(G)$	:	Centre of group G
$o(G)$	:	Order of G
S_n	:	Symmetric group of degree n
$\cong$	:	is isomorphic to

1

Preliminaries

Introduction

In this chapter we remind or acquaint the reader about some basic concepts in mathematics that we reckon the reader would already be in the know of, but in case not, we strongly recommend one to glance through the contents of this chapter before venturing into the subsequent text. We basically explain the concepts of sets along with operations in sets and then go on to define the all-important notion of a mapping/function(and permutations), which finally lead us to the definition of a binary composition/operation.

In the second half of this chapter we take a peek at the results from number theory and try to discuss most of the relevant results that could be useful in the main text. Having done this chapter, one is fully equipped to understand and grasp the subsequent material that follows.

Sets

The notion of a set is most fundamental in Mathematics, but it is not our endeavour in this text to enter into the axiomatic study of set theory. We'll, instead, borrow the word 'set' from the language and be content to refer to it as a collection of objects. To give it a more precise shape, by a set, we will mean a collection of objects such that given any object, it is possible to ascertain whether that object belongs to the given collection or not. For instance, we can talk of set of all natural numbers, set of all students in a particular class, etc. If x is an element (member) of a set A we say x belongs to A and express it as $x \in A$. If y is not a member of A we say y does not belong to A and write $y \notin A$. We shall use capital letters A, B, X, Y etc. for denoting sets and small letters, a, b, c, x, y etc. for the elements (or members or objects).

Two sets A and B are said to be *equal* if they contain precisely the same elements and we write $A = B$.

A set can be described in various ways. For example, if A is the set containing 1, 2, 3, 4, 5, 6, we can write it as

$$A = \{1, 2, 3, 4, 5, 6\}$$
$$A = \{1, 2, ..., 6\}$$
$$A = \{x \in \mathbf{N} \mid x \leq 6\}$$

where $\mathbf{N}$ is set of all natural numbers. The last notation reading as: those x in the set of natural numbers which satisfy the property that $x \leq 6$.

We do not repeat any element while writing the elements in a set. Again, the order in which the elements are written is immaterial. Thus {1, 2, 3} and {2, 1, 3} mean the same set.

A set having no element is called an *empty set* or a *null set* or a *void set.* It is denoted by Φ or φ. Obviously any two empty sets are equal. A set will be called *finite* if either it is empty or has finite number of elements, *i.e.,* the elements can be listed by natural numbers such that the process of listing stops after a certain definite stage. A set with infinite number of elements is referred to as an infinite set.

The set {1, 2, 3, ..., 1000} is a finite set, whereas the set of all integers is infinite. Again the set of all rational numbers whose square is 2 is an empty set.

We use the notation $o(S)$ or $|S|$ to mean the number of elements in the set S and read it as *order of S* (sometimes also called its *cardinality*).

Subsets

We say a set A is contained in a set B (in symbols $A \subseteq B$) if every element of A is in B. A is then called subset of B and B is called superset of A. If in addition to this there is at least one element in B which is not in A, we say A is strictly contained in B ($A \subset B$) and call A a proper subset of B. $A \not\subset B$ means A is not a subset of B. Also $A \subseteq B$ and $B \supseteq A$ mean the same.

It is clear then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Also, $A \subseteq A$, $\varphi \subseteq A$ for any set A.

Definition: By *union* of two sets A and B, we mean the set $A \cup B$ which contains all the elements of A as well as B. Thus $A \cup B = \{x \mid x \in A \text{ or } x \in B \text{ (or both)}\}$.

By *intersection* of two sets A and B, we mean the set $A \cap B$ which contains all the elements of A and B. Thus $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

The *difference* of two sets A and B is defined to be the set

$$A - B = \{x \mid x \in A, \ x \notin B\}.$$

In case $B \subset A$, then $A - B$ is called the complement of B in A. If there is no confusion regarding the set A, complement of B in A is denoted by B'.

Example 1: Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$

Then $A \cap B = \{3\}$

$A \cup B = \{1, 2, 3, 4, 5, 6\}$

$A - B = \{1, 2\}$

Theorem 1: *If A, B, C are sets then the following results hold:*

(*i*) $A \cap A = A$, $A \cup A = A$

(*ii*) $A \cap \varphi = \varphi$, $A \cup \varphi = A$

(*iii*) $A \cap B = B \cap A$, $A \cup B = B \cup A$, $A \cap B \subseteq A \subseteq A \cup B$

(*iv*) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$

(*v*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(*vi*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof: We will prove (*v*), and leave others for the reader to try as an exercise.

Let $x \in A \cap (B \cup C)$ be any element.

Then $x \in A$ and $x \in B \cup C$

$\Rightarrow x \in A$ and $x \in B$ or $x \in C$.

If $x \in B$, then as $x \in A$, $x \in A \cap B$

If $x \in C$, then as $x \in A$, $x \in A \cap C$.

i.e. $x \in A \cap B$ or $x \in A \cap C$ (or both, of course)

$\Rightarrow x \in (A \cap B) \cup (A \cap C)$

$\Rightarrow A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ ... (1)

Again, $y \in (A \cap B) \cup (A \cap C)$

$\Rightarrow y \in A \cap B$ or $y \in A \cap C$

$\Rightarrow y \in A$ and B or $y \in A$ and C

$\Rightarrow y \in A$ and $y \in B$ or C

$\Rightarrow y \in A$ and $y \in B \cup C$

$\Rightarrow y \in A \cap (B \cup C)$

$\Rightarrow (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ ...(2)

(1) and (2) give us the result.

Theorem 2: (*DeMorgan's laws*). *For sets A, B in a set X,*

(*i*) $X - (A \cup B) = (X - A) \cap (X - B)$ *or* $(A \cup B)' = A' \cap B'$

(*ii*) $X - (A \cap B) = (X - A) \cup (X - B)$ *or* $(A \cap B)' = A' \cup B'$

Proof: (*i*) Let $x \in X - (A \cup B)$ be any element.

Then $x \in X$, $x \notin A \cup B$

$\Rightarrow x \in X$, $x \notin A$, $x \notin B$

$\Rightarrow x \in X - A$, $x \in X - B$

$\Rightarrow x \in (X - A) \cap (X - B)$

$\Rightarrow X - (A \cup B) \subseteq (X - A) \cap (X - B)$ ...(1)

Again $y \in (X - A) \cap (X - B)$

$\Rightarrow y \in X - A$, and $y \in X - B$

$\Rightarrow y \in X$, $y \notin A$ and $y \in X$, $y \notin B$

$\Rightarrow y \in X$ and $y \notin A \cup B$

$\Rightarrow y \in X - (A \cup B)$

$\Rightarrow (X - A) \cap (X - B) \subseteq X - (A \cup B)$ ...(2)

(1) & (2) give us the result.

(*ii*) Prove similarly.

Definition: Given two elements a, b of a set of X, we define the ordered pair (a, b) to be the set $\{\{a\}, \{a, b\}\}$. a is called the first component (or first co-ordinate) and b is called the second component (or second co-ordinate).

We show $(a, b) = (c, d) \Leftrightarrow a = c, b = d$

If $a = c, b = d$ then the result is obvious.

Conversely, $(a, b) = (c, d)$

$$\Rightarrow \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$$

Since the two sets are equal, they contain same elements.

Thus, $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$

If $\{a\} = \{c\}$, then $\{a, b\} = \{c, d\}$

$$\Rightarrow a = c \text{ and } b = d \text{ (as } a = c)$$

Again, if $\{a\} = \{c, d\}$ then $\{a, b\} = \{c\}$

$$\Rightarrow a = c, a = d, a = c, b = c$$

$$\Rightarrow a = c = b = d$$

$$\Rightarrow a = c, b = d$$

Hence the result follows.

We thus notice, the order in which the elements are written is important in as much as (a, b) is not same as (b, a) unless $a = b$, whereas, of course, the two sets $\{a, b\}$ and $\{b, a\}$ are same.

Relations

Definition: Given two sets A and B, the cartesian product $A \times B$ is defined by

$A \times B = \{(a, b) \mid a \in A, b \in B\}$. Thus it is the set of all ordered pairs of elements from A and B.

As an example, if $A = \{1, 2\}$, $B = \{3, 4, 5\}$, then

$$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$$

Also, then $B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2), (5, 1), (5, 2)\}$

thus $A \times B$ may not equal $B \times A$.

One can, of course, talk of $A \times A$, which we also write as A^2. Similarly, we can talk of A^3, A^4 and so on. In fact, $A^n = \{(a_1, a_2, ..., a_n) \mid a_i \in A\}$, the set of all n-tuples $(a_1, a_2, ..., a_n)$, $a_i \in A$.

Any subset of $A \times B$ is called a (binary) relation from A to B, *e.g.*,

$$R_1 = \{(1, 3), (1, 4), (1, 5)\}$$

$$R_2 = \{(1, 3)\}, \quad R_3 = \{(2, 3), (1, 5)\}$$

are all relations from A to B.

A relation from A to A is called a relation in A (or on A).

If R is a relation from A to B and $(a, b) \in R$, then we also express this fact by writing aRb and say a is R-related to b.

If R_1 is a relation from A to B and R_2 is a relation from C to D then R_1 and R_2 are said to be equal if $A = C$, $B = D$ and $aR_1b \Leftrightarrow aR_2b$, $a \in A$, $b \in B$.

Let now, A be a non empty set. A relation R in A is called

Reflexive: if $(a, a) \in R$ for all $a \in A$

Symmetric: if whenever $(a, b) \in R$ then $(b, a) \in R$

Anti-Symmetric: if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$

Transitive: if whenever (a, b), $(b, c) \in R$ then $(a, c) \in R$

A relation R is called an *equivalence relation* if it is reflexive, symmetric and transitive.

A relation R on a set A is called a *partial order* relation, if it is reflexive, anti-symmetric and transitive.

Example 2: If $A = \{1, 2, 3\}$ then

$R_1 = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$ is reflexive

$R_2 = \{(1, 1), (2, 2)\}$ is not reflexive

$R_3 = \{(1, 2), (2, 1)\}$ is symmetric but not reflexive

$R_4 = \{(1, 1), (1, 2)\}$ is neither reflexive nor symmetric, but is transitive.

Example 3: Let A be the set of all lines in a plane. Let $R \subseteq A \times A$ where

$R = \{(l, m) \mid l, m \in A, l \parallel m\}$ then R is

Reflexive: as $(l, l) \in R$ for all $l \in A$

as $l \parallel l$ for all $l \in A$

Symmetric: as if $(l, m) \in R$ then $l \parallel m$

$\Rightarrow m \parallel l$

$\Rightarrow (m, l) \in R$

Transitive: as if $(l, m) \in R$, $(m, n) \in R$

then $l \parallel m$, $m \parallel n$

$\Rightarrow l \parallel n \Rightarrow (l, n) \in R$

Thus relation of parallelism is an equivalence relation.

Example 4: Let $\mathbf{Z}$ = set of integers then the usual $\leq$ is a partial order relation on $\mathbf{Z}$ as it is

Reflexive: as $a \leq a$ for all $a \in \mathbf{Z}$

Anti-Symmetric: as $a \leq b$, $b \leq a \Rightarrow a = b$

Transitive: as $a \leq b$, $b \leq c \Rightarrow a \leq c$.

Example 5: Let $R = \{(m, n) \mid m, n \in \mathbf{Z}, m \mid n\}$ where by $x \mid y$ (x divides y) we mean, $\exists z$, s.t., $y = xz$.

then R is a partial order relation. Verify?

Example 6: The relation of equality on integers is an equivalence relation.

Example 7: Let $\mathbf{Z}$ = set of integers. Let $n \neq 0$ be any fixed integer. For any $a, b \in \mathbf{Z}$, we define a relation

$a \equiv b \pmod{n}$ (read as a is congruent to b mod n)

$\Leftrightarrow n$ divides $a - b$

Then this is an equivalence relation as

Reflexivity: $a \equiv a \pmod{n}$

as $a - a$ is divisible by n

as $0 = a - a = 0n$.

Symmetry: Let $a \equiv b \pmod{n}$

Then n divides $a - b$

$\Rightarrow$ $\exists\ c$, s.t., $a - b = nc$

$\Rightarrow$ $b - a = -nc = (-c)n$

$\Rightarrow$ $b \equiv a \pmod{n}$.

Transitivity: Let $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

Then $n \mid a - b$, $n \mid b - c$

$\Rightarrow$ $\exists\ c_1$ & c_2 s.t., $a - b = nc_1$

$b - c = nc_2$

Now, $a - c = (a - b) + (b - c)$

$= nc_1 + nc_2 = n(c_1 + c_2) = nc_3$

$\therefore$ $\exists\ c_3 \in \mathbf{Z}$, s.t., $a - c = nc_3$

$\Rightarrow$ n divides $a - c$

or that $a \equiv c \pmod{n}$.

Equivalence Classes

Let X be a non-empty set and let $\sim$ be an equivalence relation on X. For any $a \in X$, we define equivalence class of a by

$$cl(a) = \{x \in X \mid x \sim a\}$$

i.e., equivalence class of a contains all those members of X, which are related to a under the relation $\sim$. The following theorem gives us certain important properties of equivalence classes.

Theorem 3: *Let $\sim$ be an equivalence relation on a non-empty set X. Then for any $a, b \in X$*

(*i*) $cl(a) \neq \varphi$

(*ii*) *Either* $cl(a) \cap cl(b) = \varphi$ *or* $cl(a) = cl(b)$

i.e., two equivalence classes are either equal or have no element in common.

(*iii*) $X = \bigcup_{a \in X} cl(a)$

Proof: (*i*) Since $a \sim a$, by reflexivity

$a \in cl(a)$, $\therefore\ cl(a) \neq \varphi$.

(*ii*) Let $cl(a) \cap cl(b) \neq \varphi$

Then $\exists$ some $x \in cl(a) \cap cl(b)$

$\Rightarrow x \in cl(a)$ & $x \in cl(b)$

$$\Rightarrow x \sim a \quad \& \quad x \sim b$$
$$\Rightarrow a \sim x \quad \& \quad x \sim b$$
$$\Rightarrow a \sim b.$$

Now if $y \in cl(a)$ be any element
then $y \sim a$ and as $a \sim b$ we find $y \sim b$

$$\Rightarrow y \in cl(b)$$

thus $cl(a) \subseteq cl(b)$
Similarly $cl(b) \subseteq cl(a)$
Hence $cl(a) = cl(b)$.

(*iii*) Clearly any element $x \in X$ will be in at least one class, namely $cl(x)$ and hence is a member of $\bigcup_{a \in X} cl(a)$.

Again, if $t \in \bigcup_{a \in X} cl(a)$ then $t \in cl(x)$ for some x and as $cl(x) \subseteq X$, $t \in X$

Showing that X equals the union of all equivalence classes of X.

Definition: Let X be a non-empty set. Let K = set of non-empty subsets of X such that every two distinct members of K are disjoint, then K is called a *partition* of X, if X equals the union of all members of K.

In view of this definition, we can say that if X be a non-empty set, with an equivalence relation defined on it, then the set of all equivalence classes of X partitions the set X.

Mappings or Functions

Let A and B be two non-empty sets. A relation f from A to B is called a mapping (or a map or a function) from A to B if for each $a \in A$, $\exists$ a unique $b \in B$ s.t., $(a, b) \in f$(and in that case we write $b = f(a)$ and b is called *image* of a under f and a is called *pre-image* of b under f). We express this by writing $f : A \to B$.

Thus mapping is that relation from A to B in which each member of A is related to some member of B and no member of A is related to more than one member of B, although more than one member of A can be related to the same member of B. A is called the *domain* of f and B is called the *co-domain* of f. A mapping $f : A \to A$ is also sometimes called a *transformation* of the set A.

The subset of B which contains only those members which have pre images in A is called *range* of f.

One can, of course, have more than one mapping from A to B.

A mapping $f : A \to B$ is called *one–one* (1–1) *or injective* mapping, if

$$f(x) = f(y) \Rightarrow x = y$$

or if $$x \neq y \Rightarrow f(x) \neq f(y)$$

Thus under one–one mapping all members of A are related to different members of B.

A mapping $f : A \to B$ is called *onto* or *surjective* mapping, if range of f equals B, *i.e.*, each member of B has a pre iimage under f.

A map which is both 1–1 and onto is sometimes referred to as a one-to-one correspondence or a *bijective* map.

To check whether a map $f : A \to B$ is well defined or not, we need verify that $x = y \Rightarrow f(x) = f(y)$.

Example 8: Let **N** = set of natural numbers. Define a map $f : \mathbf{N} \to \mathbf{N}$ s.t., each $a \in \mathbf{N}$ is connected to its square. Since each natural number has a unique square in **N** itself, we find *f* will be a well-defined mapping. We express this by writing

$$f : \mathbf{N} \to \mathbf{N}, \text{ s.t.,}$$
$$f(x) = x^2 \quad \text{for all } x \in \mathbf{N}$$

We notice that in the notation of our definition

$$f = \{(1, 1), (2, 4), (3, 9), (4, 16),.....\}$$
$$= \{(x, x^2) \mid x \in \mathbf{N}\}$$

Example 9: For any set *A*, the mapping $f : A \to A$, s.t.,

$$f(x) = x \quad \text{for all } x \in A$$

is called the *identity* map. It is trivially a well defined one-one map. It is also onto.

Example 10: If **Z** = set of integers, then the map $f : \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 2x$$

is 1–1 but not onto. $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$

But $1 \in \mathbf{Z}$ has no pre image.

Example 11: The map $f : \mathbf{N} \to \{1\}$, s.t.,

$$f(x) = 1 \quad \text{for all } x \in \mathbf{N}$$

where **N** = set of naturals is onto map but not 1–1.

Example 12: Let $f : \mathbf{R}^3 \to \mathbf{R}^3$ s.t.,

$$f(x, y, z) = (x + z, x + y + 2z, 2x + y + 3z)$$

be the mapping defined on $\mathbf{R}^3$. We show it is not onto.

Let $(a, b, c) \in \mathbf{R}^3$ be any element. If (x, y, z) is its pre image under *f*, then we should have

$$f(x, y, z) = (a, b, c)$$

i.e., $(x + z, x + y + 2z, 2x + y + 3z) = (a, b, c)$

i.e.,
$$x + 0 + z = a$$
$$x + y + 2z = b$$
$$2x + y + 3z = c \text{ should hold}$$

In matrix form, we have

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Augmented matrix is

$$\begin{bmatrix} 1 & 0 & 1 & a \\ 1 & 1 & 2 & b \\ 2 & 1 & 3 & c \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & a \\ 0 & 1 & 1 & b-a \\ 1 & 0 & 1 & c-a \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & a \\ 0 & 1 & 1 & b-a \\ 0 & 0 & 0 & c-b-a \end{bmatrix}$$

$$R_2 \to R_2 - R_1 \qquad R_3 \to R_3 - R_1$$
$$R_3 \to R_3 - R_2$$

Hence solution of above equations exists only when $c - b - a = 0$. Thus we cannot find a pre image for elements $(a, b, c) \in \mathbf{R}^3$ where $c - b - a = 0$ does not hold. Hence f is not onto.

Equality of Mappings

Two mappings f and g from A to B *should* be equal if they 'behave' exactly in the same way. We formalise this in

Theorem 4: *Two maps* $f : A \to B$ *and* $g : A \to B$ *are equal iff* $f(x) = g(x)$ *for all* $x \in A$.

Proof: Let $f = g$.

Let $a \in A$ be any element and let $f(a) = b$.

then $(a, b) \in f \Rightarrow (a, b) \in g$

$\Rightarrow b = g(a)$

or that $f(x) = g(x)$ for all x.

Conversely, let $f(a) = g(a)$ for all $a \in A$

Let $x \in f$ be any element, then $x = (a, f(a))$ for some $a \in A$.

Since $f(a) = g(a), \quad x = (a, g(a)) \in g$

i.e., $x \in f \Rightarrow x \in g$

or that $f \subseteq g$

Similarly, $g \subseteq f$

and hence $f = g$.

Definition: Let $f : A \to B$ be a mapping and suppose C and D are subsets of A and B respectively, s.t., $f(x) \in D$ for all $x \in C$. We say f induces the map $g : C \to D$ where $g(x) = f(x)$ for all $x \in C$ and in that case g is called a *restriction* of f.

Composition of Mappings

Let $f : A \to B$ and $g : B \to C$ be two mappings.

We define a mapping (to be denoted by *gof*) from A to C by the rule

$gof(x) = g(f(x))$ for all $x \in A$

That it is well defined is confirmed by the fact that

$x = y$

$\Rightarrow f(x) = f(y)$

$\Rightarrow g(f(x)) = g(f(y))$

$\Rightarrow (gof)x = (gof)y$

One can, of course, extend this idea to more than two mappings.

Remark: *gof* is also denoted by *gf*.

Theorem 5: *If* $f : A \to B$ and $g : B \to C$ *are one-one* (*onto*) *mappings then so is gof.*

Proof: Let f and g be one-one

Since $(gof)\ x = (gof)\ y$

$\Rightarrow g(f(x)) = g(f(y))$

$\Rightarrow f(x) = f(y)$ [as g is 1 – 1]

$\Rightarrow x = y$ [as f is 1 – 1]

We find *gof* is one-one.

Again, if f, g are onto, and $c \in C$ be any element, then $\exists\ b \in B$ s.t., $g(b) = c$ (g being onto). Again, for this $b \in B$, $\exists$ some $a \in A$ s.t.,

$f(a) = b$ as f is onto

Now $(gof)\ a = g(f(a)) = g(b) = c$

Hence *gof* is onto.

The converse of the above theorem does not hold (see exercises).

Theorem 6: *A mapping* $f : X \to Y$ *is one-one onto iff* $\exists$ *a mapping* $g : Y \to X$ *such that gof and fog are identity maps on X and Y respectively.*

Proof: Let $f : X \to Y$ be one-one onto.

Define a mapping $g : Y \to X$, s.t.,

$$g(y) = x \quad \textit{iff} \quad f(x) = y$$

Since f is onto, for any $y \in Y$, $\exists$ an $x \in X$ s.t., $f(x) = y$ and as f is one-one, this x is unique and hence g is well defined.

Now *gof* is a map from $X \to X$

For any $x \in X$ let $f(x) = y$, then by definition of g

$$g(y) = x$$

Now $(gof)\ x = g(f(x)) = g(y) = x$

Showing thereby that *gof* is identity map.

Similarly *fog* will also be identity map.

Conversely, let $f : X \to Y$ be a map for which it is possible to find some $g : Y \to X$ such that *fog* and *gof* are identity maps on Y and X respectively.

Let $f(x_1) = f(x_2)$

Then $g\ (f(x_1)) = g(f(x_2))$ [g is well defined map]

$\Rightarrow (gof)\ x_1 = (gof)\ x_2$

$\Rightarrow x_1 = x_2$ [*gof* is identity map]

$\Rightarrow f$ is 1 – 1

Again, let $y \in Y$ be any element

Then $y = (fog)y$ (*fog* is identity map)

$= f(g(y))$

thus for $y \in Y$, $\exists\ g(y) \in X$, s.t., $f(g(y)) = y$ *i.e.*, $g(y)$ is pre-image of y, hence f is onto.

Remark: The above mapping g is called inverse of f and is denoted by f^{-1}. It is easy to see that f^{-1} will also be 1–1 onto.

We can restate the above theorem as:

Theorem 7: *A map f is invertible iff it is one-one onto.*

Remark: If g is a mapping such that *gof* is identity map, then g is called left inverse of f. Similarly, one can define right inverse of f.

If $f : X \to X$ has both right and left inverses then it is easily seen that the two are equal.

Problem 1: Let X be a non empty set. Show that $f : X \to X$ is one-one iff f has a left inverse.

Solution: Suppose f is one-one.

Let $x_0 \in X$ be any fixed element

Define $g : X \to X$, s.t.,

$g(x) = y$ if $\exists\ y \in X$ s.t., $f(y) = x$

$= x_0$ otherwise.

Suppose $g(x) = y$ and $g(x) = y'$, then $f(y) = x$ and $f(y') = x$, *i.e.*, $f(y) = f(y') \Rightarrow y = y'$ as f is 1–1 and so y is uniquely determined. Thus $g : X \to X$ is well defined mapping.

Conversely, let g be a left inverse of f

Let $f(x_1) = f(x_2)$

Then $x_1 = (gof)\,x_1 = g(f(x_1)) = g(f(x_2)) = (gof)\,x_2 = x_2$ or that f is 1–1.

Remark: One can show that f is onto iff it has a right inverse.

Problem 2: Let $f : \mathbf{Z} \to \mathbf{Z}$ be defined by

$f(x) = x$, if x is even

$= 2x - 1$ if x is odd

Show that f is 1–1 but not onto. Find a left inverse of f.

Solution: Suppose f is onto. Since $3 \in \mathbf{Z}$, it has a pre image. Let $f(x) = 3$. Then by definition of f, x cannot be even, *i.e.*, x is odd and thus $f(x) = 2x - 1 = 3 \Rightarrow x = 2$ which is a contradiction. Hence f is not onto.

Define now $g : \mathbf{Z} \to \mathbf{Z}$, s.t.,

$g(2x) = 2x$

$g(2x - 1) = x$

then $(gof)(2x) = g(f(2x)) = g(2x) = 2x$

$(gof)(2x - 1) = g(f(2x - 1)) = g(2(2x - 1) - 1) = 2x - 1$

i.e., g will be left inverse of f and by previous problem f is $1 - 1$.

Definition: Let $f : A \to B$ be a function. Let $X \subseteq A$ then we define $f(X) = \{f(x) \mid x \in X\}$, which is, of course, a subset of B, it is called image of X.

Again, if $Y \subseteq B$ then $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, which is a subset of A. (f^{-1} here is only a notation and not essentially the inverse function). It is called pre-image of Y.

Theorem 8: *Let $f : X \to Y$ be a function then*

(*i*) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$

(*ii*) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

(*iii*) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

(*iv*) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

(*v*) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

(*vi*) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$

where A_1, A_2 are subsets of X and B_1, B_2 are subsets of Y.

Proof: We leave it for the reader to try.

Theorem 9: *If $f : A \to B$, $g : B \to C$, $h : C \to D$ be maps then*

(*i*) $ho(gof) = (hog)of$

(*ii*) *If $i : A \to A$, $j : B \to B$ be identity maps then*
$foi = f$ *and* $jof = f$

Proof: (*i*) $ho(gof)$ and $(hog)of$ are both maps from $A \to D$

Since for any $x \in A$

$[(hog)of]\ x = (hog)(f(x)) = h\ (gf(x)))$

$[ho(gof)]\ x = h(gof)x) = h\ (g(f(x)))$

$h((gof)x) = (ho(gof))x$

we get result (*i*).

(*ii*) Since foi and f are both maps from $A \to B$ and also for any $x \in A$

$(foi)x = f(i(x)) = f(x)$, we find $foi = f$

Again, jof and f are maps from $A \to B$ and for any $x \in A$

$(jof)x = j(f(x)) = f(x)$

$\Rightarrow jof = f$

Cor.: If $f : A \to A$ be any mapping and $i : A \to A$ be identity map, then $foi = iof = f$.

Binary Compositions

If a, b are any two natural numbers then we know that $a + b$ is always a natural number and has a definite unique value. Thus + (addition) is an operation that *joins* two elements of **N** the set of naturals to give us a unique element of the same set **N**. This 'joining process' reminds us of the definition of a map. If we define a map

$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \text{ such that}$$
$$f((a, b)) = a + b$$

then the definition of mapping is satisfied and it is nothing but what we have mentioned above. Thus addition on natural numbers **N** is a map from $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$. We call such maps *Binary compositions* or *Binary operations*. In general a mapping $f : A \times A \to A$ is called a binary composition or binary operation in A (or on A). One could, of course, have more than one binary composition on the same set. In fact, multiplication is another binary composition on **N** whereas subtraction is not (why?). Subtraction would be binary composition on integers.

The mapping $f : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$, s.t.,

$$f(a, b) = \frac{ab}{2}$$

where **Q** = rationals is a binary composition on **Q**.

We sometimes express the above by saying that $*$ is a binary composition defined on **Q** by $a * b = \frac{ab}{2}$. In fact this notation is generally more convenient to use.

A binary composition $*$ is called commutative if

$$a * b = b * a \qquad \text{for all } a, b$$

and is called associative if

$$a * (b * c) = (a * b) * c \qquad \text{for all } a, b, c$$

Addition on natural numbers is both commutative and associative binary composition. If we define $*$ on **N** by $a * b = a^2 + b$ then it is easy to see that $*$ is a binary composition on **N** but is not associative.

If $*$ is a binary composition on a set X and $a, b \in X$ be any two elements, then $a * b \in X$, by definition. This fact is also sometimes expressed by saying that X is closed under $*$. The name is quite appropriate in as much as when two elements are 'joined' through the composition, the resulting element remains inside the set itself. In other words, the system remains *closed* under the operation. The concept of binary composition is most fundamental in the study of algebra and in fact forms a pedestal for the systems that we shall come across later in the text.

Exercises

1. Prove the following, for sets A, B, C

(i) $A \subseteq B, \quad B \subseteq C \Rightarrow A \subseteq C$

(ii) $A \subseteq B \Leftrightarrow A \cup B = B, \quad A \subseteq B \Leftrightarrow A \cap B = A$

(*iii*) If $A \cap B = A \cap C$ and $A \cup B = A \cup C$ then $B = C$

(*iv*) Show by examples that conclusion in (*iii*) fails if any of the two conditions does not hold.

2. $A \Delta B = (A - B) \cup (B - A)$ is called symmetric difference of two sets A and B. Show that it is equal to $(A \cup B) - (A \cap B)$. Show also that

$$A \Delta B = B \Delta A, \quad A \Delta (B \Delta C) = (A \Delta B) \Delta C.$$

3. Prove the results if theorem 1.

4. Let $A = \{1, 2, 3, 4\}$. Give example of a relation in A which is (*i*) equivalence relation, (*ii*) partial order relation, (*iii*) reflexive, not symmetric, (*iv*) symmetric, not reflexive, (*v*) reflexive, transitive not symmetric, (*vi*) transitive but not reflexive or symmetric.

5. Define a relation R on $\mathbf{Z}$ the set of integers by

xRy iff $x^2 + y^2$ is a multiple of 2. Show that R is an equivalence relation. Show further that it has only two equivalence classes.

6. Show by an example that we can have maps f and g such that fog is one-one (onto) whereas f or g is not one-one (onto).

7. If A be a finite set then show that any one-one map $f : A \to A$ is also onto.

8. Let $f : A \to B$ be a map between two finite sets, show that

(*i*) If f is 1-1 then $o(A) \leq o(B)$

(*ii*) If f is onto then $o(B) \leq o(A)$

(*iii*) If $o(A) = o(B)$ then f is 1-1 and onto iff it is either 1-1 or onto.

9. Let A and B be two sets with n elements each. Show that the number of one-one onto maps from A to B is $n!$.

10. Let $f : A \to B$ be an invertible mapping. Show that the inverse is unique.

11. Show that the set of all odd integers is not closed under subtraction. What can be said about set of all even integers?

12. Show that matrix addition and matrix multiplication are binary compositions on set of matrices.

Permutations

Let S be a non empty set. Any 1-1, onto mapping $f : S \to S$ is called a permutation (or a non singular transformation) of S. We shall use the notation $A(S)$ to denote the set of all permutations of S. To have some more information about $A(S)$ we first consider

Example 13: Let $S = \{1, 2, 3\}$

Consider the maps $f : S \to S$, s.t.,

$$f(1) = 2$$
$$f(2) = 3$$
$$f(3) = 1$$

and $g : S \to S$, s.t., $g(1) = 2$, $g(2) = 1$, $g(3) = 3$ then both f, g are permutations on S. Again the identity map $I : S \to S$, s.t., $I(x) = x$ for all $x \in S$ is also a permutation. It is easy

to check that the maps *fog*, *gof* and *fof* are also permutations of *X*. (In fact, we have already shown that φ, ψ 1-1 onto maps implies $\varphi o\psi$, $\psi o\varphi$ etc. are 1-1 onto in case these maps exist.) Hence the set $A(S)$ contains I, f, g, fog, gof, fof. Since the number of ways in which 3 elements can be connected with 3 elements in 1-1 onto way is 3! = 6, these would be all the members of $A(S)$.

We thus have a non-empty set $A(S)$ having these six members. In view of the results proved earlier we find

$$\varphi o(\psi o\eta) = (\varphi o\psi)o\eta \quad \text{for all } \varphi,\ \psi,\ \eta \in A(S)$$
$$\theta oI = Io\theta = \theta \quad \text{for all } \theta \in A(S)$$

Again as each one-one onto map is invertible, we notice each member of $A(S)$ has an inverse, which would also be one-one onto and hence be a member of $A(S)$.

All these properties taken together give us a system called a group, which we shall be discussing in the next chapter.

In fact, this particular $A(S)$ is also denoted by S_3 and is called *symmetric group* of degree 3. We have considered the set S having three elements. If the set S contains n elements, we have a similar situation and get $A(S)$ or S_n, which would finally turn out to be a group (to be called symmetric group of degree n). These groups are called *permutation groups* (or *transformation groups*). See ahead under groups.

Number of elements in S_n will be $\underline{\lfloor n}$ as number of 1-1 onto maps from $\{1, 2, \ldots\ldots n\}$ to itself is $\underline{\lfloor n}$. Notice there are n possible choices for selecting image of 1 under a 1-1 onto map. After selecting image of 1 we are left with $n - 1$ choices to select image of 2 and like this there are $n - 2$ choices left for image of 3. Proceeding this way we observe that S_n will have $n(n - 1)\ (n - 2)\ \ldots\ldots\ 2.1 = \underline{\lfloor n}$ members.

One could denote the elements of the set S by x_1, x_2, x_3 etc. instead of 1, 2, 3, but for convenience we use 1, 2, 3.

We now introduce a notation to represent permutations. Consider the above set $A(S) = S_3$.

The mapping f (as defined above) could be written as

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

where first row consists of all members of S and the second row consists of their respective images.

Similarly, $$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Again since *fog* will be given by

$$(fog)1 = f(g(1)) = f(2) = 3$$
$$(fog)2 = f(g(2)) = f(1) = 2$$
$$(fog)3 = f(g(3)) = f(3) = 1$$

we can write $fog = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

In fact, the computation as done above could be achieved through the product

$$fog = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

by starting from right bracket towards the first (left) bracket. For instance

$$1 \xrightarrow{g} 2,\ 2 \xrightarrow{f} 3 \qquad 2 \xrightarrow{g} 1,\ 1 \xrightarrow{f} 2 \qquad 3 \xrightarrow{g} 3,\ 3 \xrightarrow{f} 1$$

or that under fog $\quad 1 \to 3,\ 2 \to 2,\ 3 \to 1.$

In this manner we can compute the product of any number of permutations.

We simplify this notation a little further. Since in each representation, the first row is same we omit writing it and simply represent f by (123), fog by (13), g by (12) etc.

In f, $\quad 1 \to 2,\ 2 \to 3,\ 3 \to 1.$

In fog, $\quad 1 \to 3,\ 3 \to 1$. Since 2 is not mentioned it is understood $2 \to 2$.

Again in g, $\quad 1 \to 2,\ 2 \to 1$ and 3 remains fixed, *i.e.*, $3 \to 3$.

The computation of the product is also done similarly by starting from the right. For instance

$fog = (123)(12) = (13)$

In fact, all the members of S_3 in our new notation can be listed as I, (123), (12), (13), (23), (132).

Suppose now that $S = \{1, 2, 3, 4, 5, 6\}$

and $$f = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 3 & 5 & 6 & 1 & 4\end{pmatrix}$$

then in our single row representation f will be written as (1235)(46).

$1 \to 2,\ 2 \to 3,\ 3 \to 5$ and as $5 \to 1$ and 1 occurs at the first place, so we close the bracket. We start again by considering 4, the element which had not yet figured in the first bracket and find $4 \to 6$ & $6 \to 4$. Thus we get the second bracket (4 6). These brackets (1 2 3 5) and (4 6) are called cycles of the permutation. It is very clear from the example that either a permutation will be a cycle itself or we can write it as a product of cycles, where no element will be common in any two cycles, which will be called disjoint cycles. We formalize these results through the following theorems and definitions.

Theorem 10: *Let S be a non empty set and f a permutation of S. For a, b ∈ S, define a relation ~ on S by* $a \sim b \Leftrightarrow f^n(a) = b$ *for some integer n. This relation ~ is an equivalence relation.* [$f^n = fofof$ ..... *of n times*].

Proof: $a \sim a$ as $f^0(a) = i(a) = a$ where i or I is identity map.

$$a \sim b \Rightarrow \exists\ n,\ \text{s.t.},\ f^n(a) = b$$
$$\Rightarrow a = f^{-n}(b) \Rightarrow b \sim a$$

where f^{-n} the inverse of f^n exists as f is 1–1 onto.

Finally, $a \sim b,\ b \sim c \Rightarrow \exists$ integers m, n s.t.,

$$f^m(a) = b,\ f^n(b) = c$$

Clearly then $f^{m+n}(a) = (f_o^n f^m)\ a = f^n\ (f^m\ (a)) = f^n(b) = c$

$\Rightarrow a \sim c$

Hence ~ is an equicalence relation and thus partitions S into disjoint equivalence classes.

Remark: Many a time we write fg in place of fog, for convenience and thus $fof = ff = f^2$ etc.

Definition: The equivalence class of any element $a \in S$ is called *orbit* of a (under f).

Thus $cl(a) = \{x \in S \mid x \sim a\}$

$= \{f^n(a) \mid n \text{ integer}\}$ = orbit of a.

see page 155 also.

Theorem 11: *If S is a finite set and $f \in A(S)$ then $\exists$ a +ve integer m such that orbit of x is $\{x, f(x), f^2(x), \ldots\ldots, f^{m-1}(x)\}$.*

Proof: Since S is finite, $A(S)$ has finite number of elements.

As $f \in A(S)$, f^2, f^3, ... all are in $A(S)$ and as order of $A(S)$ is finite, after a certain stage some power of f will be identity of $A(S)$. Let m be the smallest +ve integer such that $f^m(x) = x$.

Now $x, f(x), f^2(x), \ldots., f^{m-1}(x)$ will all be distinct as if $f^i(x) = f^j(x)$ for some i, j, $0 \le i > j \le m-1$.

then $f^{i-j}(x) = x$

But $i - j < m$ leads to a contradiction to the choice of m. Hence $x, f(x), f^2(x), \ldots., f^{m-1}(x)$ are distinct elements of the orbit of x. To show the orbit contains no other elements suppose x' is any other element in the orbit, then $\exists$ some integer n s.t.,

$f^n(x) = x'$

But $n = mq + r$ for some integers q, r, where $0 \le r \le m-1$

$\Rightarrow x' = f^n(x) = f^{mq+r}(x) = f^r . f^{mq}(x) = f^r[f^{mq}(x)]$

$= f^r(x),\ 0 \le r \le m-1$

$\Rightarrow x'$ is one of the earlier members, proving our theorem.

Cyclic Permutations

Let S be a finite set. A permutation f of S is called a cyclic permutation or a cycle if $\exists$ elements $x_1, x_2, \ldots., x_n$ in S s.t.,

$$f(x_1) = x_2, f(x_2) = x_3, \ldots\ldots f(x_{n-1}) = x_n, f(x_n) = x_1$$

and all other elements remain fixed under f *i.e.*, $f(x) = x$ for all other $x \in S$.

We denote f by $(x_1\ x_2 \ldots.x_n)$ in that case and say it is a cycle of length n. It is also called n-cycle. In particular a cycle of length 2 is called a *transposition*.

Cycles of a Permutation

Suppose we have a permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 7 & 3 & 5 \end{pmatrix}$$

$= (124)(36)(57)$ then (124), (36), (57) are called cycles of the permutation f.

We formalise it in

Definition: Let S be a finite set and $x \in S$. Let $f \in A(S)$. We know $\exists$ a +ve integer m s.t., $x, f(x), f^2(x) \ldots f^{m-1}(x)$ are all distinct and $f^m(x) = x$. We call

$(x\ f(x)\ f^2(x) \ldots f^{m-1}(x))$ a cycle of f.

Example 14: Consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$

here, $f(1) = 8$, $f^2(1) = f(8) = 3$, $f^3(1) = 5$, $f^4(1) = 6$, $f^5(1) = 2$,

$f^6(1) = 7$, $f^7(1) = 1$

Thus (1835627) is a cycle of f.

Again $f(4) = 4$, $f^2(4) = 4$ etc. So (4) is another cycle of f.

Problem 3: *Find orbits and cycles of the permutation*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

Solution: Consider 1,

$$f(1) = 6, f^2(1) = 2, f^3(1) = 5, f^4(1) = 1$$

thus (1625) is a cycle and {1, 6, 2, 5} is orbit of 1, 6, 2, 5

Again, if we consider 3,

$$f(3) = 4, \quad f^2(3) = 3$$

thus (34) is a cycle and {3, 4} is orbit of 3 and 4.

Remark: Notice that an orbit is a set, members of which are the constituents of the corresponding cycle.

Theorem 12: *Let f be a non trivial permutation (i.e., different from identity) of $S = \{1, 2, \ldots\ldots n\}$. Then f can be represented as product of disjoint cycles each of length greater than or equal to 2. Also the representation is unique except for the order in which the cycles occur.*

Proof: Since f is non trivial there exists at least one orbit with more than one element. Let O_1, O_2, ... O_k be the orbits each with two or more elements. Any orbit we know is of the form $\{a, f(a), f^2(a), \ldots f^{m-1}(a)\}$ for some $a \in S$, and some $m > 1$. The corresponding cycle of this orbit is

$$(a\ f(a)\ f^2(a)\ \ldots\ f^{m-1}(a))$$

Let the corresponding cycles of the orbits $O_1, O_2, \ldots, O_k$ be $f_1, f_2, \ldots, f_k$.

We claim $f = f_1\ f_2\ \ldots\ f_k$

Let $x \in S$ be any element. If x belongs to a trivial orbit of f then $f(x) = x$ and x will not belong to any of $O_1, O_2, \ldots O_k$ (orbits are equivalence classes and thus distinct orbits have no elements in common). Thus x remains fixed under $f_1, f_2, \ldots f_k$ *i.e.*, $(f_1 f_2 \ldots f_k)x = x = f(x)$

Suppose now x belongs to one of $O_1, O_2, \ldots, O_k$ say $x \in O_t$ and suppose $O_t = \{a, f(a), f^2(a), \ldots, f^{m-1}(a)\}$

Then $x = f^p(a)$ for some $p \leq m - 1$

$$\Rightarrow f(x) = f(f^p(a)) = f^{p+1}(a)$$

Again $(f_1 f_2 \ldots f_k)\ x = f_t(x)$ as $x \in O_t$ means x remains fixed under every cycle other than f_t (by definition).

But $f_t(x) = f_t(f^p(a))$

$$= f^{p+1}(a)$$

Note $f_t = (a\ f(a)\ f^2(a)\ \ldots\ f^{m-1}(a))$

Thus $(f_1 f_2 \ldots f_k)\ x = f^{p+1}(a)$

or that $(f_1 f_2 \ldots f_k)\ x = f(x)$ for all x

$$\Rightarrow f = f_1\ f_2 \ldots f_k$$

That $f_1, f_2 \ldots, f_k$ are disjoint is clear as the corresponding orbits being equivalence classes are disjoint.

To prove uniqueness, suppose f is also equal to $g_1\ g_2 \ldots g_m$.

Let $g_1 = (i_1\ i_2\ \ldots\ i_r),\ \ i_1, i_2, \ldots, i_r \in S$

and $g = g_2\ g_3\ \ldots\ g_m$

Then $f = g_1 g$

clearly now $i_1, i_2, \ldots, i_r$ do not appear in any cycle in g. Thus

$$g(a) = a \quad \text{if } a = i_1, i_2, \ldots, i_r$$

and $f(a) = g_1(a)$ if $a = i_1, i_2, \ldots, i_r$

In other words $\{i_1, f(i_1), f^2(i_1), \ldots, f^{r-1}(i_1)\}$

$$= \{i_1, g_1(i_1), g_1^2(i_1), \ldots, g_1^{r-1}(i_1)\}$$

$$= \text{orbit of } f$$

$$\Rightarrow g_1 = f_t \text{ for some } t$$

So in this way for each $g_i\ \exists$ a corresponding f_j s.t., $g_i = f_j$.

Since $f = f_1 f_2 \ldots f_k = g_1 g_2 \ldots g_m$ we can cancel the equal ones on both sides, resulting into $k = m$ (for otherwise product of some cycles of length ≥ 2 is identity, which not true).

Hence uniqueness follows.

Disjoint Permutations

Two permutations f and g of a set S are called *disjoint* if (i) for any $x \in S$, $f(x) \neq x \Rightarrow g(x) = x$ and (ii) for any $x \in S$, $g(x) \neq x \Rightarrow f(x) = x$.

For instance, $f = (12)$ and $g = (13)$ are not disjoint in S_3 as $f(1) = 2$ and $g(1) = 3 \neq 1$.

Again in S_5, $f = (132)$, $g = (45)$ are disjoint.

Theorem 13: *Any two disjoint permutations commute.*

Proof: Let f and g be any two disjoint permutations of set S. We show $fog = gof$.

Let $x \in S$ be any element.

Suppose $f(x) \neq x$ then $g(x) = x$.

Let $f(x) = y$ then $y \neq x$.

Now $(fog)x = f(g(x)) = f(x) = y$.

Also $(gof)x = g(f(x)) = g(y) = y$

because if $g(y) \neq y$

then $f(y) = y$

$\Rightarrow f(y) = f(x)$

$\Rightarrow y = x$ (f being 1–1), a contradiction.

Hence $fog = gof$ for all $x \in S$ such that $f(x) \neq x$. Again if $x \in S$ be such that $f(x) = x$ then $g(x) \neq x$. Proceeding as above, we again get $fog = gof$ which proves the theorem.

In view of the results that we have proved we find any permutation can be expressed as a product of disjoint cycles. Note for instance,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 9 & 7 \end{pmatrix} = (1324)(56)(789)$$

Again any cycle (1234) can be written as (14)(13)(12)

i.e., it can be written as a product of transpositions and combining the two results we notice any permutation can be expressed as a product of transpositions (not essentially disjoint). Since (1234) can also be written (43)(42)(41), we find the representation as product of transpositions is not unique.

The above f can be expressed as

$$f = (14)(12)(13)(56)(79)(89)$$
$$= (14)(12)(13)(56)(79)(89)(12)(12) \text{ etc.}$$

Problem 4: *Show that inverse of* (1234) *is* (4321).

Solution: Although the result is clear by definition of inverse, we notice, if we multiply (1234) with (4321) in the way explained above then as

$$(1234)(4321) = I$$

we get $(1234)^{-1} = (4321)$

In fact for any cycle (123 ... n)

$$(123 \ldots\ldots n)^{-1} = (n\ n{-}1 \ldots\ldots 321)$$

Problem 5: *Find different powers of the cycle* (1234).

Solution: $(1234)^2 = (1234)(1234) = (13)(24)$

$(1234)^3 = (1234)(13)(24) = (1432)$

$(1234)^4 = (1234)(1432) = I.$

Problem 6: *Show that* $(ab)^2 = I$ *for any transposition* (ab).

Solution: Obvious.

Problem 7: *Show that* nth *power of an* n*-cycle is* I $(n = 1, 2, 3, \ldots)$.

Solution: One can proceed as in the previous problems.

Problem 8: *If* $f = (a_1\ b_1)(a_2\ b_2)(a_3\ b_3)(a_4\ b_4)$

then $f^{-1} = (a_4\ b_4)(a_3\ b_3)(a_2\ b_2)(a_1\ b_1)$

Solution: Consider the product

$$(a_1\ b_1)\ (a_2\ b_2)\ (a_3\ b_3)\ (a_4\ b_4)\ (a_4\ b_4)\ (a_3\ b_3)\ (a_2\ b_2)\ (a_1\ b_1)$$

which comes out to be I proving our assertion.

Theorem 14: *Suppose* f *is a permutation of a finite set* S*. Then in all expressions of* f *as product of transpositions, either the number of transpostions is always even or always odd.*

Proof: Suppose there exists a permutation f in S_n for which the theorem does not hold. Then we have two representations of f,

$$f = (a_1\ b_1)(a_2\ b_2) \ldots (a_n\ b_n)$$
$$f = (c_1\ d_1)(c_2\ d_2) \ldots (c_m\ d_m)$$

where n is even and m is odd.

Since $f^{-1} = (c_m\ d_m)(c_{m-1}\ d_{m-1}) \ldots (c_2\ d_2)(c_1\ d_1)$ we find

$$I = fo\ f^{-1} = (a_1\ b_1) \ldots (a_n\ b_n)(c_m\ d_m) \ldots (c_1\ d_1)$$
$$= (x_1\ y_1)(x_2\ y_2) \ldots (x_t\ y_t) \quad (\text{where } t = n + m = \text{odd})$$

Again as any transposition $(\alpha\beta) = (1\alpha)(1\beta)(1\alpha)$ the above expression can be written as

$$I = (1x_1)(1y_1)(1x_1)(1x_2)(1y_2)(1x_2) \ldots (1x_t)(1y_t)(1x_t)$$

which would still have odd number of transpositions in the R.H.S.

Consider any $(1u)$ in the R.H.S. Since L.H.S. is identity $(1u)$ must occur twice (or even number of times) in R.H.S. so as to have 'identity effect' ultimately.

Note $u \to 1$ then $1 \to u$ will give $u \to u$. Thus each transposition in the R.H.S. occurs even number of times meaning that R.H.S. should have even number of transpositions, a contradiction, proving our theorem.

Definition: A permutation is called *even* (*odd*) permutation if it can be expressed as a product of even (odd) number of transpositions.

In view of the previous theorem, we need look for only one representation to identify even or odd permutations.

The following results are rather trivially proved

(*a*) *The product of two even permutations is even* as sum of two even numbers is even.

(*b*) *The product of two odd permutations is even* as sum of two odd numbers is even.

(*c*) *The product of an even and an odd permutation is odd* as sum of an even and an odd number is odd.

(*d*) *Inverse of an even* (*odd*) *permutation is even* (*odd*). Indeed

$$f = (a_1\ b_2)\ (a_2\ b_2)\ \ldots\ (a_n\ b_n).$$

$$\Rightarrow\quad f^{-1} = (a_n\ b_n)\ (a_{n-1}\ b_{n-1})\ \ldots\ (a_1\ b_1)$$

(*e*) *Identity permutation is always even.*

Example 15: The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 5 & 6 & 7 & 2 \end{pmatrix}$$

$$= (13)(24567)$$

$$= (13)(27)(26)(25)(24) \text{ is an odd permutation,}$$

whereas the permutation (12)(1576) is even as

$$(12)(1576) = (12)(16)(17)(15).$$

Problem 9: *Show that a cycle of even length is an odd permutation and a cycle of odd length is an even permutation.*

Solution: Consider the cycle (1234) of even length. Since (1234) = (14)(13)(12) which is odd permutation, our result is proved for a cycle of length 4. It is now trivial that the result is generalised to any cycle. Indeed

$$(123\ldots n) = (1n)(1n{-}1)\ \ldots\ (13)(12)$$

proves our assertion.

Problem 10: *Compute* $a^{-1}ba$ *where* $a = (135)(12)$, $b = (1579)$.

Solution: We have $a = (135)(12)$

$$= (1235)$$

$$\Rightarrow\ a^{-1} = (5321)$$

Thus $\quad a^{-1}ba = (5321)(1579)(1235)$

$$= (3795).$$

Theorem 15: *Let* $\sigma = (a_1\ldots a_{n1})\ldots\ldots(b_1\ldots b_{n_k})$ *be a permutation of a finite set S, written as product of disjoint cycles. Let* $o(S) = n$ *and* $n_1 + \ldots + n_k = n$. *Then*

$$\theta\ \sigma\ \theta^{-1} = (\theta(a_1)\ \ldots\ \theta(a_{n1}))\ \ldots\ldots\ (\theta(b_1)\ \ldots\ \theta(b_{n_k}))$$

for all $\theta \in S_n$.

Proof: Let $S = \{a_1,..., a_{n1},..., b_1,..., b_{n_k}\}$

Then $\theta(S) = \{\theta(a_1),..., \theta(a_{n1}),..., \theta(b_1),..., \theta(b_{n_k})\}$

Since $\theta : S \to S$ is 1–1, all elements in $\theta(S)$ are distinct. Also θ is onto $\Rightarrow \theta(S) = S$.

Now
$$\begin{aligned}(\theta\,\sigma\,\theta^{-1})(\theta\, x_i) &= (\theta\,\sigma)(\theta^{-1}\,\theta\, x_i)\\ &= (\theta\,\sigma)(x_i)\\ &= \theta(\sigma(x_i))\\ &= (\theta(x_{i+1}))\end{aligned}$$

$\therefore\ \theta\,\sigma\,\theta^{-1}$ takes any element $\theta(x_i)$ of $\theta(S) = S$ to $\theta(x_{i+1})$ and so does the mapping

$$(\theta a_1 \ldots \theta a_{n1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$$

$\therefore$
$$\theta\,\sigma\,\theta^{-1} = (\theta a_1 \ldots \theta a_{n1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$$

Remark: It follows from the above that the cycle structure of σ is same as that of $\theta\,\sigma\,\theta^{-1}$ for all $\theta \in S_n$ as σ has k cycles of length $n_1,..., n_k$ and same is true for $\theta\,\sigma\,\theta^{-1}$. *Note that σ must be written as the product of disjoint cycles.*

e.g., take $\theta = (1234)$, $\sigma = (12)(23)$

Then $\theta\,\sigma\,\theta^{-1} = \theta(12)\,(23)\theta^{-1} \neq (\theta 1\ \theta 2)\,(\theta 2\ \theta 3) = (13)(34)$

as R.H.S. (13)(34) takes 4 to 1 and $\theta(12)(23)\theta^{-1}$ takes 4 to 2.

Problem 11: *Let $S = \{1, 2, 3, 4\}$. Find all permutations θ of S such that* $\theta(12)(34)\theta^{-1} = (13)(24)$.

Solution: Now $\theta(12)(34)\theta^{-1} = (\theta 1\ \theta 2)\,(\theta 3\ \theta 4)$

$\therefore$ $(\theta 1\ \theta 2)\,(\theta 3\ \theta 4) = (13)(24)$

Again $(13)(24) = (31)(24) = (13)(42) = (31)(42)$

$(24)(13) = (24)(31) = (42)(13) = (42)(31)$

So, θ has 8 choices, namely

$\theta 1 = 1,\ \theta 2 = 3,\ \theta 3 = 2,\ \theta 4 = 4$, *i.e.*, $\theta = (23)$

$\theta 1 = 3,\ \theta 2 = 1,\ \theta 3 = 2,\ \theta 4 = 4$, *i.e.*, $\theta = (132)$

$\theta 1 = 1,\ \theta 2 = 3,\ \theta 3 = 4,\ \theta 4 = 2$, *i.e.*, $\theta = (234)$

$\theta 1 = 3,\ \theta 2 = 1,\ \theta 3 = 4,\ \theta 4 = 2$, *i.e.*, $\theta = (1342)$

$\theta 1 = 2,\ \theta 2 = 4,\ \theta 3 = 1,\ \theta 4 = 3$, *i.e.*, $\theta = (1243)$

$\theta 1 = 2,\ \theta 2 = 4,\ \theta 3 = 3,\ \theta 4 = 1$, *i.e.*, $\theta = (124)$

$\theta 1 = 4,\ \theta 2 = 2,\ \theta 3 = 1,\ \theta 4 = 3$, *i.e.*, $\theta = (143)$

$\theta 1 = 4,\ \theta 2 = 2,\ \theta 3 = 3,\ \theta 4 = 1$, *i.e.*, $\theta = (14)$

Remark: As in the previous problem, we sometimes take the liberty of writting θx for $\theta(x)$.

Problem 12: *Show that there does not exist a permutation* θ *of* $S = \{1, 2, ..., 8\}$ *such that*

$$\theta(123)\theta^{-1} = (13)(578).$$

Solution: Now $\theta(123)\theta^{-1} = (\theta(1)\theta(2)\theta(3))$ and it does not have cycle of length 2 while (13)(578) has a cycle of length 2. So, there does not exist θ such that

$$\theta(123)\theta^{-1} = (13)(578).$$

Problem 13: *Let* $A(S)$ *= set of all permutations on a set S. Show that either all permutations are even or exactly half are even.*

Solution: If all permutations are even there is nothing to prove. Suppose now $A(S)$ has odd as well as even permutations and $\exists$ m even and n odd permutations. Then $m + n = o(A(S))$.

Let $e_1, e_2, ..., e_m$ be distinct even permutations. If a be any transposition then $ae_1, ae_2, ..., ae_m$ are odd and will be distinct $[ae_i = ae_j \Rightarrow e_i = e_j]$.

Since $\exists$ in all, n odd permutations

$$m \leq n$$

Similarly interchanging roles of m, n we'll get $n \leq m$ and hence $m = n$.

Remark: Since identity is even permutation, all members of $A(S)$ cannot be odd permutations.

Aliter: Let E and O be the sets of even and odd permutations of $A(S)$ respectively.

Define $\theta : E \to O$, s.t.,

$\theta(\sigma) = \sigma(12)$

Then as σ is even, $\sigma(12)$ will be odd.

Also, $\sigma = \eta \Rightarrow \sigma(12) = \eta(12) \Rightarrow \theta(\sigma) = \theta(\eta)$

Showing that θ is well difined.

Again, $\theta(\sigma) = \theta(\eta) \Rightarrow \sigma(12) = \eta(12)$

$\Rightarrow \sigma(12)(12) = \eta(12)(12)$

$\Rightarrow \sigma = \eta$

i.e., θ is 1–1.

Also for any $\sigma \in O$, σ will be odd and thus $\sigma(12)$ will be even and $\theta(\sigma(12)) = \sigma(12)(12) = \sigma$

Shows θ is onto.

Hence $o(E) = o(O)$.

Exercises

1. Find the orbits and cycles of the set $S = \{1,2,3,4,5,6,\}$ under the following permutations

$$(i)\begin{pmatrix}1&2&3&4&5&6\\2&1&5&6&4&3\end{pmatrix},\ (ii)\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix},\ (iii)\begin{pmatrix}1&2&3&4&5&6\\2&3&1&6&5&4\end{pmatrix}$$

2. Express the following permutations as product of disjoint cycles

(*i*) (123)(234)(456)(67)

(*ii*) (12)(13)(14)(15)(16)

(*iii*) (24)(26)(28)(13)(15)(17)

3. Find out which of the following are even (odd) permutations

(*i*) (123) (12)

(*ii*) (12345) (123) (45)

(*iii*) (12) (14) (153)

4. Express the following permutations as product of transpositions

(*i*) (123 .....*n*)

(*ii*) (123)(4576)

(*iii*) (24)(345)

5. Find the orbits of all elements under the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 6 & 4 & 5 & 9 & 7 & 8 \end{pmatrix} \text{ in } S_9.$$

6. Show that $(ab)^i = a^i b^i$ holds for all a, b in S_3 where $i = 6, 7$ but it does not hold for $i = 8$.

(See remark after Problem 3 Page 58).

Some Results from Number Theory

In this section we discuss a few results pertaining to numbers although we do not plan to go through their axiomatic construction.

Definition: A non zero integer a is said to divide an integer b if $b = ac$ for some integer c and we express it as $a \mid b$.

The following results can then be proved

(*i*) $a \mid b,\ b \mid c$ then $a \mid c$

(*ii*) $a \mid b,\ a \mid c$ then $a \mid b + c$

(*iii*) $a \mid 0,\ a \mid a$

We now prove a well known result through

Theorem 16: (Euclid's Algorithm)

Let $k > 0$ be an integer and j be any integer. Then $\exists$ unique integers q and r such that $j = kq + r$, where $0 \le r < k$.

Proof: Let $S = \{j - kq \mid q \text{ is an integer}, j - kq \ge 0\}$.

Then $S \neq \varphi$, as take $q = -|j|$.

Now when $j > 0$, then $j - kq = j + kj > 0 \Rightarrow j - kq \in S$

and if $j < 0$, then $j - kq = j - kj$

$= j\,(1 - k) \ge 0$

$$\Rightarrow j - kq \in S$$

$j = 0$, then $j - kq = j - k.0$

$$= j = 0$$

$$\Rightarrow j - kq \in S$$

In any case, $S \neq \varphi$.

By well ordering principle, S has least element, say $r \in S$.

$r \in S \Rightarrow r = j - kq$ for some integer q

$\Rightarrow j = kq + r$. Also $r \geq 0$

Suppose $r \geq k$

Then $j - kq \geq k$

$\Rightarrow j - k(q + 1) \geq 0$

$\Rightarrow j - k(q + 1) \in S$

But $j - k(q + 1) < j - kq$ as $k > 0$, contradicting $r = j - kq$ is least element of S.

$\therefore 0 \leq r < k$.

Uniqueness: Suppose $j = kq + r = kq' + r'$, $0 \leq r, r' < k$. Then $k(q - q') = r' - r$. Suppose $r' > r$. Then $r' - r > 0$. But $k \mid r' - r \Rightarrow k \leq r' - r$. Since $r, r' < k$, $r' - r < k$, a contradiction.

$\therefore r' \not> r$. Similarly $r \not> r'$ $\therefore r = r' \Rightarrow kq = kq' \Rightarrow q = q'$.

An important application of this result is the *basis representation theorem*.

Theorem 17: (Basis Representation Theorem).

Let $b > 0$ be an integer and let $N > 1$ be any integer. Then N can be expressed as

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b + a_0,$$

where m and a_is are integers such that $m > 0$ and $0 \leq a_i < b$. Also then these a_is are uniquely determined. (b is called base of representation of N).

Proof: If $N < b$,

then $N = 0b^m + 0b^{m-1} + \ldots + 0b + N$

is the representation of N as required.

Let $N \geq b > 0$. By Euclid's algorithm $\exists$ integers q, r such that

$$N = bq + r, \quad 0 \leq r < b \leq N$$

Since $N - r > 0$, $bq > 0 \Rightarrow q > 0$ as $b > 0$.

If $q < b$, then $N = bq + r$ is the required representation of n.

If $q \geq b > 0$, then as above by Euclid's algorithm $\exists$ integers q_1, r_1 such that

$$q = bq_1 + r_1, \quad 0 \leq r_1 < b \leq q$$

Since $q - r_1 > 0$, $bq_1 > 0 \Rightarrow q_1 > 0$ as $b > 0$.

Now $N = bq + r = b(bq_1 + r_1) + r$

$\Rightarrow N = b^2 q_1 + br_1 + r$

If $q_1 < b$, then it is the required representation of N. In this way, after finite number of steps, we shall get

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b + a_0$$

where $a_i's$ are integers such that

$$0 \le a_i < b \quad \text{for all } i = 1, \ldots, m.$$

Uniqueness of $a_i s$ follows as:

Suppose $N = c_m b^m + c_{m-1} b^{m-1} + \ldots + c_1 b + c_0$ where each c_i is an integer such that $0 \le c_i < b$. We can choose same m in both the representations of N because if one representation of N has lesser terms we can always insert zero coefficients and thus make the number of terms to be same.

$\therefore$ $0 = (a_m - c_m)b^m + \ldots + (a_1 - c_1)b + (a_0 - c_0)$

Let $a_i - c_i = d_i$.

Then $d_m b^m + \ldots + d_1 b + d_0 = 0$.

We have to show that $d_i = 0$ for all i.

Suppose for some i, $d_i \neq 0$. Let k be the least subscript such that $d_k \neq 0$

Then $d_k b^k + d_{k+1} b^{k+1} + \ldots + d_m b^m = 0$

$\Rightarrow d_k b^k = -(d_{k+1} b^{k+1} + \ldots + d_m b^m)$

$\Rightarrow d_k = -(d_{k+1} b + d_{k+2} b^2 + \ldots + d_m b^{m-k})$

$\Rightarrow d_k = -b(d_{k+1} + d_{k+2} b + \ldots + d_m b^{m-k-1})$

$\Rightarrow b \mid d_k$

$\Rightarrow b \mid \mid d_k \mid$

$\Rightarrow b \le \mid d_k \mid$

But $a_k, c_k < b \Rightarrow \mid a_k - c_k \mid < b$

$\Rightarrow \mid d_k \mid < b,$

So, we get a contradiction

$\therefore$ $d_i = 0$ for all $i = 1, \ldots, m$

$\therefore$ $a_i = c_i$ for all $i = 1, \ldots, m$

Note: When the integer N is expressed as

$$N = a_m b^m + \ldots + a_1 b + a_0, \quad 0 \le a_i < b,$$

we write $N = (a_m a_{m-1} \ldots a_1 a_0)b$

and say that N is $a_m a_{m-1} \ldots a_0$ to the base b.

For example,

$132 = 1.10^2 + 3.10 + 2$ (Here base is 10)

Then as above

$132 = (132)_{10}$

So, numbers that we usually write are to the base 10.

Again, if we want to write 132 to the base 2, we first write

$1\ 3\ 2 = 2^7 + 2^2 = 2^7 + 0.2^6 + 0.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 0.2 + 0$

and by basis representation theorem, then

$$132 = (10000100)_2$$

Problem 14: *If a, b are integers with $b \neq 0$, show that there exist unique integers q and r satisfying $a = bq + r$ where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$.*

Solution: By Euclid's algorithm, there exist unique integers q', r' such that

$$a = q'|b| + r', \quad \text{where } 0 \leq r' < |b|$$

(as $|b| > 0$ when $b \neq 0$).

Case 1: $0 \leq r' \leq \frac{1}{2}|b|$

Take $r' = r$, $q' = q$ (if $b > 0$), $q' = -q$ (if $b < 0$)

Since $-\frac{1}{2}|b| < 0 \leq r' = r \leq \frac{1}{2}|b|$,

$$-\tfrac{1}{2}|b| < r \leq \tfrac{1}{2}|b|$$

Also $a = q'|b| + r'$ becomes

$a = qb + r$ if $b > 0$

and $a = (-q)(-b) + r$ if $b < 0$

$= qb + r$

where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$

Case 2: $\frac{1}{2}|b| < r' < |b|$

Take $r' = r + |b|$

$q' = q - 1$ if $b > 0$

$= -q - 1$ if $b < 0$

Now $\frac{1}{2}|b| < r' = r + |b|$

$\Rightarrow -\frac{1}{2}|b| < r$

Also $r' = r + |b| < |b|$

$\Rightarrow r < 0 < \frac{1}{2}|b|$

$\therefore -\frac{1}{2}|b| < r < \frac{1}{2}|b|$

Again $a = |b|\, q' + r'$ becomes

$a = b(q - 1) + r + b$ when $b > 0$

$= bq + r$

Also, when $b > 0$, $a = |b|q' + r'$ becomes

$$a = -b(-q - 1) + r - b$$
$$= bq + r$$

where $-\frac{1}{2}|b| < r < \frac{1}{2}|b|$.

The Greatest Common Divisor

A special case in Euclid's algorithm arises when the remainder is zero. We discuss it in this section.

Definition: An integer $d > 0$ is called greatest common divisor (g.c.d.) of two integers a, b (non zero) if

(i) $d|a$, $d|b$

(ii) If $c|a$, $c|b$ then $c|d$

We write d = g.c.d.(a, b) or simply $d = (a, b)$.

Remarks:

(i) $(a, 0) = |a|$, $(0, b) = |b|$

Clearly, $|a|\,|a$, $|a|\,|0$

If $c|a$, then $c|\,|a| \Rightarrow (a, 0) = |a|$

Similarly $(0, b) = |b|$

(ii) If $a|b$, then $(a, b) = |a|$

$|a|\,|a$, and $a|b \Rightarrow |a|\,|b$

If $c|a$, $c|b$, then $c|\,|a|$

$\therefore (a, b) = |a|$

(iii) g.c.d. of a and b does not depend on signs of a and b

i.e., $(a, b) = (-a, b) = (a, -b) = (-a, -b)$

Let $d = (a, b)$. Then $d|a$, $d|b \Rightarrow d|-a$, $d|b$

$c|-a$, $c|b \Rightarrow c|a$, $c|b \Rightarrow c|d$

$\therefore d = (-a, b)$. Similarly for others.

We now show the existence and uniqueness of g.c.d. of integers a and b.

Theorem 18: *Let a, b be two integers. Suppose either $a \neq 0$ or $b \neq 0$. Then $\exists$ greatest common divisor d of a, b such that*

$$d = ax + by \text{ for some integers } x, y.$$

d is uniquely determined by a and b.

Proof: Let $S = \{au + bv \mid u, v \text{ are integers and } au + bv > 0\}$.

If $a > 0$, then $a = a.1 + b.0 > 0 \Rightarrow a \in S$.

If $a < 0$, then $-a = a(-1) + b.0 > 0 \Rightarrow -a \in S$.

Similarly, if $b > 0$ then $b \in S$ and if $b < 0$ then $-b \in S$. Since one of a and b is non zero, either $\pm a \in S$ or $\pm b \in S$. In any case $S \neq \varphi$.

By well ordering principle S has a least element, say d.

Now $d \in S \Rightarrow d = ax + by$ for some integers x and y. Also $d > 0$.

Let $a = dq + r$, $0 \leq r < d$.

Let $r \neq 0$. Since $r = a - dq$

$= a - (ax + by)q$

$= a(1 - xq) + b(-yq) > 0$

$\Rightarrow r \in S$.

But $r < d$, contradicting the fact that d is least element of S. So, $r = 0$.

Therefore, $a = dq \Rightarrow d \mid a$.

Similarly, $d \mid b$.

Suppose, $c \mid a,\ c \mid b \Rightarrow c \mid ax + by = d$.

So, d is a greatest common divisor of a and b.

If d' is also greatest common divisor of a and b, then $d' \mid a, d' \mid b, \Rightarrow d \mid d'$ Similarly, $d \mid a, d \mid b \Rightarrow d' \mid d$. Since $d, d' > 0$, $d = d'$. So d is uniquely determined by a and b.

Remark: x and y in above theorem need not be unique.

For, $d = ax + by$

$\Rightarrow d = a(x - b) + b(a + y)$

If $x - b = x$, $a + y = y \Rightarrow b = 0 = a$, which is not true. So either

$x - b \neq x$ or $a + y \neq y$.

Definition: If g.c.d.$(a, b) = 1$, then a and b are said to be *relatively prime* or *coprime.*

Cor. 1: Two integers a, b are relatively prime if and only if $\exists$ integers x, y such that $ax + by = 1$.

Proof: Suppose a, b are relatively prime. Then g.c.d.$(a, b) = 1$. By above theorem $\exists$ integers x, y such that $ax + by = 1$.

Conversely, let $ax + by = 1$ for some integers x, y. Let d = g.c.d.(a, b). Then $d \mid a, d \mid b \Rightarrow d \mid ax, d \mid by \Rightarrow d \mid ax + by = 1 \Rightarrow d = 1$.

So, a, b are relatively prime.

Cor. 2: If g.c.d.$(a, b) = d$, then g.c.d.$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: g.c.d.$(a, b) = d$

$\Rightarrow \exists$ integers x, y such that

$d = ax + by$

$\Rightarrow 1 = \frac{a}{d}x + \frac{b}{d}y$

$$\Rightarrow \text{ g.c.d. } \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \text{ by Cor 1.}$$

Cor. 3: If $a \mid bc$, with g.c.d.$(a, b) = 1$, then $a \mid c$

Proof: g.c.d.$(a, b) = 1 \Rightarrow \exists$ integers x, y s.t.,

$$ax + by = 1 \Rightarrow acx + bcy = c$$

Now $\quad a \mid ac, a \mid bc \Rightarrow a \mid acx, a \mid bcy$

$$\Rightarrow a \mid acx + bcy = c$$

Cor. 4: If g.c.d.$(a, b) = 1$ and g.c.d.$(a, c) = 1$, then g.c.d.$(a, bc) = 1$.

Proof: Since g.c.d.$(a, b) = 1$, $\exists$ integers x, y such that $ax + by = 1$. Also, g.c.d.$(a, c) = 1$, $\exists$ integers u, v such that $au + cv = 1$.

$$\therefore \quad 1 = (ax + by)(au + cv)$$

$$= a(axu + cxv + byu) + bc(yv)$$

By Cor. 1, g.c.d.$(a, bc) = 1$.

We now give a practical method of finding greatest common divisor of two integers. We first prove the following result.

Lemma: If $a = bq + r$, then g.c.d.(a, b) = g.c.d.(b, r).

Proof: Let g.c.d.$(a, b) = d$.

Then $d \mid a, d \mid b \Rightarrow d \mid a, d \mid bq \Rightarrow d \mid a - bq = r$. Suppose $c \mid b, c \mid r$.

Then $c \mid bq$, $c \mid r \Rightarrow c \mid bq + r \Rightarrow c \mid a$, $c \mid b \Rightarrow c \mid d$. Thus d = g.c.d. (b, r).

Let a, b be two integers.

Since g.c.d.(a, b) = g.c.d.$(|a|, |b|)$, let $a \geq b > 0$.

Let $a = bq_1 + r_1$, $0 \leq r_1 < b$.

If $r_1 = 0$, then $b \mid a$ and g.c.d.$(a, b) = b$.

Let $r_1 \neq 0$. Divide b by r_1 to get integers q_2 and r_2 s.t.,

$$b = r_1 q_2 + r_2, \; 0 \leq r_2 < r_1$$

If $r_2 = 0$, then g.c.d.$(b, r_1) = r_1$ and so by above lemma, g.c.d.$(a, b) = r_1$

If $r_2 \neq 0$, then proceed as above till we get remainder as zero,

We have

$$a = q_1 b + r_1, \qquad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2$$

$$\cdots\cdots\cdots$$

$$r_{n-2} = q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

By above lemma,

$$\text{g.c.d.}(a, b) = \text{g.c.d.}(b, r_1) = \ldots\ldots = \text{g.c.d.}(r_n, 0) = r_n$$

So, last remainder r_n is g.c.d. of a and b.

For example, to determine g.c.d.(56, 72), we divide 72 by 56 to get,

$$72 = 56 + 16$$
$$56 = 16 \times 3 + 8$$
$$16 = 8 \times 2 + 0.$$

Since last non zero remainder is 8, g.c.d.(56, 72) = 8.

Also,
$$\begin{aligned} 8 &= 56 - 16 \times 3 \\ &= 56 - (72 - 56) \times 3 \\ &= 56 \times (4) + 72\ (-3) \\ &= 56x + 72y \text{ where } x = 4,\ y = -3 \end{aligned}$$

which shows us the way to find x, y s.t.,

g.c.d. $(a, b) = ax + by$

Theorem 19: *Let* $k > 0$. *Then* g.c.d.$(ka, kb) = k$ *g.c.d.*(a, b).

Proof: Let g.c.d.$(a, b) = d$

Then $d \mid a,\ d \mid b \Rightarrow kd \mid ka,\ kd \mid kb$

Also $\exists$ integers x, y s.t.,

$$d = ax + by$$
$$\Rightarrow kd = kax + kby$$

Let $c \mid ka,\ c \mid kb$ then $c \mid kax,\ c \mid kby$

$$\Rightarrow c \mid kax + kby = kd$$
$$\Rightarrow \text{g.c.d. } (ka, kb) = kd = k\ g.c.d.\ (a, b)$$

(Note, as $k > 0$, $d > 0$ we get $\Rightarrow kd > 0$)

Cor.: For any integer $k \neq 0$, g.c.d. $(ka, kb) = |k|$ g.c.d.(a, b).

Proof: For $k > 0$, result follows form above theorem.

Let $k < 0$. Then g.c.d.(ka, kb)

$$= \text{g.c.d.}(-ka, -kb)$$
$$= -k \text{ g.c.d.}(a, b) \text{ by above theorem}$$
$$= |k| \text{ g.c.d.}(a, b)$$

Definition: The *least common multiple* of two non zero integers a and b, denoted by l.c.m.(a, b) is the positive integer m s.t.,

(*i*) $a \mid m,\ b \mid m$

(*ii*) if $a \mid c,\ b \mid c$, with $c > 0$, then $m \mid c$.

Theorem 20: *For positive integers a and b*

$$\text{g.c.d.}(a, b) \times \text{l.c.m.}(a, b) = ab$$

Proof: Let d = g.c.d.(a, b)

Now $\quad \dfrac{ab}{d} = a.\dfrac{b}{d} \Rightarrow a \left| \dfrac{ab}{d} \right.$ as $\dfrac{b}{d}$ is integer

Also $\quad \dfrac{ab}{d} = b.\dfrac{a}{d} \Rightarrow b \left| \dfrac{ab}{d} \right.$ as $\dfrac{a}{d}$ is integer

Let $m = \dfrac{ab}{d}$, then $a \mid m$ and $b \mid m$

Suppose now $a \mid c$, $b \mid c$. Since $(a, b) = d$, $\exists$ integers x, y s.t., $d = ax + by$.

$\therefore \quad \dfrac{c}{m} = \dfrac{cd}{ab} = \dfrac{c(ax+by)}{ab} = \left(\dfrac{c}{b}\right)x + \left(\dfrac{c}{a}\right)y = \text{integer}$

$\Rightarrow m \mid c.$

Thus m = l.c.m. $(a, \ b)$, *i.e.*, $\dfrac{ab}{d}$ = l.c.m. $(a, \ b)$

or that ab = g.c.d. $(a, \ b) \times$ l.c.m. $(a, \ b)$.

Problem 15: *Let* g.c.d. $(a, \ b) = 1$.

Show that g.c.d.$(a + b, \ a^2 - ab + b^2) = 1$ *or* 3.

Solution: Let g.c.d.$(a + b, \ a^2 - ab + b^2) = d$

Then $\quad d \mid a + b, \ d \mid a^2 - ab + b^2$

$\Rightarrow d \mid (a + b)^2 = a^2 + b^2 + 2ab, \ d \mid a^2 - ab + b^2$

$\Rightarrow d \mid 3ab$

Let $\quad$ g.c.d.$(d, \ a) = e$

Then $\quad e \mid d \mid a + b \Rightarrow e \mid a + b$ and $e \mid a$

$\therefore \quad e \mid (a + b) - a = b$

So, $\quad e \mid$ g.c.d.$(a, \ b) = 1 \Rightarrow e = 1$

$\therefore \quad$ g.c.d.$(d, \ a) = 1$

Similarly, $\quad$ g.c.d.$(d, \ b) = 1$

$\therefore \quad d \mid 3 \Rightarrow d = 1$ or 3.

Problem 16: *Let* g.c.d.$(a, b) = 1$. *Show that* g.c.d.$(a^n, b^n) = 1$ *for every integer* $n \geq 1$.

Solution: Since g.c.d. $(a, \ b) = 1$, $\exists$ integers x, y such that $ax + by = 1$.

$\Rightarrow (ax + by)(ax + by) = 1$

$\Rightarrow a^2x^2 + 2abxy + by^2 = 1$

$\Rightarrow a^2x^2 + b(2axy + y^2) = 1$

$\Rightarrow$ g.c.d.$(a^2, b) = 1$

In this way we will get

g.c.d.$(a^n, b) = 1$ or g.c.d.$(b, a^n) = 1$

Proceeding as above, we get

$$\text{g.c.d.}(b^n, a^n) = 1$$

Definition: By a Linear Diophantine equation we mean an equation $ax + by = c$ in two unknowns x and y, where a, b, c are given integers and one of a, b is not zero. The name is due to the mathematician Diophantus. A natural question arises as to when would such an equation have a solution? The answer is provided by

Theorem 21: *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ where d = g.c.d. (a, b). If x_0, y_0 is a particular solution, then the other solutions are given by*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

for varying integer t.

Proof: Suppose $ax + by = c$ has a solution.

Let $x = x_0, y = y_0$ be a solution.

Then $ax_0 + by_0 = c$. Let $d = \text{g.c.d.}(a, b)$.

$$\therefore \quad d \mid a, d \mid b \Rightarrow d \mid ax_0, d \mid by_0$$
$$\Rightarrow d \mid ax_0 + by_0 = c$$

Conversely, let $d \mid c$. Let $c = dk$.

Since d = g.c.d. (a, b), $\exists$ integers x_0, y_0 s.t.,

$$ax_0 + by_0 = d \Rightarrow a(x_0k) + b(y_0k) = dk = c$$
$$\Rightarrow ax + by = c \text{ has a solution } x = x_0k, \quad y = y_0k.$$

To prove the second assertion, let x_0, y_0 be a given solution of $ax + by = c$.

Let x', y' be any solution of $ax + by = c$.

$$\therefore \quad ax_0 + by_0 = ax' + by' = c$$
$$\Rightarrow a(x_0 - x') = b(y' - y_0)$$
$$\Rightarrow \frac{a}{d}(x_o - x') = \frac{b}{d}(y' - y_0), \text{ where } d = \text{g.c.d. } (a, b)$$
$$\Rightarrow \frac{b}{d} \left| \frac{a}{d}(x_0 - x') \right.$$

Since $\text{g.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

$$\frac{b}{d} | x_0 - x' \Rightarrow \frac{b}{d} | x' - x_0$$
$$\Rightarrow x' - x_0 = \frac{b}{d}t, \qquad t \text{ is an integer}$$

$$\Rightarrow \quad x' = x_0 + \frac{b}{d}t \quad \Rightarrow \quad \frac{a}{d}\frac{b}{d}t = \frac{b}{d}(y_0 - y')$$

$$\Rightarrow \quad \frac{a}{d}t = y_0 - y' \quad \Rightarrow \quad y' = y_0 - \frac{a}{d}t$$

It can be easily seen that for all values of t, $x' = x_0 + \frac{b}{d}t, y' = y_0 - \frac{a}{d}t$ is a solution of $ax + by = c$ as

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$

$$= ax_0 + by_0 = c.$$

Problem 17: *Determine all the solutions in the integers of the following Diophantine equation* $56x + 72y = 40$.

Solution: We first find g.c.d.(56, 72).

Now $72 = 56 + 16$

$56 = 3 \times 16 + 8$

$16 = 2 \times 8$

Hence, g.c.d.(56, 72) = 8.

$8 = 56 - 3 \times 16$

$= 56 - 3 \times (72 - 56)$

$= 4 \times 56 - 3 \times 72$

$\Rightarrow 40 = 56 \times 20 + 72 \times (-15)$

$\Rightarrow x = 20, y = -15,$ is a solution of $56x + 72y = 40$.

By above theorem any other solution is given by $\left(20 + \frac{72}{8}t, -15 - \frac{56}{8}t\right)$

$= (20 + 9t, -15 - 7t)$ for any integer t.

Prime Numbers

An integer $p > 1$ is called a *prime number* if 1 and p are the only divisors of p.

Theorem 22: *If a prime number p divides ab, then either p divides a or p divides b.*

Proof: Let $ab = pc$ for some integer c.

Suppose p does not divide a.

Then g.c.d.$(a, p) = 1$

$\therefore \quad p \mid ab$ and g.c.d.$(a, p) = 1$

$\Rightarrow p \mid b$

We generalise the above result in the following theorem.

Theorem 23: *If p divides $a_1a_2 \ldots a_n$, then p divides a_i for some i.*

Proof: We prove the result by induction on n.

If $n = 1$, then result is clearly true.

If $n = 2$, the result follows from above.

Let the result be true for naturals less than n.

Suppose $p \mid a_1 \ldots a_n = (a_1 \ldots a_{n-1})a_n$

$\Rightarrow p \mid a_1 \ldots a_{n-1}$ or $p \mid a_n$

If p divides $a_1 \ldots a_{n-1}$, then by induction hypothesis p divides a_i, for some i.

So result is true in this case also.

By induction result is true for all $n > 1$.

Composite Numbers

A composite number is an integer $n > 1$ such that n is not prime.

Problem 18: *Prove that if $2^n - 1$ is prime, then n is prime.*

Solution: Let $2^n - 1 = p$ = prime.

Let n be not prime.

Then $n = rs$, $1 < r, s < n$

$$\therefore \quad p = 2^n - 1$$
$$= 2^{rs} - 1 = (2^r)^s - 1$$
$$= x^s - 1, \; x = 2^r > 2 \text{ as } r > 1$$
$$= (x - 1)(x^{s-1} + x^{s-2} + \ldots + x + 1)$$

Either $x - 1 = 1$ or $x^{s-1} + \ldots + x + 1 = 1$

$x - 1 = 1 \Rightarrow x = 2$, which is not true

and $x^{S-1} + \ldots + x + 1 = 1$

$\Rightarrow x^{s-1} + \ldots + x = 0$, which is not true

$\therefore$ n is prime.

Problem 19: *Prove that $n^4 + 4$ is composite if $n > 1$.*

Solution: $n^4 + 4 = (n^2 + 2)^2 - 4n^2$

$$= (n^2 + 2 - 2n)(n^2 + 2 + 2n)$$
$$n > 1 \Rightarrow n \geq 2 \Rightarrow n^2 \geq 2n \Rightarrow n^2 - 2n \geq 0$$
$$\Rightarrow n^2 - 2n + 2 \geq 2$$

Also $n^2 + 2 + 2n > 1$

$\therefore n^4 + 4$ is composite as both $n^2 + 2 + 2n$ and $n^2 + 2 + 2n < n^4 + 4$.

Congruences

Let a, b, c, $(c > 0)$ be integers. We say a is congruent to b modulo c if c divides $a - b$ and we write this as $a \equiv b \pmod{c}$. This relation '$\equiv$' on the set of integers is an equivalence relation as seen earlier.

Addition, subtraction and multiplication in congruences behave naturally.

Let $a \equiv b \pmod{c}$

$a_1 \equiv b_1 \pmod{c} \Rightarrow c \mid a - b,\ c \mid a_1 - b_1$

$\Rightarrow c \mid (a + a_1) - (b + b_1)$

$\Rightarrow a + a_1 \equiv b + b_1 \pmod{c}$

Similarly $a - a_1 \equiv b - b_1 \pmod{c}$

Also $c \mid a - b,\ c \mid a_1 - b_1$

$\Rightarrow c \mid aa_1 - ba_1,\ c \mid ba_1 - bb_1$

$\Rightarrow c \mid (aa_1 - ba_1) + (ba_1 - bb_1)$

$\Rightarrow c \mid aa_1 - bb_1$

$\Rightarrow aa_1 \equiv bb_1 \pmod{c}$

We may, however, not be able to achieve the above result in case of division. Indeed $\frac{a}{a_1}$ or $\frac{b}{b_1}$ may not even be integers.

Again, cancellation in congruences in general may not hold.

i.e., $ad \equiv bd \pmod{c}$ need not essentially imply

$a \equiv b \pmod{c}$

For example, $2.2 \equiv 2.1 \pmod{2}$

but $2 \not\equiv 1 \pmod{2}$

However, cancellation holds if g.c.d.$(d,\ c) = 1$.

i.e., if $ad \not\equiv bd \pmod{c}$

and g.c.d.$(d, c) = 1$

then $a \equiv b \pmod{c}$.

Proof: $ad \equiv bd \pmod{c}$

$\Rightarrow c \mid ad - bd$

$\Rightarrow c \mid d\,(a - b)$

$\Rightarrow c \mid a - b$ as g.c.d.$(c, d) = 1$

$\Rightarrow a \equiv b \pmod{c}$.

Problem 20: *If* $a \equiv b$ (*mod* n), *prove that* g.c.d.$(a, n) =$ g.c.d.(b, n).

Solution: Let d = g.c.d.(a, n)

Then $d \mid a,\ d \mid n$. But $n \mid a - b$

$\therefore$ $d \mid a - b,\ d \mid a$

$\Rightarrow d \mid a - (a - b) = b$

$\therefore$ $d \mid b,\ d \mid n$

Let $c \mid b,\ c \mid n \Rightarrow c \mid b,\ c \mid a - b$ as $n \mid a - b$

$\Rightarrow c \mid a - b + b = a$

$\Rightarrow c \mid a,\ c \mid n$

$\Rightarrow c \mid d$ as d = g.c.d.$(a,\ n)$

$\Rightarrow$ g.c.d.$(b,\ n) = d$

Problem 21: *Establish that if a is an odd integer, then*

$$a^{2^n} \equiv 1 \ (mod\ 2^{n+2}) \text{ for any } n \geq 1.$$

Solution: We prove the result by induction on n.

Let $n = 1$. Then

$$a^{2^n} = a^2$$

and $2^{n+2} = 2^3 = 8$

Let $a = 2k + 1$. Then

$$a^2 = 4k^2 + 4k + 1$$

$$= 4k\ (k + 1) + 1$$

$\therefore$ $a^2 - 1 = 4k\ (k + 1)$

= multiple of 8 as either k is even or $k + 1$ is even.

$\therefore$ $a^2 \equiv 1 \pmod 8$

So, result is true for $n = 1$.

Assume that the result is true for $n = k$.

Then $a^{2^k} \equiv 1 \pmod{2^{k+2}}$

Now $a^{2^{k+1}} - 1 = (a^{2^k})^2 - 1$

$= (a^{2^k} - 1)\ (a^{2^k} + 1)$

= (multiple of 2^{k+2}) $(a^{2^k} + 1)$ by induction hypothesis.

But a = odd $\Rightarrow a^{2^k}$ = odd $\Rightarrow a^{2^k} + 1$ = even

$\therefore$ $a^{2^{k+1}} - 1$ = multiple of 2^{k+3}

$\therefore$ $a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$

So, result is true for $n = k + 1$.

By induction, result is true for all $n \geq 1$.

Problem 22: *Show that for any integer a,*

$$a^3 \equiv 0,\ 1,\ or\ 8 \ (mod\ 9)$$

Solution: Let $a = 3k + r,\ \ 0 \le r < 3$

If $r = 0$, then $a = 3k$

$\Rightarrow\ a^3 = 27k^3 \equiv 0 \pmod 9$

If $r = 1$, then $a = 3k + 1$

$\therefore\ a^3 = 27k^3 + 1 + 9k^2 + 9k$

$\Rightarrow\ a^3 \equiv 1 \pmod 9$

If $a = 3k + 2$, then $a^3 = 27k^3 + 8 + 27k^2 + 36k^2$

$\Rightarrow\ a^3 \equiv 8 \pmod 9$

$\therefore\ a^3 \equiv 0,\ 1 \text{ or } 8 \pmod 9$.

Problem 23: *If* $ca \equiv cb\ (mod\ n)$, *then* $a \equiv b\ \left(mod\ \frac{n}{d}\right)$,

where d = g.c.d.$(c,\ \ n)$.

Solution: d = g.c.d. $(c,\ \ n)$

$$\Rightarrow\ 1 = \text{g.c.d.}\left(\frac{c}{d}, \frac{n}{d}\right)$$

Also $ca \equiv cb \pmod n$

$\Rightarrow\ ca - cb = nk$ for some integer k

$$\Rightarrow\ \frac{c}{d}a - \frac{c}{d}b = \frac{n}{d}k$$

$$\Rightarrow\ \frac{n}{d}\left|\frac{c}{d}(a-b)\right.$$

$$\Rightarrow\ \frac{n}{d}\left|a-b\right. \text{ as g.c.d.}\left(\frac{c}{d}, \frac{n}{d}\right) = 1$$

$$\Rightarrow\ a \equiv b\ \left(mod\ \frac{n}{d}\right).$$

Problem 24: *Find the remainder obtained by dividing* $1! + 2! + 3! + 4! + ... + 100!$ *by* 12.

Solution: Each number 4! onwards is a multiple of 12.

$\therefore\ 1! + 2! + 3! + 4! + ... + 100! \equiv 1! + 2! + 3! + 0 + ... + 0 \pmod{12}$

$\Rightarrow\ 1! + 2! + 3! + 4! + ... + 100! \equiv 9 \pmod{12}$

$\Rightarrow$ 9 is the required remainder.

Problem 25: *Find the remainder when* 2^{50} *is divided by* 7.

Solution: Now $2^3 \equiv 1 \pmod 7$

$$\Rightarrow\ (2^3)^{16} \equiv 1^{16} \equiv 1 \pmod 7$$

$$\Rightarrow\ 2^{48} \equiv 1 \pmod 7$$

$\Rightarrow 2^{48} - 2^2 \equiv 2^2 \pmod 7$

$\Rightarrow 2^{50} \equiv 4 \pmod 7$

$\therefore$ 4 is the remainder.

Problem 26: *What is the remainder when the sum* $1^5 + 2^5 + 3^5 + ... + 99^5 + 100^5$ *is divided by* 4.

Solution: Note $1 \equiv 1 \pmod 4 \Rightarrow 1^5 \equiv 1 \pmod 4$

$2^2 \equiv 0 \pmod 4 \Rightarrow 2^5 \equiv 0 \pmod 4$

$3^2 \equiv 1 \pmod 4 \Rightarrow 3^5 \equiv 3 \pmod 4$

$\Rightarrow 3^5 \equiv -1 \pmod 4$

$4^2 \equiv 0 \pmod 4 \Rightarrow 4^5 \equiv 0 \pmod 4$

$\therefore 1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 - 1 + 0 \equiv 0 \pmod 4$

Any numbers after these will be of the form $2k + 1$, $2k + 2$, $2k + 3$, $2k + 4$, $k > 1$.

Now$(2k + 1)^2 \equiv 1 \pmod 4 \Rightarrow (2k + 1)^5 \equiv 2k + 1 \equiv 1 \pmod 4$

$(2k + 2)^2 \equiv 0 \pmod 4 \Rightarrow (2k + 2)^5 \equiv 0 \pmod 4$

$(2k + 3)^2 \equiv 1 \pmod 4 \Rightarrow (2k + 3)^5 \equiv 2k + 3 \equiv -1 \pmod 4$

$(2k + 4)^2 \equiv 0 \pmod 4 \Rightarrow (2k + 4)^5 \equiv 0 \pmod 4$

$\therefore \quad 1^5 + 2^5 + 3^5 + 4^5 + ... \; 99^5 + 100^5 \equiv 0 \pmod 4$

So, remainder is 0 when above number is divided by 4.

Chinese Remainder Theorem

Theorem 24: *Consider* $ax \equiv b \pmod c$*, where a, b, c are integers such that* $d = (a, c)$ *divides b.*

Let $x = x_0$ *be a solution. Then the given congruence has exactly d mutually incougruent solutions modulo c.*

Proof: Let $x = x_0 + t\dfrac{c}{d}$ where t is any integer.

Consider $a\left(x_0 + t\dfrac{c}{d}\right)$

$= ax_0 + t\dfrac{a}{d}c \equiv b \pmod c$

Then $x_0 + t\dfrac{c}{d}$ is a solution of $ax \equiv b \pmod c$ for any integer.

Let $S = \left\{x_0, x_0 + \dfrac{c}{d}, x_0 + 2\dfrac{c}{d}, \cdots, x_0 + (d-1)\dfrac{c}{d},\right\}$

Then every integer in S is a solution of $ax \equiv b \pmod c$. We show that no two integers are mutually congruent modulo c.

Let $x_0 + i\frac{c}{d} \equiv x_0 + j\frac{c}{d} \pmod{c}$, $0 \le i, j < d$, $i \ne j$.

Then c divides $(i - j)\ \frac{c}{d}$. Let $i > j$, So, d divides $(i - j)$, a contradiction as both i and j are less than d. This proves our assertion.

Let y be a solution of $ax \equiv b \pmod{c}$ other than x_0. Then $ax_0 \equiv ay \pmod{c}$ implies c divides $a(x_0 - y)$. So, $\frac{c}{d}$ divides $\frac{a}{d}(x_0 - y)$.

Since, $\left(\frac{c}{d}, \frac{a}{d}\right) = 1$, $\frac{c}{d}$ divides $x_0 - y$ or $y - x_0$.

So, $y - x_0 = t\frac{c}{d}$, for some integer t. Therefore, $y = x_0 + t\frac{c}{d}$, for some integer t.

Let $t = dq + r$, $0 \le r < d$.

Then $y = x_0 + (dq + r)\frac{c}{d}$

$$\equiv x_0 + qc + r\frac{c}{d}$$

$$= x_0 + r\frac{c}{d} \pmod{c}, \quad 0 \le r \le d$$

Since, $x_0 + r\frac{c}{d} \in S$, any solution of $ax \equiv b \pmod{c}$ is congruent to some integer in S modulo c.

Thus, there are exactly d mutually incongruent solutions modulo c.

Cor: Let $(a, c) = 1$. Then there exists an integer $\overline{a}$ such that $a\overline{a} \equiv 1 \pmod{c}$. $\overline{a}$ is uniquely determined modulo c, called the inverse of a modulo c.

Proof: Since $(a, c) = 1$, there exists unique solution of $ax \equiv 1 \pmod{c}$ by above theorem. So, there exists an integer $\overline{a}$ such that $a\overline{a} \equiv 1 \pmod{c}$. $\overline{a}$ is uniquely determined modulo c by above theorem.

We now prove the Chinese remainder theorem.

Theorem 25: (Chinese Remainder Theorem): *Let $n_1, n_2,...,n_r$ be pairwise relatively prime integers. Consider the following system of congruences*

$$a_1x \equiv b_1 \pmod{n_1}$$
$$a_2x \equiv b_2 \pmod{n_2}$$
$$\dots$$
$$a_rx \equiv b_r \pmod{n_r}$$

where a_i and n_i are relatively prime integers for all i. Then there exists an integer x that satisfies the above system of congruences. Further, any two solutions of the above system of congruences are congruent modulo M, where $M = n_1 n_2....n_r$.

Proof: Consider $a_ix \equiv b_i \pmod{n_i}$

Since $(a_i, n_i) = 1$, there exists an integer c_i such that $a_ic_i \equiv b_i \pmod{n_i}$ for all i.

Let $m_i = \dfrac{M}{n_i}$. Then $(n_i, m_i) = 1$ for all i,

for, let p be a prime dividing (n_i, m_i). Then $p|n_i$, $p|m_i = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_r$ implies $p|n_i$, $p|n_j$ $(j \neq i)$ contradicting $(n_i, n_j) = 1$ for $i \neq j$.

By above theorem there exists an integer $\bar{m}_i$ such that $m_i \bar{m}_i \equiv 1 \pmod{n_i}$ for all i.

Consider $X = c_1 m_1 \bar{m}_1 + c_2 m_2 \bar{m}_2 + \cdots + c_r m_r \bar{m}_r$

Then $a_i X = a_i c_1 m_1 \bar{m}_1 + a_i c_2 m_2 \bar{m}_2 + \cdots + a_i c_r m_r \bar{m}_r$

$\equiv a_i c_i m_i \bar{m}_i \pmod{n_i}$ as each term except ith term contains n_i

$\equiv b_i \pmod{n_i}$ for all i as $a_i c_i \equiv b_i \pmod{n_i}$ and $m_i \bar{m}_i \equiv 1 \pmod{n_i}$

So, X is a common solution of the given system of congruences.

Suppose, y is also a common solution.

Then $a_i X \equiv a_i y \pmod{n_i}$ for all i

Since $(a_i, n_i) = 1$ for all i

$X \equiv y \pmod{n_i}$ for all i.

So, $n_i \mid X - y$ for all i

Therefore, M = l.c.m of $n_1, n_2 \ldots, n_r$ divides $X - y$.

Hence, $X \equiv y \pmod{M}$

Note: See Problem 41 on page 247 also.

Problem 27: Solve the following system of congruences,

$x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$

Solution: Here $c_1 = 3$, $c_2 = 4$, $c_3 = 6$, $M = 140$

$m_1 = 35$, $m_2 = 28$, $m_3 = 20$

Consider $m_1 \bar{m}_1 \equiv 1 \pmod 4$. Then $35\ \bar{m}_i \equiv 1 \pmod 4$

becomes $3\bar{m}_1 \equiv 1 \pmod 4$. So, $\bar{m}_1 = 3$

Consider $m_2 \bar{m}_2 \equiv 1 \pmod 5$. Then $28\,\bar{m}_2 \equiv 1 \pmod 5$

becomes $3\bar{m}_2 \equiv 1 \pmod 5$. Then, $\bar{m}_2 = 2$

Consider $m_3 \bar{m}_3 \equiv 1 \pmod 7$. Then $20\,\bar{m}_3 \equiv 1 \pmod 7$

becomes $6\bar{m}_3 \equiv 1 \pmod 7$. So, $\bar{m}_3 = 6$

Therefore, $X = c_1 m_1 \bar{m}_1 + c_2 m_2 \bar{m}_2 + c_3 m_3 \bar{m}_3$

$= 315 + 224 + 720$

$= 1259 \equiv 139 \pmod{140}$

So, $X = 139$ is a solution.

Problem 28: *Find three consecutive integers, first of which is divisible by square of a prime, second divisible by cube of a prime and third divisible by fourth power of a prime.*

Solution: Let x, $x + 1$, $x + 2$ be three consecutive integers such that $x \equiv 0 \pmod{5^2}$, $x \equiv -1 \pmod{3^3}$, $x \equiv -2 \pmod{2^4}$

Then $c_1 = 0$, $c_2 = -1$, $c_3 = -2$, $M = 10800$

$m_1 = 432$, $m_2 = 400$, $m_3 = 675$

Consider $m_2\overline{m}_2 \equiv 1 \pmod{27}$. Then $400\,\overline{m}_2 \equiv 1 \pmod{27}$

becomes $22\overline{m}_2 \equiv 1 \pmod{27}$ or $-5\overline{m}_2 \equiv 1 \pmod{27}$. So, $\overline{m}_2 = 16$

Consider $m_3\overline{m}_3 \equiv 1 \pmod{16}$. Then $675\,\overline{m}_3 \equiv 1 \pmod{16}$

becomes $3\overline{m}_3 \equiv 1 \pmod{16}$. So, $\overline{m}_3 = -5$

Therefore, $X = c_2m_2\overline{m}_2 + c_3m_3\overline{m}_3$

$= -6400 + 6750$

$= 350$

Hence, 350, 351 and 352 are the required integers.

Before we finish with this chapter we recall the *Well Ordering Principle*, which states that any non empty subset of real numbers which is bounded below has least element. It is sometimes denoted by W.O.P.

Exercises

1. Prove that if a and b are integers with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.

2. Use Euclid's algorithm to establish that

(i) every odd integer is of the form $4k + 1$ or $4k + 3$.

(ii) the square of any integer is either of the form $3k$ or $3k + 1$.

(iii) the cube of any integer is of the from $9k$, $9k + 1$ or $9k + 8$.

3. If $(a, b) = 1$, show that $(a + b, a - b)$ is either 1 or 2.

4. If $(a, b) = 1$, show that

(i) $(2a + b, a + 2b) = 1$ or 3

(ii) $(a + b, a^2 + b^2) = 1$ or 2

(iii) $(ac, b) = (c, b)$

5. Given x and y, let $m = ax + by$, $n = cx + dy$, where $ad - bc = \pm 1$. Prove that $(m, n) = (x, y)$.

6. Let $\Phi_n = 2^{2^n} + 1$. Prove that if $n < m$, then Φ_n divides $\Phi_m - 2$. (Φ_n is called Fermat number).

7. Prove that if $n \neq m$, $(\Phi_n, \Phi_m) = 1$.

8. Prove that l.c.m.$(ab, ad) = a$ [l.c.m.(b, d)].

9. Prove that if a, b are non zero integers, then g.c.d.$(a, b) \mid$ l.c.m.(a, b).

10. Prove that if $2^n + 1$ is prime, then n is a power of 2.

11. Let d = (826, 1890). Use Euclid's algorithm to compute d and then express d as a linear combination of 826 and 1890.

12. Show that $a^n \mid b^n$ implies $a \mid b$.

13. Determine all solutions in the positive integers of the following Diophantine equation $172x + 20y = 100$. (Ans. (5, 7))

14. Find the remainder when 41^{65} is divided by 7.

15. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

16. Prove that if $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$ with g.c.d.$(b, n) = 1$, then $a \equiv c \pmod{n}$.

17. If $a \equiv b \pmod{n_1}$, and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$ where $n = (n_1, n_2)$.

18. Which of the following congruences hold

(*i*) 12, 345, 678, 987, 654, 321 $\equiv 0 \pmod{12, 345, 678}$

(*ii*) 12, 345, 678, 987, 654, 321 $\equiv 0 \pmod{12, 345, 679}$

19. Solve the system of congruences

(*i*) $x \equiv 5 \pmod 7$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 8$, $x \equiv 2 \pmod 3$

(*ii*) $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 8$, $x \equiv 2 \pmod 3$

20. Prove that if $|a| < \frac{k}{2}$, $|b| < \frac{k}{2}$ and $a \equiv b \pmod k$, then $a = b$.

21. Prove that if $bd \equiv bd' \pmod p$ where p = prime and $p \nmid b$ then $d \equiv d' \pmod p$.

A Quick Look at what's been done

- If A and B are two non-empty sets then any subset of $A \times B$ is called a **relation** from A to B.
- A relation f from A to B is called a f**unction** or a **mapping** from A to B, if for every a in A there exists a unique b in B s.t., (a, b) belongs to $A \times B$, and in that case we write $b = f(a)$ and b is called **image** of a under f. We express this by writing $f: A \to B$. Thus a mapping from A to B is a rule that *connects* each element of A to a unique element of B
- A mapping $f: A \to B$ is called **one-one** if $f(x) = f(y) \Rightarrow x = y$. It is called **onto,** if for every b in B there exists an a in A s.t., $f(a) = b$, and a is then called **pre-image** of b.
- A mapping $f: A \times A \to A$ is called a **binary composition** or a **binary operation**. Thus a binary composition 'joins' two elements of a set to give a unique element of the same set.
- A one-one onto mapping from $A \to A$ is called a **permutation.**
- Prime and composite numbers, congruence relations, g.c.d., l.c.m., Basis representation theorem, Chinese remainder theorem have been discussed in the later part of this chapter.

2

Groups

Introduction

In the previous chapter we studied the notions of relations, maps and in particular binary compositions. We now come to the study of different algebraic structures or algebraic systems, which means a non empty set with one or more binary compositions. We start with groups which occupy a very important seat in the study of abstract algebra.

Definition: A non empty set G, together with a binary composition $*$ (star) is said to form a group, if it satisfies the following postulates

(i) *Associativity*: $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$

(ii) *Existence of Identity*: $\exists$ an element $e \in G$, s.t.,

$$a * e = e * a = a \quad \text{for all } a \in G$$

(e is then called *identity*)

(iii) *Existence of Inverse*: For every $a \in G$, $\exists\ a' \in G$ (depending upon a) s.t.,

$$a * a' = a' * a = e$$

(a' is then called inverse of a)

Remarks: (i) Since $*$ is a binary composition on G, it is understood that for all $a, b \in G$, $a * b$ is a unique member of G. This property is called *closure property*.

(ii) If, in addition to the above postulates, G also satisfies the *commutative law*

$$a * b = b * a \quad \text{for all } a, b \in G$$

then G is called an *abelian group* or *a commutative group*.

(iii) Generally, the binary composition for a group is denoted by '.' (dot) which is so convenient to write (and makes the axioms look so natural too).

This binary composition '.' is called product or multiplication (although it may have nothing to do with the usual multiplication, that we are so familiar with). In fact, we even drop '.' and simply write ab in place of $a \,.\, b$.

In future, whenever we say that G is a group it will be understood that there exists a binary composition '.' on G and it satisfies all the axioms in the definition of a group.

If the set G is finite (i.e., has finite number of elements) it is called a *finite group* otherwise, it is called an *infinite group*.

We shall always (unless stated otherwise) use the symbols e for identity of a group and a^{-1} for inverse of element a of the group.

Definition: By order of a group, we will mean the number of elements in the group and shall denote it by $o(G)$ or $| G |$.

We now consider a few examples of systems that form groups (or do not form groups).

Example 1: The set **Z** of integers forms an abelian group w.r.t. the usual addition of integers.

It is easy to verify the postulates in the definition of a group as sum of two integers is a unique integer (thus closure holds). Associativity of addition is known to us. 0 (zero) will be identity and negatives will be the respective inverse elements. Commutativity again being obvious.

Example 2: One can easily check, as in the previous example, that sets **Q** of rationals, **R** of real numbers would also form abelian groups w.r.t. addition.

Example 3: Set of integers, w.r.t. usual multiplication does not form a group, although closure, associativity, identity conditions hold.

Note 2 has no inverse w.r.t. multiplication as there does not exist any integer a s.t., $2 . a = a . 2 = 1$.

Example 4: The set G of all +ve irrational numbers together with 1 under multiplication does not form a group as closure does not hold. Indeed $\sqrt{3} . \sqrt{3} = 3 \notin G$, although one would notice that other conditions in the definition of a group are satisfied here.

Example 5: Let G be the set $\{1, -1\}$. Then it forms an abelian group under multiplication. It is again easy to check the properties.

1 would be identity and each element is its own inverse.

Example 6: Set of all 2×2 matrices over integers under matrix addition would be another example of an abelian group.

Example 7: Set of all non zero complex numbers forms a group under multiplication defined by

$$(a + ib)\ (c + id) = (ac - bd) + i\ (ad + bc)$$

$1 = 1 + i.0$ will be identity,

$\dfrac{a}{a^2 + b^2} - i \dfrac{b}{a^2 + b^2}$ will be inverse of $a + ib$.

Note $a + ib$ non zero means that not both a & b are zero. Thus $a^2 + b^2 \neq 0$.

Example 8: The set G of all nth roots of unity, where n is a fixed positive integer forms an abelian group under usual multiplication of complex numbers.

We know that complex number z is an nth root of unity if $z^n = 1$ and also that there exist exactly n distinct roots of unity.

In fact the roots are given by $e^{2\pi ir/n}$

where $r = 1, 2, ..., n$ and $e^{ix} = \cos x + i \sin x$.

If $a, b \in G$ be any two members, then $a^n = 1$, $b^n = 1$ thus $(ab)^n = a^n b^n = 1$.

$\Rightarrow ab$ is an nth root of unity

$\Rightarrow ab \in G \Rightarrow$ closure holds.

Associativity of multiplication is true in complex numbers.

Again, since $1.\ a = a\ .\ 1 = a$, $\quad 1$ will be identity.

Also for any $a \in G$, $\dfrac{1}{a}$ will be its inverse as $\left(\dfrac{1}{a}\right)^n = \dfrac{1}{a^n} = 1$.

So, inverse of $e^{2\pi ir/n}$ is $e^{2\pi i(n-r)/n}$ and identity is $e^{2\pi i0/n} = 1$

Commutativity being obvious, we find G is an abelian group.

As a particular case, if $n = 4$ then G is $\{1, -1, i, -i\}$

Example 9: (*i*) Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1, ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

then G forms a group. G is not abelian as $ij \neq ji$.

This is called the ***Quaternion Group***.

(*ii*) If set G consists of the eight matrices

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}, \begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix}, \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},$$

$$\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}, \begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix}, \text{ where } i = \sqrt{-1}$$

then G forms a non abelian group under matrix multiplication. (Compare with part (*i*)).

Example 10: Let $G = \{(a, b) \mid a, b$ rationals, $a \neq 0\}$. Define $*$ on G by

$$(a, b) * (c, d) = (ac, ad + b)$$

Closure follows as $a, c \neq 0 \Rightarrow ac \neq 0$

$$[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f)$$
$$= (ace, acf + ad + b)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d)$$
$$= (ace, acf + ad + b)$$

proves associativity.

$(1, 0)$ will be identity and $(1/a, -b/a)$ will be inverse of any element (a, b).

G is not abelian as

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$
$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

Example 11 (a): The set G of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over reals, where $ad - bc \neq 0$, i.e., with non zero determinant forms a non abelian group under matrix multiplication.

It is called the **general linear group** of 2×2 matrices over reals and is denoted by $GL(2, \mathbf{R})$.

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will act as identity and

the matrix $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ will be inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

one can generalise and prove

(b) If G be the set of all $n \times n$ invertible matrices over reals, then G forms a group under matrix multiplication.

(c) The set of 2×2 matrices over $\mathbf{R}$ with determinant value 1 forms a non abelian group under matrix multiplication and is called the **special linear group**, denoted by $SL(2, \mathbf{R})$.

One can take any field (e.g., $\mathbf{Q}$, $\mathbf{C}$ or $\mathbf{Z}_p$) in place of $\mathbf{R}$ in the above examples.

Example 12: Let $G = \{2^r \mid r = 0, \pm 1, \pm 2, \ldots\}$

We show G forms a group under usual multiplication.

For any $2^r, 2^s \in G$, $2^r . 2^s = 2^{r+s} \in G$

Thus closure holds.

Associativity is obvious.

Again as $1 \in G$, and $x . 1 = 1 . x = x$ for all $x \in G$

1 is identity.

For any $2^r \in G$, as $2^{-r} \in G$ and $2^r . 2^{-r} = 2^0 = 1$,

we find each element of G has inverse. Commutativity is evidently true.

Example 13: *Group of Residues* : Let $G = \{0, 1, 2, 3, 4\}$. Define a composition $\oplus_5$ on G by $a \oplus_5 b = c$ where c is the least non –ve integer obtained as remainder when $a + b$ is divided by 5. For example. $3 \oplus_5 4 = 2$, $3 \oplus_5 1 = 4$, etc. Then $\oplus_5$ is a binary composition on G (called addition modulo 5). It is easy to verify that G forms a group under this.

One can generalise this result to

$$G = \{0, 1, 2, \ldots, n - 1\}$$

under addition modulo n where n is any positive integer.

We thus notice

$$a \oplus_n b = \begin{cases} a + b & \text{if } a + b < n \\ a + b - n & \text{if } a + b \geq n \end{cases}$$

Also, in case there is no scope of confusion we drop the sub suffix n and simply write $\oplus$. This group is generally denoted by $\mathbf{Z}_n$.

Example 14: Let $G = \{x \in \mathbf{Z} \mid 1 \leq x < n, x, n \text{ being co-prime}\}$ where $\mathbf{Z}$ = set of integers and x, n being co-prime means H.C.F of x and n is 1.

We define a binary composition $\otimes$ on G by $a \otimes b = c$ where c is the least +ve remainder obtained when $a \,.\, b$ is divided by n. This composition $\otimes$ is called multiplication modulo n.

We show G forms a group under $\otimes$.

Closure: For $a, b \in G$, let $a \otimes b = c$. Then $c \neq 0$, because otherwise $n \mid ab$ which is not possible as a, n and b, n are co-prime.

Thus $c \neq 0$ and also then $1 \leq c < n$.

Now if c, n are not co-prime then $\exists$ some prime no. p s.t., $p|c$ and $p|n$.

Again as $ab = nq + c$ for some q

We get $p|ab$ $\quad [p|n \Rightarrow p|nq,\ p|c \Rightarrow p|nq + c]$

$\Rightarrow p|a$ or $p|b$ (as p is prime)

If $p|a$ then as $p|n$ it means a, n are not co-prime.

But a, n are co-prime.

Similarly $p|b$ leads to a contradiction.

Hence c, n are co-prime and thus $c \in G$, showing that closure holds.

Associativity: Let $a, b, c \in G$ be any elements.

Let $a \otimes b = r_1$, $(a \otimes b) \otimes c = r_1 \otimes c = r_2$

then r_2 is given by $r_1 c = nq_2 + r_2$

Also $a \otimes b = r_1$ means

$$ab = q_1 n + r_1$$

thus $$ab - q_1 n = r_1$$

$$\Rightarrow (ab - q_1 n)c = r_1 c = nq_2 + r_2$$

$$\Rightarrow (ab)c = r_2 + nq_2 + nq_1 c = n(q_1 c + q_2) + r_2$$

or that r_2 is the least non-negative remainder got by dividing $(ab)c$ by n.

Similarly, if $a \otimes (b \otimes c) = r_3$ then we can show that r_3 is the least non –ve remainder got by dividing $a(bc)$ by n.

But since $a(bc) = (ab)c$, $r_2 = r_3$

Hence $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.

Existence of Identity: It is easy to see that

$$a \otimes 1 = 1 \otimes a = a \quad \text{for all } a \in G$$

or that 1 will act as identity.

Existence of Inverse: Let $a \in G$ be any element then a and n are co-prime and thus we can find integers x and y s.t., $ax + ny = 1$

By division algorithm, we can write

$$x = qn + r, \quad \text{where } 0 \leq r < n$$

$$\Rightarrow ax = aqn + ar$$

$\Rightarrow ax + ny = aqn + ar + ny$

$\Rightarrow 1 = aqn + ar + ny$

or that $ar = 1 + (-aq - y)n$

i.e., $a \otimes r = 1$. Similarly $r \otimes a = 1$. If r, n are co-prime, r will be inverse of a.

If r, n are not co-prime, we can find a prime number p s.t., $p \mid r$, $p \mid n$

$\Rightarrow p \mid qn$ and $p \mid r$

$\Rightarrow p \mid qn + r$

$\Rightarrow p \mid x$

$\Rightarrow p \mid ax$ also $p \mid ny$

$\Rightarrow p \mid ax + ny = 1$

which is not possible. Thus r, n are co-prime and so $r \in G$ and is the required inverse of a.

It is easy to see that G will be abelian. We denote this group by U_n or $U(n)$ and call it the group of integers under multiplication modulo n.

Remark: Suppose $n = p$, a prime, then since all the integers 1, 2, 3, ..., $p - 1$ are co-prime to p, these will all be members of G. One can show that

$$G = \{2, 4, 6, ..., 2(p - 1)\}$$

where $p > 2$ is a prime forms an abelian group under multiplication modulo $2p$.

Example 15: Let $G = \{0, 1, 2\}$ and define $*$ on G by

$$a * b = |a - b|$$

Then closure is established by taking a look at the composition table

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Since $a * 0 = |a - 0| = a = 0 * a$, 0 is identity

and $a * a = |a - a| = 0$ shows each element will be its own inverse.

But the system $(G, *)$ fails to be a group as associativity does not hold.

Indeed $1 * (1 * 2) = 1 * 1 = 0$

but $(1 * 1) * 2 = 0 * 2 = 2$

Example 16: Let $S = \{1, 2, 3\}$ and let $S_3 = A(S)$ = set all permutations of S. We showed in the previous chapter that this set satisfies associativity, existence of identity and existence of inverse conditions in the definition of a group. Also clearly, since f, g permutations on S imply that fog is a permutation on S the closure property is ensured. Hence S_3 forms a group. That it is not abelian follows by the fact that $fog \neq gof$ (see details in previous chapter under permutations). This would, in fact, be the smallest non abelian group and we shall have an occasion to talk about this group again under the section on permutation groups.

Remark: Let X be a non empty set and let $M(X)$ = set of *all* maps from X to X, then $A(X) \subseteq M(X)$. $M(X)$ forms a semi group (see definition ahead) under composition of maps. Identity map also lies in $M(X)$ and as a map is invertible iff it is 1-1, onto *i.e.*, a permutation, we find $A(X)$ the subset of all permutations forms a group, denoted by S_X or Sym(X) and is called symmetric group of X. If X is finite with say, n elements then $o(M(X)) = n^n$ and $o(S_X) = \lfloor \underline{n}$ and in that case we use the notation S_n for S_X.

In the definition of a group, we only talked about the existence of identity and inverse of each element. We now show that these elements would also be unique, an elementary but exceedingly useful result. We prove it along with some other results in

Lemma: *In a group G,*

(1) *Identity element is unique.*

(2) *Inverse of each $a \in G$ is unique.*

(3) $(a^{-1})^{-1} = a$, *for all* $a \in G$, *where* a^{-1} *stands for inverse of* a.

(4) $(ab)^{-1} = b^{-1}\, a^{-1}$ *for all* $a, b \in G$

(5) $ab = ac \Rightarrow b = c$
$ba = ca \Rightarrow b = c$ *for all* $a, b, c \in G$
(called the cancellation laws).

Proof: (1) Suppose e and e' are two elements of G which act as identity.
Then, since $e \in G$ and e' is identity,
$$e'e = ee' = e$$
and as $e' \in G$ and e is identity
$$e'e = ee' = e'$$
The two $\Rightarrow e = e'$
which establishes the uniqueness of identity in a group.

(2) Let $a \in G$ be any element and let a' and a'' be two inverse elements of a, then
$$aa' = a'a = e$$
$$aa'' = a''a = e$$
Now $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.
Showing thereby that inverse of an element is unique. We shall denote inverse of a by a^{-1}.

(3) Since a^{-1} is inverse of a
$$aa^{-1} = a^{-1}a = e62$$
which also implies a is inverse of a^{-1}
Thus $(a^{-1})^{-1} = a$.

(4) We have to prove that ab is inverse of $b^{-1}a^{-1}$ for which we show
$$(ab)\ (b^{-1}a^{-1}) = (b^{-1}a^{-1})\ (ab) = e.$$
Now
$$\begin{aligned}(ab)\ (b^{-1}a^{-1}) &= [(ab)\ b^{-1}]\ a^{-1} \\ &= [(a(bb^{-1})]\ a^{-1} \\ &= (ae)\ a^{-1} = aa^{-1} = e\end{aligned}$$

Similarly $(b^{-1}a^{-1})(ab) = e$

and thus the result follows.

(5) Let $ab = ac$, then

$$b = eb = (a^{-1}a)b$$
$$= a^{-1}(ab) = a^{-1}(ac)$$
$$= (a^{-1}a)c = ec = c$$

Thus $ab = ac \Rightarrow b = c$

which is called the left cancellation law.

One can similarly, prove the right cancellation law.

Example 17 (*a*): Let $X = \{1, 2, 3\}$ and let $S_3 = A(X)$ be the group of all permutations on X. Consider $f, g, h \in A(X)$, defined by

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1$$
$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3$$
$$h(1) = 3, \quad h(2) = 1, \quad h(3) = 2$$

It is easy then to verify that $fog = goh$

But $f \neq h$.

(*b*) If we consider the group in example 10, we find

$$(1, 2) * (3, 4) = (3, 6) = (3, 0) * (1, 2)$$

But $(3, 4) \neq (3, 0)$

Hence we notice, cross cancellations *may not* hold in a group.

Theorem 1: *For elements a, b in a group G, the equations ax = b and ya = b have unique solutions for x and y in G.*

Proof: Now $ax = b$

$$\Rightarrow a^{-1}(ax) = a^{-1}b$$
$$\Rightarrow ex = a^{-1}b$$

or $x = a^{-1}b$

which is the required solution of the equation $ax = b$.

Suppose $x = x_1$ and $x = x_2$ are two solutions of this equation, then

$$ax_1 = b \text{ and } ax_2 = b$$
$$\Rightarrow ax_1 = ax_2$$
$$\Rightarrow x_1 = x_2 \quad \text{by left cancellation}$$

Showing that the solution is unique.

Similarly $y = ba^{-1}$ will be unique solution of the equation $ya = b$.

Theorem 2: *A non empty set G together with a binary composition '.' is a group if and only if*

(1) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(2) *For any* $a, b \in G$, *the equations* $ax = b$ *and* $ya = b$ *have solutions in* G.

Proof: If G is a group, then (1) and (2) follow by definition and previous theorem.

Conversely, let (1) and (2) hold. To show G is a group, we need prove existence of identity and inverse (for each element).

Let $a \in G$ be any element.

By (2) the equations $ax = a$

$ya = a$

have solutions in G.

Let $x = e$ and $y = f$ be the solutions.

Thus $\exists\ e, f \in G$, s.t., $ae = a$

$fa = a$

Let now $b \in G$ be *any* element then again by (2) $\exists$ some x, y in G s.t.,

$ax = b$

$ya = b.$

Now $ax = b \Rightarrow f.(a\ .\ x) = f\ .\ b$

$\Rightarrow (f\ .\ a)\ .\ x = f\ .\ b$

$\Rightarrow a\ .\ x = f\ .\ b$

$\Rightarrow b = f\ .\ b$

Again $y\ .\ a = b \Rightarrow (y\ .\ a)\ .\ e = b\ .\ e$

$\Rightarrow y\ .\ (a\ .\ e) = b\ .\ e$

$\Rightarrow y\ .\ a = be$

$\Rightarrow b = be$

thus we have $b = fb$ ...(*i*)

$b = be$ ...(*ii*)

for any $b \in G$

Putting $b = e$ in (*i*) and $b = f$ in (*ii*) we get

$e = fe$

$f = fe$

$\Rightarrow e = f.$

Hence $ae = a = fa = ea$

i.e., $\exists\ e \in G$, s.t., $ae = ea = a$

$\Rightarrow e$ is identity.

Again, for any $a \in G$, and (the identity) $e \in G$, the equations $ax = e$ and $ya = e$ have solutions.

Let the solutions be $x = a_1$, and $y = a_2$

then $aa_1 = e, \quad a_2a = e$

Now $a_1 = ea_1 = (a_2a)a_1 = a_2(aa_1) = a_2e = a_2.$

Hence $aa_1 = e = a_1a$ for any $a \in G$

i.e., for any $a \in G$, $\exists$ some $a_1 \in G$ satisfying the above relations $\Rightarrow a$ has an inverse. Thus each element has inverse and, by definition, G forms a group.

Remark: While proving the above theorem we have assumed that equations of the type $ax = b$ and $ya = b$ have solutions in G. The result may fail, if only one type of the above equations has solution. Consider for example:

G to be a set with at least two elements. Define '.' on G by $a \,.\, b = b$ for all $a, b \in G$.

then $$a \,.\, (b \,.\, c) = a \,.\, c = c$$
$$(a \,.\, b) \,.\, c = b \,.\, c = c$$

shows associativity holds.

Again as $ab = b$, the equation $ax = b$ has a solution for any $a, b \in G$.

We notice that G is not a group, as cancellation laws do not hold in G.

As let $a, b \in G$ be any two distinct members, then

$$ab = b$$
$$bb = b \Rightarrow ab = bb$$

But $$a \neq b.$$

Definition: A non empty set G together with a binary composition '.' is called a *semi-group* if

$$a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c \quad \text{for all } a, b, c \in G$$

Obviously then every group is a semi-group. That the converse is not true follows by considering the set **N** of natural numbers under addition.

The set G in example 15 is not a semi group.

Theorem 3: *Cancellation laws may not hold in a semi-group.*

Proof: Consider M the set of all 2×2 matrices over integers under matrix multiplication, which forms a semi-group.

If we take $$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$$

then clearly $$AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

But $$B \neq C.$$

Set of natural numbers under addition is an example of a semi-group in which cancellation laws hold.

Theorem 4: *A finite semi-group in which cancellation laws hold is a group.*

Proof: Let $G = \{a_1, a_2, ..., a_n\}$ be a finite semi-group in which cancellation laws hold.

Let $a \in G$ be any element, then by closure property

$$aa_1, aa_2, ..., aa_n$$

are all in G.

Suppose any two of these elements are equal

say, $aa_i = aa_j$ for some $i \neq j$

then $a_i = a_j$ by cancellation

But $a_i \neq a_j$ as $i \neq j$

Hence no two of $aa_1, aa_2, ..., aa_n$ can be equal.

These being n in number, will be distinct members of G (Note $o(G) = n$).

Thus if $b \in G$ be any element then

$$b = aa_i \quad \text{for some } i$$

i.e., for $a, b \in G$ the equation $ax = b$ has a solution ($x = a_i$) in G.

Similarly, the equation $ya = b$ will have a solution in G.

G being a semi-group, associativity holds in G.

Hence G is a group (by theorem 2).

Remark: The above theorem holds only in finite semi-groups. The semi-group of natural numbers under addition being an example where cancellation laws hold but which is not a group.

Theorem 5: *A finite semi-group is a group if and only if it satisfies cancellation laws.*

Proof: Follows by previous theorem.

Definition: A non empty set G together with a binary composition '.' is said to form a *monoid* if

(i) $a(bc) = (ab)c \quad \forall\ a, b, c \in G$

(ii) $\exists$ an element $e \in G$ s.t., $ae = ea = a \quad \forall\ a \in G$

e is then called identity of G. It is easy to see that e is unique.

So all groups are monoids and all monoids are semi-groups.

When we defined a group, we insisted that $\exists$ an element e which acts both as a right as well as a left identity and each element has both sided inverse. We show now that it is not really essential and only one sided identity and the *same* sided inverse for each element could also make the system a group.

Theorem 6: *A system* $< G, . >$ *forms a group if and only if*

(i) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(ii) $\exists\ e \in G$, *s.t.*, $ae = a$ *for all* $a \in G$

(iii) *for all* $a \in G$, $\exists\ a' \in G$, *s.t.*, $aa' = e$.

Proof: If G is a group, we have nothing to prove as the result follows by definition.

Conversely, let the given conditions hold.

All we need show is that $ea = a$ for all $a \in G$

and $a'a = a$ for any $a \in G$

Let $a \in G$ be any element.

By (iii) $\exists\ a' \in G$, s.t., $aa' = e$

$\therefore$ For $a' \in G$, $\exists\ a'' \in G$, s.t., $a'a'' = e$ (using (iii))

Now $a'a = a'(ae) = (a'a)e = (a'a)(a'a'')$

$= a'(aa')a'' = a'(e)a'' = (a'e)a'' = a'a'' = e.$

Thus for any $a \in G$, $\exists\ a' \in G$, s.t., $aa' = a'a = e$

Again $ea = (aa')a = a(a'a) = ae = a$

$\therefore$ $ae = ea = a$ for all $a \in G$

i.e., e is identity of G.

Hence G is a group.

(See Problem 6 for another proof).

It would now be a routine exercise to prove

Theorem 7: *A system $< G, . >$ forms a group if and only if*

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(*ii*) $\exists\ e \in G$, *s.t.,* $ea = a$ *for all* $a \in G$

(*iii*) *for all* $a \in G$, $\exists$ *some* $a' \in G$, *s.t.,* $a'a = e$.

A natural question to crop up at this stage would be what happens, when one sided identity and the other sided inverse exists. Would such a system also form a group? The answer to which is provided by

Example 18. Let G be a finite set having at least two elements. Define '.' on G by

$ab = b$ for all $a, b \in G$

then clearly associativity holds in G.

Let $e \in G$ by any fixed element.

Then as $ea = a$ for all $a \in G$

e will act as left identity.

Again $a \,.\, e = e$ for all $a \in G$

$\Rightarrow$ e is right inverse for any element $a \in G$.

But we know G is not a group (cancellation laws do not hold in it).

Hence for a system $< G, . >$ to form a group it is essential that the same sided identity and inverse exist.

A Notation: Let G be a group with binary composition '.'. If $a \in G$ be any element then by closure property $a \,.\, a \in G$. Similarly $(a \,.\, a) \,.\, a \in G$ and so on.

It would be very convenient (and natural!) to denote $a \,.\, a$ by a^2 and $a \,.\, (a \,.\, a)$ or $(a \,.\, a) \,.\, a$ by a^3 and so on. Again $a^{-1} \,.\, a^{-1}$ would be denoted by a^{-2}. And since $a \,.\, a^{-1} = e$, it would not be wrong to denote $e = a^0$. It is now a simple matter to understand that under our notation

$$a^m \,.\, a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

where m, n are integers.

In case the binary composition of the group is denoted by +, we will talk of sums and multiples in place of products and powers. Thus here $2a = a + a$, and $na = a + a + \ldots + a$ (n times), if n is a +ve integer. In case n is –ve integer then $n = -m$, where m is +ve and we define $na = -ma = (-a) + (-a) + \ldots + (-a)$ m times.

Problem 1: *If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \leq r \leq n$, s.t., $a^r = e$.*

Solution: Since $o(G) = n$, G has n elements.

Let $a \in G$ be any element. By closure property a^2, a^3, ... all belong to G.

Consider $e, a, a^2, ..., a^n$

These are $n + 1$ elements (all in G). But G contains only n elements.

$\Rightarrow$ at least two of these elements are equal. If any of $a, a^2, ..., a^n$ equals e, our result is proved. If not, then $a^i = a^j$ for some i, j, $1 \le i, j \le n$. Without any loss of generality, we can take $i > j$

then $a^i = a^j$

$\Rightarrow a^i . a^{-j} = a^j . a^{-j}$

$\Rightarrow a^{i-j} = e$ where $1 \le i - j \le n$.

Putting $i - j = r$ gives us the required result.

Problem 2: *Show that a finite semi-group in which cross cancellation holds is an abelian group.*

Solution: Let G be the given finite semi-group. Let $a, b \in G$ be any elements. Since G is a semi-group, by associativity

$$a(ba) = (ab)a$$

By cross cancellation then $ba = ab \Rightarrow G$ is abelian.

Since G is abelian, cross cancellation laws become the cancellation laws. Hence G is a finite semi-group in which cancellation laws hold.

Thus G is a group.

Problem 3: *If G is a group in which* $(ab)^i = a^i b^i$ *for three consecutive integers i and any a, b in G, then show that G is abelian.*

Solution: Let $n, n + 1, n + 2$ be three consecutive integers for which the given condition holds. Then for any $a, b \in G$,

$$(ab)^n = a^n b^n \quad ...(1)$$

$$(ab)^{n+1} = a^{n+1} b^{n+1} \quad ...(2)$$

$$(ab)^{n+2} = a^{n+2} b^{n+2} \quad ...(3)$$

Now $(ab)^{n+2} = a^{n+2} b^{n+2}$

$\Rightarrow (ab)(ab)^{n+1} = a^{n+2}\ b^{n+2}$

$\Rightarrow (ab)(a^{n+1} b^{n+1}) = a^{n+2}\ b^{n+2}$

$\Rightarrow ba^{n+1} = a^{n+1} b$ (using cancellation) ...(4)

Similarly $(ab)^{n+1} = a^{n+1} b^{n+1}$

gives $(ab)(ab)^n = a^{n+1} b^{n+1}$

i.e., $(ab)(a^n b^n) = a^{n+1} b^{n+1}$

$\Rightarrow ba^n = a^n b$

$\Rightarrow ba^{n+1} = a^n ba$

$\Rightarrow a^{n+1} b = a^n ba$ using (4)

$\Rightarrow ab = ba.$

Hence G is abelian.

Remark: Conclusion of the above result may not follow if the given result holds only for two consecutive integers.

Consider, for example, the Quaternion group. One can check that $(ab)^i = a^i b^i$ for $i = 4, 5$ but the group is not abelian.

See also Exercise 6 on Page 25.

Problem 4: *Suppose* $(ab)^n = a^n b^n$ *for all* $a, b \in G$ *where* $n > 1$ *is a fixed integer.*

Show that (*i*) $(ab)^{n-1} = b^{n-1}a^{n-1}$

(*ii*) $a^n b^{n-1} = b^{n-1}a^n$

(*iii*) $(aba^{-1}b^{-1})^{n(n-1)} = e$ *for all* $a, b \in G$

Solution: (*i*) We have

$$[b^{-1}(ba)b]^n = b^{-1}(ba)^n b$$

and $$[b^{-1}(ba)b]^n = (ab)^n$$

$$(ab)^n = b^{-1}(ba)^n b$$

$$\Rightarrow (ab)^{n-1}ab = b^{-1}(b^n a^n)b$$

$$\Rightarrow (ab)^{n-1} = b^{n-1}a^{n-1} \quad \text{for all } a, b \in G$$

(*ii*) Now $(a^{-1}b^{-1}ab)^n = a^{-n}b^{-n}a^n b^n$

and $(a^{-1}b^{-1}ab)^n = a^{-n}(b^{-1}ab)^n$

$= a^{-n}b^{-1}a^n b$

$\therefore$ $a^{-n}b^{-n}a^n b^n = a^{-n}b^{-1}a^n b$

$\Rightarrow a^n b^{n-1} = b^{n-1}a^n$ for all $a, b \in G$

(*iii*) Consider $(aba^{-1}b^{-1})^{n(n-1)}$

$= [(aba^{-1}b^{-1})^{n-1}]^n$

$= [(ba^{-1}b^{-1})^{n-1}a^{n-1}]^n$ by (*i*)

$= [ba^{-(n-1)}b^{-1}a^{n-1}]^n = [b(a^{-(n-1)}b^{-1}a^{n-1})]^n$

$= b^n(a^{-(n-1)}b^{-1}a^{n-1})^n = b^n a^{-(n-1)}b^{-n}a^{n-1}$

$= a^{-(n-1)}b^n b^{-n}a^{n-1}$ by (*ii*)

$= e$ for all $a, b \in G$.

Problem 5: *Let G be a group and suppose there exist two relatively prime positive integers m and n such that* $a^m b^m = b^m a^m$ *and* $a^n b^n = b^n a^n$ *for all* $a, b \in G$. *Show that G is abelian.*

Solution: Since m, n are relatively prime, there exist integers x and y such that $mx + ny = 1$.

For any a, b we have

$$(a^m b^n)^{mx} = (a^m b^n)(a^m b^n).....(a^m b^n) \quad mx \text{ times}$$

$$= a^m(b^n a^m b^n.....b^n a^m)b^n$$

$$= a^m(b^n a^m)^{mx-1} b^n$$
$$= a^m(b^n a^m)^{mx}(b^n a^m)^{-1} b^n$$
$$= a^m c^m (b^n a^m)^{-1} b^n \qquad \text{where } c = (b^n a^m)^x$$
$$= c^m a^m (b^n a^m)^{-1} b^n$$
$$= c^m\ a^m a^{-m} b^{-n} b^n = c^m = (b^n a^m)^{mx}$$

Similarly $(a^m b^n)^{ny} = (b^n a^m)^{ny}$

giving $(a^m b^n)^{mx+ny} = (b^n a^m)^{mx+ny}$

$$\Rightarrow a^m b^n = b^n a^m \qquad \text{for all } a, b \in G \qquad \ldots(1)$$

Now $ab = a^{mx+ny}\ b^{mx+ny}$

$$= a^{mx} \cdot (a^{ny}\ b^{mx}) b^{ny}$$
$$= a^{mx}(a^m\ k^m) b^{ny} \text{ where } d = a^y,\ k = b^x$$
$$= a^{mx}(k^m\ d^n) b^{ny} \text{ by (1)}$$
$$= a^{mx} \cdot b^{mx} \cdot a^{ny} \cdot b^{ny}$$
$$= (a^x)^m \cdot (b^x)^m \cdot (a^y)^n \cdot (b^y)^n$$
$$= (b^x)^m \cdot (a^x)^m \cdot (b^y)^n \cdot (a^y)^n$$
$$= b^{mx}(a^{mx} \cdot b^{ny}) \cdot a^{ny} = b^{mx}\ (b^{ny} \cdot a^{mx}) \cdot a^{ny}$$
$$= b^{mx+ny} \cdot a^{mx+ny} = ba.$$

Hence G is abelian.

Remark: In the following problem we give another proof to theorem 6 done earlier.

Problem 6: *Let G be a semi-group, Suppose $\exists\ e \in G$, s.t., $ae = a$ for all $a \in G$ and for each $a \in G$, $\exists\ a' \in G$, s.t., $aa' = e$. Show that G is a group.*

Solution: We first show that G satisfies the right cancellation law.

Let $ac = bc$.

As given $\exists\ c' \in G$, s.t., $cc' = e$

$\therefore$ $(ac)c' = (bc)c'$

$\Rightarrow a(cc') = b(cc')$

$\Rightarrow ae = be \Rightarrow a = b.$

We now show that e is left identity.

Consider, $(ea)a' = e(aa') = e \cdot e = e$

Also $aa' = e$

$\therefore$ $aa' = (ea) = a'$

By right cancellation law,

$$a = ea \quad \text{for all } a \in G$$

$\therefore$ e is also left identify of G.

Again $(a'a)a' = a'(aa') = a'e = a'$

and $ea' = a'$

$$\Rightarrow (a'a)a' = ea'$$

$\Rightarrow a'a = e$ by right cancellation law

$\Rightarrow a'$ is also left inverse of a

So, G is a group.

Problem 7: *If in a semi-group S,* $x^2y = y = yx^2 \quad \forall x, y$, *then show that S is abelian.*

Solution: $x^2y = y \Rightarrow x^2y^2 = y^2$

$yx^2 = y \qquad \forall\, x, y \in S$

$\Rightarrow xy^2 = x \qquad \forall\, x, y \in S$

$\Rightarrow x^2y^2 = x^2$

So $x^2 = y^2 \quad \forall\, x, y \in S$

Now $x^2y = y \Rightarrow y^2y = y \Rightarrow y^3 = y \quad \forall\, y \in S$

Also $yx^2y = y^2$ ...(*i*)

Now $xy^2 = x \Rightarrow xy^2x = x^2$ ...(*ii*)

By (*i*) and (*ii*), $xy^2x = yx^2y$

Since $y = y^3 \quad \forall\, y \in S$, we get

$$\begin{aligned} xy &= (xy)^3 = xy\ xy\ xy \\ &= xy\ xy\ x^3y = x(yx)^2x(xy) \\ &= (yx)x^2(yx)\ (xy) \\ &= yx^3\ yx^2y = yxy\ x^2y \\ &= (yx)xy^2x \\ &= yx^2y^2x \\ &= y(y^2x) \quad (\text{as } y = yx^2) \\ &= y^3x \\ &= yx \qquad (\text{as } y^3 = y) \end{aligned}$$

Thus $xy = yx \ \forall\, x, y \in S$

Hence S is abelian.

Problem 8: *If G is a semi-group such that given* $a \in G$, $\exists$ *unique* $a' \in G$ *such that* $aa'a = a$, *then show that G is a group.*

Solution: Let e, f be idempotents in G, *i.e.*, $e^2 = e$, $f^2 = f$. (See Exercise 8). We show $(ef)^2 = ef$.

Now $ef \in G \Rightarrow \exists\, g \in G$, s.t.,

$(ef)\ g\ (ef) = ef$ ...(*i*)

Also $ef(gefg)\ ef = (efgef)\ gef = (ef)\ gef = ef$

$\Rightarrow g = gefg$ ...(*ii*)

Again, $(ef)\ (ge)\ (ef) = efgef = ef$

$\Rightarrow ge = g$ ...(*iii*)

Also, $ef(fg)\ ef = efgef = ef$

$\Rightarrow fg = g$ ...(*iv*)

Now $g^2 = (ge)\ (fg)$ by (*iii*) and (*iv*)

$= g(ef) = g$ by (*ii*)

i.e., g is an idempotent.

Also, $g^3 = g^2g = gg = g \Rightarrow ggg = g$

But $g(ef)\ g = g$ and so $g = ef$ and

Thus ef is an idempotent, *i.e.*, $(ef)^2 = ef$

Now $(ef)\ f\ (ef) = (ef)\ (ef) = ef$

and $(ef)\ e\ (ef) = ef$

$\Rightarrow f = e$ showing thereby that G has unique idempotent, say e.

Now $aa'a = a \Rightarrow (a'a)^2 = a'a \Rightarrow a'a$ is an idempotent.

$\Rightarrow a'a = e$.

Similarly $aa' = e$

Now $a = aa'a = ae$

$a = aa'a = ea$

$\Rightarrow ae = ea = a \quad \forall\ a \in G$

$\Rightarrow e$ is identity of G.

Also given $a \in G$, $aa' = e = a'a$ showing that a' is inverse of a.

Hence G is a group.

Exercises

1. Check whether the following systems form a group (a semi-group) or not

(*a*) G = set of rational numbers under composition $*$ defined by $a * b = \dfrac{ab}{2}$, a, $b \in G$

(*b*) $G = \{\pm 1, \pm i\}$, where $i = \sqrt{-1}$ under multiplication.

(*c*) $G = \{1, w, w^2\}$ where w is cube root of unity under multiplication.

(*d*) Set of all 2×2 matrices over integers under matrix multiplication.

(*e*) Set of all matrices of the form $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$, $\theta \in \mathbf{R}$, under matrix multiplication.

(*f*) Q = set of all rational numbers under $*$ where $a * b = a + b - ab$.

(*g*) $G = \{2, 4, 6, 8\}$ under multiplication modulo 10.

(*h*) $G = \{1, 2, 3\}$ under multiplication modulo 4.

(*i*) $G = \{(a, b) \mid a, b \in \mathbf{Z}\}$ under $*$ defined by

$(a, b) * (c, d) = (ac + bd, ad + bc)$.

2. Let $M = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \mid a, b \text{ reals}, a + b \neq 0 \right\}$. Show that M is a semi-group under matrix multiplication and has a right identity and a left inverse for each element. Show that M does not form a group.

3. Let G be the set $\{\pm e, \pm a, \pm b, \pm c\}$ where

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ c = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Show that G forms a group under matrix multiplication.

4. Let (G, o) be a group. Define $*$ on G by $a * b = boa$. Is $(G, *)$ a group?

5. Let $\bar{\mathbf{R}} = \mathbf{R} - \{0\}$, where $\mathbf{R}$ = reals. Define $*$ on $\bar{\mathbf{R}}$ by $x * y = xy$ if $x > 0$

$= x/y$ if $x < 0$

Show that $(\bar{\mathbf{R}}, *)$ is non abelian group.

6. Show that a group G is abelian iff $(ab)^2 = a^2b^2$.

7. Prove that a group in which every element is its own inverse is abelian.

8. In a group G, an element a is called *Idempotent* if $a^2 = a$. Show that a is idempotent iff $a = e$.

9. Find all the elements in U_{15}, that satisfy $a^2 = 1$.

10. Show that if G be a group of even order then it has at least one element $(\neq e)$ which is its own inverse.

11. (*i*) Show that the power set of a finite set X is a finite semi-group under intersection, has identity and all elements are idempotent.

(*ii*) Show that a finite semi-group G with identity is a group iff G contains only one idempotent.

12. For any a, x in a group, show that $(x^{-1} ax)^n = x^{-1} a^n x$ where n is a positive integer.

13. If in a semi group S, $x^{k+1} = x$ for some $k \geq 1$ and $xy^k x = yx^k y \quad \forall\ x, y \in S$ then show that S is abelian.

14. Show that a monoid is a group if and only if cancellation laws hold in it.

Subgroups

We have seen that **R**, the set of real numbers, forms a group under addition, and **Z**, the set of integers, also forms a group under addition. Also **Z** is a subset of **R**. It is one of the many situations which prompts us to make

Definition: A non empty subset H of a group G is said to be a subgroup of G, if H forms a group under the binary composition of G.

Obviously, if H is a subgroup of G and K is a subgroup of H, then K is subgroup of G.

If G is a group with identity element e then the subsets $\{e\}$ and G are trivially subgroups of G and we call them the *trivial* subgroups. All other subgroups will be called non-trivial (or proper subgroups).

Thus it is easy to see that the even integers form a subgroup of (**Z**, +), which is a subgroup of (**Q**, +) which is a subgroup of (**R**, +).

Again the subset $\{1, -1\}$ will be a subgroup of $G = \{1, -1, i, -i\}$ under multiplication.

Notice that $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ mod 5 is not a subgroup of **Z** under addition as addition modulo 5 is not the composition of **Z**. Similarly, $\mathbf{Z}_5$ is not a subgroup of $\mathbf{Z}_6$ etc.

We sometimes use the notation $H \leq G$ to signify that H is a subgroup of G and $H < G$ to mean that H is a proper subgroup of G.

It may be a little cumbersome at times to check whether a given subset H of a group G is a subgroup or not by having to check all the axioms in the definition of a group. The following two theorems (especially the second one) go a long way in simplifying this exercise.

Theorem 8: *A non empty subset H of a group G is a subgroup of G iff*

(i) $a, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let H be a subgroup of G then by definition it follows that (i) and (ii) hold.

Conversely, let the given conditions hold in H.

Closure holds in H by (i).

Again $a, b, c \in H \Rightarrow a, b, c \in G \quad \Rightarrow \quad a(bc) = (ab)c$

Hence associativity holds in H.

Also for any $a \in H$, $a^{-1} \in H$ and so by (i)

$aa^{-1} \in H \Rightarrow e \in H$

thus H has identity.

Inverse of each element of H is in H by (ii).

Hence H satisfies all conditions in the definition of a group and thus it forms a group and therefore a subgroup of G.

Theorem 9: *A non void subset H of a group G is a subgroup of G iff* $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: If H is a subgroup of G then, $a, b \in H \Rightarrow ab^{-1} \in H$ (follows easily by using definition).

Conversely, let the given condition hold in H.

That associativity holds in H follows as in previous theorem.

Let $a \in H$ be any element $(H \neq \varphi)$

then $a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

So H has identity.

Again, for any $a \in H$, as $e \in H$

$$ea^{-1} \in H \Rightarrow a^{-1} \in H$$

i.e., H has inverse of each element.

Finally, for any $a, b \in H$,

$a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$

i.e., H is closed under multiplication.

Hence H forms a group and therefore a subgroup of G.

Remark: If the binary composition of the group is denoted by +, the above condition would read as $a, b \in H \Rightarrow a - b \in H$. Note also that e is always in H.

The following theorem may not prove to be very useful in as much as it confines itself to finite subsets only but nevertheless it has its importance.

Theorem 10: *A non empty finite subset H of a group G is a subgroup of G iff H is closed under multiplication.*

Proof: If H is a subgroup of G then it is closed under multiplication by definition, so there is nothing to prove.

Conversely, let H be a finite subset s.t.,

$$a, b \in H \Rightarrow ab \in H$$

Now $a, b, c \in H \Rightarrow a, b, c \in G$

$\Rightarrow a(bc) = (ab)c$

$\therefore$ Associativity holds in H.

$\Rightarrow H$ is a semi-group.

Again, trivially the cancellation laws hold in H (as they hold in G) and thus H is a finite semi-group in which cancellation laws hold. Hence H forms a group.

Aliter: Let H be a finite subset s.t., $a, b \in H \Rightarrow ab \in H$

We show $a \in H \Rightarrow a^{-1} \in H$.

If $a = e$ then $a^{-1} = a \in H$

Let $a \neq e$, then by closure $a, a^2, a^3 \ldots \in H$

Since H is finite, for some n, m, $a^n = a^m$, $n > m$

i.e., $a^{n-m} = e$, $n - m > 1$ as $a \neq e$

i.e., $a^{n-m-1}.\ a = e$

$\Rightarrow a^{n-m-1} = a^{-1}$

where $n-m-1 \geq 1$ and therefore,

$a^{n-m-1} \in H$. Hence $a \in H \Rightarrow a^{-1} \in H$ and thus H is a subgroup of G (Theorem 8).

Example 19: Consider the group $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ under multiplication modulo 20 (See Page 49).

Then $H = \{1, 11\}$ $K = \{1, 9, 13, 17\}$ are subgroups of U_{20} as these are closed under multiplication modulo 20. For instance, $9 \otimes_{20} 13 = 17$, $9 \otimes 17 = 13$ etc.,

whereas $T = \{1, 7, 13, 19\}$ is not a subgroup as $7 \otimes 7 = 9 \notin T$.

See next example also.

Example 20: Let $U_n = \{x \in \mathbf{Z} | 1 \leq x < n, (x, n) = 1\}$ then this forms a group (See Page 49).

Let m be any divisor of n and let

$U_{n(m)} = \{x \in U_n \,|x = 1 \bmod m\}$ then $U_{n(m)}$ forms a subgroup of U_n. See exercises.

Thus, in previous example $n = 20$ and $m = 5$ and 4 in H and K, i.e., $H = U_{20(5)}$ and $K = U_{20(4)}$.

Recall $x = 1 \bmod m$ means $m|(x - 1)$ or that $x = mt + 1$, $t = 0, 1, 2...$

Definition: Let G be a group. Let

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$$

then $Z(G)$ is called *centre* of the group G.

Theorem 11: *Centre of a group G is a subgroup of G.*

Proof: Let $Z(G)$ be the centre of the group G.

Then $Z(G) \neq \varphi$ as $e \in Z(G)$

Again, $x, y \in Z(G) \Rightarrow xg = gx$

$$yg = gy \quad \text{for all } g \in G$$

$$\Rightarrow g^{-1} x^{-1} = x^{-1} g^{-1}$$

$$g^{-1} y^{-1} = y^{-1} g^{-1} \quad \text{for all } g \in G$$

Now $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1}$

$$= (xg)y^{-1} (g^{-1}g)$$

$$= xg(y^{-1} g^{-1})g = xg(g^{-1} y^{-1})g$$

$$= x(gg^{-1})y^{-1}g$$

$$= (xy^{-1})g \quad \text{for all } g \in G$$

$$\Rightarrow \quad xy^{-1} \in Z(G)$$

Hence $Z(G)$ is a subgroup.

Remark: Obviously, G is abelian iff $Z(G) = G$.

Definition: Let G be a group. $a \in G$ be any element. The subset $N(a) = \{x \in G \mid xa = ax\}$ is called *normalizer* or *centralizer* of a in G.

It is easy to see that normalizer is a subgroup of G. (See page 71 also.)

Problem 9: *Find centre of* S_3.

Solution: We have $S_3 = \{I, (12), (13), (23), (123), (132)\}$

Centre of S_3, $Z(S_3) = \{\sigma \in S_3 \mid \sigma\theta = \theta\sigma \text{ for all } \theta \in S_3\}$

Since $(12)(13) = (132)$

$(13)(12) = (123)$

We find (12), (13) do not commute.

$\Rightarrow$ (12) & (13) do not belong to $Z(S_3)$

Again, $(23)(132) = (12)$

$(132)(23) = (13)$

$\Rightarrow$ (23), (132) do not belong to $Z(S_3)$

Also, $(123)(12) = (13)$

$(12)(123) = (23)$

Shows $(123) \notin Z(S_3)$

Hence $Z(S_3)$ contains only I. (See also Problem 55 Page 151)

Problem 10: *Let G be the group of all 2×2 non singular matrices over the reals. Find centre of G.*

Solution: If $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any element of the centre $Z(G)$ of G then it should commute with all members of G. In particular we should have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Rightarrow b = c,\ a = d$$

Also $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ gives

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$$\Rightarrow a + b = a,\ b = c = 0$$

Hence any member $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $Z(G)$ turns out to be of the type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

In other words, members of the centre $Z(G)$ are the 2×2 scalar matrices of G.

Problem 11: *Let G be a group in which*

$$(ab)^3 = a^3b^3$$

$$(ab)^5 = a^5b^5, \quad \textit{for all } a, b \in G$$

Show that G is abelian.

Solution: We first show that $b^2 \in Z(G)$ for all $b \in G$.

We know $(a^{-1}ba)^3 = a^{-1}\, b^3a$

By given condition $(a^{-1}ba)^3 = a^{-3}\,(ba)^3 = a^{-3}\, b^3a^3$

$$\Rightarrow a^{-1}\, b^3a = a^{-3}\, b^3a^3$$

$$\Rightarrow a^2b^3 = b^3a^2 \quad \text{for all } a, b \in G$$

Similarly, $(a^{-1}\, ba)^5 = a^{-1}\, b^5\, a$

$$(a^{-1}\, ba)^5 = a^{-5}\, b^5a^5$$

$$\Rightarrow a^{-1}\, b^5a = a^{-5}\, b^5a^5$$

$$\Rightarrow a^4b^5 = b^5a^4 \Rightarrow a^4b^3b^2 = b^5a^4$$

$$\Rightarrow (a^2)^2\, b^3b^2 = b^5a^4 \Rightarrow b^3a^4b^2 = b^5a^4$$

$$\Rightarrow a^4b^2 = b^2a^4 \Rightarrow aa^3b^2 = b^2a^4$$

$$\Rightarrow ab^2a^3 = b^2a^4$$

$$\Rightarrow ab^2 = b^2a \quad \text{for all } a, b \in G$$

$\therefore$ $b^2 \in Z(G)$ for all $b \in G$

Now $(ab)^4 = (ab)^5\,(ab)^{-1} = a^5b^5b^{-1}\, a^{-1}$

$= a^5b^4a^{-1} = a^5a^{-1}b^4$, as $b^2 \in Z(G) = a^4b^4$

$\therefore$ $(ab)^i = a^i b^i$ for three consecutive integers $i = 3, 4, 5$

So, $ab = ba$ for all $a, b \in G$, by problem done earlier.

Hence G is abelian.

Problem 12: *Show that* $N(x^{-1} ax) = x^{-1} N(a)x$ *for all* $a, x \in G$.

Solution: Let $y \in N(x^{-1} ax)$

then $(x^{-1} ax)\, y = y\, (x^{-1} ax)$

$\Rightarrow y^{-1} x^{-1} axy = x^{-1} ax$

$\Rightarrow xy^{-1} x^{-1} a = axy^{-1} x^{-1}$

$\Rightarrow xy^{-1} x^{-1} \in N(a)$

$\Rightarrow xy^{-1} x^{-1} = b \in N(a)$

$y^{-1} = x^{-1} bx$

$\Rightarrow y = x^{-1} b^{-1} x,\ b^{-1} \in N(a)$ as $b \in N(a)$

$\Rightarrow y \in x^{-1} N(a)x$

$\therefore$ $N(x^{-1} ax) \subseteq x^{-1} N(a)\, x$

Let $z \in x^{-1} N(a)x \Rightarrow z = x^{-1} cx,\ c \in N(a)$

$\therefore$ $z(x^{-1} ax) = (x^{-1} cx)\, (x^{-1} ax)$

$= x^{-1} cax$

$= x^{-1} acx$ as $c \in N(a)$

$= (x^{-1} ax)\, (x^{-1} cx)$

$= (x^{-1} ax)z$

$\Rightarrow z \in N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x \subseteq N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x = N(x^{-1} ax)$ for all $a, x \in G$.

It would be an easy exercise to show that intersection of two subgroups will be a subgroup.

In fact, one can prove that if $\{H_i \mid i \in I\}$ be any set of subgroups of a group G then $\bigcap_{i \in I} H_i$ will be a subgroup of G.

Problem 13: *Show that union of two subgroups may not be a subgroup.*

Solution: Let $H_2 = \{2n \mid n \in \mathbf{Z}\}$

$H_3 = \{3n \mid n \in \mathbf{Z}\}$

where $(\mathbf{Z}, +)$ is the group of integers. H_2 and H_3 will be subgroups of $\mathbf{Z}$. Indeed

$2n - 2m = 2(n - m) \in H_2$

Now $H_2 \cup H_3$ is not a subgroup as $2, 3 \in H_2 \cup H_3$

but $2 - 3 = -1 \notin H_2 \cup H_3$

Can union of two subgroups be a subgroup? The answer is provided by

Theorem 12: *Union of two subgroups is a subgroup iff one of them is contained in the other.*

Proof: Let H, K be two subgroups of a group G and suppose $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

Conversely, let H, K be two subgroups of G s.t., $H \cup K$ is also a subgroup of G. We show one of them must be contained in the other. Suppose it is not true, *i.e.*,

$$H \not\subseteq K, K \not\subseteq H$$

Then $\exists\, x \in H$ s.t., $x \notin K$

$\exists\, y \in K$ s.t., $y \notin H$

Also then $x, y \in H \cup K$ and since $H \cup K$ is a subgroup, $xy \in H \cup K$

$\Rightarrow xy \in H$ or $xy \in K$

If $xy \in H$, then as $x \in H$, $x^{-1}(xy) \in H \Rightarrow y \in H$, which is not true.

Again, if $xy \in K$, then as $y \in K$, $(xy)y^{-1} \in K \Rightarrow x \in K$ which is not true.

i.e., either way we land up with a contradiction.

Hence our supposition that $H \not\subseteq K$ and $K \not\subseteq H$ is wrong.

Thus one of the two is contained in the other. (See exercises also).

Definition: Let H be a subgroup of a group G. For $a, b \in G$, we say a is congruent to b mod H if $ab^{-1} \in H$.

In notational form, we write $a \equiv b \bmod H$.

It is easy to prove that this relation is an equivalence relation. Corresponding to this equivalence relation, we get equivalence classes. For any $a \in G$, the equivalence class of a, we know will be given by

$$cl(a) = \{x \in G \mid x \equiv a \bmod H\}.$$

Definition: Let H be a subgroup of G and let $a \in G$ be any element. Then $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

We show in the following theorem that any right coset of H in G is an equivalence class. To be exact we state and prove:

Theorem 13: *$Ha = \{x \in G \mid x \equiv a \bmod H\} = cl(a)$ for any $a \in G$.*

Proof: Let $x \in Ha$

Then $x = ha$ for some $h \in H$

$\Rightarrow xa^{-1} = h$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow x \equiv a \bmod H$

$\Rightarrow x \in cl(a)$

thus $Ha \subseteq cl(a)$.

Again let $x \in cl(a)$ be any element.

Then $x \equiv a \bmod H$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow xa^{-1} = h$ for some $h \in H$

$\Rightarrow x = ha \in Ha$

thus $cl(a) \subseteq Ha$

and hence $Ha = cl(a)$.

Having established that right cosets are equivalence classes, we are free to use the results that we know about equivalence classes. We can, therefore, say now that *any two right cosets are either equal or have no element in common* and also that *union of all the right cosets of H in G will equal G*.

Remark: Note that a coset is not essentially a subgroup. If G be the Quaternion group then $H = \{1, -1\}$ is a subgroup of G. Take $a = i$, then $Ha = \{i, -i\}$ which is not a subgroup of G. (it doesn't contain identity). See theorem 15 ahead.

Lemma: *There is always a* 1 – 1 *onto mapping between any two right cosets of H in G.*

Proof: Let Ha, Hb be any two right cosets of H in G.

Define a mapping $f : Ha \to Hb$, s.t.,

$f(ha) = hb$

Then $h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$

$\Rightarrow f(h_1a) = f(h_2a)$

i.e., f is well defined.

$f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$

Showing f is 1–1.

That f is onto, is easily seen, as for any $hb \in Hb$, ha would be its pre image.

The immediate utility of this lemma is seen, if the group G happens to be finite, because in that case the lemma asserts that any two right cosets of H in G have the same number of elements. Since $H = He$ is also a right coset of H in G, this leads us to state that all right cosets of H in G have the *same* number of elements as are in H (G, being, of course, finite). We are now ready to prove

Theorem 14 (Lagrange's): *If G is a finite group and H is a subgroup of G then* $o(H)$ *divides* $o(G)$.

Proof: Let $o(G) = n$.

Since corresponding to each element in G, we can define a right coset of H in G, the number of distinct right cosets of H in G is less than or equal to n.

Using the properties of equivalence classes we know

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_t$$

where t = no. of distinct right cosets of H in G.

$$\Rightarrow o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_t)$$

(reminding ourselves that two right cosets are either equal or have no element in common).

$$\Rightarrow o(G) = o(H) + o(Ha) \underset{t \text{ times}}{+ \ldots +} o(H) \quad \text{using the above lemma}$$

$$\Rightarrow o(G) = t.\ o(H)$$

or that $o(H) \mid o(G)$

and we have proved a very important theorem.

But a word of caution here. Converse of Lagrange's theorem does not hold. See under permutation groups.

Remarks: (i) If G is a group of prime order, it will have only two subgroups G and $\{e\}$. See theorem 25 also.

(ii) A subset $H \neq G$ with more than half the elements of G cannot be a subgroup of G.

We have been talking about *right cosets* of H in G all this time. Are there left cosets also? The answer should be an obvious yes. After all we can similarly talk of

$$aH = \{ah \mid h \in H\}, \quad \text{for any } a \in G$$

which would be called a *left coset*. One can by defining similarly an equivalence relation ($a \equiv b \bmod H \Leftrightarrow a^{-1} b \in H$) prove all similar results for left cosets. It would indeed be an interesting 'brushing up' for the reader, by proving these results independently.

We now come to a simple but very important

Theorem 15: *Let H be a subgroup of G then*

(*i*) $Ha = H \Leftrightarrow a \in H$; $aH = H \Leftrightarrow a \in H$

(*ii*) $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $aH = bH \Leftrightarrow a^{-1} b \in H$

(*iii*) *Ha (or aH) is a subgroup of G iff $a \in H$.*

Proof: (*i*) Let $Ha = H$

Since $e \in H$, $ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H$.

Let $a \in H$, we show $Ha = H$.

Let $x \in Ha \Rightarrow x = ha$ for some $h \in H$

Now $h \in H$, $a \in H \Rightarrow ha \in H \Rightarrow x \in H \Rightarrow Ha \subseteq H$

Again, let $y \in H$, since $a \in H$

$ya^{-1} \in H$

$\Rightarrow ya^{-1} = h$ for some $h \in H$

$\Rightarrow y = ha \in Ha$

$\Rightarrow H \subseteq Ha$

Hence $Ha = H$.

(*ii*) $Ha = Hb$

$\Leftrightarrow (Ha)b^{-1} = (Hb)b^{-1}$

$\Leftrightarrow Hab^{-1} = He$

$\Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ using (*i*)

(*iii*) If $a \in H$ then $Ha = H$ which is a subgroup. Conversely, if Ha is a subgroup of G then $e \in Ha$ and thus the right cosets Ha and He have one element e in common and hence $Ha = He = H \Rightarrow a \in H$ by (*i*).

Corresponding results for left cosets can be tackled similarly.

Definition: Let G be a group and H, a subgroup of G. Then *index* of H in G is the number of distinct right (left) cosets of H in G. It is denoted by $i_G(H)$ or $[G:H]$. (See Problem 15).

A look at the proof of Lagrange's theorem suggests that if G is a finite group, then $i_G(H) = \dfrac{o(G)}{o(H)}$.

It is, of course, possible for an infinite group G to have a subgroup $H \neq G$ with finite index.

Consider

Example 21: Let $< \mathbf{Z}, + >$ be the group of integers under addition.

Let $H = \{3n \mid n \in \mathbf{Z}\}$ then H is a subgroup of $\mathbf{Z}$. We show H has only three right cosets in $\mathbf{Z}$ namely H, $H + 1$, $H + 2$.

If $a \in \mathbf{Z}$ be any element ($\neq 0, 1, 2$) then we can write (by division algorithm).

$$a = 3n + r, \qquad 0 \leq r < 3$$

which gives

$$H + a = H + (3n + r) = (H + 3n) + r = H + r$$

where $0 \leq r < 3$

Hence H has only 3 right cosets in $\mathbf{Z}$ and thus has index 3.

Notice, $H - 1 = (H + 3) - 1 = H + (3 - 1) = H + 2$ etc.

Example 22: Let $G = < \mathbf{R} - \{0\}, . >$, *i.e.*, let G be the group of non zero real numbers under multiplication. Let $H = \{1, -1\}$. Then H is a subgroup of G where $i_G(H)$ is infinite. Notice H has infinite number of right cosets in G, these being, $\{2, -2\}$, $\{3, -3\}$, $\{4, -4\}$, ... etc.

Definition: Let H be a subgroup of a group G, we define

$C(H) = \{x \in G \mid xh = hx \text{ for all } h \in H\}$ then $C(H)$ is called *centralizer* of H in G.

Also the set

$$\begin{aligned} N(H) &= \{x \in G \mid xH = Hx\} \\ &= \{x \in G \mid xHx^{-1} = H\} \end{aligned}$$

is called *normalizer* of H in G.

It is an easy exercise to see that both $C(H)$ and $N(H)$ are subgroups of G. See problems ahead.

Again as $\quad x \in C(H) \Rightarrow xh = hx \quad \text{for all } h \in H$

$$\Rightarrow xH = Hx$$

$$\Rightarrow x \in N(H)$$

we notice $C(H) \subseteq N(H)$.

However, $C(H)$ need not be equal to $N(H)$ as consider the Quaternion group $G = \{\pm 1, \pm i, \pm j, \pm k\}$ and let $H = \{\pm 1, \pm i\}$.

Then $N(H) = G$ and $C(H) = \{\pm 1, \pm i\}$.

Showing that $C(H) \neq N(H)$

Remark: (i) One can define $C(H)$ or $N(H)$ in the same way even if H happens to be only a non empty subset of G.

(ii) See page 65. Notice $N(a) = C(a)$, when $H = \{a\}$

Problem 14: *Show that* $C(H) = G \Leftrightarrow H \subseteq Z(G)$.

Solution: Let $C(H) = G$. Let $h \in H$ be any element. Then $x \in G \Rightarrow x \in C(H)$ $\Rightarrow xh = hx \Rightarrow$ any element h in H commutes with all elements of $G \Rightarrow h \in Z(G) \Rightarrow$ $H \subseteq Z(G)$.

Conversely, let $H \subseteq Z(G)$. Let $x \in G$. Since $H \subseteq Z(G)$ each element of H commutes with every element of G.

$$\Rightarrow xh = hx \quad \text{for all } h \in H$$
$$\Rightarrow x \in C(H) \Rightarrow G \subseteq C(H) \Rightarrow G = C(H).$$

Problem 15: *Show that there exists a one-one onto map between the set of all left cosets of H in G and the set of all right cosets of H in G where H is a subgroup of a group G.*

Solution: Let $\Im$ = set of all left cosets of H in G.

$\Re$ = set of all right cosets of H in G.

Define a mapping $\theta : \Im \to \Re$, s.t.,

$$\theta(aH) = Ha^{-1} \quad a \in G$$

θ is well defined as $aH = bH$

$$\Rightarrow a^{-1} b \in H$$
$$\Rightarrow Ha^{-1} = Hb^{-1}$$
$$\Rightarrow \theta(aH) = \theta(bH)$$

Taking the steps backwards, we find θ is 1–1. Again, for any $Ha \in \Re$, $a^{-1}H$ is the required pre-image under θ proving that θ is onto.

If G is finite, then the above result reduces to saying that number of left cosets of H in G is same as the number of right cosets of H in G.

Problem 16: *Let H be a subgroup of a group G and* $N(H) = \{a \in G \mid aHa^{-1} = H\}$. *Prove that N(H) is a subgroup of G which contains H.*

Solution: $N(H) \neq \phi$ subset of G as

$$eHe^{-1} = H \Rightarrow e \in N(H)$$

Let now $a, b \in N(H)$ be any two elements, then

$$aHa^{-1} = H$$
$$bHb^{-1} = H$$

then $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1})b = b^{-1}Hb$

$$\Rightarrow (b^{-1}b)Hb^{-1}b = b^{-1}Hb$$
$$\Rightarrow H = b^{-1}Hb$$
$$\Rightarrow aHa^{-1} = a(b^{-1} Hb)a^{-1}$$
$$\Rightarrow aHa^{-1} = ab^{-1}Hba^{-1}$$
$$\Rightarrow H = (ab^{-1}) H(ab^{-1})^{-1}$$
$$\Rightarrow ab^{-1} \in N(H) \quad \textit{i.e.}, N(H) \text{ is a subgroup of } G.$$

Since $h \in H \Rightarrow hHh^{-1} = H$ $(Ha = H \Leftrightarrow a \in H$ etc.)

we find $h \in N(H)$ showing that $H \subseteq N(H)$.

Problem 17: *Suppose that H is a subgroup of a group G such that whenever* $Ha \neq Hb$ *then* $aH \neq bH$. *Prove that* $gHg^{-1} \subseteq H$ *for all* $g \in G$.

Solution: It is given that if $Ha \neq Hb$ then $aH \neq bH$

thus if $aH = bH$ then $Ha = Hb$. ...(1)

Let now $g \in G$, $h \in H$ be any elements, then

$$(g^{-1}\ h)H = g^{-1}(hH) = g^{-1}H \quad (h \in H)$$

$\therefore$ By (1) $\quad H(g^{-1}\ h) = Hg^{-1}$

$$\Rightarrow (g^{-1}\ h)\ (g^{-1})^{-1} \in H \quad (Ha = Hb \Rightarrow ab^{-1} \in H)$$

$$\Rightarrow g^{-1}hg \in H \quad \text{for all } h \in H$$

$$\Rightarrow g^{-1}\ Hg \subseteq H.$$

Problem 18: *If $G = S_3$ and $H = \{I, (13)\}$, write all the left cosets of H in G.*

Solution:
$$(12)H = \{(12)I, (12)(13)\} = \{(12), (132)\}$$
$$= (123)H \quad \text{(Show!)}$$
$$(23)H = \{(23)I, (23)(13)\} = \{(23), (132)\} = (132)H$$
$$(13)H = H \text{ as } (13) \in H$$
$$IH = H$$

are all the left cosets of H in G.

Definition: Let H and K be two subgroups of a group G. We define $HK = \{hk \mid h \in H, k \in K\}$ then HK will be a non empty subset of G (Sometimes, called the *complex* of H and K). Will it form a subgroup? The answer is provided by

Theorem 16: *HK is a subgroup of G iff $HK = KH$.*

Proof: Let HK be a subgroup of G. We show $HK = KH$

Let $\quad x \in HK$ be any element

Then $\quad x^{-1} \in HK$ (as HK is a subgroup)

$$\Rightarrow x^{-1} = hk \quad \text{for some } h \in H, k \in K$$

$$\Rightarrow x = (hk)^{-1} = k^{-1}\ h^{-1} \in KH$$

thus $\quad HK \subseteq KH$

Again let $\quad y \in KH$ be any element

Then $\quad y = kh \quad$ for some $k \in K$, $h \in H$

$$\Rightarrow \quad y^{-1} = h^{-1}\ k^{-1} \in HK$$

$$\Rightarrow \quad y \in HK \quad \text{(as } HK \text{ is a subgroup)}$$

$$\Rightarrow \quad KH \subseteq HK$$

Hence $\quad HK = KH.$

Conversely, let $HK = KH$.

Let $\quad a, b \in HK$ be any two elements, we show $ab^{-1} \in HK$

$$a, b \in HK \Rightarrow a = h_1k_1 \quad \text{for some } h_1, h_2 \in H$$
$$b = h_2k_2 \qquad\qquad k_1, k_2 \in K$$

Then $\quad ab^{-1} = (h_1k_1)\ (h_2k_2)^{-1} = (h_1k_1)\ (k_2^{-1}h_2^{-1})$

$$= h_1(k_1k_2^{-1})\ h_2^{-1}$$

Now $(k_1k_2^{-1})\,h_2^{-1} \in KH = HK$

thus $(k_1k_2^{-1})\,h_2^{-1} = hk$ for some $h \in H,\ k \in K$

Then $ab^{-1} = h_1(hk) = (h_1h)k \in HK$

Hence HK is a subgroup.

(See another proof later in Problem 21).

Remarks: (*i*) $HK = KH$ does not mean that each element of H commutes with every element of K. It only means that for each $h \in H,\ k \in K,\ hk = k_1h_1$ for some $k_1 \in K$ and $h_1 \in H$.

(*ii*) If G has binary composition +, we define

$$H + K = \{h + k \mid h \in H,\ k \in K\}.$$

Theorem 17: *If H and K are finite subgroups of a group G then*

$$o(HK) = \frac{o(H)\,.\,o(K)}{o(H \cap K)}.$$

Proof: Let $D = H \cap K$ then D is a subgroup of K and as in the proof of Lagrange's theorem, $\exists$ a decomposition of K into disjoint right cosets of D in K and

$$K = Dk_1 \cup Dk_2 \cup \ldots \cup Dk_t$$

and also $$t = \frac{o(K)}{o(D)}$$

Again, $HK = H\left(\bigcup_{i=1}^{t} Dk_i\right)$ and since $D \subseteq H$, $HD = H$

Thus $$HK = \bigcup_{i=1}^{t} Hk_i = Hk_1 \cup Hk_2 \cup \ldots \cup Hk_t$$

Now no two of $Hk_1, Hk_2, \ldots, Hk_t$ can be equal as if $Hk_i = Hk_j$ for some i, j

then $k_ik_j^{-1} \in H \Rightarrow k_ik_j^{-1} \in H \cap K \Rightarrow k_ik_j^{-1} \in D \Rightarrow Dk_i = Dk_j$

which is not true.

Hence $o(HK) = o(Hk_1) + (Hk_2) + \ldots + o(Hk_t)$

$$= o(H) + o(H) + \ldots + o(H)$$

$$= t\ .\ o(H)$$

$$= \frac{o(H)\,.\,o(K)}{o(H \cap K)}$$

which proves the result.

Aliter: We have $HK = \{hk \mid h \in H,\ k \in K\}$.

Let $H \cap K = \{x_1, x_2, \ldots, x_n\}$ and suppose $o(H) = r$, $o(K) = s$

Now $hk = (hx_i)(x_i^{-1}k) \in HK \quad \forall\ i = 1, 2, \ldots, n$

Also $hx_i \in H,\ x_i^{-1}\ k \in K$ as $x_i \in H$ & K

Thus $hk = (hx_i)\left(x_i^{-1}\,k\right) \in HK \quad \forall\ i = 1, 2, \ldots, n$

or that hk can be written in at least n different ways. We show these are the only n ways that hk can be expressed as an element of HK.

Suppose $hk = h_1k_1$

$\Rightarrow h^{-1}h_1 = kk_1^{-1} \in H \cap K$

$\Rightarrow h^{-1}h_1 = x_i$

and $kk_1^{-1} = x_i$ for some $i = 1, 2, ..., n$

or that $h_1 = hx_i$

$k_1 = x_i^{-1}k$

and thus $hk = h_1k_1 = (hx_i)(x_i^{-1}k)$

Hence each hk can be written in exactly n different ways.

Since h can be chosen in r ways, k can be chosen in s ways, we find hk can be chosen in $\frac{rs}{n}$ ways.

Thus $o(HK) = \frac{rs}{n} = \frac{o(H).o(K)}{o(H \cap K)}$.

Note $o(H \cap K) \geq 1$ as $H \cap K \neq \varphi$ as $e \in H \cap K$.

Cor.: If H and K are subgroups of a finite group G such that $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$ then $o(H \cap K) > 1$.

Proof: We have

$$o(G) \geq o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}.\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)}$$

$$\Rightarrow o(H \cap K) > 1.$$

Problem 19: *Suppose G is a finite group of order pq, where p, q are primes and $p > q$. Show that G has at most one subgroup of order p.*

Solution: Suppose H, K are two subgroups of order p.

Then as $o(H \cap K) \mid o(H) = p$, we find

$o(H \cap K) = 1$ or p

If $o(H \cap K) = 1$, then

$$o(HK) = \frac{o(H).o(K)}{o(H \cap K)} = \frac{p.p}{1} = p^2 > pq = o(G) \qquad [p > q \Rightarrow p^2 > pq]$$

which is not possible. Hence $o(H \cap K) = p = o(H)$

and as $H \cap K \subseteq H$, we find $H \cap K = H$

Similarly, $H \cap K = K$ and hence $K = H$.

Later, we will show that there exists at least one subgroup of order p. (See page 210). Thus, for instance, a group of order 15 will have only one subgroup of order 5.

Example 23: Let $G = S_3$, and suppose $H = \{I, (12)\}$, $K = \{I, (13)\}$, then $o(H) = o(K) = 2$ and

$$o(HK) = \frac{2 \times 2}{1} = 4.$$

Since $4 \nmid 6 = o(G)$, HK is not a subgroup of G.

Remark: We have defined the product HK of two subgroups H and K. The same definition can be used for the product, even if H, K happen to be subsets of G. We will be using this a little later when we come to product of two cosets.

Problem 20: *Let H be a non empty subset of a group G. Define* $H^{-1} = \{h^{-1} \in G \mid h \in H\}$. *Show that*

(*i*) *If $HH^{-1} \subseteq H$ then H is a subgroup of G.*

(*ii*) *If $HH \subseteq H$ and $H^{-1} \subseteq H$ then H is a subgroup of G.*

(*iii*) *If H is a subgroup of G then $HH = H$, $H = H^{-1}$ and $HH^{-1} = H$.*

(*iv*) *If H, K are subgroups of G then $(HK)^{-1} = K^{-1}H^{-1}$.*

Solution: (*i*) Let $a, b \in H \Rightarrow a \in H, b^{-1} \in H^{-1}$

$\Rightarrow ab^{-1} \in HH^{-1} \subseteq H \Rightarrow H$ is a subgroup of G.

(*ii*) Let $a, b \in H \Rightarrow ab \in HH \subseteq H$

Again $a \in H \Rightarrow a^{-1} \in H^{-1} \subseteq H \Rightarrow H$ is a subgroup of G.

(*iii*) Let $x \in HH \Rightarrow x = ab$, $a \in H$, $b \in H$

H being a subgroup,

$a, b \in H \Rightarrow ab \in H \Rightarrow x \in H \Rightarrow HH \subseteq H$

Again $h \in H \Rightarrow h = he \in HH \Rightarrow H \subseteq HH$, hence $HH = H$.

Now, $x \in H \Rightarrow x^{-1} \in H \Rightarrow (x^{-1})^{-1} \in H^{-1} \Rightarrow x \in H^{-1} \Rightarrow H \subseteq H^{-1}$

and $a \in H^{-1} \Rightarrow a = b^{-1}$, $b \in H$,

but $b \in H \Rightarrow b^{-1} \in H \Rightarrow a \in H$

$\Rightarrow H^{-1} \subseteq H$ and hence $H = H^{-1}$

it, therefore, follows that $HH^{-1} = H$.

(*iv*) Let $x \in (HK)^{-1} \Rightarrow x = y^{-1}$ where $y \in HK$

$y \in HK \Rightarrow y = hk$, $h \in H, k \in K$

$\Rightarrow y^{-1} = k^{-1}h^{-1} \in K^{-1}H^{-1}$

$\Rightarrow x \in K^{-1}H^{-1}$ or that $(HK)^{-1} \subseteq K^{-1}H^{-1}$

Again, $x \in K^{-1}H^{-1} \Rightarrow x = ab$, $a \in K^{-1}, b \in H^{-1}$

$\Rightarrow a = k^{-1}, b = h^{-1}$ $k \in K, h \in H$

$\therefore x = k^{-1}h^{-1} = (hk)^{-1} = y^{-1}$

where $y = hk \in HK \Rightarrow y^{-1} \in (HK)^{-1} \Rightarrow x \in (HK)^{-1}$

$\Rightarrow K^{-1}H^{-1} \subseteq (HK)^{-1}$. Hence $HK = K^{-1}H^{-1}$

We give a different proof of theorem 16 done earlier in

Problem 21: *Let H, K be subgroups of G. Show that HK is a subgroup of G if and only if HK = KH.*

Solution: Suppose HK is a subgroup of G.

Then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$

using previous problem.

Conversely, let

$$\begin{aligned} HK &= KH \\ (HK)(HK)^{-1} &= (HK)(K^{-1}H^{-1}) \\ &= (HK)\ (KH) = H(KK)H \\ &= H(KH) = H(HK) \\ &= (HH)K = HK \end{aligned}$$

By previous problem then, HK is a subgroup of G.

Exercises

1. Show that intersection of two subgroups of a group G is a subgroup of G.
2. Let G be the Quaternion group. Find centre of G. Find also the normalizer of i in G.
3. Show that a group cannot be written as union of two (proper) subgroups, although it is possible to express it as union of three subgroups.
4. If H is a subgroup of G, show that
   $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ is a subgroup of G.
   Show further that $g^{-1}Hg$ is abelian if H is abelian.
5. Show that $U_{n(m)}$ as defined in example 20 on page 64, is a subgroup of U_n.
6. Let G be a finite abelian group under addition and let $n \in \mathbf{Z}$ be a fixed positive integer. Show that $nG = \{nx \mid x \in G\}$ and $G[n] = \{x \in G \mid nx = 0\}$ are subgroups of G, where 0 is identity of G. (See problem 48 on page 263).
7. If G is a group of order 91, show that it cannot have two subgroups of order 13.
8. If $H \subseteq K$ are two subgroups of a finite group G then show that $i_G(H) = i_G(K)\ i_K(H)$.
9. Show that normalizer of an element a in a group G is a subgroups of G.
10. Show that $H = \{0, 2, 4\}$ is a subgroup of $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ addition modulo 6.
11. Let G be the group of all 3×3 invertible matrices over reals. Show that
    $$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \ a, b, c \in \mathbf{R} \right\}$$ is a subgroup of G.
12. If H and K are subgroups whose orders are relatively prime then show that $H \cap K = \{e\}$.

13. If H and K are two subgroups of finite indices in G then show that $H \cap K$ is also of finite index in G.

14. If $N(H)$ be the normalizer of H in a group G then show that $Z(G) \subseteq N(H)$, where $H \leq G$.

15. Show that for a group G, $Z(G) = \underset{a \in G}{\cap} N(a)$.

16. Show that the centralizer $C(H)$ of a subgroup H of a group G is a subgroup of G.

17. Prove (without using the result from equivalence classes) that two right cosets are either equal or have no element in common.

18. If $o(G) = 6$ and $H \neq K$ are subgroups of G each of order 2 then show that HK cannot be a subgroup of G. Show also that G cannot have two subgroups of order 3.

19. $H = \{I, (12)\}$ and $K = \{I, (23)\}$ are subgroups of S_3 show that HK is not a subgroup of S_3. (See Problem 54 on Page 150 also).

20. Show by an example that we can have an infinite subset H in a group G where H is closed under multiplication but does not form a subgroup of G.

Cyclic Groups

Definition: Order of an element : Let G be a group and $a \in G$ be any element. We say a is of order (or period) n if n is the least +ve integer s.t., $a^n = e$. If binary composition of G is denoted by +, this would read as $na = 0$, where 0 is identity of G.

If it is not possible to find such n, we say a has infinite order. Order of a is be denoted by $o(a)$ or $|a|$. It is obvious that $o(a) = 1$ iff $a = e$.

***Cyclic Group*:** A group G is called a *cyclic* group if $\exists$ an element $a \in G$, such that every element of G can be expressed as a power of a. In that case a is called *generator* of G. We express this fact by writing $G = < a >$ or $G = (a)$.

Thus G is called cyclic if $\exists$ an element $a \in G$ s.t., $G = \{a^n \mid n \in \mathbf{Z}\}$. Again, if binary composition of G is denoted by +, the words 'power of a' would mean multiple of a.

Note we are not saying that generator is unique. Indeed if a is generator so would be a^{-1}. We shall come a little later to the question of number of generators that a cyclic group has. A simple example of a cyclic group is the group of integers under addition, 1 being its generator.

Again the group $G = \{1, -1, i, -i\}$ under multiplication is cyclic as we can express its members as i, i^2, i^3, i^4. Thus i (or $-i$) is a generator of this group.

Example 24: The group $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ addition modulo $n (n \geq 1)$ is a cyclic group. 1 and $-1 = n - 1$ will be its generators. But it can have more generators besides these. (See Theorem 30 ahead).

Consider, $\mathbf{Z}_8 = \{0, 1, 2, \ldots 7\}$ addition modulo 8

Then we can check that 1, 3, 5, 7 will be generators of $\mathbf{Z}_8$

Notice that

$3^1 = 3,\ 3^2 = 3 \oplus 3 = 6,\quad 3^3 = 3 \oplus 3 \oplus 3 = 1$

$3^4 = 3 \oplus 3 \oplus 3 \oplus 3 = 4$ and so on

i.e., $< 3 > = \{3, 6, 1, 4, 7, 2, 5, 0\}$ or that 3

is a generator of $\mathbf{Z}_8$. Observe also that 1, 7 and 3, 5 are each others inverses.

See also page 89.

On the other hand, U_n, the group under multiplication modulo n is not cyclic for every n. For instance U_5 is cyclic. (See Problem 40 on page 135) but U_8 is not cyclic.

Theorem 18: *Order of a cyclic group is equal to the order of its generator.*

Proof: Let $G = < a >$ *i.e.*, G is a cyclic group generated by a.

Case (*i*): $o(a)$ is finite, say n, then n is the least +ve integer s.t., $a^n = e$.

Consider the elements $a^0 = e, a, a^2, ..., a^{n-1}$

These are all elements of G and are n in number.

Suppose any two of the above elements are equal

say $\quad a^i = a^j$ with $i > j$

then $\quad a^i \,.\, a^{-j} = e \Rightarrow a^{i-j} = e$

But $0 < i - j \leq n - 1 < n$, thus $\exists$ a +ve integer $i - j$, s.t., $a^{i-j} = e$ and $i - j < n$, which is a contradiction to the fact that $o(a) = n$.

Thus no two of the above n elements can be equal, *i.e.*, G contains at least n elements. We show it does not contain any other element. Let $x \in G$ be any element. Since G is cyclic, generated by a, x will be some power of a.

Let $\quad x = a^m$

By division algorithm, we can write

$m = nq + r \quad$ where $0 \leq r < n$

Now $\quad a^m = a^{nq+r} = (a^n)^q \,.\, a^r = e^q . a^r = a^r$

$\Rightarrow x = a^r \qquad$ where $0 \leq r < n$

i.e., x is one of $a^0 = e, a, a^2, ..., a^{n-1}$

or G contains precisely n elements

$\Rightarrow o(G) = n = o(a)$

Case (*ii*): $o(a)$ is infinite.

In this case no two powers of a can be equal as if $a^n = a^m$ $(n > m)$ then $a^{n-m} = e$, *i.e.*, it is possible to find a *+ve* integer $n - m$ s.t., $a^{n-m} = e$ meaning thereby that a has finite order.

Hence no two powers of a can be equal. In other words G would contain infinite number of elements.

Problem 22: *If $a \in G$ be of finite order n and also $a^m = e$ then show that $n \mid m$.*

Solution: Let $o(a) = n$, then by definition n is the least *+ve* integer s.t., $a^n = e$.

Suppose $\quad a^m = e \quad$ for some m

By division algorithm, $m = nq + r, \quad$ where $0 \leq r < n$

$$a^m = a^{nq+r}$$

$$\Rightarrow e = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

where $0 \leq r < n$

Since n is such least +ve integer, we must have $r = 0$

i.e., $m = nq$ or that $n \mid m$.

Problem 23: *If G is a finite abelian group then show that $o(ab)$ is a divisor of l.c.m. of $o(a)$, $o(b)$.*

Solution: Let $o(a) = n$, $o(b) = m$, $o(ab) = k$.

Let l = l.c.m. (m, n)

then $m \mid l,\ n \mid l, \quad \Rightarrow l = mr_1,\ l = nr_2$

Now $(ab)^l = a^l b^l$ (G is abelian)

$$= a^{nr_2} b^{mr_1} = e \cdot e = e$$

$$\Rightarrow o(ab) \mid l$$

$$\Rightarrow k \mid l.$$

Problem 24: *If in a group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$ then show that $o(b) = 31$.*

Solution: We have $b^2 = aba^{-1}$

$$\Rightarrow b^4 = (aba^{-1})\ (aba^{-1})$$

$$= ab(a^{-1}a)^{nr} b^2\, ab^{mr1} = ab^2a^{-1}$$

$$= a(aba^{-1})\ a^{-1}$$

$$\Rightarrow b^4 = a^2ba^{-2}$$

$$\Rightarrow b^8 = (a^2ba^{-2})\ (a^2ba^{-2}) = a^2b^2a^{-2}$$

$$= a^2(aba^{-1})a^{-2} = a^3ba^{-3}$$

$$\Rightarrow b^{16} = a^4ba^{-4} \text{ (as above)}$$

$$\Rightarrow b^{32} = a^5ba^{-5} = b \quad \text{as } a^5 = e$$

$$\Rightarrow b^{31} = e \Rightarrow 31 \text{ is a multiple of } o(b)$$

Since 31 is a prime number, it is the least +ve integer such that $b^{31} = e$

$$\Rightarrow o(b) = 31.$$

We are, of course, taking $b \neq e$.

Problem 25: *Let G be a finite group with more than one element. Show that G has an element of prime order.*

Solution: Let $e \neq a \in G$

Consider $a, a^2, \ldots, a^t, \ldots$

Since G is finite, for some integers i and j, $a^i = a^j$, $i > j$.

So, $a^{i-j} = e$

$$\Rightarrow a^n = e,\ n = i - j > 0$$

Since $a \neq e$, $n > 1$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_i's are distinct primes

So, $\left(a^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r - 1}}\right)^{p_r} = e$

$\Rightarrow o\left(a^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r - 1}}\right) = 1$ or p_r

If $o\left(a^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r - 1}}\right) = p_r$, then the result follows

Let $a^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r - 1}} = e$

Then proceeding as above, we get an element of prime order as $a \neq e$.

Problem 26: *Suppose that G is a finite group with the property that every non identity element has prime order. If Z(G) is non trivial, prove that every non identity element of G has the same order.*

Solution: Let $e \neq a \in Z(G)$. Let $o(a)$ = prime p.

Let $b \in G$ such that $o(b)$ = prime q.

Since $a \in Z(G)$, $ab = ba$.

So, $(ab)^{pq} = a^{pq} b^{pq} = e$

$\Rightarrow$ $o(ab)$ divides pq

$\Rightarrow$ $o(ab) = 1$, p or q

If $o(ab) = 1$, then $a = b^{-1}$

$\Rightarrow o(a) = o(b^{-1}) = o(b)$

$\Rightarrow p = q$.

If $o(ab) = p$, then $(ab)^p = e$

$\Rightarrow a^p b^p = e$

$\Rightarrow b^p = e$

$\Rightarrow q = o(b) \mid p \Rightarrow q = p$.

Similarly, if $o(ab) = q$, then $p = q$.

Therefore, every non identity element of G has the same order.

Theorem 19: *A subgroup of a cylic group is cyclic.*

Proof: Let $G = < a >$ and let H be a subgroup of G. If $H = \{e\}$, there is nothing to prove. Let $H \neq \{e\}$. Members of H will be powers of a. Let m be the least +ve integer s.t., $a^m \in H$. We claim $H = < a^m >$.

Let $x \in H$ be any element. Then $x = a^k$ for some k. By division algorithm, $k = mq + r$ where $0 \leq r < m$

$\Rightarrow r = k - mq$

$\Rightarrow a^r = a^k \,.\, a^{-mq} = x \,.\, (a^m)^{-q} \in H$

But m is the least +ve integer s.t., $a^m \in H$, meaning thereby that $r = 0$.

Thus $k = mq$

or that $x = a^k = (a^m)^q$

i.e., any member of H is a power of a^m.

or that H is cyclic, generated by a^m.

See exercise 19 on page 98 for converse.

Remark: Any subgroup of $< \mathbf{Z}, + >$ will therefore, be of the type $n\mathbf{Z}$ = set of multiples of n, where n is an integer (≥ 0). We write $n\mathbf{Z} = < n >$.

Also $m\mathbf{Z} \subseteq n\mathbf{Z}$ if and only if $n \mid m$. So $m\mathbf{Z} = n\mathbf{Z}$ if and only if $m = \pm n$.

Example 25: Let $H = < a > = \{an \mid n \in \mathbf{Z}\} = a\mathbf{Z}$

$K = < b > = \{bm \mid m \in \mathbf{Z}\} = b\mathbf{Z}$

be two subgroups of $< \mathbf{Z}, + >$, then $\mathbf{Z}$ being abelian, $H + K = K + H$

$\Rightarrow H + K$ is a subgroup of $\mathbf{Z}$.

[Note here $HK = H + K$].

We show $H + K = < d > = d\mathbf{Z}$, where d = g.c.d.(a, b)

Now $x \in H + K$

$\Rightarrow$ $x \in < a > + < b >$

$\Rightarrow$ $x = an + bm, \quad n, m \in \mathbf{Z}$

$\Rightarrow$ $x \in < d >$ [as $d \mid a, d \mid b \Rightarrow d \mid an + bm \Rightarrow d \mid x$]

Thus $H + K \subseteq < d >$.

Again, $y \in < d > \Rightarrow y = td$

$\Rightarrow y = t(ax + by) = atx + bty \in H + K$

Hence $H + K = < d >$

i.e., $a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$.

Theorem 20: *A cyclic group is abelian.*

Proof: Let $G = < a >$. If $x, y \in G$ be any elements then $x = a^n$, $y = a^m$ for some integers m, n.

Now $xy = a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n = y \cdot x$

Hence G is abelian.

Remark: In view of the above result, all non abelian groups are non-cyclic. $< \mathbf{Q}, + >$ the group of rationals under addition serves as an example of an abelian group which is not cyclic. For, suppose $\frac{m}{n} \in \mathbf{Q}$ is a generator of $\mathbf{Q}$, then any element of $\mathbf{Q}$ should be a multiple of $\frac{m}{n}$. Now $\frac{1}{3n} \in \mathbf{Q}$, and if $\frac{m}{n}$ is a generator, we should be able to write $\frac{1}{3n} = k \frac{m}{n}$, for some k

$$\Rightarrow \frac{1}{3} = km$$

Which is not possible as k, m are integers, whereas $\frac{1}{3}$ is not. Hence no element can act as generator of $\mathbf{Q}$.

Klein's four group (See page 154) would be an example of a finite abelian group which is not cyclic. It is the group of matrices $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, $\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$ and $\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ under matrix multiplication.

Another such group would be U_8. see exercise 5.

Theorem 21: *If G is a finite group, then order of any element of G divides order of G.*
Proof: Let $a \in G$ be any element.

Let $H = \{a^n \mid n \text{ an integer}\}$

then H is a cyclic subgroup of G, generated by a, as

$$x, y \in H \Rightarrow x = a^n, y = a^m$$

$$\therefore \quad xy^{-1} = a^n \,.\, a^{-m} = a^{n-m} \in H$$

By Lagrange's theorem $o(H) \mid o(G)$. But $o(H) = o(a)$

$$\therefore \quad o(a) \mid o(G).$$

Cor.: If G is a finite group then for any $a \in G$

$$a^{o(G)} = e$$

Proof: $o(a) \mid o(G) \Rightarrow o(G) = o(a)k$ For some k

Now $a^{o(G)} = a^{o(a)k} = (a^{o(a)})^k = e^k = e$

Thus any element of a finite group, has finite order (which is less than or equal to the order of the group).

Example 26: The group $< \mathbf{Z}, + >$ of integers is an example of a group in which each non identity element is of infinite order.

As another example consider $G = \{2^r : r = 0, \pm 1, \ldots\}$

then we know G forms a group under multiplication (see examples of groups). No non identity element in G has finite order as

$$(2^r)^n = 1 \text{ iff } 2^{rn} = 1$$

$$\text{iff } r = 0 \text{ or } n = 0.$$

Remark: If G is a finite group of order n and $\exists$ an element $a \in G$, s.t., $o(a) = n$ then G is cyclic, generated by a. Clearly $o(a) = n$ gives $a^n = e$, and lesser powers not equal to e and thus $G = \{a, a^2, \ldots, a^n = e\}$.

Problem 27: *Show that a group of even order has an element of order 2 and that the number of elements of order 2 is odd.*

Solution: Let $o(G) =$ even

Let $H = \{x \in G \mid x^2 = e\}$, $K = \{x \in G \mid x^2 \neq e\}$,

Then $G = H \cup K$

Now, $x \in K \Rightarrow x^{-1} \neq x$ also is in K.

$\Rightarrow$ number of elements in K is even and thus number of elements in H will also be even.

Since $e \in H$ ($e^2 = e$), $\exists$ some $x \in H$, s.t., $x \neq e$.

Now, $x \neq e$, $x \in H \Rightarrow o(x) = 2$

$\Rightarrow G$ has an element of order 2.

Every element of order 2 is in H, and as $e \in H$, $o(H)$ = even, the number of elements of order 2 is odd.

Problem 28: Let G be a finite group whose order is not divisible by 3. Suppose $(ab)^3 = a^3b^3$ for all $a, b \in G$, then show that G is abelian.

Solution: Let $a, b \in G$ be any elements.

Then as $(ab)^3 = a^3b^3$

we get $ababab = a^3b^3$

$\Rightarrow baba = a^2b^2$ (cancellation)

$\Rightarrow (ba)^2 = a^2b^2$ ...(1)

Again as $(ba)^3 = b^3a^3$

we get $(ba)(ba)^2 = b^3a^3$

$\Rightarrow (ba)a^2b^2 = b^3a^3$ using (1)

$\Rightarrow a^3b^2 = b^2a^3$ ...(2)

Consider now $(a^{-1}b^{-2}ab^2)^3 = (a^{-1})^3 (b^{-2}ab^2)^3 = a^{-3} (b^{-2}ab^2)^3$

$= a^{-3} (b^{-2}a^3b^2)$

$= a^{-3} (b^{-2}b^2a^3)$ from (2)

$= a^{-3}a^3 = e$

$\Rightarrow o(a^{-1}b^{-2}ab^2) \mid 3$

$\Rightarrow o(a^{-1}b^{-2}ab^2) = 1$ or 3

If $o(a^{-1}b^{-2}ab^2) = 3$ then $3 \mid o(G)$ which is not true.

Hence $o(a^{-1}b^{-2}ab^2) = 1$

$\Rightarrow a^{-1}b^{-2}ab^2 = e$

$\Rightarrow ab^2 = b^2a$ ...(3)

Again from (1) $(ba)^2 = a^2b^2 = a(ab^2) = a(b^2a)$ using (3)

$\Rightarrow (ba)\ (ba) = ab^2a$

$\Rightarrow bab = ab^2 \Rightarrow ba = ab$

or that G is abelian.

The result that we are going to prove now might raise doubts in the minds of the reader as to the validity of the assertion we made earlier that converse of Lagrange's theorem does not hold. But we promise to prove that little later. For now we prove

Theorem 22: *Converse of Lagrange's theorem holds in finite cyclic groups.*

Proof: Let $G = < a >$ be a finite cyclic group of order n.

Then $o(G) = o(a) = n$

Suppose $m \mid n$. We show $\exists$ a subgroup of G having order m.

Since $m \mid n$, $\exists\ k$ s.t., $n = mk$

Let H be the cyclic group generated by a^k

then H is a subgroup of G and $o(H) = o(a^k)$

We show $o(a^k) = m$

Now $(a^k)^m = a^{km} = a^n = e$, as $o(a) = n$

Suppose now, that $(a^k)^t = e$

Then $a^{kt} = e$

$\Rightarrow o(a) \mid kt \Rightarrow n \mid kt$

$\Rightarrow km \mid kt \Rightarrow m \mid t$

thus $o(a^k) = m$

which proves the result.

Remark: One can go a step further here and show that such a subgroup (as taken above) would also be unique. Suppose H' is another subgroup of G s.t., $o(H') = m$. Since H' is a subgroup of a cyclic group $G = < a >$, H' will be generated by some power of a.

Let $H' = < a^p >$

By division algorithm,

$p = kq + r \qquad 0 \leq r < k$

$\Rightarrow mp = mkq + mr \qquad 0 \leq mr < mk$

$\Rightarrow a^{mp} = a^{mkq + mr} = (a^{mk})^q \cdot a^{mr}$

$= a^{mr} \qquad (o(a) = n = mk)$

Now $o(H') = o(a^p) = m$

$\Rightarrow (a^p)^m = e$

thus $a^{mr} = e$ where $0 \leq mr < n$

But this $\Rightarrow mr = 0$ (as $o(a) = n$)

$\Rightarrow r = 0$ as $m \neq 0$

hence $p = kq$

Thus $H' = < a^p > = < a^{kq} > \subseteq < a^k > = H$

But $o(H') = o(H)$

$\Rightarrow H = H'$.

We thus conclude:

Theorem 23: *If G is a finite cyclic group of order n then the number of distinct subgroups of G is the number of distinct divisors of n, and there is a unique subgroup of G of any given order.*

So subgroups of G are of the type $< a^k >$ where k is a divisor of n and $< a^{n/m} >$ is the unique subgroup of order m. As a particular case, suppose $G = < a >$ has order 30. Since divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30, $\exists$ eight subgroups of G, namely

$$< a > = \{e, a, a^2, ..., a^{29}\} = G$$

$< a^2 > = \{e, a^2, a^4, ..., a^{28}\}$

$< a^3 > = \{e, a^3, a^6, ..., a^{27}\}$

$< a^5 >, < a^6 >, < a^{10} >, < a^{15} >$ and $< a^{30} > = \{e\}$ having order 30, 15, 10, 6, 5, 3, 2, 1.

Consider again, the cyclic group $\mathbf{Z}_{30} = \{0, 1, 2, ..., 29\}$ under addition modulo 30 . $o(\mathbf{Z}_{30}) = 30$ and as 30 has 8 divisors 1, 2, 3, 5, 6, 10, 15, 30, $\mathbf{Z}_{30}$ will have eight subgroups namely

$< 1 > = \{0, 1, 2, ..., 29\} = \mathbf{Z}_{30}$

$< 2 > = \{0, 2, 4, ..., 28\}$

$< 3 > = \{0, 3, 6, ..., 27\}$

$< 5 >, < 6 >, < 10 >, < 15 >, < 30 > = \{0\}$

having order 30, 15, 10, 6, 5, 3, 2, 1.

In view of the above theorem these would be the only subgroups of $\mathbf{Z}_{30}$.

Problem 29: *Let G be a cyclic group of order n and suppose d divides n. Show that* $x^d = e$ *has exactly d solutions.*

Solution: Let $G = < a >$, then $o(G) = o(a) = n$. Since $d \mid n$, there exists a unique subgroup H of G with order d. Let $H = < b >$

Then $o(H) = o(b) = d$.

$$H = \{b, b^2, ..., b^{d-1}, b^d = e\}$$

If $b^i \in H$ be any element, then

$$(b^i)^d = (b^d)^i = e$$

Thus, every element of H is a solution of $x^d = e$, which gives d distinct solutions in G.

Let now $c \in G$ be any solution of $x^d = e$ then $c^d = e$

and, therefore, $o(c) \mid d$. If $o(c) = m$, then $m \mid d = o(H)$ and thus there exists a subgroup K of H s.t., $o(K) = m$. since K is unique of order m, and $< c >$ is also of order m, $K = < c >$ or that $< c > \subseteq H$ as $K \subseteq H$ and so $c \in H$ and thus any solution of $x^d = e$ is in H.

Hence there exist exactly d solutions.

Theorem 24: *A group G of prime order must be cyclic and every element of G other than identity can be taken as its generator.*

Proof: Let $o(G) = p$, a prime

Take any $a \in G$, $a \neq e$

and let $H = \{a^n \mid n$ an integer$\}$ then H is a cyclic subgroup of G.

$\therefore$ $o(H) \mid o(G) \Rightarrow o(H) = 1$ or p

But $o(H) \neq 1$ as $a \in H$, $a \neq e$,

Thus $o(H) = p \Rightarrow H = G$, *i.e.*, G is a cyclic group generated by a. Since a was taken as any element (other than e), any element of G can act as its generator.

(See also theorem 30 later).

Cor.: A group of prime order is abelian.

Theorem 25: *A group G of prime order cannot have any non trivial subgroups.*

Proof: If H is any subgroup of G then as $o(H) \mid o(G) = p$, a prime

we find $o(H) = 1$ or p

i.e., $H = \{e\}$ or $H = G$.

Theorem 26: *A group of finite composite order has at least one non-trivial subgroup.*

Proof: Let $o(G) = n = rs$ where $1 < r, s < n$

Since $n > 1$, $\exists\ e \neq a \in G$. Consider a^r.

Case (*i*): $a^r = e$

then $o(a) \leq r$, let $o(a) = k$

then $1 < k \leq r < n$ $(k > 1$, as $a \neq e)$

Let $H = \{a, a^2, a^3, ..., a^k = e\}$

then H is a non empty finite subset of G and it is closed under multiplication, thus H is a subgroup of G. Since $o(H) = k < n$, we have proved the result.

Case (*ii*): $a^r \neq e$, then since $(a^r)^s = a^{rs} = a^n = a^{o(G)} = e$

$o(a^r) \leq s$. Let $o(a^r) = t$ then $1 < t \leq s < n$.

If we take $K = \{a^r, a^{2r}, ..., a^{tr} = e\}$ then K is a non empty finite subset of G, closed under multiplication and is therefore a subgroup of G. Its order being less than n, it is the required subgroup.

Theorem 27: *If G is a group having no non-trivial subgroups then G must be finite having prime order.*

Proof: Suppose G has infinite order.

Then we can find $a \in G$, s.t., $a \neq e$.

Let $H = < a >$, then H is a cyclic subgroup of G and $H \neq \{e\}$. But G has no non-trivial subgroups.

Thus $H = G$

$\Rightarrow G = < a >$

Consider now the subgroup $K = < a^2 >$

Now $a \notin < a^2 >$, because if $a \in < a^2 >$ then $a = a^{2t}$ for some integer t

$\Rightarrow a^{2t-1} = e \Rightarrow o(a) \leq 2t - 1$

meaning thereby that $o(a)$ is finite, which is not true. Thus $a \notin < a^2 >$.

Again $< a^2 > \neq \{e\}$, because then $a^2 = e$ would again mean that $o(a)$ is finite (≤ 2).

Thus $< a^2 >$ is a non-trivial subgroup of G which is not possible. Hence $o(G)$ cannot be infinite.

So $o(G)$ is finite and as it cannot be composite by previous theorem, it must be prime.

Summing up, what we have done above proves

Theorem 28: *The only groups which have no non-trivial subgroups are the cyclic groups of prime order and the group* $\{e\}$.

All this time we have been talking about cyclic groups and their generators without being very sure as to how many generators a cyclic group could have. To resolve this, we consider

Theorem 29: *An infinite cyclic group has precisely two generators.*

Proof: Let $G = < a >$ be an infinite cyclic group.

As mentioned earlier, if a is a generator of G then so would be a^{-1}.

Let now b be any generator of G,

then as $b \in G$, a generates G, we get $b = a^n$ for some integer n

again as $a \in G$, b generates G, we get $a = b^m$ for some integer m

$$\Rightarrow a = b^m = (a^n)^m = a^{nm}$$

$$\Rightarrow a^{nm-1} = e \Rightarrow o(a) \text{ is finite and } \leq nm - 1$$

Since $o(G) = o(a)$ is infinite, the above can hold only if

$$nm - 1 = 0 \Rightarrow nm = 1$$

$$\Rightarrow m = \frac{1}{n} \text{ or } n = \pm 1 \text{ as } m, n \text{ are integers.}$$

i.e., $b = a$ or a^{-1}

In other words, a and a^{-1} are precisely the generators of G.

Question to be answered now is how many generators a finite cyclic group would have. Before we come to the answer we first define what is popularly known as the ***Euler's φ function*** (or Euler's totient function).

For any integer n, we define $\varphi(1) = 1$ and for $n > 1$, $\varphi(n)$ to be the number of +ve integers less then n and relatively prime to n. As an example $\varphi(6) = 2$, $\varphi(10) = 4$ etc.

Note 1, 5 are less than 6 and relatively prime to 6 and 1, 3, 7, 9 (four in number) are less than 10 and relatively prime to 10 etc. Obviously, $\varphi(p) = p - 1$, if p is a prime. The following two results can be helpful at times.

(*i*) If $p_1, p_2, \ldots, p_n$ are distinct prime factors of n (>1), then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

(*ii*) If m, n are co-prime then

$\varphi(mn) = \varphi(m)\ \varphi(n)$, $(m, n \geq 1)$

We are now ready to prove

Theorem 30: *Number of generators of a finite cyclic group of order n is* $\varphi(n)$.

Proof: Let $G = < a >$ be a cyclic group of order n

then $o(a) = o(G) = n$

We claim a^m is generator of G iff $(m, n) = 1$, *i.e.*, m, n are relatively prime.

[For instance, if $n = 8$, then $\varphi(8) = 4$ will be number of generators as we will show a, a^3, a^5, a^7 will generate G and no other element can generate G. So here m can have values 1, 3, 5, 7].

Let now a^m be a generator of G for some m

Since $a \in G$, $a = (a^m)^i$ for some i

$$\Rightarrow a^{mi-1} = e \Rightarrow o(a) \mid mi - 1$$

$$\Rightarrow n \mid mi - 1$$

$\Rightarrow mi - 1 = nj$ for some integer j

i.e., $mi - nj = 1$

$\Rightarrow (m, n) = 1.$

Conversely, let $(m, n) = 1$

Then $\exists$ integers x and y s.t.,

$mx + ny = 1$

$\Rightarrow a^{mx + ny} = a$

$\Rightarrow a^{mx} \cdot a^{ny} = a$

$\Rightarrow a^{mx} (a^n)^y = a$

$\Rightarrow a^{mx} = a$ as $o(a) = n$

$\Rightarrow a = (a^m)^x$

Since every element of G is a power of a and a itself is a power of a^m, we find a^m generates G, which proves our result.

Remark: We thus realize that if a is a generator of a finite cyclic group G of order n, then other generators of G are of the type a^m where m and n are coprime.

See also, Example 24 on page 78.

In fact an integer k will be a generator of $\mathbf{Z}_n$ if and only if k and n are coprime, and thus generators of $\mathbf{Z}_n$ would indeed be the elements of U_n.

Theorem (Euler's) 31: *Let a, n $(n \geq 1)$ be any integers such that* g.c.d. $(a, n) = 1$. *Then*

$a^{\varphi(n)} \equiv 1 \ (mod\ n)$.

Proof: Let $U_n = \{x \mid x \text{ is an integer, } (x, n) = 1, 1 \leq x < n\}$

Then U_n is a group under multiplication modulo n.

By definition of Euler's φ-function,

$o(U_n) = \varphi(n)$.

If $n = 1$, then $\varphi(n) = \varphi(1) = 1$ and $a^{\varphi(n)} = a^1 \equiv 1 \pmod 1$ (as 1 divides $a - 1$)

Let $n > 1$

Now by Euclid's algorithm

$a = nq + r$, for some integers q, r where $0 \leq r < n$.

If $r = 0$. then $a = nq \Rightarrow n \mid a \Rightarrow (a, n) = n > 1$, a contradiction

$\therefore$ $1 \leq r < n$

Also $(r, n) = d \Rightarrow d \mid r,\ d \mid n \Rightarrow d \mid a - nq,\ d \mid nq$

$\Rightarrow d \mid a,\ d \mid n$

$\Rightarrow d \mid (a, n) = 1$

$\Rightarrow d = 1$

$\therefore$ $(r, n) = 1$ and $1 \leq r < n$

$\Rightarrow r \in U_n$

Also $a = nq + r \Rightarrow a \equiv r \pmod n$

It follows from Lagrange's theorem that,

$$r \otimes r \otimes \ldots \otimes r = \text{identity of } U_n = 1 \quad [a^{o(G)} = e]$$

where $\otimes$ is composition multiplication modulo n in U_n and $\varphi(n)$ is order of group U_n.

$\therefore$ $r^{\varphi(n)} - nq_1 = 1$, for some integer q_1

$\Rightarrow r^{\varphi(n)} \equiv 1 \pmod{n}$

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

so $a \equiv r \pmod{n} \Rightarrow a^{\varphi(n)} \equiv r^{\varphi(n)} \pmod{n}$.

Theorem (Fermat's) 32: *For any integer a and prime p,*

$$a^p \equiv a \pmod{p}.$$

Proof: If $(a, p) = 1$, then by Euler's theorem

$a^{\varphi(p)} \equiv 1 \pmod{p}$

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ as $\varphi(p) = p - 1$

$\Rightarrow a^{p} \equiv a \pmod{p}$

If $(a, p) = p$, then $p \mid a \Rightarrow p \mid a^p$

$\therefore$ $p \mid a^p - a$

$\Rightarrow a^p \equiv a \pmod{p}$.

(Note $(a, p) = 1$ or p as 1 and p are only divisors of p).

Problem 30: *Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.*

Solution: Suppose p and $p + 2$ are consecutive primes, $p > 3$. We show that 12 divides their sum.

$p > 3 \Rightarrow$ g.c.d. $(p, 3) = 1$

$\Rightarrow p^2 \equiv 1 \pmod{3}$ by Fermat's theorem

$\Rightarrow 3 \mid p^2 - 1$

$\Rightarrow 3 \mid (p - 1)(p + 1)$

If $3 \mid p - 1$, then $p - 1 = 3k \Rightarrow p = 3k + 1 \Rightarrow p + 2 = 3k + 3 =$ multiple of 3.

But $p + 2$ is a prime > 3.

So, we get a contradiction

Therefore, $3 \mid p + 1 \Rightarrow$ $p + 1 =$ multiple of 3

Since p is odd, $p + 1$ is also a multiple of 2

So, $p + 1$ is a multiple of 6.

Therefore, $p + (p + 2) = 2p + 2 = 2(p + 1) =$ multiple of 12.

$\Rightarrow$ $12 \mid p + (p + 2)$

Suppose p, $p + 2$, $p + 4$ are three consecutive odd integers that are prime, $p > 3$.

By above $12 \mid 2p + 2$, $12 \mid (p + 2) + (p + 4) = 2p + 6$,

So, $12 \mid 2p + 6 - (2p + 2) = 4$, a contradiction

Hence, 3, 5 and 7 are only three consecutive odd primes.

Problem 31: *Show that if G is a group of order* 10 *then it must have a subgroup of order* 5.

Solution: By Lagrange's theorem such a subgroup can exist.
We first claim that all elements of G cannot be of order 2. Suppose it is so.
Let $a, b \in G$ be two different elements with order 2.
Let $H = < a >$, $K = < b >$ be the cyclic subgroups generated by a and b
then $o(H) = 2$, $o(K) = 2$
Since all elements of G are of order 2, it must be abelian (see exercises).
$\therefore$ $HK = KH \Rightarrow HK$ is a subgroup of G

and as $$o(HK) = \frac{o(H) \, . \, o(K)}{o(H \cap K)} = \frac{2 \times 2}{1} = 4$$

[Note $H \cap K = \{e\}$ as $a \neq b$]
By Lagrange's theorem $o(HK)$ would divide $o(G)$
i.e., $4 \mid 10$ which is not true hence our assumption is wrong and thus all elements of G cannot have order 2.
Again, since G is finite, $o(a) \mid o(G)$ for all $a \in G$
$\Rightarrow \exists$ at least one element $a \in G$, s.t., $o(a) = 5$ or 10.
If $o(a) = 5$, then $H = < a >$ is a subgroup of order 5.
If $o(a) = 10$, then $H = < a^2 >$ is a subgroup of order 5.
In any case our result is proved.

Problem 32: *Let G be a group such that intersection of all its subgroups which are different from* $\{e\}$ *is a subgroup different from* $\{e\}$. *Prove that every element of G has finite order.*

Solution: Let $a \in G$ be any element.

If $a = e$, $o(a) = 1$

Let $a \neq e$ and suppose $o(a)$ is not finite.

Consider the cyclic subgroups $< a >$, $< a^2 >$, $< a^3 >$, ...

Since each $< a^i > \neq \{e\}$ as $o(a)$ is not finite

$< a > \cap < a^2 > \cap < a^3 > \cap \ldots \neq \{e\}$ by given condition.

As intersection of cyclic subgroups is cyclic subgroup

$$\bigcap_i < a^i > = < a^m > \text{ for some integer } m$$

Again, $< a^m > \subseteq < a^i >$ for all i

In particular, $< a^m > \subseteq < a^{2m} >$

But $< a^{2m} > \subseteq < a^m >$

(multiples of $2m$ are multiples of m)

$$\Rightarrow \langle a^m \rangle = \langle a^{2m} \rangle$$

Thus $a^m \in \langle a^m \rangle \Rightarrow a^m \in \langle a^{2m} \rangle$

$$\Rightarrow a^m = (a^{2m})^k$$

$$\Rightarrow a^{m(2k-1)} = e$$

$\Rightarrow o(a)$ is finite, a contradiction.

Hence the result follows.

Theorem 33: *If G is a finite group of order n and for every divisor d of n $\exists$ unique subgroup of order d, then G is cyclic.*

Proof: Let $d \mid n$.

Define $A(d) = \{x \in G \mid o(x) = d\}$

Suppose $A(d) \neq \varphi$. Then $\exists\ x \in G$ s.t., $o(x) = d$.

Let $H = \langle x \rangle$. Then $o(x) = o(H) = d$. This gives $\varphi(d)$ generators of H or $\varphi(d)$ elements of order d in H. If $\exists\ y \in G$, $y \notin H$ s.t., $o(y) = d$, then $K = \langle y \rangle$ is a subgroup of order d. It is given that G has unique subgroup of order d. So, $K = H \Rightarrow y \in H$, a contradiction. Thus, the number of elements in G of order d is $\varphi(d)$.

So, $o(A(d)) = \varphi(d)$ if $A(d) \neq \varphi$

and $o(A(d)) = 0$ if $A(d) = \varphi$ for all $d \mid n$

Clearly, $G = \bigcup_{d|n} A(d)$

Let $d_1, \ldots, d_s$ be all divisors of n.

Suppose $A(d_1) = \varphi, \ldots, A(d_i) = \varphi$

and $A(d_{i+1}) \neq \varphi, \ldots, A(d_s) \neq \varphi$

(Note, if $A(d) = \varphi$ for all $d \mid n$, then $o(G) = 0$, a contradiction. So, $A(d) \neq \varphi$ for some $d \mid n$)

$\therefore$ $o(A(d_1)) = \ldots = o(A(d_i)) = 0$

and $o(A(d_{i+1})) = \varphi(d_{i+1}) \ldots, o(A(d_s)) = \varphi(d_s)$

Now $G = \bigcup_{d|n} A(d) \Rightarrow o(G) = \sum_{d|n} o(A(d))$

$$\Rightarrow n = \varphi(d_{i+1}) + \ldots + \varphi(d_s)$$

By problem 26, $n = \sum_{d|n} \varphi(d)$

$$\Rightarrow \varphi(d_1) + \ldots + \varphi(d_i) + \varphi(d_{i+1}) + \ldots + \varphi(d_s) = \varphi(d_{i+1}) + \ldots + \varphi(d_s)$$

$$\Rightarrow \varphi(d_1) + \ldots + \varphi(d_i) = 0, \text{ a contradiction}$$

So, $A(d) \neq \varphi$ for all $d \mid n$. In particular

$A(n) \neq \varphi \Rightarrow \exists\ x \in A(n) \Rightarrow \exists\ x \in G$ s.t., $o(x) = n = o(G) \Rightarrow G$ is a cyclic group.

Problem 33: *Show that in a cyclic group of order n, $\exists\ \varphi(m)$ elements of order m for every divisor m of n. Deduce that $n = \sum_{d|n} \varphi(d)$.*

Solution: Let m divide n. Then $\exists$ a unique subgroup H of G, s.t., $o(H) = m$.

Let $H = < b >$

Then $m = o(H) = o(b)$

The number of elements of order m in H equals the number of generators of H. But the number of generators of H is $\varphi(m)$. So, the number of elements of order m in H is $\varphi(m)$. If $k \in G$ s.t., $o(k) = m$, then $K = < k >$ has order m. Since G, has unique subgroup of order m, $K = H$.

$\therefore$ $k \in H$. So, all elements of order m belong to H.

This gives total number of elements of order m in G to be $\varphi(m)$.

Let $a \in G$ s.t., $o(a) = d$. Then $d \mid o(G) = n$.

From above $\exists$ $\varphi(d)$ elements of order d in G. In this way, count all elements of G to get

$$n = \sum_{d|n} \varphi(d).$$

Problem 34: *Let G be a group.*

Show that $o(a^n) = \dfrac{o(a)}{(o(a), n)}$ *for all* $a \in G$

where n is an integer and $(o(a), n)$ = *g.c.d.* $(o(a), n)$.

Solution: Let $o(a) = m$.

Let $d = (m, n) \Rightarrow \dfrac{m}{d}, \dfrac{n}{d}$ are integers

$\therefore$ $(a^n)^{m/d} = (a^m)^{n/d} = e^{n/d} = e$

Let $(a^n)^r = e \Rightarrow a^{nr} = e$

$\Rightarrow o(a) \mid nr$

$\Rightarrow m \mid nr$

$\Rightarrow \dfrac{m}{d} \Big| \dfrac{n}{d} r$

$\Rightarrow \dfrac{m}{d} \mid r$ as $\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = 1$

$\Rightarrow r \geq \dfrac{m}{d}$

$\therefore$ $o(a^n) = \dfrac{m}{d} = \dfrac{o(a)}{(o(a), n)}$.

Problem 35: *Let* $a \in G$ *be such that o(a) = n. Let* $H = < a^r >$, $K = < a^s >$. *Show that* $H \subseteq K$ *iff g.c.d.* (n, s) *divides g.c.d* (n, r). *Hence deduce that* $H = K$ *iff g.c.d*(n, s) = *g.c.d*(n, r).

Solution: Suppose $H \subseteq K$ then $o(H) \mid o(K)$

$\Rightarrow o(<a^r>) \mid o(<a^s>)$

$\Rightarrow \dfrac{o(a)}{(o(a), r)}$ divides $\dfrac{o(a)}{(o(a), s)}$ (see above problem)

$\Rightarrow \frac{n}{(n,r)}$ divides $\frac{n}{(n,s)}$

$\Rightarrow$ g.c.d.(n, s) divides g.c.d.(n, r)

Conversely, Let g.c.d.(n, s) divide g.c.d(n, r)

Let d = g.c.d.(n, s), k = g.c.d.(n, r)

then $d \mid k$

Let $x \in < a^r >$ then $x = a^{rt}$

Now $k \mid r \Rightarrow r = ku$

and $d \mid k \Rightarrow k = dv$

and so $r = duv$

Since, d = g.c.d.(n, s), $\exists$ integers p and q

s.t., $d = np + sq$

and thus $r = (np + sq)uv$

Hence, $x = a^{rt} = a^{(np + sq)uvt}$

$= a^{npuvt}.a^{squvt} = a^{squvt}$ as $o(a) = n$.

$\in < a^s > = K$

and so $H \subseteq K$.

Finally, suppose now $H = K$

then $o(H) = o(K) \Rightarrow o(a^r) = o(a^s)$

i.e., $\frac{o(a)}{(o(a), r)} = \frac{o(a)}{(o(a), s)}$

i.e., g.c.d. (n, r) = g.c.d.(n, s)

Conversely, let g.c.d.(n, r) = g.c.d.(n, s)

then by first part $< a^r > \subseteq < a^s >$

and $< a^s > \subseteq < a^r >$

i.e., $H = K$.

Problem 36: *Let G be a group. Suppose $a, b \in G$, s.t.,*

(*i*) $ab = ba$

(*ii*) $(o(a), o(b)) = 1$.

Show that $o(ab) = o(a)o(b)$.

Solution: Let $o(a) = m$, $o(b) = n$

Then $(ab)^{mn} = a^{mn}b^{mn}$ as $ab = ba$

$= (a^m)^n (b^n)^m$

$= e$

Let $(ab)^r = e \Rightarrow a^r b^r = e$

$\Rightarrow a^r = b^{-r}$

$\Rightarrow (a^r)^n = (b^{-r})^n = (b^n)^{-r} = e$

$\Rightarrow o(a) \mid rn$

$$\Rightarrow m \mid rn$$
$$\Rightarrow m \mid r \quad \text{as } (m, n) = 1$$

Similarly, $n \mid r$

$$\Rightarrow \text{l.c.m. of } (m \ \& \ n) \mid r$$
$$\Rightarrow mn \mid r \Rightarrow mn \leq r$$

$\therefore \quad o(ab) = mn.$

Problem 37: *If a group has finite number of subgroups, then show that it is a finite group.*

Solution: Let G be a group which has n finite number of subgroups. Let $e \neq a \in G$. We show $o(a)$ = finite.

Since G has finite number of subgroups, $< a^i > = < a^j >$ for some integers i, j with $i \neq j$.

$$\Rightarrow a^i = (a^j)^r \Rightarrow a^{i-jr} = e$$
$$\Rightarrow i - jr = 0 \text{ or } o(a) = \text{finite}$$
$$\Rightarrow j \text{ divides } i \text{ or } o(a) = \text{finite}$$

If $o(a)$ is not finite, then j divides i and similarly we'll get that i divides j and so $i = j$, a contradiction.

Hence $o(a)$ = finite for all $a \in G$

Consider $< a >$. If $G = < a >$ then $o(G)$ = finite.

If $G \neq < a >$, let $H_1 = < a >$. Then $o(H_1)$ = finite.

Let $a_2 \in G$ s.t., $a_2 \notin H_1$. Let $H_2 = < a_2 >$.

Then $o(H_2)$ = finite.

If $G = H_1 \cup H_2$ then G is finite.

If $G \neq H_1 \cup H_2$ then $\exists\ a_3 \in G$, s.t., $a_3 \notin H_1 \cup H_2$.

Let $H_3 = < a_3 >$, then H_3 is finite. Suppose in this way, we get $H_1, H_2, ..., H_{n-1}$ to be finite number of subgroups of G.

If $G = H_1 \cup H_2 \cup ... \cup H_{n-1}$, then $\exists\ a_n \in G$, $a_n \notin H_i\ \forall i = 1, 2, ..., n - 1$. Thus $< a_n > \neq H_i\ \forall i = 1, 2, ..., n - 1$.

Then $H_n = < a_n >$ is finite.

Thus each subgroup of G is finite and hence G is finite.

Problem 38: *Show that the number of elements of prime order p in a finite group G is a multiple of p − 1.*

Solution: Let $x \in G$ s.t., $o(x) = p$. Let $H = < x >$. This gives $\varphi(p) = p - 1$ elements of order p, namely generators of H. If these are the only elements of order p, then we are done, otherwise $\exists\ y \in G$, $y \notin H$, $o(y) = p$. Let $K = < y >$.

Then $H \cap K = \{e\}$ as $o(H \cap K)$ divides $o(H)$ and $o(K) \Rightarrow o(H \cap K) = 1$ or p.

If $o(H \cap K) = p = o(H) = o(K)$ then $H \cap K = H = K \Rightarrow y \in H$, a contradiction.

So, $o(H \cap K) = 1 \Rightarrow H \cap K = \{e\}$. So, $K = < y >$ gives another $\varphi(p) = p - 1$ elements of order p not in H. In this way, since G is finite, we shall have multiple of $p - 1$ elements of order p.

It is easy to see that U_2 and U_4 are cyclic groups while U_8 is not cyclic (See Exercise 5). So, question arises for what n, U_2n is cyclic. Before, we answer it, we prove

Lemma: *If a is an odd integer, then for $k \geq 3$.*

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Proof: We prove the result by induction on k.
Let $k = 3$. Then $2^{k-2} = 2$.

So, $a^{2^{k-2}} = a^2 \equiv 1 \pmod 8$

Therefore, the result is true for $k = 3$
Assume that the result holds for $k = n > 3$.

Then $a^{2^{n-2}} \equiv 1 \pmod{2^n}$

$\Rightarrow a^{2^{n-2}} = 1 + b2^n$ for some integer b

$\Rightarrow a^{2^{n-1}} = 1 + (b2^n)^2 + 2(b2^n)$, on squaring
$= 1 + 2^{n+1}(b + b^2 2^{n-1})$
$\equiv 1 \pmod{2^{n+1}}$.

So, the assertion is true for $k = n + 1$
By induction, the result is true for all $k \geq 3$.

Theorem 34: *U_{2^n} is not cyclic for $n \geq 3$*

Proof: Let $a \in U_{2^n}$,. Then g.c.d. $(a, 2^n) = 1$.

So, a is an odd integer

Now $o(U_{2^n}) = \varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$

By above lemma $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for $n \geq 3$

$$\Rightarrow a^{\frac{\varphi(2^n)}{2}} \equiv 1 \pmod{2^n} \quad \text{for } n \geq 3$$

$$\Rightarrow o(a) \leq \frac{\varphi(2^n)}{2} < \varphi(2^n) \quad \text{for } n \geq 3$$

Therefore, there is no element in U_{2^n} whose order is $\varphi(2^n)$.

Hence, U_{2^n} is not cyclic for all $n \geq 3$.

Remark: If $a \in U_n$, then $a^{o(U_n)} = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$.
If $o(a) = \varphi(n)$, then a is called a primitive root of n.
In that case, U_n is cyclic.
So, U_n is cyclic if and only if n has a primitive root. By number theory, n has a primitive root if n is one of the following type:

$$n = 2,\ 4,\ p^r\ (p = \text{odd prime}),\ 2p^r (p = \text{odd prime})$$

Hence, U_n is cyclic, if n is of the above form.

In particular, U_p is cyclic for all prime p.

Also, U_{2p} is cyclic for all odd prime p.

Further, if U_n is cyclic, then the number of generators of U_n is $\varphi(\varphi(n))$. Equivalently, if n has a primitive root, then the number of primitive roots of n is $\varphi(\varphi(n))$.

Exercises

1. Show that a group having five or less elements is abelian.

2. For elements a, b, x in a group G. Show that

(i) $o(a) = o(a^{-1})$

(ii) $o(a) = o(x^{-1}ax)$.

(iii) $o(a^k) \leq o(a)$

(iv) $o(ab) = o(ba)$

(v) If $a \in G$ be the only element of order n then that $a \in Z(G)$, the centre of G.

3. If a finite group possesses an element of order 2, show that it possesses an odd number of such elements.

4. Let G be a finite group. Let $a \in G$ be such that $o(a) = o(G)$. Show that G is cyclic, generated by a. Hence show that a group of order n is cyclic iff it has an element of order n.

5. Show that every element in U_8 is its own inverse (so is of order 2) and hence U_8 is not cyclic.

6. Let G be a group and $a \in G$. Show that

$H = < a > = \{a^n \mid n \text{ an integer}\}$

is a subgroup of G and also if K is any subgroup of G s.t., $a \in K$, then $H \subseteq K$

7. let $a \in G$ be such that $o(a) = mn$, where m, n are coprime. Show that $a = bc$, where $o(a) = m$, $o(c) = n$. (See Problem 48 on page 146).

8. Show that a subgroup ($\neq \{e\}$) of an infinite cyclic group is infinite.

9. Show that elements of finite order in any abelian group form a subgroup.

10. Show that for $n > 2$, the order of U_n is even.

11. If G is a cyclic group of order p, a prime then show that any non identity element of G is of order p.

12. Let G be a cyclic group of order 6 generated by a. Let H, K be the subgroups generated by a^2, a^3 respectively. Prove that $o(H) = 3$, $o(K) = 2$, $G = HK$ and $H \cap K = \{e\}$.

13. Find order of each element in the group $G = \{\pm 1, \pm i\}$ under multiplication.

14. Find all the subgroups of the quaternion group G and show that $\exists$ no two non-trivial subgroups H, K of G s.t., $H \cap K$ is identity only.

15. Let $A(\mathbf{R})$ be the group of all permutations on $\mathbf{R}$, where $\mathbf{R}$ = set of reals. Let $f : \mathbf{R} \to \mathbf{R}$ s.t., $f(x) = -x$ and $g : \mathbf{R} \to \mathbf{R}$ s.t., $g(x) = 1 - x$. Show that f and g are both elements of order 2.

16. Show that $\mathbf{Q} - \{0\}$ under multiplication is not cyclic.

17. Show that a finite cyclic group with three or more elements has even number of generators.

18. If order of a group G is pq, where p, q are primes, then show that every proper subgroup of G is cyclic.

19. Show that S_3 is not cyclic, although all its subgroups (different from S_3) are cyclic. Same is true for U_8.

20. Let $H_n = < n >$ and $H_m = < m >$. Show that $H_n \cap H_m = < k >$ where k = l.c.m. (n, m)

21. Write down all the 12 subgroups of $\mathbf{Z}_{60}$. How many generators it has?

22. Let G be an abelian group and p be a prime. Let H be a subset of G where if $x \in H$ then $o(x) = p^r$ for some r. Show H is a subgroup of G.

A Quick Look at what's been done

- A **group** is defined to be a non-empty set together with a binary composition, satisfying the conditions of associativity and presence of identity and inverse elements. A group that also satisfies commutative property is called **abelian**.
- A non-empty subset of a group is called a **subgroup** if it forms a group under the same binary composition of the group.
- A non-empty subset H of a group G is a subgroup iff $ab^{-1} \in H$ for all $a, b \in H$.
- Product HK of subgroups is a subgroup iff $HK = KH$. If $o(G)$ (read order G) means the number of elements in G, then $o(HK) = o(H).o(K)/o(H \cap K)$; H, K being finite.
- **Lagrange's theorem states** that the order of a subgroup divides order of the group where the group is finite. *Converse may not hold.*
- If n is the least positive integer s.t., $a^n = e$, then n is called the **order of *a***. If no such n exists we say a has infinite order.
- A group G is called a **cyclic** group, if every element of G can be expressed as a power of an element of G and in that case that element is called a generator of G. An infinite cyclic group has two generators, whereas the number of generators of a group of order n is $\varphi(n)$,where φ is Euler's function.
- Order of a cyclic group is same as the order of its generator.
- Subgroup of a cyclic group is cyclic.
- Converse of Lagrange's theorem holds in cyclic groups.
- If G is a finite cyclic group of order n then number of distinct subgroups of G is the number of distinct divisors of n and there is a unique subgroup of G of any given order.
- A group of prime order has no non-trivial subgroups, whereas a group of composite order must have at least one.

3

Normal Subgroups, Homomorphisms, Permutation Groups

Introduction

We take up a very special class of subgroups called the normal subgroups here that lead us to another class of groups called factor or quotient groups. We later take up the notion of isomorphism (a *type* of equality) in algebraic systems. In the end, we discuss the permutation groups.

Definition: A subgroup H of a group G is called a *normal subgroup* of G if $Ha = aH$ for all $a \in G$.

A normal subgroup is also called *invariant* or *self conjugate* subgroup.

Clearly G and $\{e\}$ are normal subgroups of G and are referred to as the trivial normal subgroups. A group $G \neq \{e\}$ is called a **simple group** if the only normal subgroups of G are $\{e\}$ and G. Any group of prime order is simple. See theorem 25 on page 86. This group has no subgroups (let alone the normal ones) except $\{e\}$ and G.

It is easy to see that if H is a normal subgroup of G and K is a subgroup of G s.t., $H \subseteq K \subseteq G$ then H is normal in K. Again, if G is abelian, all its subgroups will be normal. We use the notation $H \trianglelefteq G$ to convey that H is normal in G.

Example 1: $H = \{1, -1\}$ is a normal subgroup of the Quaternion group G. Indeed $Ha = \{a, -a\} = aH$ for any $a \in G$.

The following two theorems give us equivalent conditions under which a subgroup of a group is normal. So one could also take any one of these as definition of a normal subgroup.

Theorem 1: *A subgroup H of a group G is normal in G iff $g^{-1}Hg = H$ for all $g \in G$.*

Proof : Let H be normal in G

then $Hg = gH$ for all $g \in G$

$\Rightarrow g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)H = H.$

Conversely, let $g^{-1}Hg = H$ for all $g \in G$

Then $g(g^{-1}Hg) = gH$

$\Rightarrow (gg^{-1})Hg = gH$

$\Rightarrow Hg = gH.$

Hence H is normal.

Theorem 2: *A subgroup H of a group G is normal in G iff $g^{-1}hg \in H$ for all $h \in H$, $g \in G$.*

Proof: Let H be normal in G, then

$$Ha = aH \quad \text{for all } a \in G$$

Let $h \in H$, $g \in G$ be any elements, then

$hg \in Hg = gH$

$\Rightarrow hg = gh_1$ for some $h_1 \in H$

$\Rightarrow g^{-1}hg = h_1 \in H$

which proves the result.

Conversely, let $a \in G$ be any element,

then $a^{-1}ha \in H$ for all $h \in H$

$\Rightarrow a(a^{-1}ha) \in aH$ for all $h \in H$

$\Rightarrow ha \in aH$ for all $h \in H$

$\Rightarrow Ha \subseteq aH$

Taking $b = a^{-1}$, we note, as $b \in G$

$b^{-1}\ hb \in H \qquad h \in H$

$\Rightarrow aha^{-1} \in H$ for all $h \in H$

$\Rightarrow (aha^{-1})a \in Ha$ for all $h \in H$

$\Rightarrow ah \in Ha$ for all $h \in H$

$\Rightarrow aH \subseteq Ha.$

Hence $Ha = aH$, showing H is normal.

Remark: Evidently, it makes no difference in the argument if the above condition is read as $ghg^{-1} \in H$ for all $h \in H$, $g \in G$.

The next theorem also gives us an equivalent condition for a subgroup to be normal, but the importance of this theorem is much more in as much as it helps us to form what would be known as Quotient groups. The very statement of the theorem suggests the presence of a binary composition. (We would also remind the reader here that we *did* talk about the product of two subsets of a group in a remark earlier).

Theorem 3: *A subgroup H of a group G is normal subgroup of G iff product of two right cosets of H in G is again a right coset of H in G.*

Proof: Let H be a normal subgroup of G.

Let Ha and Hb be any two right cosets of H in G.

then $$(Ha)(Hb) = H(aH)b$$
$$= H(Ha)b$$
$$= HHab$$
$$= Hab \qquad ab \in G$$

Conversely, we are given that product of any two right cosets of H in G is again a right coset.

To show H is normal, let $g \in G$ be any element.

Then Hg and Hg^{-1} are two right cosets of H in G. Thus $HgHg^{-1}$ is also a right coset of H in G.

We claim $HgHg^{-1} = He$

Now $egeg^{-1} \in HgHg^{-1}$

$\Rightarrow e \in HgHg^{-1}$

Also $e \in H$

thus H and $HgHg^{-1}$ are two right cosets having one element common. Recalling the properties of equivalence classes we know that two right cosets are either equal or have no element in common. Thus, (as e is common element)

$$H = HgHg^{-1}$$

Now $hgh_1g^{-1} \in HgHg^{-1}$ for all $h, h_1 \in H, g \in G$

$\Rightarrow hgh_1g^{-1} \in H$ for all $h, h_1 \in H, g \in G$

$\Rightarrow h^{-1}(hgh_1g^{-1}) \in h^{-1}H$

$\Rightarrow gh_1g^{-1} \in H$ for all $h_1 \in H, g \in G$

$\Rightarrow H$ is normal in G.

Hence the result.

Let H be a subgroup of a group G. Define

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

then as seen earlier (see exercises, page 77) $g^{-1}Hg$ forms a subgroup of G.

Again, if we define a mapping $f : H \to g^{-1}Hg$, by

$$f(h) = g^{-1}hg$$

then f will be a 1–1 onto mapping.

In case G is finite, this would mean that both H and $g^{-1}Hg$ (for any $g \in G$) will have same number of elements.

Using this result we have thus proved that *if H be a subgroup of a finite group G s.t., there is no other subgroup of G having the same number of elements as H has, then H is normal in G.* After all, H and $g^{-1}Hg$ (for any $g \in G$) have same number of elements would mean (by given condition) that they are equal and $H = g^{-1}Hg$ means H is normal.

Problem 1: *Prove that a non empty subset H of a group G is normal subgroup of G $\Leftrightarrow$ for all $x, y \in H$, $g \in G$, $(gx)(gy)^{-1} \in H$.*

Solution: Let H be normal subgroup of G.

Let $x, y \in H$, $g \in G$ be any elements,

then $(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \in H$

as $xy^{-1} \in H$, $g \in G$, H is normal in G.

Conversely, we show H is normal subgroup of G.

Let $x, y \in H$ be any elements,

then $xy^{-1} = exy^{-1}\ e = (ex)\ (ey)^{-1} \in H$ as $e \in G$

i.e., H is a subgroup of G.

Again, let $h \in H$, $g \in G$ be any elements

then as $(gh)(ge)^{-1} \in H$

we get $(gh)(eg^{-1}) \in H$

$\Rightarrow ghg^{-1} \in H$

$\Rightarrow H$ is normal.

Problem 2: Show that the normaliser $N(a)$ of a in a group G may not be a normal subgroup of G.

Solution: Let $G = S_3$ and $a = (23)$, then $N(a) = N((23)) = \{\sigma \in S_3 \mid \sigma(23) = (23)\sigma\} = \{I, (23)\}$

Since, $N(a)(12) = \{(12), (132)\}$

and $(12)N(a) = \{(12), (123)\}$

we find $N(a)(12) \neq (12)N(a)$ or that $N(a)$ is not normal.

Problem 3: *If N is a normal subgroup of order 2, of a group G then show that $N \subseteq Z(G)$, the centre of G.*

Solution: Let $N = \{a, e\}$.

Since $e \in Z(G)$ (centre being a subgroup contains e) all that we want to show is that $a \in Z(G)$

i.e., $ag = ga$ for all $g \in G$

or $g^{-1}ag = a$ for all $g \in G$

Let $g \in G$ be any element then as $a \in N$ and N is normal, $g^{-1}ag \in N = \{a, e\}$

$\Rightarrow g^{-1}ag = a$ or $g^{-1}ag = e$

Since $g^{-1}ag = e \Rightarrow ag = ge \Rightarrow ag = eg \Rightarrow a = e$, which is not true

we get $g^{-1}\ ag = a \ \Rightarrow a \in Z(G)$

or $N \subseteq Z(G)$.

Problem 4: *Show that a subgroup of index 2 in a group G is a normal subgroup of G.*

Solution: Let H be a subgroup of G, with index 2 then number of distinct right (left) cosets of H in G is 2 and also then G is union of these two right (left) cosets.

Let $g \in G$ be arbitrary.

Case *(i)*: $g \in H$, then $Hg = gH$ $(=H)$

Hence H is normal.

Case *(ii)*: $g \notin H$ then $gH \neq H$, $Hg \neq H$.

Thus Hg and $H = He$ are the two distinct right cosets of H in G and

$$G = Hg \cup H$$

Similarly, $$G = gH \cup H$$

$$\Rightarrow Hg \cup H = gH \cup H$$

$$\Rightarrow Hg = gH \quad (\text{as } Hg \cap H = gH \cap H = \varphi)$$

$$\Rightarrow H \text{ is normal in } G.$$

Remark: Converse is not true. Indeed $H = \{1, -1\}$ has index 4 in the Quaternion group and is normal.

Problem 5: *If H is a subgroup of a group G such that $(aH)(Hb)$ for any $a, b \in G$ is either a left or a right coset of H in G then H is normal.*

Solution: Let $a \in G$ be any element.

Now $$e = aeea^{-1} = (ae)(ea^{-1}) \in aHHa^{-1}.$$

Also $$e \in H = He = eH$$

Thus (aH) (Ha^{-1}) and H are two right(left) cosets of H in G and contain a common element e.

$$\Rightarrow aHHa^{-1} = H$$

$$\Rightarrow aHa^{-1} = H \Rightarrow H \text{ is normal.}$$

Problem 6: *Show by an example that we can find three groups $E \subseteq F \subseteq G$, where E is normal in F, F is normal in G but E is not normal in G.*

Solution: Let G be the group $\{\pm e, \pm a, \pm b, \pm c\}$

where $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $c = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

If $E = \{e, a\}$, $F = \{\pm e, \pm a\}$ then E is normal in F and F is normal in G as $i_F(E) = 2$ and $i_G(F) = 2$. But E is not normal in G as $cac^{-1} = -a \notin E$, where $c \in G$, $a \in E$.

See problem 63 on page 155 for another example.

Problem 7: *If a cyclic subgroup K of G is normal in G then every subgroup of K is normal in G.*

Solution: Suppose K is generated by a.

Let H be any subgroup of K. We show H is normal in G. Since H is a subgroup of a cyclic group, H will be cyclic.

Let a^m be generator of H.

Let $g \in G$ and $h \in H$ be any elements.

Then $h = (a^m)^n$ for some integer n

therefore, $g^{-1}hg = g^{-1}(a^m)^n g = g^{-1}(a^n)^m g = (g^{-1}a^n g)^m$.

As $K = \langle a \rangle$, $a^n \in K$ and as K is normal in G

we get $g^{-1}a^n g \in K = \langle a \rangle$.

Thus $g^{-1}a^n g = a^t$ for some t

$\therefore$ $g^{-1}hg = (a^t)^m = (a^m)^t \in H$

Hence H is normal in G.

Problem 8: *Show that the only abelian simple groups are groups of prime order.*

Solution: Let G be a group of prime order, then G is cyclic and therefore, abelian. Also then it contains no non-trivial subgroups. Hence it is simple.

Again, if G be abelian and simple, then each subgroup of G is normal (as G is abelian) it being simple, it contains no non-trivial normal subgroups. Hence G contains only trivial subgroups *i.e.*, G is finite of prime order. (See theorem 28 on page 87).

Problem 9: *If H and K are two normal subgroups of a group G s.t., $H \cap K = \{e\}$ then show that $hk = kh$ for all $h \in H$, $k \in K$.*

Solution: Let $h \in H$, $k \in K$ be any elements,

then $h \in H$, $k \in K \subseteq G$, H is normal in G

gives $k^{-1}hk \in H \Rightarrow k^{-1}hkh^{-1} \in H$

Again $h^{-1} \in H \subseteq G$, $k \in K$, K is normal in G

gives $(h^{-1})^{-1}\, kh^{-1} \in K \Rightarrow hkh^{-1} \in K \Rightarrow k^{-1}\, hkh^{-1} \in K$

i.e., $k^{-1}\, hkh^{-1} \in H \cap K = (e)$

$\Rightarrow k^{-1}\, hkh^{-1} = e$

$\Rightarrow hk = kh$.

Remark: If G is the Quaternion group then all its subgroups are normal (see exercise 5 on page 114).

If $H = \{\pm 1, \pm i\}$, $K = \{\pm 1, \pm j\}$

then $ij \neq ji$. Note here $H \cap K \neq \{e\}$.

Problem10: *If G is the union of proper normal subgroups s.t., any two of them have only e in common, then G is abelian.*

Solution: Let $G = H_1 \cup H_2 \cup \ldots\ldots \cup H_k$

Let $x, y \in G$ be any elements, then $x \in H_i$, $y \in H_j$ for some i, j.

Case *(i)*: If $i \neq j$ then $xy = yx$ using previous problem.

Case *(ii)*: $i = j$, then $x, y \in H_i$.

Now since H_i is a proper subgroup of G, $\exists$ some $g \in G$ s.t., $g \notin H_i$ (and $g \in H_t$ for some $t \neq i$)

Thus again by previous problem, g commutes with both x and y

i.e., $xg = gx$ and $yg = gy$.

Now $g \notin H_i \Rightarrow gx \notin H_i$

$\therefore gx$ also commutes with x, y and $xy \in H_i$

Also $(xy)g = g(xy)$

$$= (gx)y = y(gx)$$
$$= y(xg) = (yx)g$$
$$\Rightarrow \quad xy = yx \text{ (cancellation)}$$

Hence G is abelian.

Problem 11: *Show that a subgroup N of G is normal iff $xy \in N \Rightarrow yx \in N$.*

Solution: Let N be normal in G and let $xy \in N$.

Since $yx = y(xy)y^{-1}$

and $xy \in N$, $y \in G$, N is normal in G we find

$$y(xy)y^{-1} \in N \Rightarrow yx \in N.$$

Conversely, let $n \in N$, $g \in G$ be any elements

then $n \in N \Rightarrow (ng)\, g^{-1} \in N$

$\Rightarrow g^{-1}(ng) \in N$ (given condition)

$\Rightarrow N$ is normal in G.

Problem 12: *Show that a subgroup H of G is normal iff $Ha \neq Hb \Rightarrow aH \neq bH$.*

Solution: Let H be normal in G and suppose $Ha \neq Hb$

then $aH \neq bH$

as $Ha = aH$, $Hb = bH$ as H is normal in G.

Conversely, let $Ha \neq Hb \Rightarrow aH \neq bH$

then $aH = bH \Rightarrow Ha = Hb$

i.e., $a^{-1}b \in H \Rightarrow ab^{-1} \in H$

Let now $g \in G$, $h \in H$ be any elements, then

$$h^{-1} \in H \Rightarrow h^{-1}gg^{-1} \in H$$
$$\Rightarrow (h^{-1}g)\,(g^{-1}) \in H \Rightarrow (h^{-1}g)^{-1}\, g \in H$$
$$\Rightarrow g^{-1}hg \in H$$
$$\Rightarrow H \text{ is normal in } G.$$

Problem 13: *Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$ then show that N is a normal subgroup of G.*

Solution: We know that intersection of subgroups is a subgroup and also subsets of the type xHx^{-1} are subgroups.

Hence $\bigcap_{x \in G} xHx^{-1}$ is a subgroup of G.

Let $g \in G$ be any element, then

$$gNg^{-1} = g(\cap xHx^{-1})g^{-1} = \cap\, (gxHx^{-1}g^{-1}) = \cap\, (yHy^{-1}) = N$$

showing thereby that N is normal.

We have used above the result $g(H \cap K) = gH \cap gK$ for subgroups H, K and $g \in G$. It is true as

$x \in g(H \cap K) \Rightarrow x = ga,\ a \in H \cap K$

$a \in H \Rightarrow ga \in gH \Rightarrow x \in gH \Rightarrow x \in gH \cap gK$

$a \in K \Rightarrow ga \in gK \Rightarrow x \in gK$

Also $y \in gH \cap gK \Rightarrow y \in gH,\ y \in gK$

$\Rightarrow y = gh,\ y = gk, \quad h \in H,\ k \in K$

$\Rightarrow gh = gk$

$\Rightarrow h = k \ \Rightarrow h, k \in H \cap K$

$\therefore\ y = gh \in g\ (H \cap K)$ proving the result.

Problem 14: *Let H be a subset of a group G. Let $N(H) = \{x \in G \mid Hx = xH\}$ be the normalizer of H in G.*

We have already shown that $N(H)$ is a subgroup of G. Show

(*i*) *If H is a subgroup of G then $N(H)$ is the largest subgroup of G in which H is normal.*

(*ii*) *If H is a subgroup of G then H is normal in G iff $N(H) = G$.*

(*iii*) *Show by an example, the converse of* (*ii*) *fails if H is only a subset of G.*

(*iv*) *If H is a subgroup of G and K is a subgroup of $N(H)$ then H is normal subgroup of HK.*

Solution: (*i*) We show H is normal in $N(H)$.

Since $Hh = hH$ for all $h \in H$, we find

$h \in N(H)$ for all $h \in H$.

Thus $H \leq N(H)$.

Again by definition of $N(H)$, $Hx = xH$ for all $x \in N(H)$

$\Rightarrow$ H is normal in $N(H)$.

To show that $N(H)$ is the largest subgroup of G in which H is normal, suppose K is any subgroup of G such that H is normal in K.

then $k^{-1} Hk = H$ for all $k \in K$

$\Rightarrow Hk = kH$ for all $k \in K$

$\Rightarrow k \in N(H)$ for all $k \in K$

$\Rightarrow K \subseteq N(H)$.

(*ii*) Let H be a normal subgroup of G

then $N(H) \subseteq G$ (by definition)

Let $x \in G$ be any element,

then $xH = Hx$ as H normal in G.

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

Hence $G = N(H)$.

Conversely, let $G = N(H)$, H is a subgroup of G (given)

Let $h \in H$, $g \in G$ be any elements

Then $g \in N(H)$ as $N(H) = G$

$\Rightarrow gH = Hg$

$\Rightarrow H$ is normal in G.

(*iii*) Consider $G = < a > = \{e, a, a^2, a^3\}$
then G being cyclic is abelian group.
Take $H = \{a\}$
then H is a subset and not a subgroup of G ($e \notin H$)
Also $N(H) = G$ as G is abelian.

(*iv*) Let K be a subgroup of $N(H)$
then $k \in K \Rightarrow k \in N(H) \Rightarrow Hk = kH$

i.e., $Hk = kH$ for all $k \in K$

$\Rightarrow HK = KH$

$\Rightarrow HK$ is subgroup of $N(H)$

Note, $h \in H \Rightarrow Hh = hH$ $(=H)$

$\Rightarrow H \subseteq N(H)$ Also $K \subseteq N(H)$

Again $H \subseteq HK \subseteq N(H)$

Hence H is a subgroup of HK
$\Rightarrow$ H is normal subgroup of HK
$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$.

Problem 15: *Let H be normal in G such that o(H) and* $\frac{o(G)}{o(H)}$ *are co-prime. Show that H is unique subgroup of G of given order.*

Solution: Let $o(H) = m$, $\frac{o(G)}{o(H)} = n$. Suppose K is a subgroup of G of order m.

Then $o(HK) = \frac{m \cdot m}{d}$, where $d = o(H \cap K)$

Since H is normal, $HK \leq G$

Thus $o(HK) \mid o(G)$

$$\Rightarrow \quad m \cdot \frac{m}{d} \mid m \cdot n \;\Rightarrow\; \frac{m}{d} \mid n$$

$$\Rightarrow \quad d\frac{m}{d} \mid dn \Rightarrow m \mid dn$$

$\Rightarrow$ $m \mid d$ as $(m, n) = 1$

But $d \mid m$ as $H \cap K \leq H$

Thus $d = m$ and hence

$o(H \cap K) = o(H) = o(K)$

$\Rightarrow$ $H = K$.

Quotient Groups

Let G be a group and N a normal subgroup of G. Let us collect all the right cosets of N in G and form a set to be denoted by $\frac{G}{N}$ or G/N. Since N is normal in G, product of any two right

cosets of N will again be a right coset of N in G, *i.e.*, we have a well defined binary composition on $\frac{G}{N}$ (Prove it). We now show formally that this set $\frac{G}{N}$ forms a group under this product as its binary composition.

For $Na, Nb \in \frac{G}{N}$, $NaNb = Nab \in \frac{G}{N}$

If $Na, Nb, Nc \in \frac{G}{N}$ be any members, then

$Na(NbNc) = Na(Nbc) = Na(bc) = N(ab)c = NabNc = (NaNb)\ Nc.$

Again $Ne \in \frac{G}{N}$ will act as identity of $\frac{G}{N}$ and for any $Na \in \frac{G}{N}$, Na^{-1} will be the inverse of Na. Thus $\frac{G}{N}$ forms a group, called the *Quotient group* or the *factor group* of G by N.

It is easy to see that if G is abelian then so would be any of its quotient groups as

$$NaNb = Nab = Nba = NbNa.$$

Converse of this result may not hold. See example later.

Remarks: (*i*) In $\frac{G}{N}$, as N is normal, it is immaterial whether we use the word right cosets or left cosets, as $Na = aN$ for all a.

(*ii*) It would indeeed be interesting to see what $\frac{G}{\{e\}}$ and $\frac{G}{G}$ are equal to.

Are these G and $\{e\}$ respectively ? Well not really but 'almost' so. We will take it up when we come to isomorphisms.

Theorem 4: *If G is a finite group and N is a normal subgroup of G then*

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}.$$

Proof: Since G is finite, using Lagrange's theorem

$$\frac{o(G)}{o(N)} = \text{number of distinct right cosets of } N \text{ in } G$$

$$= o\left(\frac{G}{N}\right).$$

Theorem 5: *Every quotient group of a cyclic group is cyclic.*

Proof: Let $G = < a >$ be a cyclic group.

Then G is abelian, so every subgroup of G is normal. Let H be any subgroup of G. We show $\frac{G}{H}$ is cyclic. In fact we claim $\frac{G}{H}$ is generated by Ha.

Let $Hx \in \dfrac{G}{H}$ be any element.

Then $x \in G = < a >$, *i.e.*, x will be some power of a

Let $x = a^m$

Then
$$Hx = Ha^m = Ha\ a\ \ldots\ldots\ a \quad (m \text{ times})$$
$$= Ha\ Ha\ \ldots\ldots\ Ha \quad (m \text{ times})$$
$$= (Ha)^m$$

i.e., any element Hx of $\dfrac{G}{H}$ is a power of $Ha \Rightarrow Ha$ generates $\dfrac{G}{H}$

or that $\dfrac{G}{H}$ is cyclic.

Remarks:(*i*) The above result is proved for $m > 0$. In case $m \leq 0$, the proof follows similarly. Notice $a^m = a^{-n} = (a^{-1})^n$ where $n > 0$ and remembering that $Ha^{-1} = (Ha)^{-1}$ and so $(Ha^{-1})^n = (Ha)^{-n} = (Ha)^m$.

(*ii*) If $G = < a >$ is cyclic and $H \leq G$, then $o(G/H)$ is the least +ve integer m, s.t., $a^m \in H$.

We know if $H \leq G$, then $H = <a^m>$ where m is the least +ve integer s.t., $a^m \in H$ (see page 81).

Also, $G/H = < Ha >$. So $o(G/H) = o(Ha) = m$

as $(Ha)^m = Ha^m = H$ as $a^m \in H$ and if $(Ha)^r = H$, then $Ha^r = H \Rightarrow a^r \in H \Rightarrow m \leq r$ as m is such least.

Hence, $o(Ha) = m$ and so $o(G/H) = m$.

(*iii*) Converse of this result is not true. See under permutation groups, page 149.

Example 2: Let G be the set of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Then it is easy to see that G will form a group under matrix multiplication. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity, $\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$ will be inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Also G is not abelian.

Let N be the subset containing members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a subgroup of G. (Prove!) Also it is normal as the product of the type

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - \frac{b}{d} \\ 0 & 1 \end{bmatrix} \in N$$

So we get the quotient group $\frac{G}{N}$. We show $\frac{G}{N}$ in abelian.

Let $Nx, Ny \in \frac{G}{N}$ be any elements, then $x, y \in G$.

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian iff $NxNy = NyNx$

$$\Leftrightarrow Nxy = Nyx$$
$$\Leftrightarrow xy\,(yx)^{-1} \in N$$
$$\Leftrightarrow xyx^{-1}y^{-1} \in N$$

All we need check now is that the product

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}\begin{bmatrix} \frac{1}{c} & -\frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix}$$ is a matrix of the type $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$.

Thus we can have an abelian quotient group, without the 'parent' group being abelian.

Example 3: Let $< \mathbf{Z}, + >$ be the group of integers and let $N = \{3n \mid n \in \mathbf{Z}\}$ then N is a normal subgroup of $\mathbf{Z}$.

$\frac{\mathbf{Z}}{N}$ will consist of members of the type $N + a$, $a \in \mathbf{Z}$

We show $\frac{\mathbf{Z}}{N}$ contains only three elements. Let $a \in \mathbf{Z}$ be any element, where $a \neq 0, 1, 2$ then we can write, by division algorithm,

$$a = 3q + r \quad \text{where } 0 \leq r \leq 2$$
$$\Rightarrow N + a = N + (3q + r) = (N + 3q) + r = N + r \quad \text{as } 3q \in N.$$

but r can take values 0, 1, 2.

Hence $N + a$ will be one of

$$N,\ N + 1,\ N + 2$$

or that $\frac{\mathbf{Z}}{N}$ contains only these three members.

Remarks: (*i*) This example also tells us that in case of cosets, $Ha = Hb$ may not necessarily mean $a = b$. For instance, $N + 4 = N + 1$, but $4 \neq 1$ in above example.

$$[N + 4 = (N + 3) + 1 = N + 1].$$

(*ii*) This serves as an example of an infinite group which has a subgroup N having finite index in G.

(*iii*) This is also an example of a finite quotient group G/H, where the 'parent' group G is not finite. It is, however, easy to see that quotient group of a finite group is finite.

(*iv*) If $\frac{G_1}{N} = \frac{G_2}{N}$ then $G_1 = G_2$

Let $g_1 \in G_1$ be any element, then $Ng_1 \in \frac{G_1}{N} = \frac{G_2}{N}$

$\Rightarrow Ng_1 = Ng_2$ for some $g_2 \in G_2$

$\Rightarrow g_1 g_2^{-1} \in N \subseteq G_2 \Rightarrow g_1 g_2^{-1} = g$ for some $g \in G_2$

$\Rightarrow g_1 = gg_2^{-1} \in G_2 \Rightarrow G_1 \subseteq G_2$. Similarly $G_2 \subseteq G_1$. Hence $G_1 = G_2$.

Problem 16: *Find the order of the element* $< 6 > + 5$ *in the group* $\frac{\mathbf{Z}_8}{< 6 >}$.

Soluton: We have $\mathbf{Z}_8 = \{0, 1, 2, ..., 7\}$ mod 8

and $< 6 > = \{0, 6, 12\} = H$ (say)

Then, $$\frac{\mathbf{Z}_8}{< 6 >} = \frac{\mathbf{Z}_8}{H} = \{H, H+1, H+2, H+3, H+4, H+5\}$$

$$= \{< 6 >, < 6 >+1, < 6 >+2, < 6 >+3, < 6 >+4, < 6 >+5\}$$

Now, $< 6 > + 5 \neq < 6 >$, the identity

Again $2(< 6 > + 5) = < 6 > +10 = < 6 > + 4 \neq < 6 >$

Similarly, $3(< 6 >+5)$, $4(< 6 >+5)$, $5(< 6 >+5)$ are not $< 6 >$

whereas $6(< 6 >+5) = < 6 >+30 =< 6 >$ = identity and hence order of $< 6 >+5$ will be 6.

Problem 17: *Let N be a normal subgroup of a group G. Show that* $o(Na) | o(a)$ *for any* $a \in G$.

Soluton: Let $o(a) = n$

then n is the least +ve integer s.t., $a^n = e$.

This gives $Na^n = Ne$

$$\Rightarrow \underset{(n \text{ times})}{Na \,.\, a.....a} = N$$

$$\Rightarrow \underset{(n \text{ times})}{Na \,.\, Na.....Na} = N$$

$\Rightarrow (Na)^n = N$, $Na \in \frac{G}{N}$ and N is identity of $\frac{G}{N}$

$\Rightarrow o(Na) \mid n$ or $o(Na) \mid o(a)$.

Problem 18: *If G is a group such that* $\frac{G}{Z(G)}$ *is cyclic, where* $Z(G)$ *is centre of G then show that G is abelian.*

Solution: Let us write $Z(G) = N$. Then $\frac{G}{N}$ is cyclic. Suppose it is generated by Ng.

Let $a, b \in G$ be any two elements,

then $Na, Nb \in \dfrac{G}{N}$

$\Rightarrow$ $Na = (Ng)^n$, $Nb = (Ng)^m$ for some n, m

$\Rightarrow$ $Na = Ng \,.\, Ng \,\ldots\ldots\, Ng = Ng^n$

$Nb = Ng^m$

$\Rightarrow$ $ag^{-n} \in N, bg^{-m} \in N$

$\Rightarrow$ $ag^{-n} = x, bg^{-m} = y$ for some $x, y \in N$

$\Rightarrow$ $a = xg^n, b = yg^m$

$\Rightarrow$ $ab = (xg^n)(yg^m) = x(g^n y)\, g^m$

$= x(yg^n)\, g^m$ as $y \in N = Z(G)$

$= xyg^n\, g^m$

$= xyg^{n+m}$

Similarly, $ba = (yg^m)(xg^n) = y(g^m x)\, g^n = y(xg^m)\, g^n$

$= (yx)g^{m+n}$

$\Rightarrow$ $ab = ba$ as $xy = yx$ as $x, y \in Z(G)$

Showing that G is abelian.

Remarks: (*i*) We are talking about $\dfrac{G}{Z(G)}$ assuming, therefore, that $Z(G)$ is a normal subgroup of G, a result which is easily seen to be true. See exercises.

(*ii*) One can, moving on same lines as in the above solution prove that if G/H is cyclic, where H is a subgroup of $Z(G)$ then G is abelian.

(*iii*) If G is a non abelian group then $G/Z(G)$ is not cyclic.

(*iv*) If $\dfrac{G}{H}$ is cyclic for some normal subgroup H of G then G may not be abelian. Take G = Quaternion group and $H = \{\pm 1, \pm i\}$ then $o(G/H) = \dfrac{8}{4} = 2$ a prime. So G/H is cyclic, but G is not abelian.

Problem 19: *Let G be a non-abelian group of order pq where p, q are primes then o(Z(G))* = 1.

Solution: Since G is non-abelian, by Problem 18, $\dfrac{G}{Z(G)}$ is not cyclic.

Now, $o(Z(G)) \mid o(G) = pq$

$\Rightarrow o(Z(G)) = 1, p, q$ or pq

$o(Z(G)) = pq \Rightarrow Z(G) = G$

$\Rightarrow G$ is abelian which is not so.

$o(Z(G)) = p \Rightarrow o(G/Z(G)) = \dfrac{pq}{p} = q$. a prime, meaning $G(Z(G))$ is cyclic which is also not true.

Similarly, $o(Z(G)) = q$ cannot hold and we are left with the only possibility that $o(Z(G)) = 1$.

Problem 20: *Give an example of an infinite group in which every element is of finite order.*

Solution: (*a*) Let $< \mathbf{Q}, + >$ and $< \mathbf{Z}, + >$ be the groups of rationals and integers under addition. Then the quotient group

$$\frac{\mathbf{Q}}{\mathbf{Z}} = \left\{ \mathbf{Z} + \frac{m}{n} \,\middle|\, \frac{m}{n} \in \mathbf{Q} \right\}$$

is an infinite group. See exercises. Consider any member $\mathbf{Z} + \dfrac{m}{n}$ of $\dfrac{\mathbf{Q}}{\mathbf{Z}}$.

Since $$n\left(\mathbf{Z} + \frac{m}{n}\right) = \mathbf{Z} + n\frac{m}{n} = \mathbf{Z} + m = \mathbf{Z} = \text{Zero of } \frac{\mathbf{Q}}{\mathbf{Z}}$$

we find $\mathbf{Z} + \dfrac{m}{n}$ has finite order $\leq n$. Hence we have our example.

(*b*) Consider again

$$G = \left\{ \mathbf{Z} + \frac{m}{p^n} \,\middle|\, m, n \geq 0,\ n \text{ are integers, } p = \text{fixed prime} \right\}$$

Then G is a subgroup of $\dfrac{\mathbf{Q}}{\mathbf{Z}}$.

Now $$p^n\left(\mathbf{Z} + \frac{m}{p^n}\right) = \mathbf{Z} + \frac{m}{p^n}p^n = \mathbf{Z} + m = \mathbf{Z} = \text{zero of } G$$

$$\Rightarrow \text{ order of } \mathbf{Z} + \frac{m}{p^n} \text{ divides } p^n$$

$$\Rightarrow \text{ order of } \mathbf{Z} + \frac{m}{p^n} \text{ is } p^r,\ r \leq n$$

$\Rightarrow$ order of every element in G is finite and is of the form p^r.

Since G is inifinite, we find this would serve as an example of an infinite p-group. (See chapter 5 ahead).

Again, we can show that every subgroup $H(\neq G)$ of G is of finite order. Hence this is also an example of an infinite group in which every proper subgroup is of finite order.

Problem 21: Show that $<\mathbf{Q}, +>$ has no proper subgroup of finite index.

Solution: Suppose H is any proper subgroup of $<\mathbf{Q}, +>$ having finite index n.

Then, $o(\mathbf{Q}/H) = n$.

Since H is proper subgroup of $\mathbf{Q}$, $\exists\ \frac{a}{b} \in \mathbf{Q}$ s.t., $\frac{a}{b} \notin H$

Now, if $x + H \in \frac{\mathbf{Q}}{H}$ be *any* element

then $$n(x + H) = H \Rightarrow nx + H = H$$

$$\Rightarrow nx \in H \quad \forall\ x \in \mathbf{Q}$$

Take $x = \frac{a}{nb}$, then $n\frac{a}{nb} \in H$ i.e., $\frac{a}{b} \in H$ which is not true.

Hence, such a subgroup does not exist. (See exercise 20 on Page 115 also.)

Exercises

1. Show that every subgroup of a cyclic group is normal.
2. Show that intersection of two normal subgroups is a normal subgroup.
3. If H, K are two subgroups of G such that one of them is normal then prove that HK is a subgroup of G. Show further that if both H and K are normal then so is HK.
4. If H and N are two subgroups of G such that N is normal in G then show that $H \cap N$ is a normal subgroup of H. Show by an example that $H \cap N$ may not be normal in G.
5. Every subgroup of an abelian group is normal. Prove that converse is not true. (Consider Quaternion group).
6. Prove that centre of a group is a normal subgroup.
7. Show that $C(H)$ is a normal subgroup of $N(H)$, where $H \leq G$.
8. If A, B, C are normal subgroup of a group G where $B \subseteq A$ then show that
$$A \cap BC = B(A \cap C).$$
9. If H be a normal subgroup of G and $i_G(H) = m$ then show that for any $x \in G$, $x^m \in H$.
10. Show that if every cyclic subgroup of G is normal then every subgroup of G is normal.
11. Prove that if p is a prime number, then any group G of order $2p$ has a normal subgroup of order p.
12. Let N be a normal subgroup of G then show that $\frac{G}{N}$ is abelian iff $xyx^{-1}y^{-1} \in N$, for all $x, y \in G$.
13. Let N be a normal subgroup of a finite group G such that $o(N)$ and $o\left(\frac{G}{N}\right)$ are co-prime. Show that N is unique subgroup of G of order $o(N)$ and that if $x \in G$ be an element such that $x^{o(N)} = e$ then $x \in N$.

14. Give example of a group in which there exist elements a, b such that $o(a)$, $o(b)$ are finite but $o(ab)$ is not finite.

15. Let H and K be two normal subgroups of a group G such that $o(H)$ and $o(K)$ are relatively prime. Prove that $hk = kh$ for all $h \in H$, $k \in K$.

16. Show that a subgroup H of a group G is normal in G iff the set $\frac{G}{H}$ of all its right cosets is closed under multiplication.

17. Let N be a normal subgroup of G such that $o(G/N) = m$ and H is a subgroup of G s.t., $o(H) = n$ and $(m, n) = 1$ then show that $H \subseteq N$.

18. If H and K are two normal subgroups of G such that (G/H) and (G/K) are abelian then show that $\frac{G}{H \cap K}$ is abelian.

19. Show that $o\left(\mathbf{Z} + \frac{5}{4}\right)$ in $\frac{\mathbf{Q}}{\mathbf{Z}}$ is 4.

20. Show that $\frac{\mathbf{Q}}{\mathbf{Z}}$ is an infinite group and is not cyclic. (See Problem 21)

Homomorphisms-Isomorphisms

In this section we introduce the reader to the idea of an isomorphism which could also be termed as an 'indirect' equality in algebraic systems. Indeed, if two systems have the same number of elements and *behave* exactly in the same manner, nothing much is lost in calling them equal, although at times the idea of equality may look little uncomfortable, especially in case of infinite sets.

Definition: Let $< G, * >$ and $< G', o >$ be two groups.

A mapping $f : G \to G'$ is called a homomorphism if

$$f(a * b) = f(a)\ o\ f(b) \quad a, b \in G$$

As *agreed* earlier, and when there is no scope of confusion, we shall use the same symbol '.' for both binary compositions.

With that as notation we find a map

$f : G \to G'$ is a homomorphism if

$$f(ab) = f(a)f(b)$$

If, in addition, f happens to be one-one, onto, we say f is an *isomorphism* and in that case write $G \cong G'$.

Also clearly then

$$f(a_1a_2 \ldots\ldots a_n) = f(a_1)f(a_2) \ldots\ldots f(a_n)$$

holds under an isomorphism (homomorphism)

An onto homomorphism is called *epimorphism.*

A one-one homomorphism is called *monomorphism.*

A homomorphism from a group G to itself is called an *endomorphism* of G.

An isomorphism from a group G to itself is called *automorphism* of G.

If $f : G \to G'$ is onto homomorphism, then G' is called *homomorphic image* of G.

Example 4: Let $< \mathbf{Z}, + >$ and $< \mathbf{E}, + >$ be the groups of integers and even integers.

Define a map $f : \mathbf{Z} \to \mathbf{E}$, s.t.,

$$f(x) = 2x \quad \text{for all } x \in \mathbf{Z}$$

then f is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

that f is 1–1 is clear by taking the steps backwards.

f is a homomorphism as

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

Also f is onto as any even integer $2x$ would have x as its pre-image.

Hence f is an isomorphism.

In fact this example shows that a subset can be isomorphic to its superset.

See Cor. on page 131 also.

Example 5: Let f be a mapping from $< \mathbf{Z}, + >$ the group of integers to the group $G = \{1, -1\}$ under multiplication defined as

$$f : \mathbf{Z} \to G, \text{ s.t.,}$$
$$f(x) = 1 \quad \text{if } x \text{ is even}$$
$$= -1 \quad \text{if } x \text{ is odd}$$

then f is clearly well defined. We check, if it is a homomorphism.

Let $x, y \in \mathbf{Z}$ be any elements.

Case (*i*): x, y are both even, then $x + y$ is even and as

$$f(x + y) = 1, f(x) = 1, f(y) = 1$$

we notice $\quad f(x + y) = 1 = 1.1 = f(x) \,.\, f(y)$

Case (*ii*): x, y are both odd, then $x + y$ is even and

$$f(x + y) = +1 = (-1)(-1) = f(x)\, f(y)$$

Case (*iii*): x is odd, y is even, then $x + y$ is odd and

$$f(x + y) = -1 = (-1)\ (1) = f(x)\, f(y)$$

thus in all cases $f(x + y) = f(x)\, f(y)$

Showing thereby that f is a homomorphism. Is it an isomorphism?

Ontoness is obvious, but f is not 1–1 as $f(x) = f(y)$ does not necessarily mean $x = y$. Indeed $f(2) = f(4)$ but $2 \neq 4$.

Example 6: *Let* $\mathbf{R}^+$ *be the group of positive real numbers under multiplication and* $\mathbf{R}$ *the group of all real numbers under addition. Then the map*

$$\theta : \mathbf{R}^+ \to \mathbf{R} \text{ s.t.,}$$
$$\theta(x) = \log x$$

is an isomorphism.

θ is clearly well defined.

$$\begin{aligned} & \theta(x) = \theta(y) \\ \Rightarrow \quad & \log x = \log y \\ \Rightarrow \quad & e^{\log x} = e^{\log y} \\ \Rightarrow \quad & x = y \end{aligned}$$

shows that θ is one-one.

Since $\theta(xy) = \log xy = \log x + \log y = \theta(x) + \theta(y)$

we find θ is a homomorphism.

Finally, if $y \in \mathbf{R}$ be any member, then

Since $e^y \in \mathbf{R}^+$ and $\theta(e^y) = y$, we gather that θ is onto and hence on isomorphism. (The map $f : \mathbf{R} \to \mathbf{R}^+$, s.t., $f(a) = e^a$ can also be considered.)

Example 7: *Let G be a group and N, a normal subgroup of G. Define a map*

$$f : G \to \frac{G}{N} \text{ s.t.,}$$

$$f(x) = Nx, \quad x \in G$$

then f is clearly well defined. Again

$$f(xy) = Nxy = NxNy = f(x)\, f(y)$$

shows f is a homomorphism.

It is sometimes called the *natural* (or *canonical*) *homomorphism*. That f is onto, hardly needs any comment.

The relation of isomorphism in groups is an equivalence relation (See exercises). Thus whenever a group G is isomorphic to another group G', G' will be isomorphic to G. So we shall simply say that G and G' are isomorphic and denote it by $G \cong G'$.

In most of the theorems and definitions that follow we shall be using G, G' etc., for groups.

Theorem 6: *If $f : G \to G'$ is a homomorphism then*

(*i*) $f(e) = e'$

(*ii*) $f(x^{-1}) = (f(x))^{-1}$

(*iii*) $f(x^n) = [f(x)]^n$, *n an integer.*

where e, e' are identity elements of G and G' respectively.

Proof: (*i*) We have

$$\begin{aligned} & e \,.\, e = e \\ \Rightarrow\ & f(e \,.\, e) = f(e) \\ \Rightarrow\ & f(e) \,.\, f(e) = f(e) \\ \Rightarrow\ & f(e) \,.\, f(e) = f(e) \,.\, e' \\ \Rightarrow\ & f(e) = e' \quad \text{(cancellation)} \end{aligned}$$

(*ii*) Again $xx^{-1} = e = x^{-1}x$

$$\Rightarrow f(xx^{-1}) = f(e) = f(x^{-1}x)$$
$$\Rightarrow f(x)\, f(x^{-1}) = e' = f(x^{-1})\, f(x)$$
$$\Rightarrow (f(x))^{-1} = f(x^{-1}).$$

(*iii*) Let n be a +ve integer.

$$f(x^n) = \underset{(n \text{ times})}{f(x\,.\,x\,.....x)}$$
$$= f(x)\,.f(x)\,.....\,f(x) \quad (n \text{ times})$$
$$= (f(x))^n.$$

If $n = 0$, we have the result by (*i*). In case n is –ve integer, result follows by using (*ii*).

Problem 22: *Show that* $< \mathbf{Q}, + >$ *cannot be isomorphic to* $< \mathbf{Q}^*, \cdot >$, *where* $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ *and* $\mathbf{Q}$ = *rationals.*

Solution: Suppose f is an isomorphism from $\mathbf{Q}$ to $\mathbf{Q}^*$. Then as $2 \in \mathbf{Q}^*$, f is onto, $\exists\ \alpha \in < \mathbf{Q}, + >$, s.t., $f(\alpha) = 2$.

$$\Rightarrow \quad f\left(\frac{\alpha}{2} + \frac{\alpha}{2}\right) = 2$$

$$\text{or} \quad f\left(\frac{\alpha}{2}\right) f\left(\frac{\alpha}{2}\right) = 2$$

$$\Rightarrow \quad x^2 = 2 \quad \text{where } x = f\left(\frac{\alpha}{2}\right) \in \mathbf{Q}^*$$

But that is a contradiction as there is no rational no. x s.t., $x^2 = 2$. Hence the result follows.

Problem 23: *Find all the homomorphisms from* $\dfrac{\mathbf{Z}}{4\mathbf{Z}}$ *to* $\dfrac{\mathbf{Z}}{6\mathbf{Z}}$.

Solution: Let $f : \dfrac{\mathbf{Z}}{4\mathbf{Z}} \to \dfrac{\mathbf{Z}}{6\mathbf{Z}}$ be a homomorphism.

Then $f(4\mathbf{Z} + n) = n\, f(4\mathbf{Z} + 1)$

So, f is completely known if $f(4\mathbf{Z} + 1)$ is known.

Now order of $(4\mathbf{Z} + 1)$ is 4 and so $o(f(4\mathbf{Z} + 1))$ divides 4 (See problem 24 ahead).

Also $o(f(4\mathbf{Z} + 1))$ divides 6 and thus $o(f(4\mathbf{Z} + 1)) = 1$ or 2

If $o(f(4\mathbf{Z} + 1)) = 1$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z}$ = zero of $\dfrac{\mathbf{Z}}{6\mathbf{Z}}$

Hence $f(4\mathbf{Z} + n)$ = zero

If $o(f(4\mathbf{Z} + 1)) = 2$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z} + 3$

$\Rightarrow f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$

Also $f(4\mathbf{Z} + n + 4\mathbf{Z} + m) = f(4\mathbf{Z} + n + m)$

$= 6\mathbf{Z} + 3(n + m)$

$$= (6\mathbf{Z} + 3n) + (6\mathbf{Z} + 3m)$$
$$= f(4\mathbf{Z} + n) + f(4\mathbf{Z} + m)$$

Thus there are two choices for f and it can be defined as

$$f : \frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}} \text{ s.t.,}$$
$$f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$$

Notice $4\mathbf{Z} + n = 4\mathbf{Z} + m$

$$\Rightarrow n - m \in 4\mathbf{Z}$$
$$\Rightarrow 3(n - m) \in 12\mathbf{Z} \subseteq 6\mathbf{Z}$$
$$\Rightarrow 3(n - m) \in 6\mathbf{Z}$$
$$\Rightarrow 6\mathbf{Z} + 3n \in 6\mathbf{Z} + 3m$$

i.e., f is well defined.

So there are two homomorphisms from $\frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}}$. In fact, in general, there are d homomorphisms from $\frac{\mathbf{Z}}{m\mathbf{Z}} \to \frac{\mathbf{Z}}{n\mathbf{Z}}$ where d = g.c.d.(m, n)

Definition: Let $f : G \to G'$ be a homomorphism. The **Kernel** of f, (denoted by Ker f) is defined by

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

where e' is identity of G'.

Theorem 7: *If $f : G \to G'$ be a homomorphism, then Ker f is a normal subgroup of G.*

Proof: Since $f(e) = e'$, $e \in$ Ker f, thus Ker $f \neq \varphi$. Again,

$$x, y \in \text{Ker } f \Rightarrow f(x) = e'$$
$$f(y) = e'$$

Now $f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)(f(y))^{-1} = e' \cdot e'^{-1} = e'$

$$\Rightarrow xy^{-1} \text{ Ker } f$$

Hence it is a subgroup of G.

Again, for any $g \in G$, $x \in$ Ker f

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g)$$
$$= (f(g))^{-1}f(x)\, f(g) = (f(g))^{-1}\, e'\, f(g)$$
$$= (f(g))^{-1}f(g) = e'$$
$$\Rightarrow g^{-1}xg \in \text{Ker } f$$

or that it is a normal subgroup of G.

Theorem 8: *A homomorphism $f : G \to G'$ is one-one iff Ker $f = \{e\}$.*

Proof: Let $f : G \to G'$ be one-one.

Let $x \in$ Ker f be any element

then $f(x) = e'$ and as $f(e) = e'$

$f(x) = f(e) \Rightarrow x = e$ as f is 1-1

Hence Ker $f = \{e\}$.

Conversely, let Ker f contain only the identity element.

Let $f(x) = f(y)$

Then $f(x)\ (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \text{Ker } f = \{e\}$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$ or that f is one-one.

Problem 24: *Let $f : G \to G'$ be a homomorphism. Let $a \in G$ be such that $o(a) = n$ and $o(f(a)) = m$. Show that $o(f(a)) \mid o(a)$ and f is* 1-1 *iff $m = n$.*

Solution: Since $o(a) = n$

we find $a^n = e \Rightarrow f(a^n) = f(e)$

$\Rightarrow f(a \,.\, a \,.....\, a) = f(e)$

$\Rightarrow (f(a))^n = e'$

$\Rightarrow o(f(a)) \mid n = o(a)$

Again, let f be 1–1.

Since $o(f(a)) = m$

we find $(f(a))^m = e'$

$\Rightarrow f(a) \,.\, f(a) \,.....\, f(a) = e'$

$\Rightarrow f(a \,.\, a \,.....\, a) = e'$

$\Rightarrow f(a^m) = e' = f(e)$

$\Rightarrow a^m = e$ (f is 1–1)

i.e., $o(a) \mid m$ or $n \mid m$, but already $m \mid n$

Hence $m = n$.

Conversely, let $o(a) = o(f(a))$.

Then $f(x) = f(y)$

$\Rightarrow f(x)\ (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow o(f(xy^{-1})) = 1$

$\Rightarrow o\,(xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y$

$\Rightarrow f$ is 1-1.

Remark: Under an isomorphism, order of any element is preserved.

Problem 25: *Show that the group $\langle \mathbf{R}, + \rangle$ of real numbers cannot be isomorphic to the group R^* of non zero real numbers under multiplication.*

Solution: $-1 \in R^*$ and order of -1 is 2 as $(-1)^2 = 1$. But $\mathbf{R}$ has no element of order 2. As

if $x \in \mathbf{R}$ is of order 2 then $2x = x + x = 0$. But this does not hold in $<\mathbf{R}, +>$ for any x except $x = 0$.

By above remark, under an isomorphism order of an element is preserved. Thus there cannot be any isomorphism between $\mathbf{R}$ and R^*.

Problem 26: *Show that every non zero homomorphism of* $<\mathbf{Q}, +>$ *to itself is an automorphism.*

Solution: Let $\theta : \mathbf{Q} \to \mathbf{Q}$, be any non zero homomorphism. We first show that

$$\theta\left(\frac{m}{n}\right) = \frac{m}{n}\theta(1) \text{ for any } \frac{m}{n} \in \mathbf{Q}$$

Suppose, $\theta(1) = p/q$

Then $$\frac{p}{q} = \theta(1) = \theta\left(\frac{n}{n}\right) = \theta\left(\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}\right) = n\theta\left(\frac{1}{n}\right)$$

Thus $$\theta\left(\frac{1}{n}\right) = \frac{1}{n}\theta(1)$$

So $$\theta\left(\frac{m}{n}\right) = \theta\left(\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}\right) = m\theta\left(\frac{1}{n}\right) = \frac{m}{n}\theta(1)$$

We now show θ is 1–1 onto.

Let $\frac{m}{n} \in$ Ker θ be any element. Then

$$\theta\left(\frac{m}{n}\right) = 0 \Rightarrow \left(\frac{m}{n}\right)\theta(1) = 0 \Rightarrow \frac{m}{n} = 0 \quad \text{or} \quad \theta(1) = 0$$

If $\theta(1) = 0$, then $\theta\left(\frac{1}{n}\right) = 0$ and $\theta(m) = m\theta(1) = 0$, $\forall\ m, n, n \neq 0$

$$\Rightarrow \theta\left(\frac{m}{n}\right) = 0 \quad \forall m, n, n \neq 0$$

or that θ is the zero homomorphism which is not so.

Hence $\frac{m}{n} = 0 \Rightarrow$ Ker $\theta = \{0\}$

$\Rightarrow \theta$ is 1–1

Let again $\frac{m}{n} \in \mathbf{Q}$ be any element then as

$$\theta\left(\frac{m}{n} \cdot \frac{q}{p}\right) = \frac{mq}{np}\theta(1) = \frac{m}{n}$$

we gather that θ is onto and hence is an automorphism.

Problem 27: *Let G be a group and* $f : G \to G$ *s.t.,* $f(x) = x^{-1}$ *be a homomorphism. Show that G is abelian.*

Solution: Let $x, y \in G$ be any elements.

$$\begin{aligned} xy &= (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1}) \\ &= f(y^{-1})\, f(x^{-1}) \\ &= yx, \text{ hence } G \text{ is abelian.} \end{aligned}$$

Theorem 9: (Fundamental theorem of group homomorphism). *If $f : G \to G'$ be an onto homomorphism with $K = Ker\, f$, then* $\dfrac{G}{K} \cong G'$.

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G.

Proof: Define a map $\varphi : \dfrac{G}{K} \to G'$, s.t.,

$$\varphi(Ka) = f(a), \quad a \in G$$

We show φ is an isomorphism.

That φ is well defined follows by

$$\begin{aligned} & Ka = Kb \\ \Rightarrow\ & ab^{-1} \in K = \text{Ker } f \\ \Rightarrow\ & f(ab^{-1}) = e' \\ \Rightarrow\ & f(a)(f(b))^{-1} = e' \\ \Rightarrow\ & f(a) = f(b) \\ \Rightarrow\ & \varphi(Ka) = \varphi(Kb) \end{aligned}$$

By retracing the steps backwards, we will prove that φ is 1–1.

Again as $$\begin{aligned} \varphi(KaKb) &= \varphi(Kab) = f(ab) = f(a)\, f(b) \\ &= \varphi(Ka)\ \varphi(Kb) \end{aligned}$$

we find φ is a homomorphism.

To check that φ is onto, let $g' \in G'$ be any element. Since $f : G \to G'$ is onto, $\exists\, g \in G$, s.t.,

$$f(g) = g'$$

Now $$\varphi(Kg) = f(g) = g'$$

Showing thereby that Kg is the required pre-image of g' under φ.

Hence φ is an isomorphism.

Remark: The above theorem is also called *first theorem of isomorphism*. It can also be stated as:

If $f : G \to G'$ is a homomorphism with $K = \text{Ker } f$, then $\dfrac{G}{\text{Ker}\, f} \cong f(G)$.

Theorem 10: (Second theorem of Isomorphism). *Let H and K be two subgroups of a group G, where H is normal in G, then*

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

Proof: It is easy to see that $H \cap K$ will be a normal subgroup of K and as $H \subseteq HK \subseteq G$, H will be normal in HK.

Define a map $f : K \to \dfrac{HK}{H}$ s.t.,

$$f(k) = Hk$$

then as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

we find f is well defined.

Again $f(k_1k_2) = Hk_1k_2 = Hk_1Hk_2 = f(k_1)f(k_2)$

shows f is a homomorphism.

That f is onto is obvious and thus using Fundamental theorem, we find

$$\frac{HK}{H} \cong \frac{K}{\text{Ker } f}$$

Since
$$\begin{aligned} k \in \text{Ker } f &\Leftrightarrow f(k) = H \\ &\Leftrightarrow Hk = H \\ &\Leftrightarrow k \in H \\ &\Leftrightarrow k \in H \cap K \quad (k \in K \text{ as } \text{Ker } f \subseteq K) \end{aligned}$$

We find $\text{Ker } f = H \cap K$

and our theorem is proved.

Lemma: *If H and K are two normal subgroups of a group G such that $H \subseteq K$, then $\dfrac{K}{H}$ is a normal subgroup of $\dfrac{G}{H}$, and conversely.*

Proof: $\dfrac{K}{H}$ is a non empty subset of $\dfrac{G}{H}$, by definition.

For any $Hk_1, Hk_2 \in \dfrac{K}{H}$

$$(Hk_1)(Hk_2)^{-1} = (Hk_1)(Hk_2^{-1}) = Hk_1k_2^{-1} \in \frac{K}{H}$$

i.e., $\dfrac{K}{H}$ is a subgroup.

Again, for any $Hk \in \dfrac{K}{H}$ and $Hg \in \dfrac{G}{H}$, we notice,

$$\begin{aligned} (Hg)^{-1}(Hk)(Hg) &= Hg^{-1}HkHg \\ &= Hg^{-1}kg \in \frac{K}{H} \end{aligned}$$

as $g \in G$, $k \in K$, K is normal in G gives $g^{-1}kg \in K$.

We leave the converse as an exercise for the reader.

Theorem 11: (Third theorem of isomorphism). *If H and K are two normal subgroups of G such that $H \subseteq K$, then*

$$\frac{G}{K} \cong \frac{G/H}{K/H}.$$

Proof: The above lemma ensures that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk of $\frac{G/H}{K/H}$.

Define a map $f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$$f(Ha) = Ka, \quad a \in G$$

f is well defined as

$$\begin{aligned} & Ha = Hb \\ \Rightarrow \quad & ab^{-1} \in H \subseteq K \\ \Rightarrow \quad & Ka = Kb \\ \Rightarrow \quad & f(Ha) = f(Hb) \end{aligned}$$

f is a homomorphism as

$$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)\, f(Hb).$$

Ontoness of f is obvious.

Using Fundamental theorem of group homomorphism we can say

$$\frac{G}{K} \cong \frac{G/H}{\text{Ker } f}$$

We claim $\text{Ker } f = \frac{K}{H}$

A member of Ker f will be some member of $\frac{G}{H}$.

Now $Ha \in \text{Ker } f \Leftrightarrow f(Ha) = K$ (identity of G/K)

$$\begin{aligned} & \Leftrightarrow Ka = K \\ & \Leftrightarrow a \in K \\ & \Leftrightarrow Ha \in \frac{K}{H} \end{aligned}$$

Hence we find $\frac{G}{K} \cong \frac{G/H}{K/H}$

which proves our result. It is also called *Freshman's theorem*.

Remark: Since $\frac{K}{H} = \text{Ker } f$, we notice that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and hence we

can talk of $\frac{G/H}{K/H}$. Thus we need not prove separately that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$.

Theorem 12: *Let $f: G \to G'$ be an onto homomorphism with Ker $f = K$. For H' a subgroup of G', define*

$$H = \{x \in G \mid f(x) \in H'\}$$

Then

(*i*) *H is a subgroup of G and $K \subseteq H$.*

(*ii*) *H' is normal subgroup of G' iff H is normal in G.*

(*iii*) *If H' is normal in G' then $\frac{G'}{H'} \cong \frac{G}{H}$.*

(*iv*) *This association gives a one-one onto mapping from the family $\boldsymbol{S}'$ of all subgroups of G' onto the family $\boldsymbol{S}$ of all subgroups of G, that contain K.*

Proof: (*i*) $H \neq \varphi$ as $f(e) = e' \in H'$ shows $e \in H$

Again, $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)(f(y))^{-1} \in H'$.

$\Rightarrow f(xy^{-1}) \in H' \Rightarrow xy^{-1} \in H$

Thus H is a subgroup.

Since $x \in$ Ker $f = K \Rightarrow f(x) = e' \in H'$

we find $x \in H \Rightarrow K \subseteq H$.

(*ii*) Let H be normal in G.

Let $g' \in G'$, $h' \in H'$ be any elements. Since f is onto $\exists\ g \in G$, $h \in G$ such that $f(g) = g'$, $f(h) = h'$. Since $h' \in H$, $h \in H$

Now

$g'^{-1} h'g' = (f(g))^{-1} f(h) f(g)$

$= f(g^{-1}) f(h) f(g) = f(g^{-1}hg) \in H'$

as $g \in G$, $h \in H$, H is normal in G means $g^{-1}hg \in H$

Thus H' is normal in G'.

Conversely, let H' be normal in G'.

For any elements $h \in H$, $g \in G$,

$f(g^{-1} hg) = (f(g))^{-1} f(h) f(g) \in H'$

as $f(h) \in H'$, $f(g) \in G'$, H' is normal in G'

$\Rightarrow g^{-1}hg \in H$ or that H is normal in G.

(*iii*) Define a mapping $\varphi: G \to \frac{G'}{H'}$ s.t.,

$$\varphi(g) = H' f(g)$$

then φ is well defined as $g_1 = g_2$

$$\Rightarrow f(g_1) = f(g_2)$$

$$\Rightarrow H' f(g_1) = H' f(g_2)$$
$$\Rightarrow \varphi(g_1) = \varphi(g_2)$$

φ will be a homomorphism as

$\varphi(g_1 g_2) = H' f(g_1 g_2) = H' f(g_1) f(g_2) = H' f(g_1)\ H' f(g_2)$
$= \varphi(g_1)\varphi(g_2)$

Again, for any $H'g' \in \dfrac{G'}{H'}$ since $g' \in G'$ and f is onto $\exists\ g \in G$, s.t., $f(g) = g'$

or that $\varphi(g) = H' f(g) = H'g'$ showing that φ is onto.

By fundamental theorem then

$$\frac{G'}{H'} \cong \frac{G}{\text{Ker } \varphi}$$

Now $x \in \text{Ker } \varphi \Leftrightarrow \varphi(x) = H'$
$\Leftrightarrow H' f(x) = H'$
$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$

Hence $\text{Ker } \varphi = H$

(*iv*) Define a mapping $\psi : \boldsymbol{S'} \to \boldsymbol{S}$, s.t.,

$$\psi(H') = H$$

where, of course, H is $\{x \in G \mid f(x) \in H'\}$ for any H' in $\boldsymbol{S'}$ By (*i*) we know that it is subgroup of G, containing K and is thus a member of $\boldsymbol{S}$. ψ is, therefore, a well defined mapping.

Let now $\psi(H') = \psi(T')$ where $H', T' \in \boldsymbol{S'}$

then $H = T$ where

$H = \{x \in G \mid f(x) \in H'\}$

$T = \{x \in G \mid f(x) \in T'\}$

Now for any $h' \in H' \subseteq G'$, since $f : G \to G'$ is onto, we can find $h \in G$, s.t., $f(h) = h' \in H'$

But this shows $h \in H = T$
$\Rightarrow f(h) \in T'$
$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$

Similarly $T' \subseteq H'$

i.e., $H' = T'$ or that ψ is one-one.

We show now ψ is onto.

Let $H \in \boldsymbol{S}$ be any member, then H is a subgroup of G and $K \subseteq H$.

Consider $f(H) = \{f(h) \mid h \in H\}$

then $f(H) \neq \varphi$ as $e \in H \Rightarrow f(e) = e' \in f(H)$

Again, for any $f(h_1), f(h_2) \in f(H)$, $h_1, h_2 \in H$

and $(f(h_1))(f(h_2))^{-1} = f(h_1 h_2^{-1}) \in f(H)$

i.e., $f(H)$ is a subgroup of G'.

We show $f(H) = H'$ is the required pre-image of H under ψ,

i.e., we show $\psi(H') = H$,

For that we need show $H = \{x \in G \mid f(x) \in H'\}$

Let $x \in H$ then $f(x) \in f(H) = H'$

$$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$$

or that $H \subseteq \{x \in G \mid f(x) \in H'\}$

Again, if $x \in \{x \in G \mid f(x) \in H'\}$

then $f(x) \in H' = f(H)$

$\exists\ h \in H$, s.t., $f(x) = f(h)$

$$\Rightarrow f(xh^{-1}) = e'$$

$$\Rightarrow xh^{-1} \in \text{Ker } f = K$$

$$\Rightarrow x \in Kh \subseteq H \quad [K \subseteq H]$$

Thus $\{x \in G \mid f(x) \in H'\} \subseteq H$

Hence $H = \{x \in G \mid f(x) \in H'\}$

or that $\psi(H') = H$ and so ψ is onto.

which completes the proof.

In the following problems we state and prove a *milder version* of the above theorem and its application.

Problem 28: *Let $f : G \to G'$ be an onto homomorphism from group G to G'. Let H be a subgroup of G and H', a subgroup of G'. Then*

(*i*) *$f(H)$ is a subgroup of G'.*

(*ii*) *$f^{-1}(H')$ is a subgroup of G containing $K = Ker\ f$, where by $f^{-1}(H')$ we mean $\{x \in G \mid f(x) \in H'\}$*

Notice that the set $f^{-1}(H')$ is defined here whether or not f has an inverse. The notation f^{-1} as used here is only symbolic.

Solution: (*i*) Since e = identity of G belongs to H

we have $f(e) \in f(H)$

$$\Rightarrow f(H) \neq \varphi.$$

Let $x, y \in f(H) \Rightarrow x = f(h_1),\ y = f(h_2)$ where $h_1, h_2\ H$.

$$\therefore \quad xy^{-1} = f(h_1)\ (f(h_2))^{-1}$$

$$= f(h_1)\ (f(h_2{}^{-1})$$

$$= f(h_1h_2^{-1}) \in f(H) \quad \text{as } h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$$

So, $f(H)$ is a subgroup of G'.

(*ii*) Let, $a, b \in f^{-1}(H')$

$$\Rightarrow f(a), f(b) \in H'$$

$$\Rightarrow f(a)\ .\ f(b)^{-1} \in H'$$

$$\Rightarrow f(ab^{-1}) \in H'$$

$\Rightarrow ab^{-1} \in f^{-1}(H')$

Also $f(e) = e'$ = identity of $G' \in H'$

$\Rightarrow e \in f^{-1}(H')$

$\Rightarrow f^{-1}(H') \neq \varphi$

So, $f^{-1}(H')$ is a subgroup of G

Also $k \in K \Rightarrow f(k) = e' \in H$

$\Rightarrow k \in f^{-1}(H')$

$\Rightarrow K \subseteq f^{-1}(H')$

This proves (*ii*).

Problem 29: (*i*) *Let f: $G \to G'$ be a homomorphism and suppose $g \in G$ be such that $f(g) = g'$. Then if $f^{-1}(g') = \{x \in G \mid f(g) = g'\}$ be the set containing all the pre images of g' under f, show that $f^{-1}(g') = Kg$ where $K = Ker\ f$.*

(ii) If f: $U_{30} \to U_{30}$ be a homomorphism s.t., Ker $f = \{1, 11\}$ and $f(7) = 7$ then find all the elements of U_{30} that are mapped to 7. Conversely, find a homomorphism f: $U_{30} \to U_{30}$.

s.t., Ker $f = \{1, 11\}$ and $f(7) = 7$.

Solution: (*i*) Let $x \in f^{-1}(g')$ be any element

Then $f(x) = g' \Rightarrow f(x) = f(g)$

$\Rightarrow f(x)(f(g))^{-1} = e'$

$\Rightarrow f(xg^{-1}) = e'$

$\Rightarrow xg^{-1} \in \text{Ker } f = K$

$\Rightarrow x \in Kg \Rightarrow f^{-1}(g') \subseteq K$

Again, Let $k \in K$ be any element,

then $f(kg) = f(k)f(g) = e'g' = g'$

$\Rightarrow Kg \in f^{-1}(g') \quad \forall\ k \in K$

$\Rightarrow Kg \subseteq f^{-1}(g')$

and hence $f^{-1}(g') = Kg$

(*ii*) By part (*i*), set of pre images of 7 is $K7$, where $K = \text{Ker } f = \{1, 11\}$

Thus set of pre images of 7 is

$K7 = \{1 \otimes 7, 11 \otimes 7\} = \{7, 17\}$

Conversely, let f: $U_{30} \to U_{30}$ be a homomorphism s.t.,

Ker $f = \{1, 11\}$ and $f(7) = 7$.

then $f(1) = 1, f(11) = 1, f(7) = 7$

Also as $7 \otimes 11 = 17$.

$$f(7\otimes 11) = f(17) \Rightarrow f(17) = f(7)\otimes f(11) = 7\otimes 1 = 7$$

$$7\otimes 17 = 29 \Rightarrow f(29) = f(7)\otimes f(17) = 7\otimes 7 = 19$$

Similarly, we get other values

$$f(13) = 13,\ f(19) = 19,\ f(23) = 13$$

Remark: As mentioned in previous problem f^{-1} is only symbolic and not essentially inverse.

Theorem 13: *Let N be a normal subgroup of G. Then there exists a* 1-1 *onto mapping from* ***A****, the set of all subgroups of G, containing N and* ***B****, the set of all subgroups of G/N.*

Proof: Let $f : G \to G/N$, s.t.,

$f(x) = Nx$

be the natural homomorphism.

If $H \leq G$ then $f(H) = \{f(h) \mid h \in H\} = \{Nh \mid h \in H\} = \dfrac{H}{N}$

Define θ: $\boldsymbol{A} \to \boldsymbol{B}$, s.t.,

$$\theta(H) = f(H) = \frac{H}{N}$$

Then $H = K \Rightarrow \dfrac{H}{N} = \dfrac{K}{N} \Rightarrow \theta(H) = \theta(K) \Rightarrow \theta$ is well defined.

Again $\theta(H) = \theta(K) \Rightarrow \dfrac{H}{N} = \dfrac{K}{N}$.

Now $h \in H \Rightarrow Nh \in \dfrac{H}{N} = \dfrac{K}{N} \Rightarrow \exists\ k \in K$, s.t., $Nh = Nk \Rightarrow hk^{-1} \in N \subseteq K$

i.e., $hk^{-1} = k_1$, for some $k_1 \in K$ and so $h = k_1k^{-1} \in K$ and thus $H \subseteq K$

Similarly $K \subseteq H$ and so $H = K$, showing that θ is 1-1.

Let $\overline{H} \in \boldsymbol{B}$ be any member, then $\overline{H}$ is a subgroup of G/N.

Let $H = \{x \in G \mid f(x) \in \overline{H}\}$ then H is a subgroup of G

$[x, y \in H \Rightarrow f(x), f(y) \in \overline{H}.\ f(xy^{-1}) = f(x)\ [f(y)]^{-1} \in \overline{H} \Rightarrow xy^{-1} \in H]$

If $n \in N = \text{Ker}\, f$ then $f(n) = N =$ identity of G/N and as identity is in $\overline{H}$

$$f(n) \in \overline{H} \Rightarrow n \in H \text{ or that } N \subseteq H$$

Thus H is a subgroup of G, containing N and clearly, by definition of H, we find

$$\theta(H) = \overline{H}$$

Hence θ is onto.

Problem 30: *Let N be a normal subgroup of G, then show that any subgroup of G/N is of the type* $\dfrac{H}{N}$*, where H is a subgroup of G and* $N \subseteq H$.

Solution: Let $\overline{H}$ be any subgroup of G/N.

Let $f : G \to G/N$, s.t., $f(x) = Nx$ be the natural homomorphism.

Let $H = \{x \in G \mid f(x) \in \overline{H}\}$, then $H \leq G$ and $N \subseteq H$ as in above theorem.

Now $\dfrac{H}{N} = \{Nh \mid h \in H\} = \{f(h) \mid h \in H\} = f(H) = \overline{H}$

which proves the result.

Problem 31: *Find all the subgroups of* $\dfrac{\mathbf{Z}}{(12)}$, *where*

$\mathbf{Z}$ = *group of all integers under addition*

and (12) = *subgroup of* $\mathbf{Z}$ *consisting of all multiples of* 12.

Solution: By above problem, any subgroup of $\dfrac{\mathbf{Z}}{(12)}$ is of the form $\dfrac{H}{(12)}$ where H is a subgroup of $\mathbf{Z}$ under addition and contains (12). But any subgroup of $\mathbf{Z}$ under addition is (n) = set of all multiples of n, $n \geq 0$.

$\therefore$ H = (2), (3), (4), (6), (12). So subgroups of $\dfrac{\mathbf{Z}}{(12)}$ are

$$\frac{(2)}{(12)}, \frac{(3)}{(12)}, \frac{(4)}{(12)}, \frac{(6)}{(12)}, \frac{(12)}{(12)}$$

Note $\dfrac{(2)}{(12)} = \{(12), (12) + 2, (12) + 4, (12) + 6, (12) + 8, (12) + 10\}$

$$\frac{(3)}{(12)} = \{(12), (12) + 3, (12) + 6, (12) + 9\}$$

$$\frac{(4)}{(12)} = \{(12), (12) + 4, (12) + 8\}$$

$$\frac{(6)}{(12)} = \{(12), (12) + 6\}$$

$$\frac{(12)}{(12)} = \{(12)\}.$$

Problem 32: *Show that any infinite cyclic group is isomorphic to* $< \mathbf{Z}, + >$ *the group of integers.*

Solution: Let $G = < a >$ be any infinite cyclic group.

Define $f : G \to \mathbf{Z}$, *s.t.*,

$f(a^i) = i, \quad i \in \mathbf{Z}$

Since $G = < a >$ is of infinite order, $a^i \in G$ for all $i \in \mathbf{Z}$ and $a^i = a^j$ for no $i \neq j$.

Thus $a^i = a^j \Rightarrow i = j \Rightarrow f(a^i) = f(a^j)$ or that f is well defined.

Again $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j \Rightarrow f$ is 1-1.

$f(a^i \cdot a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$

shows that f is a homomorphism.

f is obviously onto and hence the isomorphism is established.

Cor.: Every subgroup of an infinite cyclic group is an infinite cyclic group which is isomorphic to the group itself.

Problem 33: *Any finite cyclic group of order n is isomorphic to* $\mathbf{Z}_n$ *the group of integers addition modulo n.*

Solution: Let $G = <a>$ be a cyclic group s.t.,

$$o(G) = o(a) = n$$

then $G = \{e, a, a^2, ..., a^{n-1}\}$, $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\}$

Define $f : G \to \mathbf{Z}_n$ s.t., $f(a^i) = i$

f is clearly well defined 1-1 onto mapping.

Again $f(a^i \cdot a^j) = f(a^{i \oplus j}) = i \oplus j = f(a^i) \oplus f(a^j)$

Thus f is a homomorphism and hence an isomorphism.

Remark: Any two cyclic groups of same order (finite or infinite) are isomorphic.

Problem 34: *Show that any finite cyclic group of order n is isomorphic to the quotient group* $\frac{\mathbf{Z}}{N}$, *where* $<\mathbf{Z}, +>$ *is group of integers and* $N = <n>$.

Solution: Let $G = <a>$ be of order n

Define $f : \mathbf{Z} \to G$, s.t.,

$f(m) = a^m$

then f is clearly well defined onto map.

Since $f(m + k) = a^{m+k} = a^m \, a^k = f(m) \cdot f(k)$

f is a homomorphism and therefore, by Fundamental theorem $G \cong \frac{\mathbf{Z}}{\text{Ker } f}$

We show $\text{Ker } f = N = <n>$

Now $m \in \text{Ker } f \Leftrightarrow f(m) = e$

$\Leftrightarrow a^m = e$

$\Leftrightarrow o(a) \mid m$

$\Leftrightarrow n \mid m$

$\Leftrightarrow m \in <n>$

Hence $G \cong \frac{\mathbf{Z}}{<n>}$.

Remark: In view of the above results, we notice

$$\mathbf{Z}_n \cong \frac{\mathbf{Z}}{<n>}.$$

Compare the solution of problem 31 on page 130 and the comments on page 85 just after theorem 23.

Problem 35: *If G is the additive group of reals and N is the subgroup of G consisting of integers, prove that $\frac{G}{N}$ is isomorphic to the group H of all complex numbers of absolute value 1 under multiplication.*

Solution: Define a map

$$f : G \to H, \text{ s.t.,}$$
$$f(\alpha) = e^{2\pi i\alpha}$$

where $| e^{2\pi i\alpha} | = | \cos 2\pi\alpha + i \sin 2\pi\alpha |$

$$= \sqrt{\cos^2(2\pi\alpha) + \sin^2(2\pi\alpha)} = 1$$

We show f is onto.

Let $h \in H$ be any element, then $h = a + ib$

where $| a + ib | = 1 = \sqrt{a^2 + b^2}$

If $a + ib = r(\cos\theta + i \sin\theta)$

then $(a + ib) = 1 \Rightarrow r = 1$

$\therefore$ $a + ib = \cos\theta + i \sin\theta = e^{i\theta}$

then $$f\left(\frac{\theta}{2\pi}\right) = e^{\frac{\theta}{2\pi}\cdot 2\pi i} = e^{i\theta}$$

$\Rightarrow$ $\frac{\theta}{2\pi}$ is the required pre-image.

Again f is a homomorphism, as

$$f(\theta_1 + \theta_2) = e^{2\pi(\theta_1+\theta_2)i} = e^{2\pi\theta_1 i} \cdot e^{2\pi\theta_2 i}$$
$$= f(\theta_1)\, f(\theta_2)$$

By fundamental theorem of group homomorphism

$$H \cong \frac{G}{\text{Ker } f}$$

We claim $\text{Ker } f = N$

Now $\alpha \in \text{Ker } f \Leftrightarrow f(\alpha) = 1$

$\Leftrightarrow e^{2\pi i\alpha} = 1$

$\Leftrightarrow \cos 2\pi\alpha + i \sin 2\pi\alpha = 1 = 1 + i0$

$\Leftrightarrow \cos 2\pi\alpha = 1, \sin 2\pi\alpha = 0$

$\Leftrightarrow 2\pi\alpha = 2\pi\alpha\, n \pm 0$ where n is an integer

$\Leftrightarrow \alpha = n$

$\Leftrightarrow \alpha \in N$

thus $\text{Ker } f = N$

and hence $H \cong \frac{G}{N}$.

Problem 36: *Let G be the group of all non zero complex numbers under multiplication and let G′ be the group of all real* 2×2 *matrices of the form* $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, *where not both a and b are zero, under matrix multiplication, show that* $G \cong G'$.

Solution: Define a map

$$\varphi : G \to G', \text{ s.t.,}$$

$$\varphi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

φ is clearly well-defined.

Also

$$\varphi[(a + ib)\ \varphi(c + id)] = \varphi[(ac - bd) + i(ad + bc)] = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}$$

and

$$\varphi(a + ib)\ \varphi(c + id) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}$$

shows that φ is a homomorphism.

Again for $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, the required pre-image is $(a + ib)$.

Thus φ is onto.

Also, $\varphi(a + ib) = \varphi(c + id)$

$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$\Rightarrow a = c,\ b = d \Rightarrow a + ib = c + id$$

Hence φ is an isomorphism.

Problem 37: *Suppose G is a group of order* p^2, *where p is a prime. Let* $\varphi : G \to H$ *be an onto homomorphism, where H is a group. Then show that either* φ *is an isomorphism or* φ *maps each element x of G onto the identity e of H and* $H = \{e\}$ *or else, for each* $y \in H$, $\exists$ *exactly p elements x of G such that* $\varphi(x) = y$.

Solution: $\varphi : G \to H$ is an onto homomorphism

$o(G) = p^2$.

Since Ker φ is a subgroup of G, by Lagrange's theorem $o(\text{Ker } \varphi) \mid o(G) = p^2$

$\Rightarrow$ $o(\text{Ker } \varphi) = 1, p$ or p^2

Case *(i)*: $o(\text{Ker } \varphi) = 1 \Rightarrow \text{Ker } \varphi = \{e\}$

$\Rightarrow \varphi$ is 1-1.

hence φ is an isomorphism.

Case *(ii)*: $o(\text{Ker } \varphi) = p^2$

$\Rightarrow$ Ker $\varphi = G$

$\Rightarrow$ for all $x \in G$, $x \in$ Ker $\varphi \Rightarrow \varphi(x) = e$ for all $x \in G$

Since φ is onto, each element of H has a pre-image, but all members of G are mapped to e.

$\therefore$ $H = \{e\}$.

Case *(iii)*: $o(\text{Ker } \varphi) = p$

Let $y \in H$ be any element then as φ is onto, $\exists\ x \in G$, s.t., $\varphi(x) = y$

Let Ker $\varphi = \{a_1 = e, a_2, a_3, ..., a_p\}$

We claim $xa_1, xa_2, ..., xa_p$ are distinct.

Suppose $xa_i = xa_j$, then $a_i = a_j$

which is not true.

Thus $xa_1, xa_2, ..., xa_p$ are distinct members of G.

Now $\varphi(xa_i) = \varphi(x)\varphi(a_i)$ $i = 1, 2, ..., p.$

$= ye = y$ for all i $(a_i \in \text{Ker } \varphi)$

thus y has p pre-images $x = xa_1, xa_2, ..., xa_p$

To show that y does not have more than p pre-images, let x' be any other pre-image of y under φ

Then $\varphi(x') = y = \varphi(x)$

$\Rightarrow (\varphi(x))^{-1}\ \varphi(x') = e$

$\Rightarrow \varphi(x^{-1}\ x') = e$

$\Rightarrow x^{-1}\ x' \in \text{Ker } \varphi$

$\Rightarrow x^{-1}\ x' = a_i$ for some i

$\Rightarrow x' = xa_i$ for some i

i.e., it is one of the p pre-images, we have considered.

Hence y has exactly p pre-images.

Problem 38: *Find all the homomorphisms from* $\mathbf{Z}_{20} \to \mathbf{Z}_8$. *How many of these are onto?*

Solution: Let f: $\mathbf{Z}_{20} \to \mathbf{Z}_8$ be any homomorphism

where $\mathbf{Z}_{20} = \{0, 1, 2, ..., 19\}$ mod 20

$\mathbf{Z}_8 = \{0, 1, 2, ..., 7\}$ mod 8

Suppose $f(1) = a$, then for any $x \in \mathbf{Z}_{20}$

$$f(x) = f(1 + 1+...+1) = xf(1) = xa$$

i.e., all homomorphisms are determined if we know a

Since $a \in \mathbf{Z}_8$ $o(a) \mid o(\mathbf{Z}_8) = 8$.

Again, (See Problem 24, page 120) $o(f(1)) \mid o(1) = 20$ or that $a \mid 20$

Hence possible values of $o(a)$ are 1, 2, 4

Now, if $o(a) = 1$, then a is identity of $\mathbf{Z}_8$

i.e., $a = 0$

if $o(a) = 2$, then $2a = 0 \Rightarrow a = 4$ as $4 \oplus 4 = 0$

if $o(a) = 4$, then $4a = 0 \Rightarrow a = 2$ as $2 \oplus 2 \oplus 2 \oplus 2 = 0$

or $a = 6$ as $6 \oplus 6 \oplus 6 \oplus 6 = 0$

Hence possible values of a will be 0, 4, 2, 6

meaning thereby that $\exists$ 4 homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_8$

If f: $\mathbf{Z}_{20} \to \mathbf{Z}_8$ is an onto homomorphism then by Fundamental theorem

$$\mathbf{Z}_8 \cong \frac{\mathbf{Z}_{20}}{\text{Ker}\, f}$$

$$\Rightarrow o(\mathbf{Z}_8) = \frac{o(\mathbf{Z}_{20})}{o(\text{Ker}\, f)}$$

$$\Rightarrow o(\text{Ker}\, f) = \frac{20}{8} = \frac{5}{2}$$

which is not possible. Hence none of the homomorphisms is onto.

Problem 39: *Prove that if* $\frac{G}{H} \cong \frac{G}{K}$ *and G is cyclic then H = K. Show by an example that H may not equal K when G is not cyclic.*

Solution: Let $G = < a >$ and suppose $H = < a^n >$ and $K = < a^m >$. Then n is the smallest +ve integer s.t., $a^n \in H$ (see theorem 19, chapter 2). Thus H, Ha, ..., Ha^{n-1} are distinct right cosets of H in G and no more. So $i_G(H) = n$.

Similarly, $i_G(K) = m$.

Now $\frac{G}{H} \cong \frac{G}{K} \Rightarrow i_G(H) = i_G(K)$

$\Rightarrow n = m$ or that $H = K$.

For the second part take G to be the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ then G is not cyclic (It is not abelian).

Let $H = \{\pm 1, \pm i\}$, $K = \{\pm 1, \pm j\}$

then H, K are normal subgroups of G and $\frac{G}{H} = \{H, Hj\}$, $\frac{G}{K} = \{K, Ki\}$

The mapping $H \to K$, $Hj \to Ki$ will be an isomorphism, whereas $H \neq K$.

Problem 40: *Show that the group* $\mathbf{Z}_4$ *under addition modulo* 4 *is isomorphic to the group* U_5 *under multiplication mod* 5. *Give two isomorphisms between* U_5 *and* $\mathbf{Z}_4$.

Solution: The group $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ addition mod 4 is cyclic group of order 4 and has $\varphi(4) = 2$ generators 1 and 3.

($1^1 = 1$, $1^2 = 1 \oplus 1 = 2$, $1^3 = 1 \oplus 1 \oplus 1 = 3$, $1^4 = 0$.

Also $3^1 = 3$, $3^2 = 3 \oplus 3 = 2$, $3^3 = 1$, $3^4 = 0$).

Also the group $U_5 = \{1, 2, 3, 4\}$ multiplication mod 5 is cyclic group of order 4 having generators 2 and 3.

($2^1 = 2$, $2^2 = 2 \otimes 2 = 4$, $2^3 = 3$, $2^4 = 1$; $3^1 = 3$, $3^2 = 3 \otimes 3 = 4$, $3^3 = 2$, $3^4 = 1$).

Since any two cyclic groups of same order are isomorphic (Remark on page 131) we find $\boldsymbol{Z}_4$ and U_5 are isomorphic.

The following maps are the two isomorphisms:

$\theta : U_5 \to \mathbf{Z}_4$ s.t.,

$\theta(1) = \theta(2^4) = 0$

$\theta(2) = 1$

$\theta(3) = \theta(2^3) = \theta(2 \otimes 2 \otimes 2) = \theta(2) \oplus \theta(2) \oplus \theta(2) = 3$

$\theta(4) = \theta(2^2) = \theta(2 \otimes 2) = \theta(2) \oplus \theta(2) = 1 \oplus 1 = 2$

$\psi : U_5 \to \mathbf{Z}_4$ s.t.,

$\psi(1) = 0$

$\psi(2) = 3$

$\psi(3) = \psi(2 \otimes 2 \otimes 2) = \psi(2) \oplus \psi(2) \oplus \psi(2) = 3 \oplus 3 \oplus 3 = 1$

$\psi(4) = \psi(2 \otimes 2) = \psi(2) \oplus \psi(2) = 3 \oplus 3 = 2$

Notice under an isomorphism a generator is mapped to a generator.

The Dihedral Group

Let $G = \{x^i y^j \mid i = 0, 1, j = 0, 1, \ldots\ldots, n-1, x^2 = e = y^n, xy = y^{-1}x\}$

Then G is a group, called the dihedral group. ($n \geq 3$).

In fact, we can also write G as

$$G = \begin{Bmatrix} y, y^2, \ldots\ldots, y^{n-1}, y^n = e \mid x^2 = e = y^n, xy = y^{-1}x \\ xy, xy^2, \ldots\ldots, xy^{n-1}, x \end{Bmatrix}$$

$o(G) = 2n$. We write $G = D_{2n}$

What is the product $(xy)(xy^2)$ in terms of elements of G written as above?

Now $xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1}$

$\Rightarrow xyx = y^{-1}$ as $x^2 = e \Rightarrow x = x^{-1}$

$\therefore (xy)(xy^2) = (xyx)y^2$

$= y^{-1}y^2 = y$

Also, how to find yxy^2?

Since $xy = y^{-1}x \Rightarrow yxy = x$

$\Rightarrow yxy^2 = xy$

In this way, we can compute the product of any two elements of G

We first find $Z(G)$

Consider $y^i \quad (1 \le i \le n)$

Then $y^i (xy^i) = (y^i x y^i)\, y^{-i+j}$

$= xy^{-i+j}$

Note $xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1}$

$\Rightarrow (xyx^{-1})^i = y^{-i}$

$\Rightarrow xy^i x^{-1} = y^{-i}$

$\Rightarrow y^i x y^i = x$

(This is a very useful relation in D_{2n}).

Also $(xy^i)y^i = xy^{i+j}$

If $y^i \in Z(G)$, then y^i must commute with xy^j for all j, $1 \le j \le n$.

$\therefore \quad xy^{-i+j} = xy^{i+j}$ for all j, $1 \le j \le n$

$\Rightarrow y^{2i} = e$

$\Rightarrow o(y)$ divides $2i$

$\Rightarrow n$ divides $2i$

Case 1: n = odd

Then $n \mid 2i$ and $(n, 2) = 1$

$\Rightarrow n \mid i$

$\Rightarrow n \le i$. But $i \le n$

$\therefore \quad i = n$.

So, $y^i = y^n = e$.

Similarly, if $xy^i \in Z(G)$, then $(xy^i)\, x = x(xy^i)$

$\Rightarrow xy^i x^{-1} = x^2 y^i$

$\Rightarrow y^{-i} = x^2 y^i$

$\Rightarrow y^{2i} = e$ as $x^2 = e$

$\Rightarrow o(y) \mid 2i \Rightarrow n \mid 2i \Rightarrow n \mid i \Rightarrow n = i$

$\therefore \quad xy^i = xy^n = x$

But $x \notin Z(G)$ as $xy = y^{-1} x$ (and $x \in Z(G)$ should imply $xy = yx$,

i.e., $yx = y^{-1} x \Rightarrow y^2 = e \Rightarrow o(y) = n \mid 2 \Rightarrow n \le 2$, a contradiction as $n \le 3$).

So, $Z(G)$ does not contain any element of the type xy^i. Also if $y^i \in Z(G)$, then $i = n$

$\therefore \quad Z(G) = \{e\}$.

Case 2: n = even. Let $n = 2m$

Then as above $n \mid 2i$

$\Rightarrow 2m \mid 2i$

$\Rightarrow m \mid i$

$\Rightarrow i = m$ or $2m = n$

i.e., $y^i = y^m$ or $y^{2m} = y^n = e$

Clearly $y^m \in Z(G)$ as $(xy^k)\, y^m = xy^{k+m}$

and $y^m(xy^k) = (y^m x y^m)\, y^{k-m}$

$= xy^{k-m} = xy^{k+m}$

as $y^{2m} = e \Rightarrow y^m = y^{-m}$

$\therefore$ only powers i of y s.t., $y^i \in Z(G)$ are $i = m$ and $2m$.

Similarly, as in case 1, if $xy^i \in Z(G)$,

then $n \mid 2i \Rightarrow 2m \mid 2i \Rightarrow m \mid i \Rightarrow i = m$ or $2m$

But $xy^{2m} = xy^n = xe = x \notin Z(G)$

Also $(xy^m)\, y = xy^{m+1}$

and $y(xy^m) = yxy^m$

So, if $xy^m \in Z(G)$, then $xy^{m+1} = yxy^m$

$\Rightarrow xy = yx$

$\Rightarrow y^{-1}x = yx$

$\Rightarrow y^2 = e$

$\Rightarrow o(y)$ divides 2

$\Rightarrow n$ divides 2

$\Rightarrow n \leq 2$, a contradiction

$\therefore$ $Z(G) = \{e, y^m\}$, where $n = 2m$.

Thus, we have proved the following:

If n = odd, then $Z(D_{2n}) = \{e\}$ and if n = even $= 2m$, then $Z(D_{2n}) = \{e, y^m\}$.

Remarks (*i*) In the group G above, let us take x and y to be two permutations (members of S_n) where $o(x) = 2$ and $o(y) = n$, $(n \geq 3)$ with the condition that $xyx^{-1} = y^{-1}$

Suppose n is odd then if we take $y = (1\ 2\ 3 \ldots n)$ and $x = (1)(2n)\ (3\ n-1)\ \ldots (n-3,\ 5)$ then $o(y) = n$ and $o(x) = 2$.

and $xy\,x^{-1} = (x(1)\, x(2)\, x(3) \ldots x(n-3)\, x(n-2)\, x(n-1)\, x(n))$

$= (1\ n\ n-1 \ldots 5\ 4\ 3\ 2)$

$= (n\ n-1 \ldots 5\ 4\ 3\ 2\ 1) = y^{-1}$

Let n be even. Take $y = (1\ 2\ 3 \ldots n)$. Then $o(y) = n$.

Let $x = (1,\ n-3)(2,\ n-4) \ldots (n-3,\ 1)(n-2,\ n)\ (n-1)\ (n\ n-2)$

Then $xy\,x^{-1} = (x(1)\, x(2)\, x(3) \ldots x(n-2)\, x(n-1)\, x(n))$

$= (n-3\ n-4\ n-5 \ldots n\ n-1\ n-2)$

$= (n\ n-1\ n-2 \ldots 2\ 1) = y^{-1}$

(*ii*) Let $H = \langle y \rangle$. Then $x \notin H$ as $x \in H$ *implies* $x = y^i$

So, $xy^i = x^2 = e$ implies $xy^{i+1} = y$. Therefore, $y^2 = xy^{i+1}\, xy^{i+1} = y^{-i-1}y^{i+1} = e$ which implies $o(y) = n \mid 2$, a contradiction as $n \geq 3$. So, $G = H \cup xH$. This gives $o(G) = 2n$.

(*iii*) We can also regard the Dihedral group G to be the subgroup of $GL(2, \mathbf{C})$, the group of non singular 2×2 matrices over $\mathbf{C}$, the field of complex numbers. Let $n \geq 3$ and α be an nth root of unity.

Let $\alpha = e^{\frac{2\pi i}{n}}$.

Then $o(\alpha) = n$ in **C***, the group of non zero complex numbers under multiplication.

Let $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2, \mathbf{C}), \quad Y = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} \in GL(2, \mathbf{C}),$

Then $o(X) = 2$, $o(Y) = n$, and $XY = \begin{bmatrix} 0 & \alpha^{-1} \\ \alpha & 0 \end{bmatrix}$, $y^{-1} = \begin{bmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{bmatrix}$, $Y^{-1}X = \begin{bmatrix} 0 & \alpha^{-1} \\ \alpha & 0 \end{bmatrix} = XY.$

So, $XYX^{-1} = Y^{-1}$

Let $G = \langle X, Y \mid o(X) = 2, o(Y) = n, XYX^{-1} = Y^{-1} \rangle$

Let $H = \langle Y \rangle$.

Then $X \notin H$ as in (*ii*) above.

So, $G = H \cup XH$ and $o(G) = 2n$ as $o(H) = n$.

This gives $G = \{Y, Y^2, \ldots Y^n = I, XY, XY^2, \ldots, XY^{n-1}, XY^n = X\}$

Problem 41: *Show that* $N = \{y, y^2, \ldots\ldots, y^{n-1}, y^n = e\}$ *is a normal subgroup of* D_{2n}.

Solution: N is a subgroup of D_{2n} generated by y.

Let $g \in D_{2n}, y^i \in N$

If $g = y^j$, then $gy^i g^{-1} = y^j y^i y^{-j}$

$= y^i \in N.$

Let $g = xy^j, \quad 1 \le j \le n.$

Then $gy^i g^{-1}$

$= xy^j y^i (xy^j)^{-1}$

$= xy^{i+j} y^{-j} x^{-1}$

$= xy^i x^{-1}$

$= (xyx^{-1})^i$

$= y^{-i} \in N \quad (\text{as } xyx^{-1} = y^{-1})$

$\therefore N$ is a normal subgroup of G.

Problem 42 : *Let G be a group of order 2p, where p is an odd prime. Show that either G is cyclic or dihedral.*

Solution: Since G is of even order, it has an element of order 2. Let $b \in G$ be such that $o(b) = 2$. Let $H = \langle b \rangle$. If every non identity element of G has order 2 then G is abelian.

Any element of G can have order either 2 or p as $o(G) = 2p$.

Suppose $c \in G$, $c \neq b$ and $o(c) = 2$.

Let $K = \langle c \rangle$ then $HK \le G$ and $o(HK) = \frac{2 \times 2}{1} = 4$.

$\Rightarrow$ $4 \mid o(G)$, but that cannot hold as p is odd. So all elements ($\neq e$) of G cannot have order 2 implying that G has an element of order p. Let $o(a) = p$, $a \in G$. If G is abelian then $o(ab) = 2p = o(G)$ (see page 94) and thus G is cyclic.

Suppose now G is non abelian.

Let $M = < a >$ then $M \leq G$ having index 2

i.e., M will be normal.

$\Rightarrow b^{-1}ab \in M = < a >$

$\Rightarrow b^{-1}ab = a^i$

$\Rightarrow (b^{-1}ab)^i = a^{i^2} \Rightarrow b^{-1}a^ib = a^{i^2}$

$\Rightarrow b^{-1}(b^{-1}ab)b = a^{i^2} \Rightarrow a = a^{i^2} \Rightarrow a^{i^2-1} = e$

i.e., $i^2 \equiv 1 \pmod{p}$.

So p divides $i - 1$ or p divides $i + 1$

If p divides $i - 1$ then $a^{i-1} = e \Rightarrow a^i = a$

So $b^{-1}ab = a \Rightarrow ab = ba$

$\Rightarrow G$ is abelian, a contradiction.

If p divides $i + 1$ then $a^{i+1} = e \Rightarrow a^i = a^{-1}$

So $b^{-1}ab = a^{-1}$

Now $G = M \cup Mb$

$\therefore$ $G = \{e, a, ..., a^{p-1}, b, ab, ..., a^{p-1}b | a^p = e = b^2, b^{-1}ab = a^{-1}\}$

or that G is dihedral.

Problem 43: *Show that* $\frac{G}{N}$ *is isomorphic to the multiplicative group* $\{1, -1\}$, *where* $G = D_{2n}$ and $N = \{y, y^2, ..., y^{n-1}, y^n = e\}$.

Solution: Define $\theta : G \to W = \{1, -1\}$

$\theta(y^j) = 1$ for all $j = 1, 2, ..., n$

$\theta(xy^j) = -1$ for all $j = 1, 2, ..., n$

Clerarly θ is onto mapping.

Also $\theta(y^j\ xy^k)$

$= \theta(y^jxy^j\ y^{k-j})$

$= \theta(xy^{k-j})$

$= -1$

and $\theta(y^j)\ \theta(xy^k) = 1 . (-1) = -1$

$\therefore$ $\theta(y^j\ xy^k) = \theta(y^j)\ (xy^k)$

Similarly, $\theta(xy^k\ y^j) = \theta(xy^{k+j}) = -1$

and $\theta(xy^k)\ \theta(y^j) = (-1)\ (1) = -1$

$\therefore$ $\theta(xy^k\ y^j) = \theta(xy^k)\ \theta(y^j)$

So, θ is a homomorphism.

$\therefore$ $\frac{G}{\text{Ker}\ \theta} \cong W$

$$\text{Ker } \theta = \{g \in G \mid \theta(g) = 1\}$$
$$= \{y^j \mid 1 \le j \le n\}$$
$$= N$$

$$\therefore \quad \frac{G}{N} \cong W.$$

Problem 44: *Let G be the dihedral group of order 2n, n ≥ 2. Let m divide n. Let G′ be the dihedral group of order 2m. Then there exists a normal subgroup K of G such that* $\frac{G}{K} \cong G'$ (i.e., $\frac{D_{2n}}{K} \cong D_{2m}$).

Solution: Let $n = mk$

Let $G = \{e, a,...,a^{n-1}, b, ab,...,a^{n-1}b \mid a^n = e = b^2, b^{-1}ab = a^{-1}\}$

Now $o(a) = n$ implies $o(a^m) = k$

Let $K = < a^m >$. Then $o(K) = o(a^m) = k$.

We show that K is normal in G.

Let $g \in G$, $x \in K$. Now $g \in G$, implies $g = a^ib$ and $x \in K$ implies $x = a^{mr}$

So, $g^{-1}xg = b^{-1}a^{-i}a^{mr}a^{ib}$

$= b^{-1}a^{mr}b = a^{-mr} \in K$ as $b^{-1}ab = a^{-1}$.

This shows that K is normal in G.

Define θ: $G \to G' = \{e, x, ..., x^{m-1}, y, xy,...,x^{m-1}y \mid x^m = e = y^2, y^{-1}xy = x^{-1}\}$ s.t.,

$\theta(a^i) = x^i$

$\theta(b) = y$

$\theta(a^ib) = x^iy$

Then θ is a homomorphism and also θ is onto

If $a^i \in \text{Ker } \theta$, then $x^i = e$ implies $i \equiv 0 \pmod m$.

So, $a^i = a^{mu} \in K$. If $a^ib \in \text{Ker } \theta$, then $x^iy = e$ implies $x^i = y$.

So, $\theta(a^i) = \theta(b)$ implies $a^ib \in K$. But $a^i \in K$.

Therefore, $b \in K$ which implies $b = a^{mv} = e$.

So, Ker $\theta \subseteq K$. But $K \subseteq$ Ker θ.

Therefore, Ker $\theta = K$.

Hence, $$\frac{G}{K} \cong G'.$$

Exercises

1. If $f : G \to G'$ is a homomorphism then show that

$$f(G) = \{f(a) \mid a \in G\}$$

is a subgroup of G'. We also write $f(G) = \text{Im}f$ (Image f). Show further that if H is normal in G then $f(H)$ is normal in $f(G)$, *i.e.*, homomorphic image of a normal subgroup is normal.

2. For a fixed element a in a group G, define

$$f_a : G \to G, \text{ s.t., } f_a(x) = a^{-1} xa, \; x \in G$$

Show that f_a is an isomorphism.

3. Let f, g be homomorphisms from $G \to G'$. Show that

$$H = \{x \in G \mid f(x) = g(x)\} \text{ is a subgroup of } G.$$

4. Let G be a finite abelian group. Suppose $o(G)$ and n are co-prime. Show that $\varphi : G \to G$, s.t., $\varphi(x) = x^n$ is an isomorphism (in other words, any $g \in G$ can be expressed as $g = x^n$ where $x \in G$).

5. Show that the relation of isomorphism in groups is an equivalence relation.

6. Prove that the group $G = \{1, -1\}$ under multiplication is isomorphic to $G' = \{0, 1\}$ under addition modulo 2.

7. Show that $2\mathbf{Z} \cong 3\mathbf{Z}$ by considering the mapping $2x \to 3x$. Generalise.

8. Let G be the group of real numbers under addition. Show that $\theta : G \to G$, s.t., $\theta(x) = [x]$ is not a homomorphism, where $[x]$ is the greatest integer not greater than x.

9. Show that $f : \mathbf{C} \to \mathbf{C}$, s.t. $f(z) = \bar{z}$ is an automorphism where $\mathbf{C}$ = complex numbers.

10. Let G be the group of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ s.t., $ad - bc \neq 0$, under matrix multiplication and G' be the group of non zero real numbers under multiplication. Show that the map $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to ad - bc$ is an onto homomorphism.

11. Show that homomorphic image of

(*a*) an abelian group is abelian.

(*b*) a cyclic group is cyclic.

(*c*) a finite group is finite.

12. Show that converse does not hold in all the cases of the previous problem. (See example 9, page 149).

13. Let $\mathbf{R}$ be the set of real numbers. For $a, b \in \mathbf{R}$, $(a \neq 0)$ define $T_{ab} : \mathbf{R} \to \mathbf{R}$, s.t., $T_{ab}(x) = ax + b$.

Let G be set of all such maps and let $N = \{T_{1b} \in G\}$. Show that G is a group and N is a normal subgroup of G and that $\dfrac{G}{N}$ is isomorphic to the group of non zero real numbers under multiplication.

14. If φ is a homomorphism of a group G onto $\bar{G}$ with Kernel K and $\bar{N}$ is a normal subgroup of $\bar{G}$

$$N = \{x \in G \mid \varphi(x) \in \bar{N}\}$$

then prove that $\frac{G}{N} \cong \frac{\bar{G}}{\bar{N}}$ and $\frac{G}{N} \cong \frac{G/K}{N/K}$.

15. Show that $\frac{\mathbf{Z}_n}{<m>} \cong \mathbf{Z}_m$, where m is a divisor of n.

16. Let G be the group of non zero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1. Show that $\frac{G}{N}$ is isomorphic to the group of all positive real numbers under multiplication. (The group N, the unit circle in the complex plane, is called the *circle group*.)

17. Suppose the group $\frac{G}{H}$ is isomorphic to a group G'. Show that there exists an onto homomorphism θ from G to G' such that Ker $\theta = H$.

18. For any group G, show that $\frac{G}{\{e\}} \cong G$ and $\frac{G}{G} \cong \{e\}$.

19. Show that a simple group has no non-trivial homomorphic image.

20. Show that a subgroup N of G is normal in G if and only if $\exists$ a group H and a homomorphism $\theta : G \to H$ s.t., Ker $\theta = N$.

21. Let $G \cong G^*$ show that G is cyclic iff G^* is cylic. Hence show that $<\mathbf{Z}, +>$ is not isomorphic to $<\mathbf{Q}, +>$

22. If G is a cyclic group of order n and $p \mid n$, prove that there exists a homomorphism of G onto a cyclic group of order p. Find its Kernel.

23. Show that U_{10} is isomorphic to $\mathbf{Z}_4$ but not to U_{12}.

24. Show that a cyclic group of order n is isomorphic to multiplicative group of nth roots of unity. [Consider $a^r \to e^{2\pi ir/n}$].

25. Let G and G' be two finite groups s.t., $(o(G), o(G')) = 1$. Show that $\exists$ a unique (trivial) homomorphism from G to G'.

Permutation Groups

In Chapter 1 we discussed permutations, and in Chapter 2 we gave an example of permutation groups. We continue the discussion starting with

Theorem (Cayley's) 14: *Every group G is isomorphic to a permutation group.*

Proof: Let G be the given group and $A(G)$ be the group of all permutations of the set G.

For any $a \in G$, define a map $f_a : G \to G$, s.t.,

$$f_a(x) = ax$$

then as $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

f_a is well defined.

Again, $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ (cancellation in group G)

$\Rightarrow f_a$ is 1–1.

Also, for any $y \in G$, since $f_a(a^{-1} y) = a(a^{-1} y) = y$, we find $a^{-1} y$ is pre-image of y or that f_a is onto and hence a permutation on G.

Thus $f_a \in A(G)$.

Let K be the set of all such permutations. We show K is a subgroup of $A(G)$. $K \neq \varphi$ as $f_e \in K$.

Let $f_a, f_b \in K$ be any members

then since $f_b \; o \; f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x)) = f_b(b^{-1}x) = b(b^{-1}x)$

$= ex = f_e(x)$ for all x

we find $f_{b^{-1}} = (f_b)^{-1}$ (Note $f_e = I$, identity of $A(G)$).

Also as $(f_a \; o \; f_b)\; x = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$ for all x

we find $f_{ab} = f_a \; o \; f_b$

Now $f_a \; o \; (f_b)^{-1} = f_a \; o \; f_{b^{-1}} = f_{ab^{-1}} \in K$

Showing that K is a subgroup of $A(G)$.

Define now a mapping $\varphi : G \to K$, s.t.,

$\varphi(a) = f_a$

then φ is well defined, 1-1 map as

$a = b$

$\Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x) \quad \forall \; x$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \varphi(a) = \varphi(b)$

φ is obviously onto, and since

$\varphi(ab) = f_{ab} = f_a \; o \; f_b = \varphi(a)\; \varphi(b)$

φ is a homomorphism and hence an isomorphism which proves our assertion. Note K being a subgroup of a permutation group is a permutation group.

Remark: In particular, if G is a finite group of order n then G is isomorphic to a subgroup of S_n.

Problem 45: *Using Cayley's theorem, find the permutation group K isomorphic to the group G = {2, 4, 6, 8} under multiplication modulo 10.* (*Here 6 is the identity of G and G = <2>*).

Solution: The set K as defined in the Cayley's theorem above is given by

$K = \{f_a \mid a \in G\}$, where f_a is defined by $f_a(x) = ax$. Thus here $a = 2, 4, 8, 6$ and

$$f_2(2) = 4, \quad f_2(4) = 8, \quad f_2(8) = 6, \quad f_2(6) = 2$$
$$f_4(2) = 8, \quad f_4(4) = 6, \quad f_4(8) = 2, \quad f_4(6) = 4$$
$$f_8(2) = 6, \quad f_8(4) = 2, \quad f_8(8) = 4, \quad f_8(6) = 8$$
$$f_6(2) = 2, \quad f_6(4) = 4, \quad f_6(8) = 8, \quad f_6(6) = 6$$

Thus $f_6 = I$ and $K = \{f_2, f_4, f_8, f_6 = I\}$

If we identify f_2 with the permutation (1234), we notice the others are (13)(24), (1432) and thus K is {(1234), (13)(24), (1432), I} and this is the required premutation group isomorphic to G.

In fact the isomorphism can be viewed as $\theta: G \to K$, s.t.,

$$\theta(2) = (1234), \ \theta(4) = (13)(24), \ \theta(8) = (1432), \ \theta(6) = I$$

Problem 46: *Using Cayley's theorem find the permutation group isomorphic with the dihedral group of order 8.*

Solution: The dihedral group of order 8 is given by

$$G = \{a, a^2, a^3, a^4 = e, ab, a^2b, a^3b, b \mid a^4 = e = b^2, b^{-1}ab = a^{-1}\}$$

The set K as defined in the Cayley's theorem above is given by $K = \{f_x \mid x \in G\}$ where f_x is defined by $f_x(y) = xy$ and $G \cong K$ by the theorem. We determine K, which will be the required permutation group.

Now, $f_a(a) = a^2, \ f_a(a^2) = a^3, f_a(a^3) = a^4 = e, \ f_a(ab) = a^2b$

$$f_a(a^2b) = a^3b, \ f_a(a^3b) = b, f_a(b) = ab, \ f_a(e) = a$$

Thus f_a can be identified with the permutation (1234)(5678)

Again, $f_{a^2}(a) = a^3, \ f_{a^2}(a^2) = e, f_{a^2}(a^3) = a, \ f_{a^2}(ab) = a^3b$

$$f_{a^2}(a^2b) = b, \ f_{a^2}(a^2b) = ab, f_{a^2}(b) = a^2b, \ f_{a^2}(e) = a^2$$

and thus, f_{a^2} can be identified with (13)(24)(57)(68).

Continuing like this, we can say, f_{a^3} = (1432)(5876)

Again, $f_{ab}(a) = aba = b, \ f_{ab}(a^2) = aba^2 = a^3b$ etc., and we get

$$f_{ab} = (18)(27)(36)(45)$$

and similarly,

$$f_{a^2b} = (15)(28)(37)(46)$$
$$f_{a^3b} = (16)(25)(38)(47)$$
$$f_b = (17)(26)(35)(48)$$

and finally, therefore,

K = {(1234)(5678), (13)(24)(57)(68), (1432)(5876), I, (18)(27)(36)(45), (15)(28)(37)(46), (16)(25)(38)(47), (17)(26)(35)(48)}

which is the required permutation group that is isomorphic with the dihedral group of order 8.

Theorem 15: *Order of any permutation f in S_n is equal to the l.c.m. of the orders of the disjoint cycles of f.*

Proof: Let $f = f_1 f_2 \ldots f_n$

be the representation of f as product of disjoint cycles $f_1, f_2, \ldots, f_n$

Let $o(f_i) = r_i \quad i = 1, 2, \ldots, n$

then $f_i^{r_i} = I$ (identity of S_n)

Let $r = \text{l.c.m.}(r_1, r_2, \ldots, r_n)$

Now $f^r = (f_1 f_2 \ldots f_n)^r = f_1^r f_2^r \ldots f_n^r$ as f_i are disjoint and so commutative.

Since $r_i \mid r$ for all i, we have $r = r_i k_i, \quad i = 1, 2, \ldots, n$

Thus $f^r = f_1^{r_1 k_1} f_2^{r_2 k_2} \ldots f_n^{r_n k_n} = I \cdot I \ldots I = I$

Suppose now $f^t = I$

$$\Rightarrow (f_1 f_2 \ldots f_n)^t = I$$
$$\Rightarrow f_1^t f_2^t \ldots f_n^t = I$$
$$\Rightarrow f_1^t = f_2^t = \ldots = f_n^t = I$$

as $f_1, f_2, \ldots, f_n$ are disjoint. (Note if some $f_i^t \neq I$ then L.H.S. cannot be I).

$$\Rightarrow r_i \mid t \quad \text{for all } i$$
$$\Rightarrow r \mid t$$

Hence $r = o(f)$.

Example 8: Order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 1 & 3 \end{pmatrix} = (1245)(36)$$

is l.c.m.(4, 2) = 4 as $o(1245) = 4$ and $o(36) = 2$.

Problem 47: *Show that an odd permutation is of even order.*

Solution: Let σ be an odd permutation and suppose $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$ (as product of disjoint cycles). If $l = \text{l.c.m.}(o(\sigma_1), o(\sigma_2)), \ldots \sigma(\sigma_k))$ then $l = o(\sigma)$.

If each σ_i is of odd length then each σ_i is even permutation and thus σ is even permutation, which is not true.

Hence some cycle σ_j is of even length and $o(\sigma_j) =$ even

$\Rightarrow 2 | o(\sigma_j)$ and as $o(\sigma_j) | l$, we find $2 \mid l$ or that $l = o(\sigma)$ is even.

One may notice here that an even permutation need not be of odd order. Indeed (12)(34) is even permutation of order 2 whereas I is even permutation of order 1.

Problem 48: *Suppose $f = (123456)$. Show that we can write $f = gh$, where $o(g) = 2$, $o(h) = 3$.*

Solution: We have $o(f) = 6 = 2 \times 3$

Since g.c.d. (2, 3) = 1, $\exists$ integers x, y, s.t., $2x + 3y = 1$.

In fact $2(-1) + 3(1) = 1$

Now $f = f^1 = f^{2(-1)+3(1)} = f^{-2}.f^3 = f^3 \cdot f^{-2} = gh$ (say),

where $g = f^3$ and $o(g) = o(f^3) = 2$

as $f^3 = (14)(25)(36)$, $(f^3)^2 = f^6 = I$

Also $h = f^{-2}$ and $o(h) = o(f^{-2}) = o(f^2) = 3$

as $f^2 = (123456)(123456) = (135)(246)$

See Exercise 7 on page 97.

Theorem 16: *The set A_n of all even permutations of S_n ($n \geq 2$) is a normal subgroup of S_n and $o(A_n) = \frac{o(S_n)}{2}$ and index of A_n in S_n is 2.*

Proof: Since identity permutation is even, A_n is a non empty subset of S_n.

Again, $f, g \in A_n \Rightarrow f, g$ are even permutations
$\Rightarrow f, g^{-1}$ are even permutations
$\Rightarrow fog^{-1}$ is even
$\Rightarrow fog^{-1} \in A_n$

or that A_n is a subgroup of S_n.

If $f \in A_n$ and $g \in S_n$ be any members then g^{-1} *o* fog will be even permutation, showing that g^{-1} *o* $fog \in A_n$ or that A_n is a normal subgroup of S_n.

Let $G = \{1, -1\}$ be the group under multiplication.

Define a map $\varphi : S_n \to G$, s.t.,
$\varphi(f) = 1$ if f is even permutation
$= -1$ if f is odd permutation

then φ is an onto mapping as S_n ($n \geq 2$) must contain even as well as odd permutations. (Identity permutation and (12) will be in S_n). To show that φ is a homomorphism, let $f, g \in S_n$ be any members.

Case (*i*): Both f, g are even, then fog is even

$$\varphi(fog) = 1 = 1.1 = \varphi(f)\varphi(g)$$

Case (*ii*): Both f, g are odd, then fog is even

$$\varphi(fog) = 1 = (-1)(-1) = \varphi(f)\varphi(g)$$

Case (*iii*) : One of f, g is odd, other even.

Suppose f is odd and g is even, then fog is odd

$$\varphi(fog) = -1 = (-1)(1) = \varphi(f)\varphi(g)$$

hence φ is an onto homomorphism and thus by Fundamental theorem of homomorphism

$$G \equiv \frac{S_n}{\text{Ker } \varphi}$$

Since $f \in \text{Ker } \varphi \Leftrightarrow \varphi(f) = 1$

$\Leftrightarrow f$ is even $\Leftrightarrow f \in A_n$

we have $\text{Ker } \varphi = A_n$

or that $G \cong \dfrac{S_n}{A_n}$

But $o(G) = 2 \Rightarrow o\left(\dfrac{S_n}{A_n}\right) = 2$

$$\Rightarrow \frac{o(S_n)}{o(A_n)} = 2$$

$$\Rightarrow \frac{o(S_n)}{2} = o(A_n)$$

Also then index of A_n in S_n is 2.

Note: A_n is called the *alternating group* of degree n. Also it would be the largest subgroup of S_n in view of the Lagrange's theorem. See remark on page 70.

Problem 49: *Show that if H be any subgroup of* S_n ($n \geq 2$) *then either all permutations in H are even or exactly half are even.* (*See Problem* 13, *Chapter* 1 *also*).

Solution: Since H is a subgroup, it must contain the identity permutation which is even. So H cannot contain only odd permutations. If all members of H are even, we are done. Suppose it contains both odd as well as even permutations. Let $G = \{1, -1\}$ be the group under multiplication.

Define a map $\varphi : H \to G$, s.t.,

$\varphi(f) = 1$ if f is even

$= -1$ if f is odd

then as in above theorem, φ is an onto homomorphism. Also if K = set of all even permutations of H then $\text{Ker } \varphi = K$. By Fundamental theorem then

$$\frac{H}{\text{Ker } \varphi} \cong G \text{ or } \frac{H}{K} \cong G$$

$$\Rightarrow o\left(\frac{H}{K}\right) = o(G) = 2$$

$$\Rightarrow \frac{o(H)}{2} = o(K)$$

which proves the result.

Problem 50: Let *H be a subgroup of* S_n *such that H contains an odd permutation. Show that there exists a subgroup M of H with index 2 in H.*

Solution: Since $A_n \trianglelefteq S_n$ and $H \leq S_n$, $K = HA_n$ will be a subgroup of S_n.
Also $A_n \subseteq K \subseteq S_n$ implies that either $K = S_n$ or $K = A_n$ (A_n is largest, see note above). Also as

$H \subseteq HA_n = K$ and H has an odd permutation, K has an odd permutation and so $K \neq A_n$. Hence $K = S_n$.

Now $\dfrac{HA_n}{A_n} \cong \dfrac{H}{H \cap A_n}$ (Second theorem of isomorphism)

and as $HA_n = K = S_n$ we have $\dfrac{S_n}{A_n} \cong \dfrac{H}{H \cap A_n} \Rightarrow o\left(\dfrac{H}{H \cap A_n}\right) = o\left(\dfrac{S_n}{A_n}\right) = 2$

Take $M = H \cap A_n$ then index of M in H is 2.

Example 9: Consider $S_3 = \{I, (12), (13), (23), (123), (132)\}$

Let A_3 be the alternating group, then

$$A_3 = \{I, (123), (132)\}$$

$$o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2$$

In fact $\dfrac{S_3}{A_3} = \{A_3, A_3(12)\}$

Also as $A_3 = (A_3(12))^2$

$A_3(12) = (A_3(12))^1$

we find $\dfrac{S_3}{A_3}$ is a cyclic group generated by $A_3(12)$. Otherwise also a group of prime order is cyclic.

Since S_3 is not abelian, S_3 cannot be cyclic.

We recall the following results that we proved earlier

1. Quotient group of a cyclic group is cyclic.
2. Quotient group of an abelian group is abelian.
3. Homomorphic image of an abelian group is abelian.
4. Homomorphic image of a cyclic group is cyclic.

That the converse of all these results is not true follows by considering the above example. Notice, we have the natural onto homomorphism from $S_3 \to S_3/A_3$ and S_3/A_3 is abelian.

Problem 51: *Show that for* $n \geq 3$, *the subgroup generated by* 3*-cycles is* A_n.

Solution: Let H be a subgroup generated by 3-cycles, then every element of H is a product of finite number of 3-cycles and as each 3-cycle is even permutation, every element of H will be even permutation or that $H \subseteq A_n$. Again if $f \in A_n$ then f is product of even number of transpositions.

Since product of any two distinct transpositions can be written as a product of three cycles $[(ab)(cd) = (abc)(bcd), (ab)(bc) = (abc)]$ we find f can be expressed as a product of 3-cycles $\Rightarrow f \in H$ and hence $H = A_n$.

Problem 52: *If H is a subgroup of* S_n *with index 2 then show that* $H = A_n$. *Thus* A_n *is the only subgroup of index 2 in* S_n.

Solution: Since index of H in S_n is 2, H is normal in S_n and $o\left(\frac{S_n}{H}\right) = 2$.

If $H\sigma \in \frac{S_n}{H}$ be any element,

then $(H\sigma)^2 = H \Rightarrow H\sigma^2 = H \Rightarrow \sigma^2 \in H \; \forall \; \sigma \in S_n$

Suppose σ is a cycle of length 3, then

$\sigma^3 = I \Rightarrow \sigma^4 = \sigma$ and as $\sigma^2 \in H$,

We get $\sigma^4 \in H$, i.e., $\sigma \in H$.

Thus every cycle of length 3 is in H. But, A_n is generated by cycles of length 3 (see above problem).

Thus, $A_n \subseteq H$ or that $H = A_n$. See Note on page 148.

Problem 53: *Show that the smallest subgroup of S_n, containing* (12) *and* (1 2 3 ..... n) *is S_n.*

Solution: Let H be the smallest subgroup of S_n, containing (12) and (1 2 3 ..... n). We need show $S_n \subseteq H$.

If $f \in S_n$ be any element, then f can be expressed as a product of transpositions and as any transpositon $(ab) = (1a)(1b)(1a)$, f can be expressed as a product of transpositions of the type $(1x)$. We show all transpositions (12), (13), (14), ..., $(1n)$ are in H, which will imply that f is in H, as f is nothing but product of some such members.

Now $(1n) = (n\ n-1\ .....\ 321)(12)(123\ .....\ n) \in H$

$\Rightarrow$ $(n\ n{-}1) = (n\ n{-}1\ .....\ 321)(1n)(123\ .....\ n) \in H$

$(n{-}1\ n{-}2) = (n\ n{-}1\ .....\ 321)(n\ n{-}1)(123\ .....\ n) \in H$

and so on.

Showing that (43), (32) etc. are in H.

Now $(12) \in H$

$\Rightarrow$ $(13) = (12)(23)(12) \in H$

$\Rightarrow$ $(14) = (13)(34)(13) \in H$

.....

$(1n) \in H$

Hence $H = S_n$.

Problem 54: *Give an example of two subgroups H, K which are not normal, but HK is a subgroup.*

Solution: Let $H = \{I, (12)\}$

$K = \{I, (123), (132)\}$

be two subgroups of S_4 (that these are subgroups can be verified).

Here $HK = \{I, (12), (123), (132), (12)(123), (12)(132)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

$KH = \{I, (123), (132), (12), (123)(12), (132)(12)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

Thus $HK = KH \Rightarrow HK$ is a subgroup.

Now $H(123) = \{(123), (12)(123)\} = \{(123), (23)\}$

$(123)H = \{(123), (13)\}$

or that $H(123) \neq (123)H$

i.e., $Ha \neq aH$ for some $a \in S_4$

$\Rightarrow H$ is not normal in S_4.

Similarly one can check that $K(14) \neq (14)K$

or that K is not normal in S_4.

Problem 55: *Show that* $Z(S_n) = \{I\}$, $(n \geq 3)$.

Solution: Let $f \in Z(S_n)$ be such that $f \neq I$

then $\exists\ a$ s.t., $f(a) = b$ where $b \neq a$

Let $c \neq a, b$ be any element (note $n \geq 3$)

Let g be the mapping where $g(a) = a$

$g(b) = c$

$g(c) = b$

then $g \in S_n$

Now $(fg)a = f(g(a)) = f(a) = b$

$(gf)a = g(f(a)) = g(b) = c$

$\Rightarrow fg \neq gf$ *i.e.*, $f \notin Z(S_n)$

Thus if $f \neq I$ then it cannot belong to $Z(S_n)$ or that $Z(S_n) = \{I\}$.

Cor.: S_n is non abelian $\forall\ n \geq 3$. Note G is abelian iff $G = Z(G)$.

Problem 56 : *Let G be a group of order 2m, where m is add. Show that G has a subgroup of order m.*

Solution: Since G is of even order, it has an element a with order 2. Let $n = 2m = o(G)$.

Let $x \in G$. Define f_x: $G \to G$, s.t., $f_x(g) = xg$, then f_x is a permutation.

Let θ: $G \to A(G) = S_n$ be defined such that $\theta(x) = f_x$

Then θ is easily seen to be a homomorphism.

If $x \in$ Ker θ be any element, then

$\theta(x) = I$ i.e., $f_x = \mathrm{I}$

$\Rightarrow f_x(e) = I(e) \Rightarrow x = e$ or that Ker $\theta = \{\mathrm{e}\}$ and so θ is 1–1.

Hence $G \cong \theta(G) = H$, say. Then $H \leq S_n$

Now $a \in G$, and $\theta(a) = f_a$

and $(f_a)^2 = f_a f_a = f_{a^2} = f_e = I$ $\qquad (o(a) = 2)$

Thus $o(f_a) = 2 = o(a) = o(\theta(a))$ (See Problem 24 on page 120).

Now $f_a(x) = ax \neq x$ for any $x \in G$, as $a \neq e$.

Thus f_a doesn't fix any element of G.

Since $o(f_a) = 2$, f_a is product of disjoint transpositions and the number of transpositions in f_a is m which is odd.

Thus f_a is an odd permutation in $\theta(G) = H$.
So by problem 50 on Page 148, H has a subgroup M such that index of M in H is 2.

$$\text{i.e., } \frac{o(H)}{o(M)} = 2, \text{ But } o(H) = o(G) = 2m.$$

and thus $o(M) = m$.

Since M is a subgroup of H, it will be a subgroup of G and has order m.

Problem 57: *Show that in S_n the number of distinct cycles of length r is* $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$, $(r \leq n)$.

Solution: Since the number of distinct arrangements of r objects chosen out of n objects in ${}^nP_r = \frac{n!}{(n-r)!}$ and the cycles

$(a_1a_2 \ldots\ldots a_r)$, $(a_2a_3 \ldots\ldots a_ra_1)$, $(a_3a_4 \ldots\ldots a_ra_1a_2)$, ..., $(a_ra_1 \ldots\ldots a_{r-1})$

are same, we find the number of distinct r-cycles will be $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$.

Problem 58: *Show by an example that converse of Lagrange's theorem may not hold.*

Solution: Consider the alternating group A_4.

$$o(A_4) = \frac{o(S_4)}{2} = \frac{|4}{2} = 12$$

We show although $6 \mid 12$, A_4 has no subgroup of order 6. Suppose H is a subgroup of A_4 and $o(H) = 6$.

By previous problem the number of distinct 3-cycles in S_4 is

$$\frac{1}{3} \cdot \frac{4!}{(4-3)!} = \frac{4.3.2.1}{3.1} = 8.$$

Again, as each 3-cycle will be even permutation all these 3-cycles are in A_4.

Obviously then, at least one 3-cycle, say σ, does not belong to H (o(H) = 6).

Now $\sigma \notin H \Rightarrow \sigma^2 \notin H$, because if $\sigma^2 \in H$

then $\sigma^4 \in H$

$\Rightarrow \sigma \in H$

as $\sigma^3 = I$ as $o(\sigma) = 3$.

Let $K = <\sigma> = \{I, \sigma, \sigma^2\}$ then $o(K) = 3$ $(= o(\sigma))$

and $H \cap K = \{I\}$ $(\sigma, \sigma^2 \notin H)$

$\Rightarrow o(HK) = \dfrac{o(H).o(K)}{o(H \cap K)} = \dfrac{6.3}{1} = 18$, not possible as $HK \subseteq A_4$ and $o(A_4) = 12$.

Problem 59: *Show that A_4 is the only subgroup of order 12 in S_4.*

Solution: Let H be any subgroup of order 12 in S_4. Let $H \neq A_4$.

Then H contains an odd permutation.

Thus H has 6 odd and 6 even permutations.

$\Rightarrow H \cap A_4$ is a subgroup of A_4 of order 6

$\Rightarrow A_4$ has subgroup of order 6

But that is not possible by above problem. Hence the result.

Problem 60 : *Let G be a group and $H = \{g^2 \mid g \in G\}$. Show that H may not be a subgroup of G and in case it is a subgroup then it must be normal.*

Solution: For the first part, suppose $G = A_4$ then A_4 contains all the twelve even permutations of S_4, which are I, (12)(34), (13)(24), (14)(23) and the 8 3-cycles (See Problem 58 above). Since $I^2 = I$, $((ab)(cd))^2 = I$ and square of any 3-cycle is a 3-cycle we notice H will contain I and the 8 3-cycles or that $o(H) = 9$ and as $9 \nmid 12$, H cannot be a subgroup. Suppose now, H is a subgroup then if $h \in H$, $g \in G$ be any elements, then

$$g^{-1} \in G \Rightarrow g^{-2} \in H, \text{ also } gh \in G \Rightarrow (gh)^2 \in H$$

$\Rightarrow g^{-2}(gh)(gh) \in H \Rightarrow g^{-1}hg \in H$ or that H is normal in G.

Remark: One may notice here that if G happens to be abelian, then H will be a subgroup.

Problem 61: *Show that* (123) *is not the cube of any member of S_n.*

Solution: We first show that if $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)$ is any cycle

then $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^3 = (\alpha_1\ \alpha_4\ \alpha_7)\ (\alpha_2\ \alpha_5\ \alpha_8)\ (\alpha_3\ \alpha_6\ \alpha_9)$

Since $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^2 = (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)\ (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)$

$= (\alpha_1\ \alpha_3\ \alpha_5\ \alpha_7\ \alpha_9\ \alpha_2\ \alpha_4\ \alpha_6\ \alpha_8)$

$(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^3 = (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)\ (\alpha_1\ \alpha_3\ \alpha_5\ \alpha_7\ \alpha_9\ \alpha_2\ \alpha_4\ \alpha_6\ \alpha_8)$

$= (\alpha_1\ \alpha_4\ \alpha_7)\ (\alpha_2\ \alpha_5\ \alpha_8)\ (\alpha_3\ \alpha_6\ \alpha_9)$

Suppose now (1 2 3) $= \alpha^3$ for some $\alpha \in S_n$, then as α can be expressed as product of disjoint cycles

Let $\alpha = \sigma_1\ \sigma_2 \ldots\ldots\ \sigma_k$ where σ_i are disjoint cycles

Then $\alpha^3 = \alpha_1^3\ \alpha_2^3 \ldots\ldots\ \alpha_k^3$ (as disjoint cycles commute)

Also $\alpha^3 = (123)$

$\Rightarrow \alpha^9 = (123)^3 = I \Rightarrow o(\alpha) = 9$

thus each σ_i will be of length 3 or 9 as order of a permutation is the l.c.m. of the orders (lengths) of its disjoint cycles.

Again there is at least one σ_i whose length is 9 otherwise if all have length 3 then l.c.m. will be 3 implying $o(\alpha) = 3$ which is not true.

Without loss of generality take length of σ_i to be 9.

Now if length of any σ_i is 3 then $\sigma_i^3 = I$.

So $\alpha^3 = (123) = \sigma_1^3\ \sigma_2^3\ .....\ \sigma_k^3$

$= \sigma_1^3 \times$ other cubes of cycles of length 9

Let $\sigma_1 = (\alpha_1\ \alpha_2.....\alpha_9)$

$\Rightarrow \sigma_1^3 = (\alpha_1\ \alpha_4\ \alpha_7)(\alpha_2\ \alpha_5\ \alpha_8)(\alpha_3\ \alpha_6\ \alpha_9)$

$\Rightarrow (123) = (\alpha_1\ \alpha_4\ \alpha_7)(\alpha_2\ \alpha_5\ \alpha_8)(\alpha_3\ \alpha_6\ \alpha_9) \times$ other cycles which do not contain $\alpha_1, \alpha_2....., \alpha_9$

(as all are disjoint) which will be a contradiction as each α_i is different and so if $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 3$ then α_4 is such that it is fixed in L.H.S. but in R.H.S. $\alpha_4 \to \alpha_7$. Hence the result.

Example 10: Consider $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

Let us denote these elements by e, x, y, z then the following table gives us the respective products

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

which also shows that closure holds in K_4 and thus K_4 forms a group. It is called **Klein's four group** which is a subgroup of S_4. It is a finite abelian group, which is not cyclic (as it contains no element of order 4 = $o(K_4)$).

Remarks: (*i*) We could also take the elements e, x, y, z to be the matrices $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ under matrix multiplication.

(*ii*) We may further notice that any non cyclic abelian group of order 4 is of the type $G = \{e, a, b, ab\}$. Here each element (except e) will have order 2. [$x \in G \Rightarrow o(x) \mid o(G) \Rightarrow o(x) = 1$, 2 or 4. But $o(x) = 4$ gives $x^4 = e$ and then G will be cyclic].

Thus $o(a) = o(b) = o(ab) = 2$

i.e., $a^2 = b^2 = (ab)^2 = e$

Clearly this group G is isomorphic to the Klein's four group [$e \to I$, $a \to (12)\ (34)$, $b \to (13)(24)$, $ab \to (14)(23)$]. Hence every non cyclic (abelian) group of order 4 is isomorphic to the Klein's four group.

Problem 62: *Given that order of any element of A_4 is 1, 2 or 3 show that $o(Z(A_4)) = 1$.*

Solution: We show $Z(A_4)$ has no element of order 2 or 3.

Suppose $a \in Z(A_4)$ s.t., $o(a) = 2$.

Let $b \in A_4$ be any element of order 3, then as $ab = ba$ (a is in centre).

$(o(a), o(b)) = 1$, we find $o(ab) = o(a).o(b) = 2 \times 3 = 6$.

which is not possible by given condition. So, $Z(A_4)$ has no element of order 2.

Similarly it has no element of order 3. So it can only contain I.

Problem 63: *Show by an example that we can find three groups $E \subseteq F \subseteq G$ such that E is normal in F, F is normal in G whereas E is not normal in G.*

Solution: Let $E = \{I, (12)(34)\}$

$F = K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

$G = A_4$

then E is not normal in G as

$E(123) = \{I\ (123), (12)(34)(123)\} = \{(123), (243)\}$

$(123)E = \{(123)\ I, (123)(12)(34)\} = \{(123), (134)\}$

Showing that $E(123) \neq (123)E$ $\quad (123) \in A_4 = G$.

E would be normal in F as index of E in F is 2. Otherwise also as F is abelian, E will be normal in F.

Also F is normal in G as

Let $\theta \in A_4$ and $(ab)(cd) \in K_4$ be any element.

(a, b, c, d being any of 1, 2, 3, 4)

then $\theta(ab)(cd)\theta^{-1} = (\theta(a)\ \theta(b))\ (\theta(c)\ \theta(d)) \in K_4$ as all permutations with this cycle structure are in K_4.

$\Rightarrow K_4$ is normal in A_4.

Note that all elements in K_4 are even permutations and so belong to A_4.

See Problem 6 on page 103 for another example.

Orbits and Stabilizers

Definition: Let G be any group of permutations on a set S. For any $a \in S$, Stabilizer of a is defined to be the set

$$\text{stab}(a) = \{f \in G \mid f(a) = a\}$$

i.e., those maps in G, which fix a.

It is easy to see that stab(a) forms a subgroup of G.

$$\text{stab}(a) \neq \varphi \text{ as } I \in \text{stab}(a)$$

$f, g \in \text{stab}(a) \Rightarrow f(a) = a,\ g(a) = a$

$\therefore fg^{-1}(a) = f(g^{-1}(a)) = f(a) = a \Rightarrow fg^{-1} \in \text{stab}(a)$

Again for any $a \in G$, orbit (a) is defined to be the set $\{x \in S \mid x = f(a)$ for some $f \in G\}$ $= \{f(a) \mid f \in G\}$.

So it is a subset of S containing images of a in S.

Example 11: Suppose G = {I, (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)}

then $\text{stab}(1) = \{I, (24)(56)\}$

$\text{stab}(4) = \{I, (56)(13)\}$

$\text{stab}(5) = \{I, (12)(34), (13)(24), (14)(23)\}$

orb(1) = {1, 2, 3, 4}

orb(3) = {3, 4, 1, 2}

Theorem 17 (Orbit-stabilizer): *Let G be a finite group of permutations of a set S. Then for any $a \in S$,*

$o(G) = o(orbit(a)) \times o(stab\ (a))$

Proof: Since stab(a) $\leq G$

$$\frac{o(G)}{o(\text{stab}(a))} = \text{Index of stab}(a) \text{ in } G.$$

= Number of left cosets of stab(a) in G

Let H = stab(a) and let G/H denote the set of all left cosets of H in G.

Define φ : orb(a) $\to G/H$ s.t.,

$\varphi\ (\sigma(a)) = \sigma H$

Then $\varphi\ (\sigma(a)) = \sigma(\eta(a))$

$\Leftrightarrow \sigma H = \eta\ H \Leftrightarrow \sigma^{-1}\eta \in H$

$\Leftrightarrow \sigma^{-1}\eta(a) = a$ (def. of stab.)

$\Leftrightarrow \eta(a) = \sigma(a)$

i.e., φ is well defined 1–1

Again for any $\sigma H \in G/H$, $\sigma(a)$ is the required pre-image $\Rightarrow \varphi$ is onto

Thus o(orb(a)) = $o(G/H)$ = No. of distinct left cosets of H in G.

= Index of H in G

$$= \frac{o(G)}{o(H)}$$

Giving the required result.

Note: G/H here is only a notation and not essentially a quotient group.

Theorem 18: (Generalised Cayley's theorem): *Let H be a subgroup of G and $\mathcal{L} = \{aH \mid a \in G\}$ then $\exists$ a homomorphism $\theta : G \to A(\mathcal{L})$ s.t., Ker θ is the largest normal subgroup of G contained in H.*

Proof: Define $\theta : G \to A(\mathcal{L})$ s.t.,

$\theta(g) = f_g$

where $f_g : \mathcal{L} \to \mathcal{L}$ s.t.

$f_g\ (aH) = gaH$

To show that θ is well defined, we need prove that $f_g \in A(\mathcal{L})$

Now $f_g(aH) = f_g(bH)$

$\Rightarrow\ gaH = gbH$

$\Rightarrow\ aH = bH \quad \Rightarrow f_g$ is 1-1

Again for any $aH \in \mathcal{L}$,

$f_g(g^{-1}aH) = aH$, showing that

f_g is onto and thus $f_g \in A(\mathcal{L})$

We have $\theta(gh) = f_{gh},\ \theta(g)\theta(h) = f_g f_h$

and since $f_{gh}(aH) = ghaH$

$f_g f_h(aH) = f_g(f_h(aH)) = f_g(haH) = ghaH$

we find $f_{gh} = f_g f_h$

or that θ is a homomorphism.

Since Kernel of a homomorphism is normal subgroup, we have Ker θ, a normal subgroup of G.

Again, if $g \in$ Ker θ then

$$\theta(g) = I = \text{Identity of } A(\mathcal{L})$$
$$\Rightarrow f_g = I$$
$$\Rightarrow f_g(aH) = aH \quad \forall\ aH \in \mathcal{L}$$

In particular,

$$f_g(eH) = eH \Rightarrow geH = eH \Rightarrow gH = H$$
$$\Rightarrow g \in H$$
$$\Rightarrow \text{Ker } \theta \subseteq H$$

Let now K be any normal subgroup of G, contained in H. Let $k \in K$ be any element. We want to show that $k \in$ Ker θ or that $\theta(k) = I$.

or that $f_k = I$

or that $f_k(aH) = aH \quad \forall\ aH$

Now $f_k(aH) = kaH = a(a^{-1}ka)\ H = ahH = aH$

[Note $a^{-1}ka \in K \subseteq H$]

Hence $K \subseteq$ Ker θ which proves the theorem.

Remarks: (*i*) If we wish to work with right cosets, θ can be defined by $\theta(g) = f_g$ where $f_g(Ha) = Hag^{-1}$.

(*ii*) If $H = \{e\}$, the above theorem is the Cayley's theorem, as then Ker$\theta = \{e\} \Rightarrow \theta$ is 1–1.

Cor. (Index theorem): If $H \neq G$ is a subgroup of a finite group G, s.t., $o(G)$ does not divide $i_G(H)!$ then G has a non trivial normal subgroup. (*i.e.*, G is not simple).

Proof: By above theorem, we find Ker θ is a normal subgroup of G.

Since Ker $\theta \subseteq H \neq G$, Ker $\theta \neq G$

If Ker $\theta = \{e\}$, then θ is 1-1 and thus $\theta : G \to A(\mathcal{L})$ is 1-1 homomorphism *i.e.*, G is isomorphic to a subgroup T of $A(\mathcal{L})$.

$$\Rightarrow o(G) = o(T)$$

But $o(T) \mid o(A(\mathcal{L})) \Rightarrow o(G) \mid o(A(\mathcal{L})) = i_G(H)!$ a contradiction and so Ker $\theta \neq \{e\}$ and is the required non trival normal subgroup.

Problem 64: *Let H be a subgroup of a finite group G such that o(H) and* $(i_G(H)-1)!$ *are coprime then show that H is normal in G.*

Solution: Let $S = \{aH \mid a \in G\}$ = Set of left cosets of H in G.

Define $\theta : G \to A(S)$ s.t.,

$\theta(g) = T_g$

where $T_g : S \to S$ s.t., $T_g(aH) = gaH$

Then as seen in generalised Cayley's theorem, θ is a homomorphism and Ker $\theta \subseteq H$.

Also then $\frac{G}{\text{Ker}\theta} \cong T$ where $T \leq A(S)$

$\Rightarrow o(G/\text{Ker } \theta) = o(T)$ where $o(T) \mid o(A(S)) = \underline{\mid i_G(H)}$

Let $i_G(H) = \frac{o(G)}{o(H)} = n$

then $o(T) \mid \underline{\mid n}$ and thus $\frac{o(G)}{o(\text{Ker}\theta)} \mid \underline{\mid n}$

Again Ker $\theta \leq H \Rightarrow o(\text{Ker } \theta) \mid o(H)$

$\Rightarrow o(H) = m.o(\text{Ker } \theta)$ for some m

$\Rightarrow \frac{o(G)}{n} = m.o(\text{Ker } \theta)$

$\Rightarrow nm = \frac{o(G)}{o(\text{Ker}\,\theta)}$

or that $nm \mid \underline{\mid n} \Rightarrow nm \mid n.\underline{\mid n-1} \Rightarrow m \mid \underline{\mid n-1}$

Also $m \mid o(H)$ and as they are coprime, $m = 1$ or that $H = \text{Ker } \theta$ i.e., $H \trianglelefteq G$.

Problem 65: *Suppose that G is a finite group and p is the smallest prime divisor of o(G). Show that a subgroup H of index p in G is normal in G.*

Solution: Let $\mathscr{S}$ = set of all left cosets of H in G.

Then $o(\mathscr{S}) = p$

Define $\theta : G \to A(\mathscr{S})$ s.t.,

$\theta(g) = T_g$

where $T_g : \mathscr{S} \to \mathscr{S}$ s.t.,

$T_g(xH) = gxH$

Then θ is a homomorphism s.t. Ker $\theta \subseteq H$.

Let Ker $\theta = K$ then $K \subseteq H$ and K is normal in G.

$\frac{G}{K}$ is isomorphic to a subgroup of $A(\mathscr{S}) = S_p$ (Using Fundamental theorem)

$\therefore\ o\left(\frac{G}{K}\right)$ divides $p!$

If $m \mid o\left(\frac{G}{K}\right)$ then $m \mid o(G)$ [as $o(G) = o(K)\ [G : K]$].

Since p is the smallest prime dividing $o(G)$, $m = 1$ or p.

$\therefore \; o\left(\frac{G}{K}\right)$ is divisible by 1 or p only.

$$\Rightarrow \; o\left(\frac{G}{K}\right) = 1 \text{ or } p$$

But $o(G/K) = [G : K] = [G : H]\,[H : K]$

$$= p[H : K]$$

$$\geq p$$

$\therefore \quad o\left(\frac{G}{K}\right) = p \Rightarrow [H : K] = 1$

$$\Rightarrow H = K$$

$$\Rightarrow H = \text{Ker } \theta \text{ is normal in } G.$$

Remark: The result that a subgroup of index 2 is normal now follows from this problem also.

Exercises

1. In S_3, show that we can find elements, a, b s.t., $(ab)^2 \neq a^2b^2$. Also show that there exist four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.

2. Find order of all elements in S_3 and list all its subgroups.

3. Show that S_4 has no element of order greater than 4.

4. Using Index theorem show that if a group G of order 35 has a subgroup H of order 7 then H is normal in G.

5. Let $H = \{I, (123), (132)\}$, $K = \{I, (12)\}$ be two subgroups of S_3. Write all the left and right cosets of H and K in S_3. Hence show that H is normal whereas K is not normal in S_3.

6. Verifty Cayley's theorem for (i) a cyclic group of order 3.

(ii) $G = \{1, -1, i, -i\}$.

7. In S_5, show that we can find elements a, b s.t., $o(a) = o(b) = 3$ and $o(ab) = 5$.

[Take $a = (123)$, $b = (145)$]

8. Let $\sigma = (1234)$ be a 4 cycle. Show that σ^k is also a 4-cycle iff k and 4 are co-prime. Generalise!

9. Show that product of two transpositions is either (i) the identity or (ii) a 3-cycle or (iii) a product of two 3-cycles. (See problem 51).

10. Show that A_8 contains an element of order 15. [Note (123), (45678) are even permutations].

11. Show that $\frac{S_4}{K_4} = \{K_4, K_4(12), K_4(13), K_4(23), K_4(123), K_4(132)\}$

[**Hint:** $K_4(14) = K_4(23)$ as $(14)(23) \in K_4$, $K_4(124) = K_4(132)$ as $(124)(123) = (14)(23) \in K_4$ etc.]

Generators of a Subgroup

Let S be a non empty subset of a group G. Let

$H = \{x_1x_2 \ldots\ldots x_n \mid n$ is finite but not fixed, x_i or $x_i^{-1} \in S\}$

then H is a subgroup of G and contains S. $S \neq \varphi \Rightarrow H \neq \varphi$

Again, $x, y \in H \Rightarrow x = x_1 x_2 \ldots\ldots x_n \quad x_i$ or $x_i^{-1} \in S$

$y = y_1 y_2 \ldots\ldots y_m \quad y_j$ or $y_j^{-1} \in S$

$\Rightarrow \quad xy^{-1} = x_1x_2 \ldots\ldots x_n \cdot y_m^{-1} y_{m-1}^{-1} \ldots\ldots y_2^{-1} \cdot y_1^{-1} \in H$

Showing that H is a subgroup of G.

$S \subseteq H$ follows by definition of H.

This subgroup H is called the subgroup of G, generated by S and we write $H = < S >$.

Indeed if $S = \{a\}$, $H = < a >$ the subgroup we've been talking about earlier.

Theorem 19: *$H = < S >$ is the smallest subgroup of G containing S.*

Proof: Suppose K is a subgroup of G containing S

$x \in H \Rightarrow x = x_1x_2 \ldots\ldots x_n, \quad x_i$ or $x_i^{-1} \in S$

if $x_i \in S$ then $x_i \in K$ as $S \subseteq K$

if $x_i^{-1} \in S$ then $x_i^{-1} \in K \Rightarrow x_i \in K$ (as K is a subgroup)

i.e, $x_i \in K$ for all i

$\Rightarrow \quad x \in K \Rightarrow H \subseteq K$

or that H is the smallest subgroup containing S.

Remark: (*i*) $H = < S >$ will be the intersection of all subgroups of G containing S.

(*ii*) We use the notation $< a, b >$ to denote the subgroup generated by a, b.

Problem 66: Show that $< a, b > = < a, ab >$

Solution: We have

$a, ab \in < a, ab >$

$\Rightarrow a^{-1} ab \in < a, ab >$

$\Rightarrow b \in < a, ab >$

So, $a, b \in < a, ab >$ and as $< a, b >$ is the smallest subgroup generated by a, b,

we get, $< a, b > \subseteq < a, ab >$

Again, $a, b \in < a, b > \Rightarrow a, ab \in < a, b >$

and so $< a, ab > \subseteq < a, b >$

giving us the desired result.

Example 12: Let $G = S_3, \quad S = \{(12), (13)\}$

$(13)(12) = (231) = (123) \in H$

$(12)(13) = (132) \in H$

$(12)(123) = (23) \in H$

$(12)(12) = I \in H$

we find all members of S_3 are in $H = < S >$

i.e., $< S > = S_3$.

Note (12), (13) $\in S \subseteq H$.

Problem 67: *Show that* $S_4 = <(123), (24)>$

Solution: Let $G = <(123), (24)>$

Now $(24)^{-1}(123)(24) = (143)$ is in G.

Let $H = <(123)>$, $K = <(143)>$. Then $o(HK) = 9$ and $HK \subseteq G \Rightarrow o(G) \geq 9 \Rightarrow o(G) = 12$ or 24.

If $o(G) = 12$, then index of G in S_4 is 2, but A_4 is the only subgroup of index 2 in S_4 and as G contains an odd permutation, $G \neq A_4$. Thus $o(G) \neq 12 \Rightarrow o(G) = 24$ and hence $G = S_4$.

Remark: In fact $S_4 = <(ab), (acd)>$ i.e., it is generated by a transposition and a 3-cycle having one common letter with the transposition.

Problem 68: *Show that* $S_5 = <(1234), (2345)>$

Solution: Let $G = <(1234), (2345)>$

Let $H = <(1234)> = \{(1234), (13)(24), (1432), I\}$

$K = <(2345)> = \{(2345), (24)(35), (2543), I\}$

Then $o(HK) = 16$ and $HK \subseteq G$.

So, $o(G) \geq 16$.

But G is a subgroup of S_5.

Therefore, $o(G) = 20, 24, 30, 40, 60$ or 120

If $o(G) = 60$, then $G = A_5$ as only subgroup of S_5 of index 2 is A_5. But G contains odd permutations. So, G cannot be A_5. Therefore, $o(G) \neq 60$.

If $o(G) = 30$, then index of G in S_5 is 4.

So, there exists a homomorphism $\theta : S_5 \to A(S)$

where S is the set of all left cosets of G in A_5

such that Ker $\theta \neq \{I\}$ and Ker $\theta \subseteq G$.

Therefore, $o(\text{Ker } \theta) \leq 30$. Also Ker θ is a normal subgroup of S_5. Since A_5 is the only normal subgroup of S_5, this case is not possible.

So, $o(G)$ cannot be 30. Similarly, $o(G)$ cannot be 40.

Now G has an orbit of order 5. So, 5 divides $o(G)$.

Therefore, $o(G)$ cannot be 24.

Again, (13)(24)(24)(35) = (13)(35) = (351) is in G.

So, 3 divides $o(G)$. Therefore, $o(G)$ can not be 20. Hence, $o(G) = 120$. Thus, $G = S_5$.

Problem 69: *Show that every finitely generated subgroup of* $< \mathbf{Q}, + >$ *is cyclic. Hence show that* $< \mathbf{Q}, + >$ *is not finitely generated.*

Solution: Let H be a subgroup of $< \mathbf{Q}, + >$ such that H is generated by

$$\left\{\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots\ldots, \frac{m_r}{n_r}\right\}$$

Let g.c.d. $(m_1 n_2 \ldots n_r, m_2 n_1 n_3 \ldots nr, \ldots, m_r n_1 \ldots n_{r-1}) = d$

Then there exist integers $a_1, a_2 \ldots, a_r$ such that

$a_1 m_1 n_2 \ldots n_r + a_2 m_2 n_1 n_3 \ldots n_r + \ldots + a_r m_r n_1 \ldots n_{r-1} = d$

So, $a_1 \frac{m_1}{n_1} + a_2 \frac{m_2}{n_2} + \cdots a_r \frac{m_r}{n_r} = \frac{d}{n_1 n_2 \cdots n_r}$.

Since $\frac{m_1}{n_1}, \frac{m_2}{n_2}, \cdots, \frac{m_r}{n_r} \in H$, $\frac{d}{n_1 n_2 \cdots n_r} \in H$

We show that $H = \left\langle \frac{d}{n_1 n_2 \cdots n_r} \right\rangle$.

Let $x \in H$.

Then $x = \alpha_1 \frac{m_1}{n_1} + \alpha_2 \frac{m_2}{n_2} + \ldots + \alpha_r \frac{m_r}{n_r}$

$$= \frac{\alpha_1 m_1 n_2 \cdots n_r + \cdots + \alpha_r m_r n_1 n_2 \cdots n_{r-1}}{n_1 n_2 \cdots n_r}$$

$$= \frac{\alpha_1 du_1 + \alpha_2 du_2 + \cdots + \alpha_r du_r}{n_1 n_2 \cdots n_r}$$

$$= (\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r) \frac{d}{n_1 n_2 \cdots n_r}$$

So, $H = \left\langle \frac{d}{n_1 n_2 \ldots\ldots n_r} \right\rangle$.

Therefore, H is cyclic

If we take $H = \mathbf{Q}$ then $< \mathbf{Q}, + >$ is cyclic which is not true (See remark on page 82).

Hence $< \mathbf{Q}, + >$ is not finitely generated.

Problem 70: *Let* $H = \left\langle \frac{2}{3}, \frac{5}{7} \right\rangle$. *Show that* $H = \left\langle \frac{1}{21} \right\rangle$.

Solution: By above problem g.c.d. (14,15) =1 implies $H = \left\langle \frac{1}{21} \right\rangle$.

Problem 71: *Let* $n > 1$ *be an integer. Prove by induction that* S_n *is generated by the set* $\{(12), (13) \ldots, (1n)\}$.

Solution: Let $n = 2$. Then $S_2 = \{I, (12)\}$. So, S_2 is generated by $\{(12)\}$. Therefore, the result

is ture for $n = 2$. Let $n > 2$. Suppose the result is true for premutation groups on $n-1$ letters.

Consider $G = S_n$. Let $H = \{\sigma \in S_n | \sigma(n) = n\}$. Then H is a subgroup of G. Also, H is a group of permutations on $n-1$ letters, 1, 2,..., $n-1$. By induction hypothesis, H is generated by $\{(12), (13), ..., (1\ n-1)\}$

Let $K = \langle(123...n)\rangle$

Now $(123...n) = (1n)(1n-1)\ ...(12)$

Also, $H \cap K = \{I\}$.

So, $G = HK$ as $o(H) = n-1!$ and $o(K) = n$.

If $f \in G$, then $f = hk$, $h \in H$, $k \in K$.

Since h is product of transpositions (12),(13),...,(1n–1), k is product of transpositions (12),(13),...,(1n), f is product of transpositions (12)(13)...(1n).

Therefore, S_n is generated by $\{(12), (13),...,(1n)\}$

Problem 72: *Show that the dihedral group of order 8 is generated by* $\{(1234), (14)(23)\}$.
Solution: Let G be the dihedral group of order 8.

Then $G = \{a, a^2, a^3, a^4 = e, ab, a^2b, a^3b, b \mid b^{-1}ab = a^{-1}, a^4 = e = b^2\}$

Let $a = (1234)$, $b = (14)(23)$.

Then $a^4 = e = b^2$

Also $b^{-1}ab = bab^{-1} = b(1234)b^{-1} = (b(1)b(2)b(3)b(4)) = (4321) = a^{-1}$.

$ab = (1234)(14)(23) = (1)(24)(3)$

$a^2b = (13)(24)(14)(23) = (12)(34)$

$a^3b = (1432)(14)(23) = (13)$

So, $G = \{(1234), (13)(24), (1432), I, (24), (12)(34), (13), (14)(23)\}$

$= \langle(1234), (14)(23)\rangle$

Commutators

Let $a, b \in G$, G a group. Then $a^{-1}\ b^{-1}\ ab$ is called a *commutator* of a and b, or simply a commutator in G. Let S denote the set of all commutators in G and let G' denote the subgroup of G generated by S then G' is called *commutator* subgroup of G or *derived group* of G.

Theorem 20: *Let G' be the commutator subgroup of a group G then*

(*i*) *G' is normal in G.*

(*ii*) $\frac{G}{G'}$ *is abelian and*

(*iii*) *G' is the smallest subgroup of G such that* $\frac{G}{G'}$ *is abelian.*

(*iv*) *If $H \leq G$,* s.t. $G' \subseteq H$, then $H \trianglelefteq G$.

Proof: Let $g \in G$, $x \in G'$

$x \in G' \quad \Rightarrow x = c_1 \ldots\ldots c_n$ c_i or $c_i^{-1} \in S$ = Set of commutators

$c_i \in S \quad \Rightarrow c_i$ is a commutator

$\Rightarrow c_i = a_i^{-1}\, b_i^{-1}\, a_i b_i$ for some $a_i, b_i \in G$

$c_i^{-1} \in S \quad \Rightarrow c_i^{-1}$ is a commutator

$\Rightarrow c_i^{-1} = \alpha_i^{-1}\, \beta_i^{-1}\, \alpha_i \beta_i$ for some $\alpha_i, \beta_i \in G$

$\Rightarrow c_i = \beta_i^{-1}\, \alpha_i^{-1}\, \beta_i\, \alpha_i$

$\Rightarrow c_i$ is a commutator

$\therefore$ for each i, c_i is a commutator.

Now, $g^{-1}xg = g^{-1}(c_1 \ldots\ldots c_n)g$

$= (g^{-1}c_1 g)\,(g^{-1}c_2 g) \ldots\ldots (g^{-1}c_n g)$

but $g^{-1}c_i g = g^{-1}(a_i^{-1}\, b_i^{-1}\, a_i\, b_i)g$

$= (g^{-1}a_i g)^{-1}(g^{-1}\, b_i g)^{-1}(g^{-1}a_i g)(g^{-1}\, b_i g)$

$= \alpha_i^{-1}\, \beta_i^{-1}\, \alpha_i\, \beta_i$ where $\alpha_i = g^{-1}\, a_i g$, $\beta_i = g^{-1}\, b_i g$

$\therefore \quad g^{-1}c_i g \in S$ for all i

$\therefore \quad g^{-1}xg \in G'$

So, G' is a normal subgroup of G.

Consider $G'x\ G'y$. Then

$G'x\ G'y = G'y\ G'x$

$\Leftrightarrow \quad G'xy = G'yx$

$\Leftrightarrow \quad (xy)(yx)^{-1} \in G'$

$\Leftrightarrow \quad xyx^{-1}y^{-1} \in G'$

which is true as G' contains all commutators of G.

$\therefore \ \dfrac{G}{G'}$ is abelian.

Suppose $\dfrac{G}{K}$ is abelian. We show that $G' \subseteq K$.

Since $\dfrac{G}{K}$ is abelian,

$Kx\ Ky = Ky\ Kx$ for all $x, y \in G$

$\Leftrightarrow \quad Kxy = Kyx$ for all $x, y \in G$

$\Leftrightarrow \quad xyx^{-1}\, y^{-1} \in K$ for all $x, y \in G$

$\Rightarrow K$ contains S, the set of all commutators of G.

But G' is the smallest subgroup of G containing S.

$\therefore \quad G' \subseteq K$.

Finally, for part (*iv*) , if $g \in G$, $h \in H$ be any elements, then $h^{-1}g^{-1}hg \in G' \Rightarrow h^{-1}g^{-1}hg \in H$ $\Rightarrow g^{-1}hg \in hH = H \Rightarrow H \trianglelefteq G$.

Cor.: G is abelian $\Leftrightarrow\ G' = \{e\}$.

Proof: Let G be abelian. Let $K = \{e\}$

Then $\frac{G}{K} = \frac{G}{\{e\}}$ is abelian.

$\therefore$ $G' \subseteq K = \{e\}$, but $\{e\} = K \subseteq G'$

$\therefore$ $G' = \{e\}$.

Alternatively, if G is abelian

then $a^{-1}\, b^{-1}\, ab = e \quad \forall\ a, b$

$\therefore$ $S = \{e\} \Rightarrow G' = \{e\}$ as G' is the smallest group containing S.

Conversely, let $G' = \{e\}$. Now $\frac{G}{G'}$ is abelian $\Rightarrow$ $\frac{G}{\{e\}}$ is abelian.

But $\frac{G}{\{e\}} \cong G \Rightarrow G$ is abelian.

Or, otherwise, if $a, b \in G$ be any elements then as $a^{-1}b^{-1}ab \in G' = \{e\}$

$\Rightarrow a^{-1}b^{-1}ab = e \Rightarrow ab = ba.$

Problem 73: *For $G = S_3$, prove that $G' = A_3$.*

Solution: $o(G')$ divides $o(G) = 6$

$\Rightarrow$ $o(G') = 1, 2, 3$ or 6

$o(G') = 1 \Rightarrow G' = \{I\} \Rightarrow G$ is abelian, a contradiction.

$o(G') = 6 = o(G) \Rightarrow G' = G$. But $\frac{G}{A_3}$ is abelian being of order 2

$\therefore\ G' \subseteq A_3 \Rightarrow G \subseteq A_3$ a contradiction.

If $o(G') = 2$, then $\frac{G}{A_3}$ is abelian

$\Rightarrow$ $G' \subseteq A_3 \Rightarrow o(G') = 2$ divides $o(A_3) = 3$, a contradiction.

$\therefore$ $o(G') = 3$

But A_3 is only subgroup of order 3 in S_3.

$\therefore$ $G' = A_3$.

Problem 74: *If N is a normal subgroup of G and $N \cap G' = \{e\}$, show that $N \subseteq Z(G)$.*

Solution: Let $n \in N, x \in G$

Then $x^{-1}\, n^{-1}\, xn \in G'$

But $x^{-1}\, n^{-1}\, xn = (x^{-1}\, n^{-1}\, x)\, n \in N$ as N is a normal subgroup of G.

$\therefore$ $x^{-1}\, n^{-1}\, xn \in G' \cap N = \{e\}$

$\Rightarrow$ $x^{-1}\, n^{-1}\, xn = e$

$\Rightarrow$ $xn = nx$ for all $x \in G$

$\Rightarrow$ $n \in Z(G)$ for all $n \in N$

$\Rightarrow$ $N \subseteq Z(G)$.

Exercises

1. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$, the group of quaternions. Let $S = \{i, j\}$. Show that S generates G.
2. Let $G = S_n$, S = set of all transpositions in G. Show that S generates G.
   (*i.e.*, S_n $(n \geq 2)$ is generated by $(n - 1)$ transpositions (12), (23), ..., $(n-1\ n)$
3. Show that the set $\{1\}$ generates the group $\mathbf{Z}$ of integers under addition.
4. Show that $< a, b > = < a^{-1}, b^{-1} >$
5. Prove that the alternating group $A_n (n \geq 3)$ may be generated by $(n - 2)$, 3-cycles of the form (123), (124), ..., (12n).
6. If H, K are subgroups of G, show that $H \subseteq K \Rightarrow H' \subseteq K'$.
7. Let G be a simple non abelian group. Show that $G = G'$.
8. Show that $S_4 = <(12), (134)>$.

A Quick Look at what's been done

- A subgroup H of a group G is called a **normal subgroup** of G if $Ha = aH$, $\forall\ a \in G$. Equivalently, H is normal iff $g^{-1} h\, g \in H$ for all $g \in G$ and $h \in H$.
- A group having no non-trivial normal subgroup is called a **simple group**.
- The set of all right (left) cosets of H in G forms a group under the binary composition defined by $HaHb = Hab$ and is called the **quotient** or **factor group** of G by H.
- Quotient groups of cyclic (abelian) groups are cyclic (abelian). Converse, however, does not hold.
- **Kernel** of a homomorphism contains those elements that are mapped to the identity. It forms a normal subgroup.
- If there exists a one-one onto homomorphism between two groups the groups are said to be **isomorphic**. There are three isomorphism theorems, the first one is also called the **Fundamental theorem of group homomorphism** which states that homomorphic image of a group G is isomorphic to a quotient group of G.
- Any infinite cyclic group is isomorphic to $<\mathbf{Z}, +>$ and a finite cyclic group of order n is isomorphic to $\mathbf{Z}_n$.
- **Cayley's theorem** says that every group is isomorphic to a permutation group.
- Converse of Lagrange's theorem does not hold, in general, as $o(A_4)$ is divisible by 6 but it has no subgroup of order 6.
- The commutator subgroup of a group is a normal subgroup.

4

Automorphisms and Conjugate Elements

Introduction

We start by recalling that by an automorphism we mean an isomorphism of a group G to itself. Also under permutation groups we noticed that the set of all permutations (1–1 onto maps) forms a group. We show now that set of all automorphisms also forms a group, the two being closely related. We intend studying a few results pertaining to these groups. To begin with we take up few examples of automorphisms.

Example 1: Let G be a group, then the identity map $I : G \to G$, s.t., $I(x) = x$ is trivially an automorphism of G. In fact, it is sometimes called the *trivial* automorphism of G.

Example 2: Let $\mathbf{Z}$ = group of integer under addition

then $f : \mathbf{Z} \to \mathbf{Z}$, s.t.,

$f(n) = -n$

is an automorphism as $f(n) = f(m) \Rightarrow -n = -m \Rightarrow n = m \Rightarrow f$ is 1–1.

Again, since for any $n \in \mathbf{Z}$, $f(-n) = n$ we find f is onto.

Now $f(n + m) = -(n + m) = -n - m = f(n) + f(m)$

shows f is a homomorphism and hence an automorphism.

Example 3: If G be an abelian group and $f : G \to G$ be such that $f(x) = x^{-1}$ then as $f(xy) = (xy)^{-1} = y^{-1} x^{-1} = x^{-1} y^{-1} = f(x) f(y)$,

f is a homomorphism.

Again $f(x) = f(y) \Rightarrow x^{-1} = y^{-1}$

$\Rightarrow x = y \Rightarrow f$ is 1–1.

f is clearly onto and hence an automorphism.

Example 4: If G be a non-abelian group, then the above defined map $f : G \to G$ s.t., $f(x) = x^{-1}$ is not an automorphism.

Since G is non-abelian, $\exists\, x, y \in G$ s.t., $xy \neq yx$

Now if $f(xy) = f(x)f(y)$

then $(xy)^{-1} = x^{-1}\, y^{-1}$

$\Rightarrow (xy)^{-1} = (yx)^{-1}$

$\Rightarrow xy = yx$, a contradiction.

Hence f is not an automorphism.

We notice then $f: G \to G$, s.t., $f(x) = x^{-1}$ is an automorphism iff G is abelian.

Example 5: Let G be a finite abelian group of order n (n = odd > 1). We show G has a non-trivial automorphism.

Define $f: G \to G$, s.t.,

$f(x) = x^{-1}$

then f is an automorphism (as seen above).

Now if $f = I$

Then $f(x) = x$ for all $x \in G$

$\Rightarrow x^{-1} = x$ for all $x \in G$

$\Rightarrow x^2 = e$ for all $x \in G$

$\Rightarrow o(x) \mid 2$ for all $x \in G$

$\Rightarrow o(x) = 1$ or 2 for all $x \in G$

If $x \neq e$ then $o(x) = 2$ and as $o(x) \mid o(G)$

$2 \mid o(G) \Rightarrow o(G)$ is even, which is not true

Hence $f \neq I$

and the result is proved.

Let G be a group and let Aut G denote the set of all automorphisms of G. One can in the routine way show (and we urge the reader to try) that Aut G forms a group under the composition of mappings. We, however, prove this result through the following theorem which gives us little more information about Aut G.

Theorem 1: *Let G be a group. Let Aut G denote the set of all automorphisms of G and A(G) be the group of all permutations of G. Then Aut G is a subgroup of A(G).*

Proof: Since $I \in$ Aut G, Aut $G \neq \varphi$

Let $T \in$ Aut G. Then T is 1–1 onto from G to G.

$\therefore$ T is a permutation of G.

$\therefore$ $T \in A(G)$. So, Aut $G \subseteq A(G)$.

Let $T_1, T_2 \in$ Aut G.

Then $(T_1\ T_2)(xy) = T_1(T_2(xy))$

$= T_1(T_2(x)T_2(y))$ as T_2 is a homomorphism

$= T_1(T_2(x))T_1(T_2(y))$ as T_1 is a homomorphism

$= (T_1T_1)(x).(T_1T_2)(y)$ for all $x, y \in G$

$\therefore$ $T_1\ T_2$ is a homomorphism from G into G.

Again, $(T_1T_2)\,(x) = (T_1\ T_2)\,(y)$

$$\Rightarrow T_1(T_2(x)) = (T_1(T_2(y))$$
$$\Rightarrow T_2(x) = T_2(y) \quad \text{as } T_1 \text{ is 1–1}$$
$$\Rightarrow x = y \quad \text{as } T_2 \text{ is 1–1}$$

$\therefore$ T_1T_2 is 1–1

Let $x \in G$. Since $T_1 : G \to G$ is onto $\exists\ y \in G$ s.t. $T_1(y) = x$.

Again as $T_2 : G \to G$ is onto, $\exists\ z \in G$ s.t. $y = T_2(z)$

$$\Rightarrow T_1(T_2(z)) = x$$
$$\Rightarrow (T_1\ T_2)(z) = x$$

$\therefore$ T_1T_2 is also onto.

So, $T_1T_2 \in$ Aut G.

Let $T \in$ Aut G. Then T is 1–1 onto $\Rightarrow$ T is invertible and

$$T^{-1} : G \to G \quad \text{s.t. } T^{-1}(x) = y \Leftrightarrow T(y) = x$$
$$\text{as } TT^{-1} = I = T^{-1}\ T$$

T^{-1} is 1–1 as $T^{-1}(x_1) = T^{-1}(x_2)$

$$\Rightarrow TT^{-1}(x_1) = TT^{-1}(x_2)$$
$$\Rightarrow I(x_1) = I(x_2)$$
$$\Rightarrow x_1 = x_2$$

Let $x \in G$ then $y = T(x) \in G$

$$\therefore \quad T^{-1}(y) = T^{-1}(T(x)) = (T^{-1}T)\,x = x$$

$\therefore$ T^{-1} is onto.

Let $T^{-1}(xy) = z$ then $T(z) = xy$

Let $T^{-1}(x) = x_1,\ T^{-1}(y) = y_1$

Then $x = T(x_1), \quad y = T(y_1)$

$$\Rightarrow T(z) = xy = T(x_1)\ T(y_1) = T(x_1y_1)$$

as T is a homomorphism.

$$\therefore \quad z = x_1y_1 \text{ as } T \text{ is } 1-1$$

So $T^{-1}(xy) = z = x_1y_1 = T^{-1}(x)\ T^{-1}(y)$ for all $x, y \in G$

$$\Rightarrow T^{-1} \text{ is a homomorphism.}$$

Thus $T^{-1} \in$ Aut G

Hence, Aut G is a subgroup of $A(G)$.

(Thus Aut G forms a group).

Inner Automorphisms

Let $g \in G$. Define $T_g : G \to G$ s.t.

$$T_g(x) = gxg^{-1} \quad \text{for all } x \in G$$

Then T_g is 1–1 as

$$T_g(x) = T_g(y)$$

$\Rightarrow gxg^{-1} = gyg^{-1}$

$\Rightarrow x = y.$

Let $x \in G$. Then $g^{-1} xg \in G$.

and $T_g(g^{-1} xg) = g(g^{-1} xg) g^{-1} = x$

$\therefore$ T_g is onto

Also $T_g(xy) = g(xy) g^{-1}$

$= (gxg^{-1}) (gyg^{-1})$

$= T_g(x) T_g(y)$ for all $x, y, \in G$

Hence T_g is automorphism of G and it is called an *inner automorphism* of G.

Theorem 2: *The set I(G) of all inner automorphisms of G is a subgroup of Aut G.*

Proof: $T_e \in I(G)$ where e = identity of G.

$\therefore$ $I(G) \neq \varphi$

Let $T_{g_1}, T_{g_2} \in I(G)$

Then $T_{g_1} T_{g_2}(x) = T_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1}$

$= (g_1 g_2) x (g_1 g_2)^{-1}$

$= T_{g_1 g_2}(x)$ for all $x \in G$

$\therefore$ $T_{g_1} T_{g_2} = T_{g_1 g_2} \in I(G)$

Let $T_g \in I(G)$

Then $T_g T_{g-1} = T_e = I$ (as $T_e(x) = exe^{-1} = x$ for all $x \in G$)

and $T_{g-1} T_g = I$

$\therefore$ $T_{g-1} = (T_g)^{-1} \Rightarrow (T_g)^{-1} \in I(G)$

$\therefore$ $I(G)$ is a subgroup of Aut G.

In fact, $I(G)$ is normal in Aut G. See exercises.

A question arises, when is $T_{g_1} = T_{g_2}$?

Suppose $T_{g_1} = T_{g_2}$

then $T_{g_1}(x) = T_{g_2}(x)$ for all $x \in G$

$\Leftrightarrow$ $g_1 x g_1^{-1} = g_2 x g_2^{-1}$ for all $x \in G$

$\Leftrightarrow$ $g_2^{-1} g_1 x = x g_2^{-1} g_1$ for all $x \in G$

$\Leftrightarrow$ $g_2^{-1} g_1 \in Z(G)$

$\Leftrightarrow$ $g_1 Z(G) = g_2 Z(G)$

$\therefore$ $T_{g_1} = T_{g_2} \Leftrightarrow g_1 Z(G) = g_2 Z(G)$

In view of this, we have the following

Theorem 3: $\dfrac{G}{Z(G)} \cong I(G)$, *where* $I(G)$ *is set of all inner automorphisms of* G.

Proof: Define $\theta : \dfrac{G}{Z(G)} \to I(G)$, s.t.,

$$\theta(g\,Z(G)) = T_g$$

θ is well defined as

$$g_1Z(G) = g_2Z(G) \Rightarrow g_2^{-1}\, g_1 \in Z(G)$$
$$\Rightarrow T_{g_1} = T_{g_2} \text{ (from above)}$$
$$\Rightarrow \theta(g_1\, Z(G)) = \theta(g_2\, Z(G))$$

θ is 1–1 as $\theta(g_1\, Z(G)) = \theta(g_2\, Z(G))$

$$\Rightarrow T_{g_1} = T_{g_2}$$
$$\Rightarrow g_2^{-1}\, g_1 \in Z(G)$$
$$\Rightarrow g_1Z(G) = g_2Z(G)$$

θ is onto as $T_g \in I(G) \Rightarrow g \in G$

and $gZ(G) \in \dfrac{G}{Z(G)}$ s.t., $\theta(gZ(G)) = T_g$

Also $\theta(g_1Z(G)\; g_2(Z(G)) = \theta(g_1 g_2\, Z(G))$

$$= T_{g_1}\, T_{g_2}$$
$$= T_{g_1}\, T_{g_2}$$
$$= \theta(g_1Z(G))\theta(g_2Z(G))$$

$\therefore$ θ is a homomorphism and hence an isomorphism.

If G is a finite group, then $o(Z(G))$ = finite.

$\therefore$ $o\left(\dfrac{G}{Z(G)}\right) = \dfrac{o(G)}{o(Z(G))}$. But $o\left(\dfrac{G}{Z(G)}\right) = o(I(G))$

$\therefore$ $o(I(G)) = \dfrac{o(G)}{o(Z(G))}$.

Note: Theorem 3 can also be proved as follows

Define $\varphi : G \to I(G)$, s.t., $\varphi(g) = T_g$ for all $g \in G$.

Then φ is onto homomorphism. Show that Ker $\varphi = Z(G)$,

then $\dfrac{G}{\text{Ker}\,\varphi} \cong I(G)$.

Problem 1: *Let T be an automorphism of G. Show that* $o(Ta) = o(a)$ *for* $a \in G$. *Deduce that* $o(bab^{-1}) = o(a)$ *for all* $a, b \in G$.

Solution: We refer the reader to problem 24, page 120.

Suppose now $o(a) = n$

Then $(Ta)^n = Ta^n = T(e) = e$

If $(Ta)^m = e$ then $T(a^m) = T(e)$

$\Rightarrow a^m = e \Rightarrow m \geq n$

$\therefore$ $o(Ta) = n = o(a)$

If $o(a)$ = infinite, then $o(Ta)$ is also infinite for

$o(Ta) = n < \infty \Rightarrow (Ta)^n = e$

$\Rightarrow T(a^n) = T(e) \Rightarrow a^n = e \Rightarrow o(a)$ = finite, a contradiction.

$\therefore$ $o(Ta)$ = infinite.

Now $bab^{-1} = T_b(a)$

$\therefore$ $o(T_b(a)) = o(a)$

$\Rightarrow o(bab^{-1}) = o(a)$.

Problem 2: *Let G be an infinite cyclic group. Determine Aut G.*

Solution: Let $G = < a >$.

Let $T \in$ Aut G

We show that $G = < Ta >$

Let $x \in G$

Since T is onto, $\exists\ y \in G$ s.t., $x = T(y)$

$y \in G \Rightarrow y = a^r$ for some integer r

$\therefore$ $x = Ty = Ta^r = (Ta)^r$

$\therefore$ Ta is a generator of G.

But G has only 2 generators, namely a, a^{-1}.

$\therefore$ $Ta = a$ or $Ta = a^{-1}$.

$\therefore$ T has only two choices and thus

$o(\text{Aut } G) \leq 2$

Define $T : G \to G$ s.t.,

$T(x) = x^{-1}$

then $T \in$ Aut G

Also $T \neq I$ as $T = I \Rightarrow T(x) = x$ for all x

$\Rightarrow x^{-1} = x$ for all $x \Rightarrow a^{-1} = a \Rightarrow a^2 = e$

$\Rightarrow o(a)$ is finite, a contradiction

$\therefore T \neq I$. Thus G has at least two automorphisms.

$\therefore o(\text{Aut } G) \geq 2$

$\Rightarrow o(\text{Aut } G) = 2$.

In fact, Aut $G = \{I, T \mid T(x) = x^{-1}$ for all $x \in G\}$

Since $o(\text{Aut } G) = 2$, Aut G is a cyclic group of order 2, and as any cyclic group of order n is isomorphic to $\mathbf{Z}_n$ (group under addition module n), Aut $G \cong \mathbf{Z}_2$.

(**Note :** Here Aut G has very small order, while G is of very large order).

Problem 3: *Let G be a finite cyclic group of order n. Determine Aut G.*

Solution: Let $G = < a >$, $o(G) = o(a) = n$.

Let $T \in \text{Aut } G$

Then as in problem 2,

$G = < Ta >$,

But G has only $\varphi(n)$ generators, therefore T has only $\varphi(n)$ choices

$\therefore \quad o(\text{Aut } G) \leq \varphi(n)$

Define $T_m : G \to G$ s.t.,

$T_m(x) = x^m, \quad (m, n) = 1, \ 1 \leq m < n$

Then $T_m \in \text{Aut } G$ (Verify)

If $T_r = T_s$, then $T_r(a) = T_s(a)$

$\Rightarrow a^r = a^s$. Let $r > s$

$\Rightarrow a^{r-s} = e$

$\Rightarrow o(a) \mid r - s$

$\Rightarrow n \mid r - s$

$\Rightarrow n \leq r - s < n$, a contradiction

$\therefore \quad T_r \neq T_s$ for all r, s $(r \neq s)$, $1 \leq r, s \leq m$

where $(r, n) = (s, n) = 1$

This gives at least $\varphi(n)$ automorphisms of G.

$o(\text{Aut } G) \geq \varphi(n)$

$\Rightarrow o(\text{Aut } G) = \varphi(n)$

Infact, $\text{Aut } G = \{T_m \mid T_m(x) = x^m, (m, n) = 1\}_{1 \leq m < n}$

We thus find $o(\text{Aut } G) = \varphi(n)$

We show that $\text{Aut } G \cong U_n$ the group of integers multiplication modulo n.

Define $\theta : \text{Aut } G \to U_n$ s.t.

$\theta(T_m) = m, \quad 1 \leq m < n, \ (m, n) = 1$

Then $\theta(T_r) = \theta(T_s)$

$\Rightarrow r = s \Rightarrow x^r = x^s \Rightarrow T_r(x) = T_s(x) \ \forall \ x$

$\Rightarrow T_r = T_s \Rightarrow \theta$ is 1–1

Given $m \in U_n$, $1 \leq m < n$, $(m, n) = 1$,

$\exists \ T_m \in \text{Aut } G$ s.t. $\theta(T_m) = m$

$\therefore \ \theta$ is onto.

To show that θ is a homomorphism, we prove $\theta(T_r \ T_s) = \theta(T_r) \otimes \theta(T_r)$

Now for $1 \leq r, s < n$, $(r, n) = 1 = (s, n)$,

$T_r \ T_s(x) = T_r(x^s) = (x^s)^r = x^{r \otimes s} = T_{r \otimes s}(x)$

$\Rightarrow T_r \ T_s = T_{r \otimes s}$

$\Rightarrow \theta(T_r \ T_s) = \theta(T_{r \otimes s})$

$= r \otimes s = \theta(T_r) \otimes \theta(T_s)$.

$\therefore \ \theta$ is a homomorphism and so an isomorphism.

Hence Aut $G \cong U_n$

This completely determines Aut G.

(**Note:** By problems 2 and 3, cyclic groups of order 3 and 4 and infinite cyclic groups have automorphism Group of order 2 which are isomorphic. But groups themselves are non-isomorphic. Also, Aut G is abelian, whenever G is cyclic).

Problem 4: If $f : G \to G$ *s.t.*,

$$f(x) = x^n$$

is an automorphism, where n is some fixed integer, show that

$$a^{n-1} \in Z(G) \quad \textit{for all } a \in G.$$

Solution: Let $a \in G$ be any element. Consider

$$\begin{aligned} f(a^{-n}\, x\, a^n) &= (a^{-n}\, x\, a^n)^n \\ &= a^{-n}\, x^n\, a^n \\ &= f(a^{-1})\, f(x)\, f(a) \\ &= f(a^{-1}\, xa) \end{aligned}$$

$\therefore \quad a^{-n}\, x\, a^n = a^{-1}\, xa$ as f is one-one

$\therefore \quad xa^{n-1} = a^{n-1}\, x$ for all x

Thus $a^{n-1} \in Z(G) \quad \forall\, a \in G$.

Problem 5: *Show that Aut* $\boldsymbol{Q} \cong \boldsymbol{Q}^*$, *where* $< \boldsymbol{Q}, + >$ *is group of rationals and* $< \boldsymbol{Q}^*, . >$ *is group of non zero rationals.*

Solution: Define a mapping

$$\theta : \text{Aut } \mathbf{Q} \to \mathbf{Q}^*, \text{ s.t.,}$$
$$\theta(\sigma) = \sigma(1), \quad \sigma \in \text{Aut } \mathbf{Q}$$

Then $\sigma(1) \neq 0$ as if $\sigma(1) = 0$

then $\sigma(1) = \sigma(0) \Rightarrow 1 = 0$ as σ is 1–1

So we get a contradiction. Thus, $\sigma(1) \in \mathbf{Q}^*$

Now $\theta(\sigma o \eta) = \sigma o \eta(1) = \sigma(\eta(1))$

$$= \sigma\left(\frac{m}{n}\right) \text{ say}$$

$$= \frac{m}{n}\sigma(1) \quad \text{(See Problem 26 on Page 121)}$$

$$= \eta(1)\sigma(1) = \sigma(1)\eta(1) = \theta(\sigma).\theta(\eta)$$

i.e., θ is a homomorphism.

Let now $\sigma \in$ Ker θ be any element, then

$$\theta(\sigma) = 1 \text{ identity of } \mathbf{Q}^*$$
$$\Rightarrow \sigma(1) = 1 \Rightarrow \sigma(x) = x \quad \forall\, x \in \mathbf{Q}$$
$$\Rightarrow \sigma = I \text{ identity}$$
$$\Rightarrow \text{Ker } \theta = \{I\} \Rightarrow \theta \text{ is 1–1}$$

To show ontoness of θ,

Let $x \in \mathbf{Q}^*$ be any element,

Define $\psi : \mathbf{Q} \to \mathbf{Q}$ s.t.,

$$\psi\left(\frac{a}{b}\right) = \frac{ax}{b}$$

then it is easy to see that ψ is an automorphism and thus $\psi \in$ Aut $\mathbf{Q}$

Since $\theta(\psi) = \psi(1) = 1.x = x$

we find θ is onto and hence an automorphism.

Problem 6: *Let $f : G \to G$ be a homomorphism (i.e. f is endomorphism of G) Suppose f commutes with every inner automorphism of G. Show that*

(*i*) $K = \{x \in G \mid f^2(x) = f(x)\}$ *is a normal subgroup of* G.

(*ii*) G/K *is abelian*.

Solution: (*i*) $f^2(e) = f(f(e)) = f(e) \Rightarrow e \in K$ (where e is identity of G)

$\therefore$ $K \neq \varphi$

Let $x, y \in K$ then $f(x) = f^2(x)$

$f(y) = f^2(y)$

So $f^2(xy^{-1}) = f(f(xy^{-1}))$

$= f(f(x)\, f(y^{-1})) = f(f(x)\, f(y)^{-1})$

$= f^2(x)\, f(f(y))^{-1}$

$= f^2(x)\, f^2(y))^{-1}$

$= f(x)\, f(y^{-1})$

$= f(xy^{-1})$

$\Rightarrow xy^{-1} \in K$.

Thus K is a subgroup of G.

Let $g \in G$, $x \in K$. Consider

$f^2(gxg^{-1}) = f(f(gxg^{-1}))$

$= f(f T_g(x))$

$= f(T_g f(x))$ as $f T_g = T_g f$

$= f(g)\, f^2(x)\, f(g^{-1})$

$= f(g)\, f(x)\, f(g^{-1})$ as $x \in K \Rightarrow f(x) = f^2(x)$

$= f(gxg^{-1})$

$\therefore$ $gxg^{-1} \in K$ for all $x \in K$, $g \in G$

$\therefore$ K is a normal subgroup of G.

(*ii*) Now $\dfrac{G}{K}$ is abelian

$\Leftrightarrow KxKy = KyKx$ for all $x, y \in G$

$\Leftrightarrow Kxy = Kyx$ for all $x, y \in G$

$\Leftrightarrow xyx^{-1}y^{-1} \in K$ for all $x, y \in G$

Now, $f^2(xyx^{-1}\, y^{-1}) = f(f(xyx^{-1}\, y^{-1}))$

$$= f(f(T_x y y^{-1})) = f(f T_x y))\, f(y^{-1}))$$
$$= f(T_x f(y))\, f(y)^{-1} = f(x)\, f(y)\, x^{-1})\, f(y)^{-1})$$
$$= f(x\, T_{f(y)}\, x^{-1}) = f(x)\, f\, T_{f(y)}\, x^{-1}$$
$$= f(x)\; T f_{(y)}\, f(x^{-1}) = f(x)\, f(y)\, f(x^{-1})\, f(y)^{-1}$$
$$= f(x)\, f(y)\, f(x^{-1})\, f(y^{-1})$$
$$= f(xyx^{-1}\, y^{-1})$$

$\therefore$ $xyx^{-1}\, y^{-1} \in K$

$\Rightarrow \dfrac{G}{K}$ is abelian.

Problem 7: *For any integer* $a > 1$, $n > 0$ *show that*

$n \mid \varphi(a^n - 1)$

Solution: Let $G = < b >$ s.t. $o(G) = o(b) = a^n - 1$

Define $T : G \to G$ s.t.,

$T(x) = x^a$

Since $(a\ ,\ a^n - 1) = 1$, $T \in$ Aut G

by exercise 1 (*iii*)

Also $T^2(x) = T(T(x))$

$= T(x^a) = (x^a)^a = x^{a^2}$

In general, $T^r(x) = x^{a^r}$

$\therefore$ $T^n(x) = x^{a^n} = x$ for all $x \in G$

(as $x^{o(G)} = e \Rightarrow x^{a^n - 1} = e \Rightarrow x^{a^n} = x$)

$\therefore$ $T^n = 1$

If $T^m = 1$, then $T^m(b) = b$

$\Rightarrow b^{a^m} = b \Rightarrow b^{a^m - 1} = e$

$\Rightarrow o(b) \mid (a^m - 1)$

$\Rightarrow a^n - 1 \mid (a^m - 1) \Rightarrow a^n - 1 \leq (a^m - 1)$

$\Rightarrow a^n \leq a^m \Rightarrow n \leq m$

$\therefore$ $o(T) = n$

Also $o(\text{Aut } G) = \varphi(a^n - 1)$, by problem 3

$T \in \text{Aut } G \Rightarrow o(T) \mid o(\text{Aut } G)$

$\Rightarrow n \mid \varphi(a^n - 1)$.

Characteristic Subgroups

A subgroup H of G is called a *characteristic subgroup* of G if

$T(H) \subseteq H$ for all $T \in$ Aut G.

Example 6: Let G be a cyclic group of order 4

$$G = \{e, a, a^2, a^3\}$$

Then Aut $G = \{I, T\}$, where $T(x) = x^3$ for all $x \in G$ by problem 3.

Let $H = \{e, a^2\} \leq G$

$\therefore$ $I(H) = \{I(e), I(a^2)\} = H$

$T(H) = \{T(e), T(a^2)\} = \{e, a^6 = a^2\} = H$

$\therefore$ H is a characteristic subgroup of G. (See exercise 19)

Problem 8: *Show that a characteristic subgroup of a group G is a normal subgroup of G. Is the converse true?*

Solution: Let H be a characteristic subgroup of G. Let $g \in G$, $h \in H$.

Now $T(H) \subseteq H, \quad \forall\ T \in$ Aut G

In particular, $T_g(H) \subseteq H$, T_g being inner automorphism

Thus $ghg^{-1} = T_g(h) \in T_g(H) \subseteq H$

$\therefore$ H is a normal subgroup of G.

Converse, however is not true.

Let G be an abelian group of order 4.

Then $G = \{e, a, b, ab \mid a^2 = e = b^2 = (ab)^2, ab = ba\}$

Let $H = \{e, a\} \leq G$.

Then H is normal subgroup of G as index of H in G is 2.

Let $T : G \to G$ s.t $T(a) = b$, $T(b) = a$, $T(ab) = ab$, $T(e) = e$

Then $T \in$ Aut G

But $T(a) = b \notin H \Rightarrow H$ is not characteristic subgroup of G.

Problem 9: *Let K be a subgroup of H and H, a subgroup of a group G. Suppose K is characteristic subgroup of G and* $\frac{H}{K}$ *is a characteristic subgroup of* $\frac{G}{K}$ *. Show that H is a characteristic subgroup of G.*

Solution: Let $\sigma \in$ Aut G. To show that $\sigma(h) \in H$ for all $h \in H$.

Define $\eta: \frac{G}{K} \to \frac{G}{K}$ by

$\eta(\mathrm{Kg}) = K\sigma(g)$

Then η is well defined as

$Kg_1 = Kg_2$ implies $g_1 g_2^{-1} \in K$.

So, $\sigma(g_1 g_2^{-1}) \in K$ as K is characteristic subgroup of G.

Therefore, $\sigma(g_1)\ \sigma(g_2)^{-1} \in K$

or $K\sigma(g_1) = K\sigma(g_2)$

Consider $\eta(Kg_1 Kg_2) = \eta(Kg_1 g_2)$

$= K\sigma(g_1 g_2)$

$= K\sigma(g_1)\sigma(g_2)$
$= K\sigma(g_1)K\sigma(g_2)$
$= \eta(Kg_1)\eta(Kg_2)$

So, η is a homomorphism.

Let $Kg \in$ Ker η. Then $\eta(Kg) = K$.

So, $K\sigma(g) = K$ or $\sigma(g) \in K$.

Therefore, $\sigma^{-1}\sigma(g) \in K$ as K is characteristic subgroup of G. which means that $g \in k$ or $Kg = K$.

So, Ker η = {Identity K}.

This shows that η is one-one.

Let $Kx \in \frac{G}{K}$. Then there exists $g \in G$ such that $\sigma(g) = x$.

So, $\eta(Kg) = K\sigma(g) = Kx$. This shows that η is onto.

Therefore, $\eta \in$ Aut $\frac{G}{K}$.

Now $h \in H$ implies $Kh \in \frac{H}{K}$.

Since $\frac{H}{K}$ is characteristic subgroup of G, $\eta(Kh) \in \frac{H}{K}$.

So, $K\sigma(h) = Kh_1$, $h_1 \in H$.

Therefore, $\sigma(h)h_1^{-1} \in K \subseteq H$ implies $\sigma(h) \in H$

Hence H is a characteristic subgroup of G.

Problem 10: *Show that if* $o(Aut\ G) > 1$, *then* $o(G) > 2$.

Solution: Suppose $o(G) \leq 2$.

If $o(G) = 1$ then G has only one automorphism, namely identity map I, contradicting $o(\text{Aut } G) > 1$.

If $o(G) = 2$, then $G = \{e, a \mid a^2 = e, a \neq e\}$.

Since $o(\text{Aut } G) > 1$, $\exists\ T \in$ Aut G s.t. $T \neq I$.

$\therefore\ \exists\ x \in G$ s.t., $T(x) \neq x$. But $T(e) = e$.

$\therefore\ T(a)$ must be a, contradicting that $\exists\ x$ s.t. $T(x) \neq x$.

$\therefore\ o(G) \neq 2$

Hence $o(G) > 2$.

Problem 11: *If G is any group in which* $g^2 \neq e$ *for some* $g \in G$, *then show that G has a non-trivial automorphism.*

Solution: If G is abelian, then $T : G \to G$ s.t., $T(x) = x^{-1}$ for all $x \in G$ is an automorphism of G by Example 3. If $T = I$, then $T(g) = I(g) \Rightarrow g^{-1} = g \Rightarrow g^2 = e$, a contradiction.

If G is non-abelian, then some inner automorphism of G is non-trivial as

$T_x = I$ for all $x \in G \Rightarrow T_x(y) = y$ for all $x, y \in G$

$\Rightarrow xyx^{-1} = y$ for all $x, y \in G$

$\Rightarrow xy = yx$ for all $x, y \in G$

$\Rightarrow G$ is abelian, a contradiction.

In any case, G has non-trivial automorphism (see example 5 also).

The reader may go through the following problem only after acquainting himself (herself) with vector spaces.

Problem 12: *Show that a finite group having more than two elements has a non-trivial automorphism.*

Solution: If $\exists\ g \in G$ s.t., $g^2 \neq e$, then result follows by problem 11.

Let $g^2 = e$ for all $g \in G$.

Then G is abelian. G can be regarded as a vector space V over $\mathbf{Z}_2$, the field $\{0, 1\}$ mod 2, by defining $g_1 + g_2 = g_1 g_2$ for all $g_1, g_2 \in G$ and $\alpha g = e$ *if* $\alpha = 0$ and $\alpha g = g$ if $\alpha = 1$. Then any invertible linear map $V \to V$ is an automorphism of G and conversely. (**Note:** e is zero of V and $-g$ is negative of g in V). If V is finite dimensional, then $T : V \to V$ s.t. $T(\alpha_1 e_1 + ... + \alpha_n e_n) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + ... \alpha_n e_n$ is 1–1 onto linear map. ($T \neq I$).

Here $\{e_1..., e_n\}$ is a basis of V.

If G is finite, then dim V is finite $= n > 1$ and $o(V) = 2^n = o(G)$. If $o(G) = 4$ and $g^2 = e$ for $g \in G$ then

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

are all invertible linear maps from V into V. So $o(\text{Aut } G) = 6$ and Aut G is non-abelian.

Problem 13: *Show that Aut* $S_3 \cong S_3$.

Solution: Let $H = \{(12), (13), (23)\}$, *i.e*, H be the subset of S_3 containing all members of order 2 in $G = S_3$.

Let $T \in$ Aut G be any member, then $T : G \to G$ is an is isomorphism. Since $H \subseteq G$, $T(h) \in G\ \forall\ h \in H$. By problem 1, $o(T(a)) = o(a)\ \forall\ a \in G$, thus if $h \in H$ be any member then $o(h) = 2$ and so $o(T(h)) = o(h) = 2$ i.e., $T(h) \in H$ is $\forall\ h \in H$.

So $T : H \to H$ is a mapping (*i.e*., T can be restricted to H, and we denote this restriction of T to H by T'). Also since $T : G \to G$ is 1–1, $T' : H \to H$ will be 1–1. Again as H is finite $T' : H \to H$ is 1–1 it will also be onto and hence T' is a permutation on H *i.e.,* $T' \in A(H)$.

Define θ: Aut $G \to A(H)$, s.t.,

$$\theta(T) = T'$$

Then θ is well defined as

$$T_1 = T_2 \Rightarrow T_1' = T_2' \Rightarrow \theta(T_1) = \theta(T_2)$$

Also θ is 1–1, as let $\theta(T_1) = \theta(T_2)$

$$\Rightarrow T_1' = T_2'$$

$$\Rightarrow T_1'(h) = T_2'(h) \qquad \forall\ h \in H$$

$$\Rightarrow T_1(h) = T_2(h) \qquad \forall\ h \in H$$

i.e., T_1 and T_2 agree on elements of H. We show they agree on all elements of G.

Now $T_1[(123)] = T_1[(13)(12)] = T_1(13)\ T_1(12) = T_2(13)\ T_2(12) = T_2(13)(12) = T_2[(123)]$

Similarly $T_1[(132)] = T_2[(132)]$ and of course, $T_1(I) = T_2(I)$

Thus T_1 & T_2 agree on all elements of G and so $\theta(T_1) = \theta(T_2) \Rightarrow T_1 = T_2 \Rightarrow \theta$ is 1–1.

Since θ will be onto from Aut $G \to \theta$(Aut G)

o(Aut G) = $o(\theta$(Aut G))

But θ(Aut G) $\subseteq A(H)$

$\Rightarrow o((\theta(\text{Aut } G)) \leq o(A(H)) = \lfloor 3 = 6$

i.e., o(Aut G) ≤ 6

Also since $G \cong I(G)$ when $G = S_3$ (See exercise 7)

$o(I(G)) = o(G) = 6$

But $I(G) \leq$ Aut G and so $6 \leq o$(Aut G)

Hence o(Aut G) = 6

$\Rightarrow$ Aut $G = I(G)$

Hence Aut $S_3 \cong S_3$.

Problem 14: *Show that Aut* $S_4 \cong S_4$.

Solution: Let $\sigma \in$ Aut S_4, then σ takes (12) into a transposition as Klein's 4-group is a characteristic subgroup of S_4. To each transposition (ab) there correspond four cycles of length 3 which have one common letter with (ab) namely (acd), (adc), (bcd), (bdc) and S_4 is generated by (ab) and any of these four cycles. This is true for each transposition. So, we have counted 24 generators of S_4.

So if $S_4 = \langle(12), (134)\rangle$ then

$\sigma(S_4) = \langle\sigma(12), \sigma(134)\rangle = S_4$

$\therefore$ o(Aut S_4) ≤ 24

But, $S_4 \cong I(S_4)$ and $I(S_4) \leq$ Aut S_4

$\Rightarrow o$(Aut S_4) ≥ 24

Thus o(Aut S_4) = 24 = $o(I(S_4))$

$\Rightarrow$ Aut $S_4 = I(S_4)$ or that Aut $S_4 \cong S_4$.

(See problem 13 on page 221 also)

Exercises

1. Show that the following maps are automorphisms

(*i*) G = cyclic group of order 6, $f: G \to G$. s.t. $f(x) = x^5$.

(*ii*) G = group of positive real numbers under multiplication

$f: G \to G$, s.t., $f(x) = x^2$.

(*iii*) G = finite abelian group of order n. $f : G \to G$, s.t.,

$$f(x) = x^m, \quad 1 \le m < n, (m, n) = 1.$$

2. Let H be a subgroup of G. Show that $T(H)$ is subgroup of G for all $T \in$ Aut G.

3. If H is normal in G, show that $T(H)$ is also normal in G for all $T \in$ Aut G.

4. Show that $I(G)$ is a normal subgroup of Aut G.

5. Show that $I(G) = \{ I \}$ if and only if G is abelian.

6. If $\frac{G}{Z(G)}$ is cyclic then (show that) G is abelian (See page 111). Deduce that G is abelian if Aut G is cyclic.

7. Show that $G \cong I(G)$ if $G = S_3$.

8. Show that the commutator subgroup of a group G is a characteristic subgroup of G.

9. If $G_1 \cong G_2$, show that $I(G_1) \cong I(G_2)$ and Aut $G_1 \cong$ Aut G_2.

10. If G is (non-cyclic) abelian group of order 4, then show that Aut $G \cong S_3$.
(By solved problem 11 and this exercise it follows that two non-isomorphic groups may have isomorphic automorphism groups).

11. If G is a finite group and $T \in$ Aut G s.t., $T(x) = x$ if and only if $x = e$ (such an automorphism is called a fixed point free automorphism). Show that $g \in G$ can be written as $x^{-1} T(x)$ for some $x \in G$.

12. Further in exercise 11, if $T^2 = I$, show that G is abelian and $o(G) =$ odd.

13. Let $o(G) = 2n$. Let H be a subgroup of G consisting of only those elements of G whose order is not 2. Suppose $o(H) = n$. Show that n is odd and H is abelian.

14. If H is a characteristic subgroup of G, show that $T(H) = H$ for all $T \in$ Aut G.

15. (*i*) If H is a characteristic subgroup of K and K is normal in G, show that H is normal in G.

(*ii*) Show if H is characteristic subgroup of K and K is characteristic subgroup of G then H is characteristic subgroup of G, i.e., the characteristic property is transitive.

16. If K is a characteristic subgroup of G and $T \in$ Aut G, show that

$$T' : \frac{G}{K} \to \frac{G}{K} \text{ s.t., } T'(Kg) = K(Tg) \text{ for all } g \in G$$

is an automorphism. Further, show that the map $T \to T'$ is a homomorphism of Aut G into Aut (G/K).

17. Let G be an abelian group. Let $H = \{x \in G \mid x^n = e, n = \text{fixed integer}\}$. Show that H is a characteristic subgroup of G.

18. If H is a unique subgroup of order m in G, show that H is characteristic subgroup of G.

19. Show that every subgroup of a finite cyclic group is characteristic subgroup.

20. Prove that automorphism group of a finite group is finite.

21. Let G be the group of all $n \times n$ non-singular matrices over a field F. Let y' denote the transpose of matrix y. Define

$$\theta : G \to G \text{ s.t.}$$
$$\theta(x) = (x^{-1})'$$

Show that $\theta \in \text{Aut } G$ and θ is an outer automorphism of G unless either $F = \mathbf{Z}_2$ and $n \leq 2$ or $F = \mathbf{Z}_3$ and $n = 1$. (An automorphism of G is called an *outer automorphism* of G if it is not an inner automorphism).

Conjugate Elements

Definition: Let G be a group, $a, b \in G$. Define a relation $\sim$ on G as follows:

$$a \sim b \Leftrightarrow \exists\ c \in G \text{ s.t. } a = c^{-1}\, bc$$

It is not difficult to see that $\sim$ is an equivalence relation on G. If $a \sim b$ *we say* a *is conjugate* to b (or a, b *are conjugates and relation* $\sim$ *is called conjugate relation on* G).

Let $cl(a)$ denote the equivalence class of a in G then $cl(a)$ is called *conjugate class or conjugacy class* of a in G. Since $\sim$ is an equivalence relation on G, it divides G into disjoint equivalence classes.

$$\therefore \quad G = \bigcup_{a \in G} cl(a), \text{ where}$$
$$cl(a) = \{x \in G \mid x \sim a\}$$
$$= \{x \in G \mid x = y^{-1}\, ay,\ y \in G\}$$
$$= \{y^{-1}\, ay \mid y \in G\}$$
$$= \text{set of all conjugates of } a \text{ in } G.$$

Remarks: (i) $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$

Suppose $cl(a) = \{a\}$. Then $y^{-1}ay = a$ for all $y \in G$

$\therefore$ $ya = ay$ for all $y \in G$

$\therefore$ $a \in Z(G)$

Conversely, let $a \in Z(G)$. Let $x \in cl(a)$ be any element, then $x = y^{-1}ay$ for some $y \in G$

$$\Rightarrow x = ay^{-1}y \quad (\text{as } a \in Z(G)$$
$$\Rightarrow x = a \Rightarrow cl(a) = \{a\}.$$

(ii) G is abelian $\Leftrightarrow cl(a) = \{a\}$ for all $a \in G$

G is abelian $\Leftrightarrow G = Z(G)$

$\Leftrightarrow a \in Z(G)$ for all $a \in G$

$\Leftrightarrow cl(a) = \{a\}$ for all $a \in G$.

We shall denote by $k(G)$ or k, the number of conjugate classes in G. It follows by remark (ii) that $o(G) = k \Leftrightarrow G$ is abelian.

Normalizer or Centralizer of an element $a \in G$ was defined to be the set $N(a) = \{x \in G \mid xa = ax \text{ for all } x \in G\}$. Also $N(a) \leq G$. It can be shown that $N(a) = G \Leftrightarrow a \in Z(G)$

$$N(a) = G \Leftrightarrow g \in N(a) \text{ for all } g \in G$$
$$\Leftrightarrow ga = ag \text{ for all } g \in G$$
$$\Leftrightarrow a \in Z(G).$$

So, by remark (*i*) it follows that

$$N(a) = G \Leftrightarrow cl(a) = \{a\}.$$

Problem 15: *Suppose $a \in G$ has only two conjugates in G then show that N(a) is a normal subgroup of G.*

Solution: Let a, $g^{-1}ag$ be two conjugates of a in G. We show

$$G = N(a) \cup N(a)g$$

Let $x \in G$. Consider $x^{-1}ax$. Then $x^{-1}ax = a$ or $g^{-1}ag$.

If $x^{-1}ax = a$, then $xa = ax \Rightarrow x \in N(a)$

If $x^{-1}ax = g^{-1}ag$, then $xg^{-1}a = axg^{-1}$

$$\Rightarrow xg^{-1} \in N(a)$$
$$\Rightarrow x \in N(a)g$$
$$\therefore \quad G = N(a) \cup N(a)g$$

and thus index of $N(a)$ in G is 2, showing thereby that $N(a)$ is a normal subgroup of G.

Problem 16: *Let G be a finite group and x, y be conjugate elements of G. Show that the number of distinct elements $g \in G$ s.t. $g^{-1}xg = y$ is $o(N(x))$.*

Solution: Let $g = g_1, g_2 \ldots, g_n$ be distinct elements of G s.t., $g_i^{-1}xg_i = y$

Let $S = \{g = g_1, g_2 \ldots, g_n\}$

We show that $S = N(x)g$

Suppose $s \in S$ then $s = g_i$ for some $i, 1 \le i \le n$

If $s = g_1 = g$, then $s = g = eg \in N(x)\, g$

If $s \neq g_1$, then $s = g_i$, $i \neq 1$

and $g^{-1} xg = g_i^{-1} xg_i$

$$\Rightarrow g_i g^{-1} x = x g_i g^{-1}$$
$$\Rightarrow g_i g^{-1} \in N(x)$$
$$\Rightarrow g_i \in N(x)$$
$$\Rightarrow s \in N(x)g$$

or that $S \subseteq N(x)g$

Again $z \in N(x)g \Rightarrow z = hg, \quad h \in N(x)$

$$\Rightarrow z^{-1} xz = g^{-1} h^{-1} xhg$$
$$\Rightarrow z^{-1} xz = g^{-1} xg \quad \text{as } xh = hx$$
$$\Rightarrow z^{-1} xg = y$$
$$\Rightarrow z = g_i \quad \text{for some } i$$
$$\Rightarrow z \in S$$
$$\Rightarrow N(x)g \subseteq S$$

Hence $S = N(x)g$

and thus $o(S) = o(N(x)g) = o(N(x))$

(**Note:** As $gg_i^{-1} x = xgg_i^{-1}$ for all $i = 1,..., n$

$gg_i^{-1} \in N(x)$ for all i

$\Rightarrow N(x)g = N(x)g_i$ for all i)

Problem 17: *Suppose X is a conjugate class of non trivial elements of G. Let $T \in$ Aut G. Show that $T(X) = \{T(x) \mid x \in X\}$ is a conjugate class of elements of G.*

Solution: Let $X = cl(a), \quad a \neq e$

We show that $T(X) = cl(Ta)$

Let $y \in T(X) \Rightarrow y = Tx, \quad x \in X = cl(a)$

$= T(g^{-1} ag), \quad g \in G$

$= T(g)^{-1} T(a) T(g) \in cl(T(a))$

$\therefore \quad T(X) \subseteq cl(Ta)$

Again $z \in cl(Ta) \Rightarrow z = h^{-1} T(a) h, \quad h \in G$

$= (Th_1)^{-1} Ta Th$

(as T is onto $\Rightarrow h = Th_1, \quad h_1 \in G$)

$= Th_1^{-1} Ta Th$

$= T(h^{-1} ah)$

$\in T(cl(a)) = T(X)$

$T(X) = cl(Ta)$

Hence $T(X)$ is a conjugate class of G.

The following theorem helps us to determine the order of conjugate class of an element.

Theorem 4: *Let G be a finite group, $a \in G$.*

Then $$o(cl(a)) = \frac{o(G)}{o(N(a))}$$

where cl(a) is the conjugate class of a.

Proof: Since $N(a) \leq G$, G can be written as union of disjoint right cosets of $N(a)$ in G.

Let $G = \bigcup_{i=1}^{t} N(a)x_i \qquad [t \leq n = o(G)]$

Then $o(G) = t \; . \; o(N(a))$ ...(1)

[Arguments being similar as in the proof of Lagrange's theorem, page 66].

Let $S = \{x_1^{-1} ax_1,..., x_t^{-1} ax_t\}$

Suppose $x_i^{-1} ax_i = x_j^{-1} ax_j \quad$ for $i \neq j$

Then $x_i x_j^{-1} a = ax_i x_j^{-1}$

$\Rightarrow x_i x_j^{-1} \in N(a)$

$\Rightarrow N(a)x_i = N(a)x_j$, a contradiction

$\therefore$ all elements in S are distinct i.e., $o(S) = t$

We show that $S = cl(a)$

Let $s \in S$ then $s = x_i^{-1} a x_i$, for some i, $1 \le i \le t$

$\Rightarrow s$ is conjugate of a

$\Rightarrow s \in cl(a) \Rightarrow S \subseteq cl(a)$

Again $x \in cl(a) \Rightarrow x = g^{-1} a g$, $g \in G$

$g \in G \Rightarrow g \in N(a) x_i$ for some i, $1 \le i \le t$

$\Rightarrow g = y x_i$, $y \in N(a)$

Thus $x = x_i^{-1} y^{-1} a y x_i$

$= x_i^{-1} a x_i$ as $ya = ay$

$\Rightarrow x \in S$

$\therefore$ $cl(a) \subseteq S \Rightarrow S = cl(a)$

and so $o(cl(a)) = o(S) = t$

and hence from (1) we get $o(cl(a)) = \dfrac{o(G)}{o(N(a))}$.

Remark: Since $G = \bigcup_{a \in G} (cl(a))$

$$o(G) = \sum_{a \in G} o(cl(a))$$

$$= \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$= o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

(By remark (i) earlier $o(cl(a)) = 1 \Leftrightarrow a \in Z(G)$).

$\therefore$ $$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

i.e., $$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

This equation is called ***class equation*** of G.

Problem 18: *Let G be a finite group and $x \in G$ then show that*

$$o(N(x)) \ge o\left(\frac{G}{G'}\right).$$

Solution: We show that $cl(x) \subseteq G'x$

Let $y \in cl(x) \Rightarrow y = g^{-1} x g$, $g \in G$

$= (g^{-1} x g)(x^{-1} x)$

$= (g^{-1} x g^{-1} x^{-1}) x$

$\in G'x$

$\therefore$ $cl(x) \subseteq G'(x)$

$\therefore$ $o(cl(x)) \le o(G'x)$

$$\therefore \qquad \frac{o(G)}{o(N(x))} \leq o(G'x) = o(G')$$

$$\therefore \qquad \frac{o(G)}{o(G')} \leq o(N(x)).$$

Problem 19: *If index of Z(G) in G is n then show that any conjugate class has at most n elements.*

Solution: We have

$$n = \frac{o(G)}{o(Z(G))} \text{ and } o(cl(a)) = \frac{o(G)}{o(N(a))}$$

Since $Z(G) \subseteq N(a)$ always

$$o(Z(G)) | o(N(a)) \Rightarrow o(N(a)) = k.o(Z(G))$$

i.e., $$o(Cl(a)) = \frac{o(G)}{o(N(a))} = \frac{n.o(Z(G))}{k.o(Z(G))} = \frac{n}{k}$$

Thus, maximum value of $o(cl(a))$ is when $k = 1$, proving the result.

Problem 20: *Let G be group of order p^n, p = prime, n = + ve integer. Show that* $o(Z(G)) > 1$.

Solution: If $G = Z(G)$, $o(Z(G)) = o(G) > 1$.

If $G \neq Z(G)$, then $\exists$ some $a \in G$, s.t., $a \notin Z(G)$.

Then $N(a) < G$ [as $a \notin Z(G) \Rightarrow at \neq ta$ for some $t \in G$, i.e., $t \notin N(a)$, $t \in G$].

$$\therefore \qquad o(N(a)) = p^m, \quad m < n$$

i.e., $$\frac{o(G)}{o(N(a))} = p^{n-m}, \quad n - m > 0$$

i.e. $$o(cl(a)) = p^{n-m} = \text{multiple of } p$$

$$\therefore \qquad \sum_{a \notin Z(G)} o(cl(a)) = \text{multiple of } p = kp, \text{ (say)}$$

By class equation of G

$$p^n = o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$\Rightarrow o(Z(G)) = p^n - kp = p(p^{n-1} - k)$$

$$\Rightarrow p \mid o(Z(G)) \Rightarrow o(Z(G) > 1.$$

Remark: It follows from above problem that if G is a finite non-abelian simple group then $o(G)$ is divisible by at least two distinct primes. Since G is simple, it has no non-trivial normal subgroup. Now $Z(G)$ is a normal subgroup of G. $Z(G) = G \Rightarrow G$ is abelian, which is not so. Thus $Z(G) = \{e\}$, which means $o(G)$ cannot be of the type p^n, i.e., it is not divisible by only one prime.

Problem 21: *A group of order p^2 (p = prime) is abelian.*

Solution: Suppose $o(G) = p^2$ and G is non-abelian.

Then $Z(G) \neq G$. So $\exists\ a \in G$, s.t., $a \notin Z(G)$ and as in previous problem, $N(a) \subsetneq G$.

Again, $Z(G) \subseteq N(a)$ always but as $a \notin Z(G)$, $Z(G) \subsetneq N(a)$

Now $o(Z(G)) \mid o(G) = p^2 \Rightarrow o(Z(G)) = 1, p$ or p^2

But $o(Z(G)) > 1$ by problem 16

and $o(Z(G)) = p^2 \Rightarrow Z(G) = G$ which is not true

Hence $o(Z(G)) = p$

Again, $o(N(a)) \mid o(G) = p^2$ gives $o(N(a)) = 1, p$ or p^2

Since $N(a) \neq G$, $o(N(a)) \neq p^2$

Also $Z(G) \subsetneq N(a) \Rightarrow o(N(a)) > 1$

$\therefore$ $o(N(a)) = p$

But that means $Z(G) = N(a)$, a contradiction

Hence G is abelian.

Note: If $o(Z(G)) = p$, then $o\left(\frac{G}{Z(G)}\right) = \frac{p^2}{p} = p$, a prime $\Rightarrow \frac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian.

A question arises whether group of order p^3 (p = prime) is abelian? The answer is no as the Quaternion group is non-abelian and has order 2^3. Infact, there exist non-abelian groups of order p^3 for all primes p.

For example

Let $$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \begin{array}{l} a, b\ c \text{ are arbitrary} \\ \text{elements of a field } F \end{array} \right\}$$

Then G is a non-abelian group of order p^3 if F is a field of order p. It is called the *Heisenberg group* over F. In general, order of the Heisenberg group over F is $(o(F))^3$. (See page 251 also).

Problem 22: *Let G be a non abelian group of order p^3. Determine $o(Z(G))$ and k = number of conjugate classes of G.*

Solution: Since G is non-abelian, $\exists\ a \in G$, s.t., $Z(G) \subsetneq N(a) \subsetneq G$ as in previous problems.

Now $o(Z(G)) \mid o(G) = p^3 \Rightarrow o(Z(G)) = 1, p, p^2$ or p^3

Similarly, $o(N(a)) = 1, p, p^2$ or p^3

$o(Z(G)) \neq 1$. By problem 16

$o(Z(G)) \neq p^3$ as $Z(G) \neq G$

so $o(Z(G)) = p$ or p^2

Similarly, $o(N(a)) = p$ or p^2 and as $Z(G) \subsetneq N(a)$

We find $o(Z(G)) = p$ and $o(N(a)) = p^2$

Let now k be the total number of conjugate classes. Since

$$G = \bigcup_{a \in G} cl(a)$$

$$o(G) = \sum_{a \in G} o(cl(a)) = \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

i.e., $$p^3 = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

As number of conjugate classes when $a \in Z(G)$ is $o(Z(G)) = p$

$[a \in Z(G) \Leftrightarrow cl(a) = \{a\}$, i.e., $o(cl(a)) = 1]$

So remaining classes are $k - p$, each will have order given by

$$o(cl(a)) = \frac{o(G)}{o(N(a))} = \frac{p^3}{p^2} = p$$

Hence $p^3 = p + (k - p)p \Rightarrow k = p^2 + p - 1$.

Problem 23: *Find all the conjugate classes of the quaternion group.*

Solution: We have the quaternion group

$$G = \{\pm 1, \pm i, \pm j, \pm k\}$$

Let us determine the conjugate class of i.

Now, in general, we know that

$< a > \subseteq N(a)$ in any group

$[x \in < a > \Rightarrow x = a^m$ and as $a.a^m = a^m.a$, we find $a^m \in N(a)]$

Thus $< i > \subseteq N(i)$ or $\{i, i^2, i^3, i^4 = 1\} \subseteq N(i)$

and, therefore, $< i > \subseteq N(i) \leq G$ gives

$4 | o(N(i)) | 8$

Again, since $j \notin N(i)$ as $ji \neq ij$

and $j \in G$,

$$N(i) \subsetneq G$$

Hence $o(N(i)) = 4$ or that $< i > = N(i)$

Since $$o(cl(a)) = \frac{o(G)}{o(N(a))}$$ (Page 184)

$$o(cl(i)) = \frac{8}{4} = 2$$

$\Rightarrow cl(i) = \{i, -i\}$ as $i \in cl(i)$ always and as $-i = kik^{-1}$, $-i \in cl(i)$

$[kik^{-1} = ki(-k) = -(k(ik)) = -(-kki) = k^2 i = -i]$

Similarly other conjugate classes will be $\{\pm j\}$, $\{\pm k\}$, $\{1\}$ $\{-1\}$

Notice as $1, -1 \in Z(G)$ $o(cl(1)) = 1$, $o(cl(-1)) = 1$

as $o(cl(a)) = 1 \Leftrightarrow a \in Z(G)$

We can verify the class equation here

$$o(G) = o(Z(G)) + \Sigma_{a \notin Z(G)} o(cl(a))$$

$$8 = 2 + (2 + 2 + 2)$$

Problem 24: *Suppose G is a finite group and k(G) = number of conjugate classes of G is* 3. *Then show that either G is a cyclic group of order* 3 *or is non-abelian group* S_3 *of order 6* (*upto isomorphism*).

Solution: If all three classes of G are of length one, then $o(G) = 3 \Rightarrow G$ is cyclic group of order 3. Suppose G has one class of length > 1. Then G is non-abelian. Let C_1, C_2, C_3, be three classes.

Suppose $o(C_3) > 1$.

If $o(C_1) = o(C_2) = 1$

then $o(C_3) = n - 2$

where $n = o(G)$. But $o(C_3) = n - 2 \mid o(G) = n$

Also $n - 2 \mid n - 2$

$\therefore$ $n - 2 \mid n - (n - 2) = 2$

$\Rightarrow$ $n - 2 = 1$ or 2

$\Rightarrow$ $n = 3$ or 4

In either case, G is abelian.

(as $n = 3 \Rightarrow o(G) = 3 =$ prime $\Rightarrow g$ is cyclic

$\Rightarrow G$ is abelian

$n = 4 \Rightarrow o(G) = p^2 = 2^2 \Rightarrow G$ is abelian)

We are thus left with only one option, that only one class in G is of length 1. Let $o(C_1) = 1$, $o(C_2) > 1$, $o(C_3) > 1$. $o(Z(G) = 1$.

By class equation,

$$n = o(G) = o(C_1) + o(C_2) + o(C_3)$$
$$= 1 + o(C_2) + o(C_3)$$

But $o(C_3) \mid o(G) = n$, $o(C_3) \mid o(C_3)$

$\Rightarrow o(C_3) \mid n - o(C_3) = 1 + o(C_2)$

$\Rightarrow o(C_3) \leq 1 + o(C_2)$

Similarly, $o(C_2) \leq 1 + o(C_3)$

If $o(C_3) < 1 + o(C_2)$ and $o(C_2) < 1 + o(C_3)$

then $o(C_3) \leq o(C_2)$, $o(C_2) \leq o(C_3)$

$\therefore$ $o(C_2) = o(C_3)$

$\therefore$ $o(C_3) \mid 1 + o(C_3) \Rightarrow o(C_3) \mid 1 \Rightarrow o(C_3) = 1$

a contradiction.

Thus either $o(C_3) = 1 + o(C_2)$

or $o(C_2) = 1 + o(C_3)$

If $o(C_3) = 1 + o(C_2)$

then $o(G) = 1 + o(C_2) + 1 + o(C_2)$

$\Rightarrow o(G) - 2\, o(C_2) = 2$

But $o(C_2) \mid o(G)$, $o(C_2) \mid o(C_2) \Rightarrow o(C_2) \mid 2\ o(C_2)$

$\therefore$ $o(C_2) \mid o(G) - 2\ o(C_2) = 2$

$\therefore$ $o(C_2) = 2$ and $o(C_3) = 3$

or that $o(G) = 6$

Similarly, if $o(C_2) = 1 + o(C_3)$, then $o(G) = 6$.

$\therefore$ G is non-abelian group of order 6 and so, isomorphic to S_3.

Problem 25: *Let G be a group and $e \neq a \in G$ s.t., $o(a)$ = finite. Suppose. G has only two conjugate classes. Then show that G is a finite group of order* 2.

Solution: Let $e \neq b \in G$. Since G has only 2 conjugate classes, namely $\{e\}$ and $cl(a)$. $b \in cl(a)$ $\therefore$ $b = g^{-1} ag$ for some $g \in G$.

$\therefore$ $o(b) = o(a)$ for all $b \neq e$ in G

Suppose $o(a) = mn$, $m > 1$, $n > 1$

Then $o(a^m) = m$

Since order of all non identity elements in G is same, $o(a^m) = mn$

$\therefore$ $n = mn \Rightarrow m = 1$; a contradiction

$\therefore$ $o(a) = p$ = prime.

$\therefore$ $o(b) = p$ for all $e \neq b \in G$

Suppose $p \neq 2$

then $a^2 \neq e \Rightarrow a^2 \in cl(a)$

$\therefore$ $a^2 = g^{-1} ag$ for some $g \in G$

$\therefore$ $(a^2)^2 = (g^{-1} ag)^2$

$= g^{-1} a^2 g$

$= g^{-1} (g^{-1} ag)\, g$

$= g^{-2} ag^2$

$\therefore$ $a^{2^2} = g^{-2} ag^2$

In this way, we get $a^{2^p} = g^{-p} ag^p$

Since $o(g) = o(a) = p$

$a^{2^p} = eae = a$

$\Rightarrow$ $a^{2^p - 1} = e \Rightarrow o(a) = p \mid 2^p - 1$

By Fermat's Theorem, $p \mid 2^p - 2$

$\therefore$ $p \mid (2^p - 1) - (2^p - 2) = 1$, a contradiction

$\therefore$ $p = 2$

$\Rightarrow$ $o(a) = 2$. So $o(b) = 2$ for all $e \neq b \in G$

$\Rightarrow$ G is abelian.

So, every conjugate class in G is of length one. Since G has only 2 classes, order of G is 2.

(**Note:** $\exists$ infinite groups in which no non-trivial element has finite order and group has only 2 conjugate classes. Therefore, it is necessary to assume that $\exists\ e \neq a \in G$ s.t. $o(a)$ = finite, in the above problem).

Problem 26: *Prove that a group of order* 15 *is abelian. Hence, show that it is cyclic.*

Solution: Suppose G is a group of order 15. Suppose it is non-abelian. Then $Z(G) \neq G$

$\therefore\ o(Z(G)) = 1,\ 3$ or 5 as $o(Z(G)) \mid o(G) = 15$

If $o(Z(G)) = 3$ or 5, then $o\left(\frac{G}{Z}\right) = 5$ or 3 = prime

$\Rightarrow \frac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian, a contradiction. (See Page 111)

$\therefore\quad o(Z(G)) = 1$

Thus there is only one conjugate class of length one. All other classes are of length 3 or 5 as order of class divides $o(G) = 15$. If all other classes are of length 3, then by class equation,

$o(G) = 15 = 1 + 3k$, which is not true.

Therefore, there exists one class C of length 5 and this is the only class of length 5 (by class equation).

Let $x \in C$. Then $C = cl(x)$ and

$$5 = o(C) = o(cl(x)) = \frac{o(G)}{o(N(G))} \Rightarrow o(N(x)) = 3$$

Since $x \neq e$ and $x \in N(x)$, $o(x) \mid o(N(x)) = 3 \Rightarrow o(x) = 3$.

Conversely, let $o(x) = 3$. Since $o(x) \mid o(N(x))$, $o(N(x)) = 3k$ where $k = 1$ or 5 as $o(N(x)) \mid o(G) = 15$.

If $k = 5$, then $o(N(x)) = 15 = o(G) \Rightarrow N(x) = G$.

$\Rightarrow x \in Z(G) \Rightarrow x = e$ as $Z(G) = \{e\}$, a contradiction

$\therefore\quad k = 1 \Rightarrow o(N(x)) = 3$

$$\Rightarrow o(cl(x)) = \frac{o(G)}{o(N(G))} = \frac{15}{3} = 5$$

$$\Rightarrow cl(x) = C$$

as C is the only class of length 5. Since $x \in cl(x)$ we find $x \in C$.

So, the number of elements of order 3 is 5, a contradiction as number of elements of order p (p = prime) is multiple of $p - 1$ (in this case, number of elements of order 3 will be a multiple of 2)

$\therefore$ G must be abelian.

Let $e \neq x \in G$. Since $o(x) \mid o(G) = 15$, $o(x) = 3$ or 5. If all non-identity elements in G are of order 3, let $o(x) = 3$, $o(y) = 3$, $H = \langle x \rangle$, $K = \langle y \rangle$ then $o(H) = 3 = o(K)$. Since G is abelian, H is normal in G, K is normal in $G \Rightarrow HK \leq G \Rightarrow o(HK) \mid o(G) = 15$.

But $o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = \frac{3 \times 3}{1} = 9$ and $9 \nmid 15$

we get a contradiction

$\therefore \exists\ a \in G$ s.t. $o(a) = 5$. By the same argument as above $\exists\ b \in G$, s.t. $o(b) = 3$. Since $ab = ba$, $o(a)$ and $o(b)$ are relatively prime.

$$\begin{aligned} o(ab) &= o(a)\ o(b) \\ &= 3 \times 5 = 15 \\ &= o(G) \end{aligned}$$

$\therefore$ G is cyclic group of order 15.

(**Note :** We shall prove the above result again with the help of Sylow's Theorems in the next chapter).

Problem 27: *Let G be a non-trivial finite group. Let p be least prime dividing o(G). Let* $k(G) > \dfrac{o(G)}{p}$. *Then show that* $Z(G) \neq \{e\}$.

Solution: Let $Z(G) = \{e\}$. Let $o(G) = p^{\alpha} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ where $p, p_1, p_2, \ldots, p_n$ are distinct primes s.t., $p < p_1 < \ldots < p_n$, $a > 0$, $\alpha_i \geq 0$. $k(G) > \dfrac{o(G)}{p} = p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ *and* $Z(G) = \{e\} \Rightarrow \exists$ only one class of length one and at least $p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ classes of length $\geq p$ (as order of class divides $o(G)$). This gives one identity element and at least $p(p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n})$ $= p^{\alpha} p_1^{\alpha_1} \ldots p_n^{\alpha_n} = o(G)$ elements of G which exceed $o(G)$, a contradiction. Hence $Z(G) \neq \{e\}$.

Problem 28: *Let N be normal in G, a finite group. Show that* $k(G/N) \leq k(G) - j + i$, *where j = number of conjugate classes in G of elements in N.*

Solution: $G = \underset{a \in N}{\cup} cl(a) \underset{a \notin N}{\cup} cl(a) = N \underset{a \notin N}{\cup} cl(a)$

(See Exercise 10).

Let r = number of classes $cl(a)$, $a \notin N$

$\therefore \quad k(G) = j + r$

Now $cl(Nx) = \{(Ng)^{-1}\ Nx\ (Ng) \mid g \in G\}$

$= \{Ng^{-1}\ xg \mid g \in G\}$

$= \{Ny \mid y = g^{-1}\ xg,\ \ g \in G\}$

$= \{Ny \mid y = g^{-1}\ xg,\ \ g \in G\}$

$= \{Ny \mid y \in cl(x)\}$

$= Ncl(x)$

If $x \in N$, then $g^{-1}\ xg \in N$ for all $g \in G$

$\Rightarrow cl(x) \subseteq N$

$\Rightarrow Ncl(x) = N$

$\Rightarrow cl(Nx) = N$

If $x \in cl(a)$, $a \notin N$, then $cl(x) = cl(a)$

$\Rightarrow Ncl(x) = Ncl(a)$

$\Rightarrow cl(Nx) = Ncl(a)$

But there are r such classes $cl(a)$, $a \notin N$. Therefore, there are at most $r + 1$ classes in $\frac{G}{N}$.

(For, two classes $cl(a)$, $cl(b)$, $a, b \notin N$ may give rise to same class in $\frac{G}{N}$).

$$\therefore \qquad k\left(\frac{G}{N}\right) \leq r + 1 = k(G) - j + 1.$$

Definition: Let $H \leq G$. Let $g \in G$. Then $g^{-1} Hg$ is called conjugate of H in G. The set $\{g^{-1} Hg \mid g \in G\} = cl(H)$ is called *conjugate class* of H in G. As before, we can determine the order of this conjugate class.

Theorem 5: *Let $H \leq G$, G = finite group.*

Then $$o(cl(H)) = \frac{o(G)}{o(N(H))}.$$

Proof: Since $N(H) \leq G$

$$G = \bigcup_{i=1}^{t} N(H)x_i$$

where $N(H)\, x_i \cap N(H)\, x_j = \varphi$ for some $i \neq j$

Let $S = \{x_1^{-1} Hx_1, \ldots, x_t^{-1} Hx_t\}$

We show that $S = cl(H)$

Let $g^{-1} Hg \in cl(H), \quad g \in G$

$$g \in G \Rightarrow g \in N(H)x_i \quad \text{for some } i$$
$$\Rightarrow g = yx_i, \quad y \in N(H)$$
$$\Rightarrow g^{-1} Hg = x_i^{-1} y^{-1} Hyx_i$$
$$= x_i^{-1} Hx_i \quad \text{as } y \in N(H) \Rightarrow y^{-1} Hy = H$$
$$\Rightarrow g^{-1} Hg \in S$$

$\therefore \quad cl(H) \subseteq S$

Clearly, $\quad S \subseteq cl(H)$

$\therefore \quad S = cl(H).$

Also $\quad x_i^{-1} Hx_i = x_j^{-1} Hx_j$

$$\Rightarrow x_i\, x_j^{-1}\, H = Hx_i\, x_j^{-1}$$
$$\Rightarrow x_i\, x_j^{-1} \in N(H)$$
$$\Rightarrow N(H)x_i = N(H)x_j$$
$$\Rightarrow i = j$$

$\therefore \quad o(S) = t$

$$\Rightarrow o(cl(H)) = t = \frac{o(G)}{o(N(H))}.$$

Problem 29: Let $H \neq G$ *be a subgroup of a finite group G. Show that G cannot be expressed as union of conjugates of H.*

Solution: The number of conjugates of H in G is given by $\frac{o(G)}{o(N(H))}$

So
$$o(\cup x^{-1}Hx) \leq \frac{o(G)}{o(N(H))}(o(H)-1)+1$$
$$\leq \frac{o(G)}{o(H)}(o(H)-1)+1 \text{ as } H \leq N(H)$$
$$= o(G)-\frac{o(G)}{o(H)}+1$$
$$\leq o(G)-2+1 \qquad as \frac{o(G)}{o(H)} \geq 2$$
$$= o(G)-1 < o(G)$$

Thus, G cannot be written as union of conjugates of H.

Theorem (Cauchy's) 6: *Let G be a finite group and suppose p is a prime s.t.,* $p \mid o(G)$*, then* $\exists\ x \in G$ *s.t.,* $o(x) = p$.

Proof: We first prove the result when G is abelian. We prove it by induction on $n = o(G)$. Result is vacuously true when $n = 1$. Assume it to be true for all groups having order less than $o(G)$. If G has no non-trivial subgroups, then G is cyclic group of prime order. Since $p \mid o(G)$, $o(G) = p$, $G = \langle x \rangle$ s.t. $o(x) = o(G) = p$. So result follows.

Let now H be a non-trivial subgroup of G i.e. $H \neq \{e\}, G$. Since G is abelian, H is normal in G. If $p \mid o(H)$, then, by induction hypothesis as $o(H) < o(G)$, H is abelian, $\exists\ x \in H$ s.t. $o(x) = p$, $x \in H \Rightarrow x \in G$. So, result is again true.

Let $p \nmid o(H)$.

Since $o(G) = o(G/H).\ o(H)$ and $p \mid o(G)$, we find $p \mid o\left(\frac{G}{H}\right).\ o(H)$

But $p \nmid o(H)$, hence $p \mid o(G/H)$. Also $o\left(\frac{G}{H}\right) < o(G)$ as $H \neq \{e\}$ and G is abelian means $\frac{G}{H}$ is abelian.

So, by induction hypothesis $\frac{G}{H}$ has an element Hy of order p.

$$(Hy)^p = H$$
$$\Rightarrow Hy^p = H$$
$$\Rightarrow y^p \in H$$
$$\Rightarrow (y^p)^t = e \quad \text{where } t = o(H)$$
$$\Rightarrow (y^t)^p = e$$

$\Rightarrow o(y^t) \mid p$

$\Rightarrow o(y^t) = 1$ or p

If $y^t = e$ (i.e. $o(y^t) = 1$) then $Hy^t = He = H$

$\Rightarrow (Hy)^t = H$

$\Rightarrow o(Hy) \mid t$

$\Rightarrow p \mid t = o(H)$, a contradiction

$\therefore$ $o(y^t) = p$, $y^t \in G$

So result is true in this case.

By induction, result is true for all abelian groups.

Let now G be any group. We again use induction on $o(G)$. The result is vacuously true for $o(G) = 1$. Assume result is true for all groups with order less then $o(G)$. If $T < G$ and $p \mid o(T)$ then by induction hypothesis $\exists\ x \in T$ s.t. $o(x) = p$. so, result is true in this case. Assume $p \nmid o(T)$ for all $T < G$. Consider class equation of G

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

Now $a \notin Z(G) \Rightarrow N(a) < G$

$\Rightarrow p \nmid o(N(a))$

$\Rightarrow p \mid \dfrac{o(G)}{o(N(a))}$ (as $o(G) = \dfrac{o(G)}{o(N(a))} . o(N(a))$

$\Rightarrow$ $p \mid \sum_{a \notin Z(G)} \dfrac{o(G)}{o(N(a))}$

Since $p \mid o(G)$, we have $p \mid o(G) - \sum_{a \notin Z(G)} \dfrac{o(G)}{o(N(a))} = o(Z(G))$.

But $p \nmid o(T) \quad \forall\ T < G$

and $Z(G) = G \Rightarrow G$ is abelian.

But result is true for abelian groups. Hence, by induction, result is true for all groups.

Problem 30: *Show that an abelian group of order pq* (p, q *distinct primes*) *is cyclic.*

Solution: By Cauchy's theorem, $\exists\ a, b \in G$ s.t., $o(a) = p$, $o(b) = q$. Also as $(p, q) = 1$, $ab = ba$

$$o(ab) = o(a).\ o(b) = pq$$

i.e., G has an element ab of order equal to $o(G)$

Hence G is cyclic.

Remark: In view of above problem, abelian groups of order 6, 10, 15 etc., are all cyclic.

Problem 31: *Let G be a group of order 2n, where n is an odd integer (>1). Show that G is not simple.*

Solution: Let $a \in G$ be any element. Define

f_a: $G \to G$, s.t.,

$f_a(x) = ax$

then f_a is 1–1 onto map, i.e., a permutation.

Let $\bar{G}$ = set of all such permutations then $\bar{G}$ forms a group and $G \cong \bar{G}$ (See proof of Cayley's theorem).

Since $2|o(G)$, By Cauchy's theorem, $\exists$ an element $g \in G$, s.t, $o(g) = 2$, and $f_g \in \bar{G}$. When we write the permutation f_g as product of disjoint cycles, then these cycles are either 1-cycle or 2-cycle as $o(g) = 2$, i.e, $g^2 = e$

Notice $$f_g^2(x) = f_g(fg(x)) = f_g(gx) = g^2x = x = I(x)$$

$\therefore$ $$f_g^2 = I$$

Also for any 3-cycle (abc), $(abc)^2 \neq I$.

Again f_g in the cycle form cannot have any 1-cycle also, as suppose (x) is a 1-cycle then $x \to x$.

i.e., $f_g(x) = x \Rightarrow gx = x \Rightarrow g = e$

not true as $o(g) = 2$.

Hence f_g as permutation can be expressed as product of 2-cycles only. Since $o(G) = 2n$ there can be n two cycles.

So f_g can be expressed as product of n (odd) number of transpositions or that f_g is an odd permutation.

Thus set of even permutations in $\bar{G}$ has $\frac{n}{2}$ elements (See problem 49 page 148). $f_g \in \bar{G}$, f_g is odd, so $\bar{G}$ contains both odd and even permutations.

If H contains only even permutations then,

$$o(H) = \frac{o(\bar{G})}{2} \quad \Rightarrow \quad \frac{o(\bar{G})}{o(H)} = 2$$

$\Rightarrow H$ is of index 2 in $\bar{G}$ and is, therefore, normal.

Since $G \cong \bar{G}$ and $\bar{G}$ has a normal subgroup, G will have a normal subgroup or that G is not simple.

Remark: A group of order 30 is not simple as $o(\bar{G}) = 30 = 2.15$. We can clearly have so many examples of groups which are not simple by using the above result.

Similar Permutations

Two permutations σ and $\eta \in S_n$ are called similar if they have same cycle structure when decomposed as product of disjoint cycles.

For example, $\sigma = (12)(345) \in S_5$

and $\eta = (123)(45) \in S_5$

are similar as σ has 1 cycle of length 2 and 1 cycle of length 3 same as η.

However $\sigma = (12)(34)$, $\eta = (1234)$ are not similar in S_4 as σ has 2 cycles of length 2 and η has no cycle of length 2.

Note: We talk of similar permutations only when they have been represented as product of disjoint cycles.

Theorem 7: *Two permutations $\sigma, \eta \in S_n$ are similar if and only if they are conjugate in S_n.*

Proof: Suppose $\sigma, \eta \in S_n$ are similar

Let $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$

$\eta = (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

where $n_1 + n_2 + \ldots + n_k = n$

Define $\theta = \begin{pmatrix} a_1 & \ldots & a_{n_1} & \ldots & b_1 & \ldots & b_{n_k} \\ a_1' & \ldots & a'_{n_1} & \ldots & b_1' & \ldots & b'_{n_k} \end{pmatrix}$

Then $\theta \in S_n$

and $\theta \sigma \theta^{-1} = (\theta a_1 \ldots \theta a_{n_1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$

$= (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

$= \eta$

$\therefore$ σ, η are conjugate in S_n

Conversely, suppose σ, η are conjugate in S_n.

Then $\exists\ \theta \in S_n$ s.t. $\theta\sigma\theta^{-1} = \eta$

Let $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$

Then $\eta = \theta\sigma\theta^{-1} = (\theta a_1 \ldots \theta a_{n_1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$

So σ, η are similar.

Partition of an Integer

Let n be a positive integer. A sequence of positive integers $n_1, n_2, \ldots, n_k$, where $n_1 \le n_2 \le \ldots \le n_k$, such that $n = n_1 + n_2 + \ldots + n_k$ is called a partition of n and $n_1, n_2, \ldots, n_k$ are called parts of the partition.

For example, let $n = 3$. Then $3 = 1 + 1 + 1$, $3 = 1 + 2$, $3 = 3$ are all partitions of $n = 3$. This gives 3 partitions of n. Also $n = 4$ has 5 partitions namely, $4 = 1 + 1 + 1 + 1$, $4 = 1 + 1 + 2$, $4 = 1 + 3$, $4 = 2 + 2$, $4 = 4$.

The number of partitions of n is denoted by $p(n)$. So $p(3) = 3$, $p(4) = 5$ etc.

Theorem 8: *The number of conjugate classes in S_n is $p(n)$.*

Proof: Let $\mathscr{A}$ = Set of all conjugate classes in S_n.

$\mathscr{B}$ = Set of all partitions of n.

Consider $cl(\sigma)$, $\sigma \in S_n$.

Let $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$ as product of disjoint cycles. Here

$n_1 + \ldots + n_k = n$.

We arrange cycles in such a way that $n_1 \le \ldots \le n_k$. This gives a partition

$\{n_1, n_2, ..., n_k\}$ of n.

Define $f : \mathscr{A} \to \mathscr{B}$, s.t.,

$f(cl(\sigma)) = \{n_1, n_2, ..., n_k\}$

f is well defined as $cl(\sigma) = cl(\eta)$

$\Rightarrow \sigma, \eta \in cl(\sigma)$

$\Rightarrow \sigma, \eta$ are conjugate in S_n

$\Rightarrow \sigma, \eta$ are similar in S_n

$\Rightarrow \sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$

$\eta = (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

$\Rightarrow f(cl(\sigma)) = \{n_1, ..., n_k\} = f(cl(\eta))$

Suppose $cl(\sigma) \neq cl(\eta)$

Then σ and η are not conjugate and so not similar

$\Rightarrow \sigma, \eta$ have different cycle structure

$\Rightarrow$ the corresponding partitions are different.

i.e., $\{n_1, n_2, ..., n_k\} \neq \{n'_1, n'_2, ..., n'_r\}$ where, of course,

$n = n_1 + n_2 + ... + n_k = n'_1 + n'_2 + ... + n'_r$

$\Rightarrow f(cl(\sigma) \neq f(cl(\eta)$

$\Rightarrow f$ is 1–1

f is onto for, let $\{n_1, ..., n_k\} \in \mathscr{B}$ be a partition of n. Then $n = n_1 + ... + n_k$.

Define $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k}) \in S_n$

Then $cl(\sigma) \in \mathscr{A}$

and $f(cl(\sigma)) = \{n_1, ..., n_k\}$

$\therefore f$ is both 1–1 and onto.

So, $o(\mathscr{A}) = o(\mathscr{B}) = p(n)$

$\Rightarrow$ number of conjugate classes in S_n is $p(n)$.

Problem 32: *Find all the conjugate classes in S_4 and verify the class equation.*

Solution: We know that the number of conjugate classes in S_n is $p(n)$, the number of partitions of n. Thus number of conjugate classes in S_4 will be $p(4) = 5$.

Also we know that two permutations are conjugate iff they are similar.

Thus the base elements of the different conjugate classes will be

I, (12), (123), (1234), (12)(34)

Since number of distinct 2-cycles in S_4 is $\frac{1}{2}\frac{\lfloor 4}{\lfloor 4-2} = 6$ (See problem 57 on page 152).

We find $o(cl(12)) = 6$ and its members are the 2-cycles (12), (13), (14), (23), (34), (24)

Similarly, number of distinct 3-cycles and 4-cycles are 8 and 6 respectively.

So $o(cl(123)) = 8$, $o(cl(1234)) = 6$

Since permutations of the type

$(ab)(cd)$ are (12)(34), (13)(24), (14)(23)

$o(cl(12)(34)) = 3$

Now $Z(S_4) = \{I\} \Rightarrow o(Z(S_4)) = 1$

$\Rightarrow o(cl(I)) = 1$

So the class equation

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$= o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

is verified as

$$24 = 1 + 6 + 8 + 6 + 3.$$

Problem 33: *Let* $(12) \in S_n$. *Determine all elements in* S_n *which commute with* (12).

Solution: Let $\sigma \in S_n$ s.t. $\sigma(1) = 1$, $\sigma(2) = 2$.

Then $\sigma(12)\,\sigma^{-1} = (\sigma 1 \sigma 2) = (12)$

$\Rightarrow \sigma(12) = (12)\,\sigma$

The number of such $\sigma \in S_n$ is clearly $(n-2)!$ (as $\sigma(1) = 1$, $\sigma(2) = 2$, σ will take remaining $n-2$ letters among themselves and so σ will be a permutation on $n-2$ letters).

Also, $\eta = \sigma(12) \in S_n$

and $\eta(12)\,\eta^{-1} = (\eta 1 \eta 2) = (21) = (12)$

$\Rightarrow \eta(12) = (12)\,\eta$

The number of $\eta s \in S_n$ is equal to the number of $\sigma \in S_n$ $(= (n-2)!)$

This gives $2(n-2)!$ distinct permutations in S_n commuting with (12).

Now $$o(cl(12)) = \frac{o(S_n)}{o(N(12))} = \frac{n!}{o(N(12))}$$

But $cl(12)$ is the set of those permutations in S_n which are conjugate (or similar) to (12).

$\therefore$ $o(cl(12))$ = number of cycles of length 2 in S_n.

Since (12) = (21) and the first place can be chosen in n ways, second in $n-1$ ways, we have $n(n-1)$ cycles of length 2 but each such cycle is counted twice, we get $\frac{n(n-1)}{2}$ distinct cycles of length 2.

$\therefore$ $$o(cl(12)) = \frac{n(n-1)}{2}$$

$\therefore$ $$(N(12)) = \frac{2n!}{n(n-1)} = 2\,(n-2)!$$

$\therefore$ $N(12) = \{\sigma, \sigma(12) \mid \sigma(1) = 1, \sigma(2) = 2, \sigma \in S_n\}$

= set of all permutations is S_n commuting with (12).

Problem 34: *Find all permutations in* $S_n (n \geq 4)$ *which commute with* $\sigma = (12)(34)$.

Solution: $\sigma = (12)(34)$ can be written in 8 ways in S_n as follows

$(12)(34), (21)(34), (21)(43), (12)(43)$

$(34)(12), (34)(21), (43)(21), (43)(12)$

The 1st place in σ can be chosen in n ways, 2nd in $n-1$, 3rd in $n-2$ and 4th in $n-3$ ways. This gives $n(n-1)(n-2)(n-3)$ ways in which σ can be chosen. As σ can be written in 8 ways, the number of permutations in S_n similar to σ is equal to $\frac{n(n-1)(n-2)(n-3)}{8}$ $= o(cl(\sigma))$

$$\therefore \quad o(N(\sigma)) = \frac{o(G)}{o(cl(\sigma))} = \frac{8n!}{n(n-1)(n-2)(n-3)}$$

Let $\tau \in S_n$ s.t. τ fixes 1, 2, 3, 4.

Then $\tau\sigma\tau^{-1} = (\tau 1\ \tau 2)(\tau 3\ \tau 4) = (12)(34) = \sigma$

$\therefore \quad \sigma\tau = \tau\sigma$

The number of $\tau \in S_n$ is $(n-4)!$. Clearly $\tau(12)$, $\tau(34)$, $\tau(12)(34)$ $\tau(13)(24)$, $\tau(14)(23)$, $\tau(1324)$, $\tau(1423)$

Commute with σ and the number of each such permutations

= number of $\tau \in S_n$ $(= (n-4)!)$.

So, we get $8(n-4)!$ permutations in S_n which commute with σ. Since $o(N(\sigma)) = 8(n-4)!$, these are the only permutations in S_n which commute with σ.

Problem 35: *Find two permutations in* A_5 *which are similar but not conjugate in* A_5.

Solution: Let $\sigma = (12345) \in A_5$

$\eta = (13245) \in A_5$

Since σ, η are cycles of length 5, these are similar permutations.

If σ, η are conjugate in A_5, then $\exists\ \theta \in A_5$ s.t. $\theta\sigma\theta^{-1} = \eta$

$\therefore \quad (\theta 1\ \theta 2\ \theta 3\ \theta 4\ \theta 5) = (13245)$

Since (13245) can be written in 5 ways, there are 5 cases.

Case 1: $\theta 1 = 1, \theta 2 = 3, \theta 3 = 2, \theta 4 = 4, \theta 5 = 5$

$\therefore \quad \theta = (23) \notin A_5$

Case 2: $\theta 1 = 3, \theta 2 = 2, \theta 3 = 4, \theta 4 = 5, \theta 5 = 1$

$\therefore \quad \theta = (1345) = (15)(14)(13) \notin A_5$

Case 3: $\theta 1 = 2, \theta 2 = 4, \theta 3 = 5, \theta 4 = 1, \theta 5 = 3$

$\therefore \quad \theta = (124)(35) = (14)(12)(35) \notin A_5$

Case 4: $\theta 1 = 4, \theta 2 = 5, \theta 3 = 1, \theta 4 = 3, \theta 5 = 2$

$\therefore \quad \theta = (143)(25) = (13)(14)(25) \notin A_5$

Case 5: $\theta 1 = 5, \theta 2 = 1, \theta 3 = 3, \theta 4 = 2, \theta 5 = 4$

$\therefore \quad \theta = (1542) = (12)(14)(15) \notin A_5$

So in each case we get a contradiction.

Hence σ, η are not conjugate in A_5.

Remark: Two conjugate permutations would always be similar.

Problem 36: *Find all permutations in A_5 which commute with*

(*i*) $\sigma = (12345)$ (*ii*) $\tau = (123)$ (*iii*) $\eta = (12)(34)$

Solution: (*i*) By Exercise 13, $\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = I$ are permutations in S_5 commuting with σ. Since $\sigma \in A_5$, all powers of σ belong to A_5.

$\therefore\ o(N(\sigma)) = 5$ in A_5.

$$\therefore\ o(cl(\sigma)) = \frac{o(A_5)}{o(N(\sigma))} = \frac{60}{5} = 12 \text{ in } A_5$$

$\therefore$ (12345) and (13245) break up into two conjugate classes each of length 12 in A_5.

(*ii*) Let $\theta \in S_5$ s.t. θ fixes 1, 2, 3. Then either $\theta = (45)$ or $\theta = I$. By Exercise 14, $\tau\theta, \tau^2\theta, \theta$ are all permutations in S_5 commuting with τ. Thus τ, τ^2, I are the only permutations in A_5 commuting with τ.

$\therefore\ o(N(\tau)) = 3$ in A_5

$\therefore\ o(cl(\tau)) = 20$ in A_5

$\therefore\ cl(\tau)$ has all cycles of length 3 in S_5.

(*iii*) By problem 34, there are 8 permutations in S_5 commuting with η. These are

I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423). Among these I, (12)(34), (13)(24), (14)(23) $\in A_5$.

$\therefore$ these are all permutations in A_5 commuting with η.

$o(N(\eta)) = 4$ in A_5

So, $o(cl(\eta)) = 15$ in A_5 which is same as $o(cl(\eta))$ in S_5.

$\therefore$ Conjugate class of η remains same in A_5 and S_5.

Problem 37: *Determine all the conjugate classes of A_5.*

Solution: By problem 36, A_5 has 5 conjugate classes. $cl(I) = \{I\}$,

$cl((123)) = \{$all 20 cycles of length 3$\}$,

$cl((12)(34)) = \{$all 15 permutations similar to (12)(34)$\}$,

$cl((12345)) = \{$12 cycles of length 5$\}$,

$cl((13245)) = \{$12 cycles of length 5$\}$.

This gives 60 elements in A_5 and so all classes in A_5.

Problem 38: *Show that A_5 is simple.*

Solution: Let N be normal in A_5, $N \neq \{I\}$, $N \neq A_5$. By Exercise 10, N = union of some conjugate classes in A_5. Since $I \in N$, $o(N)$ can't divide $o(A_5) = 60$. Thus A_5 is simple.

Problem 39: *Show that A_5 is the only non trivial proper normal subgroup of S_5.*

Solution: Let H be any non trivial, proper normal subgroup of S_5. Then

$$H \neq \{I\},\ H \neq S_5,\ H \trianglelefteq S_5$$

Now $H \cap A_5 \leq A_5$, we show it is normal.

Let $x \in H \cap A_5,\ g \in A_5$, then

$g^{-1}xg \in A_5$

and $x \in H,\ g \in A_5 \subseteq S_5 \Rightarrow g^{-1}xg \in H$ as $H \trianglelefteq S_5$

$\therefore$ $g^{-1}xg \in H \cap A_5 \Rightarrow H \cap A_5 \trianglelefteq A_5$

But, A_5 is simple, thus either $H \cap A_5 = \{e\}$ or $H \cap A_5 = A_5$

Suppose $H \cap A_5 = \{I\}$, then $o(H \cap A_5) = 1$

and thus $o(HA_5) = \dfrac{o(H) \cdot o(A_5)}{1}$

Since $H \trianglelefteq S_5,\ A_5 \trianglelefteq S_5$,

we have $HA_5 \leq S_5$

$\Rightarrow o(HA_5) | o(S_5)$

$\Rightarrow o(H).o(A_5) | o(S_5)$

$\Rightarrow o(H).o(A_5) | 2.o(A_5)$

$\Rightarrow o(H) | 2 \Rightarrow o(H) = 1$ or 2

But $H \neq \{I\}$ i.e., $o(H) \neq 1$ and so $o(H) = 2$

Again, $H \subseteq Z(S_5)$ [See problem 3 on page 102]

and as $Z(S_5) = \{I\}$. We get a contradiction.

Hence $H \cap A_5 \neq \{I\}$ and so $H \cap A_5 = A_5$

$\Rightarrow A_5 \subseteq H \Rightarrow o(A_5) | o(H)$

Also $o(H) | o(S_5)$

ie., $60 | o(H) | 120$ and $o(H) \neq 120$ as $H \neq S_5$

$o(H) = 60 = o(A_5),\ A_5 \subseteq H$

or that $H = A_5$.

Aliter: Let H be a non trivial proper normal subgroup of S_5. If H has an odd premutation then the number of even permutations in H is equal to the number of odd permutations in H. Let K be the set of all even permutations in H. Then

$$K \subseteq A_5$$

Let $g \in A_5,\ k \in K$, then $g^{-1}kg$ is an even permutation. Since H is normal in S_5. $g^{-1}\,kg \in H$. So $g^{-1}kg$ is an even permutation in H.

$$\Rightarrow g^{-1}kg \in K \Rightarrow K \text{ is normal in } A_5.$$

But A_5 is simple, so either $K = A_5$ or $K = \{I\}$

If $K = \{I\}$ then H has only one odd permutations $\Rightarrow o(H) = 2$ which means that $H \subseteq Z(S_5) = \{\text{I}\}$ a contradiction

So $K = A_5$, i.e., $A_5 \subseteq H$

But, $H \subseteq A_5$ (See note on page 148)

Hence $H = A_5$

Exercises

1. Let G be non-abelian group. Show that for all $x \in G$, $Z(G) < N(x)$.

2. Let X be a conjugate class of elements in G and let $\overline{X} = \{x^{-1} \mid x \in X\}$. Show that $\overline{X}$ is a conjugate class of elements in G.

3. Find all the conjugate classes of S_3 and verify the class equation.

4. Find which of the following permutations in S_6 are conjugate

(i) $x = (12)(456)$, $y = (345)$

(ii) $x = (14)(23)$, $y = (53)(16)$

and if x, y are conjugate, find z s.t., $zxz^{-1} = y$

5. Suppose that G is finite. Prove that if $o(G)$ is odd, then $\{e\}$ is the only conjugate class X such that $X = \overline{X}$. If $o(G)$ is even, show that $\exists$ at least one conjugate class $X \neq \{e\}$ such that $X = \overline{X}$.

6. Prove that if G is a finite group with $k(G)$ even, then $o(G)$ is a even.

7. Let G be a finite group. Show that $k(G) = 2$ if and only if G is cyclic group of order 2.

8. Let G be a finite non-abelian group. Show that $k(G) > o(Z(G)) + 1$.

9. Let N be normal in G. Show that either $cl(a) \cap N = \varphi$ or $cl(a) \subseteq N$ for all $a \in G$.

10. Let $N \leq G$. Show that N is normal in G if and only if $N = \underset{a \in N}{\cup} cl(a)$.

11. Let $o(G) = p^n$, p being a prime and $n > 0$. Let N be normal in G, ($N \neq \{e\}$). Show that $N \cap Z(G) \neq \{e\}$.

12. If G is finite non-abelian group such that $\dfrac{G}{Z(G)}$ is abelian, then show that

$$k(G) \geq o\left(\frac{G}{Z(G)}\right) + o(Z(G)) - 1.$$ (**Hint** : Use Problem 28)

13. Show that permutations in S_n commuting with $\sigma = (1\ 2\ \ldots,\ n)$ are

$$\sigma,\ \sigma^2,\ldots,\ \sigma^{n-1},\ \sigma^n = I.$$

14. Show that permutations in S_n commuting with $\sigma = (1\ 2\ \ldots,\ r)$, $1 < r \leq n$, are τ, $\sigma\tau$, $\sigma^2\tau$, ..., $\sigma^{r-1}\tau$ where τ fixes 1, 2,..., r.

A Quick Look at what's been done

- An isomorphism from a group G to itself is called an **automorphism** of G. The set of all automorphisms of G is denoted by Aut G, which itself forms a group.
- Automorphism under which x is mapped to axa^{-1} for any a in G is called an **inner automorphism.** If $I(G)$ denotes the set of all inner automorphisms of G then $I(G)$ is a normal subgroup of Aut G, where Aut G is a subgroup *of* $A(G)$ the group of permutations on G.
- If $Z(G)$ denotes the centre of G then $G/Z(G) \cong I(G)$.
- If G is a finite cyclic group of order n then Aut G is isomorphic to U_n, the group under multiplication modulo n.
- Aut S_3 is isomorphic to S_3.
- A subgroup H of a group G is called a **characteristic subgroup** of G if $T(H) \subseteq H$ for all $T \in$ Aut G.
- Two elements a,b of a group G are called **conjugate** if $\exists$ some $c \in G$ s.t., $a = c^{-1}bc$. This relation is an equivalence relation, giving us equivalence classes. Here, $cl(a) = \{a\}$ iff $a \in Z(G)$.
- If G is a finite group, $a \in G$, then $o(cl(a)) = o(G)/o(N(a))$, where $N(a)$ denotes the **normalizer** of a.
- The **class equation** of a group G is given by $o(G) = o(Z(G)) + \sum o(G)/o(N(a))$, where $a \notin Z(G)$
- **Cauchy's theorem** for groups states that if G is a finite group and p is a prime dividing $o(G)$, then $\exists$ some $x \in G$ s.t., $o(x) = p$.
- Two permutations are similar iff they are conjugate, where by similar permutations we mean two permutations, which have the same cycle structure when expressed as product of disjoint cycles.
- A_5 is simple.

5

Sylow Theorems and Direct Products

Introduction

In this chapter we plan to discuss p-groups, Sylow's three theorems and their applications. The ideas developed are so useful that plenty can be known about the nature of a group by knowing only its order. Direct products of groups with applications and the Fundamental theorem of finite abelian groups are taken up at the end.

Definition: A p-group is a group in which every element has order p^r where p = prime. Here p is same for all elements and r may vary.

The group $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ and the Quaternion group are examples of finite p-groups. Here $p = 2$. For example of an infinite p-group, see problem 20 on page 113.

S_3 is not a p-group.

Since we shall mainly be studying finite groups, the following result will be useful.

Theorem 1: *Let G be a finite group. Then G is a p-group if and only if $o(G) = p^n$.*

Proof: Suppose G is a p-group. Let q be a prime dividing $o(G)$. By Cauchy's theorem $\exists\, x \in G$ s.t. $o(x) = q$. But $o(x) = p^r$ as G is a p-group.

$\therefore\ q = p^r \Rightarrow q = p$. So, p is the only prime dividing $o(G)$. Thus $o(G) = p^n$.

Conversely, let $o(G) = p^n$ (p = prime).

Let $x \in G$. Then $o(x) \mid o(G) = p^n \Rightarrow o(x) = p^r$.

$\therefore$ every element of G has order which is some power of p. So, G is a p-group.

Remarks:

(i) Any finite p-group has non-trivial centre. (See problem 20, page 186)

(ii) A p-group may or may not be abelian. See examples above.

Problem 1: *Let G be a finite group with the property that if H, K are two subgroups of G then either $H \subseteq K$ or $K \subseteq H$. Show that G is a cyclic p-group.*

Solution: If G has no proper subgroups then G is a cyclic group of prime order and thus the result holds.

Suppose now G has a proper subgroup $H(\neq G)$.

We first show that G will be cyclic.

Since $H \underset{\neq}{\subset} G, \exists\ x \in G$, s.t., $x \notin H$.

Let $K = \langle x \rangle$, then $K \not\subseteq H$ as $x \in K$, $x \notin H$

Thus, by given condition, $H \subseteq K$

If $K = G$ then G is cyclic (as K is cyclic)

Suppose $K \neq G$ then $\exists\ y \in G$ s.t., $y \notin K$

Let $L = \langle y \rangle$ then $L \not\subseteq K$ and by given condition $K \subseteq L$

If $L = G$, G will be cyclic, if $L \neq G$ proceed as above and as G is finite, after a finite number of steps, we find G will be cyclic.

To show that G is a p-group, suppose $p \neq q$ are two primes which divide $o(G)$. Since G is cyclic, $\exists$ subgroups H and K of G with $o(H) = p$, $o(K) = q$ (coverse of Lagrange's theorem holds in cyclic groups)

Now $H \not\subseteq K$ as $o(H) \nmid o(K)$

$K \not\subseteq H$ as $o(K) \nmid o(H)$

a contradiction to the given condition.

Hence there can be only be one prime dividing $o(G)$ or that G is a p-group.

The converse of the above problem also holds as can be seen by

Problem 2: *Let G be a finite cyclic p-group. Show that if H and K be any two subgroups of G then either $H \subseteq K$ or $K \subseteq H$.*

Solution: Let $G = \langle a \rangle$, then $o(G) = o(a) = p^n$ for some prime p.

Let H be a subgroup of G, then H is cyclic.

Let $H = \langle a^m \rangle$.

Let d = g.c.d. (m, p^n)

Then $d = mx + p^n y$ for some integers x and y

Now $a^d = a^{mx+p^n y} = a^{mx} \cdot a^{p^n y} = (a^m)^x \in H$ [as $o(a) = p^n$]

Thus $\langle a^d \rangle \subseteq H$

Again as $d \mid m, \quad m = dq$

So $a^m = (a^d)^q \in \langle a^d \rangle$

or that $H = \langle a^m \rangle \subseteq \langle a^d \rangle$

and hence $H = \langle a^d \rangle$ where $d \mid p^n$

and so $H = \left\langle a^{p^i} \right\rangle$

Let K be another subgroup of G, then $K = \left\langle a^{p^k} \right\rangle$. Suppose $i \geq k$ and let $i = k + t$ where $t \geq 0$ is an integer

Now $a^{p^i} = a^{p^{k+t}} = \left(a^{p^k}\right)^{p^t} \in K$

which implies $H = \left\langle a^{p^i} \right\rangle \subseteq K$

If $k \geq i$, then $K \subseteq H$

which proves the result.

Problem 3: *In a finite p-group G, every proper subgroup is a proper subgroup of its normaliser in G.* (*In other words, if* $o(G) = p^n$, $H \leq G$, $H \neq G$, *then* $\exists\ g \in G$, $g \notin H$, s.t. $gHg^{-1} = H$).

Solution: We prove the result by induction on n. Let $n = 1$. Then $o(G) = p$. Since

$$H \neq G,\ o(H) = 1.$$

$\therefore\ H = \{e\}$ or $gHg^{-1} = g\{e\}g^{-1} = \{e\} = H$ for all $e \neq g \in G$.

$$g \neq e \Rightarrow g \notin H.$$

Thus result is true for $n = 1$. Assume it to be true for all groups having order less than p^n. Let $o(G) = p^n$. Suppose $H = N(H)$.

Since $Z(G) \subseteq N(H) = H$, $H \neq G$

$\frac{H}{Z(G)}$ is a proper subgroup of $\frac{G}{Z(G)}$

Now $o\left(\frac{G}{Z(G)}\right) = p^m,\ m < n$

(as $o(Z(G)) > 1$ by problem 20, page 186)

For convenience, we write $Z(G) = N$, then by induction hypothesis, $\exists\ Ng \in \frac{G}{N}$, $Ng \notin \frac{H}{N}$, s.t.,

$$Ng\ \frac{H}{N}\ (Ng)^{-1} = \frac{H}{N}$$

$$\Rightarrow Ng\ Nh\ Ng^{-1} \in \frac{H}{N} \quad \forall\ h \in H$$

$$\Rightarrow Nghg^{-1} \in \frac{H}{N} \quad \forall\ h \in H$$

$$\Rightarrow Nghg^{-1} = Nh_1 \quad \text{for some } h_1 \in H$$

$$\Rightarrow ghg^{-1}h_1^{-1} \in N = Z(G) \subseteq H$$

$$\Rightarrow ghg^{-1} \in H \quad \forall\ h \in H$$

$$\Rightarrow gHg^{-1} \subseteq H$$

$$\Rightarrow gHg^{-1} = H \text{ as } o(gHg^{-1}) = o(H)$$

Thus $g \in N(H)$ and as $Ng \notin \frac{H}{N}$, $g \notin H$, or that $N(H) \neq H$, a contradiction. Hence $H \subset N(H)$.

Thus result is true for n also.

By induction, result is true for all $n \geq 1$.

Problem 4: *Let* $o(G) = p^n$ (p = *prime*). *If* $H \leq G$ *s.t.* $o(H) = p^{n-1}$, *show that* H *is normal in* G.

Solution: Now $H \subseteq N(H) \subseteq G$

Since $o(H) = p^{n-1} \mid o(N(H)) \mid o(G) = p^n$

$o(N(H)) = p^{n-1}$ or p^n

If $o(N(H)) = p^n = o(G)$,

then $N(H) = G$

and so H is normal in G.

If $o(N(H)) = p^{n-1}$,

then $N(H) = H$

Since $Z(G) \subseteq N(H) = H$

$$o\left(\frac{H}{Z(G)}\right) = p^{n-1-m}, \text{ where } o(Z(G)) = p^m,\ m > 0$$

and $$o\left(\frac{G}{Z(G)}\right) = p^{n-m},$$

We now prove the result by induction on n. When $n = 1$, $H = \{e\}$ and so H is normal in G. Assume result to be true for all p-groups with order less then $o(G)$. Here $\frac{G}{Z(G)}$ is a p-group s.t. $o\left(\frac{G}{Z(G)}\right) = p^{n-m}$, $n - m < n$ (as $m > 0$) and $o\left(\frac{H}{Z(G)}\right) = p^{n-m-1}$. By induction hypothesis, $\frac{H}{Z(G)}$ is normal is $\frac{G}{Z(G)} \Rightarrow H$ is normal in G. So $N(H) = G \Rightarrow H = G$, a contradiction. Thus $o(N(H)) \neq p^{n-1}$. So result is true for n also. By induction, result is true for all $n > 0$.

Remark: This problem follows by problem 3 also as

$o(H) \mid o(N(H)) \mid o(G)$ gives

$o(N(H)) = p^{n-1}$ or p^n

$o(N(H)) = p^n \Rightarrow N(H) = G \Rightarrow H$ is normal in G.

$o(N(H)) = p^{n-1}$ is not possible as $H < G$, thus $H < N(H)$ by problem 1.

Problem 5: *Let G be a finite p-group of order* p^m. *Show that G has normal subgroups* $G_0, G_1, \ldots G_m$ *s.t.*

$$\{e\} = G_0 < G_1 < \ldots < G_{m-1} < G_m = G$$

and $o(G_i) = p^i$ *for all* $i = 0, 1, \ldots, m$.

Solution: We prove the result by induction on m. The result is clearly true for $m = 0, 1$. Assume it to be true for all p-groups with order less than $o(G)$.

Let $o(G) = p^m$, $m > 1$.

Let $e \neq z \in Z(G)$.

Let $o(z) = p^n$, $n > 0$.

Let $G_1 = \langle z^{p^{n-1}} \rangle \leq Z(G)$

Then $o(G_1) = p$ and G_1 is normal in G.

Let $\bar{G} = \dfrac{G}{G_1}$.

then $o(\bar{G}) = p^{m-1}$.

By induction hypothesis $\bar{G}$ has normal subgroups $\bar{G}_i$ (i = 0, 1..., m – 1) s.t.,

$$\{e\} = \bar{G}_0 < \bar{G}_1 < \ldots < \bar{G}_{m-1} = \bar{G}$$

where $o(\bar{G}_i) = p^i$ for all i

But $\bar{G}_i < \bar{G} \Rightarrow \bar{G}_i = \dfrac{G_{i+1}}{G_1}$ where $G_1 < G_{i+1}$.

Since $\bar{G}_i = \dfrac{G_{i+1}}{G_1}$ is normal in $\bar{G} = \dfrac{G}{G_1}$, G_{i+1} is normal in G for all i.

$\therefore$ $G_1 < G_2 < \ldots < G_m = G$

and $o(G_{i+1}) = p^{i+1}$

Since $G_0 = \{e\}$, the subgroups G_0, G_1,..., G_m are the required subgroups. So result is true for m. By induction result is true for all $m \geq 0$.

Problem 6: *If G is a finite non abelian p-group then show that* $p^2 \mid o(Aut\ G)$

Solution: Since G is a p-group. $o(Z(G)) > 1$ (See problem 20 page 186)

Suppose $o(G) = p^n$ and let $o(Z(G)) = p^m$

Since G is non abelian, $o(Z(G)) < o(G)$, thus $m < n$ and also $m \geq 1$.

Thus $$o\left(\frac{G}{Z(G)}\right) = p^{n-m}, \quad n - m \geq 1$$

If $n - m = 1$ then $o\left(\dfrac{G}{Z(G)}\right) = p \Rightarrow \dfrac{G}{Z(G)}$ is cyclic.

$\Rightarrow G$ is abelian (See problem 18, page 111)

which is not true. Hence $n - m \geq 2$

Again $$\frac{G}{Z(G)} \cong I(G) \Rightarrow o\left(\frac{G}{Z(G)}\right) = o(I(G))$$

$\Rightarrow p^2$ divides $o(I(G))$

and as $I(G) \leq$ Aut G we find $p^2 \mid o(\text{Aut } G)$.

We now prove the converse of Lagrange's Theorem for finite abelian groups.

Theorem 2: *Let G be an abelian group of order n. Then for every divisor m of n, G has a subgroup of order m.*

Proof: We prove the result by induction on n. When $n = 1$, $G = \{e\}$ and so result is clearly true for $n = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $o(G) = n$, $m \mid n$, $m > 1$. Let p be a prime dividing m. So, $p \mid n = o(G)$. By Cauchy's Theorem $\exists\ x \in G$ s.t. $o(x) = p$. Let $K = \langle x \rangle$.

Then $o(K) = o(x) = p$. Since G is abelian, K is normal in G.

Now $o\left(\frac{G}{K}\right) = \frac{n}{p} < n$. Also $\frac{G}{K}$ is abelian. Let $m = pm_1$.

Now $m = pm_1 \mid o(G) = o\left(\frac{G}{K}\right) o(K)$

$\Rightarrow m_1 \mid o\left(\frac{G}{K}\right)$

By induction hypothesis $\exists$ subgroup $\frac{H}{K}$ of $\frac{G}{K}$ s.t. $o\left(\frac{H}{K}\right) = m_1$. $H \leq G$.

$\therefore$ $o(H) = o(K)m_1 = pm_1 = m$

So, result is true in this case also. Hence by induction, theorem is proved.

Cor. : Converse of Lagrange's theorem holds in finite cyclic groups. (A result, we proved earlier also)

Remark: In case of finite cyclic groups we notice its not only that converse of Lagrange's theorem holds but for each divisor of $o(G)$ there exists a unique subgroup (See page 85). This is, however, not essentially true in finite abelian groups. For instance, in $K_4 = \{e, a, b, c\}$ there are three subgroups of order 2.

Sylow *p*-subgroups

Let p be a prime s.t. p^n divides order of a group G and p^{n+1} does not divide it. Then a subgroup H of G s.t. $o(H) = p^n$ is called a Sylow p-subgroup of G or p-Sylow subgroup of G.

We now discuss three theorems due to Sylow called Sylow's theorems. First theorem shows the existence of a Sylow p-subgroup of G for every prime p dividing $o(G)$ while second theorem shows that any two Sylow p-subgroups of G are conjugate. The third theorem gives the number of Sylow p-subgroups of G.

Our next theorem is a partial converse to Lagrange's theorem.

Theorem 3 (Sylow's First Theorem): *Let p be a prime and m, a +ve integer s.t. p^m divides o(G). Then $\exists$ a subgroup H of G s.t. $o(H) = p^m$.*

Proof: We prove the theorem by induction on $o(G)$. Result is vacuously true when $o(G) = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $p^m \mid o(G)$. If K is a subgroup of G s.t. $K \neq G$ and $p^m \mid o(K)$, then by induction $\exists\ H \leq K$ s.t., $o(H) = p^m$. $H \leq K \Rightarrow H \leq G$. So result holds in this case. Assume p^m does not divide order of any proper subgroup of G. Consider class equation of G.

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$a \notin Z(G) \Rightarrow N(a) \neq G \Rightarrow p^m \nmid o(N(a))$$

But $$p^m \mid o(G) \Rightarrow p^m \mid \frac{o(G)}{o(N(a))} . o(N(a))$$

$$\Rightarrow \; p \mid \frac{o(G)}{o(N(a))} \text{ for all } a \notin Z(G)) \text{ as } p^m \nmid o(N(a))$$

$$\Rightarrow \; p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$\Rightarrow \; p \mid o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} = o(Z(G))$$

$$\Rightarrow \exists\, x \in Z(G) \text{ s.t. } o(x) = p$$

Let $K = \langle x \rangle \subseteq Z(G) \Rightarrow K$ is normal in G.

Now $o(G/K) < o(G)$ and $p^m \mid o(G) = o(G/K).\, o(K)$, $p^m \nmid o(K)$ and thus $p^{m-1} \mid p^m \mid o(G/K)$. (Notice in case $m = 1$, the result follows by Cauchy's theorem).

By induction hypothesis $\exists$ a subgroup $\frac{H}{K}$ of $\frac{G}{K}$ s.t. $o\left(\frac{H}{K}\right) = p^{m-1}$.

$\therefore$ $$o(H) = p^m, \; \frac{H}{K} \leq \frac{G}{K} \Rightarrow H \leq G$$

Thus result is true in this case also.

Hence by induction the theorem follows.

Remark: Suppose G is a group of order $2^3.3^2.5$ then Sylow's First theorem says that G has at least one subgroup each of order 2, 2^2, 2^3, 3, 3^2, 5. But the theorem does not say anything about the group G having a subgroup of order 6, 10, 15 or any other divisor of $o(G)$ that has two or more distinct prime factors.

In view of theorems 2 and 3 above we observe that converse of Lagrange's theorem holds for all finite abelian groups and all finite groups of prime-power order.

Cor.: If p is a prime s.t. $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$, then a $\exists$ Sylow p-subgroup of G.

Proof: Take $m = n$ and use the above theorem.

Thus if $o(G) = 2^3.3^2.5$, any subgroup of order 8 will be a Sylow 2-subgroup and any subgroup of order 9 will be a sylow 3-subgroup of G and so on.

Remark: Sometimes the statement of this corollary is taken as Sylow's first theorem. In fact, another (more general) version of the theorem would be

If G a finite group of order $n = p^k q$ $(k \geq 1)$, *where p is a prime and q, a +ve integer,* (*p, q relatively prime*) *then for each i,* $1 \leq i \leq k$, *G has a subgroup of order* p^i.

Double Cosets

Definition: Let $H, K \leq G$. Let $a, b \in G$. Define a relation '~' on G as follows:

$$a \sim b \Leftrightarrow \exists\ h \in H,\ k \in K \text{ s.t. } a = hbk$$

It can be easily shown that '~' is an equivalence relation on G. So, it divides G into disjoint union of equivalence classes. Equivalence class of $a \in G$ is given by

$$\begin{aligned} cl(a) &= \{x \in G \mid a \sim x\} \\ &= \{hak \mid h \in H,\ k \in K\} \\ &= HaK, \text{ called double coset of } H \text{ and } K \text{ in } G. \end{aligned}$$

$$G = \bigcup_a cl(a) = \bigcup_a Hak$$

Define $f : HaK \to HaKa^{-1}$ s.t.,

$f(hak) = haka^{-1}$ for all $h \in H,\ k \in K$

Clearly, f is well defined as $hak = h'ak'$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

f is 1–1 as $f(hak) = f(h'ak')$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

$$\Rightarrow hak = h'ak'$$

Let $haka^{-1} \in HaKa^{-1} \Rightarrow hak \in Hak$ and

$f(hak) = haka^{-1}$

$\therefore$ f is both 1–1 and onto.

Thus, $o(Hak) = o(HaKa^{-1})$, (if H, K are finite)

$$= \frac{o(H)\, o(aKa^{-1})}{o(H \cap aKa^{-1})} = \frac{o(H)\, o(K)}{o(H \cap aKa^{-1})}$$

If G is a finite group, then

$$o(G) = \sum_a o(HaK) = \sum_a \frac{o(H)o(K)}{o(H \cap aKa^{-1})}$$

We are now ready to prove Sylow's second theorem.

Theorem 4 (Sylow's Second theorem): *Any two Sylow p-subgroups of a finite group G are conjugate in G.*

Proof: Let P, Q be Sylow p-subgroups of G. Let $o(P) = p^n = o(Q)$ where $p^{n+1} \nmid o(G)$. Suppose P and Q are not conjugate in G.

i.e., $P \neq gQg^{-1}$ for any $g \in G$

By the discussion done above

$$o(PxQ) = \frac{o(P)\, o(Q)}{o(P \cap xQx^{-1})}$$

Since, $P \cap xQx^{-1} \leq P$

$o(P \cap xQx^{-1}) = p^m,\ m \leq n$

If $m = n$, then $P \cap xQx^{-1} = P$

$\Rightarrow P \subseteq xQx^{-1}$

$\Rightarrow P = xQx^{-1}$ as $o(xQx^{-1}) = o(Q) = o(P)$

which is a contradiction.

$\therefore$ $m < n$ and thus $o(PxQ) = p^{2n-m}$, $m < n$ for all $x \in G$

$\Rightarrow o(PxQ) = p^{n+1}$ (p^{n-m+1}) = multiple of p^{n+1}

Thus $o(G) = \sum_x o(PxQ)$ = multiple of p^{n+1}

$p^{n+1} \mid$ R.H.S. $\Rightarrow p^{n+1} \mid o(G)$, a contradiction

$\therefore$ $P = gQg^{-1}$ for some $g \in G$.

Before we prove Sylow's third theorem, we prove

Lemma: *Let P be a Sylow p-subgroup of G. Then the number of Sylow p-subgroups of G is equal to* $\dfrac{o(G)}{o(N(P))}$.

Proof: We know that

$$o(cl(P)) = \frac{o(G)}{o(N(P))} \text{ (See theorem 5 page 167)}$$

Since $cl(P) = \{Q \mid Q \leq G,\ Q = gPg^{-1},\ g \in G\}$

= set of all Sylow p-subgroups of G,

the number of Sylow p-subgroups of G is $\dfrac{o(G)}{o(N(P))}$.

Theorem 5 (Sylow's Third Theorem): *The number of Sylow p-subgroups of G is of the form* $1 + kp$ *where* $(1 + kp) \mid o(G)$, *k being a non-negative integer.*

Proof: Let P be a Sylow p-subgroup of G.

Let $o(P) = p^n$. Now $G = \bigcup_x PxP$

$= \bigcup_{x \in N(P)} PxP \cup \bigcup_{x \notin N(P)} PxP$

$x \in N(P) \Rightarrow Px = xP \Rightarrow PPx = PxP$

$\Rightarrow Px = PxP$

$\therefore$ $\bigcup_{x \in N(P)} PxP = \bigcup_{x \in N(P)} Px = N(P)$

as $P \leq N(P)$ and union of disjoint right cosets equals the set

$x \notin N(P) \Rightarrow Px \neq xP \Rightarrow xPx^{-1} \neq P$

$\Rightarrow o(P \cap xPx^{-1}) = p^m$, $m < n$

(as in Sylow's second theorem)

$\Rightarrow o(PxP) = P^{2n-m}$, $m < n$

$$\therefore \quad o(G) = o(N(P)) + \sum_{x \notin N(P)} o(PxP)$$

$$= o(N(P)) + \sum_{x \notin N(P)} p^{2n-m}$$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \sum \frac{p^{2n-m}}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))}, \quad t = \text{integer}$$

Since L.H.S. = integer, $p^{n+1} \dfrac{t}{o(N(P))} = r = \text{integer}$

$$\therefore \quad p^{n+1}t = r.o(N(P))$$

Again as $P \leq N(P)$

$o(P) \mid o(N(P))$

$\Rightarrow p^n \mid o(N(P))$

$\Rightarrow o(N(P)) = p^n u$

$P^{n+1}t = r\ o(N(P))$

$\Rightarrow pt = r.u$

$\Rightarrow p \mid ru$

If $p \mid u$ then $p^{n+1} \mid o(N(P)) \mid o(G) \Rightarrow p^{n+1} \mid o(G)$, a contradiction.

$\therefore p \mid r \Rightarrow \dfrac{r}{p} = \text{integer} \Rightarrow \dfrac{t}{u} = \text{integer } k = \dfrac{r}{p}.$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))} = 1 + p\frac{t}{u} = 1 + kp$$

By above lemma, $\dfrac{o(G)}{o(N(P))}$ = number of Sylow p-subgroups of G.

$\therefore$ The number of Sylow p-subgroups is of the form $1 + kp = \dfrac{o(G)}{o(N(P))}$

$\Rightarrow (1 + kp) \mid o(G)$.

This proves the theorem.

Note: If $o(G) = p^n q$, $(p, q) = 1$ then the number of Sylow p-subgroups is

$1 + kp$, where $(1 + kp) \mid p^n q$

$\Rightarrow (1 + kp) \mid q$ as $(1 + kp, p^n) = 1$

Cor.: If P is the only Sylow p-subgroups of G, then P is normal in G and conversely.

Proof: By Sylow's third theorem

$$\frac{o(G)}{o(N(P))} = 1 \Rightarrow o(G) = o(N(P))$$

Since $N(P) \leq G$

$N(P) = G$

$\Rightarrow$ P is normal in G.

Conversely, if Sylow p-subgroup P is normal in G, then

$$N(P) = G \Rightarrow o(N(P)) = o(G)$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1$$

$\Rightarrow$ The number of Sylow p-subgroups of G is 1

$\Rightarrow$ P is the only Sylow p-subgroup of G.

Lemma: *Let P be a Sylow p-subgroup of G. Let $x \in N(P)$ s.t. $o(x) = p^i$. Then $x \in P$.*

Proof: Let $o(P) = p^n, \quad p^{n+1} \nmid o(G)$

Now $(Px)^{p^i} = Px^{p^i} = Pe = P$

[P is normal in $N(P)$ and $x \in N(P)$]

$\Rightarrow o(Px) \mid p^i$

$\Rightarrow o(Px) = p^j, j \geq o$

Let $j > 0$. $\bar{K} = <Px> \leq \frac{N(P)}{P}$ s.t. $o(\bar{K}) = p^j$

Since $(\bar{K}) \leq \frac{N(P)}{P}$, $\bar{K} = \frac{K}{P}$ where $K \leq N(P)$

$$p^j = o(\bar{K}) = \frac{o(K)}{o(P)} = \frac{o(K)}{p^n}$$

$\Rightarrow o(K) = p^{n+j}, \quad j > 0$

But $o(K) \mid o(N(P)) \mid o(G)$

$\Rightarrow p^{n+j} \mid o(G), \quad j > 0$, a contradiction

$\therefore j = 0$ $o(Px) = p^j = 1$

$\Rightarrow Px = P \Rightarrow x \in P$.

Theorem 6: *Every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

Proof: Let $H \leq G$ s.t. $o(H) = p^m$ i.e. H is a p-subgroup of G.

Let $\mathscr{S}$ = set of all Sylow p-subgroups of G.

Then $o(\mathscr{S}) = 1 + kp$

Define a relation $\sim$ on $\mathscr{S}$ as follows:

For $P_1, P_2 \in \mathscr{S}$, let $P_1 \sim P_2 \Leftrightarrow \exists\, x \in H$ s.t. $P_1 = xP_2x^{-1}$. It can be shown that $\sim$ is an equivalence relation on $\mathscr{S}$. For $P \in \mathscr{S}$ equivalence class of P in $\mathscr{S}$ is given by $cl(P) = \{xPx^{-1} \mid x \in H\}$.

If $N_H(P) = \{x \in H \mid xP = Px\}$ then $N_H(P) \leq H$.

Thus $o(cl(P)) = \frac{o(H)}{o(N_H(P))}\, p^s, \; s \geq 0$. (See theorem 5 page 193)

Suppose H is not contained in any Sylow p-subgroup of G. Then $H \not\subseteq P$.

$\therefore$ $\exists$ some $x \in H$ s.t. $x \notin P$

If $xPx^{-1} = P$, then $x \in N(P)$ and $o(x) = p^i$ [as $x \in H$, $o(x) \mid o(H)$]

$\Rightarrow$ $x \in P$ by above lemma, which is not true

Hence $xPx^{-1} \neq P$, $x \in H$

$\Rightarrow$ P, xPx^{-1} are distinct members of $cl(P) \Rightarrow o(cl(P)) > 1$

$\therefore$ $o(cl(P)) = p^s$, $s > 0$ $\Rightarrow o(cl(P))$ = multiple of p

This is true for all $P \in \mathscr{S}$

Since $\mathscr{S} = \cup\, cl(P)$

$o(\mathscr{S}) = \sum o(cl(P))$ = a multiple of p

$\Rightarrow$ $1 + kp$ = a multiple of p, a contradiction.

Hence H is contained in some Sylow p-subgroup of G.

Cor.: Let G be a finite group, and P be a p-subgroup of G then P is Sylow p-subgroup of G if and only if no p-subgroup of G properly contains P.

Proof: Suppose P is a Sylow p-subgroup of G. Let H be a p-subgroup of G. If $P \subset H$ then $o(H) > o(P) = p^n \Rightarrow o(H) = p^{n+m}$, $m > 0$.

But $H \leq G \Rightarrow o(H) \mid o(G)$

$\Rightarrow p^{n+m} \mid o(G)$, a contradiction as $p^{n+1} \nmid o(G)$

$\therefore$ no p-subgroup of G contains P properly.

Conversely, since P is a p-subgroup of G, $\exists$ a Sylow p-subgroup Q of G s.t., $P \subseteq Q$. But no p-subgroup contains P properly.

$\therefore$ $Q = P$

$\Rightarrow$ P is a Sylow p-subgroup of G.

Remark: In a finite group G, no Sylow p-subgroup can be properly contained in a p-subgroup.

Problem 7: *Let* $o(G) = 30$. *Show that*

(*i*) *Either Sylow* 3*-subgroup or Sylow* 5*-subgroup is normal in* G.

(*ii*) G *has a normal subgroup of order* 15.

(*iii*) *Both Sylow* 3*-subgroup and Sylow* 5*-subgroup are normal in* G.

Solution: $o(G) = 30 = 2 \times 3 \times 5$

The number of Sylow 3-subgroups is $1 + 3k$ and $(1 + 3k) \mid 10 \Rightarrow k = 0$ or 3

If $k = 0$, then Sylow 3-subgroup is normal.

Let $k \neq 0$, then $k = 3$. This gives 10 Sylow 3-subgroups H_i each of order 3 and so we have 20 elements of order 3. [Notice (for $i \neq j$) $o(H_i \cap H_j) \mid o(H_i) = 3 \Rightarrow o(H_i \cap H_j) = 1$ only and so these 20 elements are different. Each H_i has one element e of order 1 and other two of order 3. $a \in H_i \Rightarrow o(a) \mid o(H_i) = 3 \Rightarrow o(a) = 1, 3$].

The number of Sylow 5-subgroups is $1 + 5k'$ and $(1 + 5k') \mid 6 \Rightarrow k' = 0$ or 1.

If $k' = 0$. Then Sylow 5-subgroup is normal.

Let $k' \neq 0$. Then $k' = 1$. This gives 6 Sylow 5 subgroups each of order 5 and we get 24 elements of order 5. But we have already counted 20 elements of order 3. Thus we have more than 44 elements in G, a contradiction. So,. either $k = 0$ or $k' = 0$.

i.e., either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

Which proves (*i*).

Let H be a Sylow 3-subgroup of order 3 and K, a Sylow 5-subgroup of order 5.

By (*i*), either H is normal in G or K is normal in G.

In any case, $HK \leq G$, $o(HK) = 15$ as $o(H \cap K)$ divides $o(H) = 3$ and $o(K) = 5 \Rightarrow o(H \cap K) = 1$. Since index of HK in G is 2, HK is normal in G. This proves (*ii*).

Suppose, H is normal in G, K is not normal in G. By (*i*) G has 6 Sylow 5-subgroups and so 24 elements of order 5. But $o(HK) = 15 \Rightarrow HK$ is cyclic (*See problem* 10 *ahead*) $\Rightarrow HK$ has $\varphi(15) = 8$ elements of order 15. Thus G has $24 + 8 = 32$ elements, a contradiction.

$\therefore$ K is normal in G.

If H is not normal in G, they by (*i*), G has 10 Sylow 3-subgroups and so 20 elements of order 3. From above HK has 8 elements of order 15 and K has 4 elements of order 5. This gives $20 + 8 + 4 = 32$ elements in G, a contradiction.

$\therefore$ H is normal in G. So both H and K are normal in G.

This proves (*iii*).

Problem 8: *Find all the Sylow p-subgroups of S_4 and show none of them is normal.*

Solution: We have $o(S_4) = 24 = 2^3 \times 3$

Thus S_4 has Sylow 2-subgroups and Sylow 3-subgroups.

Number of Sylow 2-subgroups is $(1 + 2k)$

where $(1 + 2k) \mid 3$ i.e., $k = 0$, or 1

i.e., either there is a unique (thus normal) Sylow 2-subgroup or 3 Sylow 2-subgroups.

Consider

$$H = \{e, a, a^2, a^3, b, ab, a^2b, a^3b \mid a^4 = e = b^2, b^{-1}ab = a^{-1}\}$$

where $a = (1234)$ and $b = (13)$

then H is a Sylow 2-subgroup of S_4

Again as $gag^{-1} = (g(1)g(2)g(3)g(4)) = (3124) \notin H$

where $g = (132)$

as b, ab, a^2b, a^3b, a^2 are all of order 2 and $a^3 = a^{-1} = (4321)$

H is not normal.

We can write

$$H = \{I, (1234), (13)(24), (1432), (14)(23), (24), (12)(34), (13)\}$$

The other two Sylow 2-subgroups would be (the conjugates)

$$(12)H(12)^{-1} = \{I, (2134), (23)(14), (2431), (24)(13), (14), (12)(34), (23)\}$$

$$(23)H(23)^{-1} = \{I, (1324), (12)(34), (1423), (14)(23), (34), (13)(24), (12)\}$$

So S_4 has 3 Sylow 2-subgroups which are not normal.

Again number of Sylow 3-subgroups is $(1 + 3k) \mid 8$ i.e., $k = 0$ or 1

i.e., $\exists$ either a unique (thus normal) Sylow 3-subgroup.

or 4 Sylow 3-subgroups.

It is easily seen that

$$\{I, (123), (132)\},\ \{I, (124), (142)\},\ \{I, (134), (143)\}$$

and $\{I, (234), (243)\}$ are the four Sylow 3-subgroups (and so they are not normal)

Problem 9: *Let G be group of order* 231. *Show that* 11*-Sylow subgroup of G is contained in the centre of G.*

Solution: $o(G) = 231 = 3 \times 7 \times 11$.

The number of Sylow 11-subgroups of G is $1 + 11k$ and $(1 + 11k) \mid 21$. Clearly then $k = 0$.

So, Sylow 11-subgroup H of G is normal in G.

The number of Sylow 7-subgroups of G is $1 + 7k'$ and $(1 + 7k') \mid 33$. So, $k' = 0$.

Thus, Sylow 7-subgroup K of G is normal in G.

$$o(H) = 11,\ o(K) = 7$$

Now $o\left(\frac{G}{K}\right) = 33 = 3 \times 11$ and $3 \nmid (11 - 1)$, thus $\frac{G}{K}$ is cyclic and so $\frac{G}{K}$ is abelian. (See problem 10)

But G' is smallest subgroup of G such that G/G' is abelian (G' denotes the commutator subgroup of G).

$\therefore\ G' \subseteq K \Rightarrow o(G') = 1$ or 7. If $o(G') = 1$, then

$G' = \{e\} \Rightarrow x^{-1}y^{-1}xy = e \Rightarrow xy = yx$ for all $x, y \in G \Rightarrow G$ is abelian $\Rightarrow G = Z(G)$ $\Rightarrow H \subseteq Z(G)$.

Let $o(G') = 7 \Rightarrow G' = K$

Clearly $H \cap K = \{e\}$ as $o(H \cap K)$ divides $o(H) = 11$ and $o(K) = 7$.

Let $x \in H, y \in G$ Then $x^{-1}y^{-1}xy \in G' = K$. Also

$x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in H$ as H is normal in G.

$\therefore\ x^{-1}y^{-1}xy \in H \cap K = \{e\}$

$\Rightarrow xy = yx$ for all $y \in G, x \in H$

$\Rightarrow H \subseteq Z(G)$.

Problem 10: *Let* $o(G) = pq$*, where* p, q *are distinct primes,* $p < q$*,* $p \nmid q - 1$*. Show that G is cyclic.*

Solution: The number of Sylow p-subgroups is $1 + kp$ and $(1 + kp) \mid q \Rightarrow$ $1 + kp = 1$ or q, $1 + kp = 1 \Rightarrow$ Sylow p-subgroup is unique $\Rightarrow$ Sylow p-subgroup H is normal in G.

$1 + kp = q \Rightarrow kp = q - 1 \Rightarrow p \mid q - 1$, a contradiction.

Thus $1 + kp \neq q$ and so Sylow p-subgroup is normal.

The number of Sylow q-subgroups is $1 + k'q$ and $(1 + k'q) \mid p \Rightarrow 1 + k'q = 1$ or p

If $1 + k'q = p$, then $k'q = p - 1 \Rightarrow q \mid p - 1 \Rightarrow q \leq p - 1 < p$, a contradiction. $1 + k'q = 1 \Rightarrow$ Sylow q-subgroup K is normal in G.

$o(H) = p$, $o(K) = q$, $H \cap K = \{e\}$, H is normal is G, K is normal in G.

$[x \in H \cap K \Rightarrow o(x) \mid o(H), o(x) \mid o(K) \Rightarrow o(x) = 1]$

Thus $hk = kh$ for all $h \in H$, $k \in K$

Let $H = < a >$, $K = < b >$ (Groups of prime order are cyclic)

$o(a) = o(H) = p$, $o(b) = o(K) = q$

Now $ab = ba$, $(o(a), o(b)) = (p, q) = 1$

$o(ab) = a(a)\ o(b) = pq = o(G)$

$\Rightarrow G$ is cyclic.

Problem 11: (Wilson's Theorem): *Using Sylow's theorems show that* $(p - 1)! \equiv -1 (mod\ p)$ *for any prime p.*

Solution: Consider S_p, then order of S_p is $p(p - 1)(p - 2) \ldots 2.1$

The number of Sylow p-subgroups of order p in S_p are of the form $1 + kp$, where k is a non -ve integer. Since each Sylow p-subgroup is of order p, we get $(p - 1)$ elements of order p. Again, any two groups of order p have only identity in common and thus the number of elements of order p in S_p is $(1 + kp)(p - 1)$. Also any element of order p in S_p is a cycle of length p and the number of cycles of length p in S_p is $(p - 1)!$

So $(1 + kp)(p - 1) = (p - 1)!$

i.e., $(p - 1)! \equiv -1 (\text{mod } p)$.

Problem 12: *Let p be a prime dividing* $o(G)$ *and* $(ab)^p = a^p b^p$ *for all* $a, b \in G$. *Show that*

(*i*) *Sylow p-subgroup P is normal in G.*

(*ii*) $\exists$ *a normal subgroup N of G s.t.* $P \cap N = \{e\}$ *and* $G = PN$

(*iii*) *G has non-trivial centre.*

Solution: Let $p^n \mid o(G)$, $p^{n+1} \nmid o(G)$

Let $H = \{x \in G \mid x^{p^n} = e\}$

$H \neq \varphi$ as $e^{p^n} = e \Rightarrow e \in H$

Let $x, y \in H \Rightarrow (xy^{-1})^{p^n} = x^{p^n} (y^{-1})^{p^n} = e.e = e$

$\Rightarrow xy^{-1} \in H$

$H \leq G$

Let q be a prime dividing $o(H)$.

Then $x \in H$ s.t. $o(x) = q$

But $x \in H \Rightarrow o(x) \mid p^n \Rightarrow q \mid p^n \Rightarrow q = p$

$\therefore$ H is a p-group. $o(H) = p^m$, $m \leq n$.

Let P be a Sylow p-subgroup of G.

Then $o(P) = p^n$. Let $x \in P \Rightarrow x^{p^n} = e$

$\Rightarrow x \in H \Rightarrow P \subseteq H \Rightarrow o(P) \mid o(H) \Rightarrow p^n \mid p^m \Rightarrow n \leq m \ \therefore\ m = n$

So, $o(H) = p^n = o(P)$

$\Rightarrow H = P.$

Thus H is the only Sylow p-subgroup of G and so is normal in G.

This proves (i)

Define $\theta : G \to G$ s.t.

$\theta(x) = x^{p^n}$

Then θ is a homomorphism.

$$\Rightarrow \frac{G}{\text{Ker } \theta} \cong ImG \quad \text{is normal in } G \quad [\theta(G) = ImG]$$

Since $x \in \text{Ker } \theta \Leftrightarrow \theta(x) = e$

$\Leftrightarrow x^{p^n} = e$

$\Leftrightarrow x \in H = P$

$P = \text{Ker } \theta$

Let $N = ImG$ which is normal in G.

(as $\theta(x) \in N$, $g \in G \Rightarrow g^{-1}\theta(x)g = g^{-1}x^{p^n}g$

$= (g^{-1}xg)^{p^n} = \theta(g^{-1}xg) \in N$)

Let $x \in P \cap N \Rightarrow x \in P, x \in N$

$\Rightarrow x^{p^n} = e, \quad x = \theta(y) = y^{p^n}$

$\Rightarrow y^{p^{2n}} = e \Rightarrow o(y) = p^r,\ r \le n$

as $p^{n+1} \nmid o(G)$

we get $y^{p^r} = e,\ r \le n$

$\Rightarrow y^{p^n} = (y^{p^r})^{p^{n-r}} = e \Rightarrow x = e$

$\Rightarrow P \cap N = \{e\}$

Also $\frac{G}{P} \cong N \Rightarrow \frac{o(G)}{o(P)} = o(N)$

$\Rightarrow o(G) = o(P).\ o(N)$

But $o(PN) = o(P)\ o(N)$

$\Rightarrow o(G) = o(PN)$

$\Rightarrow PN = G$

This proves (ii).

Let $z \in Z(P)$, $z \neq e$. Let $g \in G$.

Since $G = PN$, $g = xy$, $x \in P$, $y \in N$

Also P is normal in G, N is normal in G, $P \cap N = \{e\}$

$\Rightarrow x'y' = y'x'$ for all $x' \in P$, $y' \in N$

Now $zg = z(xy) = (zx)y$

$= (xz)y$ as $z \in Z(P)$

$= x(zy) = x(yz)$ as $z \in P, y \in N$

$= (xy)z = gz$ for all $g \in G$

$\therefore \quad z \in Z(G)$

$\therefore \quad Z(G) \neq \{e\}$

which proves (*iii*).

Problem 13: *Show that Aut* $S_4 \cong S_4$.

Solution: We know $Z(S_4) = \{ I \}$ and thus $S_4 \cong I(S_4)$ (See theorem 3 page 170)

Now the number of Sylow 3-subgroups in S_4 is $1 + 3k$, where $(1 + 3k) \mid 24$ $[o(S_4) = 24 = 2^3 \times 3^1]$

i.e., $k = 0, 1$ are possible values.

$k = 0$ means only one subgroup, but we have more than one Sylow 3-subgroup. In fact S_4 has the following 4 Sylow 3-subgroups

$$P_1 = \{I, (123), (132)\},\ P_2 = (I, (124), (142)\}$$

$$P_3 = \{I, (234), (243)\},\ P_4 = \{I, (134), (143)\}$$

[Notice if H be a Sylow 3-subgroup of S_4 then $o(H) = 3^1$. Also $a \in H \Rightarrow o(a) | o(H) = 3 \Rightarrow o(a) = 1, 3$].

Let $\mathscr{A} = \{P_1, P_2, P_3, P_4\}$

Let $T \in$ Aut G, $G = S_4$, then $T : G \to G$ is an automorphism

$\therefore\ T(P_i) \leq G\ \forall\ i$

Also $o(T(P_i)) = o(P_i)$ (See problem 1 page 171)

$\Rightarrow\ o(T(P_i)) = 3$ and $T(P_i) \leq G$

$\Rightarrow\ T(P_i)$ is a Sylow 3-subgroup of G, $\forall\ i$

$\Rightarrow\ T(P_i) \in \mathscr{A}\ \forall\ i$

$\Rightarrow\ T$ is a map form $\mathscr{A} \to \mathscr{A}$ and is 1–1 as it is 1–1 from $G \to G$

Also then T will be onto ($\mathscr{A}$ being finite)

Define θ : Aut $G \to A(\mathscr{A})$, s.t.,

$$\theta(T) = T' \text{ where } T' \text{ is restriction of } T \text{ on } \mathscr{A}$$

then by above discussion, θ is well defined.

If $\theta(T_1) = \theta(T_2)$

then $T'_1 = T'_2$

$\Rightarrow\ T'_1(P_i) = T'_2(P_i) \qquad i = 1, 2, 3, 4$

$\Rightarrow\ (T'_2)^{-1}\ T'_1\ (P_i) = P_i$

$\Rightarrow\ \varphi\ (P_i) = P_i\ \forall\ i$ where $\varphi = (T'_2)^{-1}\ T'_1$

$\Rightarrow\ \varphi$ is identity map on $\mathscr{A}$ and, therefore, on G.

(If $\varphi \neq I$, than φ must not fix some transposition as every element in G is product of transpositions. Suppose $\varphi(12) \neq (12)$. Also $o(\varphi(12)) = o(12) = 2$ and Klein's four group is a

characteristic subgroup of S_4. $\varphi(12)$ must be a transposition So, either $\varphi(12)$ is a transposition disjoint from (12) or not. Suppose $\varphi(12) = (34)$ or $\varphi(12) = (23)$. If $\varphi(12) = (34)$, then $\varphi(P_1) \neq P_1$ and if $\varphi(12) = (23)$, than $\varphi(P_2) \neq P_2$. So, $\varphi = I$).

Thus $(T_2')^{-1}\ T_1' = I \Rightarrow T_1 = T_2 \Rightarrow \theta$ is 1–1

$o(\text{Aut } G) \leq o(A(\not\infty))$ = 4! = 24

But $o(I(G)) = o(G) = 24$

$\Rightarrow o(\text{Aut } G) \leq 24 = o(I(G))$

$\Rightarrow o(\text{Aut } G) = o(I(G))$ [as $o(I(G)) \leq o(\text{Aut } G)$ by def.]

$\Rightarrow I(G) = \text{Aut } G \Rightarrow \text{Aut } G \cong G$

or that Aut $S_4 \cong S_4$.

(See Page 180 also)

Problem 14: *If G is a finite non-abelian simple group and $H \leq G$ show that $[G : H] \geq 5$.*

Solution: Let $[G : H]$ = index of H in $G = n$.

Let $\mathcal{L}$ = set of all left cosets of H in G.

Then $o(\mathcal{L}) = n$.

Define $\theta : G \to A(\mathcal{L}) = S_n$ s.t.,

$\theta(g) = T_g$

where $T_g : \mathcal{L} \to \mathcal{L}$ s.t.,

$T_g(xH) = gxH$

It can be shown that T_g is 1–1 and so onto.

$\therefore\ T_g \in A(\mathcal{L})$ and θ is a homomorphism.

Let $g \in \text{Ker } \theta \Rightarrow \theta(g) = T_g = I$

$\Rightarrow gxh = xH$ for all $x \in G$

$\Rightarrow gH = H \Rightarrow g \in H$

$\therefore$ Ker $\theta \subseteq H$

Since Ker θ is normal in G and G has no non-trivial normal subgroup Ker $\theta = \{e\}$ or G. But Ker $\theta = G \Rightarrow H = G$ which is not true. $\therefore$ Ker $\theta = \{e\}$.

Thus, G is isomorphic to a subgroup of S_n.

Let $n = 4$, then G is a subgroup of S_4.

Since G is simple $G \neq S_4$ and $o(G)$ must be divisible by at least two primes (for if $o(G)$ is divisible by one prime only, then G has non-trivial centre as normal subgroup).

$\therefore$ $o(G) = 2^2 \times 3$ or $o(G) = 2 \times 3$

If $o(G) = 2^2 \times 3$, then Sylow 3-subgroup or Sylow 2-subgroup is normal. So, $o(G) \neq 2^2 \times 3$. If $o(G) = 2 \times 3$ and G is non-abelian then $G \cong S_3$

$\Rightarrow G$ has normal subgroup A_3.

In either case, we get a contradiction. Hence $n \neq 4$.

If $n = 3$, then G is a subgroup of S_3. Since G is simple, $G \neq S_3$. $\therefore\ G < S_3 \Rightarrow$

$o(G) = 1, 2$ or 3 which is not possible as G is non-abelian.

Clearly, $n \neq 1, 2$.

$\therefore \quad n > 4$

$\therefore \quad [G : H] \geq 5.$

Problem 15: *Show that if G is a group of order 60 and has more than one Sylow 5-subgroup then G is simple.*

Solution: $o(G) = 60 = 2^2 \times 3 \times 5$. The number of Sylow 5-subgroups is $1 + 5k$, s.t., $(1 + 5k) \mid 12 \Rightarrow k = 0, 1$

If $k = 0$, then $\exists$ a unique normal Sylow 5-subgroup. Since G has more than one Sylow 5-subgroup, $k = 1$, and thus $\exists$ 6 Sylow 5-subgroups each of order 5 and hence these are $6 \times 4 = 24$ elements of order 5.

Suppose G has a non trivial normal subgroup H i.e., G is not simple.

Then possible values of $o(H)$ case 2, 3, 4, 5, 6, 10, 12, 15, 20, 30

Case (*i*): $o(H) = 5, 10, 15, 20$ or 30

i.e., $5 \mid o(H)$ then since $5^{1+1} \nmid o(H)$, we find H has a Sylow 5-subgroup P. Then $P \subseteq H \subseteq G$.

If Q is any conjugate of P then $Q = gPg^{-1}$ for some $g \in G$.

$$P \subseteq H \Rightarrow gPg^{-1} \subseteq gHg^{-1} \Rightarrow Q \subseteq gHg^{-1} = H \text{ as } H \trianglelefteq G$$

$\Rightarrow$ all the six conjugates (6 Sylow 5-subgroups of H are conujgates) are contained in H.

$\Rightarrow$ all the 24 elements of order 5 are in H and also $e \in H$. So $o(H) \geq 25$ or that $o(H) = 30$ is the only possibility. But a group of order 30 has a unique normal Sylow 5-subgroup (see Problem 7 on page 216). So we get a conctradiction and thus this case does not hold.

Case (*ii*): $o(H) = 2, 3, 4$

Let $\bar{G} = \dfrac{G}{H}$, then $o(\bar{G}) = \dfrac{o(G)}{o(H)} = \dfrac{60}{2,3,4} = 30, 20, 15$

But again, we know that groups of order 30, 20, 15 have a unique normal Sylow 5-subgroup. So in each case $\bar{G}$ has a unique normal subgroup $\bar{K}$ of order 5.

Let $f : G \to \bar{G}$ be the natural onto homomorphism. Since $\bar{K} \trianglelefteq \bar{G}$, its pre image K will be normal in G.

Now $o(\bar{K}) = 5$ and $o(\bar{K}) \mid o(K) \Rightarrow 5 \mid o(K)$ (See page 120)

Not possible because of case (*i*)

Thus, case (*ii*) is also ruled out

Finally, suppose $o(H) = 6$ or 12

Then we know (See page 236) that H contains a unique normal Sylow subgroup, say N.

Thus N is characteristic subgroup of H

$\Rightarrow N \trianglelefteq G$ (See exercises 18, 15 on page 181)

Since N is a Sylow subgroup of H and $o(H) = 2 \times 3$ or $o(H) = 2^2 \times 3$

Sylow subgroups are of order 2^1 or 3^1 or 2^2

i.e., 2, 3 or 4. So $o(N) = 2, 3, 4$ which is not possible as seen earlier.

Hence the result follows.

Problem 16 : *A_5 is simple*

Solution: $o(A_5) = 60$, Let $\sigma = (12345)$, $\eta = (13245)$

then $H = <\sigma> = <\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = I>$

$= \{(12345), (13524), (14253), (15432), I\}$

and $K = <\eta> = \{(13245), (12534), (14352), (15423), I\}$

are two Sylow 5-subgroups of A_5 and thus by previous problem A_5 is simple.

Problem 17: *Show that there is no simple group of order* 144.

Proof: Let G be a group of order $144 = 2^4 \times 3^2$, and suppose G is simple.

The number of Sylow 3-subgroups of G is $1 + 3k$ and $(1 + 3k) \mid 16 \Rightarrow k = 0, 1, 5$. If $k = 0$, then Sylow 3-subgroup is unique and normal, which is not possible.

If $k = 1$, then $\exists$ 4 Sylow 3-subgroups of G and if P is any one of these then as $\frac{o(G)}{o(N(P))} = 4$ = number of Sylow 3-subgroups, we find $N(P)$ is a subgroup of G with index 4 which is not possible in view of problem 14 above.

If $k = 5$, then $\exists$ 16 Sylow 3-subgroups each of order 9 in G. Let H_1, H_2, be any Sylow 3-subgroups. Since $H_1 \cap H_2 \leq H_1$, $o(H_1 \cap H_2) \mid 9 \Rightarrow o(H_1 \cap H_2) = 1, 3$ or 9. If $o(H_1 \cap H_2) = 9$, then $o(H_1 \cap H_2) = o(H_1) = o(H_2), \Rightarrow H_1 = H_1 \cap H_2 = H_2$, a contradiction. If $o(H_1 \cap H_2) = 3$, then $H_1 \cap H_2$ is normal in H_1 and H_2. Since $N(H_1 \cap H_2)$ is the largest subgroup of G in which $H_1 \cap H_2$ is normal.

$$H_1 \subseteq N(H_1 \cap H_2), \quad H_2 \subseteq N(H_1 \cap H_2)$$

$$\Rightarrow H_1H_2 \subseteq N(H_1 \cap H_2) \subseteq G$$

Again as $o(H_1H_2) = \frac{o(H_1)\, o(H_2)}{o(H_1 \cap H_2)} = 27,$

$o(N(H_1 \cap H_2)) \geq 27$ and divides $o(G) = 144$

$\therefore$ $o(N(H_1 \cap H_2)) = 36, 48, 72$ or 144

But then $[G : N(H_1 \cap H_2)] = 4, 3, 2$ or 1 which is not possible by problem 9.

$\therefore$ $o(H_1 \cap H_2) = 1$

i.e., any two Sylow 3-subgroups of G intersect trivially. This gives 128 elements of order 3^i ($i = 1$ or 2). Since Sylow 2-subgroup is of order 16 and not normal, there are at least 16 elements of order 2^i ($i = 1, 2, 3$ or 4) and one identity element. So, we get 145 elements in G, a contradiction.

Showing that G is a simple group.

Problem 18: *Let G be a finite group. Let H be normal in G. If p be a prime dividing $o(G)$ s.t. $([G : H]), p) = 1$, show that H contains every Sylow p-subgroup of G.*

Solution: Let $[G : H] = m$

$\therefore$ $(m, p) = 1 \Rightarrow p \nmid m \Rightarrow p^i \nmid m,\ i > 0$

Let $p^n \mid o(G),\ p^{n+1} \nmid o(G)$

Then $$o(G) = \frac{o(G)}{o(H)} \cdot o(H)$$
$$= [G : H]\ o(H)$$
$$= m \cdot o(H)$$

Since $p^n \mid o(G),\ p^n \mid m \Rightarrow p^n \mid o(H)$

$\therefore$ By Sylow's first theorem $\exists\ K \leq H$ s.t. $o(K) = p^n$.

$\therefore$ K is Sylow p-subgroup of G.

Let P be any Sylow p-subgroup of G

Then $P = gKg^{-1},\ g \in G$

$\therefore$ $K = g^{-1} Pg$. But $K \subseteq H$

$\therefore$ $g^{-1} Pg \subseteq H$

$\Rightarrow P \subseteq gHg^{-1} = H$ as H is normal in G.

Hence H contains all Sylow p-subgroups of G.

Problem 19: *Let G be a finite group and $H \leq G$. Suppose p is a prime dividing $o(G)$. Let P be a Sylow p-subgroup of H contained in some Sylow p-subgroup S of G. Show that $P = S \cap H$.*

Solution: Since $P \subseteq S,\ P \subseteq H$

$P \subseteq S \cap H$

Also $S \cap H \leq S \Rightarrow S \cap H$ is a p-subgroup.

Since $S \cap H \leq H$, $S \cap H$ is a p-subgroup of H.

$\therefore$ $P \subseteq S \cap H \subseteq H$

As P is Sylow p-subgroup of H, there is no p-subgroup of H properly containing P.

$P = S \cap H$.

Problem 20: *If in above problem, Q is another Sylow p-subgroup of H s.t. $Q \subseteq T$ where T = Sylow p-subgroup of G, then show that $S \neq T$ if $P \neq Q$.*

Solution: By above problem

$P = S \cap H,\ Q = T \cap H$

If $S = T$, then $P = Q$ and the result follows.

Problem 21: *If G is a finite group and p is a prime dividing $o(H)$ where $H \leq G$, then show that the number of Sylow p-subgroups of H is less than or equal to the number of Sylow p-subgroups of G.*

Solution: If $P_1, \ldots P_r$ are Sylow p-subgroups of H, then $\exists$ Sylow p-subgroups $S_1, \ldots, S_r$ of G s.t. $P_1 \subseteq S_1, \ldots, P_r \subseteq S_r$. By above problem since $P_1, \ldots, P_r$ are distinct, so are $S_1, \ldots, S_r$.

$\therefore$ The number of Sylow p-subgroups of $G \geq r$ = the number of Sylow p-subgroups of H.

Problem 22: *Let p be a prime dividing* $o(G)$. *Show that*

(i) *If K is normal in G and P is a Sylow p-subgroup of G, then* $P \cap K$ *is a Sylow p-subgroup of G.*

(ii) $\frac{PK}{K}$ is a *Sylow p-subgroup of* $\frac{G}{K}$

(iii) *Every Sylow p-subgroup of* $\frac{G}{K}$ *is of the form* $\frac{PK}{K}$ *where P is a Sylow p-subgroup of G.*

Solution: (i) Suppose $P \cap K$ is not a Sylow p-subgroup of K. Then $\exists$ Sylow p-subgroup Q of K s.t., $P \cap K \subset Q \subseteq R$ where R = Sylow p-subgroup of G.

Since P and R are Sylow p-subgroups of G,

$P = xRx^{-1}$ for some $x \in G$

$xQx^{-1} \subseteq x(K \cap R)x^{-1}$

$\subseteq (xKx^{-1}) \cap (xRx^{-1})$

$= K \cap P$ as K is normal in G

$\subset Q$

But $o(xQx^{-1}) = o(Q) \Rightarrow xQx^{-1} = Q$, a contradiction.

$\therefore$ $P \cap K$ is a Sylow p-subgroup of K.

(ii) Let $p^m \mid o(K)$, $p^{m+1} \nmid o(K)$

Then $o(P \cap K) = p^m$ by (i)

But $o\left(\frac{PK}{K}\right) = \frac{o(P)\,o(K)}{o(P \cap K)\,o(K)} = \frac{o(P)}{o(P \cap K)} = \frac{p^n}{p^m} = p^{n-m}$

Now $p^n \mid o(G)$, $p^m \mid o(K) \Rightarrow p^{n-m} \mid o\left(\frac{G}{K}\right)$

Also $p^{n-m+1} \nmid o(G/K)$

$\therefore$ $\frac{PK}{K}$ is a Sylow p-subgroup of $\frac{G}{K}$.

(iii) Let $\frac{H}{K}$ be a Sylow p-subgroup of $\frac{G}{K}$

Let $p^n \mid o(G)$, $p^{n+1} \nmid o(G)$

$p^m \mid o(K)$, $p^{m+1} \nmid o(K)$

Let $o(K) = p^m v$, $(p, v) = 1$

$o(G) = p^n u$, $(p, u) = 1$

$\therefore$ $p^{n-m} \mid o(G/K)$, $p^{n-m+1} \nmid o\left(\frac{G}{K}\right)$

$\Rightarrow$ order of Sylow p-subgroup of $\frac{G}{K}$ is p^{n-m}

$$\Rightarrow\ o\left(\frac{H}{K}\right) = p^{n-m}$$

$\Rightarrow\ o(H) = o(K)\ p^{n-m} = p^n v,\ \ (p,\ v) = 1$

Let P be a Sylow p-subgroup of H then P is also a Sylow p-subgroup of G.

Clearly, $PK \subseteq H$ as $P \subseteq H$, $K \subseteq H$

$$\text{and } o(PK) = \frac{o(P)\,o(K)}{o(P \cap K)} = \frac{p^n p^m v}{p^m}$$

(as by (i) $P \cap K$ is Sylow p-subgroup of K)

$\therefore\ o(PK) = p^n v,\ \ (p,\ v) = 1$

$= o(H)$

$\therefore\ H = PK$

$$\Rightarrow\ \frac{H}{K} = \frac{PK}{K} \text{ where } P = \text{Sylow } p\text{-subgroup of } G$$

This proves (iii).

Problem 23: *Let G be a group of order pqr, $p < q < r$ being primes. Prove that some Sylow subgroup of G is normal. Hence, show that G is not simple.*

Solution: Suppose that no Sylow subgroup of G is normal.

Then the number of Sylow p-subgroups of G is $1 + kp$ and $(1 + kp) \mid qr \Rightarrow 1 + kp = q$, r or qr $(\geq q)$

The number of Sylow q-subgroup of G is $(1 + k'q) \mid pr \Rightarrow 1 + k'q = p$, r or pr. If $1 + k'q = p$, then $q \mid p - 1 \ \Rightarrow\ q < p$, a contradiction.

$\therefore$ The number of Sylow q-subgroups of G is r or pr $(\geq r)$

Also the number of Sylow r-subgroups of G is $(1 + k''r) \mid pq \Rightarrow 1 + k''r = p$, q or pq. If $1 + k''r = p$ or q then $r \mid (p - 1)$ or $r \mid (q - 1) \Rightarrow r < p$ or $r < q$, a contradiction.

$\therefore$ The number of Sylow r-subgroups of G is pq.

Sylow p-subgroups give at least $q\,(p - 1)$ elements of order p and Sylow q-subgroups give at least $r\,(q - 1)$ elements of order q and Sylow r-subgroups give $pq\,(r - 1)$ elements of order r.

$\therefore\ \ o(G) = pqr \geq q\,(p - 1) + r\,(q - 1) + pq\,(r - 1) + 1$

$\therefore\ \ 0 \geq rq - q - r + 1 = (q - 1)\,(r - 1)$

$\therefore\ \ (q - 1)\,(r - 1) \leq 0$, a contradiction.

Thus, some Sylow subgroup of G is normal.

Hence G is not a simple group.

Problem 24: *Let G be a group of order pqr, $p < q < r$ being primes. Prove that*

(i) *Sylow r-subgroup is normal in G.*

(ii) *G has a normal subgroup of order qr.*

(iii) *If $q \nmid r - 1$ then Sylow q-subgroup is normal in G.*

Solution: (*i*) Suppose that Sylow *r*-subgroup is not normal in *G*. Then the number of Sylow *r*-subgroups is *pq* (See previous problem). Denote these by $H_1,\ldots, H_{pq}$. $o(H_i) = r$ for all *i*. By previous problem, either Sylow *p*-subgroup or Sylow *q*-subgroup is normal in *G*. Let Sylow *q*-subgroup *H* be normal in *G*. Then $HH_1,\ldots, HH_{pq}$ are subgroups of order *qr*.

Suppose $HH_i = HH_j$. Then $H_i, H_j \subseteq HH_i = HH_j$

$\Rightarrow H_iH_j \subseteq HH_i \Rightarrow o(H_iH_j) \leq o(HH_i)$

$\Rightarrow r^2 \leq qr$

$\Rightarrow r \leq q$, a contradiction

$\therefore$ $HH_1,\ldots, HH_{pq}$ are distinct subgroups.

Let $K_i = HH_i$

Then $K_1 \cap K_2 \leq K_1$.

$\Rightarrow o(K_1 \cap K_2) = 1, q, r$ or qr.

If $o(K_1 \cap K_2) = 1$, then $o(K_1 K_2) = q^2r^2 > pqr$, a contradiction.

If $o(K_1 \cap K_2) = q$, then $o(K_1 K_2) = qr^2 > pqr$, a contradiction.

If $o(K_1 \cap K_2) = r$, then $o(K_1 K_2) = q^2r > pqr$, a contradiction.

If $o(K_1 \cap K_2) = qr = o(K_1)$, then $K_1 = K_1 \cap K_2$.

Also $K_2 = K_1 \cap K_2 \Rightarrow K_1 = K_2$, a contradiction.

Thus Sylow *q*-subgroup is not normal. If Sylow *p*-subgroup is normal, then $\exists$ $p - 1$ elements of order *p*.

Sylow *r*-subgroups give $pq(r - 1)$ elements of order *r*.

The number of Sylow *q*-subgroups is $1 + kq$ and $(1 + kq) \mid pr \Rightarrow 1 + kq = p, r$ or pr.

If $1 + kq = p$, then $q \mid (p - 1) \Rightarrow q < p$, a contradiction.

$\therefore$ $1 + kq = r$ or $pr > p$.

This gives more than $p(q - 1)$ elements of order *q*.

Thus $o(G) = pqr > pq(r - 1) + (p - 1) + p(q - 1) + 1$

or that $0 > 0$, a contradiction.

Hence Sylow *p*-subgroup is normal in *G*, and we get a contradiction.

$\therefore$ Sylow *r*-subgroup is normal in *G*.

(*ii*) Let *H* be a Sylow *r*-subgroup.

H is normal in *G* by (*i*).

Let *K* be a Sylow *q*-subgroup, $o(K) = q$

Since *H* is normal in *G*, $HK \leq G$ and $o(HK) = qr$.

Also *p* is smallest prime dividing $o(G)$ and $\dfrac{o(G)}{o(HK)} = p$,

HK is normal in *G*.

(*iii*) If $q \nmid (r - 1)$, then *HK* is cyclic group of order *qr*. The number of elements of order *qr* is $\varphi(qr) = \varphi(q)\,\varphi(r) = (q - 1)(r - 1)$. Suppose Sylow *q*-subgroup is not normal. Then, the number of Sylow *q*-subgroups is $1 + kq$ and

$(1 + kq) \mid pr \Rightarrow 1 + kq = p, r$ or pr

$\Rightarrow 1 + kq = r$ or pr as $p < q$

$\Rightarrow 1 + kq = pr$ as $q \nmid (r - 1)$

This gives $pr\,(q - 1)$ elements of orders q. Sylow p-subgroup gives $p - 1$ elements of order p.

Also Sylow r-subgroup gives $r - 1$ elements of order r.

Thus $o(G) \geq (r - 1) + (p - 1) + pr\,(q - 1) + (q - 1)\,(r - 1) + 1$

$pqr \geq (r - 1) + (p - 1) + pqr - pr + qr - q - r + 2$

$pr + q \geq qr + p$

$p\,(r - 1) \geq q\,(r - 1)$

$\Rightarrow p \geq q$, a contradiction.

Hence, Sylow q-subgroup is normal in G.

Problem 25: *Let G be a non-abelian group of order* 12 *in which Sylow* 3*-subgroup is normal. Show that G has an element of order* 6.

Solution: Since Sylow 3-subgroup is normal, it will be unique. Let it be H then $o(H) = 3$, which being a prime shows H is cyclic. Let $H = <a>$. Then $o(a) = o(a^{-1}) = 3$. If $cl(a)$ is the conjugate class of a in G then

$$o(cl(a)) = \frac{o(G)}{o(N(a))} = 1 \text{ or } 2$$

Notice, $cl(a) = \{g^{-1}ag \mid g \in G\}$ and $o(g^{-1}ag) = o(a) = 3$ and as a, a^{-1} are the only elements of order 3, either $cl(a) = \{a\}$ or $cl(a) = \{a, a^{-1}\}$.

Thus $o(N(a)) = 6$ or 12

$\Rightarrow \exists\ b \in N(a)$, s.t., $o(b) = 2$

$\Rightarrow ab = ba$ and $o(ab) = 6$

i.e., G has an element of order 6.

Problem 26: *If* $\sigma \in Aut\ G$ *and* $o(\sigma) = p$, *then* σ *must fix at least one Sylow p-subgroup of G.*

Solution: Let P be a Sylow p-subgroup of G. If $\sigma(P) \neq P$ then

$P, \sigma(P), \sigma^2(P), \ldots, \sigma^{p-1}(P)$ are p distinct Sylow p-subgroups of G.

Note if $\sigma^i(P) = \sigma^j(P)$, then $\sigma^{i-j}(P) = P$

Since $\theta(\sigma) = P, <\sigma> = <\sigma^{i-j}>$

$\Rightarrow \sigma = (\sigma^{i-j})^t$

$\Rightarrow \sigma(P) = (\sigma^{i-j})^t(P) = P$, a contradiction.

In this way, we'll get kp sylow p-subgroups of G. By Sylow's third theorem, there are $1 + k'p$ Sylow p-subgroups of G. Thus at least one Sylow p-subgroup of G must be fixed by σ.

Problem 27: *If H is normal in G and P is a Sylow p-subgroup of H then* $G = N_G(P)\,H$.

Solution: Let $x \in G$. Then $x^{-1}Px$ is a Sylow p-subgroup of H as H is normal in G and $P \subseteq H$.

Thus, $x^{-1} Px = y^{-1} py$ for some $y \in H$

$\Rightarrow yx^{-1} Pxy^{-1} = P$

$\Rightarrow yx^{-1} \in N(P)$

$\Rightarrow x = (xy^{-1})\, y \in N_G(P)H.$

$\Rightarrow G = N_G(P)H.$

Problem 28: *If in a finite group G, there are at most d elements of order d for every $d \mid o(G)$ then G is cyclic.*

Solution: Let $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$

Consider Sylow p_1-group Sp_1

Then $o(Sp_1) = p_1^{\alpha_1}$

Suppose Sp_1 is not cyclic. Then the number of elements in Sp_1 of order p_1 is less than or equal to p_1

of order p_1^2 is $\leq p_1^2$

of order p_1^3 is $\leq p_1^3$

and so on ...

of order $p_1^{\alpha_1 - 1}$ is $\leq p_1^{\alpha_1 - 1}$

Thus $p_1^{\alpha_1} \leq 1 + p_1 + p_1^2 + p_1^3 + \ldots + p_1^{\alpha_1 - 1} = \dfrac{p_1^{\alpha_1} - 1}{p_1 - 1}$, a contradiction.

so Sp_1 is cyclic. Similarly each Sp_i is cyclic.

Since there are $1 + kp_1$, Sylow p_1-groups, the number of elements of order $p_1^{\alpha_1}$ is

$(1 + kp_1)\, \phi(p_1^{\alpha_1}) \leq p_1^{\alpha_1}$

$\Rightarrow (1 + kp_1)\, (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \leq p_1^{\alpha_1}$

$\Rightarrow p_1^{\alpha_1} + kp_1^{\alpha_1 + 1} - p_1^{\alpha_1 - 1} - kp_1^{\alpha_1} \leq p_1^{\alpha_1}$

$\Rightarrow p_1^{\alpha_1 - 1}\, (kp_1^2 - 1 - kp_1) \leq 0$

$\Rightarrow p_1^{\alpha_1 - 1}\, (kp_1\, (p_1 - 1) - 1) \leq 0 \Rightarrow k = 0.$

or that Sylow p_1-group is normal.

Similarly, each Sylow p_i-group is normal and cyclic.

Hence G is cyclic.

Sylow Groups in Sp^k

We now give a method of constructing Sylow p-groups inductively in the symmetric groups Sp^k.

Suppose p = prime s.t. $p^r \mid n!$ and $p^{r+1} \nmid n!$. Then $r = \displaystyle\sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right]$, where $[x]$ represents greatest integer not greater than x. (This result can be found in any book on Number theory).

In particular, if $n = p^k$, then $r = p^{k-1} + p^{k-2} + ... + 1$ we denote r by $n(k)$ to mean the highest power of p dividing $p^k!$.

When $k = 1$, then clearly $p \mid o(S_p) = p!$ and $p^2 \nmid p!$

(as $p^2 \mid p! \Rightarrow p \mid (p-1) \ ... \ 2.1$

$\Rightarrow p \mid (p - r), \quad 1 \le r \le p - 1$

$\Rightarrow p \le p - r$, a contradiction)

$\therefore$ order of Sylow p-subgroup in S_p is p and group generated by $(1\ 2...p)$ is a Sylow p-subgroup. So, We have constructed Sylow p-subgroup when $k = 1$. Assume that we have constructed it for $k - 1$. Consider Sp^k.

Divide the set of p^k letters $1, 2,...p^k$ into p sets each consisting of p^{k-1} letters as follows

$\{1, 2,... p^{k-1}\}, \{p^{k-1} + 1,..., 2p^{k-1}\},...$

$...\{(p-1)\}\ p^{k-1} + 1,..., p^{k-1}\ p = p^k\}$

Let

$\sigma = (1p^{k-1} + 1...(p-1)\ p^{k-1} + 1)\ (2p^{k-1} + 2\ ...(p-1)\ p^{k-1} + 2)...(p^{k-1}\ 2p^{k-1}\ ...\ p^k)$

= product of p^{k-1} disjoint cycles each of length p.

Note, first cycle in σ consists of first letter from each set, second cycle has second letter from each set and so on.

Clearly $\sigma^p = I$ as disjoint cycles commute.

Let $A = \{\tau \in Sp^k \mid \tau(i) = i \text{ for all } i > p^{k-1}\}$

$\therefore$ $I \in A$ i.e., $A \neq \phi$

Let $\tau, \tau' \in A \Rightarrow \tau\tau'(i) = i$ for all $i > p^{k-1}$

$\Rightarrow \tau\tau' \in A \le Sp^k$

But $\tau \in A \Rightarrow \tau$ is permutation on p^{k-1} letters, and so $A \cong Sp^{k-1}$.

By induction hypothesis Sp^{k-1} has Sylow p-subgroup. Thus A has Sylow p-subgroup P_1. $o(P_1) = p^{n(k-1)} = 1 + ... + P^{k-2}$.

Let $P_2 = \sigma P_1 \sigma^{-1}$, $P_3 = \sigma^2 P_1 \sigma^{-2}$,... $P_p = \sigma^{p-1} P_1 \sigma^{-(p-1)}$.

Each $P_i \le Sp^k$ s.t. $P_i \cong P_1$ (where $x \in P_1$ is mapped into $\sigma^i x \sigma^{-i}$).

$\therefore$ $o(P_i) = o(P_1) = p^{n(k-1)}$. Also σ takes letters of first set into second set, letters from second set into third set and so on. So, $\tau \in A \Rightarrow \sigma T \sigma^{-1}$ consists of letters from second set as $T \in A$ means $\tau(i) = i$ for all $i > p^{k-1}$. Similarly $\sigma^2 \tau \sigma^{-2}$ will consist of letters from third set on. Therefore, $P_1, P_2,..., P_{p-1}$ will have disjoint permutations and so commute with each other. Hence $T = P_1 P_2 ... P_p \le Sp^k$.

Also $o(T) = o(P_1)\ o(P_2)\ ...o(P_p)$

$= o(P_1)\ o(P_1)\ ...o(P_1)$ (p times)

$= p^{p(n(k-1))} = p^{1+n(k-1)}$

Let $P = \{\sigma^j t \mid t \in T, 0 \le j \le p - 1\}$

$= <\sigma> T$

Since $\sigma T \sigma^{-1} = \sigma(P_1 ... P_P)\sigma^{-1}$

$$= (\sigma P_1\sigma^{-1})\ (\sigma P_2\sigma^{-1})\ \ldots\ (\sigma P_p\sigma^{-1})$$
$$= P_2P_3\ldots P_pP_1 = P_1P_2\ldots P_p = T$$
$$\Rightarrow \sigma T = T\sigma$$
$$\Rightarrow <\sigma> T = T <\sigma>$$
$$\therefore\ P \le Sp^k$$

Also $<\sigma> \cap T = \{I\}$ as s takes first set into second set while T takes first set into first set,

$$\therefore \quad o(P) = o(<\sigma>)\ o(T)$$
$$= pp^{pn}\ (k-1)$$
$$= p^{p(n\,(k-1))+1}$$
$$= P^{p(1+p+\ldots+p^{k-2})+1}$$
$$= P^{1+p+\ldots+p^{k-1}} = p^{n(k)}$$

So, P is required Sylow p-subgroup of G.

Problem 29: *Find a Sylow* 3*-subgroup of* S_9.

Solution: We urge the reader to first go through the discussion on the previous two pages. Let $P_1 = \{I, (123), (132)\}$ be a Sylow 3-subgroup of S_3.

Divide the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ into 3 sets as follows

$\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}$

Let $\sigma = (147)(258)(369)$

Then $\sigma^3 = I$

Let $P_2 = \sigma P_1\sigma^{-1} = \{I, (456), (465)\}$

$P_3 = \sigma^2 P_2 \sigma^{-2} = \{I, (789), (798)\}$

Let $T = P_1P_2P_3,\ o(T) = 3^3$

Let $P = <\sigma> T$

Then $o(P) = 3^4$

Also $n(2) = 1 + 3 = 4$

$\Rightarrow P$ is a Sylow 3-subgroup of S_9.

Problem 30: *Let G be the group of* $n \times n$ *invertible matrices over the integers modulo p. p a prime. Find a p-Sylow subgroup of G.*

Solution: Let A be an $n \times n$ matrix in G. Since A is invertible, rows of A are linearly independent over the field F of integers modulo p. Since first row of A is linearly independent, it is non zero. It can be chosen in $(p^n - 1)$ ways. Second row should not be α ($\alpha \in F$) times the first row. So, second row can be chosen in $(p^n - p)$ ways. Third row should not be α times first row + β times second row ($\alpha, \beta \in F$). So, third row can be chosen in $(p^n - p^2)$ ways as α, β can be chosen in p^2 ways. In this way, last nth row can be chosen in $p^n - p^{n-1}$ ways.

$$\therefore \quad o(G) = (p^n - 1)\ (p^n - p)\ \ldots\ (p^n - p^{n-1})$$
$$= p^{1+2+\ldots+(n-1)}\ ((p^n - 1)\ (p^{n-1} - 1)\ \ldots\ (p - 1))$$

$$= p^{\frac{n(n-1)}{2}} ((p^n - 1) \ldots (p - 1))$$

Since $(p, (p^i - 1)) = 1$, order of Sylow p-subgroup of G is $p^{\frac{n(n-1)}{2}}$

Let $P = \left\{ \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & \ldots & \end{bmatrix} \{|\text{ enteries above diagonal from } F\} \right\}$

$P \neq \varphi$ as $I \in P$

Also

$$A, B \in P \Rightarrow A = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}$$

$$\Rightarrow AB = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \end{bmatrix} \in P$$

$\therefore \quad P \leq G$

Let $A \in P$. The first row in A can be chosen in p^{n-1} ways, second row in p^{n-2} ways and in this way $(n - 1)$th row in p ways and last row is fixed.

So, $o(P) = p^{n-1} p^{n-2} \ldots p^1$

$$= p^{1 + \ldots + (n-1)} = p^{\frac{n(n-1)}{2}}$$

$\therefore$ P is Sylow p-subgroup of G.

In the following problems we discuss non-abelian groups of order 6 and 8.

Problem 31: *Find all non-abelian groups of order* 8.

Solution: Let G be a non-abelian group of order 8. As $o(a) \mid o(G)$ for all $a \in G$, $o(a) = 1, 2, 4$ or 8. If for some $a \in G$, $o(a) = 8$. G is cyclic. So there is no element in G of order 8. If each non-identity element is of order 2, then G is abelian. So, $\exists\ a \in G$ s.t. $o(a) = 4$. Let $H = < a >$. Then $o(H) = o(a) = 4$.

$\therefore$ H is normal in G as index of H in G is 2.

Let $G = H \cup Hb,\ b \notin H$

Then $b^2 \in H$ as $b^2 \notin H \Rightarrow H, Hb, Hb^2$ are distinct right cosets of H in G, a contradiction.

If $b^2 = a$, then $o(b^2) = \dfrac{o(b)}{(2, o(b))} = \dfrac{o(b)}{2}$

$\Rightarrow o(a) = \dfrac{o(b)}{2} \Rightarrow o(b) = 2.\ o(a) = 8$, a contradiction.

Similarly, if $b^2 = a^3$, then $b^2 = a^{-1} \Rightarrow o(b^2) = o(a^{-1}) = 4 \Rightarrow o(b) = 8$.

So, $b^2 = e$ or a^2.

Since H is normal in G, $b^{-1}ab \in H$.

But $o(b^{-1}ab) = o(a) = 4$

$\Rightarrow b^{-1}ab = a$ or a^3

If $b^{-1}ab = a$, then $ab = ba$. Since $G = H \cup Hb$, $G = \{e, a, a^2, a^3, ab, a^2b, a^3b, b\}$ and $ab = ba$ would imply G is abelian.

$\therefore \quad b^{-1}ab = a^3$

Thus, we have two non-abelian groups G of order 8, namely

(*i*) G, generated by a, b s.t. $a^4 = e$, $b^2 = e$, $b^{-1}ab = a^3 = a^{-1}$.

(*ii*) G, generated by a, b s.t. $a^4 = e$, $-b^2 = a^2$, $b^{-1}ab = a^3 = a^{-1}$.

In fact (*i*) is the Dihedral group of order 8 and (*ii*) is the Quaternion group of order 8.

Remark: Although the Dihedral group and the Quaternion groups have same order 8, they are not isomorphic. In the Quaternion group a^2 is the only element of order 2 whereas in the Dihedral group, there are 5 elements a^2, b, ab, a^2b, a^3b of order 2. Recall if $f: G \to G'$ is an isomorphism then $o(f(a)) = o(a)\ \forall\ a \in G$.

Problem 32: *Find all non-abelian groups of order* 6.

Solution: Let G be a non-abelian group of order 6. By Cauchy's theorem, $\exists\ a, b \in G$ s.t. $o(a) = 3$, $o(b) = 2$. Let $H = < a >$ then $o(H) = o(a) = 3$. Since index of H in G is 2, H is normal in G. If $b \in H$, then $o(b) \mid o(H) \Rightarrow 2 \mid 3$, a contradiction. Thus $b \notin H$.

$\therefore$ H and Hb are distinct right cosets of H in G.

Hence $G = H \cup Hb = \{e, a, a^2, b, ab, a^2b\}$

Also H is normal in $G \Rightarrow b^{-1}ab \in H \Rightarrow b^{-1}ab = a$ or a^2.

If $b^{-1}ab = a$, then as $(o(a), o(b)) = 1$, we get $o(ab) = o(a)o(b) = 6$

i.e., G is cyclic and so abelian, which is not so.

$\therefore\ b^{-1}ab = a^2 = a^{-1}$ $(b^{-1}ab = e \Rightarrow ab = b \Rightarrow a = e$, not true)

So, there is only one non-abelian group G of order 6, namely

$G = \{e, a, a^2, b\ ab, a^2b \mid a^3 = e = b^2, b^{-1}ab = a^{-1}\}$

Indeed G is isomorphic to S_3 by the map $\theta : G \to S_3$ s.t. $\theta(e) = I$, $\theta(a) = (123)$, $\theta(a^2) = (132)$, $\theta(b) = (13)$, $\theta(ab) = (23)$.

Remark: Any non-abelian group of order 6 is isomorphic to S_3. Also since any abelian group of order 6 is cyclic (see page 195) we find there are only two abstract groups of order 6.

Problem 33: *Prove that* $\dfrac{S_4}{K_4} \cong S_3$.

Solution: We know that K_4 is normal subgroup of S_4 (See page 155)

Also $o\left(\frac{S_4}{K_4}\right) = \frac{o(S_4)}{o(K_4)} = \frac{24}{4} = 6$

Again $\frac{S_4}{K_4}$ is non-abelian as

$$K_{4(12)}\, K_{4(13)} = K_{4(12)(13)} = K_{4(132)}$$
$$K_{4(13)}\, K_{4(12)} = K_{4(13)(12)} = K_{4(123)}$$

Thus by above remark, $\frac{S_4}{K_4} \cong S_3$

Problem 34: *Show that there are only 4 non isomorphic groups of order 30.*

Solution: Let G be a group of order 30. Then G has a normal subgroup H of order 15 which is cyclic (See problem 7 page 216)

Let $H = < a >$, then $o(a) = 15$

Let $g \in G$ be such that $o(g) = 2$, then $g \notin H$ as $2 \nmid 15$

Since H is normal in G, $g^{-1}ag \in H = < a >$

Thus $g^{-1}ag = a^r$ for some r

$\Rightarrow (g^{-1}ag)^r = a^{r^2}$

$\Rightarrow g^{-1}a^r g = a^{r^2}$

$\Rightarrow g^{-1}(g^{-1}ag)g = a^{r^2}$

$\Rightarrow a = a^{r^2}$

$\Rightarrow a^{r^2-1} = e \Rightarrow o(a) \mid (r^2 - 1)$

$\Rightarrow r^2 \equiv 1 \pmod{15}$

$\Rightarrow r = 1, 4, 11 \text{ or } 14$

giving $g^{-1}ag = a, a^4, a^{11} = a^{-4}, a^{14} = a^{-1}$

So, the four groups of order 30 are

$$G_1 = \{a^{15} = e = g^2, g^{-1}ag = a\}$$
$$G_2 = \{a^{15} = e = g^2, g^{-1}ag = a^4\}$$
$$G_3 = \{a^{15} = e = g^2, g^{-1}ag = a^{-4}\}$$
$$G_4 = \{a^{15} = e = g^2, g^{-1}ag = a^{-1}\}$$

G_4 corresponds to the dihedral group of order 30 and G_1 is an abelian group which is cyclic.

Exercises

1. If N is normal in G and N, $\frac{G}{N}$ are both p-groups, show that G is a p-group.
2. If G is a finite non-trivial p-group, then show that G has a normal subgroup of index p.
3. If a group of order p^n contains exactly one subgroup each of order $p, p^2, \ldots, p^{n-1}$ then show that G is cyclic.

4. Let P be a Sylow p-subgroup of G, prove that $N(N(P)) = (N(P))$.

5. Let P be a Sylow p-subgroup of G and suppose a, b are in the centre of P. Suppose further that $a = xbx^{-1}$ for some $x \in G$. Prove that $\exists\ y \in N(P)$ s.t. $a = yby^{-1}$

(**Hint:** $P \leq N(a)$, $P \leq N(b)$ as $a, b \in Z(P)$
$xPx^{-1} \leq xN(b)x^{-1} \leq N(xbx^{-1}) = N(a)$).

6. If $o(G) = p^2q$ where p, q are primes, show that either Sylow p-subgroup or Sylow q-subgroup is normal in G.

7. If G is a group of order 385, show that both Sylow 7-subgroup and Sylow 11-subgroup are normal in G and Sylow 7-subgroup is in the centre of G.

(**Hint:** Let H, K, L be the subgroups of order 5, 7, 11, then $K, L \trianglelefteq G$ and $HK \leq G$ where $o(HK) = 35$ and so HK is cyclic.
$G = HKL = KLH$
If $x \in K$, $g \in G$ then

$xg = xklh$ $\quad k \in K,\ l \in L,\ h \in H$
$= kxlh$ as K is abelian
$= klxh$ as $K \cap L = \{e\}$, K, L normal
$= klhx$ as HK is abelian
$= gx$

or that $x \in Z(G)$)

8. Let G be group. Prove that $o\left(\dfrac{G}{Z(G)}\right)$ cannot be 77.

9. Let G be a group of order 255. Show that

(i) Sylow 17-subgroup is normal in G.

(ii) $\exists$ a normal subgroup K of order 85.

(iii) $K \subseteq Z(G)$.

(iv) G is cyclic.

10. If G is a non-abelian group of order 231, show that $Z(G)$ is Sylow 11 subgroup of G.

11. Let $o(G) = 108$. Show that either Slow 3-subgroup is normal or there exits a normal subgroup of order 9.

12. If H is a normal subgroup of order p^k of a finite group G, show that H is contained in every Sylow p-subgroup of G.

13. If $o(G) = p^nq$ with $p > q$ primes, show that G contains a unique normal subgroup of index q.

14. Show that groups of order 12, 28, 56 and 200 must contain a normal Sylow subgroup.

15. Show that groups of order 36, 42, 99, 112 and 120 are not simple.

16. Let $o(G) = pq$ where p and q are distinct primes. Prove that G has a proper normal subgroup. Prove further that if neither prime is congruent to 1 modulo the other, then G is abelian.

17. Find a Sylow 2-subgroup of S_4.

18. If p is prime number, give explicit generators for a Sylow p-subgroup of S_{p^2}.

19. Find a Sylow 2-subgroup and a Sylow 3-subgroup of S_6.

20. Show that 21 is the smallest possible odd interger that can be the order of a non-abelian group.

21. Let G_n denote the group of all nth roots of unity w.r.t. multiplication and let p be a fixed prime. Let $G = \bigcup_{m=1}^{\infty} G_{p^m}$ then show that G is a p-group.

22. Show that there are at most three groups of order 21.

Direct Products

The reader is well acquainted with the idea of product of two sets as a set of ordered pairs. We explore the possibility of getting a new group through the product of two groups. Let G_1, G_2 be any two groups.

Let $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$.

What better way could there be than to define multiplication on G by $(g_1, g_2)\,(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$. That G forms a group under this as its composition should not be a difficult task for the reader. Indeed (e_1, e_2) will be identity of G where e_1, e_2 are identities of G_1 and G_2 respectively. Also $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

We call $G = G_1 \times G_2$ *direct product or external direct product* (EDP) of G_1, G_2.

Again if G_1, G_2 are abelian then so would be $G_1 \times G_2$.

In a similar way, we can define external direct product $G_1 \times G_2 \times \ldots \times G_n$ of arbitrary groups G_1, G_2..., G_n as

$$G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

where compostion is component wise multiplication.

If compositions of the groups are denoted by + we also sometimes use the notation $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ to denote the external direct product.

Let $G = G_1 \times \ldots \times G_n$ = direct product of $G_1, \ldots, G_n$.

Define $H_1 = \{g_1, e_2, \ldots, e_n\} \mid g_1 \in G_1, e_i =$ identity of $G_i\}$

$H_2 = \{(e_1, g_2, e_3 \ldots, e_n) \mid g_2 \in G_2\}$.

.....

$H_n = \{(e_1, e_2, e_3 \ldots, g_n) \mid g_n \in G_n\}$

We show that H_1 is normal in G.

$H_1 \neq \varphi$ as $(e_1, e_2, \ldots, e_n) \in H_1$

Let $(g_1, e_2, \ldots, e_n)\,(g'_1, e_2, \ldots, e_n) \in H_1$

Then $(g_1, e_2, \ldots, e_n)\,(g'_1, e_2, \ldots, e_n)^{-1}$

$= (g_1, e_2, \ldots, e_n)\,(g_1^{-1}, e_2, \ldots e_n)$

$= (g_1 g_1^{-1}, e_2, \ldots e_n) \in H_1$

Thus $H_1 \leq G$

Let $g = (g_1 \ldots\ldots g_n) \in G$

$x = (x_1, e_2, \ldots, e_n) \in H_1$

Then $gxg^{-1} = (g_1, \ldots, g_n)\ (x_1, e_2 \ldots, e_n)\ (g_1^{-1}, \ldots, g_n^{-1})$

$= (g_1 x_1 g_1^{-1}, e_2, \ldots e_n) \in H_1$

$\therefore$ H_1 is normal in G.

Similarly, each H_i is normal in G for all $i = 1, \ldots, n$.

Let $g = (g_1, \ldots, g_n) \in G$

Then $g = (g_1, e_2, \ldots, e_n)\ (e_1, g_2, e_3 \ldots e_n) \ldots (e_1, e_2, \ldots, e_{n-1}, g_n) \in H_1 H_2 \ldots H_n$

Suppose $g = h_1 h_2 \ldots h_n = h'_1 h'_2, \ldots, h'_n,\ h_i, h'_i \in H_i$

Then $(g_1, e_2, \ldots, e_n) \ldots (e_1, \ldots e_{n-1}, g_n) = (g'_1, \ldots, e_n) \ldots (e_1, \ldots e_{n-1}, g'_n)$

$\Rightarrow (g_1, \ldots, g_n) = (g'_1 \ldots g'_n)$

$\Rightarrow g_i = g'_i$ for all $i = 1, \ldots, n$

$\Rightarrow h_i = h'_i$ for all $i = 1, \ldots, n$

So, $g \in G$ can be written uniquely as product of elements from $H_1, \ldots, H_n$.

We summarise this through the following definition.

Let $H_1, \ldots, H_n$ be normal subgroups of G. G is said to be an internal direct product (IDP) of $H_1, \ldots, H_n$ if $G = H_1 H_2 \ldots H_n$ and each $g \in G$ can be written uniquely as product of elements from $H_1, \ldots, H_n$.

Example 1: (*a*) Consider the groups $\mathbf{Z}_2 = \{0, 1\}$, $\mathbf{Z}_3 = \{0, 1, 2\}$ under addition modulo. Here $\mathbf{Z}_2 \times \mathbf{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0)\ (1, 1), (1, 2)\}$ will form a group under element wise multiplication (addition). In fact it is a cyclic group generated by (1, 1).

Indeed, $2(1, 1) = (1, 1) + (1, 1) = (1 \oplus_2 1, 1 \oplus_3 1) = (0, 2)$,

$3(1, 1) = (1, 1) + (1, 1) + (1, 1) = (1, 0)$ etc.

We further note that since two cyclic groups of same order are isomorphic, (See remark on page 131) we must have $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.

On the other hand one can show that $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not isomorphic to $\mathbf{Z}_4$. In fact $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic (whereas $\mathbf{Z}_4$ is). If $\mathbf{Z}_2 \times \mathbf{Z}_2$ is cyclic then it has a generator whose order should be same as $o(\mathbf{Z}_2 \times \mathbf{Z}_2) = 4$. But no element of $\mathbf{Z}_2 \times \mathbf{Z}_2$ has order 4. Notice, $2(1, 1) = (0, 0)$ i.e., order of $(1, 1)$ is less then or equal to 2 etc. Hence no element can be generator of $\mathbf{Z}_2 \times \mathbf{Z}_2$. One can show that $\mathbf{Z}_n \times \mathbf{Z}_m \cong \mathbf{Z}_{nm}$ iff n and m are relatively prime. (See problem 36 on page 241).

(*b*) Let us now consider $\mathbf{Z} \times \mathbf{Z}$. We know $\mathbf{Z}$ is cyclic, generated by 1. Would $\mathbf{Z} \times \mathbf{Z}$ be cyclic? Suppose it is and let (a, b) be a generator of $\mathbf{Z} \times \mathbf{Z}$.

Since $(1, 1) \in \mathbf{Z} \times \mathbf{Z}$, $\exists$ an integer m s.t., $(1, 1) = m\ (a, b)$

$\Rightarrow ma = 1,\ mb = 1, \quad m, a, b$ integers

giving the possibilities $a = \pm 1$, $b = \pm 1$. Now $(1, 2) \in \mathbf{Z} \times \mathbf{Z}$ but for no integer t, we can have $(1, 2) = t(a, b) \quad (a = \pm 1, b = \pm 1)$

Hence $\mathbf{Z} \times \mathbf{Z}$ is not cyclic.

Theorem 7: *Let H_1, H_2 be normal in G. Then G is an IDP of H_1 and H_2 if and only if*

(*i*) $G = H_1H_2$

(*ii*) $H_1 \cap H_2 = \{e\}$.

Proof: Suppose G is an IDP of H_1 and H_2. Let $g \in G$.

Then $g = h_1h_2$, $h_1 \in H_1$, $h_2 \in H_2$.

Then $G \subseteq H_1H_2$. But $H_1H_2 \subseteq G$

$\Rightarrow$ $G = H_1H_2$

Let $g \in H_1 \cap H_2 \Rightarrow g \in H_1, g \in H_2$

$\therefore$ $g = ge = eg$ is written in 2 ways as product of elements from H_1 and H_2.

$\therefore$ $g = e \Rightarrow H_1 \cap H_2 = \{e\}$.

Conversely, let $G = H_1H_2$ and $H_1 \cap H_2 = \{e\}$

Let $g \in G \Rightarrow g \in H_1H_2 \Rightarrow g = h_1h_2$, $h_1 \in H_1$, $h_2 \in H_2$

Let $g = h_1h_2 = h'_1h'_2$, $h_1, h'_1 \in H_1$, $h_2, h'_2 \in H_2$

$\Rightarrow h_1^{-1} h'_1 = h_2h_2^{-1} \in H_1 \cap H_2 = \{e\}$

$\Rightarrow h_1 = h'_1, h_2 = h'_2$

$\therefore$ G is an IDP of H_1 and H_2.

Example 2: Let $G = < a >$ be of order 6. Let $H = \{e, a^2, a^4\}$, $K = \{e, a^3\}$ then H and K are normal (G is abelian) subgroups of G. $H \cap K = \{e\}$.

$$HK = \{e, ea^3, a^2e, a^2a^3, a^4e, a^4a^3\}$$
$$= \{e, a^2, a^3, a^4, a^5, a\} = G$$

Hence G is IDP of H and K

Theorem 8: *Let H_1, H_2,..., H_n be normal in G. Then G is an IDP of H_1, H_2,..., H_n if and only if*

(*i*) $G = H_1H_2 \ldots H_n$

(*ii*) $H_i \cap H_1H_2 \ldots H_{i-1} H_{i+1} \ldots H_n = \{e\}$
for all $i = 1, \ldots n$

Proof: Suppose G is an IDP of H_1,..., H_n. Then (*i*) follows from the definition of IDP

Let $g \in H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n$

Then $g = h_i$, $h_i \in H_i$ and $g = h_1h_2 \ldots h_{i-1} h_{i+1} \ldots h_n$, $h_j \in H_j$

$\Rightarrow g = ee \ldots h_i \ldots e$

$g = h_1h_2 \ldots h_{i-1} e h_{i+1} \ldots h_n$

Since this representation of g should be unique we get $e = h_1$, $e = h_2$,..., $h_i = e$,...
or that $g = e$, which proves the result.

Conversely, let $g \in G$ then $g \in H_1 \ldots H_n \Rightarrow g = h_1 \ldots h_n$, $h_i \in H_i$

We show this representation is unique.

Let $g = h'_1 \ldots\ldots h'_n$, $h'_i \in H_i$

$\therefore$ $h_1 \ldots\ldots h_n = h'_1 \ldots\ldots h'_n$

By (*ii*) $H_i \cap H_j = \{e\}$ for all $i \neq j$ because if $x \in H_i \cap H_j$

Then $x \in H_i$, $x \in H_j$. $(j \neq i)$

$$x \in H_j \Rightarrow x \in H_1 \ldots H_j \ldots H_{i-1}\ H_{i+1} \ldots H_n$$

as $x = e \ldots x \ldots e.\ e \ldots e$

$$\Rightarrow x \in H_i \cap H_1 \ldots H_{i-1}\ H_{i+1} \ldots H_n = \{e\}$$

Also H_i is normal in G, H_j is normal in G for all i, j, thus $h_i h_j = h_j h_i$ for all $i \neq j$

$$\therefore \quad h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow h_n = (h_1^{-1} h'_1)\ (h_2^{-1} h'_2) \ldots\ldots\ldots (h_{n-1}^{-1} h'_{n-1})\ h'_n$$

$$\therefore\ h_n\ h_n'^{-1} = (h_1^{-1} h'_1) \ldots\ldots\ldots (h_{n-1}^{-1} h'_{n-1}) \in H_1 \ldots\ldots\ldots H_{n-1} \cap H_n = \{e\}$$

$$\therefore \quad h_n = h'_n$$

Similarly $h_{n-1} = h'_{n-1}, \ldots\ldots, h_1 = h'_1$

Hence G is an IDP of $H_1, \ldots\ldots, H_n$.

Remark: If G is an IDP of $H_1, H_2, \ldots\ldots, H_n$ then $H_i \cap H_j = \{e\}$, $i \neq j$.

We now show that IDP of subgroups of G is isomorphic to their external direct product (EDP).

Theorem 9: *Let G be a group and suppose G is IDP of $H_1, \ldots, H_n$. Let T be EDP of $H_1, \ldots, H_n$. Then G and T are isomorphic.*

Proof: Define $\theta : T \to G$, s.t.,

$$\theta(h_1, \ldots\ldots\ldots, h_n) = h_1 \ldots\ldots\ldots h_n, \quad h_i \in H_i$$

θ is well defined as $(h_1, \ldots, h_n) = (h'_1, \ldots, h'_n)$

$$\Rightarrow h_i = h'_1 \text{ for all } i$$

$$\Rightarrow h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow \theta(h_1, \ldots\ldots\ldots, h_n) = \theta(h'_1, \ldots\ldots\ldots, h'_n)$$

θ is homomorphism as

$$\theta(h_1, \ldots\ldots\ldots, h_n)\ (h'_1, \ldots\ldots\ldots, h'_n)$$

$$= \theta(h_1 h'_1, \ldots\ldots\ldots, h_n h'_n)$$

$$= (h_1 h'_1) \ldots\ldots\ldots (h_n h'_n)$$

$$= (h_1, \ldots, h_n)\ (h'_1, \ldots, h'_n)$$

as $h_i h_j = h_j h_i$

$h'_i h'_j = h'_j h'_i$ for all $i \neq j$

$$= \theta(h_1, \ldots, h_n)\ \theta(h'_1, \ldots, h'_n)$$

θ is 1 – 1 as $\theta(h_1, \ldots, h_n) = \theta(h'_1, \ldots, h'_n)$

$$\Rightarrow h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow h_i = h'_i \text{ for all } i \text{ by definition of IDP}$$

$$\Rightarrow (h_1, \ldots h_n) = (h'_1, \ldots, h'_n)$$

θ is onto as $g \in G \Rightarrow g = h_1 \ldots h_n, \quad h_i \in H_i$

$$= \theta(h_1, \ldots, h_n), \quad (h_1, \ldots, h_n) \in T$$

$\therefore$ θ is an isomorphism.

Hence $G \cong T$.

Problem 35: *Show that a group of order 4 is either cyclic or is an IDP of two cyclic groups of order 2 each.*

Solution: Let G be a non-cyclic group of order 4. then $G \cong K_4$, the Klein's four group. See page 154. Also then $K_4 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ see page 238. Hence $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ where $\mathbf{Z}_2$ is cyclic group of order 2. In view of above theorem then G is IDP of two cyclic groups of order 2 each.

Aliter: Let G be a group of order 4. If $x \in G$, then $o(x) \mid o(G) \Rightarrow o(x) = 1, 2$ or 4.

If $o(x) = 4$, then $x^4 = e$ and $G = \{x, x^2, x^3, x^4 = e\}$ i.e., G will be a cyclic group generated by x

Let now $o(x) \neq 4$, then $o(x) = 2$ if $x \neq e$

Let $a, b \in G$ be such that $o(a) = 2 = o(b)$

Let $A = < a > = \{e, a\}, \quad B = < b > = \{e, b\}$

Then A, B are normal subgroups of G (Notice G is abelian as it has less than 6 elements)

Also $A \cap B = \{e\}$ and as $o(AB) = \dfrac{2 \times 2}{1} = 4 = o(G)$

$G = AB$

i.e., G is an IDP of A, B, two cyclic groups of order 2 each.

See also problem 36.

Problem 36: *Let A, B be finite cyclic groups of order m and n respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.*

Solution: Let $A = < a >$, $B = < b >$

$o(A) = o(a) = m$, $o(B) = o(b) = n$

Suppose $A \times B$ is cyclic.

Let $A \times B = < (x, y) >, \quad x \in A, y \in B$

$o(A \times B) = mn = o(x, y)$

Let g.c.d. of m and n be d.

$\therefore$ $\dfrac{m}{d}$ and $\dfrac{n}{d}$ are relatively prime integers.

Consider $(x, y)^{\frac{mn}{d}} = \left(x^{\frac{mn}{d}}, y^{\frac{mn}{d}} \right)$

$= \left((x^m)^{\frac{n}{d}}, (y^n)^{\frac{m}{d}} \right)$

$= \left(e_1^{\frac{n}{d}}, e_2^{\frac{m}{d}} \right)$, e_1 = identity of A

e_2 = identity of B

$= (e_1, e_2)$

$=$ identity of $A \times B$

$\therefore \quad o(x, y) \left| \frac{mn}{d} \right.$

$\Rightarrow \quad mn \left| \frac{mn}{d} \right.$

$\Rightarrow \quad d . \frac{mn}{d} \left| \frac{mn}{d} \right.$

$\Rightarrow d \mid 1 \Rightarrow d = 1.$

$\therefore$ m and n are relatively prime.

Conversely, let m and n be relatively prime. We show $A \times B$ is cyclic, generated by (a, b). For that we prove $o(a, b) = mn = o(A \times B)$.

Consider $(a, b)^{mn} = (a^{mn}, b^{mn})$

$= ((a^m)^n, (b^n)^m)$

$= (e_1, e_2) =$ identity of $A \times B$

Let $(a, b)^r = (e_1, e_2)$

$\Rightarrow (a^r, b^r) = (e_1, e_2)$

$\Rightarrow a^r = e_1, b^r = e_2$

$\Rightarrow o(a) = m \mid r, o(b) = n \mid r$

$\Rightarrow mn \mid r$ as m, n are relatively prime.

$\Rightarrow mn \leq r$

$\therefore$ $o(a, b) = mn = o(A \times B)$

Hence $A \times B = <(a, b)>$ = cyclic group generated by (a, b).

Remark: One could generalise the above result and say If $G_1, G_2, \ldots, G_n$ be finite cyclic groups of order $m_1, m_2, \ldots, m_n$ then $G_1 \times G_2 \times \ldots \times G_n$ is cyclic if and only if m_i, m_j are relatively prime $(i \neq j)$.

Theorem 10: *Let s and t be relatively prime integers then $U_{st} \cong U_s \times U_t$*

Proof: Define $f : U_{st} \to U_s \times U_t$ s.t.,

$f(x) = (x \bmod s, x \bmod t)$

We show f is an isomorphism.

Let x and y belong to U_{st}

Let $xoy = z$. Then $xy = stq + z, \quad 1 \leq z < st$

so, $f(xoy) = f(z) = (z_1, z_2)$

where $z = sq_1 + z_1, z = tq_2 + z_2, \quad 1 \leq z_1, z_2 < st$

Let $f(x) = (x_1, x_2), f(y) = (y_1, y_2)$

where $x = sq_3 + x_1, \quad y = sq_4 + y_1, \quad 1 \le x_1, y_1 < s$

$x = tq_5 + x_2, \quad y = tq_6 + y_2, \quad 1 \le x_2, y_2 < t$

Now $f(x).f(y) = (x_1, x_2)(y_1, y_2)$

$= (x_1 y_1, x_2 y_2)$

and $x_1 = x - sq_3$

$y_1 = y - sq_4$

So $x_1 y_1 = xy + s \times$ (integer)

But $xy = stq + z \times$ (integer)

Therefore, $x_1 y_1 = s \times$ (integer) $+ z$

Again $z = sq_1 + z_1$

So $x_1 y_1 = s \times$ (integer) $+ z_1 \qquad 1 \le z_1 < st$

Similarly, $x_2 y_2 = t \times$ (integer) $+ z_2 \qquad 1 \le z_2 < st$

Therefore, $x_1 y_1 \equiv z_1 \pmod{s}$ and $x_2 y_2 \equiv z_2 \pmod{t}$

This gives, $f(x) \cdot f(y) = (x_1 y_1, x_2 y_2) = (z_1, z_2) = f(xoy)$.

and so, f is a homomorphism.

Let $f(x) = f(y)$

Then $(x_1, x_2) = (y_1, y_2)$

implies $x_1 \equiv y_1 \pmod{s}$ and $x_2 \equiv y_2 \pmod{t}$

Since, $1 \le x_1, y_1 < s, \quad 1 \le x_2, y_2 < t$

$x_1 = y_1, x_2 = y_2$

or $(x_1, x_2) = (y_1, y_2)$

So, f is one-one

Since s and t are relatively prime integers, there exist integers $\bar{s}$ and $\bar{t}$ such that

$s\bar{s} \equiv 1 \pmod{t}$ and $t\bar{t} \equiv 1 \pmod{s}$

Let $(a, b) \in U_s \times U_t$

Let $z = at\bar{t} + bs\bar{s}$

Then $z - a = a(t\bar{t} - 1) + bs\bar{s}$

$\equiv 0 \pmod{s}$

and $z - b = b(s\bar{s} - 1) + at\bar{t}$

$\equiv 0 \pmod{t}$

Let $z = stu + r, \quad o \le r < st$

If $r = 0$ then $z = stu$

So, $stu - a \equiv 0 \pmod{s}$

implies s divides a

Since $a \in U_s$, $(a, s) = 1$, contradicting s divides a.

Therefore, $r \neq 0$. So, $1 \leq r < st$

Let $(r, st) = d > 1$

Let p be a prime dividing d

Then $p \mid st$.

Let p divide s.

Also, p divides r

So, p divides $stu + r = z$ which implies p divides a as $z \equiv a \pmod{s}$, which is not true as $(a, s) = 1$.

Therefore, $d = 1$ so, $r \in U_{st}$

Now $r \equiv z \pmod{s}$ implies $r \equiv a \pmod{s}$

and $r \equiv z \pmod{t}$ implies $r \equiv b \pmod{t}$

By definition of f, $f(r) = (r \bmod s, r \bmod t) = (a, b)$

Thus f is onto and so f is an isomorphism

Cor: $\phi(st) = \phi(s)\phi(t)$, whenever s and t are relatively prime integers.

Proof: Now $o(U_{st}) = \phi(st)$ and $o(U_s \times U_t) = \phi(s)\phi(t)$

$\therefore$ By above theorem $\phi(st) = \phi(s)\phi(t)$.

Problem 37: *Show that every group of order p^2, p a prime, is either cyclic or is isomorphic to direct product of two cyclic groups, each of order p.*

Solution: Let $o(G) = p^2$. Then G is abelian (Problem 21, page 186) Suppose G is non-cyclic. Since $p \mid o(G)$ $\exists$ $a \in G$ s.t. $o(a) = p$. Let $A = < a >$, $o(A) = o(a) = p$.

Now $A \neq G \Rightarrow \exists\ b \in G$ s.t. $b \notin A$.

Also $o(b) \mid o(G) = p^2 \Rightarrow o(b) = 1, p$ or p^2

If $o(b) = p^2$, then G is cyclic.

If $o(b) = 1$, then $b = e \in A$, a contradiction.

$\therefore$ $o(b) = p$. Let $B = < b >$, $o(B) = o(b) = p$

$$A \cap B \leq A \Rightarrow o(A \cap B) \mid o(A) = p$$
$$\Rightarrow o(A \cap B) = 1 \text{ or } p$$

If $o(A \cap B) = p$, then $A = A \cap B \Rightarrow A \subseteq B \Rightarrow A = B$ as $o(A) = o(B)$, a contradiction as $b \in B$, $b \notin A$

$\therefore$ $o(A \cap B) = 1$

$\therefore$ $A \cap B = \{e\}$

Since G is abelian, A is normal in G, B is normal in G.

Also $$o(AB) = \frac{o(A)\,o(B)}{o(A \cap B)} = p^2 = o(G)$$

$\therefore \qquad G = AB$

By theorem 7, G is an IDP of A and B and by theorem 9, G is isomorphic to EDP of A and B. We also conclude from here that either $G \cong \mathbf{Z}p^2$ or $G \cong \mathbf{Z}_p \times \mathbf{Z}_{p.}$ See problem 33 on page 131.

Problem 38: *Let G be a finite abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.*

Solution: Let $o(G) = p_1^{\alpha 1} \ldots p_r^{\alpha r}$

where $p_1, \ldots, p_r$ are distinct primes.

Since G is abelian, each Sylow subgroup H_i of G is normal. $o(H_i) = p_i^{\alpha i}$.

Let $\quad g \in H_i \cap H_1 \ldots H_{i-1}\, H_{i+1} \ldots H_r$

$\Rightarrow g \in H_i,\ g \in H_1 \ldots H_{i-1}\, H_{i+1} \ldots H_r$

Let $\quad t = p_1^{\alpha 1} \ldots p_{i-1}^{\alpha t-1}\, p_{i+1}^{\alpha i+1} \ldots p_r^{\alpha r}$

$g \in H_1 \ldots H_{i-1}\, H_{i+1} \ldots H_r$

$\Rightarrow g = h_1 \ldots h_{i-1}\, h_{i+1} \ldots h_r,\ \ h_j \in H_j$

$\Rightarrow g^t = h_1^t \ldots h_{i-1}^t\ \ h_{i+1}^t \ldots h_r^t = e$ as $h_j^t = e$ for all $j \neq i$

$\Rightarrow o(g) \mid t$

But $g \in H_i \Rightarrow o(g) \mid o(H_i) = p_i^{\alpha i}$

$\Rightarrow o(g) = p_i^{\beta i},\ \ \beta_i \geq 0$

$\therefore \quad p_i^{\beta i} \mid t$

$\Rightarrow p_i^{\beta i} \mid p_1^{\alpha 1} \ldots p_{i-1}^{\alpha i-1}\, p_{i+1}^{\alpha i+1} \ldots p_r^{\alpha r}$

$\Rightarrow \beta i = 0$

$\Rightarrow o(g) = 1 \Rightarrow g = e.$

$\therefore\ H_i \cap H_1 \ldots H_{i-1}\, H_{i+1} \ldots H_r = \{e\}$ for all $i = 1, \ldots, r$

Now $o(H_1 \ldots\ldots H_r) = \dfrac{o(H_1)\, o(H_2 \ldots H_r)}{o(H_1 \cap H_2 \ldots H_r)} = o(H_1)\ o(H_2 \ldots\ldots H_r)$

Again, $\qquad o(H_2 H_3 \ldots H_r) = \dfrac{o(H_2).\, o(H_3 \ldots H_r)}{o(H_2 \cap H_3 \ldots H_r)}$

Now $\quad x \in H_2 \cap H_3 \ldots H_r$

$\Rightarrow x \in H_2$ and $x \in H_3 \ldots\ldots\ldots H_r \subseteq H_1 H_3 \ldots\ldots H_r$

$\Rightarrow x \in H_2 \cap H_1 H_3 \ldots H_r = \{e\}$

So $\ x = e$

$\therefore \quad o(H_2 \ldots\ldots\ldots H_r) = o(H_2)\ o(H_3 \ldots\ldots H_r)$

In this way, we get

$o(H_1 \ldots\ldots\ldots H_r) = o(H_1)\ o(H_2) \ldots\ldots\ldots o(H_r) = o(G)$

$\Rightarrow G = H_1 \ldots\ldots\ H_r$

By theorem 8, G is an IDP of $H_1, \ldots\ldots H_r$ and so isomorphic to EDP of $H_1, \ldots, H_r$ by theorem 9.

Remark: If G is a finite group and all its Sylow subgroups are normal then G is direct product of its Sylow subgroups.

Problem 39: *Show that if G is a group of order* 45, *it is IDP of its Sylow subgroups.*

Solution: $o(G) = 45 = 3^2 \times 5$.

Number of Sylow 5-subgroups is $(1 + 5k)$ s.t., $(1 + 5k) \mid 9$ which gives $k = 0$

i.e., $\exists$ a unique normal Sylow 5-subgroup H of G where $o(H) = 5$.

Similarly, $\exists$ *a* unique normal Sylow 3-subgroup K of order 9.

Since $o(H \cap K) \mid 9, 5$, we find $o(H \cap K) = 1 \Rightarrow H \cap K = \{e\}$

Also $$o(HK) = \frac{5 \times 9}{1} = 45 = o(G) \Rightarrow G = HK$$

Hence G is IDP of its sylow subgroups H & K.

Problem 40: *Show that there cannot exist any onto homomorphism from* $\mathbf{Z}_{16} \times \mathbf{Z}_2 \to \mathbf{Z}_4 \times \mathbf{Z}_4$

Solution: Suppose f: $\mathbf{Z}_{16} \times \mathbf{Z}_2 \to \mathbf{Z}_4 \times \mathbf{Z}_4$ is an onto homomorphism, then by fundamental theorem of group homomorphism

$$\mathbf{Z}_4 \times \mathbf{Z}_4 \cong \frac{\mathbf{Z}_{16} \times \mathbf{Z}_2}{\text{Ker } f}$$

$$\Rightarrow o(\mathbf{Z}_4 \times \mathbf{Z}_4) = o\left(\frac{\mathbf{Z}_{16} \times \mathbf{Z}_2}{\text{Ker } f}\right) = \frac{o(\mathbf{Z}_{16} \times \mathbf{Z}_2)}{o(\text{Ker } f)}$$

$$\Rightarrow 16 = \frac{32}{o(\text{Ker } f)} \quad \text{or that} \quad o(\text{Ker } f) = 2$$

Now one element of Ker f is (0,0) and the other has to have order 2 [$a \in G \Rightarrow o(a) | o(G)$] and elements of order 2 in $\mathbf{Z}_{16} \times \mathbf{Z}_2$ are (8, 0), (8, 1) and (0, 1).

Thus possible values of Ker f are

$$\{(0, 0), (8, 0)\},\ \{(0, 0), (8, 1)\},\ \{(0, 0), (0, 1)\}.$$

Let $K = \text{Ker } f = \{(0, 0), (8, 0)\}$ then

$$\frac{\mathbf{Z}_{16} \times \mathbf{Z}_2}{K} \cong \mathbf{Z}_4 \times \mathbf{Z}_4$$

Now $K + (1, 0) \in \dfrac{\mathbf{Z}_{16} \times \mathbf{Z}_2}{K}$ and

$$(K + (1,0)) + (K + (1, 0)) + \ldots + (K + (1, 0)) = (K + (8, 0)) \text{ 8 times}$$
$$= K \text{ as } (8, 0) \in K$$

Thus $o(K + (1, 0)) = 8$ in the quotient group $\dfrac{\mathbf{Z}_{16} \times \mathbf{Z}_2}{K}$. But there is no element of order 8 in $\mathbf{Z}_4 \times \mathbf{Z}_4$. Thus the above isomorphism cannot hold.

Again, suppose now $K = \text{Ker } f = \{(0, 0), (8, 1)\}$

or $= \{(0, 0), (0, 1)\}$

then since $K+(1,1)\in\dfrac{\mathbf{Z}_{16}\times\mathbf{Z}_2}{K}$ and $o(K + (1, 1)) = 16$

and there is no element of order 16 in $\mathbf{Z}_4 \times \mathbf{Z}_4$, the result fails.

Problem 41: *Let N be normal in G. If G = H × K where H, K are subgroups of G, then prove that either N is abelian or N intersects H or K non-trivially.*

Solution: Suppose $N \cap H = \{e\}$, $N \cap K = \{e\}$.

Since $G = H \times K$, H is normal in G, K is normal in G. So $nh = hn$ for all $n \in N$, $h \in H$ and $nk = kn$ for all $n \in N$, $k \in K$.

Let $n_1, n_2 \in N$.

$$n_2 \in N \Rightarrow n_2 \in G \Rightarrow n_2 = h_2k_2, \quad h_2 \in H, k_2 \in K$$

$$\begin{aligned} \therefore \quad n_1n_2 &= n_1h_2k_2 \\ &= h_2n_1k_2 \\ &= h_2k_2n_1 \\ &= n_2n_1 \end{aligned}$$

So, N is abelian.

Problem 42: *Let m and n be relatively prime integers. Let u, v be any integers. Show that* $\exists$ *an integer t s.t.* $t \equiv u \pmod m$ *and* $t \equiv v \pmod n$.

(This is a special case of the *Chinese Remainder Theorem.* See page 41).

Solution: Let $\mathbf{Z}_m$, $\mathbf{Z}_n$ denote the groups under addition modulo m, n respectively. $\mathbf{Z}_m$ and $\mathbf{Z}_n$ are cyclic groups generated by 1. By problem 35, $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic group generated by (1, 1).

Let $u = mq_1 + r, \quad 0 \le r < m$

$v = nq_2 + s, \quad 0 \le s < n$

$\therefore \quad r \in \mathbf{Z}_m, s \in \mathbf{Z}_n$

$\therefore \quad (r, s) \in \mathbf{Z}_m \times \mathbf{Z}_n$

$\therefore$ $\exists$ integer t s.t., $(r, s) = t\,(1, 1)$

$$\therefore \quad (r, s) = (\underbrace{1\oplus\ldots\oplus 1}_{t \text{ times}}, \ \underbrace{1\oplus\ldots\oplus 1}_{t \text{ times}})$$

where the composition in first coordinate is under addition modulo m and in second, under addition modulo n.

$\therefore \quad (r, s) = (t - mq_3, t - nq_4)$

$\therefore \quad r = t - mq_3, s = t - nq_4$

$\therefore \quad u = mq_1 + t - mq_3$

$v = nq_2 + t - nq_4$

$\therefore \quad t \equiv u \pmod m$

$t \equiv v \pmod n$

Problem 43: (*a*) *Show that* S_3 *cannot be written as internal direct product of two non-trivial subgroups.*

(*b*) *Show that the Quaternion group cannot be written as IDP of its non trivial subgroups.*

Solution: Suppose S_3 is an internal direct product of its subgroups H and K where $H \neq \{I\}$, $K \neq \{I\}$

Then $S_3 = HK, \quad H \cap K = \{I\}$

H is normal in S_3, K is normal in S_3

$\Rightarrow o(S_3) = 6 = o(H)\, o(K)$

$\Rightarrow$ Either $o(H) = 2$ or $o(K) = 2$

as $o(H)$ and $o(K) > 1$

In S_3, subgroups of order 2 are $\{I, (12)\}$, $\{I, (13)\}$, $\{I, (23)\}$ and none of these is normal subgroup of S_3.

$\therefore$ S_3 can't be written as IDP of two non-trivial subgroups.

Again we know (See exercise 14, page 97) that all the non-trivial subgroups of the quaternion group contain 1 and –1 and thus the condition $H_i \cap H_j = (e)\ \forall\ i \neq j$ does not hold. Hence by remark on page 240, result follows.

Problem 44: *If H, K are normal subgroups of G, show that* $\frac{G}{H \cap K}$ *is isomorphic to a subgroup of* $\frac{G}{H} \times \frac{G}{K}$.

Solution: Define $\theta : G \to \frac{G}{H} \times \frac{G}{K}$ s.t.,

$$\theta(x) = (Hx,\ Kx) \quad \text{for all } x \in G$$

θ is well defined as $x = y \Rightarrow Hx = Hy,\ Kx = Ky \Rightarrow (Hx, Kx) = (Hy, Ky)$.

θ is a homomorphism as

$$\begin{aligned}\theta(xy) &= (Hxy,\ Kxy)\\ &= (HxHy,\ KxKy)\\ &= (Hx,\ Kx)\ (Hy,\ Ky)\\ &= \theta(x)\ \theta(y) \quad \text{for all } x, y \in G\end{aligned}$$

$$\begin{aligned}\text{Ker } \theta &= \{x \in G \mid \theta(x) = \text{identity of } \frac{G}{H} \times \frac{G}{K}\}\\ &= \{x \in G \mid (Hx,\ Kx) = (H,\ K)\}\\ &= \{x \in G \mid Hx = H,\ Kx = K\}\\ &= \{x \in G \mid x \in H,\ x \in K\}\\ &= \{x \in G \mid x \in H \cap K\}\\ &= H \cap K.\end{aligned}$$

$\therefore$ $\frac{G}{\text{Ker } \theta} = \frac{G}{H \cap K}$ is isomorphic to $\theta(G)$

(Note θ is onto map from G to $\theta(G)$)

Also, $\theta(G)$ is a subgroup of $\frac{G}{H} \times \frac{G}{K}$.

$\therefore$ $\frac{G}{H \cap K}$ is isomorphic to a subgroup of $\frac{G}{H} \times \frac{G}{K}$.

Theorem 11: *Let G and H be finite groups of orders m and n respectively. Suppose that g.c.d.(m, n) = 1. Then*

$$Aut\ G \times Aut\ H \cong Aut\ (G \times H)$$

Proof: Define θ : Aut $G \times$ Aut $H \to$ Aut $(G \times H)$, s.t.,

$\theta(\sigma, \eta) = \sigma \times \eta$

where $(\sigma \times \eta)$: $G \times H \to G \times H$ is a mapping s.t.,

$(\sigma \times \eta)(x, y) = (\sigma(x), \sigma(y))$

We show that $\sigma \times \eta \in$ Aut $(G \times H)$

Consider $(\sigma \times \eta)[(x, y)\cdot(x', y')]$

$= (\sigma \times \eta)(xx', yy')$

$= (\sigma(xx'), \eta(yy'))$

$= (\sigma(x)\sigma(x'), \eta(y)\eta(y'))$

$= (\sigma(x), \eta(y))\ (\sigma(x'), \eta(y'))$

$= [(\sigma \times \eta)(x, y)][(\sigma \times \eta)(x', y')]$

So, $\sigma \times \eta$ is a homomorphism

Let $(\sigma \times \eta)(x, y) = (\sigma \times \eta)(x', y')$

Then $(\sigma(x), \eta(y)) = (\sigma(x'), \eta(y'))$

$\Rightarrow \sigma(x) = \sigma(x'), \eta(y) = \eta(y')$

$\Rightarrow x = x', y = y'$ as σ, η as are one-one

$\Rightarrow (x, y) = (x', y')$

So, $\sigma \times \eta$ is one-one

Since $G \times H$ is finite, $\sigma \times \eta$ is also onto.

Therefore, $\sigma \times \eta \in$ Aut $(G \times H)$

Let $\sigma, \sigma' \in$ Aut G, $\eta, \eta' \in$ Aut H

Then $(\sigma \times \eta)(\sigma' \times \eta')(x, y) = (\sigma \times \eta)(\sigma'(x), \eta'(y))$

$= (\sigma\sigma'(x), \eta\eta'(y))$

Also $(\sigma\sigma' \times \eta\eta')(x, y) = (\sigma\sigma'(x), \eta\eta'(y))$ for all $x \in G, y \in H$

So $(\sigma \times \eta)(\sigma' \times \eta') = \sigma\sigma' \times \eta\eta'$

Now $\theta((\sigma, \eta)(\sigma', \eta')) = \theta(\sigma\sigma', \eta\eta')$

$= \sigma\sigma' \times \eta\eta'$

$= (\sigma \times \eta)(\sigma' \times \eta')$

$= \theta(\sigma, \eta)\theta(\sigma', \eta')$

So, θ is a homomorphism

Let $\theta(\sigma, \eta) = \theta(\sigma', \eta')$

Then $\sigma \times \eta = \sigma' \times \eta'$

$\Rightarrow (\sigma \times \eta)(x, y) = (\sigma' \times \eta')(x, y)$

$\Rightarrow (\sigma(x), \eta(y)) = (\sigma'(x), \eta'(y))$

$\Rightarrow \sigma(x) = \sigma'(x), \eta(y) = \eta'(y)$ for all $x \in G, y \in H$

$\Rightarrow \sigma = \sigma', \eta = \eta'$

$\Rightarrow (\sigma, \eta) = (\sigma', \eta')$

$\Rightarrow \theta$ is 1–1

Since g.c.d. $(m, n) = 1$, there exist integers u and v

Sucth that $mu + nv = 1$

Let $\tau \in$ Aut $(G \times H)$

Let e be the identity of G and f be the identity of H

Let $x \in G$

and suppose $\tau(x', f) = (x', f)$

Now $x = x^1 = x^{mu + nv} = x^{mu} \cdot x^{nv} = x^{nv}$ as $x^m = x^{o(G)} = e$

So, $\tau(x, f) = \tau(x^{nv}, f) = \tau(x^{nv}, f^{nv}) = [\tau(x, f)]^{nv}$

$\Rightarrow (x', f) = [\tau(x, f)]^{nv}$

$\Rightarrow (x', f)^{-nv} = [\tau(x, f)]$

$\Rightarrow ((x')^{-nv}, (f)^{-nv}) = \tau(x, f)$

$\Rightarrow (x'', f) = \tau(x, f)$, where $x'' = (x')^{-nv}$

Define: $\sigma: G \to G$ s.t.,

$\sigma(x) = x'$, where $\tau(x, f) = (x', f)$

We show that $\sigma \in$ Aut G

Now $\tau(x_1x_2, f) = \tau[(x_1, f)\ (x_2, f)] = \tau(x_1, f)\ \tau(x_2, f)$

$\Rightarrow (x_1\ x_2)' = x_1'\ x_2'$

Therefore, $\sigma(x_1x_2) = (x_1x_2)' = x_1'\ x_2' = \sigma(x_1)\sigma(x_2)$

$\Rightarrow \sigma$ is a homomorphism

Let $\sigma(x_1) = \sigma(x_2)$

Then $x_1' = x_2'$

Now $\tau(x_1, f) = (x_1', f) = (x_2', f) = \tau(x_2, f)$

$\Rightarrow (x_1, f) = (x_2, f) \Rightarrow x_1 = x_2$

So, σ is one-one

Since G is finite, σ is also onto.

Therefore, $\sigma \in$ Aut G. Similarly

Define $\eta: H \to H$ s.t.,

$\eta(y) = y'$, where $\tau(e, y) = (e, y')$

Then $\eta \in$ Aut H

So $\theta(\sigma, \eta) = \sigma \times \eta = \tau$

as $\tau(x, y) = \tau[(x, f)\ (e, y)] = \tau(x, f)\ \tau(e, y)$

$= (x', f)(e, y') = (x', y')$

and $(\sigma \times \eta)(x, y) = (\sigma(x), \eta(y)) = (x', y')$

Hence θ is an isomorphism

Remark: The above result may not be true if g.c.d $(m, n) \neq 1$.

Consider $G = \mathbf{Z}_2 = H$

Then Aut $\mathbf{Z}_2 = \{I\}$ and Aut $(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$

as $\mathbf{Z}_2 \times \mathbf{Z}_2 \cong K_4$ and Aut $K_4 \cong S_3$)

So, Aut $\mathbf{Z}_2 \times$ Aut $\mathbf{Z}_2 = \{I\} \times \{I\}$

$\Rightarrow o(\text{Aut } \mathbf{Z}_2 \times \text{Aut } \mathbf{Z}_2) = 1$

while $o(\text{Aut } (\mathbf{Z}_2 \times \mathbf{Z}_2)) = o(S_3) = 6$

Therefore, Aut $\mathbf{Z}_2 \times$ Aut $\mathbf{Z}_2$ is not isomorphic to Aut $(\mathbf{Z}_2 \times \mathbf{Z}_2)$

Note: In two isomorphic groups the number of elements with a specific order will be same in both. The converse, however, may not hold as is evident by

Example 3: Let G be the set of matrices of the type $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ where $a, b, c \in F_3$. Here $F_3 = \{0, 1, 2\}$ mod 3 (See under chapter VII on Rings)

Then one can check that G forms a non-abelian group. In fact, it would be a subgroup of the groups of all 3×3 non-singular matrices over F_3.

Since each of a, b, c have three choices, $o(G) = 3^3$.

Order of each non-identity element of G will be 3 as

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2b + ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} \neq I \text{ as one of } a, b, c \text{ is non-zero}$$

and $$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If we consider the group $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$, then it is an abelian group of order 27 in which each non-identity element is of order 3. Thus both the groups have 26 elements of order 3 (plus one identity). But G and $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ cannot be isomorphic as one is abelian and the other a non-abelian group.

Exercises

1. If H, K are subgroups of a group G s.t. $G = H \times K$, show that

$$\frac{H \times K}{H \times \{e\}} \cong K, \quad \frac{G}{H} \cong K, \quad \frac{G}{K} \cong H.$$ [**Hint.** use Fundamental Theorem]

2. Let G_1, G_2, G_3 be groups. Show that

(*i*) $G_1 \times G_2 \cong G_2 \times G_1$ (*ii*) $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3$.

3. If G is an IDP of H and K, where H, K are abelian then show that G is abelian. Hence show that a group of order 99 is abelian.
4. Let G be a group. Let $H = \{(g, g) \mid g \in G\}$, Show that $H \leq G \times G$ and H is normal in $G \times G$ if and only if G is abelian. H is called *diagonal* of $G \times G$.
5. Show that
   (*i*) $Z(G_1 \times G_2 \times ... \times G_n) = Z(G_1) \times Z(G_2) \times ... \times Z(G_n)$
   (*ii*) $N(g_1, g_2, ..., g_n) = N(g_1) \times N(g_2) \times ... \times N(g_n)$, $g_i \in G_i$
6. Show that the multiplicative group of non-zero real numbers is an internal direct product of two non-trivial subgroups.
7. Show that the group G of non-zero complex numbers under multiplication is IDP of the group of +ve reals under multiplication and the circle group N of complex numbers with absolute value 1. (See exercise 16 on page 143 also).
8. Prove that the group **Q** of all rational numbers under addition can't be written as direct sum of two non-trivial subgroups.
9. If N_1 is normal in G_1 and N_2 is normal in G_2 than show that $N_1 \times N_2$ is normal in $G_1 \times G_2$ and $\dfrac{G_1 \times G_2}{N_1 \times N_2} \cong \dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$.
10. Let G be EDP of two finite groups A and B. Show that the order of element $(a, b) \in G = A \times B$ is l.c.m.$(o(a), o(b))$. Generalise the result.
11. If $G_1, G_2, ..., G_n$ are groups such that their orders are pairwise coprime, then show that
    Aut $G_1 \times$ Aut $G_2 \times ... \times$ Aut $G_n \cong$ Aut $(G_1 \times G_2 \times ... \times G_n)$
    (**Hint:** Use induction on n)

Finite Abelian Groups

Having studied direct products, one would like to know whether groups can be written as direct product of some 'simple looking' groups, Luckily, such a class of groups exists, namely finite abelian groups. The main purpose of this section is to prove that all important theorem called fundamental theorem on finite abelian groups which states that a finite abelian group is a direct product of cyclic groups of prime power order and the representation is unique except for the order in which the factors are arranged. This paves the way for us to spell out the method that gives the number of non-isomorphic finite abelian groups of a given order.

We first show that a finite abelian group can be written as a direct product of p-groups. (See problem 38 for different proof).

Theorem 12: *A finite abelian group is a direct product of its Sylow p-subgroups.*

Proof: Let G be a finite abelian group of order n. Let $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$ $p_i's$ being distinct primes.
Let $S_1,...S_r$ be distinct Sylow p_i-subgroups respectively. $o(S_i) = p_i^{\alpha_i}$ for all $i = 1,..., r$
We show that $G = S_1 \times ... \times S_r$
Since G is abelian, each S_i is a normal subgroup of G.

Let $m = p_2^{\alpha_2} \ldots p_r^{\alpha_r}$

and $T = \{x \in G \mid x^m = e\}$ Then $(p_1^{\alpha_1}, m) = 1$

and T is a subgroup of G as G is abelian.

Now $x \in S_1 \cap T \Rightarrow o(x) \mid o(S_1) = p_1^{\alpha_1}$

and $o(x) \mid m$

So, $o(x) \mid (p_1^{\alpha_1}, m) = 1$

$\Rightarrow o(x) = 1$

$\Rightarrow x = e$

$\therefore$ $S_1 \cap T = \{e\}$

As $(p_1^{\alpha_1}, m) = 1$, $\exists$ integers u, v such that

$up_1^{\alpha_1} + vm = 1$

Let $x \in G$. Then $x = x^1$

$= x^{up1^{\alpha_1} + vm}$

$= x^{vm} \cdot x^{up1^{\alpha_1}}$

$\in S_1$. T (as $(x^{vm})^{p1^{\alpha_1}} = (x^{p1^{\alpha_1}m})^v = x^{vn} = (x^n)^v = e$

$\Rightarrow o(x^{vm}) \mid p_1^{\alpha_1}$

$\Rightarrow o(x^{vm}) = p_1^{\beta_1}$

$\Rightarrow < x^{vm} >$ is a p_1 group

$\Rightarrow < x^{vm} > \subseteq S_1$

$\Rightarrow x^{vm} \in S_1$

Also $(x^{up1^{\alpha_1}})^m = x^{un} = e$

$\Rightarrow x^{up1^{\alpha_1}} \in T$)

$\therefore$ $G = S_1T$. Also as seen earlier $S_1 \cap T = \{e\}$

Since G is abelian, S_1 and T are normal subgroups of G, and thus G is IDP of S_1 and T

$\therefore$ $G = S_1 \times T$ (because of the isomorphism)

Also, $o(G) = o(S_1T)$

$= o(S_1)\ o(T)$

$\Rightarrow n = p_1^{\alpha_1}\ o(T)$

$\Rightarrow o(T) = p_2^{\alpha_2} \ldots p_r^{\alpha_r} = m$

As above, we can show that

$T = S_2 \times U$, where U is a subgroup of T such that $o(U) = p_3^{\alpha_3} \ldots p_r^{\alpha_r}$. In this way, we shall have

$$G = S_1 \times S_2 \ldots S_r$$

which proves the theorem.

Remark: Since a Sylow p-subgroup is a group of prime power order, we have established that *A finite abelian group is a direct product of groups of prime power order.*

Having *broken* G into product of groups of prime power order, we concentrate now on results pertaining to abelian groups of prime power order rather than on G itself.

Theorem 13: *Let G be an abelian group of prime power order p^n and let $a \in G$ have maximal order amongst all elements in G. Then G is IDP of A and K, where A is the cyclic subgroup generated by a and $K \leq G$. Hence G can be expressed as $G = A \times K$.*

Proof: Let $o(G) = p^n$, p a prime.

We use induction on n. If $n = 1$ then $o(G) = p$, a prime and thus G is a cyclic group of order p and if $G = \langle a \rangle$ then a is an element of maximal order p in G and also then $G = \langle a \rangle \times \{e\}$ and so the result holds for $n = 1$.

Let the result be true for abelian groups of order p^k, where $k < n$.

Let $a \in G$ be an element of maximal order and suppose $o(a) = p^m$.

In case $G = \langle a \rangle$, then $G = \langle a \rangle \times \{e\}$ and there is nothing to prove.

So assume, $G \neq \langle a \rangle$. Thus $\exists$ elements in G which are not in $\langle a \rangle = A$. Out of these elements let b be an element of minimal order.

Now $$o(b^p) = \frac{o(b)}{\text{g.c.d.}(o(b), p)} = \frac{o(b)}{p} < o(b).$$ (See Page 93)

Note as $o(b) | o(G) = p^n$, $o(b)$ is of the type p^i for some i.

So $o(b^p) < o(b) \Rightarrow b^p \in A$ as b is of minimal order s.t., $b \notin A$.

Now $b^p \in A = \langle a \rangle \Rightarrow b^p = a^i$ for some i

If $x \in G$ be any element then as

$o(x) | o(G) = p^n$, $o(x) = p^t$ for some t

and so $x^{p^t} = e$

Again as $o(a) = p^m$ is maximal order of an element in G, $p^t \leq p^m$ i.e., $p^t \mid p^m$

and so $x^{p^m} = e \quad \forall\, x \in G$

$\Rightarrow b^{p^m} = e$

Thus $$e = b^{p^m} = \left(b^p\right)^{p^{m-1}} = \left(a^i\right)^{p^{m-1}}$$

$\Rightarrow o(a^i) \leq p^{m-1}$

$\Rightarrow a^i$ cannot be a generator of $A = \langle a \rangle$ as $o(A) = o(a) = p^m$ and $o(a^i) < p^m$

$\Rightarrow (p^m, i) \neq 1$ (See theorem 30, page 88)

So p^m and i have common factors

$\Rightarrow p \mid i$ or that $i = pj$

$\Rightarrow b^p = a^i = a^{pj}$

Let $c = a^{-j}b$ then if $c \in A$, then $a^{-j}b \in A$

$\Rightarrow a^{-j}b = a_1$ for some $a_1 \in A$.

$\Rightarrow b = a^j a_1 \in A$, which is not true. Hence $c \notin A$

Again $c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e,\ c \neq e$

$\Rightarrow o(c) = p$

i.e., $\exists$ an element $c \in G$ s.t., $c \notin A$ and $o(c) = p$.

So $o(b)$ should also be p as b has minimal order

Let $B = < b >$, then $o(B) = o(b) = p$

Also, $A \cap B \leq B \Rightarrow o(A \cap B) | o(B) = p$

$\Rightarrow o(A \cap B) = 1$ or p.

If $o(A \cap B) = p$, then $o(A \cap B) = o(B)$

$\Rightarrow A \cap B = B \Rightarrow B \subseteq A$

which is not possible as $b \notin A$

Hence, $o(A \cap B) = 1$ or that $A \cap B = \{e\}$

Let $\bar{G} = G/B$.

Since $a \in G$, $Ba \in G/B = \bar{G}$

Let $Ba = \bar{a} \in \bar{G}$

Now $(\bar{a})^{o(a)} = (Ba)^{o(a)} = Ba \cdot Ba \cdots Ba = Ba^{o(a)} = Be = B =$ Identity of $\bar{G}$

$\therefore$ $o(\bar{a}) \mid o(a)$ (1)

Again, $Ba^{o(\bar{a})} = (Ba)^{o(\bar{a})} = (Ba)^{o(Ba)} = B =$ Identity of $\bar{G}$

$\Rightarrow o(\bar{a}) \in B$

Also, $a^{o(\bar{a})} \in A \Rightarrow a^{o(\bar{a})} \in A \cap B = \{e\}$

$\Rightarrow a^{o(\bar{a})} = e \Rightarrow o(a) \mid o(\bar{a}) \Rightarrow o(a) = o(\bar{a})$ from (1)

Now $\bar{a}$ will be an element of maximal order in $\bar{G}$ as if $\bar{c} \in \bar{G}$ is an element with more order than $o(\bar{a})$ then

as $o(\bar{c}) \mid o(c)$ as in (1), we get

$o(\bar{c}) \leq o(c) \Rightarrow o(c) \geq o(\bar{c}) > o(\bar{a}) = o(a)$

contradicting the fact that a is of maximal order.

Now $o(\bar{G}) < o(G)$ and so using induction we can say $\bar{G}$ is an IDP of $< \bar{a} >$ and $\bar{T}$ for some subgroup $\bar{T}$ of $\bar{G}$ and

$$\bar{G} = < \bar{a} > \bar{T}, \quad < \bar{a} > \cap \bar{T} = \{\bar{e}\}$$

$\bar{T}$ is a subgroup of $\bar{G} = G/B \Rightarrow \bar{T} = \dfrac{K}{B}$ for some $K \leq G$

We show G is IDP of A and K

Let $x \in A \cap K$ then $x \in A$ and $x \in K$

$\Rightarrow x = a^i$ for some i

and $x \in K \Rightarrow a^i \in K \Rightarrow Ba^i \in \overline{T}$

$\Rightarrow (Ba)^i \in \overline{T}$

$\Rightarrow (\overline{a})^i \in \overline{T}$

$\Rightarrow (\overline{a})^i \in <\overline{a}> \cap \overline{T} = \{\overline{e}\}$

$\Rightarrow (\overline{a})^i = \overline{e} \Rightarrow Ba^i = Be \Rightarrow a^i \in B$

$\therefore$ $a^i \in A \cap B = \{e\} \Rightarrow a^i = e$

$\therefore$ $x = a^i = e \Rightarrow A \cap K = \{e\}$

Now let $x \in G$ then $\overline{x} = Bx \in \overline{G} = <\overline{a}> \cdot \overline{T}$

$\Rightarrow \overline{x} = (a^{-j})\overline{y}, \quad \overline{y} \in \overline{T} = K/B$

$\Rightarrow Bx = (Ba)^j By = Ba^j y \qquad (\overline{y} = By)$

$\Rightarrow xy^{-1}a^{-j} \in B \subseteq K$

$\Rightarrow xy^{-1}a^{-j} = k$ for some $k \in K$

$\Rightarrow x = ka^j y = a^j z$ for some $z \in K$

or that $x \in <a>.K \Rightarrow G \subseteq AK$

i.e., $G = AK$, $A \cap K = \{e\}$

So G is an IDP of A and K and can be expressed as $A \times K$.

We are now ready to prove the fundamental theorem on finite abelian groups.

Theorem 14: (The Fundamental Theorem on Finite Abelian Groups). *A finite abelian group is direct product of cyclic groups of prime power order*.

Proof: Let G be a finite abelian group. We prove the result by induction on $o(G)$. If $o(G) = 1$, then result is trivially true. Assume that the result is true for all abelian groups of order $< o(G)$.

Let $o(G) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, p_is are distinct primes.

By theorem 12, $G = S_1 \times \ldots \times S_r$, where S_i is the Sylow p_i-subgroup of order $p_i^{\alpha i}$ ($i = 1, 2, \ldots, r$). i.e., a subgroup of prime power order.

By theorem 13, $S_i = A_i \times K_i$, where each A_i is a cyclic group.

$\Rightarrow G = (A_1 \times K_1) \times \ldots \times (A_r \times K_r)$

$= (A_1 \times \ldots \times A_r) \times (K_1 \times \ldots \times K_r)$

Now $o(K_1 \times \ldots \times K_r) < o(G)$ and $K_1 \times K_2 \ldots \times K_r$ is an abelian group. By induction hypothesis $K_1 \times \ldots \times K_r = T_1 \times \ldots \times T_s$, where each T_i is a cyclic subgroup of G of prime power order.

$\therefore$ $G = A_1 \times ... \times A_r \times T_1 \times ... \times T_s$

= direct product of cyclic subgroups of prime power orders.

$\therefore$ result is true in this case as well.

By induction result is true for all finite abelian groups G.

Note: By theorem 13, S_i is IDP of A_i and K_i

i.e., $S_i = A_i K_i, \quad A_i \cap K_i = \{e\}$

$$\therefore \quad o(S_i) = \frac{o(A_i)o(K_i)}{o(A_i \cap K_i)} = o(A_i)o(K_i)$$

But $o(S_i) = p_i^{\alpha_i}$ = prime power and thus $o(A_i)$ and $o(K_i)$ being its divisors are also prime powers.

Summing up, we notice that any finite abelian group is product of $S_1, S_2, ...,S_n$ where each S_i is a group of prime power order and each S_i is then a product of cyclic groups of prime power order. To tackle the uniqueness issue, we notice that each S_i is unique as if $x \in S_i$ then $o(x) \mid o(S_i) = p_i^{\alpha_i} \Rightarrow o(x) = p_i^{\beta i}$ and thus $x \notin S_j$ for any $j \neq i$.

We wind up the whole process by proving

Theorem 15: *Let G be a finite abelian group of order p^n, p a prime. Suppose $G = A_1 \times ... \times A_k$ where each A_i is a cyclic group of order p^{ni} with $n_1 \geq n_2 \geq ... \geq n_k > 0$. Then the integers $n_1,..., n_k$ are uniquely determined,* (*called invariants of G*).

In other words, if G is a finite abelian group of prime power order p^n and

$$G = A_1 \times A_2 \times ... \times A_k$$
$$G = B_1 \times B_2 \times ... \times B_l$$

where A_i and B_j are non trivial cyclic subgroups with

$$o(A_1) \geq o(A_2) \geq ... \geq o(A_k) > 0$$
$$o(B_1) \geq o(B_2) \geq ... \geq o(B_l) > 0$$

then $k = l$ and $o(A_i) = o(B_i)\ \forall i$.

Proof: Suppose $G = A_1 \times ... \times A_k$

and $G = B_1 \times ... \times B_l$

where A_i and $B_j s$ are cyclic groups s.t. $o(A_i) = p^{ni}$, $o(B_j) = p^{hj}$,

$n_1 \geq n_2 \geq ... \geq n_k > 0$, $h_1 \geq h_2 \geq ... \geq h_l > 0$

Our aim is to show that $k = l$ and $n_i = h_i$ for all i. Let $g \in G$. Then $g = a_1 a_2 ... a_k$, $a_i \in A_i$

Since $n_1 \geq n_i$ for all $i = 1,..., k$

$p^{ni} \mid p^{n1}$ for all $i = 1,..., k$

$\therefore$ $p^{n1} = p^{ni}\, p^{ui}$ for all $i = 1,..., k$

So, $g^{p^{n1}} = a_1^{p^{n1}}\, a_2^{p^{n1}} \ ... \ a_k^{p^{n1}}$

$= a_1^{p^{n1}}\, a_2^{p^{n2} p^{u2}} \cdots a_k^{p^{nk} p^{uk}}$

$= e$ as $(a_i)^{p^{ni}} = a_i^{o(Ai)} = e$ for all i

$\therefore \quad o(g) \mid p^{n_1}$ for all $g \in G$

$\Rightarrow o(g) \leq p^{n_1}$ for all $g \in G$

Also A_1 is a cyclic group of order $p^{n_1} \Rightarrow \exists$ an element of order p^{n_1}.

So p^{n_1} is the maximal order of elements in G. Similarly, by taking

$G = B_1 \times \ldots \times B_l$, we get p^{h_1} to be the maximal order of elements in G.

$\therefore \quad p^{n_1} = p^{h_1} \Rightarrow n_1 = h_1$

Suppose we have proved that $n_1 = h_1$, $n_2 = h_2, \ldots, n_{t-1} = h_{t-1}$. Suppose $n_t \neq h_t$. Let $n_t > h_t = m$. Define $C = \{x^{p^m} \mid x \in G\}$. Since G is abelian, C is subgroup of G.

Let $A_1 = <a_1>, \ldots, A_k = <a_k>$, $o(a_i) = o(A_i) = p^{n_i}$

$B_1 = <b_1>, \ldots, B_k = <b_k>$, $o(b_j) = o(B_j) = p^{h_j}$

We claim that

$$C = <b_1^{p^m}> \times \ldots \times <b_{t-1}^{p^m}>$$

Let $x^{p^m} \in C$, $x \in G$

Now $x \in G \Rightarrow x = x_1 \ldots x_{t-1} x_t \ldots x_l$, $x_j \in B_j$

$x_j \in B_j \Rightarrow x_j = b_j^{r_j}$

$$\therefore \quad x^{p^m} = x_1^{p^m} \ldots x_l^{p^m}$$

$$= b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m} b_t^{r_t p^m} \ldots b_l^{r_1 p^m},$$

Now for all $j \geq t$, $o(B_j) = p^{h_j} \mid p^{h_t} = p^m$

$\Rightarrow p^m = p^{h_j} p^{v_j}$

$= e$ for all $j \geq t$

$\Rightarrow b_j^{p^m} = b_j^{p^{h_j} p^{v_j}} = e$ for all $j \geq t$

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m}$

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m}$

$\in <b_1^{p^m}> \ldots <b_{t-1}^{p^m}>$

$\therefore \quad C \subseteq <b_1^{p^m}> \ldots <b_{t-1}^{p^m}>$

But $b_j^{p^m} \in C \Rightarrow <b_j^{p^m}> \subseteq C$

$\therefore \quad C = <b_1^{p^m}> \ldots <b_{t-1}^{p^m}>$

Also $x \in <b_1^{p^m}> \cap <b_2^{p^m}> \ldots <b_{t-1}^{p^m}>$

$\Rightarrow x \in B_1, x \in B_2 \ldots B_{t-1}$

$\Rightarrow x \in B_1, x \in B_2 \ldots B_{t-1} B_t \ldots B_l$

$\Rightarrow x = e$.

Similarly for other intersections.

$\therefore \quad C = <b_1^{p^m}> \times \ldots\ldots \times <b_{t-1}^{p^m}>$

Thus $o(C) = o(b_1^{p^m}) \ldots\ldots o(b_{t-1}^{p^m})$

$$= \frac{o(b_1)}{(p^m, o(b_1))} \ldots \frac{o(b_{t-1})}{(p^m, o(b_{t-1}))}$$

$$= \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m}$$

Now $G = A_1 \times \ldots\ldots \times A_k = \langle a_1 \rangle \times \ldots\ldots \times \langle a_k \rangle$ and $C \leq G$

$\Rightarrow C = \langle a_1^{p^m} \rangle \times \ldots\ldots \times \langle a_k^{p^m} \rangle$

$$\Rightarrow o(C) = \frac{o(a_1)}{(p^m, o(a_1))} \ldots\ldots \frac{o(a_k)}{(p^m, o(a_k))}$$

$$= \frac{p^{n_1}}{(p^m, p^{n_1})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

Since $n_1 = h_1, \ldots, n_{t-1} = h_{t-1}$

$$o(C) = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

So, $$\frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\Rightarrow \quad 1 = \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\geq \frac{p^{n_t}}{(p^m, p^{n_t})}, \text{ as } \frac{p^{n_j}}{(p^m, p^{n_j})} \geq 1$$

> 1 as $n_t > m \quad \Rightarrow (p^m, p^{n_t}) = p^m$

$$\Rightarrow \frac{p^{n_t}}{(p^m, p^{n_t})} = \frac{p^{n_t}}{p^m} = p^{n_t - m} > 1$$

a contradiction.

$\therefore\ n_i = h_i$ for all i

So, $o(G) = o(A_1) \ldots\ldots o(A_k) = o(B_1) \ldots\ldots o(B_l)$

$\Rightarrow p^{n_1} \ldots\ldots\ldots p^{n_k} = p^{h_1} \ldots\ldots\ldots p^{h_t}$

If $k > l$, $p^{n_1} \ldots\ldots\ldots p^{n_t}\ p^{n_t+1} \ldots\ldots\ldots p^{n_k} = p^{h_1} \ldots\ldots\ldots p^{h_t}$.

$\Rightarrow p^{n_l+1} \ldots\ldots\ldots p^{n_k} = 1$ as $n_i = h_i$ for all i

which is not true.

$\therefore\ k$ is not greater then l. Similarly l is not greater than k.

$\therefore \quad k = l$.

Remark: In theorem 15, $n_1, \ldots, n_k$ are uniquely determined but not the corresponding cyclic groups. For example, G = Klein's 4 group can be written in 2 ways as direct product of cyclic groups.

$G = A \times B = A \times C$, where $A = \{I, (12)(34)\}$

$B = \{I, (13)(24)\}$, $C = \{I, (14)(23)\}$

Problem 45: *Let G be the finite abelian group of order mp^n where $p \nmid m$. Then show that G is IDP of H and K where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$ and also that $o(H) = p^n$.*

Solution: It can be easily checked that H and K are subgroups of G.

We show $G = HK$, $HK = \{e\}$

Now as $p \nmid m$, g.c.d. $(p^n, m) = 1$ and thus there exist integers s, t such that

$$1 = sm + tp^n$$

If $x \in G$ be any element then

$$x = x^{sm+tp^n} = x^{sm} \cdot x^{tp^n}$$

Now $$\left(x^{sm}\right)^{p^n} = \left(x^{p^n m}\right)^s = e^s = e \qquad (a^{o(G)} = e)$$
$$\Rightarrow x^{sm} \in H$$

Again $$\left(x^{tp^n}\right)^m = \left(x^{p^n m}\right)^t = e^t = e \Rightarrow x^{tp^n} \in K$$

So $$x \in HK \Rightarrow G \subseteq HK \Rightarrow G = HK$$

Let now $$x \in H \cap K \Rightarrow x \in H \text{ and } x \in K$$
$$\Rightarrow x^{p^n} = e \text{ and } x^m = e$$
$$\Rightarrow o(x) \mid p^n \text{ and } o(x) \mid m$$
$$\Rightarrow o(x) = 1 \text{ as } (p^n, m) = 1$$
$$\Rightarrow x = e \text{ or that } H \cap K = \{e\}$$

Since G is abelian, H, K are normal subgroups and hence G is IDP of H and K.

Again, $$p^n m = o(G) = o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)} = o(H) \cdot o(K)$$

If, $p \mid o(K)$, then by Cauchy's theorem $\exists\, k \in K$ s.t., $o(k) = p$. Also $k \in K \Rightarrow k^m = e$ (by definition of K) and so $p \mid m$, which is not true. Thus $p \nmid o(K)$ or that $o(K)$ is not a multiple of p and hence $o(H) = p^n$.

A beautiful application of theorem 15 is

Theorem 16: *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*

Proof: Suppose G, G' are finite abelian groups of order p^n. Let G and G' be isomorphic and θ be an isomorphism from G onto G'.

Let $$G = A_1 \times \ldots \times A_k,\ A_i = \langle a_i \rangle,\ o(A_i) = p^{n_i}$$

Since θ is an isomorphism, $\theta(A_i)$ is normal subgroups of G' for all $i = 1, \ldots, k$.

$\therefore$ $\theta(A_1) \ldots\ldots \theta(A_k)$ is a subgroup of G

Also $$g' \in G' \Rightarrow \exists\, g \in G \text{ s.t. } \theta(g) = g$$
$$g \in G \Rightarrow g = x_1 \ldots\ldots x_k,\ x_i \in A_i$$

$$\Rightarrow g' = \theta(g) = \theta(x_1) \ldots\ldots \theta(x_k)$$
$$\in \theta(A_1) \ldots\ldots \theta(A_k)$$
$$\Rightarrow G' \subseteq \theta(A_1) \ldots\ldots \theta(A_k)$$
$$\Rightarrow G' = \theta(A_1) \ldots\ldots \theta(A_k)$$

Also, $\theta(A_1) \cap \theta(A_2) \ldots \theta(A_k) = \{e'\}$, e' = identity of G'

as $x \in \theta(A_1), x \in \theta(A_2) \ldots\ldots \theta(A_k)$

$\Rightarrow x = \theta(x_1) = \theta(x_2)\ldots\ldots\theta(x_k), \quad x_i \in A_i$

$$\Rightarrow \theta(x_1) = \theta(x_2\ldots\ldots x_k)$$
$$\Rightarrow x_1 = x_2 \ldots\ldots x_k$$
$$\Rightarrow x_1^{-1} x_2 \ldots\ldots x_k = e$$
$$\Rightarrow x_i = e \text{ for all } i$$
$$\Rightarrow x = e.$$

Similarly for other intersections.

$\therefore\ G' = \theta(A_1) \times \ldots \times \theta(A_k)$. Since $A_i = \langle a_i \rangle$, $\theta(A_i) = \langle \theta(a_i) \rangle$.

So $o(\theta(A_i)) = o(\theta(a_i)) = o(a_i)$ for all i

$= p^{n_i}$ for all i

Thus, G and G' have same invariants.

Conversely, suppose G and G' have same invariants.

Let $G = A_1 \times \ldots \times A_k$, $A_i = \langle a_i \rangle$

Then $G' = B_1 \times \ldots \times B_k$, $B_i = \langle b_i \rangle$, $o(A_i) = o(B_i)$

as G and G' have same invariants.

But any two cyclic groups of same order are isomorphic. A_i and B_i are isomorphic for all i. So $A_1 \times \ldots \times A_k = G$ and $B_1 \times \ldots \times B_k = G'$ are isomorphic.

We are now in a position to specify the number of non-isomorphic finite abelian groups of order p^n through

Theorem 17: *The number of non-isomorphic abelian groups (or number of distinct isomorphism classes of abelian groups) of order p^n, p a prime, equals the number of partitions of n.*

Proof: Let G be an abelian group of order p^n.

By theorem 15, $G = A_1 \times \ldots \times A_k$, $A_i = \langle a_i \rangle$, $o(A_i) = p^{n_i}$

$$o(G) = o(A_1) \ldots o(A_k)$$
$$\Rightarrow p^n = p^{n1} \ldots p^{nk} = p^{n1 + \ldots\ldots + nk}$$
$$\Rightarrow n = n_1 + \ldots\ldots + n_k, \quad n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$$

is a partition of n.

Conversely, consider any partition of n.

Let $n = n_1 + \ldots + n_k, \quad n_1 \geq n_2 \geq \ldots \geq n_k > 0$

be a partition of n.

Let A_i be a cyclic group of order p^{n_i} for all i.

Let $G = A_1 \times ... \times A_k$. Then G is an abelian group of order $p^{n_1 + ... + n_k} = p^n$.

Let $\mathcal{A}$ = set of all non-isomorphic abelian groups of order p^n.

$\mathcal{B}$ = set of all partitions of n.

Define $\theta: \mathcal{A} \to \mathcal{B}$ as follows:

Let $G \in \mathcal{A}$. Let $G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$.

Let $\theta(G) = n_1 + ... + n_k = n$

Clearly, θ is well defined.

Also $\theta(G) = \theta(G')$

$\Rightarrow n_1 + ... + n_k = m_1 + ... + m_l = n$

$\Rightarrow k = l$, $n_i = m_i$ for all i

$\Rightarrow G$ and G' have same invariants

$\Rightarrow G$ and G' are isomorphic

$\Rightarrow G = G'$

$\Rightarrow \theta$ is 1–1

Let $n = n_1 + ... + n_k$, $n_1 \geq n_2 \geq ... \geq n_k > 0$ be a partition of n. Then as seen above $G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$ is an abelian group of order p^n and

$\theta(G) = n_1 + ... + n_k$

$\therefore$ θ is onto.

$\therefore$ $o(\mathcal{A}) = o(\mathcal{B})$, which proves the result.

It is not difficult to prove that two finite abelian groups are isomorphic if and only if their Sylow subgroups are isomorphic. Now from theorem 17, we get

Theorem 18: *Let $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$ where p_is are distinct primes. Then the number of non-isomorphic abelian groups of order n is $p(\alpha_1)\, p(\alpha_2)$.....$p(\alpha_r)$ where $p(\alpha_i)$ denotes the number of partitions of α_i.*

Problem 46: *Find all the non-isomorphic abelian groups of order*

(*i*) 8 (*ii*) 6 (*iii*) 20 (*iv*) 360.

Solution:

(*i*) Since $8 = 2^3$, the number of non-isomorphic abelian groups of order 8 is given by $p(3)$, where $p(3)$ denotes the number of partitions of 3.

Since $p(3) = 3$ and $3 = 3$

$3 = 2 + 1$

$3 = 1 + 1 + 1$

The number of non isomorphic abelian groups of order 8 is 3. The groups are

$\mathbf{Z}_{2^3}$, $\mathbf{Z}_{2^2} \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

i.e., $\mathbf{Z}_8$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

(*ii*) As $6 = 2^1 \times 3^1$, the number of non-isomorphic abelian groups is $p(1)\, p(1) = 1.\ 1 = 1$. The groups being the cyclic groups $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.

(*iii*) As $20 = 2^2 \times 5^1$, the number of non-isomorphic abelian groups of order 20 is given by

$p(2)\, p(1) = 2.\ 1 = 2$

The groups being $\mathbf{Z}_4 \times \mathbf{Z}_5$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5$.

(*iv*) $o(G) = 360 = 2^3 \times 3^2 \times 5^1$

The number of non isomorphic abelian groups of order 360 is

$p(3)p(2)p(1) = 3 \times 2 \times 1 = 6$ and as

$3 = 3, \quad 3 = 2 + 1, \quad 3 = 1 + 1 + 1$

$2 = 2, \quad 2 = 1 + 1,$ we have these six groups to be

$$\mathbf{Z}_{2^3} \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_8 \times \mathbf{Z}_9 \times \mathbf{Z}_5 \cong Z_{360}$$

$$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$$

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$$

$$\mathbf{Z}_{2^3} \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 = \mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$

$$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 = \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$

Problem 47: *Suppose G is an abelian group of order 120 and suppose G has exactly three elements of order 2. Find the isomorphism class of G.*

Solution: $o(G) = 120 = 2^3 \times 3 \times 5$. So the number of non isomorphic abelian groups of order 120 will be $p(3)p(1)p(1) = 3$ and these are

$$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \cong \mathbf{Z}_{120}$$
$$\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$
$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5.$$

$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has only one element (4, 0, 0) of order 2 so it cannot be G

Again, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has (1,1,1,0,0), (1,0,1,0,0), (0,1,1,0,0) and (1,1,0,0,0) as elements of order 2

so it cannot be G

whereas $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has exactly three elements

(2, 1, 0, 0), (0, 1, 0, 0), (2, 0, 0, 0)

which have order 2 and hence G is $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

Problem 48: *Let G be a finite abelian group under addition. Let n be a +ve integer. Define* $nG = \{nx \mid x \in G\}$ *and* $G[n] = \{x \in G \mid nx = 0\}$ *then show that nG and G[n] are subgroups of G and* $\dfrac{G}{G[n]} \cong nG$.

Solution: We use 0 to denote identity of G.

Since $nx, ny \in nG \Rightarrow nx - ny = n(x - y) \in nG$, $0 = n.0 \in nG$, nG is a subgroup. Similarly one can see that $G[n]$ is a subgroup.

(See Exercise 6 on page 77)

Define a mapping $\theta : G \to nG$, s.t.,

$$\theta(x) = nx$$

then θ is a well defined onto homomorphism

$$\theta(x + y) = n(x + y) = nx + ny = \theta(x) + \theta(y) \text{ etc.,}$$

Thus by Fundamental theorem of group homomorphism $nG \cong \frac{G}{Ker\,\theta}$

Now $x \in Ker\theta \Rightarrow \theta(x) = 0 \Rightarrow nx = 0 \Rightarrow n \in G[n]$

confirms that $\frac{G}{G[n]} \cong nG$.

Remark: If binary composition of G is multiplication, the above subgroup $G[n]$ will be $\{x \in G \mid x^n = e\}$ and we can denote it by G_n. Again the subgroups nG will be $\{x^n \mid x \in G\}$ and we can denot it by G^n. We have thus shown that $\frac{G}{Gn} \cong G^n$. It can be a good exercise for the reader to write the above proof independently under the multiplicative composition.

Problem 49: *If p is a prime not dividing o(G), show that pG ≅ G, where G is a finite additive abelian group.*

Solution: By previous problem $pG \cong \frac{G}{G[p]} = \frac{G}{\{0\}} \cong G$.

Problem 50: *Let G ={1, 7, 17, 23, 49, 55, 65, 71} be the group under multiplication modulo 69. Express G as EDP and IDP of cyclic groups.*

Solution: $o(G) = 8 = 2^3$, thus as seen in problem 46 above the number of non isomorphic abelian groups is $p(3) = 3$ and these are

$$\mathbf{Z}_8,\ \mathbf{Z}_2 \times \mathbf{Z}_4 \quad \mathbf{Z}_2,\ \mathbf{Z}_2 \times \mathbf{Z}_2$$

Again, we notice that the elements 7, 23, 55 have order 4 and the elements 17, 49, 65, 71 have order 2 in G.

Since $\mathbf{Z}_8$ has an element of order 8 and G has no element of order 8, therefore, G is not $\mathbf{Z}_8$

Again $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ has no element of order 4 and so we are left with the only choice that G is $\mathbf{Z}_4 \times \mathbf{Z}_2$

To write G as IDP of cyclic groups, we pick up an element of maximum order 4 (see theorem 13), say, 7 then $< 7 > = \{7, 49, 55, 1\} = H$ is one of the factors.

Again, taking an element of order 2, say 65, we get $< 65 > = \{65, 1\} = K$. Here

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)} = \frac{4 \times 2}{1} = 8 = o(G)$$

thus $G = HK$, $H \cap K = \{1\}$ and hence this is an expression of G as IDP of H & K.

This expression is not unique as we can have other representations e.g., $G = < 7 > \cdot < 17 >$ or $< 23 > \cdot < 65 >$

Exercises

1. Find all non isomorphic abelian groups of order
(*i*) 15 (*ii*) 35 (*iii*) p^3, p a prime.

2. If G is a finite abelian group and $o(G) = p_1 p_2,...p_n$ where $p_i s$ are distinct primes, show that G is cyclic.
[**Hint:** G is direct product of Sylow p_i-subgroups]

3. Show that any abelian group of order 45 has an element of order 15.

4. If G is a finite abelian group under addition and $o(G) = mn$ s.t., $(m, n) = 1$, show that $G = G[m] \oplus G[n]$ EDP and $o(G[m]) = m$, $o(G[n]) = n$. (See problem 48).

5. Let p be a prime. Define $G(p) = \{x \in G \mid p^n x = 0 \text{ for some } n \geq 0\}$ where G is a finite abelian group. Let H be a finite abelian group where f: $G \to H$ is a homomorphism. Show that $f(G(p)) \subseteq H(p)$ for all primes p.

A Quick Look at what's been done

- A group is called a ***p*-group** if order of each element of the group is some power of p, where p is some prime. K_4 and quaternion groups are p-groups, whereas S_3 is not.
- If G is a finite group, then G is a p-group iff $o(G) = p^n$ for some n.
- If p is a prime s.t., p^n divides $o(G)$ and p^{n+1} does not divide $o(G)$ then any subgroup H of order p^n is called a Sylow ***p*-subgroup**.
- The **three theorems by Sylow** ensure that every finite group has a Sylow p-subgroup. If there are more than one Sylow p-subgroups then they are conjugate and finally the number of Sylow p-subgroups is of the type $1 + kp$, where $1 + kp$ divides $o(G)$ and $k = 0, 1, 2,\ldots\ldots$
- Survey of non-abelian groups of order 8 and 6 suggests that any non-abelian group of order 6 is isomorphic to S_3 and there are two non-abelian groups of order 8, namely the dihedral group and the quaternion group.
- There are two types of direct products, namely external direct product (EDP) and internal direct product (IDP), which are isomorphic.
- A finite abelian group is a direct product of its Sylow p-subgroups.
- **Fundamental theorem of finite abelian groups** states that *a finite abelian group is a direct product of cyclic groups of prime power order and this factorization is unique.*
- Two abelian groups of order p^n are isomorphic iff they have the same invariants.
- The number of non-isomorphic abelian groups of order p^n, where p is a prime, equals the number of partitions of n.

6

Group Actions, Solvable and Nilpotent Groups

Introduction

For this culminating chapter on groups we have selected a few more results that give an insight into the structure of groups. We start with group actions including its applications in proving a few results some of which we had proved earlier also. We then move on to solvable groups and nilpotent groups.

Group Actions

Definition: Let G be a group and A be a non empty set, then G is said to act on A if $\exists$ a function $*$ from $G \times A \to A$ satisfying

(*i*) $g_1 * (g_2 * a) = (g_1 g_2) * a$

(*ii*) $e * a = a \quad \forall\ g_1, g_2 \in G$ and $a \in A$

This mapping $*$ is called a group action of G (or a G action) on A and A is called a G-set and we express it by saying that G *acts on* A. This is also referred to as action on the left. We can define action of G on A on the right by considering mapping from $A \times G \to A$ satisfying

$$a * (g_1 g_2) = (a * g_1) * g_2 \text{ and } a * e = a \qquad \forall\ a \in A, g_1, g_2 \in G$$

Again, sometimes and when there is no scope of confusion we replace $g * a$ by $g{\cdot}a$ or ga. Also, of course, $g_1 g_2$ in (*i*) above refers to $g_1 . g_2$ in G. One may remark here that $*$ is not a binary composition.

Example 1: Let G be a group and A be any non empty set. Define $*$ from $G \times A \to A$ s.t.,

$$g * a = a \qquad \forall\ a \in A, g \in G$$

then since $g_1 * (g_2 * a) = g_1 * (a) = a = (g_1 g_2) * a$

and $e * a = a \qquad \forall\ a \in A, g_1, g_2 \in G$

We find $*$ is a group action.

Hence G acts on A and A is a G-set.

This action is called the *trivial G action.*

Example 2: Let G be any group and take $A = G$. Define $*$ by

$$g * a = ga \qquad g \in G,\ a \in A = G$$

Then $*$ is a group action as

$$g_1 * (g_2 * a) = g_1 * (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) * a$$
$$e * a = ea = a \qquad \forall\ g_1, g_2 \in G,\ a \in A$$

This action of G on itself is called action by (left) *translation* or (left) *multiplication*

If we define $*$ by $g * a = ag^{-1}$ then again $*$ is a group action as

$$g_1 * (g_2 * a) = g_1 * (a g_2^{-1}) = (a g_2^{-1}) g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2) * a$$
$$e * a = ae^{-1} = a.$$

This is referred to as action of G by (right) *translation* or (right) *multiplication*. This action is also sometimes called the *regular action* of G on itself.

Example 3: Let G be any group and let $A = G$.

Define $* : G \times A \to A$ s.t.,

$$g * a = gag^{-1} \qquad g \in G,\ a \in A$$

Then $*$ is a group action (prove!) and is called action by *conjugation*.

Example 4: Let H be a normal subgroup of G and let $A = G/H$ = the set of all left cosets of H in G. Define

$* : G \times A \to A$, s.t.,

$$g * (aH) = gag^{-1}H, \qquad g \in G,\ aH \in A = G/H$$

Then since $g_1 * (g_2 * aH) = g_1 * (g_2 a g_2^{-1})H = g_1(g_2 a g_2^{-1}) g_1^{-1} H = (g_1 g_2)a(g_1 g_2)^{-1}H$

$$= (g_1 g_2) * aH$$

and $e * aH = eae^{-1}H = aH \qquad \forall\ aH \in A$

We notice that $*$ is a group action and thus G/H is a G set.

Example 5: Let G be a group and $\mathscr{A}$ be the set of all subgroups of G.

Define $* : G \times \mathscr{A} \to \mathscr{A}$ *s.t.,*

$$g * H = gHg^{-1} \qquad g \in G,\ H \in \mathscr{A}$$

then as above one can check that $*$ is a group action.

Theorem 1: *Let G be any group and A be any non empty set. Then any homomorphism from* $G \to Sym\,(A)$ *the symmetric group of A defines an action of G on A. Conversely, every action of G on A induces a homomorphism from* $G \to Sym(A)$.

Proof: Let $\varphi : G \to \mathrm{Sym}(A)$, be any homomorphism.

For any $g \in G$, Let $\varphi(g) = \sigma_g$

where σ_g is 1-1, onto map from $A \to A$, i.e., a permutation on A.

Since φ is a homomorphism, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

i.e., $$\sigma_{g_1 g_2} = \sigma_{g_1}\sigma_{g_2}$$

Define $* : G \times A \to A$ s.t.,

$$g * a = \sigma_g(a), \quad g \in G, a \in A$$

Since $g_1 * (g_2 * a) = g_1 * (\sigma_{g_2}(a)) = \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1 g_2}(a) = g_1 g_2 * a$

and $e * a = \sigma_e(a) = a$ where $\sigma_e = I$ = identity of Sym(A). We find $*$ is a group action. (Notice as φ is a homomorphism, identity is mapped to identity, i.e., $\varphi(e) = \sigma_e = I$)

Conversely, Suppose G acts on A under the group action $*$.

Define a map $\varphi : G \to \text{Sym}(A)$, s.t.,

$$\varphi(g) = \sigma_g$$

where $\sigma_g : A \to A$, s.t., $\sigma_g(a) = g * a$,

To show that φ is well defined, we first show that $\sigma_g : A \to A$ is 1-1 onto

Now $\sigma_g(x) = \sigma_g(y) \Rightarrow g * x = g * y$

$\Rightarrow g^{-1} * (g * x) = g^{-1} * (g * y)$

$\Rightarrow (g^{-1}g) * x = (g^{-1}g) * y$

$\Rightarrow e * x = e * y \Rightarrow x = y$

or that σ_g is 1-1.

Again, if $y \in A$ be any element then $g^{-1} * y \in A$ for $g \in G$

(Note, $*$: $G \times A \to A$, $y \in A$, $g \in G \Rightarrow g^{-1} \in G \Rightarrow g^{-1} * y \in A$)

Now $\sigma_g(g^{-1} * y) = g * (g^{-1} * y) = (gg^{-1}) * y = e * y = y$

Hence, σ_g is onto and this $\sigma_g \in$ Sym A

Now $\varphi(g_1 g_2) = \sigma_{g_1 g_2}$ and $\sigma_{g_1 g_2}(a) = (g_1 g_2) * a$

and $\varphi(g_1)\varphi(g_2) = \sigma_{g_1 g_2}$ where $\sigma_{g_1 g_2}(a) = \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1}(g_2 * a)$

$= g_1 * (g_2 * a)$

$= (g_1 g_2) * a$

or that $\sigma_{g_1 g_2} = \sigma_{g_1}\sigma_{g_2}$

ie., $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

Hence φ is a homomorphism, which proves our theorem.

Remark: We thus realise that for any group action of a group G on a set A, there corresponds a homomorphism φ from $G \to$ Sym (A). This homomorphism is sometimes called the *associated* (or *corresponding*) *permutation representation* of the given action.

Consider, for instance, the trivial group action

$*$: $G \times A \to A$ s.t., $g * a = a$

If φ: $G \to$ Sym(A) be the corresponding permutation representation, then here $\varphi(g) = \sigma_g$ where

σ_g: $A \to A$ s.t., $\sigma_g(a) = g * a = a$ and thus

$\sigma_g(a) = a \qquad \forall\ a \in A$

or that $\sigma_g = I = \sigma_e$ and so $\varphi(g) = \sigma_g = I \qquad \forall\ g$

i.e., φ is the trivial homomorphism.

Cor. 1: We can prove Cayley's theorem that any group G is isomorphic to a permutation group by using above theorem. We know that any group G acts on itself (see example 2) under $*$ defined by $g * a = ga, \quad a, g \in G$.

By the above theorem, the corresponding permutation representation to this action is given by the homomorphism.

$$\varphi : G \to \text{Sym}(A), \text{ s.t.,}$$
$$\varphi(g) = \sigma_g$$

where $\sigma_g : A \to A$ s.t., $(A = G)$

$$\sigma_g(a) = g * a = ga$$

Let $\varphi(g_1) = \varphi(g_2)$

$$\Rightarrow \sigma_{g_1} = \sigma_{g_2}$$
$$\Rightarrow \sigma_{g_1}(x) = \sigma_{g_2}(x) \qquad \forall\, x \in A = G$$
$$\Rightarrow \sigma_{g_1}(e) = \sigma_{g_2}(e)$$
$$\Rightarrow g_1 e = g_2 e$$
$$\Rightarrow g_1 = g_2$$

or that φ is a 1-1 homomorphism and so G is isomorphic to a subgroup of the symmetric group $\text{Sym}(A) = \text{Sym}(G)$.

Cor. 2: Let G act on G by conjugation, then $\exists$ a homomorphism

$\varphi : G \to Sym(G)$ s.t.,

$\varphi(\sigma) = \sigma_g$

where σ_g: $G \to G$ s.t., $\sigma_g(a) = g * a = gag^{-1}$

Now here $\text{Ker}\,\varphi = \{g \in G \mid \varphi(g) = I\} = \{g \in G \mid \sigma_g = I\}$

$$= \{g \in G \mid \sigma_g(x) = \sigma_e(x) \ \ \forall\, x\}$$
$$= \{g \in G \mid gxg^{-1} = exe^{-1}\} = \{g \in G | gx = xg \ \forall\, x \in G\} = Z(G)$$

Thus by Fundamental theorem, $\varphi(G) \cong \dfrac{G}{\text{Ker}\,\varphi}$ *i.e.*, $\dfrac{G}{Z(G)} \cong I(G)$

as $\varphi(G) = \{\sigma_g \mid \sigma_g(a) = gag^{-1}\} = I(G)$ = group of all inner automorphisms of G. (see page 169 also).

Kernel of an action

Definition: Let $*$: $G \times A \to A$ be a group action then Kernel of $*$ is defined to be the set

$\text{Ker}(*) = \{g \in G \mid g * a = a \quad \forall\, a \in A\}$

i.e., those elements of G that fix all elements of A.

It is easy to see that $\text{Ker}(*)$ is a subgroup of G.

$\text{Ker}(*) \neq \varphi$ as $e \in \text{Ker}(*)$ as $e * a = a \qquad \forall\, a \in A$

If $x, y \in \text{Ker}(*)$, then $x * a = a,\ y * a = a \quad \forall\, a \in A$

Since $xy * a = x * (y * a) = x * a = a \quad \forall\, a \in A$

we find $xy \in \text{Ker}(*)$.

Again as $e * a = a,\ (x^{-1}x) * a = a$

$$\Rightarrow x^{-1} * (x * a) = a$$
$$\Rightarrow x^{-1} * a = a$$
$$\Rightarrow x^{-1} \in \text{Ker}(*)$$

Thus Ker$(*)$ is a subgroup of G. We can go a step further and show that if φ be the corresponding permutation representation of $*$ then Ker$(*)$ = Kerφ

We have φ: $G \to \text{Sym}(A)$, a homomorphism.

such that $\varphi(g) = \sigma_g$

where $\sigma_g : A \to A$ s.t., $\sigma_g(a) = g * a$

Now, Ker $\varphi = \{g \in G \mid \varphi(g) = I\} = \{g \in G \mid \sigma_g = \sigma_e\}$
$$= \{g \in G \mid \sigma_g(a) = \sigma_e(a) \quad \forall\ a\}$$
$$= \{g \in G \mid g * a = e * a\}$$
$$= \{g \in G \mid g * a = a\ \forall\ a \in A\} = \text{Ker}(*)$$

proving our assertion.

Definition: An action $*$ of G on A is said to be *faithful* if distinct elements of G induce distinct permutations of A. In other words, $*$ is said to be faithful if whenever $g * a = a$ then $g = e$.

Let $*$ be a group action.

Since Ker$(*) = \{g \in G \mid g * a = a\}$

We find, if $*$ is faithful then Ker$(*)$ contains only e as only $e * a = a$

So Ker$(*) = \{e\}$ which in turn implies that Ker $\varphi = \{e\}$ where φ is the corresponding permutation representation. This gives us that φ is 1-1.

So, if $*$ is faithful action then φ is 1-1. Conversely, If φ is 1-1 then Ker $\varphi = \{e\} \Rightarrow$ Ker$(*) = \{e\}$

i.e., e is the only element in G that gives $g * a = a$ or that $*$ is faithful

Example 6: The trivial action is not faithful (if $o(G) > 1$) as in this $g * a = a$ holds for all g and therefore, Ker$(*) = G$.

Example 7: If $*$ is the group action by left translation then $g * a = ga$ and

Ker$(*) = \{g \in G \mid g * a = a\} = \{g \in G \mid ga = a\}$
$$= \{g \in G \mid ga = ea \quad \forall\ a\}$$
$$= \{g \in G \mid g = e\} = \{e\}$$

i.e., $*$ is faithful action.

Orbits and Stabilizers

Definition: Let G be a group acting on a set A under $*$. Let $a \in A$ be any fixed element Then the set

$$G_a = \{g \in G \mid g * a = a\}$$

is called the *stabilizer* of a in G.

G_a is a subgroup of G. Indeed

$G_a \neq \varphi$ as $e \in G_a$ as $e * a = a$

Again, if $x, y \in G_a$ then $x * a = a$, $y * a = a$

and as $xy^{-1} * a = x * (y^{-1} * a) = x * (y^{-1} * (y * a))$

$= x * (y^{-1} y * a) = x * a = a$

we find $xy^{-1} \in G_a$.

Example 8: If G acts on A trivially, then for any $a \in A$

$G_a = \{g \in G \mid g * a = a\} = G$ as under trivial action $g * a = a \quad \forall g \in G$

Example 9: Suppose G acts on itself by conjugation

i.e., $g * a = gag^{-1} \ \forall g \in G, \ a \in G$

For any $a \in G$,

$G_a = \{g \in G \mid g * a = a\} = \{g \in G \mid gag^{-1} = a\}$

$= \{g \in G \mid ga = ag\} = N(a)$ the normaliser of a in G.

Definition: Let G be a group acting on a set A under $*$. For any $a \in A$, let

$Ga = \{x \in A \mid x = g * a$ for some $g \in G\}$

$= \{g * a \mid g \in G\}$

then Ga is called an *orbit* of a under G or orbit of G containing a

Since $e * a = a$, $a \in Ga$ and thus orbit is a non empty subset of A.

We may remark here that we are writing Ga in place of $G * a$.

As a particular case, if G sets on itself ($A = G$) by translation then orbit of any $a \in A = G$ is given by

$Ga = \{g * a \mid g \in G\} = \{ga \mid g \in G\} = G$

Problem 1: *Let G act on a set A under $*$.* For any $a, b \in A$, define $a \sim b$ iff $\exists\ g \in G$, s.t., *$a = g * b$, then show that $\sim$ is an equivalence relation and for any $a \in A$, the equivalence class of a is the orbit of a in G.*

Solution : Reflexivity follows as $e * a = a \quad \forall a$

and thus $a \sim a \quad \forall a$

For symmetry, assume that

$a \sim b \Rightarrow \exists\ g \in G$, s.t., $a = g * b$

Now $g^{-1} * a = g^{-1} * (g * b) = (g^{-1}g) * b = e * b = b$

shows that $b \sim a$

Transtivity is easily seen to be true.

Hence $\sim$ is an equivalence relation.

Let $a \in A$ be any element then equivalence class of a is given by

$cl(a) = \{x \in A \mid x \sim a\} = \{x \in A \mid x = g * a$ for same $g \in G\}$

$= \{g * a \mid g \in G\}$

which is nothing but the orbit of a under G.

We thus realize that orbits are equivalence classes.

So a group G acting on a set A leads to a partition of A into disjoint equivalence classes under the action of G and those classes are nothing but the orbits of elements of A. Hence A can be expressed as the union of distinct orbits of elements of A.

Example 10: Let H be a subgroup of a finite group G and suppose H acts on G under $*$

$* : H \times G \to G$ s.t.,

$h * g = hg, \qquad h \in H, g \in G$

Let $a \in G$ by any element, then orbit of a is

$H*a\ (= Ha) = \{x \in G \mid x = h * a \text{ for same } h \in H\}$

$= \{x \in G \mid x = ha \text{ for same } h \in H\}$

$= \{ha \mid h \in H\} = Ha$

the right coset of H in G.

The mapping $f : H \to H * a$ s.t.,

$f(h) = h * a = ha$

is clearly 1-1, onto and thus $o(H) = o(H * a)$

i.e., order of each orbit is equal to order of H. Since orbits of elements of G partition G into equivalence classes, we get

$G = O_1 \cup O_2 \cup ... \cup O_t.$

where O_i are distinct orbits in G.

Thus $o(G) = o(O_1) + o(O_2) + ... + o(O_t)$

$= o(H) + o(H) + ... + o(H)$ (t times)

$\Rightarrow o(H) | o(G)$

and so we have proved Lagrange's theorem.

We may notice in passing that the stabilizer of a is given by

$H_a = \{h \in H \mid h * a = a\} = \{h \in H | ha = a\}$

$= \{h \in H \mid h = e\} = \{e\}.$

Theorem 2 (Orbit-Stabilizer): *Let G be a group that acts on a set A. Let $a \in A$, then there exists a one-one onto map from Ga to the set of all left cosets of G_a in G.*

Proof: We know G_a is a subgroup of G. Let G/G_a denote the set of all left cosets of G_a in G.

Define a map $\varphi: Ga \to G/G_a$ s.t.,

$\varphi(g * a) = gG_a \qquad g \in G$

Then $g_1 * a = g_2 * a$

$\Leftrightarrow \quad g_1^{-1}(g_1 * a) = g_1^{-1}(g_2 * a)$

$\Leftrightarrow \quad (g_1^{-1} g_1) * a = g_1^{-1} * (g_2 * a)$

$\Leftrightarrow \quad a = g_1^{-1} g_2 * a$

$\Leftrightarrow \quad g_1^{-1} g_2 \in G_a \Leftrightarrow g_1 G_a = g_2 G_a$ (Definition of G_a)

$\Leftrightarrow \quad \varphi(g_1 * a) = \varphi(g_2 * a)$

Thus φ is well defined 1-1 map. φ is clearly onto.

Cor: If G is a finite group acting on A, we find from above that

$o(Ga) = o(G/G_a) =$ Index of G_a in G.

i.e., $o(Ga) = \dfrac{o(G)}{o(G_a)}$

i.e., $o(G) = o(Ga).o(G_a)$

Example 11: Let G be a group acting on itself ($A = G$) by conjugation. Let $a \in G$ be any element, then orbit of a under G is

$Ga = \{g * a \mid g \in G\} = \{gag^{-1} \mid g \in G\} = cl(a)$, the conjugate class of a (See, for definition, page 182).

Hence under the group action by conjugation, we notice each orbit is a conjugate class.

Example 12: Let G be a finite group acting on itself ($A = G$) by conjugation, i.e.,

$* : G \times G \to G$, s.t.,

$g * a = gag^{-1}$

Let $a \in G$ be any element, then the stabilizer of a in G is

$$G_a = \{g \in G \mid g * a = a\} = \{g \in G \mid gag^{-1} = a\}$$
$$= \{g \in G \mid ga = ag\} = N(a) \text{ the normalizer or centralizer of } a \text{ in } G.$$

Also, orbit of a under G is given by

$Ga = \{g * a \mid g \in G\} = \{gag^{-1} \mid g \in G\} = cl(a)$, the conjugate class of a (See Page 182).

Since $o(Ga)$ = Index of G_a in G, by previous theorem are find

$o(cl(a))$ = Index of G_a in G = Index of $N(a)$ in G

or that

$$o(cl(a)) = \frac{o(G)}{o(N(a))}$$

i.e., number of conjugates of a is the index of $N(a)$ in G.

a result we proved earlier, (see page 184).

Since the orbits (or the conjugate classes) partition G,

We can write

$$G = \bigcup_{a \in G} cl(a)$$
$$\Rightarrow o(G) = \sum_{a \in G} o(cl(a)) = \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$
$$= o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))\}$$

Recall, $a \in Z(G) \Leftrightarrow cl(a) = \{a\}$

i.e., $o(cl(a)) = 1$ (See Page 182)

Thus, $$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

and the class equation of G is established.

Notice here $\frac{o(G)}{o(N(a))}$ = Index of $N(a)$ in G, $a \notin Z(G)$

Problem 2: *Show (using group actions) that the number of conjugates of a subset S of a group G is the index of the normalizer of S in G.*

Solution: Let $\mathcal{P}(G)$ be the power set of G, i.e., $\mathcal{P}(G)$ contains all subsets of G.

Define $* : G \times \mathcal{P}(G) \to \mathcal{P}(G)$, s.t.,

$$g * S = gSg^{-1} \qquad g \in G, \quad S \in \mathcal{P}(G)$$

then clearly $*$ is the group action by conjugation.

For any $S \in \mathcal{P}(G)$, the orbit of S in G is

$G_S = \{g * S \mid g \in G\} = \{gSg^{-1} | g \in G\} = cl(S)$, the conjugate class of S and thus $o(cl(S))$ gives the number of conjugates of S.

So our aim is to show that $o(cl(S)) = \dfrac{o(G)}{o(N(S))}$

Now stabilizer of S in G is

$$G_S = \{g \in G \mid g * S = S\} = \{g \in G \mid gSg^{-1} = S\} = N(S)$$

which we know is a subgroup of G.

Let G/G_S denote the set of all left cosets of G_S in G.

Define $\varphi : cl(S) \to G/G_S$ s.t.,

$$\varphi(g * S) = gG_S \qquad g \in G$$

Then

$$g_1 * S = g_2 * S$$

$$\Leftrightarrow \; g_1^{-1} * (g_1 * S) = g_1^{-1} * (g_2 * S)$$

$$\Leftrightarrow \; g_1^{-1} g_1 * S = g_1^{-1} g_2 * S$$

$$\Leftrightarrow \; S = g_1^{-1} g_2 * S$$

$$\Leftrightarrow g_1^{-1} g_2 \in G_S \qquad \text{(Definition of } G_S\text{)}$$

$$\Leftrightarrow \; g_1 G_S = g_2 G_S$$

$$\Leftrightarrow \; \varphi(g_1 * S) = cl(g_2 * S)$$

or that φ is well defined, 1-1 mapping. φ is also easily seen to be onto.

Hence

$$o(cl(S)) = o(G/G_S) = \text{No. of distinct left cosets of } G_S \text{ in } G.$$
$$= \text{Index of } G_S \text{ in } G.$$
$$= \text{Index of } N(S) \text{ in } G.$$

giving us the required result.

Remark: We know that all the Sylow p-subgroups are conjuage and thus if P is any Sylow p-subgroup then by above remark, the number of conjugates of P is index of $N(P)$ in G, or that *the number of Sylow p-subgroups is* $\dfrac{o(G)}{o(N(P))}$.

Problem 3: *Show that there is no simple group G of order 216.*

Solution: We have $o(G) = 216 = 2^3 \cdot 3^3$

Number of Sylow 3-subgroups is $(1 + 3k)$ s.t., $(1 + 3k) \mid 2^3$

$$\Rightarrow k = 0 \text{ or } 1$$

If $k = 0$, $\exists$ a unique normal subgroup of order 27

So G is not simple.

If $k = 1$, $\exists$ 4 Sylow 3-subgroups each of order 27.

If P is any one of these, then the number of Sylow 3-subgroups is $\frac{o(G)}{o(N(P))}$ = Index of $N(P)$ in G.

where $N(P)$ is normalizer of P.

So 4 = Index of H in G, where $H = N(P)$

By Index theorem, if H is a proper subgroup of G s.t., $o(G) \nmid |i_G(H)$ then H contains a non trivial normal subgroup of G. In particular then G is not simple.

Here $o(G) \nmid |i_G(H)$ as $216 \nmid |4$

Hence the result follows.

Definition: An action of a group G on a set A is called *transitive* if there exists only one orbit. In other words, for $a, b \in A$, $a = g * b$ for some $g \in G$.

Example 13: Let $H \leq G$ and A = set of all left cosets of H in G. Then the action of G by left multiplication on A is transitive.

As if $*$ is the action, then $g * aH = gaH$

If $aH, bH \in A$ be any two members, then by taking $g = ba^{-1} \in G$, we find

$$g * aH = gaH = (ba^{-1})aH = bH$$

$\Rightarrow$ action is transitive.

Problem 4: *Let $A = \{1, 2, 3\}$ and $G = S_3$. Define $* : G \times A \to A$ s.t., $\sigma * a = \sigma(a)$. Show that $*$ is a group action and find all the stabilizers and orbits. Is the action transitive?*

Solution: Since

$$\sigma_1 * (\sigma_2 * a) = \sigma_1 * (\sigma_2(a)) = \sigma_1(\sigma_2(a))$$
$$= \sigma_1\sigma_2 * a \quad \text{and } I * a = I(a) = a$$

$*$ is a group action

For any $a \in A$, Stabilizer of a is given by

$$G_a = \{g \in G \mid g * a = a\}$$

Thus

$$G_1 = \{\sigma \in G \mid \sigma * 1 = 1\} = \{\sigma \in G \mid \sigma(1) = 1\} = \{I, (23)\}$$

Similarly then $G_2 = \{I, (13)\}$ and $G_3 = \{I, (12)\}$

Since $o(G) = o(Ga).o(G_a)$ we find

$$o(G) = o(G1).o(G_1)$$

$$\Rightarrow o(G1) = \frac{6}{2} = 3 \quad \text{and as } G_1 \subseteq A \text{ and } o(A) = 3$$

$$\therefore o(G1) = 3$$

or that $G1 = A$

Similarly $G2 = A$, $G3 = A$

or that there is only one orbit. Hence the action is transitive.

Remark: The above problem can be generalized to $G = S_n$, $A = \{1, 2, 3, ..., n\}$

Theorem 3: *Every permutation in S_n can be expressed as a unique product of disjoint cyles.*

Proof: Let $A = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n$ be any permutation.

Let $G = \langle\sigma\rangle = \langle\sigma, \sigma^2, \sigma^3, \ldots\rangle$

Define $* : G \times A \to A$ s.t.,

$$\sigma^i * (a) = \sigma^i(a) \qquad a \in A$$

then $*$ is easily seen to be a group action, which partitions A into a unique set of equivalence classes, the orbits.

Let $a \in A$ be any element and let O denote the orbit of a, then

$$O = Ga = \{\sigma^i * a \mid \sigma^i \in G\} = \{\sigma^i(a) \mid \sigma^i \in G\}$$

Also, stabilizer of a is given by

$$G_a = \{\sigma^i \in G \mid \sigma^i * a = a\} = \{\sigma^i \in G \mid \sigma^i(a) = a\}$$

By theorem 2 on page 272 we know $\exists$ a one one onto map

$$\varphi : O \to G/G_a \text{ s.t.,}$$
$$\varphi(\sigma^i(a)) = \sigma^i G_a$$

where G/G_a is set of all left cosets of G_a in G.

and $o(O) = o(G/G_a)$ = Index of G_a in $G = \dfrac{o(G)}{o(G_a)}$

Since G is cyclic (and so abelian) G_a is normal subgroup of G and thus the quotient group G/G_a exists and $o(G/G_a) = m$ = least +ve integer s.t., $\sigma^m \in G_a$ (See Page 109)

Thus $\dfrac{o(G)}{o(G_a)} = m$ and so $o(O) = m$.

Now distinct left cosets of G_a in G are

$$\sigma G_a, \sigma^2 G_a, \ldots, \sigma^m G_a = G_a \quad \text{as } \sigma^m \in G_a$$

i.e., these are

$$eG_a, \sigma G_a, \sigma^2 G_a \ldots, \sigma^{m-1} G_a$$

In view of the 1-1 onto mapping φ, we thus find the distinct members of O will be a, $\sigma(a)$, $\sigma^2(a) \ldots, \sigma^{m-1}(a)$.

Elements of O written in this manner show that σ cycles these elements, i.e., on the orbit O of length m, σ is acting as an m-cycle. We thus find a cyclic decomposition for σ in S_n. The uniqueness part follows as the orbits of G are determined uniquely. (The order in which the orbits are arranged can, of course, vary).

Example 14: Let $A = \{1, 2, \ldots, 10\}$ and let $\sigma \in S_{10}$ be the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 9 & 1 & 2 & 10 & 7 & 8 \end{pmatrix}$$

Let $G = \langle\sigma\rangle$, then proceeding as in the theorem above, we get a group action $*$ giving a unique set of orbits. Let us take any element of A, say 1, and suppose O is the orbit of 1. The stabilizer of 1 is

$$G_1 = \{\sigma^i \in G \mid \sigma^i(1) = 1\}$$

Now $\sigma(1) = 3$

$\sigma^2(1) = \sigma(3) = 4$

$\sigma^3(1) = \sigma(4) = 6$

$\sigma^4(1) = \sigma(6) = 1$

So $\sigma, \sigma^2, \sigma^3 \notin G_1$ and $\sigma^4 \in G_1$. Thus $m = 4$, the least -ve integer s.t., $\sigma^4 \in G_1$

Thus $o(O) = 4$ and the members of O are 1, $\sigma(1)$, $\sigma^2(1)$, $\sigma^3(1)$,

i.e., 1, 3, 4, 6

The corresponding cycle for σ is, therefore, (1346) proceeding similarly with the remaining elements of A, we get the other cycles, and we find σ = (1346)(2597)(810).

Problem 5: *Suppose a group G acts on two sets S and T. Show that $*$ defined by $g * (s, t) = (gs, gt)$ is a G action on $S \times T$ and prove further that stabilizer of (s, t) is the intersection of the stabilizers of s and t.*

Solution: We are given that G acts on S and T. Define $* (G \times (S \times T) \to S \times T)$ by

$$g * (s, t) = (gs, gt)$$

$g \in G, (s, t) \in S \times T$ $(g \in G, s \in S \Rightarrow gs \in S$ as S is a G set etc.)

Then $*$ is a group action as

$$g_1 * (g_2 * (s, t)) = g_1 * (g_2 s, g_2 t) = (g_1(g_2 s), g_1(g_2 t))$$

$$[(g_1 g_2) * (s, t) = ((g_1 g_2)s, (g_1 g_2)t) = (g_1(g_2 s), g_1(g_2 t))]$$

$$(g_1(g_2 s) = (g_1 g_2)s \text{ as } S \text{ is a } G \text{ set})$$

Also $e * (s, t) = (es, et) = (s, t)$

Now stabilizers of s and t are given by

$$G_s = \{g \in G \mid gs = s\}, \quad G_t = \{g \in G \mid gt = t\}$$

Stabilizer of (s, t) is given by

$$(S \times T)_{(s, t)} = \{g \in G \mid g * (s, t) = (s, t)\}$$

$$= \{g \in G \mid (gs, gt) = (s, t)\}$$

$$= \{g \in G \mid gs = s, gt = t\} = G_s \cap G_t$$

We have used the same symbol '$\cdot$' to describe the group actions of G on S and T.

Definition: Suppose G acts on two sets S and T. We say that the two actions of G are equivalent if $\exists$ *a* 1-1 onto map $\varphi : S \to T$ s.t., $\varphi(g * x) = go\varphi(x)$, $g \in G, x \in S$.

where $*$ and o are the actions of G on S and G on T respectively.

Example 15: Let G act on $S = G$ under (left) translation

i.e., $g * x = gx$ $(G \times G \to G)$

and also G act on $T = G$ under (right) translation

i.e., $gox = xg^{-1}$

Then the map $\varphi : S \to T$ s.t.,

$$\varphi(x) = x^{-1}$$

is the required equivalence.

Here $\varphi(x) = \varphi(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow x = y$ or that φ is 1-1

φ is clearly onto.

Also $\varphi(g * x) = \varphi(gx) = (gx)^{-1} = x^{-1}g^{-1}$

and $go\,\varphi(x) = \varphi(x)g^{-1} = x^{-1}\,g^{-1}$

Hence $\varphi(g * x) = go\varphi(x)$ and so φ is equivalence map.

Definition: Let G be a group acting on a set S. The set

$$F_S = \{x \in S \mid a * x = x \quad \forall\ a \in G\}$$

is called the fixed subset of S.

In example 10 F_S is the set $\{g \in G \mid hg = g \quad \forall\ h \in H\}$.

Lemma: Let G be a finite group acting on a finite set S.

Let $x_1, x_2, ..., x_n \in S$ be such that $Gx_i \neq \{x_i\}$ for any $i = 1, 2, ..., n$. Then

$$o(S) = o(F_S) + \sum_{i=1}^{n} [G : Gx_i]$$

where $[G : Gx_i]$ denotes the index of Gx_i in G.

Proof: We have $Gx_i \neq \{x_i\}$ for any $i = 1, 2, ..., n$

thus $o(Gx_i) > 1 \quad \forall\ i = 1, 2, ..., n$

Again if $x \in F_S$ then $a * x = x \quad \forall\ a \in G$

$\Rightarrow Gx = \{x\}$

i.e., orbits with one element.

Now S can be expressed as union of all its orbits (see exercises)

Thus $S = \underset{x \in S}{\cup} Gx$

$$\Rightarrow \quad o(S) = \sum_{x \in S} o(Gx) = \sum_{x \in F_S} o(Gx) + \sum_{x \notin F_S} o(Gx)$$

$$= o(F_S) + \sum_{i=1}^{n} o(Gx_i)$$

as $x \in F_S \Leftrightarrow a * x = x\ \forall\ a \in G \Leftrightarrow Gx = \{x\} \Leftrightarrow o(Gx) = 1$

Hence $$o(S) = o(F_s) + \sum_{i=1}^{n} o(Gx_i)$$

$$= o(F_S) + \sum_{i=1}^{n} [G : Gx_i] \qquad \text{(See cor. to theorem 2)}$$

Theorem 4: *If G is a finite p-group acting on a finite set S then p divides $o(S) - o(F_S)$.*

Proof: Since G is a finite p-group, $o(G) = p^n$ $(n \geq 1)$.

Thus as in above lemma

$$o(Gx_i) = [G : Gx_i] = \frac{o(G)}{o(Gx_i)} = \frac{p^n}{p^m} = p^{n-m}$$

where $n \neq m$ as $o(Gx_i) > 1$

So p divides $[G : Gxi]$ $\forall$ i

$$\Rightarrow p \text{ divides } \sum_1^n [G : Gx_i]$$

$$\Rightarrow p \text{ divides } o(S) - o(F_S).$$

We now give another proof of Cauchy's theorem that we proved earlier in chapter 4.

Theorem 5 (Cauchy's): *Let G be a finite group and let p be a prime dividing $o(G)$. Then there exists an element x in G s.t., $o(x) = p$.*

Proof: Let $S = \{(a_1, a_2, ..., a_p) \mid a_i \in G, a_1a_2 ... a_p = e\}$

Then as $a_1a_2 ... a_p = e$, $a_p = (a_1a_2 ... a_{p-1})^{-1}$

i.e., a_p is determined by the first $p - 1$ elements and so $o(S) = (o(G))^{p-1}$

Consider now the symmetric group S_p. Let $\sigma \in S_p$ be the element $\sigma = (1\ 2\ 3\ ...\ p)$

Let H be the group generated by σ *i.e.*,

$$H = <\sigma> = \{\sigma, \sigma^2, \sigma^3, ..., \sigma^p = I\}$$

Define $*$ from $H \times S \to S$, s.t.,

$$\sigma^i * (a_1, a_2, ..., a_p) = (a_{\sigma^i(1)}, a_{\sigma^i(2)}, ..., a_{\sigma^i(p)})$$
$$i = 1, 2, ..., p$$

Thus, for instance,

$$\sigma * (a_1, a_2, ..., a_p) = (a_{\sigma(1)}, a_{\sigma(2)}, ..., a_{\sigma(p)})$$
$$= (a_2, a_3, ..., a_1)$$

$$\sigma^2 * (a_1, a_2, ..., a_p) = (a_{\sigma^2(1)}, a_{\sigma^2(2)}, ..., a_{\sigma^2(p)})$$
$$= (a_3, a_4, ...a_2) \text{ etc....}$$

Since $(a_1, a_2, ..., a_p) \in S \Rightarrow a_1 (a_2 ... a_p) = e$

$$\Rightarrow (a_2 ... a_p) a_1 = e$$

$$\Rightarrow (a_2, a_3, ..., a_1) \in S$$

$*$ is well defined.

Then $*$ is a group action and H acts on S.

Again as $o(H) = p$, H is a p-group and hence by previous theorem p divides $o(S) - o(F_S)$. But p divides $o(S)$ and thus $p \mid o(F_S) \Rightarrow o(F_S) > 1$.

Let us find what members F_S has.

Let $(a_1, a_2, ..., a_n) \in F_S$ be any element. Then by definition of F_S.

$$\sigma^i * (a_1, a_2, ..., a_p) = (a_1, a_2, ..., a_p) \quad \forall\ i$$

i.e., $$\sigma * (a_1, a_2, ..., a_p) = (a_1, a_2, ..., a_p)$$

i.e., $(a_2, a_3, ..., a_1) = (a_1, a_2, ..., a_p)$

$\Rightarrow$ $a_2 = a_1, a_3 = a_2, a_4 = a_3, ..., a_1 = a_p$

i.e., $a_1 = a_2 = ... = a_p = x$ (say)

i.e., any member of F_s is of the type $(x, x, ..., x)$

s.t., $\underbrace{x.x.x...x}_{(p \text{ times})} = e$

i.e., $x^p = e$

So $F_S \subseteq \{(x, x, ..., x) \mid x^p = e\}$

Again any element of the type $(x, x, ..., x)$

clearly lies in F_s as $\sigma^i * (x, x, ..., x) = (x, x, ..., x)$. $\forall\ \sigma^i \in H$

Hence $F_S = \{(x, x, ..., x) \mid x^p = e\}$

Thus $\exists$ an element $e \neq x \in G$ s.t., $x^p = e$ or that

$o(x) = p$. Notice $(e, e, ..., e) \in F_s$ and $o(F_S) > 1$ (so $x \neq e$).

Problem 6: *Let G be a finite p-group. If $H \neq G$ is a subgroup of G then show that $H \neq N(H)$.*

Solution: Let $S = \{xH \mid x \in G\}$ be the set of all left cosets of H in G.

Define $*$ by

$$h * (xH) = hxH \quad \forall\ x \in G, h \in H$$

Then H acts on S and

$$o(S) = [G : H] = \frac{o(G)}{o(H)} = p^r, \quad r \geq 1 \text{ as } H \neq G$$

So $p \mid o(S)$. Since $p \mid [o(S) - o(F_S)]$ also we find

$p \mid o(F_S)$. Thus $o(F_S) \neq 1$

Now
$$\begin{aligned} F_S &= \{xH \mid hxH = xH \quad \forall\ h \in H\} \\ &= \{xH \mid x^{-1} hxH = H \quad \forall\ h \in H\} \\ &= \{xH \mid x^{-1} hx \in H \quad \forall\ h \in H\} \\ &= \{xH \mid x^{-1} Hx \subseteq H\} \\ &= \{xH \mid x^{-1} Hx = H\} \\ &= \{xH \mid x \in N(H)\} \end{aligned}$$

and as $o(F_S) \neq 1$, $N(H) \neq H$

(See Problem 3 on page 207 also).

Problem 7: *Let G be a group of order 12. Show that either Sylow 3-subgroup is normal or $G \cong A_4$.*

Solution: No. of Sylow 3-subgroups is $(1 + 3k)$ s.t., $(1 + 3k) \mid 4 \Rightarrow k = 0$ or 1.

If $k = 0$, $\exists$ a unique normal Sylow 3-subgroup, so we are done.

Now suppose $k \neq 0$, then $k = 1$. Then $\exists$ 4 Sylow 3-subgroups each of roder 3. If H_1 and

H_2 are any two of these four, then $o(H_1 \cap H_2) | o(H_1) = 3 \Rightarrow o(H_1 \cap H_2)) = 1$ or 3. But $o(H_1 \cap H_2) = 3$ gives $H_1 = H_2$. Thus $o(H_1 \cap H_2) = 1$.

Thus each H_i has 2 elements of order 3 or that in all $\exists\ 4 \times 2 = 8$ elements of order 3 in G.

We know (see page 273) that the number of conjugates of any subset S of G is Index of $N(S)$ in G, i.e., $\dfrac{o(G)}{o(N(S))}$.

If H is any of the four Sylow 3-subgroups, then since all Sylow 3-subgroups are conjuage, we get

$$\frac{o(G)}{o(N(H))} = 4 \Rightarrow o(N(H)) = \frac{12}{4} = 3$$

Again $H \subseteq N(H)$ always and $o(H) = o(N(H)) = 3$ gives $N(H) = H$

Let $\mathscr{A}$ = set of all the four Sylow 3-subgroups H_i, i =1, 2, 3, 4

Define $\quad * : G \times \mathscr{A} \to \mathscr{A}$ s.t.,

$$g * H = gHg^{-1} \qquad H \in \mathscr{A}$$

and let $\varphi : G \to \mathrm{Sym}\,\mathscr{A}$ be the corresponding permutation representation, then $\varphi(g) = \sigma_g$

where $\quad \sigma_g : \mathscr{A} \to \mathscr{A}$ s.t.,

$$\sigma_g(H) = g * H = gHg^{-1}$$

Let $K = \mathrm{Ker}\ \varphi$. If $g \in K$ be any element, then

$$\varphi(g) = I \Rightarrow \sigma_g = I \Rightarrow \sigma_g(H) = I(H) \Rightarrow gHg^{-1} = H \Rightarrow g \in N(H)$$

and thus $K \leq N(H)$

$$\Rightarrow o(K) | o(N(H)) = 3 \Rightarrow o(K) = 1 \text{ or } 3.$$

But $o(K) = 3 \Rightarrow K = N(H) = H$ which is not possible as H by assumption is not normal whereas $K = \mathrm{Ker}\ \varphi$ is normal.

Thus $\quad o(K) = 1 \Rightarrow \mathrm{Ker}\ \varphi = \{e\} \Rightarrow \varphi$ is 1-1.

Hence $\varphi : G \to \mathrm{Sym}\,\mathscr{A}$ is a 1-1 homomorphism

and, therefore, $G \cong T$, where $T \leq \mathrm{Sym}\,\mathscr{A} = S_4$.

Now G contains 8 elements of order 3 as shown above.

Thus T contains 8 element of order 3 and as S_4 has 8 3-cycles (elements of order 3) which are all in A_4, we find T and A_4 have at least 8 elements in common or that $o(T \cap A_4) \geq 8$,

So $\quad 8 \leq o(T \cap A_4) | o(A_4) = 12$

$$\Rightarrow o(T \cap A_4) = 12 \Rightarrow T = A_4 \begin{pmatrix} o(T) = o(G) = 12 \\ o(A_4) = 12 \end{pmatrix}$$

Hence $G \cong A_4$.

Exercises

1. Let G be a group and $S = G$. Show that $*$ defined by $a * x = axa^{-1}$, $a, x \in G$, is a group action.

2. Let $(F, +, \cdot)$ be a field. Let $G = (F, \cdot)$ the group. Let V be any vector space over F (Refer chapter on Vector spaces). Define $*$ by $\alpha * v = \alpha.v$, $\alpha \in F$, $v \in V$, where . is scalar multiplication in V Show that $*$ is a group action.

3. Let S be a non empty set and G be a group of permutations of S, *i.e.*, $G = A(S)$. Show that $*$ defined by $\theta * x = \theta(x)$ $\forall$ $x \in S$, $\theta \in G$ is a group action of G on S.

4. (*i*) Let H be a subgroup of G and $\mathscr{S}$ = set of all left cosets of H in G. Define $*$ by $g * aH = gaH$, $g \in G$, $aH \in \mathscr{S}$. Show that $*$ is a G action.

(*ii*) Let $\varphi : G \to A(\mathscr{S})$ be the homomorphism corresponding to $*$. Show that Ker φ is the largest normal subgroup of G contained in H and Ker $\varphi = \bigcap_{x \in G} xHx^{-1}$. Hence prove the generalized Cayley's theorem. (See page 156, theorem 18).

The set $\mathscr{S}$ is sometimes denoted by G/H and is called the (left) *coset space* of G relative to H. (Notice H here is not essentially normal). Again if we wish to work with right cosets, we can define $*$ by $g * Ha = Hag^{-1}$.

(*iii*) If $H \trianglelefteq G$ of index n then show that G/H is isomorphic to a subgroup of S_n. (Use Fundamental theorem and the fact that H = Ker φ).

5. Show that orbit of H in example 5 is the set of all subgroups conjugate to H and stabilizer of H in G is the normaliser of H.

6. Let G act on G by conjugation, i.e., $g * a = gag^{-1}$, a, $g \in G$ then show that Ker$(*) = Z(G)$.

7. Let G be a group acting on S and H a group acting on T where

$S \cap T = \varphi$. Let $U = S \cup T$. Define $*$ by

$(g, h) * x = gx$ if $x \in S$

$= hx$ if $x \in T$ $g \in G, h \in H, x \in U$

Show that $*$ defines an action of $G \times H$ on U.

8. Let G be a finite group acting on a finite set S. For any $g \in G$, define $S^g = \{s \in S \mid g * s = s\}$. Prove (Burnside's formula)

$$o(G) \times \text{No. of orbits} = \sum_{g \in G} o(S^g)$$

9. Let G be a group acting on a set S. If $x \in S$ and Gx is the orbit of x and $y \in Gx$, then show that $Gx = Gy$.

Normal Series

Definition: A normal subgroup H of a group G is called a *maximal normal* subgroup of G if $H \neq G$ and there exists no normal subgroup K of G s.t., $H \subset K \subset G$.

Thus $H \neq G$ is a maximal normal subgroup of G if whenever $K \lhd G$ s.t., $H \subseteq K \subseteq G$ then either $K = H$ or $K = G$.

In fact, a subgroup $H \neq G$ is called maximal subgroup of G if whenever $H \leq K \leq G$ then either $K = G$ or $K = H$.

Similarly, a normal subgroup M of G is called a *minimal normal* subgroup if only normal subgroups of G which are contained in M are $\{e\}$ and M. Thus if N is a normal subgroup of G s.t., $\{e\} \subseteq N \subseteq M$ then either $N = \{e\}$ or $N = M$.

Example 16: A_3 is a maximal normal subgroup of S_3. $o(A_3) = 3$ whereas $o(S_3) = 6$. Clearly there cannot be any subgroups of order 4 or 5 in S_3. We also notice that $o\left(\frac{S_3}{A_3}\right) = 2$, a prime and thus $\frac{S_3}{A_3}$ is a simple group. See theorem 6 ahead.

Example 17: If G is a simple group then it has no non trivial normal subgroups and so $\{e\}$ will be a (and only) maximal normal subgroup in G.

Theorem 6: *H is a maximal normal subgroup of G iff G/H is simple.*

Proof: Let H be maximal normal in G. Any subgroup of G/H is of the form K/H where $K \leq G$ and $H \subseteq K$ and also K/H is normal in $G/H \Leftrightarrow K \trianglelefteq G$.

Thus any subgroup K/H will be non trivial normal subgroup of G/H if $H \lhd K \lhd G$, which is not true as H is maximal normal. So G/H has no non trivial normal subgroup and is, therefore, simple.

Conversely: let G/H be simple. Suppose H is not maximal normal, then $\exists$ a normal subgroup K of G s.t.,

$H \subset K \subset G$ and thus K/H will be normal subgroup of G/H where $K/H \subset G/H$, a contradiction as G/H is simple.

Problem 8: *Any finite group G (with at least two elements) has a maximal normal subgroup.*

Solution: If G is simple then it has no proper normal subgroup except $\{e\}$ and thus $\{e\}$ is a maximal normal subgroup of G.

Suppose G is not simple. Then it has at last one normal subgroup $N \neq G$, $N \neq \{e\}$. If N is maximal normal, we are done. If not, then $\exists$ at least one normal subgroup M where $N \subsetneq M \subsetneq G$. If M is maximal normal, we are done. If not, we continue like this. Since G is finite, it can have finite number of subgroups and hence the above process must end after a finite number of steps. Hence G will have a maximal normal subgroup.

Problem 9: *Give an example of a maximal normal sub group which is not a maximal subgroup.*

Solution: Consider $G = \mathbf{Z}_2 \times A_5$

Then $H = \mathbf{Z}_2 \times \{I\}$ is normal in G and $G/H \cong A_5$ and so G/H will be simple and hence maximal normal subgroup of G.

Since $H \subsetneqq \{(0, I), (1, I), (0, (123), (0, (132))\} \subsetneqq G$

H is not a maximal subgroup of G.

Problem 10: *Let H, K be two distinct maximal normal subgroups of G then $G = HK$ and $H \cap K$ is a maximal normal subgroup of H as well as K.*

Solution: Since H, K are normal, HK is normal in G.

Since $H \subseteq HK \subseteq G$ and HK is maximal normal.

we must have $HK = H$ or $HK = G$

Similarly $HK = K$ or $HK = G$

Hence $HK = G$ (as $HK \neq G \Rightarrow HK = H$, $HK = K \Rightarrow H = K$).

Again by isomorphism theorem

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Thus $$\frac{K}{H \cap K} \cong \frac{G}{H}$$

Since H is maximal normal, $\frac{G}{H}$ is simple

i.e., $\frac{K}{H \cap K}$ is simple

$\Rightarrow H \cap K$ is maximal normal in K

Similarly, it is maximal normal in H.

Problem 11: *Show that $< \mathbf{Q}, + >$ has no maximal normal subgroup.*

Solution: Suppose H is a maximal normal subgroup of $< \mathbf{Q}, + >$, then $\frac{\mathbf{Q}}{H}$ is simple and so $\frac{\mathbf{Q}}{H}$ has no non trivial normal subgroup *i.e.*, it will have no non trivial subgroup ($\mathbf{Q}$ being abelian, all subgroups are normal). Thus $\frac{\mathbf{Q}}{H}$ is a cyclic group of prime order p.

Let $H + x \in \frac{\mathbf{Q}}{H}$ be any element

Then $p(H + x) = H$

i.e., $H + px = H$ or that $px \in H \quad \forall\, x \in \mathbf{Q}$

Let now $y \in \mathbf{Q}$ be any element, then $\frac{y}{p} \in \mathbf{Q}$

If $\frac{y}{p} = x$ then $y = px \Rightarrow y \in H$ or that

$\mathbf{Q} \subseteq H \subseteq \mathbf{Q} \Rightarrow H = \mathbf{Q}$, a contradiction.

Hence the result follows.

Definition: Let G be a group. A sequence of subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots\ldots\ldots \subseteq G_n = G \qquad \ldots(1)$$

is called a *normal series* of G if G_i is a normal subgroup of G_{i+1},

$$\forall\ i = 0,\ 1\ \ 2,\ldots,n-1.$$

The factor (quotient) groups $\dfrac{G_{i+1}}{G_i}$ $(\forall\ i)$ are called the *factors* of the normal series.

Here each G_i is normal in G_{i+1}, although it may not be normal in G. Also it is possible that $G_i = G_{i+1}$ for some i. The number of distinct members of (1) excluding G is called the length of the normal series.

The above is expressed in short by saying that $N = (G_0, G_1, \ldots\ldots\ldots, G_n)$ is a normal series of G. If N and M are two normal series of G s.t., $N \subseteq M$ then M is called a *refinement* of N (a proper refinement if $N \subsetneqq M$).

Remark: Some authors prefer to call the above a subnormal series. It is then called a normal series if G_i is normal in $G\ \forall\ i$.

If G is any group then

$$\{e\} = G_0 \subseteq G_1 = G$$

is an obvious example of a normal series.

Example 18: $\{I\} \subseteq A_3 \subseteq S_3$ is a normal series of S_3.

$\{I\} \subseteq E \subseteq K_4 \subseteq A_4 \subseteq S_4$ is a normal series of S_4, where

$$E = \{I,\ (12)(34)\},\ K_4 = \{I,\ (12)(34),\ (13)(24),\ (14)(23)\}$$

We've seen earlier that $E \trianglelefteq K_4$, but E is not normal in A_4 (and so in S_4).

Definition: Let G a group. A sequence of subgroups

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots\ldots\ldots \subset G_n = G$$

of G is called a *composition series* of G if

(i) each G_i is normal subgroup of G_{i+1} $(i = 0,\ 1,\ \ldots\ldots\ n-1)$,

(ii) $G_i \neq G_{i+1}$ for any i and

(iii) $\dfrac{G_{i+1}}{G_i}$ is a simple group $\forall\ i$.

The factor (quotient) groups $\dfrac{G_{i+1}}{G_i}$ are called factors of the series.

In view of theorem 6 on page 283 the condition (iii) can be replaced by "G_i is a maximal normal subgroup of G_{i+1}" $\forall\ i$.

We notice that a composition series is a normal series (converse being not true) and that a composition series has no 'gaps'.

A group can have more then one composition series.

Example 19: $\{0\} \subset <8> \subset <4> \subset \mathbf{Z}$
is a normal series of the group ($\mathbf{Z}$, +), but it is not a composition series as $<4>$ is not maximal normal in $\mathbf{Z}$. Notice $<4> \subset <2> \subset \mathbf{Z}$.

Example 20. Consider the quaternion group G. Then

$$\{1\} \subset \{1, -1\} \subset \{1, -1, i, -i\} \subset G$$
$$\{1\} \subset \{1, -1\} \subset \{1, -1, j, -j\} \subset G$$
$$\{1\} \subset \{1, -1\} \subset \{1, -1, k, -k\} \subset G$$

are all composition series of G. If we write the first series as $G_0 \subset G_1 \subset G_2 \subset G$ then

$$o\left(\frac{G}{G_2}\right) = \frac{8}{4} = 2, \quad o\left(\frac{G_2}{G_1}\right) = \frac{4}{2} = 2, \quad o\left(\frac{G_1}{G_0}\right) = 2$$

i.e., all the factor groups are of prime order and thus have no trivial normal subgroups and hence are simple.

The existence of a composition series is ensured by

Theorem 7: *Every finite group G (with more then one element) has a composition series.*

Proof: We use induction on $o(G)$.

If $o(G) = 2$ then $\{e\} = G_0 \subset G_1 = G$ is (only) composition series of G. Notice $\frac{G_1}{G_0} = \frac{G}{\{e\}} \cong G$ and as $o(G) = 2$, a prime it is simple group and, therefore, $\frac{G_1}{G_0}$ is simple.

Suppose now that the result holds for groups with order less than $o(G)$. We show result holds for G. If G is a simple group then $\{e\} \subset G$ is the composition series for G. Suppose G is not simple.

Since G is finite, it has a maximal normal subgroup $N \neq G$ and as $o(N) < o(G)$, result holds for N which then has a composition series, say,

$$\{e\} \subset N_1 \subset N_2 \subset \ldots \subset N$$

Then the series

$\{e\} \subset N_1 \subset N_2 \subset \ldots \subset N \subset G$ will be a composition series for G.

Hence the result holds.

Remark: If $o(G) = 1$, we sometimes say that the result holds trivially as then (G) is a composition series of G (without factors).

Definition: Two composition series.

$$C_1 : \{e\} = N_0 \subset N_1 \subset \ldots\ldots\ldots \subset N_t = G \quad \ldots(1)$$
$$C_2 : \{e\} = H_0 \subset H_1 \subset \ldots\ldots\ldots \subset H_m = G \quad \ldots(2)$$

of a group G are said to be equivalent if $\exists$ *a* 1-1 onto mapping between the factors of (1) and factors of (2) such that the corresponding factor groups are isomorphic. In other words (1) and (2) will be equivalent if $t = m$ and each factor group of (1) is isomorphic to some factor group of (2).

Also in this case, we write $C_1 \sim C_2$. It is easy to see that ~ is an equivalence relation.

We've seen that a finite group can have more than one composition series. The next theorem shows the equivalence of any two such composition series.

Theorem 8 (Jordan-Hölder): *Let G be a finite group. Let*

$$C_1 : \{e\} = N_0 \subset N_1 \subset ... \subset N_{t-1} \subset N_t = G \quad ...(1)$$

$$C_2 : \{e\} = H_0 \subset H_1 \subset ... \subset H_{m-1} \subset H_m = G \quad ...(2)$$

be two composition series of G. Then m = t and there exists a permutation $i \to i'$ *of* 0, 1, 2, ..., t–1 *s.t.,* $\dfrac{N_{i+1}}{N_i} \cong \dfrac{H_{i'+1}}{H_{i'}}$, $0 \le i \le t-1$

i.e., C_1 *and* C_2 *are equivalent.*

Proof: Let $o(G) = n$. We use induction on n.

If $n = 2$, we have seen (theorem 7) G has only one composition series. Hence result holds in this case.

Let now the result hold for groups with order less than $o(G)$.

Case (*i*) $N_{t-1} = H_{m-1}$. Consider the series

$$\{e\} = N_0 \subset N_1 \subset ... \subset N_{t-1} \quad ...(3)$$

$$\{e\} = H_0 \subset H_1 \subset ... \subset H_{m-1} = N_{t-1} \quad ...(4)$$

Then these are composition series for finite group N_{t-1} and as $o(N_{t-1}) < o(G)$, the result holds for (3) and (4) *i.e.*, (3) and (4) are equivalent.

Thus $t - 1 = m - 1 \Rightarrow t = m$

and also factors of (3) and (4) are isomorphic under some permutation.

Now $$\frac{N_t}{N_{t-1}} = \frac{G}{N_{t-1}} = \frac{G}{H_{m-1}} = \frac{H_m}{H_{m-1}}$$

Thus (1) and (2) will be equivalent (as $t = m$ and factors of (1) and (2) are isomorphic). Hence result holds in this case.

Case (*ii*) $N_{t-1} \neq H_{m-1}$. Let $K = N_{t-1} \cap H_{m-1}$

Then K is a finite group and has a composition series. Let

$\{e\} = K_0 \subset K_1 \subset ... \subset K_s = K$ be a composition series of K.

Since N_{t-1}, H_{m-1} are normal in G, $K = N_{t-1} \cap H_{m-1}$ will be normal subgroup of G

Again, as N_{t-1}, H_{m-1} are maximal normal subgroups of G

$$N_{t-1}.\ H_{m-1} = G$$

and $N_{t-1} \cap H_{m-1} = K$ is maximal normal subgroup of N_{t-1} and H_{m-1}. (See Problem 4)

So $K \subset N_{t-1}$, $K \subset H_{m-1}$

Consider now the series,

$$\{e\} = K_0 \subset K_1 \subset ..... \subset K_s = K \subset N_{t-1} \subset N_t = G \quad ...(5)$$

$$\{e\} = K_0 \subset K_1 \subset ..... \subset K_s = K \subset H_{m-1} \subset H_m = G \quad ...(6)$$

We show these are composition series of G. For this we need show that $\frac{N_{t-1}}{K}$ and $\frac{H_{m-1}}{K}$ are simple.

By isomorphism theorem

$$\frac{N_{t-1}}{N_{t-1} \cap H_{m-1}} \cong \frac{N_{t-1}\, H_{m-1}}{H_{m-1}} = \frac{G}{H_{m-1}}$$

So $\frac{N_{t-1}}{N_{t-1} \cap H_{m-1}} \cong \frac{G}{H_{m-1}}$ and similarly $\frac{H_{m-1}}{N_{t-1} \cap H_{m-1}} \cong \frac{G}{N_{t-1}}$ ...(7)

Now $\frac{G}{H_{m-1}} = \frac{H_m}{H_{m-1}}$ is simple as (2) is a composition series of G

$\Rightarrow$ $\frac{N_{t-1}}{N_{t-1} \cap H_{m-1}}$ is simple

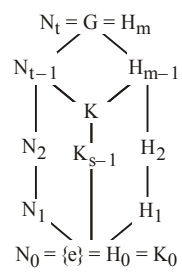
i.e., $\frac{N_{t-1}}{K}$ is simple.

Similarly, $\frac{H_{m-1}}{K}$ is simple.

Now (5) and (6) would be equivalent as

$$\frac{N_{t-1}}{K} \cong \frac{H_m}{H_{m-1}} \quad \text{and} \quad \frac{N_t}{N_{t-1}} \cong \frac{H_{m-1}}{K} \quad \text{from (7)}$$

Also lengths of (5) and (6) are equal both being $s + 2$



Now (1) and (5) are two composition series of $N_t = G$ and applying case (*i*) to these (second last terms are equal = N_{t-1}) we find they are equivalent. Hence they have same length, *i.e.*, $t = s + 2$

Similarly, (2) and (6) give $m = s + 2$

$\Rightarrow t = m$

Now (1) ~ (5), (5) ~ (6) $\Rightarrow$ (1) ~ (6)

Also (2) ~ (6) thus (1) ~ (2) as ~ is an equivalence relation.

Hence the theorem is proved.

Problem 12: *Find all the composition series of* $G = < a >$, *a cyclic group of order* 6 *and show they are equivalent.*

Solution: $G = \{e, a, a^2 a^3, a^4, a^5\}$. Since $o(G) = 6$ has four divisors 1, 2, 3, 6, G will have four subgroups, namely $\{e\}$, G and $< a^2 > = \{e, a^2, a^4\}$, $< a^3 > = \{e, a^3\}$

Composition series of G will be

$$\{e\} \subset < a^3 > \subset G$$
$$\{e\} \subset < a^2 > \subset G$$

Notice $o\left(\frac{G}{< a^3 >}\right) = \frac{6}{2} = 3$, $o\left(\frac{< a^3 >}{\{e\}}\right) = o(< a^3 >) = 2$ which are primes and so the factors are simple groups.

Again, $\frac{G}{< a^3 >} \cong \mathbf{Z}_3$, $\frac{< a^3 >}{\{e\}} \cong < a^3 > \cong \mathbf{Z}_2$

$\frac{G}{< a^2 >} \cong \mathbf{Z}_2$, $\frac{< a^2 >}{\{e\}} \cong < a^2 > \cong \mathbf{Z}_3$

$$\Rightarrow \frac{G}{< a^3 >} \cong \frac{< a^2 >}{\{e\}}, \quad \frac{< a^3 >}{\{e\}} \cong \frac{G}{< a^2 >}$$

Hence the two composition series are equivalent.

Problem 13: *Find all the composition series of* $\mathbf{Z}_{30}$ *and show they are equivalent.*

Solution: $\mathbf{Z}_{30} = \{0, 1, 2, ..., 29\}$ addition modulo 30. Besides $\{0\}$ and $\mathbf{Z}_{30}$, the other subgroups of $\mathbf{Z}_{30}$ are

$$< 2 > = \{0, 2, 4, 6, ... 28\}$$
$$< 3 > = \{0, 3, 6, ..., 27\}$$ (See page 86)

and $< 5 >, < 6 >, < 10 >, < 15 >$

Composition series will be

$\{0\} \subset < 15 > \subset < 5 > \subset G$ $\{0\} \subset < 15 > \subset < 3 > \subset G$

$\{0\} \subset < 10 > \subset < 5 > \subset G$ $\{0\} \subset < 10 > \subset < 2 > \subset G$

$\{0\} \subset < 6 > \subset < 3 > \subset G$ $\{0\} \subset < 6 > \subset < 2 > \subset G$

Here each $\frac{G_{i+1}}{G_i}$, factor group is simple.

For instance, $o\left(\frac{< 5 >}{< 15 >}\right) = \frac{o(< 5 >)}{o(< 15 >)} = \frac{6}{2} = 3$, a prime and so $\frac{< 5 >}{< 15 >}$ is simple.

Equivalence of any two composition series can be shown as in the previous problem.

Problem 14: *Show that the group* $< \mathbf{Z}, + >$ *has no composition series.*

Solution: Suppose $< \mathbf{Z}, + >$ has a composition series

$$\{0\} = H_0 \subset H_1 \subset H_2 \subset ..... \subset H_n = \mathbf{Z}$$

$\mathbf{Z}$, being abelian, all subgroups are normal and each subgroups is of the type $< m >$, $m \in \mathbf{Z}$.

Let $H_1 = < m >$ then since $\frac{H_1}{H_0} = \frac{H_1}{\{0\}} \cong H_1$

and as $\frac{H_1}{H_0}$ is simple (Def. of composition series) we find $H_1 = < m >$ is simple. But this is not possible as if $K = < 2m >$ then $K \subset H_1$ and $K \neq \{0\}$. So we get a contradiction and hence **Z** has no composition series.

(See also Theorem 9 ahead)

Problem 15: *Without referring to the Jordan-Holder theorem show that if a finite group G has two composition series*

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \leq \ldots\ldots \trianglelefteq N_r = G$$

$$\{e\} = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G$$

then r = 2 and the list of composition factors is same.

Solution: The two composition series are

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots\ldots \trianglelefteq N_r = G$$

$$\{e\} = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G$$

and thus $\frac{G}{M_1}$ and $\frac{M_1}{\{e\}}$ i..e, $\frac{G}{M_1}$ and M_1 are simple.

Also $\frac{G}{M_1}$ simple $\Rightarrow M_1$ is maximal normal in G. (See theorem 6, page 283)

Case (*i*) Suppose $M_1 = N_{r-1}$, the second series then becomes $\{e\} \trianglelefteq N_{r-1} \trianglelefteq G$.

$$\Rightarrow \frac{N_{r-1}}{\{e\}} \text{ is simple} \Rightarrow N_{r-1} \text{ is simple}$$

$\Rightarrow N_{r-1}$ has no normal subgroups contained in it and so the first composition series becomes $\{e\} \trianglelefteq N_{r-1} \trianglelefteq G$, $[\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 = G]$ or that $r = 2$ and hence the result holds.

Case (*ii*) $M_1 \neq N_{r-1}$

Then $M_1 \trianglelefteq G$, $N_{r-1} \trianglelefteq G \Rightarrow M_1 N_{r-1} \trianglelefteq G$

So $M_1 \trianglelefteq M_1 N_{r-1} \trianglelefteq G$

Since $G \mid M_1$ is simple, M_1 is maximal normal in G and thus,

either $M_1 N_{r-1} = M_1$ or $M_1 N_{r-1} = G$

Suppose $M_1 N_{r-1} = M_1$

then $N_{r-1} \trianglelefteq M_1 N_{r-1} \trianglelefteq G \Rightarrow N_{r-1} \trianglelefteq M_1 \trianglelefteq G$

$$\Rightarrow M_1 = N_{r-1} \text{ as } N_{r-1} \text{ is maximal normal in } G \text{ as } \frac{G}{N_{r-1}} \text{ is simple.}$$

so $M_1 N_{r-1} = G$

and hence by second theorem of isomorphism.

$$\frac{M_1 N_{r-1}}{M_1} \cong \frac{N_{r-1}}{M_1 \cap N_{r-1}}$$

or
$$\frac{G}{M_1} \cong \frac{N_{r-1}}{M_1 \cap N_{r-1}} \tag{1}$$

But G/M_1 is simple, so $\frac{N_{r-1}}{M_1 \cap N_{r-1}}$ is simple.

$\Rightarrow M_1 \cap N_{r-1}$ is maximal normal in N_{r-1}

$[\{e\} \subseteq M_1 \cap N_{r-1} \subseteq N_{r-1}]$

Now if $M_1 \cap N_{r-1} = \{e\}$ then there is no non-trivial normal subgroup between $\{e\}$ and N_{r-1}

$\Rightarrow N_{r-1}$ is simple

So, 1st composition series becomes

$\{e\} \trianglelefteq N_{r-1} \trianglelefteq G$ i.e., $r = 2$

hence result holds in this case also.

Suppose now $M_1 \cap N_{r-1} \neq \{e\}$

Since $M_1 \cap N_{r-1} \trianglelefteq M_1$ and M_1 is simple, we must have $M_1 \cap N_{r-1} = M_1$ and thus (1) reduces to

$$\frac{G}{M_1} \cong \frac{N_{r-1}}{M_1}$$

$\Rightarrow \frac{N_{r-1}}{M_1}$ is simple $\Rightarrow M_1$ is maximal normal in N_{r-1}

So $M_1 \trianglelefteq N_{r-1} \trianglelefteq G \Rightarrow M_1 = N_{r-1}$ which is not true in this case (*ii*)

Hence $r = 2$ and the two composition series become

$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 = G$

$\{e\} = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G$

i.e., $\{e\} \trianglelefteq N_1 \trianglelefteq G$

$\{e\} \trianglelefteq M_1 \trianglelefteq G$

are the two composition series

$\Rightarrow \frac{G}{N_1}$ and $\frac{N_1}{\{e\}}$; $\frac{G}{M_1}$ and $\frac{M_1}{\{e\}}$ are simple

$\Rightarrow \frac{G}{N_1}$ and N_1; $\frac{G}{M_1}$ and M_1 are simple

We also get $N_1 \trianglelefteq N_1M_1 \trianglelefteq G$

$M_1 \trianglelefteq N_1M_1 \trianglelefteq G$

G/M_1 simple $\Rightarrow M_1$ is maximal normal in G and similarly N_1 is maximal normal in G

$\Rightarrow$ either $N_1M_1 = N_1$ or $N_1M_1 = G$

$N_1M_1 = M_1$ or $N_1M_1 = G$

If $N_1M_1 \neq G$ then $N_1M_1 = N_1$ and $N_1M_1 = M_1 \Rightarrow N_1 = M_1$

So composition factors are same

If $N_1M_1 = G$, then as $N_1 \cap M_1 \trianglelefteq M_1$ & M_1 is simple

$N_1 \cap M_1 \trianglelefteq N_1$ & N_1 is simple

We find $N_1 \cap M_1 = \{e\}$ or $N_1 \cap M_1 = M_1$

and $N_1 \cap M_1 = \{e\}$ or $N_1 \cap M_1 = N_1$

So if $N_1 \cap M_1 \neq \{e\}$ then $N_1 \cap M_1 = M_1$

$N_1 \cap M_1 = N_1$

$\Rightarrow M_1 = N_1$

or that the composition factors are same. Suppose now $N_1 \cap M_1 = \{e\}$. Then by second theorem of isomorphsim.

$$\frac{N_1M_1}{N_1} \cong \frac{M_1}{N_1 \cap M_1} \Rightarrow \frac{G}{N_1} \cong \frac{M_1}{N_1 \cap M_1}$$

$$\Rightarrow \frac{G}{N_1} \cong \frac{M_1}{\{e\}} \cong M_1$$

Similarly, $$\frac{N_1M_1}{M_1} \cong \frac{N_1}{N_1 \cap M_1} \Rightarrow \frac{G}{M_1} \cong \frac{N_1}{N_1 \cap M_1}$$

$$\Rightarrow \frac{G}{M_1} \cong \frac{N_1}{\{e\}} \cong N_1$$

So list of composition factors is

$$\left\{\frac{G}{N_1}, \frac{N_1}{\{e\}}\right\} \text{ or } \left\{\frac{G}{N_1}, N_1\right\} \text{ or } \{M_1, N_1\}$$

and $$\left\{\frac{G}{M_1}, \frac{M_1}{\{e\}}\right\} \text{ or } \left\{\frac{G}{M_1}, M_1\right\} \text{ or } \{N_1, M_1\}$$

Problem 16: *Let* $\{e\} = G_0 \subset G_1 \subset \ldots\ldots \subset G_K = G$ *be a composition series for a group* G *and suppose* $\frac{G_i}{G_{i-1}}$ *is of finite order* n_i, *then show that* G *is of finite order* $n_1n_2 \ldots n_k$.

Solution: Since $n_i = o\left(\frac{G_i}{G_{i-1}}\right) = \frac{o(G_i)}{o(G_{i-1})}$ $i = 1, 2, \ldots, k$

we get $$n_1 n_2 \ldots n_k = \frac{o(G_1)}{o(G_0)} \cdot \frac{o(G_2)}{o(G_1)} \cdots\cdots \frac{o(G_k)}{o(G_{k-1})}$$

$$= \frac{o(G_k)}{o(G_0)} = o(G_k) = o(G).$$

Theorem 9: *An abelian group G has a composition series iff G is finite.*

Proof: If G is finite, we've already shown (theorem 7) that G has a composition series. *Conversely*, let G be an abelian group and suppose it has a composition series

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots\ldots\ldots \subset G_k = G$$

then since $\frac{G_i}{G_{i-1}}$ is an abelian simple group $\forall\ i = 1, 2, \ldots, k$

it will be a group of prime order, say, p_i (See Problem 8 on page 104)

Thus $$o\left(\frac{G_i}{G_{i-1}}\right) = p_i$$

and by above problem then $o(G) = p_1 p_2 \ldots p_k$
Hence G is a finite group.

Cor.: An infinite abelian group has no composition series.

Exercises

1. Show that A_n is maximal normal in S_n.

2. Write all the maximal normal and maximal sbgroups of S_3.

3. Find all the composition series of a cyclic group $G = < a >$ of order 12 and show they are equivalent.

4. Find all the composition series of the groups $\mathbf{Z}_{12}$, $\mathbf{Z}_{60}$ and show the equivalence. Write down all the composition series of $S_3 \times \mathbf{Z}_2$

5. Write down a composition series for Klein's four group.

6. Show that $\{I\} \subseteq K_4 \subseteq A_4 \subseteq S_4$ is not a composition series.

7. Show that a finite p-group is cyclic iff it has only one composition series.

8. Let H be a normal subgroup of a finite group G. Show that G has a composition series in which H is one of the terms.

9. Let G be a finite p-group of order p^n. Show that it has a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

where $o(G_i) = p^i \quad i = 0, 1, 2, \ldots, n$ (See Problem 5 on page 208)

10. Show that fundamental theorem of arithmetic follows from Jordan-Hölder theorem.

Solvable Groups

Definition: A group G is said to be *solvable* (or soluble) if $\exists$ a chain of subgroups

$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots\ldots\ldots \subseteq H_n = G \qquad \ldots(1)$$

s.t., each H_i is a normal subgroup of H_{i+1} and $\frac{H_{i+1}}{H_i}$ is abelian

$$\forall\ i = 0, 1, 2, \ldots, n-1.$$

Also then, the series (1) is referred to as *solvable series* of G.

Thus G is solvable if it has a normal series $(H_0, H_1, \ldots, H_n)$ s.t., its factor groups are abelian.

Example 21: Any abelian group G is solvable. Since $\{e\} = G_0 \subset G_1 = G$ is a normal series for G where $\frac{G}{\{e\}} \cong G$ is abelian.

Example 22: Every cyclic group is solvable.

Example 23: S_3 and S_4 are solvable. Since $\{I\} \subseteq A_3 \subseteq S_3$ is a normal series for S_3 where its factor groups $\frac{S_3}{A_3}$ and $\frac{A_3}{\{I\}}$ are abelian as these are of prime order.

So S_3 is an example of a non abelian group that is solvable.

$\{I\} \subseteq K_4 \subseteq A_4 \subseteq S_4$ will serve as the required normal series for S_4. Notice that $\frac{K_4}{\{I\}} \cong K_4 \Rightarrow o\left(\frac{K_4}{\{I\}}\right) = o(K_4) = 4$ and we know a group of order 4 is abelian.

Remark: Any non abelian simple group is not solvable. If G is simple, it has no proper normal subgroup except $\{e\}$. So $\{e\} \subset G$ is the only normal series of G and as $\frac{G}{\{e\}} \cong G$, $\frac{G}{\{e\}}$ is not abelian as G is non abelian. Hence G is not solvable.

We've defined commutator subgroup G' of a group G (see page 163).

Now let G' be commutator subgroup of a group G.

And let $(G')' = G'' = G^{(2)}$ be commutator subgroup of G' and $G^{(3)}$ be commutator subgroup of $G^{(2)}$ and so on then $G^{(n)}$ is called the nth commutator subgroup of G. We use this to provide us with an equivalent definition of a solvable group.

Theorem 10: *A group G is solvable iff $G^{(n)} = \{e\}$ for some +ve integer n.*

Proof: Let G be solvable. Then there exists a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots\ldots\ldots \subseteq G_n = G$$

s.t., $\frac{G_{i+1}}{G_i}$ is abelian $\quad \forall\ i = 0, 1, 2, \ldots\ldots, n-1$

Since $\frac{G_n}{G_{n-1}} = \frac{G}{G_{n-1}}$ is abelian, we get $G' \subseteq G_{n-1}$(See theorem 20 on page 163)

$\Rightarrow (G')' \subseteq G'_{n-1}$

i.e., $G^{(2)} \subseteq G'_{n-1}$

Again as $\dfrac{G_{n-1}}{G_{n-2}}$ is abelian, we get $G'_{n-1} \subseteq G_{n-2} \Rightarrow G^{(2)} \subseteq G_{n-2}$

Continuing like this, we'll get $G^{(n)} \subseteq G_0 = \{e\}$

which gives $G^{(n)} = \{e\}$.

Conversely, let $G^{(n)} = \{e\}$. Consider the series

$$\{e\} = G^{(n)} \subseteq G^{(n-1)} \subseteq G^{(n-2)} \subseteq \ldots \subseteq G^{(2)} \subseteq G^{(1)} \subseteq G^{(0)} = G$$

which will be a normal series for G, where

$\dfrac{G^{(i)}}{G^{(i+1)}} = \dfrac{G^{(i)}}{(G^{(i)})'}$ is abelian $\forall\ i$ (Theorem 20 on page 163)

and, of course, $G^{(i)} \trianglelefteq G^{(i-1)} \quad \forall\ i$

$\Rightarrow G$ is solvable

That solvability is hereditary follows by

Theorem 11: *A subgroup of a solvable group is solvable.*

Proof: Let H be any subgroup of a solvable group G.

Since G is solvable, $G^{(n)} = \{e\}$ for some +ve integer n.

Now $H \subseteq G \Rightarrow H' \subseteq G' \Rightarrow (H')' \subseteq (G')'$ *i.e.*, $H^{(2)} \subseteq G^{(2)}$

Continuing like this, we get $H^{(n)} \subseteq G^{(n)} = \{e\}$

$\Rightarrow H^{(n)} = \{e\}$

$\Rightarrow H$ is solvable.

Remark: See problem 17 ahead for another approach to this result.

Theorem 12: *Homomorphic image of a solvable group is solvable.*

Proof: Let $f : G \to H$ be an onto homomorphism, where G is solvable. Then $\exists\ a$ +ve integer n s.t., $G^{(n)} = \{e\}$

Let $a, b \in G$ be any elements, then $f(a), f(b) \in H$

$\Rightarrow f(a)\, f(b)\, (f(a))^{-1}\, (f(b))^{-1} \in H'$

Also $a, b \in G \Rightarrow aba^{-1}b^{-1} \in G'$ and as

$f(aba^{-1}\, b^{-1}) = f(a)\, f(b)\, ((f(a))^{-1}\, (f(b))^{-1} \in H'$, we find

$f(G') \subseteq H'$ as $aba^{-1}b^{-1} \in G'$

Since f is onto, we find $f(G') = H'$

Again $f : G \to H$ onto means $f(G) = H$

and, therefore, $(f(G))' = H'$

i.e. $(f(G))' = f(G')$

So $H' = f(G')$

$$\Rightarrow (H')' = (f(G'))' = [f(G')'] = f(G'') = f(G^{(2)})$$

or that $H^{(2)} = f(G^{(2)})$

Continuing like this we get

$$H^{(n)} = f(G^{(n)}) = f(\{e\}) = \{e_1\} \text{ where } e_1 \text{ is identity of } H$$

i.e., H is solvable.

Theorem 13: *Quotient group of a solvable group is solvable.*

Proof: Follows from above as a quotient group is a homomorphic image of the group under the natural homomorphism.

Problem 17: *Let H be a subgroup of a solvable group G. If*

$\{e\} = N_0 \subseteq N_1 \subseteq ... \subseteq N_{n-1} \subseteq N_n = G$ be a solvable series of G then show that

$\{e\} = N_0 \cap H \subseteq N_1 \cap H \subseteq ... \subseteq N_{n-1} \cap H \subseteq N_n \cap H = H$ is a solvable series of H. Hence show that H is solvable.

Solution: Let us put $H_i = N_i \cap H, \quad i = 0, 1, 2, ..., n.$

Then we show that

$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq ..... \subseteq H_{n-1} \subseteq H_n = H \qquad ...(1)$$

is a solvable series for H.

Since $N_i \trianglelefteq N_{i+1}$ we find $N_i \cap H \trianglelefteq N_{i+1} \cap H$

i.e., $H_i \trianglelefteq H_{i+1} \quad i = 0, 1, 2, ..., n - 1$

We show now $\dfrac{H_i}{H_{i+1}}$ is abelian $\forall\ i = 0, 1, 2, ..., n - 1$

Define a map $\theta : H_{i+1} \to \dfrac{N_{i+1}}{N_i}$, s.t.,

$$\theta(x) = xN_i \quad (i = 0, 1, 2, ..., n - 1)$$

$x \in H_{i+1} = N_{i+1} \cap H \Rightarrow x \in N_{i+1}, x \in H$

Thus $xN_i \in \dfrac{N_{i+1}}{N_i}$ and θ is well defined

Now $\theta(xy) = xyN_i = xN_i\ yN_i = \theta(x)\ \theta(y)$ shows θ is a homomorphism

Again, $x \in \text{Ker}\,\theta \Leftrightarrow \theta(x) = N_i$

$$\Leftrightarrow xN_i = N_i$$

$$\Leftrightarrow x \in N_i \Leftrightarrow x \in N_i \cap H$$

Hence Ker $\theta = N_i \cap H = H_i$

By Fundamental theorem,

$$\theta(H_{i+1}) \cong \frac{H_{i+1}}{\text{Ker}\,\theta}$$

i.e. $$\frac{H_{i+1}}{H_i} \cong \theta(H_{i+1})$$

where $\theta(H_{i+1})$ is a subgroup of $\frac{N_{i+1}}{N_i}$, which is abelian and so $\theta(H_{i+1})$ is abelian and hence because of the above isomorphism $\frac{H_{i+1}}{H_i}$ is abelian.

Thus series (1) is a solvable series of H.

Problem 18: *Let G be a solvable group and suppose $H \neq \{e\}$ is a subgroup of G then show that $H' \neq H$.*

Solution: Suppose $H' = H$, then

$$H^{(2)} = (H')' = H' = H \neq \{e\}$$

If $H^{(n)} = H$, then $H^{(n+1)} = H' = H \neq \{e\}$

Thus by induction $H^{(r)} \neq \{e\} \ \forall\ r \geq 1$

But G solvable $\Rightarrow H$ is solvable $\Rightarrow H^{(r)} = \{e\}$ for some $r \geq 1$, a contradiction. Hence $H' \neq H$.

Problem 19: *Show that a simple group is solvable if and only if it is abelian.*

Solution: Let G be a simple group. Since $G' \trianglelefteq G$ we find either $G' = \{e\}$ or $G' = G$. If G is solvable then $G' \neq G$ (See problem 18) so $G' = \{e\}$. Thus G is abelian.

Conversely, if G is abelian then $G' = \{e\}$ and so G is solvable.

Problem 20: *Show that S_n ($n \geq 5$) is not solvable.*

Solution: If S_n is solvable then A_n is solvable. But A_n ($n \geq 5$) is simple. Thus by above problem A_n is abelian which is not true. [Notice (123)(234) ≠ (234)(123)].

Hence S_n is not solvable for $n \geq 5$.

Problem 21: *Show that a finite group G is solvable iff $\exists$ a chian of subgroups.*

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$$

s.t., $\frac{H_{i+1}}{H_i}$ *is cyclic (of prime order)* $i = 0, 1, 2,\ldots,n-1$.

Solution: Let G be finite, solvable. Since G is finite, it has a composition series

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$$

where $\frac{H_{i+1}}{H_i}$ is simple, $i = 0, 1, 2,\ldots,n-1$

Since G is solvable, each subgroup H_i is solvable and hence each quotient group $\frac{H_{i+1}}{H_i}$ is solvable (Theorems 11, 13).

So each $\frac{H_{i+1}}{H_i}$ is solvable and simple

$\Rightarrow$ each $\frac{H_{i+1}}{H_i}$ is abelian (Problem 19)

Thus all subgroups of $\frac{H_{i+1}}{H_i}$ are normal and as it is simple, it has no non trivial normal subgroups and hence $\frac{H_{i+1}}{H_i}$ has no proper subgroups

$\Rightarrow$ $\frac{H_{i+1}}{H_i}$ is cyclic (of prime order) (See page 87). Conversely, $\frac{H_{i+1}}{H_i}$ cyclic means it is abelian and result follows by definition.

Theorem 14: *Let N be a normal subgroup of G s.t., N and* $\frac{G}{N}$ *are solvable then G is solvable.*

Proof: Let $\{e\} = N_0 \subseteq N_1 \subseteq ... \subseteq N_k = N$ ...(1)

and $\{N\} = \frac{G_0}{N} \subseteq \frac{G_1}{N} \subseteq \frac{G_2}{N} \subseteq ..... \subseteq \frac{G_{n-1}}{N} \subseteq \frac{G_n}{N} = \frac{G}{N}$ ...(2)

be solvable series of N and $\frac{G}{N}$. By definition of solvable series then $\frac{G_i}{N} \trianglelefteq \frac{G_{i+1}}{N}$ and $\frac{G_{i+1}/N}{G_i/N}$ is abelian $\forall\ i = 0, 1, 2, ..., n-1$

which gives $G_i \trianglelefteq G_{i+1}\ \forall\ i$ (See Lemma page 123)

Again by Third theorem of Isomorphism (Page 124) we have

$$\frac{G_{i+1}}{G_i} \cong \frac{G_{i+1}/N}{G_i/N}$$

Since $\frac{G_{i+1}/N}{G_i/N}$ is abelian, we find $\frac{G_{i+1}}{G_i}$ is abelian $\forall\ i$. Consider now the series

$$\{e\} = N_0 \subseteq N_1 \subseteq ... \subseteq N_k = N = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

then it satisfies all conditions in the definition of a solvable series and hence it is required solvable series of G showing thereby that G is solvable.

When we consider the series (2), it is clear that $G_0, G_1, ...,$ are all subgroups of G containing H.

Remark: We thus conclude that a group G with a normal subgroup N is solvable if both N and G/N are solvable. The converse, of course, being true.

Problem 22: *Show that a finite p-group is solvable, where p is prime.*

Solution: Let G be the given finite p-group, then $o(G) = p^n$ for some $n \geq 0$.

If $n = 1$, then G is a group of prime order and thus it is abelian. (See page 86)

and so G is solvable.

Suppose now $n > 1$. We use induction on n. Suppose that the result holds for all groups with order p^m where $m < n$, then by Problem 20, page 186, $o(Z(G)) > 1$.

Let $o(Z(G)) = p^t$, $t \geq 1$ (Notice $o(Z(G)) \mid o(G) = p^n$)

Thus $$o\left(\frac{G}{Z(G)}\right) = \frac{p^n}{p^t} = p^{n-t} = p^s \text{ where } s < n$$

Since result holds for groups with order p^m where $m < n$ we find $\frac{G}{Z(G)}$ is solvable.

Also $Z(G)$ is solvable as it is abelian.

Hence by above theorem G is solvable.

Problem 23: *Show that a solvable group contains at least one normal abelian subgroup H.*

Solution: Let G be a solvable group. If G is abelian then $H = G$ is the required subgroup.

Let now G be non abelian. Since G is solvable $G^{(n)} = \{e\}$ for some +ve integer n.

Now $G' \neq \{e\}$ as if $G' = \{e\}$ then G is abelian. (See page 164) which is not true. Hence $G^{(n)} = \{e\}$, $n \neq 1$

Let $H = G^{(n-1)}$ then H is a subgroup of G.

and as $H' = G^{(n)} = \{e\}$, we find H is abelian and also as $G^{(n-1)}$ is normal subgroup of G, we find H is the required subgroup.

Problem 24: *Let G be a finite solvable group, then a minimal non trivial normal subgroup of G is abelian.*

Solution: Let M be a minimal non-trivial normal subgroup of G. Since G is solvable, so would be M. Thus M has a solvable series

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = M$$

where $H_i \trianglelefteq H_{i+1}$ and $\frac{H_{i+1}}{H_i}$ is abelian.

Also then all composition factors of M will be of prime order (See problem). Thus $\exists$ a normal subgroup N of M s.t.,

$$\frac{M}{N} \text{ is of prime order (for instance, } N = H_{K-1})$$

Let $o(M/N) = p$, then $\frac{o(M)}{o(N)} = p$

Also this M/N will be abelian (See cor. on page 86).

Thus for any $x, y \in M$

$$NxNy = NyNx$$

$$\Rightarrow Nxy = Nyx \Rightarrow xyx^{-1}y^{-1} \in N$$

Again as $N \trianglelefteq M$, $g^{-1}Ng \trianglelefteq g^{-1}Mg$ for any $g \in G$

$$\Rightarrow g^{-1}Ng \trianglelefteq M \qquad \forall g \text{ as } M \text{ is normal}$$

Also $$o(g^{-1}Ng) = o(N) = \frac{o(M)}{p}$$

$$\Rightarrow o\left(\frac{M}{g^{-1}Ng}\right) = p, \text{ a prime}$$

and so $\dfrac{M}{g^{-1}Ng}$ is abelian $\forall g$

Proceeding as above, we can say (considering $\dfrac{M}{g^{-1}Ng}$ in place of M/N)

$$xyx^{-1}y^{-1} \in g^{-1}Ng \qquad \forall x, y \in M, g \in G$$

$$\Rightarrow xyx^{-1}y^{-1} \in \bigcap_{g \in G} g^{-1}Ng$$

If $K = \bigcap_{g \in G} g^{-1}Ng$ then $K \trianglelefteq G$ (See Problem 13, Page 105)

Also $$K \subseteq N \subseteq M$$

$$(k \in K \Rightarrow k \in \cap\, g^{-1}Ng \Rightarrow k \in g^{-1}Ng\ \forall g \Rightarrow k \in e^{-1}Ne \Rightarrow k \in N)$$

Since M is minimal normal either $K = M$ or $K = \{e\}$

But $K = M \Rightarrow N = M$, not possible as $o(M) = p = o(N)$

Hence $K = \{e\}$

i.e., $$xyx^{-1}y^{-1} \in K = \{e\} \qquad \forall x, y \in M$$

$$xy = yx \Rightarrow M \text{ is abelian.}$$

Problem 25: *Show that a group of order pq is solvable, where p, q are primes.*

Solution: Let $o(G) = pq$. If $p = q$ then $o(G) = p^2$ and thus G is an abelian group. (See page 186). Hence G is solvable. Let now $p > q$. Then number of Sylow p-subgroups of G is $1 + kp$ where $(1 + kp) \mid q$, *i.e.*, $1 + kp = 1$ or q.

If $1 + kp = q$ then $kp = q - 1 \Rightarrow p \mid (q - 1)$ which is not true, as $p > q$.

Hence $1 + kp = 1$ and there exists a unique normal Sylow p-subgroup, say H, of order p.

Since p is prime, H will be cyclic and so abelian and hence solvable.

Again $o\left(\dfrac{G}{H}\right) = q \Rightarrow \dfrac{G}{H}$ is abelian $\Rightarrow \dfrac{G}{H}$ is solvable $\Rightarrow G$ is solvable.

Problem 26: *Show that the following two statements are equivalent*:

(*a*) *Every group of order $p^m q^n$, where p, q are primes, is solvable.*

(*b*) *Simple groups of order $p^\alpha q^\beta$ are cyclic groups of order p or q.*

Solution: (*a*) $\Rightarrow$ (*b*)

Let G be a simple group of order $p^{\alpha}q^{\beta}$. Since G' is normal in G, we find either $G' = \{e\}$ or $G' = G$.

Since G is solvable, by (a) $G' = \{e\}$ and so G is abelian. (See page 164).

Let H be a Sylow p-subgroup of G. Then H will be normal as G is abelian and $o(H) = p^{\alpha}$

Again, G simple means either $H = G$ or $H = \{e\}$

If $H = G$, there $\alpha = 1$, $\beta = 0$ and so G is cyclic of order p

If $H = \{e\}$ then if K is sylow q-subgroup of G, it will be normal and as before, either, $K = G$ or $K = \{e\}$

If $K = G$, then $\alpha = 1$, $\beta = 0$ and so G is cyclic of order q.

If $K = \{e\}$, we get the case where $\alpha = 0$, $\beta = 0$ forcing $G = \{e\}$ which is not true as G is simple. Hence the result follows.

We now show that $(b) \Rightarrow (a)$.

Let G be a group of order $p^m q^n$.

Consider a composition series of G (which exists as G is finite) then every composition factor of this series will be a simple group of order $p^{\alpha}q^{\beta}$ for some α, β. By (b), each factor would, therefore, be cyclic and so abelian. Hence G is solvable.

Remark: There is a famous theorem of Burnside in which it is proved that every group of order $p^m q^n$ where p, q are primes, is solvable.

Problem 27: *Show that a finite solvable group G has a chain of subgroups.*

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_t = G$$

s.t., N_i *is a normal subgroup of G and* $\dfrac{N_{i+1}}{N_i}$ *is abelian,* $i = 0, 1, 2, \ldots, t-1$

Solution: We use induction on order G. If $o(G) = 2$, the result holds trivially as

$$\{e\} = G_0 \trianglelefteq G_1 = G \text{ and } \frac{G_1}{G_o} = \frac{G}{\{e\}} \cong G \text{ is abelian.}$$

Let the result hold for solvable groups having order less than $o(G)$.

If G has no non trivial normal subgroups then G is simple and solvable.

So G is abelian (See problem 19 on page 297) and thus the result holds.

Suppose now G has a non trivial normal subgroup. Let M be a minimal such subgroup. Then as in problem 24 above, M is abelian. Consider the group G/M then as $o(G/M) < o(G)$, by induction the result holds for G/M.

i.e., $\exists$ a series (for G/M)

$$\{I\} = \frac{M_0}{M} \trianglelefteq \frac{M_1}{M} \trianglelefteq \cdots \trianglelefteq \frac{M_n}{M} = \frac{G}{M}$$

s.t., $\dfrac{M_{i+1}}{M}$ is normal in G/M and

$$\frac{M_{i+1}}{M} \Big/ \frac{M_i}{M} \text{ is abelian and } M_{i+1} \trianglelefteq G \qquad \forall i = 0, 1, ..., n-1$$

$$\Rightarrow \{e\} \trianglelefteq M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_n = G \text{ and each } M_i \trianglelefteq G$$

By third theorem of isomorphism as $\dfrac{M_{i+1}/M}{M_i/M} \cong \dfrac{M_{i+1}}{M_i}$

we find $\dfrac{M_{i+1}}{M_i}$ is abelian $\forall i$.

Hence the result holds by induction.

Problem 28: *Show that* $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| a, b, c \in F \right\}$ *is a solvable group for any field F.*

Solution: Let $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ be any member of G

then $A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in G$

and G forms a group under matrix multiplication.

Also $G' = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| b \in F \right\}$

as $A, B \in G \Rightarrow A^{-1}B^{-1}AB$ is a matrix of the form $\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$\Rightarrow G' \subseteq$ R.H.S.

Also $\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b & -b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$

So R.H.S. $\subseteq G'$

Similarly, $G^{(2)} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$

Hence G is solvable.

Problem 29: *Show that the group G of all $n \times n$ invertible matrices ($n \geq 3$) over reals is not solvable.*

Solution: Let E_{ij} be the $n \times n$ matrix whose (i, j)th entry is 1 and other entries are zero.

Then $E_{ij}\, E_{jk} = E_{ik}$

and $E_{ij}\, E_{rs} = 0 \quad \text{if } j \neq r$

Now $(I + E_{ij})\,(I - E_{ij}) = I - E_{ij} + E_{ij} = 0 \quad \text{if } i \neq j$

So, $I - E_{ij} = (I + E_{ij})^{-1} \quad \text{for } i \neq j$

Thus $I + E_{ij} \in G.$

Let K be the subgroup of G generated by $\{I + E_{ij} \mid i \neq j\}$

Since $n \geq 3$, there exist three distinct integers i, j, k

Now
$$\begin{aligned}
&(I - E_{ik})\,(I + E_{kj})\,(I + E_{ik})^{-1}\,(I + E_{kj})^{-1} \\
&= (I + E_{ik})\,(I + E_{kj})\,(I - E_{ik})\,(I - E_{kj}) \\
&= (I + E_{ik})\,(I + E_{kj})\,(I - E_{kj} - E_{ik} + E_{ij}) \\
&= (I + E_{ik})\,(I - E_{kj} - E_{ik} + E_{ij} + E_{kj}) \\
&= (I + E_{ik})\,(I - E_{ik} + E_{ij}) \\
&= I + E_{ij}
\end{aligned}$$

So $I + E_{ij} \in K'$ and thus $K \subseteq K' \Rightarrow K = K' \Rightarrow K$ is not solvable $\Rightarrow G$ is not solvable.

Nilpotent Groups

Definition I: A group G is called *nilpotent* if it has a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots\ldots \subseteq G_n = G$$

such that $\dfrac{G_i}{G_{i-1}} \subseteq \mathrm{Z}\left(\dfrac{G}{G_{i-1}}\right) \quad \forall\ i = 1, 2, \ldots, n$

Definition II: We first define what we mean by nth centre of a group. Let G be a group and $Z(G)$ be its centre. We call $Z(G)$ the first centre of G and put $Z(G) = Z_1(G)$. Consider now the group $\dfrac{G}{Z(G)}$, then centre $\mathrm{Z}\left(\dfrac{G}{Z(G)}\right)$ of $\dfrac{G}{Z(G)}$ is a normal subgroup of $\dfrac{G}{Z(G)}$

So $\mathrm{Z}\left(\dfrac{G}{Z_1(G)}\right) \trianglelefteq \dfrac{G}{Z_1(G)}$

Since any normal subgroup of $\dfrac{G}{K}$ is of the form $\dfrac{H}{K}$ for a unique normal subgroup H of G, we find any normal subgroup of $\dfrac{G}{Z_1(G)}$ is of the type $\dfrac{H}{Z_1(G)}$ where $H \trianglelefteq G$

We write $H = Z_2(G)$ (Called second centre of G)

Then $Z_2(G) \trianglelefteq G$ s.t., $Z\left(\frac{G}{Z_1(G)}\right) = \frac{Z_2(G)}{Z_1(G)}$

Continuing like this we get $Z_n(G) \trianglelefteq G$, (called nth centre)

s.t., $$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left(\frac{G}{Z_{n-1}(G)}\right) \quad n > 1$$

Let us write $Z_0(G) = \{e\}$, and thus

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left(\frac{G}{Z_{n-1}(G)}\right) \quad \forall\ n = 1, 2, \ldots$$

Also then $Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots$ are normal subgroups of G. This is called the *upper central series* or *ascending central series* of G.

We say a group G is *nilpotent* if $Z_m(G) = G$ for some m. Also in that case the smallest m s.t., $Z_m(G) = G$ is called the class of nilpotency of G.

We first show the equivalence of the two definitions.

Definition I $\Rightarrow$ Definition II

Let G be nilpotent according to definition I. Then G has a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n = G$$

s.t., $$\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right) \quad \forall\ i = 1, 2, \ldots, n$$

Let $i = 1$, then

$$\frac{G_1}{G_0} \subseteq Z\left(\frac{G}{G_0}\right)$$

If $x \in G_1$ be any element, then

$$G_0 x \in \frac{G_1}{G_0} \quad \Rightarrow G_0 x \in Z\left(\frac{G}{G_0}\right)$$

$$\Rightarrow G_0 x \,.\, G_0 y = G_0 y G_0 x \quad \forall\ G_0 y \in \frac{G}{G_0}$$

$$\Rightarrow G_0 xy = G_0 yx$$
$$\Rightarrow xy\, x^{-1} y^{-1} \in G_0 = \{e\}$$
$$\Rightarrow xy = yx \quad \forall\ y \in G$$
$$\Rightarrow x \in Z(G) = Z_1(G)$$

Hence $G_1 \subseteq Z_1(G)$

Let $i = 2$, then

$$\frac{G_2}{G_1} \subseteq Z\left(\frac{G}{G_1}\right)$$

If $x \in G_2$ be any element then proceeding as above we get $xy\, x^{-1}y^{-1} \in G_1$

and as $G_1 \subseteq Z_1(G)$

$$xy\, x^{-1}y^{-1} \in Z_1(G) \quad \forall\, y \in G$$

$$\Rightarrow \quad Z_1(G)\, xy = Z_1(G)yx \Rightarrow Z_1(G)x\; Z_1(G)y = Z_1(G)y\; Z_1(G)x$$

$$\Rightarrow Z_1(G)x \in Z\left(\frac{G}{Z_1(G)}\right) = \frac{Z_2(G)}{Z_1(G)}$$

$$\Rightarrow x \in Z_2(G)$$

Hence $G_2 \subseteq Z_2(G)$

Continuing like this, we get

$$G_i \subseteq Z_i(G) \quad \forall\, i = 1, 2, \ldots n$$

Hence $G = G_n \subseteq Z_n(G)$

or that G is nilpotent according to definition II.

Definition II $\Rightarrow$ Definition I

Suppose G is nilpotent of class n then $Z_n(G) = G$. Consider the series

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots\ldots \subseteq Z_n(G) = G$$

which is a normal series and $\dfrac{Z_i(G)}{Z_{i-1}(G)} = Z\left(\dfrac{G}{Z_{i-1}(G)}\right)$

i.e., G is nilpotent according to definition I.

Example 24: An abelian group is nilpotent. Since G abelian

$$\Rightarrow G = Z(G) \textit{ i.e., } Z_1(G) = G.$$

Also then all cyclic groups will be nilpotent.

However, a nilpotent group need not be abelian and thus cyclic. Consider G, the quaternion group. Then

$$G_0 = \{1\} \subseteq G_1 = \{1, -1\} \subseteq G_2 = \{1, -1, i, -i\} \subseteq G$$

and $\quad o\left(\dfrac{G}{G_2}\right) = 2,\ o\left(\dfrac{G}{G_1}\right) = 4 \Rightarrow \dfrac{G}{G_1}, \dfrac{G}{G_2}$ are abelian

$\Rightarrow \quad Z\left(\dfrac{G}{G_1}\right) = \dfrac{G}{G_1}, Z\left(\dfrac{G}{G_2}\right) = \dfrac{G}{G_2}$. Also $Z\left(\dfrac{G}{G_0}\right) = \{G_{0^{(1)}}, G_{0^{(-1)}}\}$ is abelian

Thus $\quad Z\left(\dfrac{G}{G_0}\right) = \dfrac{G}{G_0}$ and so G is nilpotent but not abelian.

Example 25: A finite p-group is nilpotent. See exercises.

Theorem 15: *Every nilpotent group is solvable. Converse is not true.*

Proof: Let G be a nilpotent group, then G has a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n = G$$

where $\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right)$. $\forall\ i = 1, 2, \ldots n$

Which implies that $\frac{G_i}{G_{i-1}}$ is abelian $\forall\ i$

Hence G is solvable.

S_3 is solvable but not nilpotent. Notice that $Z(S_3) = \{I\}$ and so $Z_m(G) = G$ holds for no m. (In fact S_n is not nilpotent, for $n \geq 3$).

Theorem 16: *Any subgroup of a nilpotent group is nilpotent.*

Proof: Let H be a subgroup of a nilpotent group G. Since G is nilpotent, there exists a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots\ldots \subseteq G_n = G$$

s.t., $\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right)$, $i = 1, 2, \ldots, n$

Consider the series

$$\{e\} = G_0 \cap H \subseteq G_1 \cap H \subseteq G_2 \cap H \subseteq \ldots \subseteq G_n \cap H = G \cap H = H$$

It is easy to see that $G_{i-1} \cap H \trianglelefteq G_i \cap H \quad \forall\ i$. We show

$\frac{G_i \cap H}{G_{i-1} \cap H} \subseteq Z\left(\frac{G \cap H}{G_{i-1} \cap H}\right)$, $\forall\ i = 1, 2, \ldots, n$ which would establish that H is nilpotent.

Let $(G_{i-1} \cap H)x \in \frac{G_i \cap H}{G_{i-1} \cap H}$ be any element

then $x \in G_i \cap H \Rightarrow x \in G_i$ and $x \in H$.

Now $(G_{i-1} \cap H)x \in Z\left(\frac{G \cap H}{G_{i-1} \cap H}\right)$

if $(G_{i-1} \cap H)x$ commutes with all elements of $\frac{G \cap H}{G_{i-1} \cap H}$

i.e., $(G_{i-1} \cap H)x\ (G_{i-1} \cap H)y = (G_{i-1} \cap H)y\ (G_{i-1} \cap H)x \quad \forall\ y \in G \cap H$

i.e., $(G_{i-1} \cap H)xy = (G_{i-1} \cap H)yx$

i.e., $xy\ x^{-1}y^{-1} \in G_{i-1} \cap H \quad \forall\ y \in G \cap H$

i.e., $xy\ x^{-1}y^{-1} \in G_{i-1}$ and $xy\ x^{-1}y^{-1} \in H \quad \forall\ y \in G \cap H$

Now $x \in H, y \in H \Rightarrow xy\ x^{-1}y^{-1} \in H$

Again, since $\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right)$ and $x \in G_i$, we find that

$$G_{i-1}x \in \frac{G_i}{G_{i-1}} \Rightarrow G_{i-1}x \in Z\left(\frac{G}{G_{i-1}}\right)$$

$$\Leftrightarrow G_{i-1}x\ G_{i-1}y = G_{i-1}y\ G_{i-1}x \quad \forall\ y \in G$$

$$\Leftrightarrow G_{i-1}xy = G_{i-1}yx$$

$$\Leftrightarrow xy\ x^{-1}y^{-1} \in G_{i-1} \quad \forall\ y \in G$$

and hence over assertion is proved.

Theorem 17: *Homomorphic image of a nilpotent group is nilpotent.*

Proof: Let $\theta : G \to H$ be an onto homomorphism and suppose G is nilpotent. Then there exists a normal series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots\ldots \subseteq G_n = G$$

s.t., $$\frac{G_i}{G_{i-1}} \subseteq Z\left(\frac{G}{G_{i-1}}\right) \quad \forall\ i = 1, 2, \ldots, n$$

We claim

$\theta(e) = \theta(G_0) \subseteq \theta(G_1) \subseteq \theta(G_2) \subseteq \ldots \subseteq \theta(G_n) = \theta(G) = H$ is the required normal series for H where $\dfrac{\theta(G_i)}{\theta(G_{i-1})} \subseteq Z\left(\dfrac{\theta(G)}{\theta(G_{i-1})}\right)$

It is easy to see that $\theta(G_{i-1}) \trianglelefteq \theta(G_i) \quad \forall\ i$ and we leave it for the reader to try and prove it.

Let $\theta(G_i) = H_i \quad i = 1, 2, \ldots, n$

we show $\dfrac{H_i}{H_{i-1}} \subseteq Z\left(\dfrac{H}{H_{i-1}}\right)$

Let $H_{i-1}x \in \dfrac{H_i}{H_{i-1}}$ be any element,

we have to show that $H_{i-1}x \in Z\left(\dfrac{H}{H_{i-1}}\right)$

i.e., $(H_{i-1}x)\ (H_{i-1}y) = (H_{i-1}y)\ (H_{i-1}x) \quad \forall\ H_{i-1}y \in \dfrac{H}{H_{i-1}}$

i.e., $H_{i-1}xy = H_{i-1}yx$

i.e., $xy\ x^{-1}y^{-1} \in H_{i-1}\ \forall\ y \in H$

Now $x \in H_i \Rightarrow x \in \theta(G_i) \Rightarrow \exists\ a \in G_i$ s.t., $\theta(a) = x$

$y \in H \Rightarrow y = \theta(G) \Rightarrow \exists\ b \in G$, s.t., $\theta(b) = y$

Thus $xy\ x^{-1}y^{-1} = \theta(a)\ \theta(b)\ (\theta(a))^{-1}\ (\theta(b))^{-1} = \theta(ab\ a^{-1}b^{-1}) \in \theta(G_{i-1})$

Since $a \in G_i,\ G_{i-1}\ a \in \dfrac{G_i}{G_{i-1}} \subseteq Z\left(\dfrac{G}{G_{i-1}}\right)$

and so $G_{i-1}\, a \,.\, G_{i-1}\, b = G_{i-1}\, b\, G_{i-1}\, a$

i.e., $G_{i-1}\, ab = G_{i-1}\, ba$

i.e., $ab\, a^{-1}b^{-1} \in G_{i-1}$

i.e., $\theta(ab\, a^{-1}b^{-1}) \in \theta(G_{i-1}) = H.$

Hence the resuit follows.

Theorem 18: *Any quotient group of a nilpotent group is nilpotent.*

Proof: Follows from above theorem as any quotient group of a group is its homomorphic image.

Converse is, however, not true as $\frac{S_3}{A_3}$ is abelian and so nilpotent, but S_3 is not nilpotent.

Problem 30: *If H and K are nilpotent groups then show that H × K is also nilpotent.*

Solution: Let H and K be nilpotent. Then $\exists$ normal series

$$\{e_1\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots\ldots \subseteq H_n = H \quad \text{s.t.,} \quad \frac{H_i}{H_{i-1}} \subseteq Z\left(\frac{H}{H_{i-1}}\right) \quad i = 1, 2, \ldots, n$$

$$\{e_2\} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots\ldots \subseteq K_n = K \quad \text{s.t.,} \quad \frac{K_i}{K_{i-1}} \subseteq Z\left(\frac{K}{K_{i-1}}\right)$$

We can repeat terms in the series with lesser terms.

Consider the series

$\{e_1\} \times \{e_2\} = H_0 \times K_0 \subseteq H_1 \times K_1 \subseteq H_2 \times K_2 \subseteq \ldots\ldots \subseteq H_n \times K_n = H \times K$

Then one can check that this is a normal series in which

$$\frac{H_i \times K_i}{H_{i-1} \times K_{i-1}} \subseteq Z\left(\frac{H \times K}{H_{i-1} \times K_{i-1}}\right)$$

Let $(H_{i-1} \times K_{i-1})\ (h, k) \in \frac{H_i \times K_i}{H_{i-1} \times K_{i-1}}$ be any element

then $(H_{i-1} \times K_{i-1})\ (h, k)$ will belong to $Z\left(\frac{H \times K}{H_{i-1} \times K_{i-1}}\right)$

if $(H_{i-1} \times K_{i-1})\ (h, k).(H_{i-1} \times K_{i-1})\ (x, y) = (H_{i-1} \times K_{i-1})\ (x \,.\, y).(H_{i-1} \times K_{i-1})\ (h, k)$

i.e., if $(h, k)\ (x, y)\ (h, k)^{-1}\ (x, y^{-1}) \in H_{i-1} \times K_{i-1}$

i.e., if $(hx\ h^{-1}x^{-1},\ hy\ k^{-1}y^{-1}) \in H_{i-1} \times K_{i-1}$

i.e., if $h\ x\ h^{-1}x^{-1} \in H_{i-1}$

$ky\ k^{-1}y^{-1} \in K_{i-1}$

which is true.

We leave the first part (that $H_i \times K_i \trianglelefteq H_{i+1} \times K_{i+1}$) for the reader to try as an exercise.

Problem 31: *If H is a proper subgroup of a nilpotent group G then show that H is a proper*

subgroup of $N(H)$.

Solution: Since G is nilpotent, it has upper central series

$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots\ldots \subseteq Z_n(G) = G$

Now $H \subsetneqq G$, let i be the largest integer s.t., $Z_i(G) \subseteq H$

Then we get

$$Z_i(G) \subseteq H \subseteq Z_{i+1}(G) \subseteq \ldots$$

Again since $\dfrac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\dfrac{G}{Z_i(G)}\right)$

$\dfrac{Z_{i+1}(G)}{Z_i(G)}$ is abelian.

Let $g \in Z_{i+1}(G)$ and $h \in H$ be any elements, then

$h \in H \subseteq Z_{i+1}(G)$ and so $Z_i(G)g,\ Z_i(G)h \in \dfrac{Z_{i+1}(G)}{Z_i(G)}$ and thus

$$Z_i(G)g\ Z_i(G)h = Z_i(G)h\ Z_i(G)g$$
$$\Rightarrow Z_i(G)gh = Z_i(G)hg$$
$$\Rightarrow gh\ g^{-1}h^{-1} \in Z_i(G) \subseteq H$$
$$\Rightarrow gh\ g^{-1} \in H \quad \forall\ g \in Z_{i+1}(G),\ h \in H$$
$$\Rightarrow gH\ g^{-1} \subseteq H \quad \forall\ g \in Z_{i+1}(G)$$

i.e., $gH\ g^{-1} = H \ \forall\ g \in Z_{i+1}(G)$

$\Rightarrow$ any $g \in Z_{i+1}(G)$ is such that $g \in N(H)$

or that $Z_{i+1}(G) \subseteq N(H)$

But $H \subsetneqq Z_{i+1}(G)$ and hence H is a proper subgroup of $N(H)$.

Exercises

1. Show that A_4 is solvable.

2. Show that $H \times K$ is solvable iff H and K are solvable.

3. Let H and K be normal subgroups of G. Show that $\dfrac{G}{H \cap K}$ is solvable iff $\dfrac{G}{H}$ and $\dfrac{G}{K}$ are solvable.

4. Let H and K be solvable subgroups of G where K is normal. Show that HK is solvable subgroup of G.

5. Let G be a group. Show that the following are equivalent.

(i) G is solvable

(ii) G' is solvable

(*iii*) $\frac{G}{Z}$ is solvable where Z denotes centre of G.

6. Show that a simple group is solvable iff it is cyclic.

7. Show that $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \; a, b, c \in \mathbf{Z}_3 \right\}$ is a solvable group. (Hint: $o(G) = 3^3$)

8. If p, q are primes, show that groups of order p^2q, p^2q^2 are solvable.

9. Give example of a group all of whose proper subgroups are solvable but group itself is not. (Consider A_5).

10. If all proper subgroups of a non solvable group G are solvable, show that $G = G'$. (A group G such that $G = G'$ is called a perfect group).

11. Show that every group of odd order is solvable iff every finite non abelian simple group has even order.

12. Show that direct product of infinitely many solvable groups need not be solvable.

13. Show that a finite p-group is nilpotent.

14. Show that the result proved in theorem 14 for solvable groups does not hold for nilpotent groups. [Hint:Consider S_3/A_3]

15. Give an example of a solvable group G in which $H \leq G$, $H \neq G$ and $N(H) \neq H$.

16. Suppose that in a non abelian simple group, $\{e\}$ is the only conjugate class whose order is prime power. Show that a group of order p^mq^n (p, q primes) is a solvable group.

17. Let G be a nilpotent group. Show that every maximal subgroup of G is normal subgroup. Hence deduce that S_3 is not nilpotent. (Use problem 31)

18. Show that every sylow subgroup of a nilpotent group G is normal in G. (See exercise 17)

19. Show that a nilpotent group is isomorphic to the direct product of its Sylow subgroups.

20. If G is direct product of its Sylow subgroups, show that G is nilpotent. (Use exercise 13 and problem 30).

A Quick Look at what's been done

- If G is a group and $A$is a non-empty set, then ***G* is said to act on *A*** if there exists a function $*$ from $G \times A \to A$, s.t.,
  (*i*) $g_1 * (g_2 * a) = (g_1 g_2) * a$
  (*ii*) $e * a = a$ for all g_1, g_2 in G and a in A
- Let G be any group and A be any set. Then any group homomorphism from G to Sym(A) the symmetric group of A defines an action of G on A. Conversely, every action of G on A induces a homomorphism from G to Sym(A).
- The above homomorphism is called the associated (or the corresponding) permutation representation of the given action.
- If $*$ be a group action of G on A, then **kernel** of $*$ is defined to be the set Ker $(*) = \{ g \in G \mid g * a = a$ for all $a \in A\}$. This is seen to be equal to the kernel of the associated permutation representation.
- An action $*$ is said to be *faithful* if, whenever $g * a = a$ then $g = e$.
- Let G be a group acting on a set A. For each a in A, the set
  $Ga = \{x \in A \mid x = g * a$ for some $g \in G\}$
  $= \{g * a \mid g \in G\}$ is called an **orbit** of a under G.
  Again, let $a \in A$ be a fixed element, then the set $G_a = \{g \in G \mid g * a = a\}$ is called the **stabilizer** of a in G and it forms a subgroup of G.
- The **Orbit-Stabilizer theorem** says that if G is a group acting on A and $a \in A$, then there exists a one-one onto map from Ga to the set of all cosets of G_a in G.
- Every permutation in S_n can be expressed as a unique product of disjoint cycles, is proved using group actions.
- Every finite group with more than one element has a composition series.
- **Jordan-Hölder** theorem states that in a finite group any two composition series are equivalent.
- A group G is said to be solvable if there exists a chain of subgroups $\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots\ldots \subseteq H_n = G$, s.t., each H_i is a normal subgroup of H_{i+1} and H_{i+1}/H_i is abelian, $i = 1, 2, 3, \ldots, n-1$.
- Abelian and cyclic groups are solvable and so are S_3 ,S_4.
- A group G is solvable iff $G^{(n)} = \{e\}$ for some +ve integer n.
- Every nilpotent group is solvable, converse is not true.
- Subgroups, homomorphic images, quotient groups of solvable (nilpotent) groups are solvable (nilpotent).

7

Rings

Introduction

A group we noticed is a system with a non empty set and a binary composition. One can of course talk about non empty sets with two binary compositions also, the set of integers under usual addition and multiplication being an example. Though this set forms a group under addition and not under multiplication, it does have certain specific properties satisfied with respect to multiplication as well. We single out some of these and generalise the concept in the form of a ring. We start with the formal definition and generalize the concept in the form of a ring. We will then go on to study subrings and ideals (remember the normal subgroups) and various properties related to these. We start with the formal definition.

Definition: A non empty set R, together with two binary compositions + and . is said to form a *Ring* if the following axioms are satisfied:

(i) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$

(ii) $a + b = b + a$ for $a, b \in R$

(iii) $\exists$ some element 0 (called zero) in R, s.t., $a + 0 = 0 + a = a$ for all $a \in R$

(iv) for each $a \in R$, $\exists$ an element $(-a) \in R$, s.t., $a + (-a) = (-a) + a = 0$

(v) $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$ for all $a, b, c \in R$

(vi) $a \,.\, (b + c) = a \,.\, b + a \,.\, c$

$(b + c) \,.\, a = b \,.\, a + c \,.\, a$ for all $a, b, c \in R$

Remarks: (a) Since we say that + and . are binary compositions on R, it is understood that the closure properties w.r.t. these hold in R. In other words, for all $a, b \in R$, $a + b$ and $a \,.\, b$ are unique in R.

(b) One can use any other symbol instead of + and ., but for obvious reasons, we use these two symbols (the properties look so natural with these). In fact, in future, the statement that R is a ring would mean that R has two binary compositions + and . defined on it and satisfies the above axioms.

(c) Axiom (v) is named associativity w.r.t. . and axiom (vi) is referred to as distributivity (left and right) w.r.t. . and +.

(d) Axioms (i) to (iv) could be restated by simply saying that $< R, + >$ forms an abelian group.

(*e*) Since 0 in axiom (*iii*) is identity w.r.t. +, it is clear that this element is unique (see groups).

Definitions: A ring R is called a *commutative* ring if $ab = ba$ for all $a, b \in R$. Again if $\exists$ an element $e \in R$ s.t.,

$$ae = ea = a \quad \text{for all } a \in R$$

we say, R is a ring with *unity*. Unity is generally denoted by 1. (It is also called unit element or multiplicative identity).

It would be easy to see that if unity exists in a ring then it must be unique.

Remark: We recall that in a group by a^2 we meant $a \cdot a$ where '.' was the binary composition of the group. We continue with the same notation in rings as well. In fact, we also introduce similar notation for addition, and shall write na to mean $a + a + ...+ a$ (n times), n being an integer.

Example 1: Sets of real numbers, rational numbers, integers form rings w.r.t. usual addition and multiplication. These are all commutative rings with unity.

Example 2: Set **E** of all even integers forms a commutative ring, without unity (under usual addition and multiplication).

Example 3: (*a*) Let M be the set of all 2×2 matrices over integers under matrix addition and matrix multiplication. It is easy to see that M forms a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, but is not commutative.

(*b*) Let M be set of all matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ over integers under matrix addition and multiplication. Then M forms a non commutative ring without unity.

Example 4: The set $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ forms a ring under addition and multiplication modulo 7. (In fact, we could take n in place of 7).

Example 5: The set $R = \{0, 4, 6\}$ under addition and multiplication modulo 6 forms a commutative ring with unity. The composition tables are

$\oplus$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\odot$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

Since $0 \odot 4 = 0$, $2 \odot 4 = 2$, $4 \odot 4 = 4$, we notice 4 is unity of R.

Example 6: Let F be the set of all continuous functions $f : \mathbf{R} \to \mathbf{R}$, where **R** = set of real numbers. Then F forms a ring under addition and multiplication defined by:

for any $f, g \in F$

$$(f + g)x = f(x) \quad \text{for all } x \in \mathbf{R}$$

$$(f\,g)x = f(x)g(x) \quad \text{for all } x \in \mathbf{R}$$

zero of this ring is the mapping $O : \mathbf{R} \to \mathbf{R}$, s.t.,

$$O(x) = 0 \text{ for all } x \in \mathbf{R}$$

Also additive inverse of any $f \in F$ is the function $(-f) : \mathbf{R} \to \mathbf{R}$ s.t., $(-f)x = -f(x)$

In fact, F would have unity also, namely the function $i : \mathbf{R} \to \mathbf{R}$ defined by $i(x) = 1$ for all $x \in \mathbf{R}$.

Remark: Although the same notation fg has been used for product here it should not be mixed up with fog defined earlier.

Example 7: Let $\mathbf{Z}$ be the set of integers, then $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ forms a ring under usual addition and multiplication of complex numbers. $a + ib$ where $a, b \in \mathbf{Z}$ is called a Gaussian integer and $\mathbf{Z}[i]$ is called the ring of Guassian integers.

We can similarly get $\mathbf{Z}_n[i]$ the ring of Gaussian integers modulo n. For instance,

$$\mathbf{Z}_3[i] = \{a + ib \mid a, b \in \mathbf{Z}_3 = \{0, 1, 2\} \bmod 3\}$$
$$= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$$

Example 8: Let X be a non empty set. Then $\mathcal{P}(X)$ the power set of X (*i.e.*, set of all subsets of X) forms a ring under + and $\cdot$ defined by

$$A + B = (A \cup B) - (A \cap B)$$
$$A \,.\, B = A \cap B$$

In fact, this is a commutative ring with unity and also satisfies the property $A^2 = A$ for all $A \in \mathcal{P}(X)$.

Example 9: Let M = set of all 2×2 matrices over members from the ring of integers modulo 2. *It would be a finite non commutative ring*. M would have $2^4 = 16$ members as each element a, b, c, d in matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ can be chosen in 2 ways. Compositions in M are given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \oplus x & b \oplus y \\ c \oplus z & d \oplus u \end{bmatrix}$$

where $\oplus$ denotes addition modulo 2 and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \otimes x \oplus b \otimes z & a \otimes y \oplus b \otimes u \\ c \otimes x \oplus d \otimes z & c \otimes y \oplus d \otimes u \end{bmatrix}$$

$\otimes$ being multiplication modulo 2.

That M is non commutative follows as $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

But $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Example 10: Let $R = \{0, a, b, c\}$. Define + and . on R by

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

Then one can check that R forms a non commutative ring without unity. In fact (see later on page 328) it is an example of the smallest non commutative ring.

Theorem 1: *In a ring R, the following results hold*

(*i*) $a \cdot 0 = 0 \cdot a = 0$ *for all* $a \in R$

(*ii*) $a(-b) = (-a)b = -ab$ *for all* $a, b \in R$

(*iii*) $(-a)(-b) = ab$. $\forall\ a, b \in R$

(*iv*) $a(b - c) = ab - ac$. $\forall\ a, b, c \in R$

Proof: (*i*) $a \cdot 0 = a \cdot (0 + 0)$

$\Rightarrow\ a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow\ a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow\ 0 = a \cdot 0$

using cancellation w.r.t + in the group $< R, + >$.

(*ii*) $a \cdot 0 = 0$

$\Rightarrow\ a(-b + b) = 0$

$\Rightarrow\ a(-b) + ab = 0$

$\Rightarrow\ a(-b) = -(ab)$

similarly $(-a)b = -ab$.

(*iii*) $(-a)(-b) = -[a(-b)] = -[-ab] = ab$

(*iv*) $a(b - c) = a(b + (-c))$

$= ab + a(-c)$

$= ab - ac$.

Remarks: (*i*) If R is a ring with unity and $1 = 0$, then since for any $a \in R$, $a = a.1 = a.0 = 0$, we find $R = \{0\}$ which is called the *trivial* ring. We generally exclude this case and thus whenever, we say R is a ring with unity, it will be understood that $1 \neq 0$ in R.

(*ii*) If n, m are integers and a, b elements of a ring, then it is easy to see that

$$n(a + b) = na + nb$$

$$(n + m)a = na + ma$$

$$(nm)a = n(ma)$$

$$a^m a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$ (see under groups).

Problem 1: *Let $<R, +, .>$ be a ring where the group $<R, +>$ is cyclic. Show that R is a commutative ring:*

Solution: Let $< R, + >$ be generated by a. Let $x, y \in R$ be any two elements, then $x = ma$, $y = na$ for some integers m, n.

Now $xy = (ma)(na)$

$= (a + a + ... + a)(a + a + ... + a)$

m times n times

$= (mn)a^2 = (nm)a^2 = (na)(ma) = yx$

We are so much used to the property that whenever $ab = 0$ then either $a = 0$ or $b = 0$ that it may need more than a bit of convincing that the result may not always be true. Indeed in the ring of integers (or reals or rationals) this property holds. But if we consider the ring of 2×2 matrices over integers, we notice, we can have two non zero elements A, B s.t, $AB = 0$, but $A \neq 0$ $B \neq 0$. In fact, take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ then $A \neq 0$, $B \neq 0$. But $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. We formalise this notion through

Definition: Let R be a ring. An element $0 \neq a \in R$ is called a *zero-divisor*, if $\exists$ an element $0 \neq b \in R$ s.t., $ab = 0$ or $ba = 0$.

Definition: A commutative ring R is called an *Integral domain* if $ab = 0$ in $R \Rightarrow$ either $a = 0$ or $b = 0$. In other words, a commutative ring R is called an integral domain if R has no zero divisors.

An obvious example of an integral domain is $< \mathbf{Z}, +, \cdot >$ the ring of integers whereas the ring of matrices, talked about above is an example of a ring which is not an integral domain. Again, $\mathbf{Z} \times \mathbf{Z}$ will not be an integral domain (See pages 337, 372).

Remark: Some authors do not insist upon the condition of commutativity as a part of the definition of an integral domain. One can have (see examples 11, 12 ahead), non commutative rings without zero divisors.

The following theorem gives us a necessary and sufficient condition for a commutative ring to be an integral domain.

Theorem 2: *A commutative ring R is an integral domain iff for all $a, b, c \in R$ $(a \neq 0)$*

$ab = ac \Rightarrow b = c$.

Proof: Let R be an integral domain

Let $ab = ac$ $(a \neq 0)$

Then $ab - ac = 0$

$\Rightarrow$ $a(b - c) = 0$

$\Rightarrow$ $a = 0$ or $b - c = 0$

Since $a \neq 0$, we get $b = c$.

Conversely, let the given condition hold.

Let $a, b \in R$ be any elements with $a \neq 0$.

Suppose $ab = 0$

then $ab = a.0$

$\Rightarrow \quad b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark: A ring R is said to satisfy *left cancellation law* if for all $a, b, c \in R$, $a \neq 0$

$ab = ac \Rightarrow b = c$.

Similarly we can talk of *right cancellation law*. It might, of course, be noted that cancellation is of only non zero elements.

Definition: An element a in a ring R with unity, is called invertible (or a *unit*) w.r.t. multiplication if $\exists$ some $b \in R$ such that $ab = 1 = ba$.

Notice, unit and unit element (unity) are different concepts and should not be confused with each other.

Definition: A ring R with unity is called a *Division ring* or a *skew field* if non zero elements of R form a group w.r.t. multiplication.

In other words, a ring R with unity is a Division ring if non zero elements of R have multiplicative inverse.

Definition: A commutative division ring is called a *field*.

Real numbers form a field, whereas integers do not, under usual addition and multiplication. Since a division ring (field) forms groups w.r.t. two binary compositions, it must contain two identity elements 0 and 1 (w.r.t. addition and multiplication) and thus a division ring (field) has at least two elements (see remark on page 315).

Example 11: A *division ring which is not a field*. Let M be the set of all 2×2 matrices of the type $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ where a, b are complex numbers and $\bar{a}, \bar{b}$ are their conjugates, *i.e.*, if $a = x + iy$ then $\bar{a} = x - iy$. Then M is a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ under matrix addition and matrix multiplication.

Any non zero element of M will be $\begin{bmatrix} x+iy & u+iv \\ -(u-iv) & x-iy \end{bmatrix}$

where x, y, u, v are not all zero.

One can check that the matrix $\begin{bmatrix} \dfrac{x-iy}{k} & -\dfrac{u+iv}{k} \\ \dfrac{u-iv}{k} & \dfrac{x+iy}{k} \end{bmatrix}$

where $k = x^2 + y^2 + u^2 + v^2$, will be multiplicative inverse of the above non zero matrix, showing that M is a division ring. But M will not be a field as it is not commutative as

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

But $$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

Example 12: Consider

$D = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$ with $i^2 = j^2 = k^2 = -1$, then D forms a ring.

Two elements $a + bi + cj + dk$ and $a' + b'i + c'j + d'k$ are equal iff $a = a'$, $b = b'$, $c = c'$, $d = d'$.

Addition and multiplication on D are defined by

$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b') + (c + c') + (d + d')k$

and

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' - bd' + ca' - db')j + (ad' + bc' - ab' + da')k$$

The symbol + in the elements of D is just a notation and is not to be a confused with addition in real numbers. We identity an element $o + 1i + oj + ok$ by i and so on.

Thus since $i = 0 + 1i + 0j + 0k$

$j = 0 + 0i + 1j + 0k$

We have $ij = k$, $ji = -k$, etc., In fact that shows that D is non commutative. D has unity $1 = 0 + 0i + 0j + 0k$

If $a + bi + cj + dk$ be any non zero element of D (*i.e.*, at least one of a, b, c, d is non zero) then $(a + bi + cj + dk)\dfrac{(a - bi - cj - dk)}{a^2 + b^2 + c^2 + d^2} = 1$.

Hence D is a division ring but not a field.

The elements of D can also be written as quadruples (a, b, c, d).

This ring D is called the *ring of quaternions*.

Theorem 3: *A field is an integral domain.*

Proof: Let $< R, +, . >$ be a field, then R is a commutative ring.

Let $ab = 0$ in R. We want to show either $a = 0$ or $b = 0$. Suppose $a \neq 0$, then a^{-1} exists (definition of field)

thus $ab = 0$

$\Rightarrow \quad a^{-1}(ab) = a^{-1}0$

$\Rightarrow \quad b = 0.$

which shows that R is an integral domain.

Remark: Similarly we can show that a division ring is an integral domain and thus has no zero divisiors.

A 'partial converse' of the above result also holds.

Theorem 4: *A non zero finite integral domain is a field.*

Proof: Let R be a non zero finite integral domain.

Let R' be the subset of R containing non zero elements of R.

Since associativity holds in R, it will hold in R'. Thus R' is a finite semi group.

Again cancellation laws hold in R (for non zero elements) and therefore, these hold in R'.

Hence R' is a finite semi group w.r.t. multiplication in which cancellation laws hold.

$\therefore$ $< R', \cdot >$ forms a group. Note closure holds in R' as R is an integral domain.

In other words $< R, +, \cdot >$ is a field (it being commutative as it is an integral domain).

Aliter: Let $R = \{a_1, a_2, ..., a_n\}$ be a finite non zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, ..., aa_n$ are all in R and if $aa_i = aa_j$ for some $i \neq j$, then by cancellation we get $a_i = a_j$ which is not true. Hence $aa_1, aa_2, ..., aa_n$ are distinct members of R.

Since $a \in R$, $a = aa_i$ for some i

Let $x \in R$ be *any* element, then $x = aa_j$ for some j

Thus $ax = (aa_i)x = a(a_ix)$

i.e., $x = a_ix$

Hence using commutativity we find

$$x = a_ix = xa_i$$

or that a_i is unity of R. Let $a_i = 1$

Thus for $1 \in R$, since $1 = aa_k$ for some k

We find a_k is multiplicative inverse of a. Hence any non zero element of R has multiplicative inverse or that R is a field.

Example 13: An infinite integral domain which is not a field is the ring of integers.

Definition: A ring R is called a *Boolean ring* if $x^2 = x$ for all $x \in R$.

Example 14: The ring $\{0, 1\}$ under addition and multiplication mod 2 forms a Boolean ring.

Problem 2: *Show that a Boolean ring is commutative*.

Solution: Let $a, b \in R$ be any elements

Then $a + b \in R$ (closure)

By given condition

$$(a + b)^2 = a + b$$

$$\Rightarrow \quad a^2 + b^2 + ab + ba = a + b$$

$$\Rightarrow \quad a + b + ab + ba = a + b$$

$$\Rightarrow \quad ab + ba = 0$$

$$\Rightarrow \quad ab = -ba \qquad ...(1)$$

$$\Rightarrow \quad a(ab) = a(-ba)$$

$$\Rightarrow \quad a^2b = -aba$$

$$\Rightarrow \quad ab = -aba \qquad ...(2)$$

Again (1) gives

$$(ab)a = (-ba)a$$

$$\Rightarrow \quad aba = -ba^2 = -ba \qquad ...(3)$$

(2) and (3) give

$$ab = ba \ (= -aba)$$

or that R is commutative.

Problem 3: *Show that order of a finite Boolean ring is of the type 2^n, n = 0, 1, 2,....*

Solution: : Let $< R, +, . >$ be a finite Boolean ring. Then $a^2 = a \quad \forall\ a \in R$,

Thus $(a + a)^2 = a + a$

$\Rightarrow a^2 + a^2 + 2aa = a + a$

$\Rightarrow 2a^2 = 0$ or that $2a = 0 \quad \forall\ a \in R$

Thus each non zero element in the group $< R, + >$ has order 2.

By Cauchy's theorem in groups, we know if p is any prime dividing $o(R)$ then $\exists\ x \in R$, s.t., $o(x) = p$. But order of each non zero element is 2 and thus 2 is the only prime dividing $o(R)$. Hence $o(R) = 2^n$.

Problem 4: (*a*) *Show that a non zero element a in* $\mathbf{Z}_n$ *is a unit iff a and n are relatively prime.*

(*b*) *If a is not a unit then it is a zero divisor.*

Solution: (*a*) $\mathbf{Z}_n = \{0, 1, 2, ..., n - 1\} \bmod n$

Let $a \in \mathbf{Z}_n$ be a unit, then $\exists\ b \in \mathbf{Z}_n$ s.t.,

$$a \otimes b = 1$$

i.e., when ab is divided by n, remainder is 1, in other words,

$$ab = nq + 1$$

or $\quad ab - nq = 1$

$\Rightarrow$ a and n are relatively prime.

Conversely, let $(a, n) = 1$, then $\exists$ integers u, v s.t.,

$$au + nv = 1$$

$$\Rightarrow \quad au = n(-v) + 1$$

Suppose, $\quad u = nq + r, \quad 0 \le r < n, \quad r \in \mathbf{Z}_n$,

Then $\quad au = anq + ar = n(-v) + 1$

$$\Rightarrow \quad ar = n(-v - aq) + 1, \quad r \in \mathbf{Z}_n$$

i.e., $\quad a \otimes r = 1, \quad r \in \mathbf{Z}_n$

i.e., $\quad a$ is a unit.

(*b*) Let a be not a unit and suppose g.c.d$(a, n) = d > 1$

Since $d \mid a$, $a = dk$ for some k. Also $d \mid n \Rightarrow n = dt$

$$\Rightarrow a.t = dk\ \frac{n}{d} = kn = 0 \bmod n$$

i.e., a is a zero divisor.

Remark: In $\mathbf{Z}_n$, the set of units is u_n. Thus for instance, in $\mathbf{Z}_8$ 1, 3, 5, 7 are units.

Problem 5: *Show that* $\mathbf{Z}_p = \{0, 1, 2, ..., p - 1\}$ *modulo p is a field iff p is a prime.*

Solution: Let $\mathbf{Z}_p$ be a field. Suppose p is not a prime, then $\exists\ a, b$, such that $p = ab$, $1 < a, b < p$

$\Rightarrow a \otimes b = 0$ where a, b are non zero $\Rightarrow \mathbf{Z}_p$ has zero divisors.

i.e. $\mathbf{Z}_p$ is not an integral domain, a contradiction as $\mathbf{Z}_p$ being a field is an integral domain. Hence p is prime.

Conversely, let p be a prime. We need show that $\mathbf{Z}_p$ is an integral domain (it being finite will then be a field).

Let $a \otimes b = 0 \qquad a, b \in \mathbf{Z}_p$

Then ab is a multiple of p

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$ (p being prime)

$\Rightarrow a = 0$ or $b = 0$ (Notice $a, b \in \mathbf{Z}_p \Rightarrow a\ , b < p$)

$\Rightarrow \mathbf{Z}_p$ is an integral domain and hence a field.

Remark : (*i*) We can also use problem 4 to prove this result.

(*ii*) Since $\mathbf{Z}_p$ is a field, all its non zero elements are units by definition of a field.

Problem 6: *If in a ring R, with unity,* $(xy)^2 = x^2y^2$ *for all* $x, y \in R$ *then show that R is commutative.*

Solution: Let $x, y \in R$ be any elements

then $y + 1 \in R$ as $1 \in R$

By given condition

$(x(y + 1))^2 = x^2 (y + 1)^2$

$\Rightarrow (xy + x)^2 = x^2 (y + 1)^2$

$\Rightarrow (xy)^2 + x^2 + xyx + xxy = x^2(y^2 + 1 + 2y)$

$\Rightarrow x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$

$\Rightarrow xyx = x^2y$ ...(1)

Since (1) holds for all x, y in R, it holds for $x + 1, y$ also. Thus replacing x by $x + 1$, we get

$(x + 1)\ y(x + 1) = (x + 1)^2y$

$\Rightarrow (xy + y)\ (x + 1) = (x^2 + 1 + 2x)y$

$\Rightarrow xyx + xy + yx + y = x^2y + y + 2xy$

$\Rightarrow yx = xy$ using (1)

Hence R is commutative.

Problem 7: *Show that the ring R of real valued continuous functions on* $[0, 1]$ *has zero divisors.*

Solution: Consider the functions f and g defined on $[0, 1]$ by

$$f(x) = \frac{1}{2} - x, \qquad 0 \le x \le \frac{1}{2}$$

$$= 0, \qquad \frac{1}{2} \le x \le 1$$

and $$g(x) = 0, \qquad 0 \le x \le \frac{1}{2}$$

$$= x - \frac{1}{2}, \quad \frac{1}{2} \le x \le 1$$

then f and g are continuous functions and $f \neq 0$, $g \neq 0$

whereas $gf(x) = g(x)f(x) = 0 \cdot \left(\frac{1}{2} - x\right)$ if $0 \le x \le \frac{1}{2}$

$$= \left(x - \frac{1}{2}\right).0 = 0 \text{ if } \frac{1}{2} \le x \le 1$$

i.e., $gf(x) = 0$ for all x

i.e., $gf = 0$ but $f \neq 0$, $g \neq 0$.

Exercises

1. Show that a ring R is commutative iff
   $(a + b)^2 = a^2 + b^2 + 2ab$ for all $a, b \in R$.
2. If in a ring R, $x^2 = x$ for all x then show that $2x = 0$ and $x + y = 0 \Rightarrow x = y$.
3. If R is a ring with unity and $(ab)^2 = (ba)^2$ for all $a, b \in R$ and $2x = 0$ $\Rightarrow x = 0$ then show that R is commutative.
4. Let **R** be the set of real numbers. Show that **R**×**R** forms a field under addition and multiplication defined by
   $(a, b) + (c, d) = (a + c, b + d)$
   $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.
5. Let R be a commutative ring with unity. Show that
   (*i*) a is a unit iff a^{-1} is a unit.
   (*ii*) a, b are units iff ab is a unit.
6. Show that set of all units in a commutative ring with unity forms an abelian group under multiplication.
7. Give an example of a non commutative ring R in which $(xy)^2 = x^2y^2$ for all $x, y \in R$.
8. If $< R, +, \cdot >$ be a system satisfying all conditions in the definition of a ring with unity except $a + b = b + a$, then show that this condition is also satisfied.
9. Show that if $1 - ab$ is invertible in a ring with 1 then so is $1 - ba$.
10. Show that a finite commutative ring R without zero divisors has unity. (See theorem 4 page 318).

Subrings

Definition: A non empty subset S of a ring R is said to be a *subring* of R if S forms a ring under the binary compositions of R.

The ring $< \mathbf{Z}, +, \cdot >$ of integers is a subring of the ring $< \mathbf{R}, +, \cdot >$ of real numbers.

If R is a ring then $\{0\}$ and R are always subrings of R, called *trivial* subrings of R.

It is obvious that a subring of an integral domain will be an integral domain.

In practice it would be difficult and lengthy to check all axioms in the definition of a ring to find out whether a subset is a subring or not. The following theorem would make the job rather easy.

Theorem 5: *A non empty subset S of a ring R is a subring of R iff $a, b \in S \Rightarrow ab, a - b \in S$.*

Proof: Let S be a subring of R

then $a, b \in S \Rightarrow ab \in S$ (closure)

$a, b \in S \Rightarrow a - b \in S$

as $< S, + >$ is a subgroup of $< R, + >$.

Conversely, since $a, b \in S \Rightarrow a - b \in S$, we find $< S, + >$ forms a subgroup of $< R, + >$. Again for any $a, b \in S$, since $S \subseteq R$

$a, b \in R$

$\Rightarrow a + b = b + a$

and so we find S is abelian.

By a similar argument, we find that multiplicative associativity and distributivity hold in S.

In other words, S satisfies all the axioms in the definition of a ring.

Hence S is a subring of R.

Definition: A non empty subset S of a field F is called a *subfield*, if S forms a field under the operations in F. Similarly, we can define a *subdivision ring* of a division ring.

One can prove that S will be a subfield of F iff $a, b \in S, b \neq 0 \Rightarrow a - b, ab^{-1} \in S$.

We may also notice here that a subfield always contains at least two elements, namely 0 and 1 of the field. (Recall a subgroup contains identity of the group and a subfield is a subgroup of the field under both the compositions).

Sum of Two Subrings

Definition: Let S and T be two subrings of a ring R. We define

$$S + T = \{s + t \mid s \in S, t \in T\}$$

then clearly $S + T$ is a non void subset of R. Indeed $0 = 0 + 0 \in S + T$.

But our enthusiasm of defining the sum ends here when we find that *sum of two subrings may not be a subring*.

Take for instance the ring M of 2×2 matrices over integers.

Let S = set of all matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ a, b integers, and

T = set of all matrices of the type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$, x an integer.

Then S and T are subrings of M, (an easy exercise for the reader).

$S + T$ would have members of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$

i.e., matrices of the type $\begin{bmatrix} a & c \\ b & 0 \end{bmatrix}$

That $S + T$ does not form a subring follows from the fact that closure w.r.t. multiplication does not hold, as

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S + T.$$

Definition: Let S be a subset of a ring R, then the smallest subring of R containing S is called the *subring generated* by S.

Since intersection of subrings is a subring (see exercises) it is clear that the subring generated by a subset S of R will be the intersection of all subrings of R, containing S. We denote it by $< S >$. Clearly then $< S > = \{0\}$ if $S = \varphi$. One can show that $< S > = \{\Sigma n_i x_1 x_2 \ldots x_n \mid n_i \in \mathbf{Z},\ x_i \in S\}$ finite.

In particular if $x \in R$ be an element then the subring generated by x is the smallest subring of R containing x. It will be the intersection of all subrings of R, containing x. This is denoted by $< k >$. One can show that $< x > = \left\{ \sum_{i=0}^{\text{finite}} m_i x^i \mid m_i \in \mathbf{Z} \right\}$

Problem 8: *Show that* $T = \left\{ \frac{m}{2^n} \mid m, n \in \mathbf{Z}, n > 0 \right\}$ *is the smallest subring of* $\mathbf{Q}$ *containing 1/2.*

Solution: T is easily seen to be a subring. Take $m = 1$, $n = 1$, then $\frac{1}{2} \in T$.

Let S be any subring of $\mathbf{Q}$ s.t., $\frac{1}{2} \in S$

Then $\left(\frac{1}{2}\right)^n \in S \quad \forall$ +ve integers n

So $\frac{1}{2} \in S$

Again $\frac{1}{2} \in S \Rightarrow \frac{1}{2} + \frac{1}{2} = 1 \in S$

i.e., $m \in S \qquad \forall\ m \in \mathbf{Z}$

Now $\frac{1}{2^n} \in S$, $m \in S \quad \forall\ m, n \in \mathbf{Z}$, $n > 0$ and

so $\frac{m}{2^n} \in S$ i.e., $S \subseteq T$.

Definition: Let R be a ring, the set

$$Z(R) = \{x \in R \mid xr = rx \text{ for all } r \in R\}$$

is called *centre* of the ring.

It is an easy exercise to show that $Z(R)$ is a subring of R.

Problem 9: *Find centre of the quaternion ring D.*

Solution: Let $a + bi + cj + dk \in Z(D)$ be any element. Then it commutes with all elements of D. Thus

$$(a + bi + cj + dk)(0 + 1i + 0j + 0k) = (0 + 1i + 0j + 0k)(a + bi + cj + dk)$$

$$\Rightarrow 0 + 0i + 0j + ck = 0 + 0i + dj + 0k$$

or $$0 + 0i + ij + 0k = 0 + 0i + 0j - dk$$

or $$0 + 0i + ij + dk = 0 + 0i + 0j + 0k$$

Therefore, $a + bi + cj + dk = a + bi + 0j + 0k$

Now $(a + bi + 0j + 0k)(0 + 0i + ij + 0k) = (0 + 1i + 1j + 0k)(a + bi + 0j + 0k)$

$\Rightarrow 0 + 0i + aj + bk = 0 + 0i + aj - bk$

which gives $b = -b$ i.e., $b = 0$

Thus $a + bi + cj + dk = a + 0i + 0j + 0k$

which shows that $Z(D) \subseteq \{a + 0i + 0j + 0k \mid a \text{ is real number}\}$

Also $a + 0i + 0j + 0k$ commutes with every element of D as a is a real number.

Hence $Z(D) = \{a + 0i + 0j + 0k \mid a \text{ is real number}\}$

or that $Z(D) = \{(a, 0, 0, 0) \mid a \in \mathbf{R}\}$

Later we show Z(D) is isomorphic to the field **R** (See under ring isomorphisms)

Problem 10: *If R is a division ring then show that the centre Z(R) of R is a field.*

Solution: $Z(R)$ is a ring (as it is a subring).

$Z(R)$ is commutative by its definition.

$Z(R)$ has unity as $1 \,.\, x = x \,.\, 1 = x$ for all $x \in R$.

Thus we need show that every non zero element of $Z(R)$ has multiplicative inverse (in $Z(R)$).

Let $x \in Z(R)$ be any non zero element.

Then $x \in R$ and since R is a division ring, $x^{-1} \in R$.

Let $y \in R$ be any non zero element, then $y^{-1} \in R$. Now

$$x^{-1}y = (y^{-1}\, x)^{-1}$$

$$= (xy^{-1})^{-1} = yx^{-1}$$

$\Rightarrow x^{-1}$ commutes with all non zero elements of R.

Again as $x^{-1} \,.\, 0 = 0 \,.\, x^{-1} = 0$

we find $x^{-1}\, r = r.\, x^{-1}$ for all $r \in R$

$\Rightarrow x^{-1} \in Z(R)$

Showing that $Z(R)$ is a field.

Example 15: The ring R of 2×2 matrices over integers is a non commutative ring, whereas its centre $Z(R)$ will be a non zero commutative subring.

Problem 11: *If in a ring R, the equation ax = b for all a, b* ($a \neq 0$) *has a solution then show that R is a division ring.*

Solution: We first show that R has no zero divisors.

Suppose $ab = 0,\ a \neq 0,\ b \neq 0$

as $a \neq 0$, $ax = a$ has a solution, say $x = e_1$.

then $ae_1 = a$.

Again $bx = e_1$ has a solution, let $x = e_2$ be a solution of this, then $be_2 = e_1$,

Now $ab = 0 \Rightarrow (ab)e_2 = 0.\ e_2 = 0$

$\Rightarrow a(be_2) = 0$

$\Rightarrow ae_1 = 0$

$\Rightarrow a = 0$, but $a \neq 0$

Hence R is without zero divisors.

Now for any $a \neq 0$

$ax = a$ has a solution,

Let $x = e$ be a solution then $ae = a$

$\Rightarrow aex = ax$ for all x

$\Rightarrow a(ex - x) = 0$ for all x

But $a \neq 0 \Rightarrow ex - x = 0$ for all x

or that e is left identity.

Again, $(xe - x)e = xee - xe = x(ee) - xe$

$= xe - xe$ (as e is left identity)

$= 0$

But $e \neq 0$, thus $xe - x = 0$ or $xe = x$ for all x

i.e., e is right identity.

Now equation $ax = e$ has a solution for all $a \neq 0 \Rightarrow \exists\ b$ s.t., $ab = e$.

Hence a has right inverse. Since right identity also exists, $< R, . >$ forms a group or that R is a division ring.

Problem 12: *Show that a field F with 8 elements has no non trivial subfield, i.e., the only subfields of F are {0, 1} and F.*

Solution: We have $o(F) = 8$. Let $F^* = F - \{0\}$ then $o(F^*) = 7$ and $< F^*, . >$ forms a group. Since F^* is a group of prime order, it will be cyclic. Thus for each divisor of $o(F^*)$, there exists a unique subgroup of that order (See theorem 23 on page 85). As 7 is prime, $\exists$ only two subgroups H and K of $< F^*, . >$ with orders 1 and 7. Then $H \cup \{o\}$, $K \cup \{o\}$ will be subfields of F and will have orders 2 and 8, i.e., the subfields $\{0,1\}$ and F. Note as a subfield has to be a subgroup, there will be only two subfields.

Problem 13: *Let R be the ring of* 3×3 *matrices over reals. Show that*

$S = \left\{ \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} | x \text{ real} \right\}$ *is a subring of R and has unity different from unity of R.*

Solution: It is easy to check that S is a subring of R. Indeed

$$\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} \begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix} = \begin{bmatrix} 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \end{bmatrix}$$

which belongs to S.

Again since $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} = \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}$ we find

S has unity $\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$ which is different form unity $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ of R.

Remark: In continuation to the above problem we make the following observations:

(a) $< \mathbf{Z}, +, . >$ has unity 1, but its subring $< \mathbf{E}, +, . >$ of even integers has no unity.

(b) $< \mathbf{Z}, +, . >$ has same unity 1 as that of its *parent* ring $< \mathbf{Q}, +, . >$.

(c) Finally, we notice we can have a ring without unity which has a subring with unity.

Take for instance, the ring $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | a, b \in \mathbf{Z} \right\}$.

Now if $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ is unity of this ring, then

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & a \\ 0 & 0 \end{bmatrix} \text{ should be } \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

i.e., $a = 1$

Also $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ should be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ *i.e.*, $a = 1 = b$

Therefore, if R has unity then it must be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

But $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Hence R has no unity.

It is easy to check that $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbf{Z} \right\}$ is a subring of R and has unity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Problem 14: *Show that* (*i*) *Any ring of prime order is commutative*. (*ii*)*A ring of order* p^2, (*p a prime*) *may not be commutative*. (*iii*)*Smallest non commutative ring is of order* 4. (*iv*)*A ring with unity of order* p^2, (*p a prime*) *is commutative*.

Solution: (*i*) Let R be a ring of prime order p. Then $< R, + >$ is a cyclic group. Let $< R, + > = < a >$, then $o(a) = o(R) = p$. Let $x, y \in R$ be any elements, then $x = na$, $y = ma$ for some integers n, m.

Now $xy = (na)(ma) = nma^2 = mna^2 = (ma)(na) = yx$. Hence R is commutative.

(*ii*) Let R be the set of 2×2 matrices $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ over $\mathbf{Z}_2$ with second row having zero entries. Then R is a ring under matrix addition and matrix multiplication.

Since $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, we find R is non commutative and also it has $4 = 2^2$ elements.

(*iii*) Ring of order 1 being the zero ring is commutative. Rings of order 2 and 3 will be commutative by part (*i*). Thus, in view of part (*ii*), we find the smallest non commutative ring has order 4.

(*iv*) Let R be a ring with unity and be of order p^2. If $< R, + >$ is a cyclic group then R is commutative (part (*i*)). If $<R, + >$ is not cyclic then every non-zero element of $< R, + >$ is of prime order p. [order of an element divides order of the group and if order of an element equals order of the group then the group is cyclic].

Let e denote unity of R, then $o(e) = p$ (under addition)

Let $S = < e >$ be the subring of R, of order p.

Then $S = \{e, 2e, ..., (p-1)e, pe = 0\}$, $o(S) = p$

Since $o(R) = p^2$, $\exists\ a \in R$, s.t., $a \notin S$ and $o(a) = p$ under addition.

Let $T = \{a, 2a, ..., (p-1)a, pa = 0\}$ be the subring of R of order p. Every non zero element in T is of order p under addition.

If na belonging to T, $(n \neq 0)$ also belongs to S then the subring $< na > = T$ under addition is contained in S.

But $o(T) = o(S)$ and thus $< na > = T = S$.

i.e., $a \in S$, a contradiction.

Hence $S \cap T = \{0\}$.

Also $o(S + T) = \dfrac{o(S) \,.\, o(T)}{o(S \cap T)} = p^2 = o(R)$,

Thus $R = S + T$

Let $x, y \in R$, then

$x = ne + ma$, $y = re + sa$, where n, m, r, s are integers

Now $xy = (nr)e + (ns)a + (mr)a + msa^2$

$= yx$

Showing that R is commutative.

Characteristic of a Ring

Definition: Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then R is said to have *finite characteristic* and also the smallest such positive integer is called the characteristic of R.

Thus it is the smallest positive integer n such that $\underbrace{1 + 1 + \ldots\ldots + 1}_{n \text{ times}} = 0$ in R.

If no such positive integer exists then R is said to have *characteristic zero* (or infinity).

Characteristic of R is denoted by char R or ch R.

Example 16: (*a*) Rings of integers, even integers, rationals, reals, complex numbers are all of ch zero.

(*b*) Consider $R = \{0, 1\}$ mod 2

then ch $R = 2$ as

$2 \,.\, 1 = 1 \oplus 1 = 0$

$2 \,.\, 0 = 0 \oplus 0 = 0$

thus 2 is the least +ve integer s.t., $2a = 0$ for all $a \in R$.

Note $1 \,.\, 1 = 1 \neq 0$

(*c*) If R is a (non zero) finite ring, then ch $R \neq 0$. Let $o(R) = m > 1$. Since $\langle R, + \rangle$ is a group, $ma = 0 \;\forall\; a \in R$ (see cor.on page 83). Hence ch $R \neq 0$

Notice ch $R = 1$ if $R = \{0\}$.

(*d*) ch $\mathbf{Z}_n = n$

By (*c*) ch $\mathbf{Z}_n \neq 0$. Let ch $\mathbf{Z}_n = m$

Then $ma = 0 \;\forall\; a \in \mathbf{Z}_n$

i.e., $m \,.\, 1 = 0$

i.e., $\underbrace{1 \oplus 1 \oplus \ldots\ldots \oplus 1}_{(m \text{ times})} = 0$

or that $m = nq \Rightarrow n \mid m \Rightarrow m \geq n$

But $na = 0 \;\forall\; a \in \mathbf{Z}_n$ as $o(\mathbf{Z}_n) = n$ (cor. on page 83)

and thus ch $\mathbf{Z}_n \leq n$

i.e., $m \leq n$ giving $m = n$.

(*e*) Ring M in example 9 on page 314 will have characteristic 2. See exercise 17 on page 338 also.

Theorem 6: *Let R be a ring with unity. If 1 is of additive order n then ch $R = n$. If 1 is of additive order infinity then ch R is 0.*

Proof: Let additive order of 1 be n. (By this, we mean, order of 1 in the group $(R, +)$ is n). Then $n \cdot 1 = 0$ and n is such least +ve integer.

Now for any $x \in R$

$$nx = x + x + \ldots\ldots + x = 1 \cdot x + 1 \cdot x + \ldots + 1 \cdot x$$
$$= (1 + 1 + \ldots\ldots + 1)x = 0.x = 0$$

Showing that ch $R = n$.

If 1 has infinite order under addition then $\exists$ no. n s.t., $n \cdot 1 = 0$ and thus

ch $R = 0$.

Remark: The above result can also be stated as

If R is a ring with unity then R has ch $n > 0$ iff n is the smallest positive integer s.t., $n \cdot 1 = 0$.

Theorem 7: *If D is an integral domain, then characteristic of D is either zero or a prime number.*

Proof: If ch D is zero, we have nothing to prove. Suppose D has finite characteristic then $\exists$ a +ve integer m, s.t., $ma = 0$ for all $a \in D$.

Let k be such least +ve integer then ch $D = k$. We show k is a prime.

Suppose k is not a prime, then we can write

$$k = rs, \quad 1 < r, s < k$$

Now $ka = 0$ for all $a \in D$

$$\Rightarrow (rs)\, a^2 = 0 \quad \forall \ a \in D$$
$$\Rightarrow a^2 + a^2 + \ldots\ldots + a^2 = 0 \quad (rs \text{ times})$$
$$\Rightarrow (\underbrace{a + a + \ldots\ldots + a}_{r \text{ times}})(\underbrace{a + a + \ldots\ldots + a}_{s \text{ times}}) = 0$$
$$\Rightarrow (ra)\,(sa) = 0 \ \forall \ a \in D$$
$$\Rightarrow ra = 0 \text{ or } sa = 0 \ \forall \ a \in D \quad \text{(See next problem)}$$

In either case it will be a contradiction as $r, s < k$, and k is the least +ve integer s.t., $ka = 0$.

Hence k is a prime.

Problem 15: *If D is an integral domain and if $na = 0$ for some $0 \neq a \in D$ and some integer $n \neq 0$ then show that the characteristic of D is finite.*

Solution: Since $na = 0$

$$(na)x = 0 \text{ for all } x \in D$$

$\Rightarrow (a + a + ... + a)x = 0$

$\Rightarrow ax + ax + ... + ax = 0$ (n times)

$\Rightarrow a(x + x + ... + x) = 0$ for all $x \in D$

$\Rightarrow x + x + ...+ x = 0$ for all $x \in D$ as $a \neq 0$

$\Rightarrow nx = 0$ for all $x \in D$, $n \neq 0$

$\Rightarrow$ ch D is finite.

Remark: In the above situation if ch $D = k$, then $k \mid n$. Since ch $D = k$, $kx = 0$ $\forall\, x \in D$

By division algorithm,

$n = kq + r, \quad 0 \leq r < k$

$\Rightarrow na = kqa + ra$

$\Rightarrow 0 = 0 + ra, \quad 0 \leq r < k$

$\Rightarrow r = 0$ as $a \neq 0$. Hence $n = kq \Rightarrow k \mid n$.

We can thus say that *if R is a finite ring of order n then ch R divides n*, as $o<R, +> = n$ means $na = 0$. ($a^{o(G)} = e$).

Problem 16: *Let R be a finite* (*non zero*) *integral domain, then* $o(R) = p^n$, *where p is a prime*.

Solution: ch R is finite and will be prime, follows by example 16(c) and theorem 7 above.

Let ch $R = p$, a prime.

Let q be a prime dividing $o(R)$. Since $< R, + >$ is a group, by Cauchy's theorem, $\exists\, a \in R$, s.t. $o(a) = q$.

Also ch $R = p \Rightarrow pa = 0$

$\Rightarrow o(a) \mid p$

$\Rightarrow q \mid p$

$\Rightarrow q = p$ as p, q are primes.

Thus p is the only prime divinding $o(R)$

$\Rightarrow o(R) = p^n$.

Cor.: (*i*) Order of a finite field is p^n for some prime p.

See also therorem 60 on page 752.

(*ii*) There cannot be an integral domain with order that is divisible by two or more distinct primes (*i.e.*, we cannot have an integral domain with order n where n can be expressed as product of more than one prime). So we cannot have integral domains with 6 or 10 or 12 etc. elements.

Problem 17: Show that the additive and multiplicative groups of a field are not isomorphic.

Solution: Let $< F, + . >$ be a field and let $F^* = F - \{0\}$ then $< F, + >$ and $< F^*, . >$ are groups. We show they are not isomorphic.

Case (*i*) Let F be finite of say, order n.

Then $o(F^*) = n - 1$, thus they cannot be isomorphic.

Case (*ii*) Suppose F is infinite and ch $F \neq 2$.

Suppose $\varphi : F^* \to F$ is a group isomorphism.

Let $\varphi(-1) = a$

If $a = 0$, then $\varphi(-1) = 0 = \varphi(1)$

$\Rightarrow 1 = -1$ as φ is 1-1

which is not true as ch $F \neq 2$

So $a \neq 0$

Since $\varphi(1) = 0$

$\varphi((-1)(-1)) = 0$

$\Rightarrow \varphi(-1) + \varphi(-1) = 0 \Rightarrow 2a = 0$

or $(1 + 1)a = 0$, but $1 + 1 \neq 0$, as ch $F \neq 2$

Thus $a = 0$, a contradiction

Hence there is no isomorphism from $F^* \to F$.

Case (*iii*) F is infinite and ch $F = 2$

Let $\alpha \in F^*$, $\alpha \neq 1$. Let $\varphi : F^* \to F$ be a group isomorphism.

Suppose $\varphi(\alpha) = a$, then $a \neq 0$ as $a = 0 \Rightarrow \varphi(\alpha) = 0 = \varphi(1)$ or that $\alpha = 1$

which is not true

Now $\varphi(\alpha \cdot \alpha) = \varphi(\alpha) + \varphi(d) = 2a = 0$ as ch $F = 2$

So $\varphi(\alpha^2) = 0 \Rightarrow \alpha^2 \in \text{Ker } \varphi = \{1\}$ as φ is 1-1

$\Rightarrow \alpha^2 = 1$.

Now $(\alpha - 1)^2 = \alpha^2 + 1 - 2\alpha = \alpha^2 + 1$ as $2\alpha = 0$, $1 + 1 = 0$, as ch $F = 2$

$= 1 + 1 = 0$

or that $\alpha - 1 = 0 \Rightarrow \alpha = 1$, not true

Hence there is no isomorphism between F and F^*.

Remark: A finite integral domain has finite ch. Whereas an infinite integral domain may have finite or zero ch. Similarly we can have infinite fields with finite characteristic. See example 8, page 425 under polynomial rings.

Problem 18: *Let R be an integral domain of prime characteristic p, show that*

$$(a + b)^p = a^p + b^p \ \forall\ a, b \in R$$

Show by an example that we can have a ring of characteristic 4 where

$$(a + b)^4 \neq a^4 + b^4.$$

Solution: Since ch $R = p$, $px = 0\ \forall\ x \in R$ ...(1)

Now $(a + b)^p = a^p + p_{C_1} a^{p-1}b + p_{C_2} a^{p-2}b^2 + \ldots + p_{C_p} b^p$

(as R is commutative)

We can prove that $p \mid p_{C_r}$ $\forall\ r,\ 1 \leq r \leq p - 1$

(See example 3 an page 357)

Thus each p_{C_r} $(1 \le r \le p-1)$ is a multiple of p.

Since $a^{p-1}b$, $a^{p-2}b^2$, ...are all in R, we find

$^pC_1a^{p-1}b$, $^pC_2a^{p-2}b^2$, ... are all are zero, using (1)

Hence $(a+b)^p = a^p + b^p$.

Consider now the ring $\mathbf{Z}_4 = \{0,1,2,3\}$ mod 4 then ch $\mathbf{Z}_4 = 4$.

Here $(1 \oplus 3)^4 = 0$ whereas

$1^4 \oplus 3^4 = 1 \oplus 1 = 2$.

Remark: See Problem 1 on page 699 also.

Problem 19: *Let R be a ring with unity e. Suppose non unit elements of R form a subgroup of R under addition. Show that either ch R is zero or a power of a prime.*

Solution: If ch R is zero, we have nothing to prove. Let ch $R = n \neq 0$.

Suppose p and q are two distinct primes dividing n. Let $n = mpq$

Since ch $R = n$, $pe \neq 0$, $qe \neq 0$, $me \neq 0$ as $p, q, m < n$

Now $0 = ne = (me)(pe)(qe)$

If pe is a unit in R, then $0 = (mq)e$

which is not true as $mq < n$

Thus pe is non unit. Similarly, qe is non unit.

Let S be the subgroup of non unit elements of R under addition, then $pe, qe \in S$

Since p, q are coprime , $\exists$ integers r and s such that

$$1 = pr + qs$$

$$\Rightarrow e = r(pe) + s(qe) \in S$$

as $pe, qe \in S \Rightarrow r(pe) + s(qe) \in S$

Thus $e \in S \Rightarrow e$ is non unit, which is not true. Hence n is a power of a single prime.

Remarks: (*i*) If F is a field then 0 is the only non unit element of F and also $\{0\}$ is a subgroup of F under addition. Hence by above result ch F is zero or p^n for some prime p.

(*ii*) Consider the ring $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ mod 4

Here 0, 2 are non units and $\{0, 2\}$ forms a subgroup under addition and we've seen earlier ch $\mathbf{Z}_4 = 4 = 2^2$ (power of a single prime).

See exercises ahead.

Problem 20: *Let F be a field of characteristic p show that the set* $S = \{oe = 0, e, 2e, 3e, ...(p-1)e\}$ *forms a subfield of F, where e denotes the unity of F.*

Solution: $S \neq \varphi$ as $0 \in S$

Let $ne, me \in S$ be any two members and let $n + m = pq + r$, $0 \le r < p$

Then $ne + me = (n+m)e = (pq+r)e = re \in S$ as $pe = 0$

Also $-me = (p-m)e \in S$

Again, $(ne)(me) = (nm)e = se \in S$

where $nm = pq + s,\ 0 \le s < p$

Again, let $ne \in S$ be any non zero element.

Then $(n, p) = 1 \Rightarrow pu + nv = 1$ for some integers u, v

Suppose $v = pq + t,\ 0 \le t < p$

Then $e = (pu)e + (nv)e = (nv)e = (ne)(ve), \quad ve \in S$

$\Rightarrow (ne)^{-1} = ve \in S$

Hence S is a subfield of F.

Definitions: An element e in a ring R is called *idempotent* if $e^2 = e$.

An element $a \in R$ is called *nilpotent* if $a^n = 0$ for some integer n.

If R is a ring with unity, then 0 and 1 are idempotent elements. Also 0 is nilpotent element of R.

Problem 21: *A non zero idempotent cannot be nilpotent.*

Solution: Let x be non zero idempotent, then $x^2 = x$.

If x is also nilpotent then $\exists$ integer $n \ge 1$ s.t.,

$x^n = 0$

But $x^2 = x \Rightarrow x^3 = x^2 = x$

$\Rightarrow x^4 = x^2 = x$

$\Rightarrow x^n = x \Rightarrow x = 0$ a contradiction.

Problem 22: *In an integral domain R* (*with unity*) *the only idempotents are the zero and unity.*

Solution: Let $x \in R$ be any idempotent

Then $x^2 = x \Rightarrow x^2 - x = 0$

$\Rightarrow x(x - 1) = 0$

$\Rightarrow x = 0$ or $x = 1$ as R is an integral domain.

Remark: A field which is a Boolean ring has only two elements.

Problem 23: *If R is a ring with no non zero nilpotent elements then show that for any idempotent e, ex = xe for all x ∈ R and thus e ∈ Z(R).*

Solution: e idempotent $\Rightarrow e^2 = e$

Let $x \in R$ be any element, then

$(exe - ex)^2 = exeexe - exeex - exexe + exex$

$= 0$ (using $e^2 = e$)

$\Rightarrow exe - ex$ is nilpotent.

By given condition, $exe - ex = 0 \Rightarrow exe = ex$

Similarly, we get $exe = xe$

Hence $ex = xe$.

Problem 24: *Find all the idempotent and nilpotent elements of the ring* $\mathbf{Z}_4$.

Solution: $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ mod 4.

Since $0 \otimes 0 = 0$, $1 \otimes 1 = 1$, $2 \otimes 2 = 0$, $3 \otimes 3 = 1$ we find 0 and 1 are the idempotents.

Again since $2^2 = 2 \otimes 2 = 0$, 2 is nilpotent.

0, of course, is nilpotent, 3 is not nilpotent as $3^3 = 3 \otimes 3 \otimes 3 = 3$,

$3^4 = 3 \otimes 3 \otimes 3 \otimes 3 = 1$, $3^5 = 3$, it is clear that no power of 3 will give zero.

Remark: If $a^k = a$ for some $k \geq 2$, $a \neq 0$ then a cannot be nilpotent as

$$a^{k^2} = (a^k)^k = a^k = a$$

$$a^{k^3} = (a^k)^k = a^k = a$$

.....

$$\therefore \quad a^{k^n} = a \quad \forall n \in N \qquad \ldots(1)$$

If a is nilpotent, then $\exists$ some $m \in N$, s.t., $a^m = 0$

$$\therefore \quad a^r = 0, \quad \forall\, r \geq m \qquad \ldots(2)$$

Choose $n \in N$ s.t., $k^n \geq m$, then $a^{k^n} = 0$ by (2)

hence $a = 0$, which is not true.

Problem 25: *Let $n = p^r$, p a prime. Show that $\dfrac{\mathbf{Z}}{< n >}$ has no idempotents other than $< n >$ and $< n > + 1$.*

Solution: Let $< n > + m$ be an idempotent of $\dfrac{\mathbf{Z}}{< n >}$. Then

$$(< n > + m)^2 = < n > + m$$

$$\Rightarrow < n > + m^2 = < n > + m$$

$$\Rightarrow m^2 - m \in < n >$$

$$\Rightarrow n \mid m^2 - m = m(m-1)$$

$$\Rightarrow p^r \mid m(m-1)$$

Since g.c.d. $(m, m-1) = 1$,

$$p^r \mid m \text{ or } p^r \mid m - 1.$$

If $n = p^r \mid m$, then $< n > + < m > = < n >$

If $n = p^r \mid m - 1$, then $m - 1 = nk$

$$\Rightarrow \; < n > + m = < n > + nk + 1 = < n > + 1$$

So, zero and unity are the only idempotents of $\dfrac{\mathbf{Z}}{< n >}$ when $n = p^r$

Therefore $\mathbf{Z}_4$ has only 2 idempotents (See problem 24 on page 334). Similarly, $\mathbf{Z}_9$, $\mathbf{Z}_8$, $\mathbf{Z}_7$, $\mathbf{Z}_5$, $\mathbf{Z}_3$, $\mathbf{Z}_2$ have only 2 idempotents.

Problem 26: *Let g.c.d. $(m, n) = 1$, $m > 1$, $n > 1$. Show that $\dfrac{\mathbf{Z}}{< mn >}$ (or $\mathbf{Z}_{mn}$) has at least 4 idempotents.*

Solution: Since g.c.d. $(m, n) = 1$, there exist integers r and s such that $mr + ns = 1$

Suppose $n \mid r$. Then $nt = r \Rightarrow mnt + ns = 1$

$\Rightarrow n \mid 1 \Rightarrow n = 1$, a contradiction. So, n does not divide r.

Similarly m does not divide s.

Now $mr + ns = 1$

$\Rightarrow m^2r + mns = m$

$\Rightarrow m^2r = m(1 - ns)$

$\Rightarrow <mn> + m = < mn > + m^2r$

$\Rightarrow (< mn > + mr)^2 = < mn > + mr$

If $< mn > + mr = < mn >$

then $mr \in < mn > \Rightarrow mn \mid mr \Rightarrow n \mid r$, a contradiction.

Therefore, $< mn > + mr$ is a non zero idempotent of $\dfrac{\mathbf{Z}}{< mn >}$

If $< mn > + mr = < mn > + 1$

then $mn \mid mr - 1 \Rightarrow mr + mnt = 1 \Rightarrow m \mid 1$, a contradiction

So, $< mn > + mr$ is not a unity idempotent of $\dfrac{\mathbf{Z}}{< mn >}$

Similarly, $< mn > + ns$ is non zero, non unity idempotent of $\dfrac{\mathbf{Z}}{< mn >}$

If $< mn > + mr = < mn > + ns$,

then $mr - ns = mnu \Rightarrow m \mid ns \Rightarrow m \mid s$, a contradiciton.

Therefore, $< mn > + mr \neq < mn > + ns$

So, we have 4 idempotents of $\dfrac{\mathbf{Z}}{< mn >}$.

Problem 27: *Suppose* $\mathbf{Z}_n$ *has only 2 idempotents namely zero and unity. Show that* $n = p^r$ *for some prime* p.

Solution: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $r > 1$, where p_i's are distinct primes.

Then $n = p_1^{\alpha_1} \left(p_2^{\alpha_2} \cdots p_r^{\alpha_r} \right) = ts$, where g.c.d. $(t, s) = 1$.

By above problem, $\dfrac{\mathbf{Z}}{< n >}$ has at least four idempotents, a contradiction.

Therefore, $r = 1$

So, $n = p_1^{\alpha_1}$.

Product of Rings

Let R_1 and R_2 be two rings.

Let $R = \{(a, b) \mid a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \,.\, (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

i.e., under the usual compositions of component wise addition and multiplication. This ring is called the *direct product* of R_1 and R_2. One can similarly extend the definition to product of more than two rings. R_1 and R_2 are called the *component rings* of the direct product.

Problem 28: *If R and S are two rings, then*

$ch\ (R \times S) = 0$ *if* $ch\ R = 0$ or $ch\ S = 0$

$= k$ *where* $k = l.c.m.\ (ch\ R, \text{ch } S)$, *otherwise.*

Solution: Let ch $R = 0$ and suppose ch $(R \times S) = t \neq 0$

Then $t(a, b) = (0, 0)\ \forall\ a \in R, b \in S$

$\Rightarrow$ $(ta, tb) = (0, 0)$

$\Rightarrow$ $ta = 0 \quad \forall\ a \in R$, a contradiction as ch $R = 0$

Thus ch $(R \times S) = 0$

Similarly, if ch $S = 0$, then ch $(R \times S) = 0$

Let now ch $R = m$, ch $S = n$ and $k = \text{l.c.m.}(m, n)$

Then $k(a, b) = (ka, kb) = (0, 0) \quad \forall\ a \in R, b \in S$

as m, n divide k

Suppose $p(a, b) = (0, 0)$ then $(pa, pb) = (0, 0)$

$\Rightarrow pa = 0 = pb \Rightarrow m \mid p, n \mid p$

$\Rightarrow k \mid p \Rightarrow k \leq p \Rightarrow$ ch $(R \times S) = k$.

Problem 29: *Find characteristic of*

(*i*) $\mathbf{Z}_2 \times 2\mathbf{Z}$

(*ii*) $\mathbf{Z}_2 \times \mathbf{Z}_4$

Solution: ch $(\mathbf{Z}_2 \times 2\mathbf{Z}) = 0$ as ch $2\mathbf{Z} = 0$ and ch $(\mathbf{Z}_2 \times \mathbf{Z}_4) = \text{l.c.m}$ (ch $\mathbf{Z}_2$, ch $\mathbf{Z}_4$)

$= \text{l.c.m}\ (2, 4) = 4.$

Exercises

1. Show that intersection of two subrings (subfields) is a subring (subfield).
2. Give an example to show that union of two subrings may not be a subring. Prove that union of two subrings is a subring iff one of them is contained in the other.
3. Prove that centre of a ring is a subring.

4. Let R be a ring, $a \in R$. Define $N(a) = \{r \in R \mid ar = ra\}$.

Show that (*i*) $N(a)$, (called the normaliser of a in R) is a subring of R containing a. Prove further that centre of R is intersection of subrings $N(a)$, $\forall\, a \in R$.

(*ii*) If R is a division ring then so is $N(a)$, $\forall\, a \in R$.

5. If S be a subring of a division ring R, show that $ab = 0$ in $S \Rightarrow$ either $a = 0$ or $b = 0$.

6. Let S be a subring of a ring R with unity 1. If $1 \neq e \in S$ be such that $ea = ae = a$ for all $a \in S$ then show that e is a zero divisor in R.

7. Show that any subring of $< \mathbf{Z}, +, \cdot >$ the ring of integers is of the type $n\mathbf{Z}$, $n \in \mathbf{Z}$.

8. Let F be a finite field of order n. Show that for any non zero element a in F, $a^{n-1} = 1$. (Use $a^{o(G)} = e$ in groups).

9. Let S be a subring of a commutative ring R. For $a, b \in R$, we say a is congruent to b modulo $S[a \equiv b \pmod{S}]$ iff $a - b \in S$, $(a - b)r \in S$ for all $r \in R$. Show that this is an equivalence relation in R.

10. Let R be a commutative ring. If $a, b \in R$ are nilpotent then show that so are $a \pm b$ and ar for any $r \in R$. Give an example of a non commutative ring in which a, b are nilpotent but $a + b$ is not. (See exercise 25 on page 352).

11. Let e be idempotent in a ring R. Show that the set $eRe = \{eae \mid a \in R\}$ is a subring of R with unity e.

12. Show that a field of characteristic zero is infinite.

13. Show that ch of a (non zero) Boolean ring is 2. (See exercise 2 on page 322).

14. Show that if an element of a ring with unity has more than one right inverse then it has infinitely many.

16. Show that $S = \{0, 2, 4, 6, 8\}$ is a subring of $\mathbf{Z}_{10}$ with unity different from unity of $\mathbf{Z}_{10}$.

16. Show that an integral domain R of order p^n, p a prime, has characteristic p.

17. Let R be a ring with ch n. If M is the ring of 2×2 matrices over R then show that ch $M = n$.

18. Let R be a commutative ring with unity. Show that

(*i*) if $a \in R$ is a unit then a is not nilpotent.

(*ii*) If $x \in R$ is nilpotent then $1 + x$ is a unit.

[Hint: If $x^n = 0$, consider $(1 + x)\,(1 - x - x^2 \ldots\ . - x^{n-1})$]

(*iii*) The sum of a nilpotent element and a unit is a unit.

19. In a ring without unity, show that every idempotent is a zero divisor but not nilpotent.

20. If a finite field of ch p has q elements then show that $q = p^n$ for some n.

22. If F is any subfield of $\mathbf{R}$ then show that $\mathbf{Q} \subseteq F$, *i.e.*, the field $\mathbf{Q}$ has no proper subfield.

22. Show that characteristic of a simple ring (See Def. ahead) is 0 or a prime.

23. Let R be an integral domain. Show that R does not possess any non zero nilpotent element.

24. Let S be a subring of a ring R. Show that

(i) If ch S and ch R are finite, then ch $S \leq$ ch R

(ii) If S and R have same unity, then ch S = ch R.

25. Show that non unit elements in $\mathbf{Z}_n$ form an additive subgroup of $\mathbf{Z}_n$ if and only if n is a power of a prime.

Ideals

The notion of an ideal in a ring is parallel to the concept of normal subgroup in groups. The normal subgroups led us to the formation of quotient groups, ideals do the job when we define quotient rings. Many analogous results follow. We start with

Definition: A non empty subset I of a ring R is called a *right ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in r \Rightarrow ar \in I$.

I is called a *left ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in R \Rightarrow ra \in I$.

I is called a two sided or both sided ideal of R, if it is both left and a right ideal. In fact, if we say I is an ideal of R, it would mean, I is two sided ideal of R.

Example 17: In a ring R, $\{0\}$ and R are always both sided ideals.

Any ideal except these two is called a proper ideal (In fact, the name non trivial ideal will be more appropriate).

Example 18: Let $< \mathbf{Z}, +, \cdot >$ be the ring of integers. Then

$\mathbf{E}$ = set of even integers is an ideal of $\mathbf{Z}$

$a, b \in \mathbf{E} \Rightarrow a = 2n, b = 2m$

Thus $a - b = 2(n - m) \in \mathbf{E}$

Again, if $2n \in \mathbf{E}$, $r \in \mathbf{Z}$ then as

$(2n)r$ or $r(2n)$ are both in $\mathbf{E}$, $\mathbf{E}$ is an ideal.

Example 19: Let R = ring of 2×2 matrices over integers.

Let $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \text{ integers} \right\}$

then A is a right ideal of R as

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in A$$

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} ax+bz & ay+ba \\ 0 & 0 \end{bmatrix} \in A$$

But A is not a left ideal of R as

$$\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \in I, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$$

But $$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \notin A.$$

Example 20: In the same ring as above, one can check that $B = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \text{ integers} \right\}$ forms a left (but not a right) ideal of R.

We shall encounter many more examples of ideals in the due course. Looking at the conditions in the definition of an ideal and a subring, one feels, the two are rather closely related. In fact it is easy to see that *an ideal is always a subring*.

Let I be an ideal of a ring R. To show that I is a subring we need show that for $a, b \in I$, $ab \in I$.

Now $$a, b \in I \Rightarrow a \in I, b \in I \subseteq R$$
$$\Rightarrow ab \in I \text{ (def. of ideal)}$$

Hence I is a subring.

Example 21: A subring may not be an ideal.

We know that $< \mathbf{Z}, +, \cdot >$ is a subring of $< \mathbf{Q}, +, \cdot >$ where $\mathbf{Z}$ = integers, $\mathbf{Q}$ = rationals.

$$3 \in \mathbf{Z}, \frac{1}{5} \in \mathbf{Q}. \text{ But } 3 . \frac{1}{5} \notin \mathbf{Z}$$

Thus $\mathbf{Z}$ is not an ideal.

We have been talking about intersection and union of subgroups, subrings etc. Similar results hold in case of ideals. Reader is referred to the exercises. It would, of course, be interesting to ask a question at this point:

What can we say about intersection of a left and a right ideal? Will it be an ideal? The answer is in the negative.

If we consider the ideals in example 19, 20, we find $A \cap B$ would have members of the type $\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a, \text{an integer} \right\}$.

Since $$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin A \cap B$$

We notice $A \cap B$ is not a right ideal.

Problem 30: *Let S be a non empty subset of a ring R. Show that $r(s) = \{x \in R \mid Sx = 0\}$ and $l(s) = \{x \in R \mid xS = 0\}$ are respectively right and left ideals of R.*

Solution: $r(s) \neq \varphi$ as $0 \in r(s)$

Again, $x, y \in r(s) \Rightarrow sx = 0, sy = 0$

Now $S(x - y) = Sx - Sy = 0 - 0 = 0$

$\Rightarrow x - y \in r(s)$

Again, if $r \in R$ be any element then

$S(xr) = (Sx)r = 0 \,.\, r = 0$

$\Rightarrow xr \in r(s)$

Hence $r(s)$ is a right ideal. Similarly, $l(s)$ will form a left ideal.

$r(s)$ and $l(s)$ are called right and left *annihilators* of S, respectively.

$r(s)$ and $l(s)$ would both be ideals of R if S in an ideal. (Verify!)

Problem 31: *Let R be a ring such that every subring of R is an ideal of R. Further, $ab = 0$ in $R \Rightarrow a = 0$ or $b = 0$. Show that R is commutative.*

Solution: Let $0 \neq a \in R$ be any element.

Then $N(a) = \{x \in R \mid xa = ax\}$ is a subring of R and, therefore, an ideal of R. Let $r \in R$ be any element. Since $a \in N(a)$, $r \in R$ we find $ra \in N(a)$ (Def. of ideal)

Also then, $a(ra) = (ra)a$

and so $(ar - ra)a = 0$

$\Rightarrow$ $ar - ra = 0$ as $a \neq 0$

Thus $ar = ra \;\forall\; r \in R, \;\forall\; 0 \neq a \in R$

and as $0.r = r.0 = 0$ we find

$ar = ra \;\forall\; a, r \in R$

Hence R is commutative.

Sum of Two Ideals

Let A and B be two ideals of a ring R. We define $A + B$ to be the set $\{a + b \mid a \in A, b \in B\}$, called sum of the ideals A and B.

Theorem 8: *If A and B are two ideals of R then $A + B$ is an ideal of R, containing both A and B.*

Proof: $A + B \neq \varphi$ as $0 = 0 + 0 \in A + B$

Again, $x, y \in A + B$

$\Rightarrow x = a_1 + b_1$

$y = a_2 + b_2$ for some $a_1, a_2 \in A$; $b_1, b_2 \in B$

Since $x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

we find $x - y \in A + B$

Let $x = a + b \in A + B$, $r \in R$ be any elements then

$$xr = (a + b)r = ar + br \in A + B \quad \text{as } A, B \text{ are ideals}$$

$$rs = r(a + b) = ra + rb \in A + B$$

Thus $A + B$ is an ideal of R.

Again for any $a \in A$, since $a = a + 0 \in A + B$ and for any $b \in B$, since $b = 0 + b \in A + B$

we find $A \subseteq A + B$

$B \subseteq A + B$.

Remarks: (*i*) We can show that A is an ideal of $A + B$.

$a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ as A is an ideal of R. Again, if $a \in A$ and $s \in A + B$ be any elements then $s = a_1 + b_1$ for some $a_1 \in A$, $b_1 \in B$

also $as = a(a_1 + b_1)$

$= aa_1 + ab_1 \in A$

as $a, a_1 \in A \Rightarrow aa_1 \in A$

$a \in A, b_1 \in B \subseteq R \Rightarrow ab_1 \in A$

$\Rightarrow aa_1 + ab_1 \in A$

Similarly, $sa \in A$. Showing that A is an ideal of $A + B$.

(*ii*) If A is a left ideal and B, a right ideal of R then $A + B$ may not be an ideal of R.

Considering the same ideals as in examples 19, 20, we find

$A + B$ will have members of the type $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$

and as $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 2 & 2 \end{bmatrix} \notin A + B$

$A + B$ is not an ideal of R.

Definition: Let S be any subset of a ring R. An ideal A of R is said to be generated by S if

(*i*) $S \subseteq A$

(*ii*) for any ideal I of R, $S \subseteq I \Rightarrow A \subseteq I$.

We denote it by writing $A = < S >$ or $A = (S)$.

In fact $< S >$ will be intersection of all ideals of R that contain S, and is the smallest ideal containing S. If S is finite, we say $A = < S >$ is finitely generated.

If $S = \varphi$ then as $\{0\}$ is an ideal of R containing $S = \varphi$, $< S > \subseteq \{0\}$ and so $< S > = \{0\}$.

If $S = \{a\}$ then we denote $< S >$ by $< a >$ or (a) and this case is of special interest to us as it is used rather extensively. By definition, $a \in < a >$ and as it is an ideal, elements of the type ra, as, $r_1 as_1$, na are in $< a >$, where $r, r_1, s, s_1 \in R$ and n is an integer. Such an ideal is called a *principal ideal* generated by a. (See Page 401 also). One can verify that

(*i*) If R is a commutative ring, then

$$< S > = \{\Sigma n_i x_i + \Sigma r_j y_j \mid n_i \in \mathbf{Z},\ r_j \in R,\ x_i, y_j \in S\}$$

(*ii*) If R is commutative with unity then

$$< S > = \{\Sigma r_j y_j \mid r_j \in R,\ y_j \in S\}$$

(*iii*) If $S = \{a\}$, then

$$< a > = < S > = \{na + ra + as + xay \mid n \in \mathbf{Z},\ r, s, x, y \in R\}$$

(*iv*) Further if R has unity

$$< a > = \{\Sigma\, xay \mid x, y \in R\}$$

Summation being finite everywhere.

Theorem 9: *If A and B be two ideals of a ring R, then*

$$A + B = < A \cup B >.$$

Proof: We have already proved that $A + B$ is an ideal of R, containing A and B, thus $A + B$ is an ideal containing $A \cup B$.

Let I be any ideal of R, s.t., $A \cup B \subseteq I$

Let $x \in A + B$ be any element

Then $x = a + b$ for some $a \in A$, $b \in B$

Since $a \in A \subseteq A \cup B \subseteq I$

$b \in B \subseteq A \cup B \subseteq I$

we find $a + b \in I$ as I is an ideal

$\Rightarrow$ $x \in I$ or that $A + B \subseteq I$

which proves the theorem.

Thus $A + B$ is the smallest ideal of R, containing A and B. One can, of course, talk about sum of more than two ideals in the same manner.

Problem 32: *If $a \in R$ be an element and $I = aR = \{ar \mid r \in R\}$ where R is a commutative ring, then I is an ideal of R.*

Solution: $I \neq \varphi$ as $0 = a \,.\, 0 \in I$

$x, y \in I \Rightarrow x = ar_1,\ y = ar_2$ for some $r_1, r_2 \in R$

$\Rightarrow x - y = a(r_1 - r_2) \in I$

again if $x = ar_1 \in I$ and $r \in R$ be any elements

then $x\, r = (ar_1)\, r = a\,(r_1\, r) \in I$ shows that I is a right ideal. R being commutative, it will be both sided ideal.

Remark: If the ring is not commutative, one can show that aR is a right ideal and $Ra = \{ra \mid r \in R\}$ is a left ideal of R. (See exercises)

aR is always contained in $< a >$. If R is a commutative ring with unity then $aR = Ra = (a)$.

Let us understand the difference between aR and $< a >$ through the following example.

Example 22: Let $< \mathbf{E}, +, \cdot >$ be the ring of even integers. It is commutative ring without unity, Let $a = 4 \in \mathbf{E}$.

Then $< 4 > = \{4n + (2m)\ 4 \mid n, m \in \mathbf{Z}\}$

$= \{4n + 8m \mid n, m \in \mathbf{Z}\}$

whereas $4\mathbf{E} = \{4(2k) \mid k \in \mathbf{Z}\} = \{8k \mid k \in \mathbf{Z}\}$

We notice then, $< 4 > \neq 4\mathbf{E}$ as $4 \in < 4 >$ but $4 \notin 4\mathbf{E}$.

Problem 33: *If A is an ideal of a ring R with unity such that $1 \in A$ then show that $A = R$.*

Solution: Since $A \subseteq R$ always, all we need show is that $R \subseteq A$.

Let $r \in R$ be any element.

Since $1 \in A$ and A is an ideal

$$r = 1 \,.\, r \in A$$

$$\Rightarrow \quad R \subseteq A \text{ or that } A = R.$$

Problem 34: *Determine all the ideals of the ring of integers $< \mathbf{Z}, +, \cdot >$.*

Solution: Let I be any ideal of $< \mathbf{Z}, +, \cdot >$ then as $a, b \in I \Rightarrow a - b \in I$, we notice $< I, + >$ is a subgroup of $< \mathbf{Z}, + >$

Since $< \mathbf{Z}, + >$ is a cyclic group generated by 1, I will be a cyclic group generated by a multiple of 1, say n (see theorem 19 on page 81).

Thus any ideal of $< \mathbf{Z}, +, \cdot >$ is of the type $< n >$, i.e., multiple of some integer. Conversely it is easy to see that $< n >$ for any integer n is an ideal.

A similar result follows for subrings. See also exercise 1 on page 394.

Problem 35: *Let L be a left ideal of a ring R and let*

$$\lambda(L) = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$$

then show that $\lambda(L)$ is an ideal of R.

Solution: $\lambda(L) \neq \varphi$ as $0.a = 0$ for all $a \in L$

$$\Rightarrow\ 0 \in \lambda(L)$$

$$x, y \in \lambda(L) \Rightarrow xa = 0,\ ya = 0 \text{ for all } a \in L$$

$$\Rightarrow\ (x - y)a = xa - ya = 0 - 0 = 0 \text{ for all } a \in L$$

$$\Rightarrow\ x - y \in \lambda(L)$$

Again, if $x \in \lambda(L)$, $r \in R$ be any elements, then

$$xa = 0 \text{ for all } a \in L$$

Now $(rx)a = r(xa) = r.0 = 0$ for all $a \in L$

$$\Rightarrow\ rx \in \lambda\,(L)$$

$$\Rightarrow\ \lambda(L) \text{ is a left ideal of } R.$$

Also $(xr)a = x(ra) \quad r \in R,\ a \in L$

$= 0$ for all $a \in L \Rightarrow ra \in L$

$\Rightarrow xr \in \lambda(L)$

$\Rightarrow \lambda(L)$ is a right ideal of R.

Problem 36: *Show by means of an example that we can find $A \subseteq B \subseteq R$ where A is an ideal of B, B is an ideal of R, but A is not an ideal of R.*

Solution: Let R be the set containing matrices of the type $\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{bmatrix}$ over integers, then R forms a ring under matrix addition and multiplication.

Take $$A = \left\{ \begin{bmatrix} 0 & 0 & x \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \mid x \text{ an integer} \right\}$$

$$B = \left\{ \begin{bmatrix} 0 & 0 & u \\ 0 & 0 & v \\ 0 & 0 & 0 \end{bmatrix} \mid u, v \text{ integers} \right\}$$

It would be easy to verify that A is an ideal of B, B is an ideal of R. To see that A is not an ideal of R, we notice,

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \notin A .$$

Problem 37: *Let R be an integral domain with unity such that R has finite number of ideals. Show that R is a field.*

Solution: We show that non zero elements of R have multiplication inverse.

Let $a \in R$ be any non zero element. For any +ve integer n define

$a^nR = \{a^nr \mid r \in R\}$

then it is easy to see that a^nR is an ideal of R.

Since R has finite number of ideals

for some integers m, n, $n > m$, we have

$$a^mR = a^nR$$

Now $a^m = a^m.1 \in a^mR = a^nR$

$\Rightarrow a^m = a^nr$ for some $r \in R$

$\Rightarrow a^m(a^{n-m} r - 1) = 0$

$\Rightarrow a^m = 0$ or $a^{n-m} r = 1$ as R is an integral domain.

But $a \neq 0$, so, $a^m \neq 0$

$\Rightarrow a^{n-m} r = 1$ or that $(a^{n-m-1} r)a = 1$

Thus $a^{n-m-1} r$ is multiplicative inverse of a and hence R is a field.

Product of Two Ideals

Let A, B be two ideals of a ring R. We define the product AB of A and B by

$AB = \{\Sigma\, a_i b_i \mid a_i \in A,\ b_i \in B\}$

where summation is finite.

Theorem 10: *The product AB of any two ideals A and B of a ring R is an ideal of R.*

Proof: $AB \neq \varphi$ as $0 = 0 \,.\, 0 \in AB$

Let $x, y \in AB$ be any two members

then $x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n$

$y = a'_1b'_1 + \ldots\ldots + a'_mb'_m$

for some $a_i, a'_j \in A,\ b_i, b'_j \in B$

$x - y = (a_1b_1 + \ldots\ldots + a_nb_n) - (a'_1b'_1 + \ldots\ldots\ldots + a'_mb'_m)$

which clearly belongs to AB, as the R.H.S. can be written as

$x_1y_1 + x_2y_2 + \ldots\ldots\ldots + x_ky_k \quad (k = n + m)$

where $x_i \in A,\ y_i \in B.$

Again, for any $x = a_1b_1 + \ldots\ldots + a_nb_n \in AB$ and $r \in R$,

$rx = r(a_1b_1 + \ldots\ldots + a_nb_n)$

$= (ra_1)b_1 + (ra_2)b_2 + \ldots\ldots + (ra_n)b_n \in AB$

because $ra_i \in A$ as $a_i \in A$, $r \in R$, and A is an ideal.

Similarly $xr \in AB$

showing thereby that AB is an ideal of R.

Remarks: (*i*) Let $S = \{ab \mid a \in A.\ b \in B\}$

then $< S > = AB$.

Clearly $S \subseteq AB$ and as AB is an ideal, $< S > \subseteq AB$.

Again, $x \in AB \Rightarrow x = \Sigma a_ib_i,\ a_i \in A,\ b_i \in B$

$a_i \in A,\ b_i \in B \Rightarrow a_ib_i \in S,\ \forall\, i = 1, 2, \ldots\ldots,$

$\Rightarrow a_ib_i \in < S > \ \forall\, i$

$\Rightarrow x \in < S >$

$\Rightarrow AB \subseteq < S >$

and hence $< S > = AB$.

(*ii*) If R is a commutative ring with unity and A, B are finitely generated ideals of R then so are $A + B$ and AB. In fact if $A = < a_1, a_2, \ldots\ldots, a_n >$ and $B = < b_1, b_2, \ldots\ldots, b_s >$ then

$A + B = < a_1, a_2, \ldots., a_r, b_1, b_2, \ldots, b_s >$

$AB = < a_1b_1, \ldots., a_1b_s, \ldots\ldots, a_rb_1, \ldots\ldots, a_rb_s >$

This, however, may not be true for $A \cap B$. See exercises ahead.

The following problem gives us little more information about product of ideals.

Problem 38: *If A is a left and B is a right ideal of a ring R then show that AB is a two sided ideal of R whereas BA need not be even a one-sided ideal of R.*

Solution: That *AB* will be a two sided ideal of *R* follows by the theorem above. We show by an example that *BA* need not be even a one-sided ideal.

Take $$A = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} | a, b, \in \mathbf{Z}\right\}$$

$$B = \left\{\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} | c, d, \in \mathbf{Z}\right\}$$

in the ring *R* of 2×2 matrices over integers then as seen earlier *A* is left and *B* is a right ideal of *R*.

BA would have member of the type $\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$

i.e., of the type $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}, x \in \mathbf{Z}$

Now if we take $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in *BA* and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ in *R*

then $$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin BA$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin BA$$

Hence *BA* is neither a left nor a right ideal of *R*.

Problem 39: *If A , B, C are ideals of a ring R, s.t., $B \subseteq A$ then show that*

$$A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C).$$

Solution: Let $x \in A \cap (B + C)$ be any element

Then $x \in A$ and $x \in B + C$

$\Rightarrow x = b + c$ for some $b \in B$, $c \in C$

Now $b \in B \subseteq A$, also $b + c = x \in A$

$\Rightarrow (b + c) - b \in A$

$\Rightarrow c + b - b \in A$

$\Rightarrow c \in A$

$\Rightarrow x \in A \cap C$

i.e., $x = b + c$, $b \in B$, $c \in A \cap C$

thus $x \in B + (A \cap C)$

Hence $A \cap (B + C) \subseteq B + (A \cap C)$.

Again let $x \in B + (A \cap C)$

Then $x = b + k$ for some $b \in B$, $k \in A \cap C$

Since $b \in B$, $k \in C$

$x = b + k \in B + C$

and $b \in B \subseteq A$, $k \in A \Rightarrow b + k \in A$

$\Rightarrow x \in A$

$\Rightarrow x \in A \cap (B + C)$

or that $B + (A \cap C) \subseteq A \cap (B + C)$

which finally gives $A \cap (B + C) = B + (A \cap C)$

Also as $B \subseteq A$, $A \cap B = B$

thus $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

Remark: The above is sometimes called modular equality. See exercises also.

Definition: A ring $R \neq \{0\}$ is called a *simple ring* if R has no ideals except R and $\{0\}$.

Theorem 11: *A division ring is a simple ring.*

Proof: Let R be a division ring. Let A be any ideal of R s.t., $A \neq \{0\}$ then $\exists$ at least one $a \in A$ s.t., $a \neq 0$. R being a division ring, $a^{-1} \in R$ and $aa^{-1} = 1$.

Since $a \in A$, $a^{-1} \in R$, $aa^{-1} \in A$ (def. of ideal)

$\Rightarrow 1 \in A$

$\Rightarrow A = R$ (see problem 33)

i.e., only ideals that R can have are R and $\{0\}$ or that R is a simple ring.

Problem 40: *Let R be a ring with unity, such that R has no right ideals except* $\{0\}$ *and R. Show that R is a division ring.*

Solution: All that we need prove is that non zero elements of R form a group under multiplication.

Let $0 \neq a \in R$ be any non zero element.

Let $aR = \{ar \mid r \in R\}$

Then aR is a right ideal. See problem 32.

By given condition, then

$aR = R$

or $aR = \{0\}$

But $aR \neq \{0\}$ as $a \neq 0$ and $a = a.1 \in aR$

Hence $aR = R$.

Now $1 \in R \Rightarrow 1 \in aR \Rightarrow \exists\, b \in R$, s.t. $1 = ab \Rightarrow b$ is right inverse of a (w.r.t. multiplication). Thus $<R - \{0\}, \cdot>$ is a system in which associativity holds, right identity (unity) and right inverse exist (for every element).

i.e., $< R - \{0\}, \cdot >$ forms a group or that R is a division ring.

See Problem 43 on page 350 also.

Problem 41: *Let R be a ring having more than one element such that $aR = R$, for all $0 \neq a \in R$. Show that R is a division ring.*

Solution: We first show that $xy = 0 \Rightarrow x = 0$ or $y = 0$ in R.

So let $xy = 0$ and suppose $x \neq 0$, $y \neq 0$

Then $xR = yR = R$

Also $(xy)R = x(yR) = xR = R$

$\Rightarrow R = \{0\}$ as $xy = 0$

contradicting that R has more than one element.

Hence our assertion is proved.

Again, as $R \neq \{0\}$, $\exists\ 0 \neq a \in R$ and by given condition then $aR = R$

$\Rightarrow \exists\ e \in R$ s.t., $ae = a$ $\quad (e \neq 0$ as $a \neq 0)$

$\Rightarrow ae^2 = ae$

$\Rightarrow a(e^2 - e) = 0$

$\Rightarrow e^2 = e$ as $a \neq 0$.

We claim e is right unity of R.

If e is not right unity of R, then $\exists\ y \in R$ s.t., $ye \neq y$

But $(ye - y)e = ye^2 - ye = ye - ye = 0$

$\Rightarrow$ either $ye = y$ or $e = 0$, a contradiction

$\Rightarrow e$ is right unity of R.

Let $0 \neq a \in R$ be any element then $aR = R$

Now $e \in R$, $aR = R$.

$\Rightarrow e \in aR \Rightarrow \exists\ b \in R$, s.t., $e = ab$

or that b is right inverse of a.

$\Rightarrow$ every non zero element of R has right inverse.

Hence R is a division ring.

Problem 42: *Let R be a ring such that R and $\{0\}$ are the only right ideals of R. Show that either R is a division ring or has prime number of elements such that $ab = 0$ for all $a, b \in R$.*

Solution: Let $I = \{a \in R \mid aR = \{0\}\}$

then I is a right ideal of R (Verify).

By given condition then either $I = \{0\}$ or $I = R$.

If $I = \{0\}$ then $aR = \{0\}$ only when $a = 0$.

In other words, $aR = R$, for all $0 \neq a \in R$. (Notice aR is a right ideal).

Thus by previous problem, R is a division ring. (Note in this case R has more than one element, as if $R = \{0\}$ then $R = I$, which is the next case).

Now suppose $I = R$, then $aR = \{0\}$ for all $a \in R$

$\Rightarrow ar = 0$ for all $a, r \in R$

If S be any subgroup of $< R, + >$ then S will be a right ideal of R ($a \in S \subseteq R$, $r \in R \Rightarrow ar = 0 \in S$). By given condition R has only two right ideals R and $\{0\}$. Thus $< R, + >$ can have only two subgroups namely R and $\{0\}$.

$\Rightarrow < R, + >$ is a cyclic group of prime order (see Groups on page 87)

Thus R has prime number of elements (and as seen above $ab = 0$ for all $a, b \in R$).

Problem 43: *Show by an example that it is possible to have a ring R with unity where* $\{0\}$ *and R are the only ideals of R, but R is not a division ring.*

Solution: Let R be the ring of 2×2 matrices over **R**. Then it is not a division ring as $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $\in R$ is not invertible. We show R has no ideals except $\{0\}$ and R.

Let $\mathscr{A} \neq \{0\}$ be any ideal of R.

Since $\mathscr{A} \neq \{0\}$, $\exists\ 0 \neq A \in \mathscr{A}$. Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since $A \neq 0$, some entry in A is non zero. Let $a \neq 0$. Let E_{ij} denote the matrix in R whose (i, j)th entry is 1 and 0 elsewhere. Then

$$E_{ij}E_{jk} = E_{ik} \quad \text{and} \quad E_{ij}E_{rk} = 0 \quad \text{if } j \neq r$$

Now $$A = aE_{11} + bE_{12} + cE_{21} + dE_{22}$$

$$\therefore \quad AE_{11} = aE_{11} + cE_{21}$$

Thus $a^{-1}\ E_{11}AE_{11} = E_{11} \Rightarrow E_{11} \in < A >$

$$\Rightarrow < E_{11} > \subseteq < A >$$

Now $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E_{11} + E_{22} = E_{11} + E_{21}E_{11}E_{12} \in < E_{11} >$

So unity of R belongs to $< E_{11} > \Rightarrow < E_{11} > = R$

$$\Rightarrow R \subseteq < A >$$

$$\Rightarrow < A > = R$$

and so $R = < A > \subseteq \mathscr{A}$ as $A \in \mathscr{A}$

or that $\mathscr{A} = R$

Hence R is the required ring.

We thus realise that a simple ring with unity may not be a division ring, the converse, of course, being true.

Exercises

1. Show that intersection of two ideals in an ideal.
2. Give an example to show that union of two ideals may not be an ideal.
3. Prove that union of two ideals is an ideal iff one of them is contained in the other.
4. If an ideal is contained in union of two ideals then show that it is wholly contained in one of them.

5. Show that a ring cannot be expressed as a union of two proper ideals, but it is possible to express it as a union of three proper ideals.

6. Let R be the ring of 2×2 matrices over integers. If $a = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in R$, then show that aR is not a left ideal of R.

7. If A is an ideal of a ring R, let

$$[R : A] = \{x \in R \mid rx \in A \text{ for all } r \in R\}$$

Show that $[R : A]$ is an ideal of R, containing A.

8. Let R be a non commutative ring with unity. Show that $Z(R)$, the centre of R is not an ideal of R. [Hint: $Z(R)$ is properly contained in R].

9. If A, B, C are three ideals of a ring R then show that

$$A(BC) = (AB)C.$$

10. If A, B be two ideals of a ring R then show that $AB \subseteq A \cap B$. Give an example to show that $\exists$ ideals A, B s.t., $AB \neq A \cap B$.

11. If A, B, C are ideals of a ring R, then show that

(*i*) $A(B + C) = AB + AC$.

(*ii*) $(A + C)(B + C) \subseteq AB + C$.

(*iii*) $(A \cap B)(A + B) \subseteq AB$.

12. If A, B are two ideals of a ring R s.t., $A \cap B = \{0\}$ then the sum $A + B$ is called direct sum of A and B and is denoted by $A \oplus B$. Show that each element of $A \oplus B$ is uniquely expressible as $a + b$ for $a \in A$, $b \in B$.

13. If F is a field, prove that its only ideals are $\{0\}$ and F.

14. If R be a commutative ring with unity whose only ideals are $\{0\}$ and R, then show that R is a field. (See problem 40).

15. Show that if an ideal A of a ring R with unity contains a unit of R then $A = R$.

16. Let A, B be two subrings of a ring R such that for all $a \in A$, $b \in B$, ab, $ba \in A$ then show that

(*i*) $A + B$ is a subring of R.

(*ii*) A is an ideal of $A + B$.

(*iii*) $A \cap B$ is an ideal of B.

17. Show that $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \text{ rationals} \right\}$ forms a simple ring under matrix operations.

18. Let R be a ring with unity and A be any proper ideal of R. Show that no element of A can have a multiplicative inverse.

19. Show by an example that it is possible to find ideals A, B, C, such that

$$A \cap (B + C) \neq (A \cap B) + (A \cap C).$$

20. Let $S = \{a + ib \mid a, b \in \mathbf{Z}, b \text{ even}\}$. Show that S forms a subring of $\mathbf{Z}[i]$ but not an ideal of $\mathbf{Z}[i]$.

21. Let R be the ring of 2×2 matrices over integers. Show that the set S of matrices of the type $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ over integers is a subring of R but is neither a left nor a right ideal of R.

22. Let R be a commutativering and let A, B be ideals of R. Show that $\sqrt{A} = \{x \in R \mid x^n \in A \text{ for some +ve integer } n\}$ is an ideal of R such that

(*i*) $A \subseteq \sqrt{A}$ (*ii*) $\sqrt{\sqrt{A}} = \sqrt{A}$

(*iii*) If R has unity and $\sqrt{A} = R$ then $A = R$.

(*iv*) $\sqrt{AB} = \sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$

(*v*) $\sqrt{A+B} = \sqrt{\sqrt{A} + \sqrt{B}}$.

$\sqrt{A}$ is called nil radical of A.

23. Let $I = (2)$, $J = (12)$ be ideals of the ring $\mathbf{Z}$ of integers. Determine

(*i*) $I + J$ (*ii*) $I \cap J$

(*iii*) $I : J$ where $I : J = \{m \in \mathbf{Z} \mid mJ \subseteq I\}$ (*iv*) IJ

[Hint: If $I = (m)$, $J = (n)$ then $I + J = (d)$, $I \cap J = (l)$, $IJ = (mn)$

$(I : J) = (m/d)$ where d = g.c.d (a, b), l = l.c.m. (a, b).

(See under PIDs in chapter 9 also)

24. Let A, B be ideals of a ring R. Define $(A : B) = \{x \in R \mid xB \subseteq A\}$. Show that $(A : B)$ is an ideal of R. (It is called *quotient ideal*). Show further that

(*i*) $(A : B)B \subseteq A \subseteq (A : B)$

(*ii*) $(A : B)C = (A : BC)$

(*iii*) $((\bigcap_i A_i) : B) = \bigcap (A_i : B)$

(*iv*) $(A : \sum_i B_i) = \bigcap_i (A : B_i)$

A_i, B_i being ideals of R and $\Sigma B_i = \{x_1 + x_2 + \ldots\ldots + x_n \mid x_i \in B_i, n = \text{finite}\}$.

25. Let R be the ring of 2×2 matrices over integers. Show that $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are nilpotent in R but their sum is not nilpotent. Show further that the set of all nilpolent elements of R is not an ideal.

26. Let R be the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over $\mathbf{Q}$ s.t., $a = d$ and $c = 0$. Let I be the set of all such matrices for which $a = d = 0$. Show that I is an ideal of R.

27. Let R be an integral domain with unity. Let A, B be finitely generated ideals of R such that $A + B$ is a principal ideal. Then show that $A \cap B$ is finitely generated.

A Quick Look at what's been done

- A **ring** is a non-empty set R together with two binary compositions + and · (dot) where $< R, + >$ forms an abelian group, and the associative property also holds for multiplication alongwith and the product being distributive over addition. If multiplication is also commutative we say the ring is *commutative*. In addition, if there exists an element e, s.t., $ae = ea = a$, for all a in R, we say the ring has unity e.
- A commutative ring is called an integral domain if, whenever $ab = 0$ then either a is 0 or b is 0. $< \mathbf{Z}, +, \cdot >$, $\mathbf{Z}_5$ are integral domains, but $\mathbf{Z}_6$ is not an integral domain.
- A commutative ring with unity in which non-zero elements have multiplicative inverse is called a **field.**
- A field is an integral domain but converse is not true.
- $\mathbf{Z}_p$ is a field iff p is a prime.
- A non-empty subset of a ring is called a subring if it forms a ring under operations of the parent ring.
- If there exists a +ve integer n such that $na = 0$ for all a in R then R is said to have **finite characteristic** and the smallest such +ve integer is called the characteristic of R. If no such n exists we say R has **zero characteristic**.
- Order of a finite field (finite integral domain) is of the type p^n, where p is a prime.
- A ring R is called a *Boolean ring* if $a^2 = a$ for all a in R. A *Boolean ring* is always commutative.
- A non-empty subset I of a ring R is called an ideal if $a - b \in I$ and $ar, ra \in R$ for all $a, b \in I$ and $r \in R$
- Ideals are subrings but converse does not hold.
- A ring R is called **simple** if it has no ideals except R and $\{0\}$.
- Intersection, sum and product of ideals are ideals, whereas union may not be. Product of two ideals A and B is defined to be $\{\sum a_i b_i \mid a_i \in A,\ b_i \in B\}$, where summation is finite.

8

Homomorphisms and Embedding of Rings

Introduction

In this chapter we plan to discuss homomorphisms and embedding (imbedding) of rings. Moving on similar lines as in groups we have kernel of a homomorphism(which would be an ideal).We have the Fundamental Theorem of ring homomorphism, the isomorphism theorems. In groups, normal subgroups provided us with quotient groups, here ideals do the job. Towards the end we also take up the concepts of maximal and prime ideals.

Quotient Rings

Let R be a ring and let I be an ideal of R. Since $a, b \in I \Rightarrow a - b \in I$, we find I is a subgroup of $< R, + >$. Again as $< R, + >$ is abelian, I will be a normal subgroup of R and thus we can talk of $\frac{R}{I}$, the quotient group

$\frac{R}{I} = \{r + I \mid r \in R\}$ = set of all cosets of I in R (clearly left or right cosets are equal).

We know R/I forms a group under 'addition' defined by

$$(r + I) + (s + I) = (r + s) + I$$

We now define a binary composition (product) on R/I by

$$(r + I) \cdot (s + I) = rs + I$$

We show this product is well defined

Let $r + I = r' + I$ and $s + I = s' + I$

$\Rightarrow r - r' \in I$ and $s - s' \in I$

$\Rightarrow r - r' = a$ and $s - s' = b$ for some $a, b \in I$

$\Rightarrow r = r' + a, s = s' + b$

$\Rightarrow rs = (a + r')(b + s')$

$\Rightarrow rs + I = (ab + as' + r'b + r's') + I = r's' + I$

(using $x + I = I$ iff $x \in I$)

Hence the multiplication is well defined.

Since $(a + I)[(b + I)(c + I)] = (a + I)(bc + I)$
$= a(bc) + I$
$= (ab)c + I$
$= (ab + I)(c + I)$
$= [(a + I)(b + I)](c + I)$

Associativity holds w.r.t. this product.

Again, as $(a + I)[(b + I) + (c + I)] = (a + I)(b + c + I)$
$= a\ (b + c) + I$
$= (ab + ac) + I$
$= (ab + I) + (ac + I)$
$= (a + I)(b + I) + (a + I)(c + I)$

We find left distributivity holds. Similarly one can check that right distributivity also holds in R/I and hence R/I forms a ring, called the *quotient ring* or *factor ring* or *residue class ring* of R by I.

We look at it from another angle. Let R be a ring and I an ideal of R. Define, for $a, b \in R$, $a \equiv b \pmod{I}$ if $a - b \in I$. It is easy to check that this relation is an equivalence relation on R. Thus it partitions R into equivalence classes. Let for any $a \in R$, $cl(a)$ be the corresponding equivalence class of a.

Then $cl(a) = \{r + R \mid r \equiv a \pmod{I}\}$
$= \{r \in R \mid r - a \in I)\}$
$= \{r \in R \mid r - a = x \text{ for some } x \in I\}$
$= \{r \in R \mid r = a + x \text{ for some } x \in I\}$
$= \{a + x \mid x \in I\}$
$= a + I$

Thus, the quotient ring $\frac{R}{I}$ is nothing but the ring of all equivalence classes as defined above.

In fact, the binary compositions defined earlier would translate to

$$cl(a) + cl(b) = cl(a + b) \qquad a, b \in R$$
$$cl(a)\ .\ cl(b) = cl(ab)$$

It would be an interesting exercise for the reader to verify that R/I thus defined forms a ring. In fact, if R has unity 1 then $cl(1)$ will be unity of R/I.

R/I is therefore also called *quotient ring* of R modulo I.

Remarks: (*i*) It may be noticed that R/I is defined only when I is an ideal of R. If I happens to be only a subring of R then R/I may not form a ring as there the multiplication rule may not be valid. Suppose I is only a subring of R (and is not an ideal) then let $r \in R$, $a \in I$ s.t., $ar \notin I$.

Then $(a + I)(r + I) = ar + I$

gives $(0 + I)\ (r + I) = ar + I$

i.e., $0.r + I = ar + I$ or that $ar \in I$ which is not true.

(*ii*) If $I = R$ then R/I is isomorphic to the zero ring $\{0\}$ and if $I = \{0\}$ then $\frac{R}{I} \cong R$. See definition of *isomorphism* in next section.

Example 1: Let $H_4 = \{4n \mid n \in \mathbf{Z}\}$, where $< \mathbf{Z}, +, \cdot >$ is the ring of integers. Then H_4 is an ideal of $\mathbf{Z}$ and thus $\frac{\mathbf{Z}}{H_4}$ is a quotient ring and is given by

$$\frac{\mathbf{Z}}{H_4} = \{H_4, H_4 + 1, H_4 + 2, H_4 + 3\}$$

This example also shows us that quotient ring of an integral domain may not be an integral domain.

Notice $(H_4 + 2)(H_4 + 2) = H_4 + 4 = H_4 =$ zero of $\frac{\mathbf{Z}}{H_4}$ but $H_4 + 2 \neq H_4$.

On the other hand if we cosider

$$R = \{0, 2, 4, 6, 8, 10\} \bmod 12$$
$$S = \{0, 6\} \bmod 12$$

then R is not an integral domain whereas R/S is an integral domain.

We have $R/S = \{S, S + 2, S + 4\}$

Since $(S + 2)(S + 2) = S + 2$, $(S + 2)(S + 4) = S + 8 = S + 2$

and $(S + 4)(S + 4) = (S + 16) = S + 4$, we find

$\frac{R}{S}$ has no zero divisors.

Homomorphisms

Let $< R, +, \cdot >$, $< R', *, o >$ be two rings. A mapping $\theta : R \to R'$ is called a *homomorphism* if

$$\theta(a + b) = \theta(a) * \theta(b)$$
$$\theta(ab) = \theta(a) \; o \; \theta(b) \qquad a, b \in R$$

Since we prefer to use the symbols + and . for the binary compositions in a ring, we will use these symbols, even while dealing with more than one ring. In that case, the above definition *simplifies* to saying that a mapping $\theta : R \to R'$ is called a homomorphism if

$$\theta(a + b) = \theta(a) + \theta(b)$$
$$\theta(ab) = \theta(a) \cdot \theta(b)$$

One can similarly talk about *isomorphism* in rings as a one-one onto homomorphism.

Example 2: Consider the map $f : \mathbf{C} \to \mathbf{C}$, s.t.,

$$f(a + ib) = a - ib$$

then f is a homomorphism, where $\mathbf{C}$ = complex numbers,

as $f[(a + ib) + (c + id)] = f((a + c) + i(b + d))$
$= (a + c) - i(b + d)$
$= (a - ib) + (c - id)$
$= f(a + ib) + f(c + id)$

and $f[(a + ib)(c + id)] = f((ac - bd) + i(ad + bc))$
$= (ac - bd) - i(ad + bc)$
$= (a - ib)\, c - id\,(a - ib)$
$= (a - ib)(c - id)$
$= f(a + ib)\, f(c + id)$

Example 3: Let R be a commutative ring and suppose $px = 0$ for all $x \in R$, where p is a prime number. Then the mapping $f : R \to R$ defined by $f(x) = x^p$, $x \in R$ is a homomorphism.

In fact the result follows rather easily, if we can show that $p \mid p_{C_r}$, $1 \le r \le p - 1$.

Now $n = p_{C_r} = \dfrac{p!}{(p-r)!r!}$

$= \dfrac{p(p-1).....(p-r+1)(p-r)!}{(p-r)!1.2....r}$

$\Rightarrow$ $nr! = p(p-1)\ .....(p - r + 1)$

Since p divides R.H.S., it will divide $nr!$

$\Rightarrow p \mid n$ or $p \mid r!$ (whenever a prime divides product ab, it must divide at least one of a or b). But $p \nmid r!$ as 1, 2, ..., $r - 1$ are all less than p, so p cannot divide any one of them. Thus $p \nmid r!$

i.e., $p \mid n$

Now for any $x, y \in R$

$$f(x + y) = (x + y)^p = x^p + p_{C_1} x^{p-1} y + p_{C_2} x^{p-2} y^2 + ... + y^p$$

(R being commutative)

Now $p_{C_1} x^{p-1} y = px^{p-1} y = 0$ as $x^{p-1} y \in R$

$p_{C_2} x^{p-2} y^2 = (kp)\, x^{p-2} y^2 = 0$ as $p \mid p_{C_2} \Rightarrow p_{C_2} = kp$ for some k

Similarly each p_{C_r} would be some multiple of p giving that other terms are also zero.

Hence $f(x + y) = x^p + y^p = f(x) + f(y)$

Also $f(xy) = (xy)^p = x^p y^p$ (R commutative)
$= f(x) f(y)$

Thus f is a homomorphism.

Theorem 1: *If $\theta : R \to R'$ be a homomorphism, then*

(*i*) $\theta(0) = 0'$

(*ii*) $\theta(-a) = -\theta(a)$

where 0, 0′ *are zeros of the rings* R and R' *respectively.*

Proof: (*i*) Since $0 + 0 = 0$

we have $\theta(0 + 0) = \theta(0)$

$\Rightarrow \quad \theta(0) + \theta(0) = \theta(0) + 0'$

$\Rightarrow \quad \theta(0) = 0'$

(*ii*) Again, as $a + (-a) = 0$

$\theta(a + (-a)) = \theta(0)$

$\Rightarrow \quad \theta(a) + \theta(-a) = \theta(0) = 0$

$\Rightarrow \quad -\theta(a) = \theta(-a)$

Cor.: It is clear that

$$\theta(a - b) = \theta(a + (-b)) = \theta(a) - \theta(b)$$

Remark: The terminology of epimorphism, monomorphism etc. is extended to rings also in the same way as in groups.

Definition: Let $f : R \to R'$ be a homomorphism, we define *Kernel* of f by

$$\text{Ker } f = \{x \in R \mid f(x) = 0'\}$$

where $0'$ is zero of R'.

The following two theorems are easy to prove so we'll state the results without proof.

If : $R \to R'$ is a homomorphism then

Theorem 2: *Ker f is an ideal of R.*

Theorem 3: *Ker f* = (0) *iff f is one-one.*

Problem 1: *If R is a ring with unity and* $f : R \to R'$ *is a homomorphism where* R' *is an integral domain such that Ker* $f \neq R$ *then show that* $f(1)$ *is unity of* R'.

Solution: Let $a' \in R'$ be any element. We show

$$f(1)\, a' = a' f(1) = a'$$

Now $\quad f(1)\, a' - f(1)\, a' = 0'$

$\Rightarrow f(1.1)\, a' - f(1)\, a' = 0'$

$\Rightarrow f(1)\, f(1)\, a' - f(1)\, a' = 0'$

$\Rightarrow f(1)\, [f(1)\, a' - a'] = 0'$

$\Rightarrow$ either $\quad f(1) = 0'$ or $f(1)\, a' - a' = 0'$ as R' is an integral domain.

$f(1) = 0' \Rightarrow 1 \in \text{Ker } f \Rightarrow \text{Ker } f = R$ which is not true.

Hence $f(1)a' - a' = 0'$

$\Rightarrow \quad f(1)\, a' = a'$

Similarly, we can show $a' = a' f(1)$.

Problem 2: *Let* $f : R \to R'$ *be an onto homomorphism, where R is a ring with unity. Show that* $f(1)$ *is unity of* R'.

Solution: Let $a' \in R'$ be any element.

Since f is onto, $\exists\ a \in R$, s.t., $f(a) = a'$

Now $\quad a'.\ f(1) = f(a)\ .\ f(1) = f(a\ .\ 1) = f(a) = a'$

Similarly $f(1)\ .\ a' = a'$.

Showing, thereby that $f(1)$ is unity of R'.

Problem 3: *Show by an example that we can have a homomorphism $f: R \to R'$, such that $f(1)$ is not unity of R', where 1 is unity of R.*

Solution: Consider the map $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 0 \quad \text{for all } x \in \mathbf{Z}$$

where $\mathbf{Z}$ = ring of integers

then f is a homomorphism (verify)

Again $f(1) = 0$, but 0 is not unity of $\mathbf{Z}$.

Thus although $\mathbf{Z}$ (on R.H.S.) has unity it does not equal $f(1)$.

Remarks: (*i*) If we take the map $f: \mathbf{Z} \to \mathbf{E}$, where $\mathbf{E}$ = ring of even integers, defined by $f(x) = 0$ for all x, we find, $\mathbf{E}$ does not have unity, whereas 1 is unity of $\mathbf{Z}$.

(*ii*) We recall (see page 116) that the map $f: \mathbf{Z} \to \mathbf{E}$, s.t., $f(x) = 2x$ is a group isomorphism. Thus $\mathbf{Z}$ and $\mathbf{E}$ are isomorphic as groups whereas $\mathbf{Z}$ and $\mathbf{E}$ are not isomorphic as rings. Indeed, $\mathbf{Z}$ has unity but $\mathbf{E}$ does not possess unity. In fact, f will not be a ring homomorphism.

Problem 4: *Find all the ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.*

Solution: Let $f: \mathbf{Z}_{20} \to \mathbf{Z}_{30}$ be any ring homomorphism.

Let $f(1) = a$, then $f(x) = xa$ and as done in Problem 24 under groups on page 120 we find $o(a) | o(\mathbf{Z}_{30}) = 30$ and $o(a) \mid 20 = o(\mathbf{Z}_{20})$

Thus possible values of $o(a)$ are 1, 2, 5, 10 and so possible values of a will be

$$0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27$$

which give us the ten group homomorphisms.

Since f is a ring homomorphism and in $\mathbf{Z}_{20}$, $1.1 = 1$, we find $f(1.1) = f(1)$

or $\qquad f(1)(1) = f(1)$

or $\qquad a^2 = a$ in $\mathbf{Z}_{30}$

This is satisfied by 0, 6, 15, 21 values of a .

Hence there exist four ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.

Problem 5: *Show that $2\mathbf{Z}$ is not isomorphic to $3\mathbf{Z}$ as rings. What can be said about isomorphism between $m\mathbf{Z}$ and $n\mathbf{Z}$, where m, n are positive integers?*

Solution: Suppose $2\mathbf{Z} \cong 3\mathbf{Z}$ and let $f: 2\mathbf{Z} \to 3\mathbf{Z}$ be the isomorphism.

As $\qquad 2 \in 2\mathbf{Z}, f(2) = 3n$ for some $n \in \mathbf{Z}$

Now $\qquad f(4) = f(2 + 2) = f(2) + f(2) = 6n$

$\qquad f(4) = f(2 \cdot 2) = f(2) \cdot f(2) = (3n)^2$

Thus $\qquad 6n = 3n^2$ or that $2 = 3n$

But this is not possible for any $n \in \mathbf{Z}$

Hence f is not an isomorphism.

Suppose now f: $m\mathbf{Z} \to n\mathbf{Z}$ is any ring isomorphism

Then $$f(\underbrace{m + m + \cdots + m}_{m \text{ times}}) = f(m) + f(m) + \cdots + f(m)$$
$$= mf(m)$$
$$\Rightarrow f(mm) = mf(m)$$
$$\Rightarrow f(m)f(m) = mf(m) \Rightarrow f(m) = m \quad (1)$$

Again as f is onto and $n \in n\mathbf{Z}$, $\exists\ mr \in m\mathbf{Z}$

s.t., $f(mr) = n$ or $rf(m) = n$

$$\Rightarrow f(m) \mid n$$

Again as $m \in m\mathbf{Z}, f(m) \in n\mathbf{Z}$

$$\Rightarrow f(m) = nk \text{ for same } k$$
$$\Rightarrow n \mid f(m)$$

and hence $f(m) = n$

or that $m = n$ from (1)

So if $m\mathbf{Z} \cong n\mathbf{Z}$, then $m = n$. The converse, of course, is obviously true.

Hence we conclude: $m\mathbf{Z} \cong n\mathbf{Z}$ as rings if and only if $m = n$.

(**Note:** see page 142 under groups)

Problem 6: *Let* $\mathbf{Z}$ *be the ring of integers. Show that the only homomorphisms from* $\mathbf{Z} \to \mathbf{Z}$ *are the identity and zero mappings*.

Solution: Let $f : \mathbf{Z} \to \mathbf{Z}$ be a homomorphism

Since $(f(1))^2 = f(1)f(1) = f(1.1) = f(1)$

$$f(1)[f(1) - 1] = 0$$
$$\Rightarrow f(1) = 0 \text{ or } f(1) = 1$$

If $f(1) = 0$ then $f(x) = 0\ \forall$ integers x

as $f(x) = f(1 \cdot x) = f(1)f(x) = 0 \cdot f(x) = 0\ \forall\ x$

Thus in this case f is the zero homomorphism.

If $f(1) = 1$, then for any $x \in \mathbf{Z}$

$$f(x) = f(1 + 1 + \ldots + 1) = x\, f(1) = x \qquad (x > 0)$$
$$f(x) = f(-y) = -f(y) = -[f(1 + 1 + \ldots + 1)] = -y\, f(1) = x\, f(1) = x \qquad (x < 0,\ y = -x)$$
$$f(0) = 0$$

So in this case f is identity map, which proves the result.

Problem 7: *Let R and S be two commutative rings with unity and let f:* $R \to S$ *be an onto homomorphism. If ch* $R \neq 0$*, show that ch S divides ch R.*

Solution: Suppose ch $R = n$, then n is least +ve integer such that $na = 0\ \forall\ a \in R$

So $n.1 = 0$ and n is least

$\Rightarrow 1 + 1 + \ldots + 1 = 0$ and so additive order of 1 is n.

Again as f is onto $f(1)$ is unity of S and so ch S is additive order of $f(1)$

As $o(f(1)) \mid o(1)$, we find ch $S \mid$ ch R.

Problem 8: *Show that the ring D of quaternions is isomorphic to the ring*

$$M = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \mid a, b \in \mathbf{C} \right\}.$$

Solution: Let $a + bi + cj + dk \in D$.

Then $a + bi + cj + dk = (a + bi) + (c + di)j$

Define $\theta: D \to M$, s.t.,

$$\theta(a + bi + cj + dk) = \begin{bmatrix} a+bi & c+di \\ -(c-di) & a-bi \end{bmatrix}$$

Then θ is a ring homomorphism.

We leave the proof of the fact that θ preserves addition to the reader.

Consider $\theta((a + bi + cj + dk)(a' + b'i + c'j + d'k))$

$= \theta[((a + bi) + (c + di)j)((a' + b'i) + (c' + d'i)j]$

$= \theta[(a + bi)(a' + b'i) + (a + bi)(c' + d'i)j + (c + di)(a' - b'i)j +$

$(c + di)(-c' + d'i)i]$

$$= \begin{bmatrix} (a+bi)(a'+b'i)+(c+di)(-c'+d'i) & (a+bi)(c'+di)+(c+di)(a'-b'i) \\ (-c+di)(a'+b'i)+(a-bi)(-c'+d'i) & (a-bi)(a'-b'i)+(c+di)(c'+d'i) \end{bmatrix}$$

$$= \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \begin{bmatrix} a'+b'i & c'+d'i \\ -c'+d'i & a'-b'i \end{bmatrix}$$

It is not difficult to check that θ is one-one and onto. So, θ is an isomorphism.

Hence $D \cong M$.

Theorem 4: (Fundamental Theorem of Ring Homomorphism)

If $f: R \to R'$ *be an onto homomorphism, then* R' *is isomorphic to a quotient ring of R. In fact,* $R' \cong \dfrac{R}{\operatorname{Ker} f}$.

Proof: Let $f: R \to R'$ be onto homomorphism

Define $\varphi: \dfrac{R}{\operatorname{Ker} f} \to R'$, s.t.,

$\varphi(x + I) = f(x)$ for all $x \in R$ where $I = \operatorname{Ker} f$

then φ is well defined as

$x + I = y + I$

$$\Rightarrow x - y \in I = \text{Ker } f$$
$$\Rightarrow f(x - y) = 0$$
$$\Rightarrow f(x) - f(y) = 0$$
$$\Rightarrow f(x) = f(y)$$
$$\Rightarrow \varphi(x + I) = \varphi(y + I)$$

Retracing the steps backwards we prove φ is 1–1.

Again, as

$$\varphi[(x + I) + (y + I)] = \varphi((x + y) + I) = f(x + y) = f(x) + f(y)$$
$$= \varphi(x + I) + \varphi(y + I)$$
$$\varphi[(x + I)(y + I)] = \varphi(xy + I) = f(xy) = f(x)\, f(y)$$
$$= \varphi(x + I)\ \varphi(y + I)$$

φ is a homomorphism.

Now if $r' \in R'$ be any element then as $f : R \to R'$ is onto, $\exists\ r \in R$, s.t., $f(r) = r'$ for this r, as $\varphi(r + I) = f(r) = r'$

We find $r + I$ is required pre-image of r' under φ showing thereby that φ is onto and hence an isomorphism.

Thus $\dfrac{R}{\text{Ker } f} \cong R'$. By summetry $R' \cong \dfrac{R}{\text{Ker } f}$.

Theorem 5: (First Theorem of Isomorphism)

Let $B \subseteq A$ be two ideals of a ring R. Then

$$\frac{R}{A} \cong \frac{R/B}{A/B}.$$

Proof: Define a mapping $f : \dfrac{R}{B} \to \dfrac{R}{A}$ s.t.,

$$f(r + B) = r + A$$

then f is an onto homomorphism (Prove!)

By fundamental theorem, $\dfrac{R}{A} \cong \dfrac{R/B}{\text{Ker } f}$

Again, since $r + B \in \text{Ker } f \Leftrightarrow f(r + B) = A$

$$\Leftrightarrow r + A = A$$
$$\Leftrightarrow r \in A$$
$$\Leftrightarrow r + B \in \frac{A}{B}$$

we find $\text{Ker } f = A/B$

Hence $\dfrac{R}{A} \cong \dfrac{R/B}{A/B}$.

Theorem 6: (Second Theorem of Isomorphism)

Let A, B *be two ideals of a ring* R, *then*

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

Proof: Define a mapping $f : B \to \frac{A+B}{A}$ s.t.,

$$f(b) = b + A \quad \text{for all } b \in B$$

Then f is a well defined homomorphism.

Again if $x + A \in \frac{A+B}{A}$ be any element then

$$x \in A + B \Rightarrow x = a + b, \quad a \in A, \quad b \in B$$

So, $x + A = (a + b) + A = (b + a) + A = b + (a + A) = b + A$

thus $x + A = b + A = f(b)$

i.e., b is the pre-image of $x + A$ under f or that f is onto.

By fundamental theorem then $\frac{A+B}{A} \cong \frac{B}{\text{Ker } f}$

Now $x \in \text{Ker } f \Leftrightarrow f(x) = A$

$$\Leftrightarrow x + A = A \Leftrightarrow x \in A$$

$$\Leftrightarrow x \in A \cap B \qquad (x \in \text{Ker } f \subseteq B)$$

Hence $\text{Ker } f = A \cap B$

and thus $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

Remark: Clearly then $\frac{A+B}{B} \cong \frac{A}{A \cap B}$.

Problem 9: Show that $\frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$.

Solution: Take $A = <2>$, $B = <5> = 5\mathbf{Z}$, the ideals of $\mathbf{Z}$.

Then $A + B = <d>$, where d = g.c.d. (2, 5) = 1

$A \cap B = <l>$ where l = l.c.m. (2, 5) = 10

(See exercise 23 on page 352)

So $A + B = <1> = \mathbf{Z}$

$A \cap B = <10> = 10\mathbf{Z}$

Hence using the above result that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B} \text{ we get } \frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$$

Theorem 7: *If N be an ideal of a ring R then there exists a one-one onto mapping between the set of all ideals of R, containing N and the set of ideals of R/N.*

Proof: Let $f : R \to R/N$ be the natural homomorphism defined by $f(r) = r + N$. Now, if A be any ideal of R then as $f : R \to R/N$ is onto homomorphism, $f(A)$ is an ideal of R/N.

Again, $f(A) = \{f(a) \mid a \in A\}$

$= \{a + N \mid a \in A\}$

$= \dfrac{A}{N}$.

Let now $\mathcal{K}$ be the set of all ideals of R, which contain N and $\mathcal{K}'$ be the set of all ideals of $\dfrac{R}{N}$.

Define $\varphi : \mathcal{K} \to \mathcal{K}'$ s.t.,

$\varphi(A) = f(A) = \dfrac{A}{N}$

φ is clearly well-defind.

Again $\varphi(A) = \varphi(B)$

$\Rightarrow f(A) = f(B)$

$\Rightarrow \dfrac{A}{N} = \dfrac{B}{N}$

If $a \in A$ be any element then $a + N \in \dfrac{A}{N} \Rightarrow a + N \in \dfrac{B}{N}$

$\Rightarrow a + N = b + N$ for some $b \in B$

$\Rightarrow a - b \in N \subseteq B$

$\Rightarrow a - b = b'$ for some $b' \in B$

$\Rightarrow a = b + b' \in B$

i.e., $A \subseteq B$.

Similarly, $B \subseteq A$ and thus $A = B$

showing that φ is one-one.

To show that φ is onto, let $X \in \mathcal{K}'$ be any member then X is an ideal of $\dfrac{R}{N}$.

Define $A = \{x \in R \mid f(x) \in X\}$.

We show A is the required pre-image of X under φ.

It is easy to check that A is an ideal of R.

Again, $n \in N = \text{Ker } f$

$\Rightarrow f(n) = N =$ zero of $\dfrac{R}{N}$

$0 + N \in X$ [as ideal contains zero]

$\therefore$ $f(n) \in X \Rightarrow n \in A$

or that $N \subseteq A$.

Thus A is a member of $\mathcal{K}$.

Definition of A then confirms that it is the required pre-image. Hence φ is onto.

Cor.: If N is an ideal of a ring R then any ideal of R/N is of the type A/N where A is an ideal of R, containing N. (See also problem 30, page 129, under groups).

Problem 10: Show that $\mathbf{Z}_n \cong \dfrac{\mathbf{Z}}{(n)}$.

Solution: We have $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\}$

$$\frac{\mathbf{Z}}{(n)} = \{(n),\ 1+(n),\ 2+(n),.....,\ \overline{(n-1)}+(n)\}$$

Define $\theta : \dfrac{\mathbf{Z}}{(n)} \to \mathbf{Z}_n$, s.t.,

$\theta(r + (n)) = r, \quad 0 \le r \le n-1$

Let $r + (n) = s + (n)$ and suppose $r \neq s$.

Then $r - s \in (n) \Rightarrow n \mid (r - s) \Rightarrow n \le r - s$

where $r, s \le n$. We thus get a contradiction.

Hence $r = s$ and so θ is well defined.

It is clearly seen to be 1-1.

Again, as

$$\theta((r + (n)) + (s + (n))) = \theta(\overline{r+s}+(n)) = \theta((nq + t) + (n)) \text{ for some } q,\ t,\ 0 \le t < n$$
$$= \theta(t + (n)) = t = r \oplus s = \theta(r +(n)) \oplus \theta(s + (n))$$
$$\theta((r + (n))\ (s + (n))) = \theta(rs + (n)) = \theta((nq' + k + (n)) \text{ for some } q',\ k,\ 0 \le k < n$$
$$= \theta(k + (n)) = k = r \otimes s = \theta(r + (n)) \otimes \theta(s + (n))$$

We find θ is a homomorphism and hence an isomorphism.

Remark: The above result can also be proved by using Fundamental theorem. See remark on page 131 also.

Problem 11: *Show that* $\dfrac{\mathbf{Z}}{(n)}$ *has no non zero nilpotent element iff n is square free.*

Solution: Suppose $\dfrac{\mathbf{Z}}{(n)}$ has no non zero nilpotent elements.

Let $n = p_1^{\alpha_1}\ p_2^{\alpha_2}.....p_r^{\alpha_r}$, where p_i are distinct primes.

Suppose n is not square free. Then some $\alpha_i \ge 2$. Let $\alpha_1 \ge 2$.

Let $m = p_1 .\ p_2^{\alpha_2}.... \ p_r^{\alpha_r}$ then $m < n$

Also $m + (n) \neq (n)$

Now $(m + (n))^{\alpha_1} = m^{\alpha_1} + (n) = (n)$

implies $m + (n)$ is a non zero nilpotent element in $\frac{\mathbf{Z}}{(n)}$, a contradiction.

Hence n is square free.

Conversely, let n be square free.

Suppose $m + (n)$ is a nilpotent element in $\frac{\mathbf{Z}}{(n)}$.

Then $(m + (n))^{\alpha} = (n)$ for some α

So $m^{\alpha} \in (n) \Rightarrow m^{\alpha} = nk$ for some k

Let $n = p_1 p_2 \ldots p_r$ where p_i are distinct primes

(Note n is square free)

Since $p_i \mid n \quad \forall\ i$,

$n = p_1\ p_2\ \ldots\ p_r$ divides $m \Rightarrow m + (n) = (n) =$ zero of $\frac{\mathbf{Z}}{(n)}$.

i.e., $\frac{\mathbf{Z}}{(n)}$ has no non zero nilpotent elements.

Problem 12: *Find all the nilpotent elements in* $\mathbf{Z}_{30}$.

Solution: We know $\mathbf{Z}_{30} \cong \frac{\mathbf{Z}}{(30)}$ and as $30 = 2 \times 3 \times 5$ is square free, $\frac{\mathbf{Z}}{(30)}$ or $\mathbf{Z}_{30}$ has no non zero nilpotent elements.

Remark : See problem 24 on page 334 also.

We now show that there exists a polynomial over D, the ring of quaternions which has infinite number of roots.

Problem 13: *Show that* $x^2 + 1 = 0$ *has infinite number of solutions over* D, *the ring of quaternions*.

Solution: Let $u = a + bi + cj + dk$ be a solution of $x^2 + 1 = 0$ Then $u^2 = -1$.

Let $\theta : D \to M$ be the isomorphism as defined in problem 8 on page 361.

Then $\theta(u)^2 = -\theta(1) = -I$, where I denotes the 2×2 identity matrix.

Let $\theta(u) = A = \begin{bmatrix} a+bi & c+di \\ -(c-di) & a-bi \end{bmatrix}$.

Then $A^2 = -I$ and Trace $A = 2a$

Now $A^2 = \begin{bmatrix} a+bi & c+di \\ -(c-di) & a-bi \end{bmatrix} \begin{bmatrix} a+bi & c+di \\ -(c-di) & a-bi \end{bmatrix}$

$$= \begin{bmatrix} a^2 - b^2 + 2a\,bi - c^2 - d^2 & - \\ - & -c^2 - d^2 + a^2 - b^2 - 2abi \end{bmatrix}$$

$= -I$

implies Trace $A^2 = 2(a^2 - b^2 - c^2 - d^2) = \text{Trace}\ (-I) = -2$
implies $b^2 + c^2 + d^2 = a^2 + 1$
Now $\det A = a^2 + b^2 + c^2 + d^2$
So $\det A^2 = (\det A)^2 = (a^2 + b^2 + c^2 + d^2)^2 = +1$
Therefore, $a^2 + b^2 + c^2 + d^2 = 1$. But $b^2 + c^2 + d^2 = a^2 + 1$
So, $a^2 + a^2 + 1 = 1 \Rightarrow 2a^2 = 0 \Rightarrow a = 0$
This gives $b^2 + c^2 + d^2 = 1$ and $u = 0 + bi + cj + dk$
Also $(0 + bi + cj + dk)^2 = -(b^2 + c^2 + d^2) + 0i + 0j + 0k = -1$

Therefore, the solutions of $x^2 + 1 = 0$ are given by $u = 0 + bi + cj + dk$, where $b^2 + c^2 + d^2 = 1$
There are infinite real numbers b, c, d such that $b^2 + c^2 + d^2 = 1$. For example, let p be a prime,

then take $b = \dfrac{\sqrt{p-1}}{\sqrt{p}},\ c = \dfrac{1}{\sqrt{p}},\ d = 0.$

So, $b^2 + c^2 + d^2 = \dfrac{p-1}{p} + \dfrac{1}{p} = 1.$ But the number of primes are infinite.

Hence, $x^2 + 1 = 0$ has infinite number of solutions over D.

Exercises

1. Show that the relation of isomorphism in rings is an equivalence relation.
2. Let $f : R \to R'$ be a homomorphism and let A be an ideal of R. Show that $f(A) = \{x \in R' \mid \exists\ a \in A,\ x = f(a)\}$ is an ideal of $f(R)$.
3. Show that the map $f : \mathbf{Z}_2 \to \mathbf{Z}_2$, s.t., $f(n) = n^2 - 15n$ is a homomorphism.
4. Show that $\mathbf{Z}_{70}$ has no non zero nilpotent elements.
5. Prove that any homomorphism of a field is either a monomorphism or takes each element to zero.
6. Show that homomorphic image of a commutative ring is commutative. Prove also that the converse may not hold.
7. Show that homomorphic image of a ring with unity is a ring with unity but the converse is not true.
8. Find all the six ring homomorphisms from $\mathbf{Z}_{12} \to \mathbf{Z}_{30}$.
9. Let I be an ideal of a ring R. Show that
   (a) if R is commutative then so is R/I
   (b) if R has unity 1 then $1 + I$ is unity of R/I
   (c) converse of (a) and (b) does not hold.
   [Hint: Take R = ring of matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ and I of type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$ over integers.]
10. Show that there exists an onto homomorphism from a ring R to R/I, a quotient ring of R (called the natural homomorphism) (Define $f(r) = r + I$).

11. If I is an ideal of R, show that R/I has no zero divisors iff the following is true:
(i) whenever a product of two elements of R belongs to I, at least one of these belongs to I.
(ii) $r + I \in R/I$ is unity of R/I iff $rx - x \in I$ and $xr - x \in I$ for all $x \in R$.

12. Show that the set N of all nilpotent elements in a commutative ring R forms an ideal of R and that R/N has no non zero nilpotent elements. *N is called the nilradical* of R.

13. Show that the centre of the quaternion ring D is isomorphic to the field $\mathbf{R}$ of real numbers. [Hint: Define $\theta : \mathbf{R} \to Z(D)$ s.t., $\theta(a) = (a, 0, 0, 0)$.]

14. Show that $C' = \{(a, b, 0, 0) | a, b \in \mathbf{R}\}$ is a subring of D, the ring of quaternions. Show further that $\varphi : \mathbf{C} \to C'$, s.t., $\varphi((a + ib)) = (a, b, 0, 0)$ is an isomorphism. We thus notice that the ring of quaternions contains both the fields of real and complex numbers.

15. Without using isomorphism theorem show that $\dfrac{\mathbf{Z}}{<2>} \cong \dfrac{5\mathbf{Z}}{10\mathbf{Z}}$.

[**Hint:** Define $\theta : \dfrac{\mathbf{Z}}{<2>} \to \dfrac{5\mathbf{Z}}{10\mathbf{Z}}$, s.t.,
$\theta(0 + (2)) = 0 + (10)$
$\theta(1 + (2)) = 5 + (10)$]

16. Let $G = \{2n \mid n \in \mathbf{Z}\}$, $H = \{8n \mid n \in \mathbf{Z}\}$. Show that G/H and $\mathbf{Z}_4$ (ring of integers modulo 4) are isomorphic as groups but not as rings.

17. Show that $\{0, 2, 4, 6, 8\}$ addition, multiplication mod 10 is isomorphic to $\mathbf{Z}_5$.

18. Let $f : R \to R'$ be a homomorphism. If $x \in R$ is nilpotent show that $f(x)$ is nilpotent in R'.

Embedding of Rings

A non empty subset S of a ring R is defined to be a subring of R if S forms a ring under the binary compositions of R (restricted to S). Thus a subring inherits its compositions from the parent ring. We now come to the 'reverse' process. Given a ring S, can we find a super ring R so that S is a subring of R ? The answer may not be a complete yes in the sense that a subring is defined only when we have a ring and the operations in the subring are got through these operations. But it is, of course, possible to have a ring R, so that our starting ring S is isomorphic to a subring of R. Then we can *identify* our ring S as a subring of this R. This is what is called embedding of rings.

The usefulness of embedding would be illustrated later through examples. To start with, we give

Definition: Let R and R' be two rings. A one-one homomorphism θ from R to R' is called an embedding (imbedding) mapping and in that case R' is called *extension ring* or *overring of R*.

Embedding of a ring into a ring with unity.

Let R be any ring and let $\mathbf{Z}$ be the ring of integers.

Consider $R \times \mathbf{Z} = \{(r, n) \mid r \in R, n \in \mathbf{Z}\}$

We show $R \times \mathbf{Z}$ forms a ring with unity, under addition and multiplication defined by

$$(r, n) + (s, m) = (r + s, n + m) \qquad r, s \in R, n, m \in \mathbf{Z}$$

$$(r, n) \,.\, (s, m) = (rs + ns + mr, nm)$$

Addition is well-defined as

Let $(r, n) = (r', n')$ and $(s, m) = (s', m')$

Then $r = r', n = n'$ and $s = s', m = m'$

$$\Rightarrow r + s = r' + s', n + m = n' + m'$$

$$\Rightarrow (r + s, n + m) = (r' + s', n' + m')$$

Similarly one can show that multiplication is well defined.

Associativity : $(r, n) + [(s, m) + (t, k)] = (r, n) + (s + t, m + k)$

$$= (r + (s + t), n + (m + k))$$

$$= ((r + s) + t, (n + m) + k)$$

$$= (r + s, n + m) + (t, k)$$

$$= [(r, n) + (s + m)] + (t, k)$$

Commutativity follows as above.

Again it is clear that (0, 0) will be the zero element and $(-r, -n)$ will be additive inverse of (r, n), where, of course, $-r$ is inverse of r in R and $-n$ is – ve of n in $\mathbf{Z}$.

It would be a routine exercise for the reader to check that associativity w.r.t. multiplication and distributive properties also hold.

Again, as $(r, n)\ (0, 1) = (r.\ 0 + n.\ 0 + 1r, n.1)$

$$= (r, n)$$

(0, 1) will be unity and hence $R \times \mathbf{Z}$ forms a ring with unity.

We show R can be imbedded into $R \times \mathbf{Z}$

Define a mapping $\theta : R \to R \times \mathbf{Z}$, s.t.,

$$\theta(r) = (r, 0)$$

then θ is clearly well defined mapping

Also $\theta(r) = \theta(s)$

$$\Rightarrow (r, 0) = (s, 0) \Rightarrow r = s$$

shows θ is one-one.

Again $\theta(r + s) = (r + s, 0) = (r, 0) + (s, 0) = \theta(r) + \theta(s)$

$$\theta(rs) = (rs, 0) = (r, 0)\ (s, 0) = \theta(r)\ \ \theta(s)$$

Thus θ is a homomorphism and therefore, an embedding mapping.

Hence we get

Theorem 8: *Any ring can be embedded into a ring with unity.*

Embedding of a ring into a ring of endomorphisms

We recall that a homomorphism from A to A is called an endomorphism.

Let $< V, + >$ be any additive abelian group. We denote by Hom (V, V) the set of all homomorphisms from V to V (*i.e.* it is set of all endomorphisms of V).

We show now Hom (V, V) forms a ring with unity under the operations defined by

$$(f + g)x = f(x) + g(x) \qquad x \in V$$
$$(fg)x = f(g(x)) \quad x \in V$$

where $f, g \in$ Hom (V,V).

Closure : Let $f, g \in$ Hom (V,V)

Then $(f + g)(x + y) = f(x + y) + g(x + y)$
$= (f(x) + f(y)) + (g(x) + g(y))$
$= (f(x) + g(x)) + (f(y) + g(y))$
$= (f + g)x + (f + g)y$

$\Rightarrow f + g$ is an endomorphism of V

i.e., $f + g \in$ Hom (V,V)

Again $(fg)(x + y) = f(g(x + y))$
$= f(g(x) + g(y))$
$= f(g(x)) + f(g(y))$
$= (fg)x + (fg)y$

$\Rightarrow fg \in$ Hom (V,V)

Associativity : $[f + (g + h)]x = f(x) + [(g + h)x]$
$= f(x) + (g(x) + h(x))$
$= (f(x) + (g(x)) + h(x)$
$= (f + g)x + h(x)$
$= [(f + g) + h]x$ for all x

$\Rightarrow f + (g + h) = (f + g) + h$

Commutativity follows as above.

Let $O : V \to V$ be defined by

$O(x) = 0$ for all $x \in V$

then O is easily seen to be a homomorphism.

Also since $(f + O)x = f(x) + O(x) = f(x) + 0 = f(x)$
$= 0 + f(x) = O(x) + f(x) = (O + f)x$ for all x

we have

$$f + O = f = O + f$$

or that O is zero of Hom (V, V).

Again for any $f \in$ Hom (V, V), define a map

$(-f) : V \to V$, s.t.,

$(-f)\, x = -f(x)$

then $(-f)$ is a homomorphism and $f + (-f) = O = (-f) + f$

Showing thereby that $(-f)$ is inverse of f. Associativity and distributivity can be proved easily, establishing that Hom (V, V) is a ring. The map $i : V \to V$ s.t., $i(x) = x$ for all $x \in V$ will act as unity of this ring.

Hence Hom (V, V) forms a ring with unity for any additive abelian group V.

Theorem 9: *Any ring R with unity can be embedded into a ring of endomorphisms of some additive abelian group.*

Proof: Let $< R, +, \cdot >$ be the given ring with unity then $< R, + >$ is an additive abelian group. We denote it by R^+. By what is done in the preceding pages, it follows that Hom (R^+, R^+) is a ring with unity (it being the ring of endomorphisms of the additive abelian group R^+).

Define a mapping $f : R \to \text{Hom}\ (R^+, R^+)$ s.t.,

$$f(r) = g_r \quad r \in R \quad \text{where } g_r(x) = rx \qquad x \in R^+$$

To show that f is well defined, we first show that $g_r : R^+ \to R^+$ s.t., $g_r(x) = rx$ is a homomorphism.

Since $g_r(x + y) = r(x + y) = rx + ry = g_r(x) + g_r(y)$,

we find g_r is a homomorphism.

Thus $g_r \in \text{Hom}\ (R^+, R^+)$.

Again
$$\begin{aligned} & r_1 = r_2 \\ \Rightarrow\ & r_1 x = r_2 x \qquad \text{for all } x \in R^+ \\ \Rightarrow\ & g_{r_1}(x) = g_{r_2}(x) \quad \text{for all } x \\ \Rightarrow\ & g_{r_1} = g_{r_2} \\ \Rightarrow\ & f(r_1) = f(r_2) \end{aligned}$$

or that f is a well defined mapping.

Again,
$$\begin{aligned} & f(r_1) = f(r_2) \\ \Rightarrow\ & g_{r_1} = g_{r_2} \\ \Rightarrow\ & g_{r_1}(x) = g_{r_2}(x) \quad \text{for all } x \in R^+ \\ \Rightarrow\ & r_1 x = r_2 x \quad \text{for all } x \in R^+ \end{aligned}$$

$\Rightarrow$ In particular, $r_1 \cdot 1 = r_2 \cdot 1$ as $1 \in R^+$

$$\Rightarrow\ r_1 = r_2$$

or that f is one-one.

Again $f(r_1 + r_2) = g_{r_1 + r_2}$

and $f(r_1) + f(r_2) = g_{r_1} + g_{r_2}$

where
$$\begin{aligned} g_{r_1 + r_2}(x) &= (r_1 + r_2)x = r_1 x + r_2 x = g_{r_1}(x) + g_{r_2}(x) \\ &= (g_{r_1} + g_{r_2})x \quad \text{for all } x \end{aligned}$$

means $g_{r_1 + r_2} = g_{r_1} + g_{r_2}$

or that $f(r_1 + r_2) = f(r_1) + f(r_2)$.

Now $f(r_1 r_2) = g_{r_1 r_2}$ and $f(r_1)\, f(r_2) = g_{r_1} g_{r_2}$

where
$$\begin{aligned} g_{r_1 r_2}(x) &= (r_1 r_2)x = r_1(r_2 x) = g_{r_1}(r_2 x) = g_{r_1}(g_{r_2}(x)) \\ &= (g_{r_1} g_{r_2})x \quad \text{for all } x \end{aligned}$$

$$\Rightarrow g_{r_1r_2} = g_{r_1} g_{r_2}$$

or that $f(r_1 r_2) = f(r_1)\, f(r_2)$.

Showing thereby that f is a homomorphism and hence an imbedding mapping.

Which proves the result.

Summing up all that we have done in the last few pages on imbedding and using the idea of composition of mappings, we have established

Theorem 10: *Any ring R can be embedded into a ring of endomorphisms of some additive abelian group.*

Problem 14: *If* $< \mathbf{Z}, +, \cdot >$ *be the ring of integers then show that Hom* $(\mathbf{Z}^+, \mathbf{Z}^+)$ is *isomorphic to* $\mathbf{Z}$, *where by* $\mathbf{Z}^+$ *we mean the additive abelian group* $< \mathbf{Z}, + >$.

Solution: Define a mapping $f : \mathbf{Z} \to \text{Hom}\,(\mathbf{Z}^+, \mathbf{Z}^+)$, s.t.,

$$f(r) = g_r \quad \text{for all } r \in \mathbf{Z}$$

where $$g_r(x) = rx \quad \text{for all } x \in \mathbf{Z}^+$$

then f will be a one-one homomorphism (as seen in the theorem earlier). We need show ontoness. So let $\theta \in \text{Hom}\,(\mathbf{Z}^+, \mathbf{Z}^+)$ be any element, then θ is a homomorphism from $\mathbf{Z}^+ \to \mathbf{Z}^+$. Since $1 \in \mathbf{Z}^+$, $\theta(1) \in \mathbf{Z}^+$, let $\theta(1) = t$.

We claim $\theta = g_t = f(t)$, *i.e.*, t is the required pre-image of θ under f. For this, we show

$$\theta(x) = g_t(x) \text{ for all } x \in \mathbf{Z}$$

Case (*i*): x is a +ve integer.

$$\theta(x) = \underset{(x \text{ times})}{\theta(1+1+.....+1)} = \theta(1) + \theta(1) +.....+ \theta(1) \qquad (x \text{ times})$$

$$= t + t +.....+ t \qquad (x \text{ times})$$

$$= xt = tx = g_t(x)$$

Case (*ii*): x is a –ve integer

Let $x = -y$, then

$$\theta(x) = \theta(-y) = -\theta(y) = -ty = t(-y) = tx = g_t(x)$$

Case (*iii*): x is zero

then $\theta(x) = \theta(0) = 0$ (θ is a homomorphism)

$$= t \,.\, 0 = g_t(0) = g_t(x)$$

Hence, in any case $\theta(x) = g_t(x) \quad \forall x$

$$\Rightarrow \theta = g_t$$

and thus the result follows.

Problem 15: *Show by an example that extension ring of an integral domain need not essentially be an integral domain.*

Solution: Let $\mathbf{E}$ = ring of even integers,

then $\mathbf{E}$ can be embedded into $\mathbf{E} \times \mathbf{Z}$, by defining

$f : \mathbf{E} \to \mathbf{E} \times \mathbf{Z}$, s.t.,

$f(r) = (r, 0)$

Here **E** is an integral domain, whereas **E** × **Z** is not an integral domain as (2, –2). (–2, 0) = (0, 0).

Theorem 11: *An integral domain can be embedded into a field.*

Proof: Let D be an integral domain.

Let $S = \{(a, b) \mid a, b \in D, b \neq 0\}$

Define a relation ~ on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

It is easy to see that ~ is an equivalence relation. Thus it partitions S into equivalence classes. Let equivalence class of (a, b) be denoted by $[a, b]$. Let F be the set of all these equivalence classes. We show F forms a field under addition and multiplication defined by

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a, b] \,.\, [c, d] = [ac, bd]$$

Addition is well-defined

Let $[a, b] = [a', b']$ and $[c, d] = [c', d']$

Then $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$

$\Rightarrow ab' = ba'$ and $cd' = dc'$

$\Rightarrow (ab')\, dd' = (ba')\, dd'$ and $(cd')\, bb' = (dc')\, bb'$ ...(1)

We want to show that

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

which will hold if

$$(ad + bc, bd) \sim (a'd' + b'c', b'd')$$

or if $(ad + bc)\, b'd' = bd\, (a'd' + b'c')$

or if $ab'\, dd' + bb'cd' = ba'dd' + bb'dc'$

which is true if we add equations (1) above.

Hence addition is well defined.

To verify that multiplication is well defined

Let $[a, b] = [a', b'], \quad [c, d] = [c', d']$

then as before $ab' = ba'$ and $cd' = dc'$

$\Rightarrow ab'cd' = ba'dc'$

Now $[a, b].[c, d] = [a', b']\, [c', d']$ ...(2)

if $[ac, bd] = [a'c', b'\, d']$

or if $(ac, bd) \sim (a'c', b'd')$

of if $acb'd' = bda'c'$

which is true by (2).

That addition is commutative and associative will be a routine affair to prove.

Existence of zero element

Let $[a, b] \in F$ be any element. Then

$$[a, b] + [0, b] = [ab + b0, b^2] = [ab, b^2] = [a, b]$$

as $[ab, b^2] = [a, b]$

$\Leftrightarrow (ab, b^2) \sim (a, b) \Leftrightarrow abb = b^2a$

$\Leftrightarrow ab^2 = ab^2$

thus $[0, b]$ will be zero of F. One might notice here that $[0, x] = [0, y]$ for any non zero, $x, y \in D$, as $(0, x) \sim (0, y) \Leftrightarrow 0 \,.\, y = 0.\, x$.

Existence of additive inverse

For any $[a, b]$ in F, $[-a, b]$ will be its additive inverse, as $[a, b] + [-a, b] = [ab-ba, b^2] = [0, b^2] = [0, b]$. Thus $< F, + >$ forms an abelian group.

We leave it to the reader to verify that mutiplication is commutative, associative and is distributive over addition.

Again, since for any $0 \neq x$ in D and for any $[a, b]$ in F.

$$[a, b].\ [x, x] = [ax, bx] = [a, b]$$

we notice $[x, x]$ will act as unity in F. Let now $[a, b]$ be any non zero element of F then $a \neq 0$ (b, of course is non zero). So we can talk of $[b, a]$ in F and as

$$[a, b]\ [b, a] = [ab, ba] = [ab, ab] = [x, x]$$

we find every non zero element of F has multiplicative inverse.

Hence F is a field.

We show D can be imbedded into F. Define a mapping

$\varphi : D \to F$, s.t.,

$\varphi(a) = [ax, x]$ where $0 \neq x \in D$

φ *is well-defined*

Let $a = b$

Then $ax = bx$

$\Rightarrow axx = xbx$

$\Rightarrow (ax, x) \sim (bx, x)$

$\Rightarrow [ax, x] = [bx, x]$

$\Rightarrow \varphi(a) = \varphi(b)$

φ is 1-1

Let $\varphi(a) = \varphi(b)$

Then $[ax, x] = [bx, x]$

$\Rightarrow (ax, x) \sim (bx, x)$

$\Rightarrow axx = xbx$

$\Rightarrow x^2(a - b) = 0$

$\Rightarrow a - b = 0$ as $x^2 \neq 0$

$\Rightarrow a = b.$

φ is a homomorphism

$$\varphi(a + b) = [(a + b)x, x] = [ax + bx, x]$$

$$\varphi(a) + \varphi(b) = [ax, x] + [bx, x] = [axx + xbx, x^2]$$
$$= [ax^2 + bx^2, x^2] = [ax + bx, x]$$

$\therefore$ $\varphi(a + b) = \varphi(a) + \varphi(b)$

Also $\varphi(ab) = [abx, x]$

$\varphi(a)\ \varphi(b) = [ax, x]\ [bx, x] = [abx^2, x^2] = [abx, x]$

or that $\varphi(ab) = \varphi(a)\varphi(b)$

Hence φ is 1-1 homomorphism, and is the required imbedding mapping.

Remark: The above field F is called the *field of quotients* or the quotient field of D. The reader is, however, cautioned not to confuse it with R/I.

We also sometimes use the notation $\frac{a}{b}$ to denote $[a, b]$. The logic behind this notation is clear if we consider imbedding of $\mathbf{Z}$ into $\mathbf{Q}$.

In fact, at times this notation looks more natural and convenient. For instance, $[a, b] + [c, d] = [ad + bc, bd]$.

would read as $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

or $[a, b] = [c, d]$ would mean $\frac{a}{b} = \frac{c}{d}$ or $ad = bc$

Summing up, we can, therefore, say that any integral domain D can be *enlarged* to a field F so that each element of F can be expressed as a quotient of two elements of D.

Problem 16: *Prove that if K is any field which contains D then K contains a subfield isomorphic to F, where F is the field of quotients of the integral domain D.* (*In this sense F is the smallest field containing D*).

Solution: Define a map $\theta : F \to K$, s.t.,

$$\theta([a, b]) = ab^{-1}$$

Since $a, b \in D \subseteq K$, $b \neq 0$, $\therefore$ b^{-1} exists in K. θ is well defined, 1-1 map as

$$[a_1, b_1] = [a_2, b_2]$$
$$\Leftrightarrow (a_1, b_1) \sim (a_2, b_2)$$
$$\Leftrightarrow a_1b_2 = b_1a_2 \Leftrightarrow a_1b_1^{-1} = a_2b_2^{-1}$$
$$\Leftrightarrow \theta([a_1, b_1]) = \theta([a_2, b_2])$$

Again as $\theta([a_1, b_1] + [a_2, b_2]) = \theta([a_1b_2 + b_1a_2, b_1b_2])$

$$= (a_1b_2 + b_1a_2)\ (b_1b_2)^{-1}$$
$$= a_1\, b_2b_2^{-1}\, b_1^{-1} + b_1a_2b_2^{-1}\, b_1^{-1}$$
$$= a_1b_1^{-1} + a_2b_2^{-1}$$
$$= \theta[(a_1, b_1)] + \theta([a_2, b_2])$$

and $\theta[(a_1, b_1]\ [a_2, b_2]) = \theta([a_1a_2,\ b_1b_2])$

$$= (a_1a_2)(b_1b_2)^{-1} = a_1a_2b_2^{-1}\, b_1^{-1}$$
$$= (a_1b_1^{-1})(a_2b_2^{-1}) = \theta([a_1,b_1])\ \theta([a_2,b_2])$$

we find θ is a homomorphism. Thus F will be isomorphic to $\theta(F)$ which will be a subfield of K. Hence quotient field is the smallest field containing D.

Problem 17: *If D_1 and D_2 be two isomorphic integral domains then show that their respective fields of quotients F_1 and F_2 are also isomorphic.*

Solution: Let $f : D_1 \to D_2$ be the given isomorphism. The fields of quotients F_1 and F_2 are given by

$$F_1 = \{[a, b] \mid a, b \in D_1, b \neq 0\}$$
$$F_2 = \{[x, y] \mid x, y \in D_2, y \neq 0\}$$

Define a map $\varphi : F_1 \to F_2$ s.t.,

$$\varphi([a, b]) = [f(a), f(b)]$$
$$[a, b] \in F_1 \Rightarrow a, b \in D_1, \ b \neq 0$$
$$\Rightarrow f(a), f(b) \in D_2 \text{ and } f(b) \neq 0$$
$$\Rightarrow [f(a), f(b)] \in F_2$$

φ is then well-defined and one-one as

$$\varphi([a, b]) = \varphi([a', b'])$$
$$\Leftrightarrow [f(a), f(b)] = [f(a'), f(b')]$$
$$\Leftrightarrow (f(a), f(b)) \sim (f(a'), f(b'))$$
$$\Leftrightarrow f(a) f(b') = f(b) f(a')$$
$$\Leftrightarrow f(ab') = f(ba')$$
$$\Leftrightarrow ab' = ba'$$
$$\Leftrightarrow (a, b) \sim (a', b') \Leftrightarrow [a, b] = [a', b'].$$

φ is onto, as for any $[x, y] \in F_2$, $x, y \in D_2 \Rightarrow \exists\ a, b \in D_1$ s.t., $f(a) = x, f(b) = y$

Also then $\varphi([a, b]) = [f(a), f(b)] = [x, y]$

φ *is a homomorphism*

$$\varphi([a, b] + [a', b']) = ([ab' + ba', bb'])$$
$$= [f(ab' + ba'), f(bb')]$$
$$\varphi([a, b]) + \varphi([a', b']) = [f(a), f(b)] + [f(a'), f(b')]$$
$$= [f(a) f(b') + f(b) f(a'), f(b) f(b')]$$
$$= [f(ab' + ba'), f(bb')]$$

Again $\varphi([a, b]\ [a', b']) = \varphi([aa', bb']) = [f(aa'), f(bb')]$

$$= [f(a) f(a'), f(b) f(b')]$$
$$= [f(a), f(b)]\ [f(a'), f(b')]$$
$$= \varphi([a, b])\ \varphi([a', b'])$$

which shows that φ is an isomorphism.

Remark: The converse is not true, for example the field of quotients of even integers and that of integers are same (the rationals) whereas even integers and integers are not isomorphic as integral domains.

Any two fields of quotients of an integral domain are isomorphic (showing thereby the 'uniqueness' of the field of quotients).

Problems 18: *Let D be an integral domain, $a, b \in D$ be such that $a^n = b^n$, $a^m = b^m$ for two relatively prime positive integers m, n. Prove that $a = b$.*

Solution: If $a = 0$ then $a^n = 0 \Rightarrow b^n = 0 \Rightarrow b = 0$.

Similarly $b = 0 \Rightarrow a = 0$.

Let now a, b be non zero. Let F be the field of quotients of D and let $\theta : D \to F$ be the embedding map. Suppose $\theta(a) = a_1$ and $\theta(b) = b_1$.

Since m, n are relatively prime, $\exists$ integers x, y s.t.,

$$mx + ny = 1$$

Then $$\theta(a) = a_1 = a_1^{mx + ny} = (a_1^m)^x \, (a_1^n)^y$$

Now $$a_1^m = (\theta(a))^m = \theta(a) \, . \, \theta(a) \ldots\ldots \theta(a)$$
$$= \theta(a.a\ldots\ldots a) = \theta(a^m)$$
$$= \theta(b^m) = (\theta(b))^m = b_1^m$$

Similarly, $$a_1^n = b_1^n$$

Thus, $$\theta(a) = (a_1^m)^x \, (a_1^n)^y = (b_1^m)^x \, (b_1^n)^y$$
$$= b_1^{mx + ny} = b_1 = \theta(b)$$

which gives $a = b$ as θ is 1-1.

Remark: The above solution exhibits the 'utility' of the field of quotients. What we did with a_1 and b_1 could not be done with a, b, as a, b are members of an integral domain and existence of multiplicative inverse could not be assured in D, whereas a_1, b_1 being members of a field, we could talk of the inverse elements. Note x, y being integers could also be negative. This is why the solution of the problem could not be taken as

$$a = a^{mx + ny} = (a^m)^x . (a^n)^y = (b^m)^x \, (b^n)^y = b^{mx + ny} = b.$$

Problem 19: *Show that the result of the previous problem may fail to hold in case D is not an integral domain.*

Solution: Consider the ring $D = \{0, 1, 2, \ldots\ldots, 7\}$ mod 8

Take $a = 2$, $b = 4$, $m = 3$, $n = 4$, $(m, n) = 1$

then $$a^n = 2^4 = 2 \otimes 2 \otimes 2 \otimes 2 = 0 = 4^4 = b^n$$
$$a^m = 2^3 = 0 = 4^3 = b^m$$

But $$a \neq b$$

We notice D is not an integral domain as $4 \otimes 2 = 0$ whereas 4, 2 are non zero.

Let's take yet another look at the previous problem 18 and this time we do not insist on the ring to be essentially commutative. Consider

Problem 20: *Let R be a ring without zero divisors, $a, b \in R$ be such that $a^n = b^n$, $a^m = b^m$ for two relatively prime positive integers m, n. Prove that $a = b$.*

Solution: As before $a = 0$ or $b = 0$ gives result.

So let $a \neq 0$, $b \neq 0$. Also m, n can be taken as greater than 1, otherwise the result is true anyway.

Since m, n are relatively prime, $\exists$ integers x, y s.t., $mx + ny = 1$

Now both x, y cannot be positive nor can both be negative together. So one of them must be negative. Let $y < 0$ and suppose $y = -t$, $t > 0$. Then

$$\begin{aligned} & mx = 1 - ny = 1 + tn \\ \Rightarrow\ & a^{mx} = a^{1+tn} = a \,.\, a^{tn} = a(a^n)^t \\ \Rightarrow\ & b^{mx} = a(b^n)^t = ab^{nt} \\ \Rightarrow\ & b^{mx+1} = ab^{nt+1} = ab^{mx} \\ \Rightarrow\ & (a - b)b^{mx} = 0 \\ \Rightarrow\ & a - b = 0 \ \text{ as } \ b^{mx} \neq 0 \ \text{ as } \ b \neq 0 \end{aligned}$$

i.e., $a = b$.

Problem 21: *Find the field of quotients of the integral domain*

$$\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$$

Solution: Let F be the field of quotients of $\mathbf{Z}[i]$

then
$$F = \left\{ \frac{d_1}{d_2} \mid d_1, d_2 \in \mathbf{Z}[i], d_2 \neq 0 \right\}$$

$$= \left\{ \frac{a+ib}{c+id} \mid a, b, c, d \in \mathbf{Z}, c+id \neq 0 \right\}$$

$$= \left\{ \frac{(a+ib)(c-ib)}{c^2+d^2} \mid a, b, c, d \in \mathbf{Z} \right\}$$

$$= \left\{ \frac{ac+bd}{c^2+d^2} + i\frac{(bc-ad)}{c^2+d^2} \mid a, b, c, d \in \mathbf{Z} \right\}$$

$$\subseteq F_1 = \{x + iy \mid x, y \in \mathbf{Q}\}$$

Now if $x + iy \in F_1$ be any element then as $x, y \in \mathbf{Q}$,

$$x + iy = \frac{p_1}{q_1} + i\frac{p_2}{q_2} \text{ where } p_1, p_2, q_1, q_2 \in \mathbf{Z} \text{ and } q_1 \neq 0, q_2 \neq 0$$

$$= \frac{p_1q_2 + ip_2q_1}{q_1q_2 + i.o} + \frac{e_1}{e_2}, \text{ where } e_1, e_2 \in \mathbf{Z}[i] \text{ and } e_2 \neq 0$$

$\Rightarrow \quad x + iy \in F$

or that $F = F_1$

Showing that $F_1 = \{x + iy \mid x, y \in \mathbf{Q}\}$ is the field of quotients of $\mathbf{Z}[i]$

In fact, the mapping $\theta : \mathbf{Z}[i] \to F_1$, s.t.,

$$\theta(a + ib) = a + ib$$

will be the required imbedding mapping.

Exercises

1. Give an example of an embedding mapping in which unity is not mapped to unity.
2. Show that field of reals can be embedded into the field of complex numbers.
3. Find the field of quotients of the integral domain $\mathbf{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$.
4. Show that field of quotients of a finite integral domain is the integral domain itself.

More on Ideals

Definition: Two ideals A and B are called comaximal if $A + B = R$.

Theorem 12: *If R is a commutative ring with unity and A, B are comaximal ideals of R, then* $AB = A \cap B$.

Proof: One can prove that, in general,

$AB \subseteq A \cap B$ (See exercises on page 351)

Let now $x \in A \cap B$ be any element.

Then $x \in A$ and $x \in B$

Since $1 \in R = A + B$

$\exists\ a \in A,\ b \in B$ s.t., $1 = a + b$

$\Rightarrow x \,.\, 1 = x \,.\, (a + b)$

$\Rightarrow x = xa + xb$

$\Rightarrow x = ax + xb$

Now $a \in A,\ x \in B;\ x \in A,\ b \in B \Rightarrow ax + xb \in AB$

i.e., $x \in AB$

or that $A \cap B \subseteq AB$

and thus $AB = A \cap B$.

Theorem 13: *Let R be a commutative ring with unity and let* I_1 *and* I_2 *be two ideals of R. Then*

(*i*) $\varphi : R \to \dfrac{R}{I_1} \times \dfrac{R}{I_2}$, s.t., $\varphi(x) = (x + I_1,\ x + I_2)$ *is a homomorphism s.t.,* $Ker\ \varphi = I_1 \cap I_2$.

(*ii*) I_1 *and* I_2 *are comaximal ideals of R iff* φ *is onto*

Proof: (*i*) We leave it for the reader to verify that φ is a homomorphism.

Since $x \in \text{Ker } \varphi \Leftrightarrow \varphi(x) = (I_1, I_2)$

$\Leftrightarrow (x + I_1, x + I_2) = (I_1, I_2)$

$\Leftrightarrow x + I_1 = I_1,\ x + I_2 = I_2$

$\Leftrightarrow x \in I_1,\ x \in I_2$

$\Leftrightarrow x \in I_1 \cap I_2$

we find $\text{Ker } \varphi = I_1 \cap I_2$.

(*ii*) Suppose φ is onto. Then given $(1 + I_1, 0 + I_2) \in \frac{R}{I_1} \times \frac{R}{I_2}$, $\exists\ x \in R$, s.t.,

$$\begin{aligned} &\varphi(x) = (1 + I_1, I_2) \\ \Rightarrow\ &(x + I_1, x + I_2) = (1 + I_1, I_2) \\ \Rightarrow\ &x + I_1 = 1 + I_1, \quad x + I_2 = I_2 \\ \Rightarrow\ &1 - x \in I_1, \quad x \in I_2, \\ \Rightarrow\ &(1 - x) + x \in I_1 + I_2 \Rightarrow 1 \in I_1 + I_2 \Rightarrow I_1 + I_2 = R \end{aligned}$$

or that I_1 and I_2 are comaximal.

Conversely, let $I_1 + I_2 = R$ (i.e., I_1, I_2 be comaximal)

Since $1 \in R$, $1 \in I_1 + I_2$ we get $1 = x + y$, $x \in I_1$, $y \in I_2$

$$\begin{aligned} \text{Now} \qquad (1 + I_1, I_2) &= (x + y + I_1, I_2) \\ &= (y + I_1, I_2) \\ &= (y + I_1, y + I_2) = \varphi(y) \end{aligned}$$

Similarly, $(I_1, x + I_2) = \varphi(x)$

Now for any $(a_1 + I_1, a_2 + I_2) \in \frac{R}{I_1} \times \frac{R}{I_2}$, since

$$\begin{aligned} (a_1 + I_1, a_2 + I_2) &= (1 + I_1, I_2)\ (a_1 + I_1, a_1 + I_1) + (I_1, 1 + I_2)\ (a_2 + I_1, a_2 + I_2) \\ &= \varphi(y)\varphi(a_1) + \varphi(x)\varphi(a_2) \\ &= \varphi(ya_1 + xa_2) \end{aligned}$$

we find φ is onto.

Remarks: (*i*) If φ is onto, by Fundamental theorem,

$$\frac{R}{\text{Ker}\,\varphi} \cong \frac{R}{I_1} \times \frac{R}{I_2}$$

i.e.,

$$\frac{R}{I_1 \cap I_2} \cong \frac{R}{I_1} \times \frac{R}{I_2}.$$

(*ii*) Let $R = \mathbf{Z}$ the integers and suppose m, n are co-prime integers.

Then $\exists$ integers x, y s.t.,

$$\begin{aligned} &1 = mx + ny \in (m) + (n) \\ \Rightarrow\ &(m) + (n) = R \\ \Rightarrow\ &(m), (n) \text{ are comaximal ideals} \\ \Rightarrow\ &\varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto} \\ \Rightarrow\ &\frac{\mathbf{Z}}{(m) \cap (n)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \\ \Rightarrow\ &\frac{\mathbf{Z}}{(mn)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \end{aligned}$$

$$\Rightarrow \mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n \text{ if } m, n \text{ are co-prime.}$$

(*iii*) Let m, n be co-prime integers, then

$$\varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto}$$

Consider $(a + (m), b + (n)) \in \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$, then $\exists$ an integer x s.t.,

$$\varphi(x) = (a + (m), b + (n))$$

Thus $$(x + (m), x + (n)) = (a + (m), b + (n))$$

$$\Rightarrow x + (m) = a + (m), x + (n) = b + (n)$$

$$\Rightarrow x - a \in (m), \quad x - b \in (n)$$

$$\Rightarrow x - a = \text{multiple of } m, \quad x - b = \text{multiple of } n$$

$$\Rightarrow x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$$

Proving what is popularly known as the *Chinese Remainder theorem*.

We now come to an important class of ideals which are not contained in any (other) proper ideal.

Maximal Ideals

Definition: Let R be a ring. An ideal $M \neq R$ of R is called a *maximal ideal* of R if whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

Example 4: A field F has only two ideals F and $\{0\}$. It is easy to see then that $\{0\}$ is the only maximal ideal of F.

Example 5: Let $< \mathbf{E}, +, . >$ be the ring of even integers.

Let $H_4 = \{4n \mid n \text{ an integer}\}$

then H_4 is an ideal of $\mathbf{E}$ and as $2 \notin H_4$, $H_4 \neq \mathbf{E}$.

Let A be any ideal of $\mathbf{E}$, s.t., $H_4 \subseteq A \subseteq \mathbf{E}$

Suppose $H_4 \neq A$. We show $A = \mathbf{E}$.

Since $H_4 \subset A$, $\exists$ some $x \in A$ s.t., $x \notin H_4$

By division algorithm, we can write

$x = 4q + r$ where $0 < r < 4$

Note $r = 0$ would mean $x = 4q \in H_4$. But $x \notin H_4$ so $r \neq 0$. Again, $r = 1, 3$ would imply x is odd which is not true. Hence the only value that r can have is 2.

Thus $$x = 4q + 2 \Rightarrow 2 = x - 4q \in A$$

as $x \in A$, $4q \in H_4 \subseteq A \Rightarrow x - 4q \in A$

$2 \in A \Rightarrow$ members of the type $2 + 2$, $2 + 2 + 2$, ..., $0 - 2$ are all in A

$\Rightarrow \mathbf{E} \subseteq A$. But $\mathbf{A} \subseteq \mathbf{E}$

Hence $A = \mathbf{E}$ and H_4 is, therefore, a maximal ideal of $\mathbf{E}$.

Example 6: $\{0\}$ in the ring $\mathbf{Z}$ of integers is not a maximal ideal as $\{0\} \subset H_4 \subset \mathbf{Z}$ where $H_4 = \{4n \mid n \in \mathbf{Z}\}$

Example 7: Let R^c = ring of all real valued continuous functions on [0, 1], under the operations

$$(f + g)x = f(x) + g(x)$$
$$(fg)x = f(x)g(x)$$

Let $M = \{f \in R^c \mid f(\tfrac{1}{2}) = 0\}$

then M is a maximal ideal of R^c.

Let g be a function from [0, 1] to the real nos., defined by

$$g(x) = 0 \text{ for all } x \in [0, 1]$$

then g is a real valued function and $g(\tfrac{1}{2}) = 0$, hence $g \in M$. Thus $M \neq \varphi$.

Again, if $f, g \in M$ be any two members, then

$$f(\tfrac{1}{2}) = g(\tfrac{1}{2}) = 0$$
$$(f - g)(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2}) = 0 - 0 = 0 \Rightarrow f - g \in M$$

Also for $f \in M$, $h \in R^c$

$$(hf)^{1/2} = h(\tfrac{1}{2})\, f(\tfrac{1}{2}) = h(\tfrac{1}{2}).\ 0 = 0 = (fh)^{1/2}$$
$$\Rightarrow hf, fh \in M$$

or that M is an ideal.

Define now, θ a function from [0, 1] to the reals by

$$\theta(x) = 1 \text{ for all } x \in [0, 1]$$

then θ is a continuous function. Thus $\theta \in R^c$.

But $\theta \notin M$ as $\theta(\tfrac{1}{2}) = 1 \neq 0$

So $M \neq R^c$.

Let I be any ideal of R^c s.t. $M \subset I \subseteq R^c$

then $\exists\ \lambda \in I$ s.t., $\lambda \notin M$

i.e., $\lambda(\tfrac{1}{2}) \neq 0$

Let $\lambda(\tfrac{1}{2}) = c \neq 0$

Define β from [0, 1] to reals such that

$$\beta(x) = c \text{ for all } x \in [0, 1]$$

then $\beta \in R^c$

Let $\psi = \lambda - \beta$

then $\psi(\tfrac{1}{2}) = \lambda(\tfrac{1}{2}) - \beta(\tfrac{1}{2}) = c - c = 0$

$\Rightarrow \psi \in M$

$\Rightarrow \psi \in I$ as $M \subseteq I$

i.e., $\beta = \lambda - \psi \in I$ [λ, ψ belong to I]

If γ be the function from [0, 1] to reals s.t.,

$$\gamma(x) = \frac{1}{c} \quad (c \neq 0)$$

then $\gamma \in R^c$

Now $(\gamma\beta)(x) = \gamma(x)\ \beta(x) = \frac{1}{c}.\ c = 1 = \theta(x)$ for all x

$\Rightarrow \gamma\beta = \theta$

Since $\beta \in I,\ \gamma\beta \in I$

we find $\theta \in I$

But θ is unity of the ring R^c,

thus I is an ideal containing unity

$\Rightarrow I = R^c$

Hence M is maximal.

Aliter: That M is maximal ideal can also be proved by using the Fundamental theorem of homomorphism.

Define a function $\theta : R^c \to \mathbf{R}$, s.t.,

$\theta(f) = f(\frac{1}{2})$ for all $f \in R^c$

where $\mathbf{R}$ = set of real numbers

then θ is a homomorphism as

$$\theta(f + g) = (f + g)\ (\tfrac{1}{2}) = f(\tfrac{1}{2}) + g\ (\tfrac{1}{2}) = \theta(f) + \theta(g)$$

$$\theta(fg) = (fg)(\tfrac{1}{2}) = f(\tfrac{1}{2})\ g(\tfrac{1}{2}) = \theta(f)\ \theta(g)$$

To check ontoness, we notice, if $r \in \mathbf{R}$ be any element we can define another map $\varphi : [0, 1] \to \mathbf{R}$, s.t.,

$\varphi(x) = r$ for all $x \in [0, 1]$

then φ being constant function will be continuous.

Thus $\varphi \in R^c$

Also $\theta(\varphi) = \varphi(\tfrac{1}{2}) = r$, showing that φ is pre-image of r under θ

i.e., θ is onto.

Thus by Fundamental theorem of homomorphism

$$\frac{R^c}{\text{Ker}\,\theta} \cong \mathbf{R}$$

Now $f \in \text{Ker}\ \theta \Leftrightarrow \theta(f) = 0$

$\Leftrightarrow f(\frac{1}{2}) = 0$

$\Leftrightarrow f \in M$

$\Rightarrow \text{Ker}\ \theta = M$

Hence $\frac{R^c}{M} \cong \mathbf{R}$, but $\mathbf{R}$ being a field, $\frac{R^c}{M}$ will be a field.

i.e. M is maximal ideal of R^c (see theorem 14 below).

Problem 22: *Let R^c be the ring of real valued continuous functions on* $[0, 1]$. *Let* $M = \{f \in R^c \mid f(\frac{1}{2}) = 0\}$. Let $g \in R^c$ be such that $g(x) = x - \frac{1}{2}\ \forall\ x \in [0, 1]$. *Then g is continuous and is in M. Show that* $M = < g >$.

Solution: Let $f \in M$ be any member

Define: h: $[0, 1] \to \mathbf{R}$ s.t.,

$$h(x) = \frac{f(x)}{x - \frac{1}{2}} \text{ when } x \neq \frac{1}{2}$$
$$= f(x) \text{ when } x = \frac{1}{2}$$

where **R** is the field of reals.

Then for $x \neq \frac{1}{2}$

$$(gh)x = g(x)h(x) = g(x)\frac{f(x)}{g(x)} = f(x)$$

and for $x = \frac{1}{2}$

$$(gh)x = g(x)h(x) = 0 = f(x)$$

and hence $f = gh$ (Note $h \in R^c$ as f and g are continuous)

Thus $M \subseteq < g > \subseteq M \Rightarrow M = < g >$

Problem 23: *Let R be a commutative ring with unity and let I be an ideal of R such that for any* $r \in R$, *if* $r \notin I$ *then r is a unit. Show that I is the unique maximal ideal of R.*

Solution: We first show that I is maximal ideal. Let A be any ideal of R s.t., $I \subsetneq A \subseteq R$.

Then $\exists\ a \in A$, s.t., $a \notin I$ and thus a is a unit $\Rightarrow a^{-1} \notin R$.

Now $a \in A$, $a^{-1} \in R$ so $aa^{-1} = 1 \in A$

$\Rightarrow A = R$ or that I is maximal

Let now M be any maximal ideal of R then $M \neq R$

Suppose $\exists$ some $m \in M$ s.t., $m \notin I$ then m^{-1} exists in R (by given condition) and so $mm^{-1} = 1 \in M \Rightarrow M = R$. which is not true. So there does not exist any $m \in M$ s.t., $m \notin I$ or in other words if $m \in M$ then $m \in I$.

$$\Rightarrow M \subseteq I \subseteq R$$

But I is maximal and therefore, $I = M$ proving our assertion.

Problem 24: *Let* $R = \mathbf{Z}[i] = \{a + ib | a, b \in \mathbf{Z}\}$. *Let* $M = < 2 + i >$ *then show that M is a maximal ideal of R.*

Solution: Let $M \subseteq < a + bi > \subseteq R$

Then $2 + i = (a + bi)(c + di)$

$2 - i = (a - bi)(c - di)$

So $5 = (a^2 + b^2)(c^2 + d^2)$

If $a^2 + b^2 = 1$, then $a = \pm 1$, $b = 0$ or $a = 0$, $b = \pm 1$

Thus, $a + bi = \pm 1$ or $\pm i$. In each case, $a + bi$ is a unit, so $< a + bi > = R$

If $c^2 + d^2 = 1$, then $c = \pm 1$, $d = 0$ or $c = 0$, $d = \pm 1$

Thus $2 + i = \pm(a + bi)$ or $(\pm i)(a + bi)$

$\Rightarrow (a + bi) = (\pm 1)^{-1}(2 + i)$ or $(\pm i)^{-1}(2 + i)$

In each case $a + bi \in <2 + i>$

So $(a + bi) \subseteq <2 + i> = M \subseteq <a + bi>$

$\Rightarrow M = <a + bi>$

Hence M is a maximal ideal of R.

Remark: Any ideal of $\mathbf{Z}[i]$ is of the type $<a + bi>$. See under Principal Ideal Domains in Chapter 9.

Theorem 14: *Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R iff $\frac{R}{M}$ is a field.*

Proof: Let M be maximal ideal of R. Since R is commutative ring with unity, $\frac{R}{M}$ is also a commutative ring with unity. Thus all that we need prove is that non zero elements of $\frac{R}{M}$ have multiplicative inverse.

Let $x + M \in \frac{R}{M}$ be any non zero element

then $x + M \neq M \Rightarrow x \notin M$

Let $xR = \{xr \mid r \in R\}$

It is easy to verify that xR is an ideal of R. Since sum of two ideals is an ideal, $M + xR$ will be an ideal of R.

Again as $x = 0 + x \cdot 1 \in M + xR$ and $x \notin M$ we find

$M \subset M + xR \subseteq R$

M maximal $\Rightarrow M + xR = R$

Thus $1 \in R \Rightarrow 1 \in M + xR$

$\Rightarrow 1 = m + xr$ for some $m \in M, r \in R$

$\Rightarrow 1 + M = (m + xr) + M$

$= (m + M) + (xr + M) = xr + M$

$= (x + M)(r + M)$

$\Rightarrow (r + M)$ is multiplicative inverse of $x + M$

Hence $\frac{R}{M}$ is a field.

Conversely, let $\frac{R}{M}$ be a field.

Let I be any ideal of R s.t., $M \subset I \subseteq R$

then $\exists$ some $a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is a non zero element of $\frac{R}{M}$, which being a field, means $a + M$ has multiplicative inverse. Let $b + M$ be its inverse. Then

$$\begin{aligned} & (a + M)(b + M) = 1 + M \\ \Rightarrow\ & ab + M = 1 + M \\ \Rightarrow\ & ab - 1 \in M \\ \Rightarrow\ & ab - 1 = m \text{ for some } m \in M \\ \Rightarrow\ & 1 = ab - m \in I \text{ (using def. of ideal)} \end{aligned}$$

$\Rightarrow I = R$ (ideal containing unity, equals the ring)

Hence M is maximal ideal of R.

Remarks: (*i*) $\frac{R}{M}$ being a field contains at least two elements and thus unity and zero elements of $\frac{R}{M}$ are different *i.e.*, $0 + M \neq 1 + M$ *i.e.*, $1 \notin M$ or that $M \neq R$.

(*ii*) In the converse part of the above theorem we do not require R to have unity or it to be commutative, *i.e.*, if R is a ring and M is an ideal of R s.t., $\frac{R}{M}$ is a field then M is maximal.

Suppose I is an ideal of R s.t., $M \subset I \subseteq R$. Then $\exists\ a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is non zero element of $\frac{R}{M}$ and therefore has multiplicative inverse, say, $b + M$. If $c + M$ be unity of $\frac{R}{M}$. (Note $\frac{R}{M}$ can have unity even if R doesn't have unity. See exercises on page 394).

Now $(a + M)(b + M) = c + M$.

$\Rightarrow$ $ab + M = c + M$

$\Rightarrow$ $c - ab \in M \subset I$

But $a \in I \Rightarrow ab \in I$ and so $(c - ab) + ab \in I$

$\Rightarrow$ $c \in I$

Let $r \in R$ be any element

Then $(r + M)(c + M) = r + M$

$\Rightarrow$ $rc + M = r + M$

$\Rightarrow$ $r - rc \in M \subset I$

Since $c \in I$, $rc \in I$ and thus $(r - rc) + rc \in I \Rightarrow r \in I \Rightarrow R \subseteq I$.

Hence $I = R$ and thus M is maximal ideal of R.

(*iii*) Again, the condition of commutativity is essential in the theorem is established by the fact that we can have M, a maximal ideal in R where R/M is not a field and R is a non commutative ring with unity. See next problem.

Cor.: A commutative ring R with unity is a field iff it has no proper (non trivial) ideals.

If R is a field then it has no proper ideals (see exercise 13 on page 351).

Conversely, if R has no proper ideals then $\{0\}$ must be a maximal ideal. Thus $\frac{R}{\{0\}}$ is a field and as $\frac{R}{\{0\}} \cong R$, R is a field.

Problem 25: *Let R be the ring of $n \times n$ matrices over reals. Show that R has only two ideals namely $\{0\}$ and R. Hence show that $\{0\}$ is maximal ideal of R.*

Solution: Let J be a non zero ideal of R. Let A be a non zero matrix in J. Since $A \neq 0$, it has some non zero entry. Suppose $A = (a_{ij})$ and suppose $a_{rs} \neq 0$ in A.

If E_{ij} denotes the unit matrix in R whose (i, j)th entry is 1 and 0 elsewhere

then $E_{ij} E_{kr} = 0$ if $j \neq k$

$= E_{ir}$ if $j = k$

Now $A = a_{11}E_{11} + a_{12}E_{12} + \ldots + a_{nn} E_{nn}$

Consider $E_{ir} A E_{si} = E_{ir}(a_{11}E_{11} + a_{12}E_{12} + \ldots + a_{nn} E_{nn})E_{si}$

$= E_{ir}(a_{rs} E_{rs})E_{si}$

$= a_{rs} E_{ir} E_{si}$

$= a_{rs} E_{ii} \in I$ as $A \in I \quad \forall i$

So $(a_{rs}^{-1} E_{ii})(a_{rs} E_{ii}) \in J$

$\Rightarrow E_{ii} \in I, \quad \forall i = 1, 2, 3, \ldots n$

Thus identity matrix I in R can be written as $I = E_{11} + E_{12} + \ldots + E_{nn} \in J$.

So unity of R belongs to J or that $J = R$. Hence $\{0\}$ and R are the only ideals of R and so $\{0\}$ is maximal ideal of R.

Note: Since $R \cong \frac{R}{\{0\}}$, and R is not a field, we find $\frac{R}{\{0\}}$ is not a field even though $\{0\}$ is maximal. See remark above.

Definition:

Prime Ideal: An ideal P of a ring R is called a *prime ideal* if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Example 8: $\{0\}$ in the ring $\mathbf{Z}$ of integers is a prime ideal as $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

It is an example of a prime ideal which is not maximal.

Example 9: $H_4 = \{4n \mid n \in \mathbf{Z}\}$ we've seen is a maximal ideal in the ring $\mathbf{E}$ of even integers. H_4, however, is not a prime ideal as $2 \cdot 2 = 4 \in H_4$ but $2 \notin H_4$.

In fact, H_4 is neither a maximal nor a prime ideal in $\mathbf{Z}$. (See exercise 1 also)

Example 10: In example 7, ideal M is a prime ideal of R^c as let $f, g \in R^c$ then if $fg \in M$, we get $fg(1/2) = 0$

$\Rightarrow f(1/2)\, g(1/2) = 0$

$\Rightarrow f(1/2) = 0$ or $g(1/2) = 0 \Rightarrow f \in M$ or $g \in M$.

Example 11: $H_p = \{pn \mid n \in \mathbf{Z}\}$ will be a prime ideal in $\mathbf{Z}$ for any prime p.

It will also be a maximal ideal in $\mathbf{Z}$ (see exercise 1 on page 394).

Remark: In view of the above examples and exercise 1 on page 394, we observe that in the ring $\mathbf{Z}$ of integers

(i) every ideal in $\mathbf{Z}$ is generated by some $n \in \mathbf{Z}$.

(ii) An ideal in $\mathbf{Z}$ is maximal iff it is generated by a prime.

(iii) One can show that in $\mathbf{Z}$ a prime ideal is either generated by a prime or is the zero ideal. Consequently, a non zero ideal in $\mathbf{Z}$ is prime iff it is maximal.

Let $P = < n >$ and suppose n is prime.

Let $ab \in p = < n >$, then $ab = kn \Rightarrow n \mid ab$

$\Rightarrow n \mid a$ or $n \mid b$

$\Rightarrow a \in P$ or $b \in P$

or that P is prime ideal.

Conversely, let $P = < n >$ be a prime ideal

Suppose n is not a prime and

$n = ab, \quad 1 < a, b < n$

Let $A = < a >, B = < b >$, then $P \subseteq A$ and $P \subseteq B$

Now $ab \in P$ and P is prime

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$

$\Rightarrow$ either $A = P$ or $B = P$

i.e, either $b = 1$ or $a = 1$ or that n is a prime.

(iv) $\{0\}$ is thus a prime ideal in $\mathbf{Z}$ but not maximal whereas every maximal ideal is prime.

Theorem 15: *Let R be a commutative ring. An ideal P of R is prime iff $\frac{R}{P}$ is an integral domain.*

Proof: Let P be a prime ideal of R

Let $(a + P)(b + P) = 0 + P$

Then $ab + P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow a + P = P$ or $b + P = P$

thus $\frac{R}{P}$ is integral domain.

Conversely, let $\frac{R}{P}$ be an integral domain.

Let $ab \in P$ then $ab + P = P$

$\Rightarrow (a + P)(b + P) = P$

$\Rightarrow$ $a + P = P$ or $b + P = P$ (R/P is an integral domain)

$\Rightarrow$ $a \in P$ or $b \in P$

Hence the result.

Theorem 16: *Let R be a commutative ring. An ideal P of R is a prime ideal if and only if for two ideals A, B of R, $AB \subseteq P$ implies either $A \subseteq P$ or $B \subseteq P$.*

Proof: Let P be a prime ideal of R and let $AB \subseteq P$ for two ideal A, B of R.

Suppose $A \not\subseteq P$ then $\exists$ some element $a \in A$ s.t., $a \notin P$.

Since $AB \subseteq P$, we get in particular

$aB \subseteq P$

$\Rightarrow$ $ab \in P$ for all $b \in B$

Since P is prime, we get either $a \in P$ or $b \in P$ but $a \notin P$, hence $b \in P$ for all $b \in B$.

$\Rightarrow$ $B \subseteq P$

Conversely, we show P is prime. Let $ab \in P$.

Let A and B be the ideals generated by a and b then $A = (a)$, $B = (b)$. If $x \in AB$ is any element then it is of the type

$$x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n \qquad a_i \in A,\ b_i \in B$$
$$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \ldots\ldots + (\alpha_n a)(\beta_n b)$$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a)$, $b_i \in B = (b)$

Thus $$x = (\alpha_1\beta_1)(ab) + (\alpha_2\beta_2)(ab) + \ldots\ldots + (\alpha_n\beta_n)(ab)$$ (R is commutative)

$$x = (\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots\ldots + \alpha_n\beta_n)ab$$

Since $ab \in P$, P is an ideal, all multiples of ab are in P. Thus $x \in P$

i.e., $AB \subseteq P$

$\Rightarrow$ $A \subseteq P$ or $B \subseteq P$

$\Rightarrow$ $(a) \subseteq P$ or $(b) \subseteq P$

$\Rightarrow$ $a \in P$ or $b \in P \Rightarrow P$ is prime.

Problem 26: *Let R be a commutative ring with unity such that $a^2 = a \ \forall a \in R$. If I be any prime ideal of R, Find all the elements of R/I.*

Solution: Since I is a prime ideal of R, R/I is an integral domain, and $1 + I$ is unity of R/I.

Let $r + I \in R/I$ be any member

then $(r + I)^2 = r^2 + I = r + I$ (given condition)

$\Rightarrow$ $(r + I)[(r + I) - (1 + I)] = 0 + I$

But R/I is an integral domain and therefore, either $r + I = 0 + I$ or $(r + I) = 1 + I$

or that R/I contains only two elements $0 + I$ and $1 + I$.

(See Problem 22 on page 334).

Problem 27: *Let R be a non zero commutative ring with unity. If every ideal of R is prime show that R is a field and conversely.*

Solution: To show that R is a field, we need show that every non zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ st., $ab = 0$

Then $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

i.e., $a = 0$ or $b = 0$

thus R is an integral domain.

Let now $a \in R$ be any non zero element and let

$$a^2R = \{a^2r \mid r \in R\}$$

then a^2R is an ideal of R (Verify!) and is therefore prime ideal.

Now $a \cdot a = a^2 = a^2 \cdot 1 \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

$\Rightarrow a(1 - ab) = 0$

$\Rightarrow 1 - ab = 0$ as $a \neq 0$

$\Rightarrow b$ is multiplicative inverse of a.

Hence R is a field.

Converse follows easily as a field R has no ideals except $\{0\}$ and R.

Problem 28: *Let R be a commutative ring with unity. Show that every maximal ideal of R is prime.*

Solution: We know that an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

Thus if M is maximal, then $\frac{R}{M}$ is a field and hence an integral domain.

$\Rightarrow M$ is a prime ideal (theorem 15).

Problem 29: *Let R be a commutative ring with unity and let M be a maximal ideal of R such that $M^2 = \{0\}$. Show that if N is any maximal of R then $N = M$.*

Solution: Let $m \in M$ be any element

then $m \cdot m \in M^2 = (0)$

$\Rightarrow m^2 = 0 \in N$ (N is an ideal)

By previous problem, N will be prime

$\Rightarrow m \in N$

$\Rightarrow M \subseteq N$

Thus $M \subseteq N \subseteq R$

Since M is maximal, $N = M$ or $N = R$

But N is maximal in R, thus $N \neq R$

Hence $N = M$.

Problem 30: *Show that in a Boolean ring R, every prime ideal $P \neq R$ is maximal.*

Solution: Let P be prime and I be any ideal s.t.,

$$P \subset I \subseteq R$$

then $\exists$ some $x \in I$, s.t., $x \notin P$ and as $x \in R$, $x^2 = x$.

Let now, $y \in R$ be any element, then

$$x^2y = xy$$

$$\Rightarrow x(xy - y) = 0 \in P \qquad (P \text{ is an ideal})$$

$$\Rightarrow xy - y \in P \text{ as } x \notin P \text{ and } P \text{ is prime}$$

$$\Rightarrow xy - y = p \text{ for some } p \in P$$

Then $y = xy - p \in I$

as $x \in I$, $y \in R$, $xy \in I$ and also $p \in P \subseteq I$,

Thus $y \in I$

$$\Rightarrow R \subseteq I \Rightarrow I = R \Rightarrow P \text{ is maximal.}$$

Problem 31: *Show by an example that we can have a finite commutative ring in which every maximal ideal need not be prime.*

Solution: Consider the ring $R = \{0, 2, 4, 6\}$ under addition and multiplication modulo 8.

Let $M = \{0, 4\}$ then M is easily seen to be an ideal of R.

Again as $2 \otimes 6 = 4 \in M$ but $2, 6 \notin M$, we find M is not a prime ideal. We show M is maximal.

Let $M \subseteq N \subseteq R$, where N is an ideal of R.

Since $< M, + >$ will be a subgroup of $<N, + >$, by Lagrange's theorem $o(M) \mid o(N)$. Similarly, $o(N) \mid o(R) = 4$

i.e., $2 \mid o(N),\ o(N) \mid 4$

i.e., $o(N) = 2$ or 4

if $o(N) = 2$, then $M = N$ as $M \subseteq N$

if $o(N) = 4$, then $N = R$ as $N \subseteq R$

Hence M is maximal ideal of R.

Remark: In case the finite commutative ring contains unity, then every prime ideal is maximal. See exercises.

Problem 32: *Let $R = \mathbf{Z}[i]$. Show that*

$M = \{3a + 3bi \mid a\ b \in \mathbf{Z}\}$ is a maximal ideal of R whereas $N = \{5a + 5bi \mid a, b \in \mathbf{Z}\}$ is not.

Solution: It is easy to show that M is an ideal of R. Suppose I is an ideal of R such that

$$M \subsetneq I \subseteq R$$

Then $\exists\ r + si \in I$. s.t., $r + si \notin M$

So either $3 \nmid r$ or $3 \nmid s$

Suppose $3 \nmid r$, then $(3, r) = 1$ and therefore,

$r^2 \equiv 1 \pmod 3$. Let $s = 3q + u, \quad 0 \leq u < 3$

So $s \equiv u \pmod 3$

$s^2 \equiv u^2 \pmod 3$, where $u = 0, 1$ or 2

$\equiv 0$ or $1 \pmod 3$

So $r^2 + s^2 \equiv 1$ or $2 \pmod 3$

Let $t = (r + si)(r - si) = r^2 + s^2$

then $3 \nmid t$, so $(3, t) = 1 \quad \Rightarrow 3a + tb = 1$ for some $a, b \in \mathbf{Z}$. Since $t \in I$, $3a \in M$ we find $3a \in I$.

$\Rightarrow \quad 1 \in I \Rightarrow I = R \Rightarrow M$ is maximal.

Let now $I = \langle 2 + i \rangle$, then

$5 = (2 + i)(2 - i) \in I$

i.e., $N \subseteq I \subseteq R$

If $I = N$, then $2 + i \in N$ which is not true

If $I = R$, then $I = (2 + i)(a + bi)$

$I = (2 - i)(a - bi)$

$\Rightarrow I = 5a^2 + 5b^2, \ a, b \in \mathbf{Z}$

which is not possible.

Hence N will not be a maximal ideal of R.

Problem 33: *Let $A \neq R$ be an ideal of R, then for any $x \in R$, $x \notin A$, if $A + (x) = R$, show that A is maximal ideal of R and conversely.*

Solution: Let I be an ideal of R, such that

$A \subset I \subseteq R$

then $\exists$ some $x \in I$, s.t., $x \notin A$

Let (x) be the ideal generated by x.

then $A + (x)$ is an ideal of R.

Also by given condition $A + (x) = R$

Again $A \subseteq I, x \in I \Rightarrow (x) \subseteq I$

thus $A + (x) \subseteq I$

$\Rightarrow R \subseteq I \Rightarrow I = R$

i.e., A is maximal.

Conversely, let A be maximal, $A \neq R$. Let $x \in R$, $x \notin A$.

Then $I = A + (x)$ being sum of two ideals is an ideal of R and $A \subseteq A + (x) \subseteq R$.

Since A is maximal, $A \neq A + (x)$ as $x \notin A$. Hence $A + (x) = R$.

Problem 34: *Show that* $I = <2 + 2i>$ *is not a prime ideal of* $\mathbf{Z}[i]$. *Find all elements of* $\frac{\mathbf{Z}[i]}{I}$ *What is characteristic of* $\frac{\mathbf{Z}[i]}{I}$?

Solution: Since $2 + 2i \in I$, we find $2(1 + i) \in I$

Now if $2 \in I$, then $2 = (a + bi)(2 + 2i)$

$\Rightarrow 1 = (a + bi)(1 + i)$

and also $1 = (a - bi)(1 - i)$

$\Rightarrow 1 = (a + bi)(1 + i)(a - bi)(1 - i) = 2(a^2 + b^2)$

which is not possible.

So $2 \notin I$

Again if $1 + i \in I$, then $1 + i = (a + bi)(2 + 2i)$

$\Rightarrow 1 = 2(a + bi)$ giving $1 = 2a$

which is again not possible.

Hence I is not a prime ideal.

Let now $(a + bi) + I$ be any element of $\frac{\mathbf{Z}[i]}{I}$.

Since $4 + I = (2 + 2i)(1 - i) + I = I$

as $(2 + 2i) \in I \Rightarrow (1 - i)(2 + 2i) \in I$

we find $4 \in I$

Now $a = 4q_1 + r_1 \qquad 0 \leq r_1 < 4$

$b = 4q_2 + r_2 \qquad 0 \leq r_2 < 4$

$\Rightarrow a + bi = (4q_1 + r_1) + (4q_2 + r_2)i = 4(q_1 + q_2 i) + (r_1 + r_2 i)$

$\Rightarrow (a + bi) + I = (r_1 + r_2 i) + I$ [as $4 \in I \Rightarrow 4(q_1 + q_2 i) \in I$] $0 \leq r_1, r_2 < 4$

We can thus list down all the members of $\frac{\mathbf{Z}[i]}{I}$. These being

$0 + I$	$1 + I$	$2 + I$	$3 + I$
$0 + i + I$	$1 + i + I$	$2 + i + I$	$3 + i + I$
$0 + 2i + I$	$1 + 2i + I$	$2 + 2i + I$	$3 + 2i + I$
$0 + 3i + I$	$1 + 3i + I$	$2 + 3i + I$	$3 + 3i + I$

Are some of these members equal? To answer this we notice,

Since $(2 + 2i) \in I = <2 + 2i>$, we have

$(2 + 2i) + I = I = 0 + I$

and so in the quotient ring, $2 + 2i$ can be taken as 0 or that $2 + 2i = 0$, i.e., $2i = -2$ using this we find

$0 + 2i + I = 2i + I = -2 + I = -2 + 4 + I = 2 + I$

$1 + 2i + I = 1 - 2 + I = -1 + I = -1 + 4 + I = 3 + I$ etc.,

and we are left with only eight members (the first two rows)

It is easy to see that $4a = 0 \quad \forall a \in \frac{\mathbf{Z}[i]}{I}$

$$[4(3 + i + I) = 12 + 4i + I = 4i + I = 0 + I]$$

Hence $\text{ch}\frac{\mathbf{Z}[i]}{I} = 4.$

Definition: An ideal I of a commutative ring R is called *semi prime ideal* if $a^2 \in I \Rightarrow a \in I$, for all $a \in R$

Clearly then every prime ideal is semi prime.

Example 12: Consider the ideal $I = \{6n \mid n \in \mathbf{Z}\}$ in the ring of integers. Suppose $a^2 \in I$

Then a^2 is a multiple of 6

i.e., $6 \mid a^2$

Since $2 \mid 6$, we find $2 \mid a^2 \Rightarrow 2 \mid a$ (as 2 is prime)

Similarly $3 \mid a$

$\Rightarrow 6 \mid a$ as g.c.d.(2, 3) = 1

$\Rightarrow a \in I$

Hence I is semi prime, but I is not prime as $2 \cdot 3 = 6 \in I$ but $2, 3 \notin I$.

Exercises

1. In the ring of integers, show that every ideal is generated by some integer. Show further that an ideal is maximal iff it is generated by a prime.
2. Show that intersection of two prime ideals may not be a prime ideal.
3. Show that intersection of two prime ideals is a prime ideal iff one of them is contained in the other. What can be said about sum of two prime ideals?
4. Show that intersection of two prime ideals is a semi prime ideal and so is the intersection of two semi prime ideals.
5. Let R be a commutative ring. Let I be an ideal of R and let P be a prime ideal of I. Show that P is an ideal of R.
6. Let N be the set of all nilpotent elements of a commutative ring R. Show that $N \subseteq P$ for each prime ideal P of R.
7. Show that a commutative ring R is an integral domain iff $\{0\}$ is a prime ideal.
8. Let R be a finite commutative ring with unity. Show that every prime ideal of R is a maximal ideal.
9. Show that $M = \{0, 3, 6, 9\}$ mod 12 is a maximal ideal of $\mathbf{Z}_{12}$.
10. Let R be a Boolean ring with unity and M be any proper ideal of R. Then show that R/M is a Boolean ring with unity and $R/M \cong \frac{\mathbf{Z}}{(2)}$ if and only if M is maximal.

11. Let $\{P_i\}$ $i \in X$ be a chain of prime ideals. Show that $\bigcap_i P_i$ and $\bigcup_i P_i$ are prime ideals. (By a chain, we mean either $P_i \subseteq P_j$ or $P_j \subseteq P_i$ for all $i, j \in X$).

12. Let $P \neq R$ be an ideal of R. Show P is prime ideal of R iff $R - P$ is closed under multiplication.

13. Show that an ideal A is maximal iff the pair A, B for all ideals $B \not\subseteq A$ is maximal. (See problem 33 also).

14. Show that an ideal P in a commutative ring R with unity is prime iff for ideals A, B in R, $P \subsetneq A$, $P \subsetneq B \Rightarrow AB \not\subseteq P$.

15. Show that $M = \{0, 6\}$ is a maximal ideal of the ring $R = \{0, 2, 4, 6, 8, 10\}$ mod 12 and hence R/M is a field. (Notice R has no unity, whereas $4 + M$ is unity of R/M).

16. Find all the ideals of $\mathbf{Z}_{12}$, $\mathbf{Z}_{36}$. Which of these are maximal?

A Quick Look at what's been done

- If I is an ideal of a ring R then the **quotient ring** or **factor ring** of R is defined to be the set of all left(or right) cosets of I in R and is denoted by the symbol R/I. Similar results as proved in quotient groups hold in quotient rings also.
- A mapping f: $R \to R'$ is called a homomorphism if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.
- **Fundamental theorem of ring homomorphism** states that if f:$R \to R'$ is an onto homomorphism then R' is isomorphic to R/Ker f.
- If there exists a one-one homomorphism from a ring R to a ring R' we say, R is embedded (imbedded) into R'.
- Any ring can be embedded into a ring with unity.
- Any integral domain can be embedded into a field.
- Any ring can be embedded into a ring of endomorphisms of some additive abelian group.
- An ideal M ($\neq R$) of a ring R is called a **maximal ideal** of R if whenever A is an ideal of R,s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.
- If R is a commutative ring with unity then an ideal M of R is maximal iff R/M is a field.
- An ideal P of a ring R is called a **prime ideal** if $ab \in P \Rightarrow a \in P$ or $b \in P$.
- If R is a commutative ring then an ideal P of R is a prime ideal iff R/P is an integral domain.

9

Euclidean and Factorization Domains

Introduction

In this chapter we talk about divisibility in rings in a generalized form, introduce the reader to Euclidean Domains, Principal Ideal Domains (PIDs) and Unique Factorization Domains,(UFDs), prime and irreducible elements, polynomial rings, irreducibility criteria over rationals, Noetherian rings.

Definition: Let R be a commutative ring. $a, b \in R$, $a \neq 0$, then we say $a \mid b$ (a divides b) if $\exists\ c \in R$ s.t., $b = ac$. Also then a is called a *factor* of b.

If $a, b \in R$ then an element $d \in R$ is called *greatest common divisor* (or highest common factor) of a and b if

(i) $d \mid a, d \mid b$

(ii) whenever $c \mid a, c \mid b$ then $c \mid d$

and in that case we write d = g.c.d. (a, b). In fact sometimes only (a, b) is used to denote g.c.d. of a and b.

Remark: One can prove that

(i) If $a \mid b, b \mid c$ then $a \mid c$

(ii) If $a \mid b, a \mid c$ then $a \mid b \pm c$

(iii) If $a \mid b$ then $a \mid bx$ for all $x \in R$

(iv) If R has unity then $1 \mid x$ for all $x \in R$ and if a is a unit then $a \mid x$ for all $x \in R$.

Example 1: Consider the ring $R = \{0, 1, 2, ..., 7\}$ modulo 8

then since $2 \otimes 3 = 6$, $2 \mid 6$

$2 \otimes 2 = 4$, $2 \mid 4$

Again, if $c \mid 4, c \mid 6$ then $c \mid 6 - 4 \Rightarrow c \mid 2$

Thus g.c.d.$(4, 6) = 2$

Also as $6 = 6 \otimes 1, 4 = 6 \otimes 6$

we find $6 \mid 6$ and $6 \mid 4$

Now if $c \mid 6$, $c \mid 4$

then as $c \mid 6$, we get g.c.d.$(4, 6) = 6$. Thus it is possible to have more than one g.c.d. for the same pair of elements.

Example 2: In the ring **E** of even integers we notice 4 and 6 do not have a g.c.d.

2 (the only possibility) is not a g.c.d. of 4, 6 as $2 \nmid 6$ in **E**. Indeed $6 = 2 \cdot 3$ but then $3 \notin \mathbf{E}$. Of course, 2 is the unique g.c.d. of 4 and 6 in **Z**, the ring of integers.

Definition: Let R be a commutative ring. A non zero element $l \in R$ is called *least common multiple* (l.c.m.) of two (non zero) elements $a, b \in R$ if

(i) $a \mid l$, $b \mid l$

(ii) if $a \mid x$, $b \mid x$ then $l \mid x$

We denote l by l.c.m. $(a, b) = [a, b]$

Just as proved above one can show that a pair of elements in a ring may not have an l.c.m. and a pair could have more than one l.c.m. See exercises.

Definition: Let R be a commutative ring with unity. Then $a, b \in R$ are called *associates* if $b = ua$ for some unit u in R.

We recall here that by a unit we mean an element which has multiplicative inverse. The above definition will not be 'complete' unless we show that the relation 'is an associate of' is an equivalence relation. If we denote the relation by $\sim$

then $a \sim a$ as $a = 1.\ a$ and 1 is a unit

$$a \sim b \Rightarrow b = ua \text{ where } u \text{ is a unit}$$
$$\Rightarrow u^{-1} b = a$$
$$\Rightarrow b \sim a$$

Indeed u^{-1} will be a unit if u is a unit.

Finally $a \sim b,\ b \sim c \Rightarrow b = ua$

$$c = vb \text{ for units } u, v$$

Since $c = vb = v(ua) = (vu)a$

Showing $c \sim a$

as $uu^{-1} = 1,\ vv^{-1} = 1 \Rightarrow (vu)\ (vu)^{-1} = (vu)\ (u^{-1}v^{-1}) = 1$

we notice vu is a unit.

Example 3: $3i - 4$ is an associate of $4i + 3$ in complex nos.

Problem 1: *Let R be an integral domain with unity and a, b ∈ R be non zero elements such that a | b and b | a, then a and b are associates and conversely.*

Solution: $a \mid b \Rightarrow b = xa$

$b \mid a \Rightarrow a = yb$ for some $x, y \in R$

$\therefore$ $b = xa = x(yb)$

$\Rightarrow$ $b(1 - xy) = 0$

$\Rightarrow$ $1 - xy = 0$ as $b \neq 0$

$\Rightarrow$ y is a unit in R and $a = yb$, and thus a, b are associates.

Conversely, if a, b are associates then $\exists$ a unit u, s.t., $a = bu$ (and so $au^{-1} = b$).

$\Rightarrow$ $b \mid a$ and $a \mid b$.

Theorem 1: *Let R be an integral domain with unity. If d_1 = g.c.d.(a, b) in R then d_2 is also a* g.c.d.(a, b) *iff d_1 and d_2 are associates.*

Proof: One may remark here that we prove this result only after assuming the existence of g.c.d.

Let d_1 and d_2 be both g.c.d.(a, b).

Then $d_1 \mid a$, $d_1 \mid b$

and $d_2 \mid a$, $d_2 \mid b$

by definition, we get $d_1 \mid d_2$ and $d_2 \mid d_1$

$\Rightarrow$ d_1 and d_2 are associates. (using problem 1)

Conversely, let d_1 = g.c.d.(a, b) and d_2 be an associate of d_1.

Then $ud_2 = d_1$ for some unit u

$\Rightarrow$ $d_2 \mid d_1$ and as $d_1 \mid a$, $d_1 \mid b$

we find $d_2 \mid a$ and $d_2 \mid b$

Let $x \mid a$, $x \mid b$ then $x \mid d_1$ as d_1 is g.c.d. (a, b)

Also as $d_2 = d_1u^{-1}$

$d_1 \mid d_2$

and thus $x \mid d_2$

$\Rightarrow$ d_2 = g.c.d.(a, b).

Remark: In example 1 on page 396, 2 and 6 are g.c.d. of 4 and 6. We observe there that 2 and 6 are associates, as $6 = 2 \otimes 3$ and 3 is a unit in $\mathbf{Z}_8$ ($3 \otimes 3 = 1$).

Theorem 2: *Let R be an integral domain with unity. If l_1 =* l.c.m.(a, b) *in R then l_2 is also an* l.c.m.(a, b) *iff l_1 and l_2 are associates.*

Proof: Follows similarly as the above theorem.

Problem 2: *Let R be an integral domain with unity. If* g.c.d.$(a, b) = d$ *for $a, b \in R$ then cd* and g.c.d.(ca, cb) are associates.

Solution: Let g.c.d.$(ca, cb) = d'$

Since $d \mid a$, $a = dk$

$\Rightarrow ac = dkc = cdk$

$\Rightarrow cd \mid ca$

Similarly $cd \mid cb \Rightarrow cd \mid d' \Rightarrow d' = cdt$

Again $d' \mid ca \Rightarrow ca = d's$

$\Rightarrow ca = d's \Rightarrow cdts$

$\Rightarrow a = (dt)s \Rightarrow dt \mid a$

Similarly $dt \mid b$

$$\Rightarrow dt \mid d \Rightarrow d = dtp \Rightarrow d(1 - tp) = 0$$
$$\Rightarrow 1 = tp \Rightarrow t \text{ is a unit}$$
$$\Rightarrow \text{g.c.d.}(ca, cb) = d' = cdt$$

i.e., cd and d' are associates.

Euclidean Domains

Definition: An integral domain R is called a *Euclidean domain* (or a Euclidean ring) if for all $a \in R$, $a \neq 0$ there is defined a non –ve integer $d(a)$ s.t.,

(i) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $d(a) \leq d(ab)$

(ii) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $\exists$ t and r in R s.t.,

$$a = tb + r$$

where either $r = 0$ or $d(r) < d(b)$.

Example 4: Consider the integral domain $< \mathbf{Z}, +, . >$ of integers. For any $0 \neq a \in \mathbf{Z}$, define $d(a) = \mid a \mid$, then $d(a)$ is non –ve integer.

Again, let $a, b \in \mathbf{Z}$ be any elements s.t., $a \neq 0$, $b \neq 0$

then $d(a) = \mid a \mid$

$d(ab) = \mid ab \mid = \mid a \mid \mid b \mid$

thus $d(a) \leq d(ab)$ as $\mid a \mid \leq \mid a \mid \mid b \mid$

Again let $a, b \in \mathbf{Z}$ $(a, b \neq 0)$

Suppose $b > 0$, then it is possible to write

$$a = tb + r \quad \text{where } 0 \leq r < b$$
$$t, r \in \mathbf{Z}$$

If $r \neq 0$ then $r < b \Rightarrow \mid r \mid < \mid b \mid$

$$\Rightarrow d(r) < d(b)$$

If $b < 0$ then $(- b) > 0$, $\therefore \exists$ $t, r \in \mathbf{Z}$ s.t.,

$$a = (- b)t + r \qquad \text{where } 0 \leq r < - b$$
$$a = (- t)\, b + r$$

and if $r \neq 0$, $r < - b \Rightarrow \mid r \mid < \mid b \mid$

$$\Rightarrow d(r) < d(b)$$

Hence $< \mathbf{Z}, +, . >$ is a Euclidean domain.

Remarks: (i) When we say, in the definition, that $\exists$ a non –ve integer $d(a)$ for any $0 \neq a$, we mean, $\exists$ a function d from $R - \{0\}$ to $\mathbf{Z}^+ \cup \{0\}$ where $\mathbf{Z}^+$ is set of +ve integers. This function d is called Euclidean valuation on R. Also the last condition in the definition is called *Euclidean algorithm*.

(ii) We can show that the t and r mentioned in the last (Euclidean algorithm) condition in the definition of Euclidean domain are uniquely determined iff

$$d(a + b) \leq \text{Max. } \{d(a), d(b)\}.$$

Let $d(a + b) \leq \text{Max. } \{d(a), d(b)\}$ and

Suppose $a = tb + r = t_1 b + r_1$

Let $r_1 - r \neq 0$, then $b(t - t_1) = r_1 - r \neq 0$, and so $t - t_1 \neq 0$

Now
$$\begin{aligned} d(b) &\leq d(b(t - t_1)) \\ &= d(r_1 - r) \\ &\leq \text{Max. } \{d(r_1), d(-r)\} \qquad \text{(given condition)} \\ &= \text{Max. } \{d(r_1), d(-r)\} \\ &< d(b) \text{ which is not possible.} \end{aligned}$$

Thus $r_1 - r = 0 \Rightarrow b(t - t_1) = 0$

or $t - t_1 = 0$ as $b \neq 0$

$\Rightarrow$ $t = t_1$ and $r = r_1$

Conversely, let t, r be uniquely determined and suppose

$$d(a + b) > \text{Max. } \{d(a), d(b)\} \text{ for some } a, b \text{ (non zero) in } R.$$

Now $b = 0(a + b) + b = 1 \,.\, (a + b) - a$

Also $d(-a) = d(a) < d(a + b)$

and $d(b) < d(a + b)$

Thus for b, $1 \in R$, $\exists\ t = 0$, $r = b$ or $t_1 = 1$, $r_1 = -a$ s.t., $b = t.1 + r$, $b = t_1 \cdot 1 + r_1$ where $r \neq r_1$ (as $a + b \neq 0$) $t \neq t_1$, a contradiction to the uniqueness.

Hence $d(a + b) \leq$ Max. $(d(a), d(b))$. Note that a Euclidean domain contains unity (see cor. ahead).

Theorem 3: *Let R be a Euclidean domain and let A be an ideal of R, then $\exists$ $a_o \in A$ s.t., $A = \{a_o x \mid x \in R\}$.*

Proof: If $A = \{0\}$, we can take $a_o = 0$.

Suppose $A \neq \{0\}$, then $\exists$ at least one $0 \neq a \in A$.

Let $a_o \in A$ be such that $d(a_o)$ is minimal. [Existence is ensured by the well ordering principle which states that every non empty subset of non –ve integers has least element.]

We claim A is generated by this a_o.

Let $a \in A$, $a \neq 0$ then by definition, $\exists\ t, r \in R$, s.t.,

$$a = a_o t + r \quad \text{where either } r = 0 \text{ or } d(r) < d(a_o)$$

Suppose $r \neq 0$

Then $a_o \in A$, $t \in R \Rightarrow ta_o \in A$

$\therefore$ $a \in A$, $ta_o \in A \Rightarrow a - ta_o \in A$

$$\Rightarrow r \in A$$

But $d(a_o)$ is the smallest d-value in A and $d(r) < d(a_o)$, which leads to a contradiction. Hence

$$r = 0$$

$$\Rightarrow a = ta_o$$

Thus any $a \in A$ can be put in the form ta_o

$$\Rightarrow A \subseteq \{a_o x \mid x \in R\}$$

But $\{a_o x \mid x \in R\} \subseteq A$ as $a_o \in A \Rightarrow xa_o \in A$ for all $x \in R$

Hence $A = \{a_o x \mid x \in R\}$

which proves the theorem.

Definition: Such an ideal A which contains multiples of an element a_o, including a_o of R is called a *Principal Ideal* of R, generated by a_o. We denote this by $A = (a_o)$. (See page 342 also)

In other words, the smallest ideal of R which contains a_o is called Principal Ideal generated by a_o.

In view of this definition the previous theorem will read as

Theorem 4: *Every ideal in a Euclidean domain is a principal ideal.*

Cor.: A Euclidean domain possesses unity.

Proof: Let R be a Euclidean domain then R is its own ideal and, therefore, R is generated by some element r_o of R.

Thus each element of R is a multiple of r_o.

In particular r_o is a multiple of r_o

i.e., $r_o = r_o k$ for some $k \in R$

Now if $a \in R$ is any element then as $R = (r_o)$

$a = xr_o$ for some x

hence $ak = (xr_o)\, k = x(r_o k) = xr_o = a$

i.e., k is unity of R.

Definition: An integral domain R with unity is called a *Principal Ideal Domain* (PID) if every ideal of R is a principal ideal.

In fact, if R happens to be a commutative ring with unity with above condition, we call it a principal ideal ring.

In view of the previous theorem and cor., we get

Theorem 5: *A Euclidean domain is a PID.*

In particular thus, the ring $< \mathbf{Z}, +, \cdot >$ of integers is a PID. This result follows independently if we recall (see exercise 1, page 394) that every ideal in $< \mathbf{Z}, +, \cdot >$ is a principal ideal.

Remarks: (*i*) A field F is always a PID as it has only two ideals F and $\{0\}$. F is generated by 1 and $\{0\}$ by 0.

(*ii*) One can show that there exist PIDs which are not Euclidean domains. In particular, $\mathbf{Z}[\sqrt{-19}] = \{a + \sqrt{-19}\, b \mid a, b \in \mathbf{Z}\}$ where a, b are both odd or both even, is a PID but not a Euclidean domain.

(*iii*) See page 431 for an example of an ideal which is not principal.

Problem 3: *Show that in a PID every non-zero prime ideal is maximal.*

Solution: Let $P = (p)$, $p \neq 0$, be a non zero prime ideal in a PID R.

Suppose $P \subseteq Q = (q) \subseteq R$

Then $p \in P \subseteq Q = (q)$

$\Rightarrow p = qr$

$\Rightarrow qr \in P$

$\Rightarrow q \in P$ or $r \in P$

If $q \in P$ then all multiples of q are in $P \Rightarrow Q \subseteq P$

thus $Q = P$

If $r \in P$ then $r = pt \Rightarrow r = qrt$

$\Rightarrow r(1 - qt) = 0$

$\Rightarrow 1 = qt \quad (r \neq 0)$

But $q \in Q$, $t \in R \Rightarrow qt \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$

Note $r = 0$ would mean $p = q \cdot 0 \Rightarrow p = 0 \Rightarrow P = (0)$.

Remark: In view of problem 28 page 390 we find a non zero ideal in a PID is prime iff it is maximal.

Problem 4: *Find all the prime ideals of* $\frac{\mathbf{Z}_n}{(n)}$, $(n > 1)$ *and hence of* $\mathbf{Z}_n$.

Solution: We know any ideal of R/N is of the type $\frac{A}{N}$, where A is an ideal of R, containing N. (See Cor. Page 365)

Let $(n) = N$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, where p_i are distinct primes.

Let $\frac{A}{N}$ be any prime ideal of $\frac{\mathbf{Z}}{N}$, then A is an ideal of $\mathbf{Z}$. We show it is a prime ideal of $\mathbf{Z}$. Since A is an ideal of $\mathbf{Z}$, it is of the type $A = (a)$. Suppose A is not a prime ideal of $\mathbf{Z}$. Then $\exists\ x, y \in \mathbf{Z}$, s.t., $xy \in A$ but x and y are not in A.

Now $xy \in A \Rightarrow Nxy \in A/N \Rightarrow NxNy \in A/N$

$\Rightarrow Nx$ or $Ny \in A/N$ as A/N is prime ideal

$\Rightarrow x$ or y is in A, a contradiction.

Hence $A = (a)$ is a prime ideal and thus a is a prime (see exercise 1 page 323). Also $(n) \subseteq (a)$. Since $n \in (n) \subseteq (a)$ we find $a \mid n$.

But primes dividing n are $p_1, p_2, \ldots, p_r$

Thus $a = p_i$ for same i, $1 \leq i \leq r$

Hence if $A/(n)$ is any prime ideal of $\frac{\mathbf{Z}}{(n)}$ then it is of the type $\frac{(p_i)}{(n)}$ for some i, $1 \leq i \leq r$.

Conversely, any ideal of the type $\frac{(p_i)}{(n)}$, $1 \leq i \leq r$ will be a prime ideal of $\frac{\mathbf{Z}}{(n)}$ as $\frac{\mathbf{Z}/(n)}{(p_i)/(n)} \cong \frac{\mathbf{Z}}{(p_i)}$.

Since (p_i) is a prime ideal of $\mathbf{Z}$, $\frac{\mathbf{Z}}{(p_i)}$ is an integral domain.

Thus $\frac{\mathbf{Z}/(n)}{(p_i)/(n)}$ is an integral domain and hence $\frac{(p_i)}{(n)}$ are prime ideals of $\frac{\mathbf{Z}}{(n)}$, $1 \le i \le r$.

where p_i are all the primes dividing n.

We thus conclude that if $n = p_1^{\alpha_1} p_2^{\alpha_2} .... p_r^{\alpha_r}$ then $\frac{(p_1)}{(n)}, \frac{(p_2)}{(n)}, ..., \frac{(p_r)}{(n)}$ are precisely the prime ideals of $\frac{\mathbf{Z}}{(n)}$.

We've seen earlier (see page 365) that

$$\theta : \frac{\mathbf{Z}}{(n)} \to \mathbf{Z}_n \text{ s.t.,}$$

$$\theta(m + (n)) = m,\ 0 \le m < n$$

is an isomorphism.

Now if P is a prime ideal of $\frac{\mathbf{Z}}{(n)}$, then $\theta(P)$ is a prime ideal of $\mathbf{Z}_n$.

Since $\frac{(p_i)}{(n)}$ are all the prime ideals of $\frac{\mathbf{Z}}{(n)}$, their images under θ are the prime ideals of $\mathbf{Z}_n$ i.e., $(p_1), (p_2), ..., (p_r)$ are all the prime ideals of $\mathbf{Z}_n$.

Remarks: (*i*) In particular, prime ideal of $\mathbf{Z}_p$ where p is prime is $(p) = (0)$ as $p = 0$ in $\mathbf{Z}_p$. Recall, a field has no non-trivial ideals and $\mathbf{Z}_p$ is an ideal when p is prime.

(*ii*) Since a non zero ideal in $\mathbf{Z}$ is maximal iff it is prime, the above result can similarly be proved for maximal ideals.

Problem 5: *Show that* $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$*, the ring of Gaussian integers is a Euclidean domain.*

Solution: We know that $\mathbf{Z}[i]$ is an integral domain.

For any $0 \ne x \in \mathbf{Z}[i]$, where $x = a + ib$, define

$$d(x) = d(a + ib) = a^2 + b^2$$

Then as $x \ne 0$, either $a \ne 0$ or $b \ne 0$

thus $d(a + ib) = a^2 + b^2 > 0$

Let now $x, y \in \mathbf{Z}[i]$, s.t., $x \ne 0$, $y \ne 0$ and let $x = a + ib$, $y = c + id$.

Then
$$\begin{aligned} d(xy) &= d((a + ib)(c + id)) = d((ac - bd) + i(ad + bd)) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= d(x)\, d(y) \end{aligned} \quad ...(1)$$

Since $y \ne 0$, $d(y) \ge 1$ [$y \ne 0$ means c or d is non zero]

Thus $d(xy) \ge d(x)$

We now prove the last condition in the definition of a Euclidean domain.

Let $x, y \in \mathbf{Z}[i]$ be two members where x is an ordinary +ve integer n ($x = n + i0$) and $y = a + ib$

By Euclid's division algorithm,

$$a = un + r_1 \qquad 0 \le r_1 < n$$
$$b = vn + r_2 \qquad 0 \le r_2 < n$$

Now either $r_1 \le \frac{n}{2}$ or $r_1 > \frac{n}{2}$

if $r_1 > \frac{n}{2}$ then $-r_1 < -\frac{n}{2}$

$$\Rightarrow n - r_1 < n - \frac{n}{2} = \frac{n}{2}$$

Thus
$$a = un + r_1 = un + n - n + r_1$$
$$= n(u + 1) - (n - r_1)$$
$$= nq + k_1 \quad \text{where} \quad k_1 = -(n - r_1)$$
$$|k_1| = n - r_1 < \frac{n}{2}$$

Thus whether $r_1 \le \frac{n}{2}$ or $\frac{n}{2} < r_1$

we can express

$$a = nq + k_1 \quad \text{where } |k_1| \le \frac{n}{2}$$

Similarly, $b = nq' + k_2$ where $|k_2| \le \frac{n}{2}$

i.e., $a + ib = n(q + iq') + (k_1 + ik_2)$

or $y = tn + r$ $[t = q + iq', \; r = k_1 + ik_2]$

where either $r = 0$ (k_1 & k_2 could be zero)

or $d(r) = d(k_1 + ik_2) = k_1^2 + k_2^2 \le \frac{n^2}{4} + \frac{n^2}{4} < n^2 = d(n)$

Thus, under this particular case, the result is proved.

Let now $x, y \in \mathbf{Z}[i]$ be any two non zero members then $x\bar{x}$ is a +ve integer, say, n.

We apply the above result proved, to $y\bar{x}$ and n and find that

For $y\bar{x}$ and n, $\exists\ t, r \in \mathbf{Z}[i]$, s.t.,

$$y\bar{x} = tn + r$$

where either $r = 0$ or $d(r) < d(n)$

If $r = 0$ then $y\bar{x} = tn = tx\bar{x} \Rightarrow y = tx + 0$

If $d(r) < d(n)$ then $d(y\bar{x} - tn) < d(x\bar{x})$

$$\Rightarrow d(y\bar{x} - tx\bar{x}) < d(x)\ d(\bar{x}) \qquad \text{[using (1)]}$$

$$\Rightarrow d(\bar{x})\ d(y - tx) < d(x)\ d(\bar{x})$$

$$\Rightarrow d(y - tx) < d(x) \quad [d(\bar{x}) > 0]$$

Put $y - tx = r_o$ then $d(r_o) < d(x)$

So $y = tx + r_o$ where $d(r_o) < d(x)$

combining, we get

$y = tx + r_o$, where either $r_o = 0$ or $d(r_o) < d(x)$.

Hence the result is proved.

Problem 6: *Show that* $\mathbf{Z}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbf{Z}\}$ *is a Euclidean domain.*

Solution: It is easy to see that $\mathbf{Z}[\sqrt{2}]$ is an integral domain. Define a mapping. $d : \mathbf{Z}[\sqrt{2}] - \{0\} \to \mathbf{Z}$ by

$$d(a + \sqrt{2}b) = |a^2 - 2b^2|$$

then $|a^2 - 2b^2| \geq 1$ as $a^2 - 2b^2 = 0 \Rightarrow \sqrt{2} = \dfrac{a}{b}$ which is not possible.

Again, $d[(a + \sqrt{2}\, b)\ (c + \sqrt{2}\, d)] = d[(ad + 2bd) + \sqrt{2}\ (ad + bc)]$

$$= |(ac + 2bd)^2 - 2\ (ad + bc)^2|$$

$$= |(a^2 - 2b^2)\ (c^2 - 2d^2)|$$

$$= |a^2 - 2b^2|\ |c^2 - 2d^2| \qquad \ldots(1)$$

$$\geq |a^2 - 2b^2| = d(a + \sqrt{2}\, b)$$

i.e., $d(a + \sqrt{2}\, b) \leq d[(a + \sqrt{2}b)\ (c + \sqrt{2}\, d)]$

Let now $a + \sqrt{2}\, b$ and $c + \sqrt{2}\, d$ be two members of $\mathbf{Z}[\sqrt{2}]$ and suppose $c + \sqrt{2}\, d \neq 0$, then

$$\frac{a + \sqrt{2}\, b}{c + \sqrt{2}\, d} = \frac{(a + \sqrt{2}\, b)\ (c - \sqrt{2}d)}{c^2 - 2d^2} = \frac{ac - bd}{c^2 - 2d^2} + \frac{\sqrt{2}(bc - ad)}{c^2 - 2d^2}$$

$$= m + \sqrt{2}\, n \quad \text{(say)}$$

then m and n are rationals.

Now $m = [m] + \theta$ where $[m]$ is the greatest integer not greater than m and θ is fractional part of m.

If $0 \leq \theta \leq \dfrac{1}{2}$, take $p = [m]$

and if $\dfrac{1}{2} < \theta < 1$, take $p = [m] + 1$

Thus $\exists$ an integer p, s.t, $|m - p| \leq \dfrac{1}{2}$

Similarly we can find an integer q, s.t., $| n - q | \leq \frac{1}{2}$

Put $m - p = \alpha$, $n - p = \beta$, then $|\alpha| \leq \frac{1}{2}$, $|\beta| \leq \frac{1}{2}$

Also then $= \dfrac{a+\sqrt{2}b}{c+\sqrt{2}d} = (p+\alpha)+\sqrt{2}\,(q+\beta)$

$$\Rightarrow \frac{a+\sqrt{2}b}{c+\sqrt{2}d} = (p+\sqrt{2}\,q)+(\alpha+\sqrt{2}\,\beta)$$

$$\Rightarrow a+\sqrt{2}\,b = (c+\sqrt{2}d)\,(p+\sqrt{2}q)+(c+\sqrt{2}d)\,[(m-p)+\sqrt{2}(n-q)]$$

where, of course, $(p+\sqrt{2}q) \in \mathbf{Z}[\sqrt{2}]$ as p, q are integers
we can thus write

$$a+\sqrt{2}b = (c+\sqrt{2}d)(p+\sqrt{2}q)+r$$

where $r = (c+\sqrt{2}d)\,[(m-p)+\sqrt{2}\,(n-q)]$

and as $r = (a+\sqrt{2}b)-(c+\sqrt{2}d)\,(p+\sqrt{2}q)$

we notice $r \in \mathbf{Z}[\sqrt{2}]$

Now if $r \neq 0$, $d(r) = d[(c+\sqrt{2}d)\{(m-p)+(n-q)\sqrt{2}\}]$

$$= d[(c+\sqrt{2}d)][d((m-p)+\sqrt{2}(n-q))]$$

[using (1) one may notice here that in proving (1) we do not essentially require that a, b, c, d are integers]

$$\Rightarrow d(r) = |\,c^2-2d^2\,|\,|\,(m-p)^2-2\,(n-q)^2\,|$$
$$\leq |\,c^2-2d^2\,|\,|\,(m-p)^2+2\,(n-q)^2\,|$$
$$\leq |c^2-2d^2|\left|\frac{1}{4}+\frac{2}{4}\right|$$
$$\leq |\,c^2-2d^2\,| = d(c+\sqrt{2}\,d)$$

Hence, for $a+\sqrt{2}b, c+\sqrt{2}\,d \in \mathbf{Z}[\sqrt{2}]$ $\exists\ p+\sqrt{2}\,q, r \in \mathbf{Z}[\sqrt{2}]$ s.t.,

$$(a+\sqrt{2}\,b) = (c+\sqrt{2}\,d)\,(p+\sqrt{2}\,d)+r$$

where either $r = 0$ or $d(r) < d(c+\sqrt{2}\,d)$

showing that $\mathbf{Z}[\sqrt{2}]$ is a Euclidean domain.

Theorem 6: *Let a, b be two non zero elements of a Euclidean domain R. If b is not a unit in R then* $d(a) < d(ab)$.

Proof: Let b be not a unit. Then for a, ab in R $\exists\ t, r \in R$ s.t.,

$$a = tab + r$$

where either $r = 0$ or $d(r) < d(ab)$

If $r = 0$, then $a = tab \Rightarrow a\,(1 - t\,b) = 0$

$\Rightarrow tb = 1$ or that b is a unit, which is not so.

Thus $r \neq 0$ and $d(r) < d(ab)$

Now $r = a - tab = a(1 - tb)$

Hence $d(a) \leq d(a(1 - tb)) = d(r) < d(ab)$.

Cor.: If a, b are non zero elements of a Euclidean domain R then $d(a) = d(ab)$ iff b is a unit.

If b is a unit then $\exists\ c$ s.t., $bc = 1$

Now $d(a) \leq d(ab) \leq d((ab)c) = d(a)$

$\Rightarrow d(a) = d(ab)$

Converse follows from above theorem.

Problem 7: *Show that an element x in a Euclidean domain is a unit if and only if $d(x) = d(1)$.*

Solution: Let $d(x) = d(1)$

Suppose x is not a unit, then by above theorem

$d(1) < d(1\ .\ x)$ Taking $a = 1$, $b = x$

i.e., $d(1) < d(x)$

a contradiction

$\therefore\ x$ is a unit.

Conversely, let x be a unit in R, then $\exists\ y \in R$ s.t.,

$xy = 1$

Now $d(x) \leq d(xy)$ (by definition)

$\Rightarrow d(x) \leq d(1)$

Also $d(1) \leq d(1\ .\ x)$

$\Rightarrow d(1) \leq d(x)$

Hence $d(x) = d(1)$.

Problem 8: *Show by an example that it is possible to find two elements a, b in a Euclidean domain such that $d(a) = d(b)$ but a, b are not associates.*

Solution: Consider $D = \{a + ib \mid a, b \in \mathbf{Z}\} = \mathbf{Z}[i]$, the ring of Gaussian integers

where $d(a + ib) = a^2 + b^2$

then D is a Euclidean domain. (See problem 5)

Here $d(2 + i3) = 13 = d(2 - 3i)$

but $2 + 3i$ and $2 - 3i$, are not associates.

Notice that units of D are ± 1, $\pm i$ and thus an associate of $2 + 3i$ can be

$(2 + 3i)1$, $(2 + 3i)(-1)$, $(2 + 3i)i$, $(2 + 3i)(-i)$

i.e., $2 + 3i$, $-2 - 3i$, $2i - 3$, $3 - 2i$

which are all different from $2 - 3i$.

Theorem 7: *Any two non zero elements a, b in a Euclidean domain R have a g.c.d. d and it is possible to write.*

$$d = \lambda a + \mu b \quad \text{for some } \lambda, \mu \in R$$

Proof: Let $A = \{ra + sb \mid r, s \in R\}$

then A is an ideal of R as

$0 = 0.\ a + 0.\ b \in A \Rightarrow A \neq \varphi$

Let $x, y \in A$

$\Rightarrow \quad x = r_1 a + s_1 b, \quad y = r_2 a + s_2 b \qquad r_1, r_2, s_1, s_2 \in R$

Thus $x - y = (r_1 - r_2)a + (s_1 - s_2)b \in A$

Again $x \in A, r \in R, x = r_1 a + s_1 b$

$\Rightarrow rx = r(r_1 a + s_1 b) = (rr_1)a + (rs_1)b \in A$

showing that A is an ideal of R.

Since a Euclidean domain is a PID, A will be generated by some element, say, d.

We claim $d = \text{g.c.d.}(a, b)$

Now $d \in A \Rightarrow d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Again since $a = 1.a + 0.\ b \in A$

$b = 0\ .\ a + 1\ .\ b \in A$

(Note R being a Euclidean domain has unity)

So $a \in A,\ A = (d) \Rightarrow a = \alpha d$ for some $\alpha \in R$

$b \in A,\ A = (d) \Rightarrow b = \beta d$ for some $\beta \in R$

$\Rightarrow d \mid a$ and $d \mid b$

Again, if $c \mid a$ and $c \mid b$

then $c \mid \lambda a, \quad c \mid \mu b$

$\Rightarrow c \mid \lambda a + \mu b$

i.e. $c \mid d \Rightarrow d = \text{g.c.d.}(a, b)$.

Remarks: (*i*) The theorem clearly then holds in a PID, and the next result that we prove in a PID holds in a Euclidean domain.

(*ii*) Similarly one can show that any finite number of non-zero elements $a_1, a_2 \ldots, a_n$ in a Euclidean domain (PID) R have a g.c.d. which can be put in the form $\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n, \lambda_i \in R$.

Theorem 8: *Any two non zero elements a, b in a PID R have a least common multiple.*

Proof: Let $A = (a)$, $B = (b)$ be the ideals generated by a and b.

Then $A \cap B$ is an ideal of *PID R*. Suppose it is generated by l.

We show $l = \text{l.c.m.}(a, b)$

Now $A \cap B \subseteq A, A \cap B \subseteq B$

$l \in (l) \Rightarrow l \in (a) \Rightarrow l = au$ for some u

$l \in (l) \Rightarrow l \in (b) \Rightarrow l = bv$ for some v

$\Rightarrow a \mid l$ and $b \mid l$

Again, suppose $a \mid x$ and $b \mid x$

$\Rightarrow x = a\alpha,\ x = b\beta \quad \alpha, \beta \in R$

$\Rightarrow x \in (a),\ x \in (b)$

$\Rightarrow x \in A \cap B = (l)$

$\Rightarrow x = kl \ \Rightarrow l \mid x$

Hence l = l.c.m.(a, b).

Definition: In an integral domain R with unity, a, b (non zero) are said to be *co-prime* or *relatively prime*, if g.c.d.(a, b) is a unit in R.

Problem 9: *Two elements a, b in an integral domain with unity are co-prime iff* g.c.d.$(a, b) = 1$.

Solution: Let a, b be co-prime. By theorem 1 any associate of a g.c.d. is a g.c.d.

Since 1 is associate of any unit

1 will be an associate of d = g.c.d.(a, b) = a unit

$\Rightarrow 1$ = g.c.d.(a, b)

Converse is obvious as 1 is a unit.

Problem 10: *Let R be a PID and a, b be two non zero elements of R. Show that* $[a, b]\ (a, b) = abu$ *where u is a unit and* (a, b) = g.c.d.(a, b), $[a, b]$ = l.c.m. (a, b).

Solution: Let g.c.d.$(a, b) = d$

l.c.m.$(a, b) = l$

Since R is a PID existence of d and l is ensured. We show $dl \mid ab$ and $ab \mid dl$

Since l = l.c.m.(a, b), $a \mid l$ and $b \mid l$

we get $l = au$, $l = bv$ for some $u, v \in R$

Again d = g.c.d$(a, b) \Rightarrow \exists\ x, y \in R$, s.t.,

$ax + by = d$ (theorem done)

$\Rightarrow l\,(ax + by) = dl$

$\Rightarrow lax + lby = dl$

$\Rightarrow bvax + auby = dl$

$\Rightarrow ab(vx + uy) = dl \Rightarrow ab \mid dl$ ...(1)

Again as $d \mid a$, $d \mid b$, $a = d\alpha$, $b = d\beta$, $\alpha, \beta \in R$

$\Rightarrow ab = d\ \alpha\ d\ \beta = d(\alpha\beta d)$

Now $a = d\alpha$ and $d\alpha \mid d\alpha\beta$

$b = d\beta$ and $d\beta \mid d\alpha\beta$

$a \mid d\alpha\beta,\ b \mid d\alpha\beta$

$\Rightarrow l \mid d\alpha\beta$

$\Rightarrow d\alpha\beta = lk$ for some k

Thus $ab = d(\alpha\beta k) = (dl)k$

$\Rightarrow dl \mid ab$ ...(2)

(1) and (2) imply $dl = uab$

where u is a unit (result proved).

Note: See page 433 for method explaining how to find g.c.d. in general.

Prime and Irreducible Elements

Definitions: Let R be a commutative ring with unity. An element $p \in R$ is called a *prime element* if

(i) $p \neq 0$, p is not a unit.

(ii) For any $a, b \in R$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Let R be a commutative ring with unity. An element $p \in R$ is called an *irreducible element* if

(i) $p \neq 0$, p is not a unit.

(ii) whenever $p = ab$ then one of a or b must be a unit. (In other words, p has no proper factors.)

Example 5: In the ring $< \mathbf{Z}, +, \cdot >$ of integers, every prime number is a prime element as well as irreducible element.

Example 6: Cosider the ring

$$\mathbf{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbf{Z}\}$$

under the operations defined by

$$(a + \sqrt{-5}b) + (c + \sqrt{-5}d) = (a + c) + \sqrt{-5}(b + d)$$

$$(a + \sqrt{-5}b) . (c + \sqrt{-5}d) = (ac - 5bd) + \sqrt{-5}(ad + bc)$$

(i) We show $\sqrt{-5}$ is a prime element.

$\sqrt{-5} \neq 0$, it is also not a unit as, if it were a unit then $\exists\ a + \sqrt{-5}b$, s.t.,

$$\sqrt{-5}(a + \sqrt{-5}b) = 1$$

$\Rightarrow \sqrt{-5} = 1 + 5b$, which is not possible as R.H.S. is an integer whereas L.H.S. is not an integer.

Suppose now $\sqrt{-5}$ divides $(a + \sqrt{-5}b)(c + \sqrt{-5}d)$,

then $\exists\ (x + \sqrt{-5}y)$ s.t.,

$$\sqrt{-5}(x + \sqrt{-5}y) = (a + \sqrt{-5}b)\ (c + \sqrt{-5}d)$$

which on comparison gives,

$$-5y = ac - 5bd$$

$$5(bd - y) = ac \Rightarrow 5 \mid ac$$

But 5 being a prime number

either $5 \mid a$ or $5 \mid c$.

If $5 \mid a$ then $(\sqrt{-5})(\sqrt{-5}) \mid a$

$\Rightarrow \sqrt{-5} \mid a$

$\Rightarrow \sqrt{-5} \mid a + b\sqrt{-5}$

Similarly, if $5 \mid c$ then $\sqrt{-5} \mid c + \sqrt{-5}d$

Hence $\sqrt{-5}$ is a prime element.

(*ii*) We show further that 3 is an irreducible element which is not prime.

Suppose $3 = (a + \sqrt{-5}b)\,(c + \sqrt{-5}d)\,, \quad a, b, c, d \in \mathbf{Z}$

Taking conjugates, we get

$\overline{3} = (a - \sqrt{-5}b)(c - \sqrt{-5}d)$

Thus $3.\overline{3} = (a^2 + 5b^2)(c^2 + 5d^2)$

i.e., $9 = (a^2 + 5b^2)(c^2 + 5d^2)$

$\Rightarrow$ $a^2 + 5b^2 = 1, 3$ or 9

Now $a^2 + 5b^2 = 3$ is not possible as $a, b \in \mathbf{Z}$

If $a^2 + 5b^2 = 1$ then $a = \pm 1$ and $b = 0$

If $a^2 + 5b^2 = 9$ then $a^2 + 5d^2 = 1$, giving $c = \pm 1$ and $d = 0$

Thus, if $a^2 + 5b^2 = 1$ then $a^2 + \sqrt{-5}b = \pm 1 =$ unit (see Problem 11 below)

and if $a^2 + 5b^2 = 9$ then $c + \sqrt{-5}d = \pm 1 =$ unit

Hence 3 is an irreducible element of $\mathbf{Z}[\sqrt{-5}]$.

Now $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ and thus

$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$

We show it does not divide any one of these. Suppose $3 \mid (2 + \sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$

Then $(2 + \sqrt{-5}) = 3\,(a + \sqrt{-5}b) \quad a, b \in \mathbf{Z}$

$\Rightarrow 2 - \sqrt{-5} = 3(a - \sqrt{-5}b)$

$\Rightarrow 9 = 9\,(a^2 + 5b^2)$

$\Rightarrow 1 = a^2 + 5b^2 \Rightarrow a = \pm 1,\ b = 0$

$\Rightarrow 2 + \sqrt{-5} = \pm 3$ which is not possible

Thus $3 \nmid (2 + \sqrt{-5})$. Similarly $3 \nmid (2 - \sqrt{-5})$

Hence 3 is not a prime element of $\mathbf{Z}[\sqrt{-5}]$.

Problem 11: *Find all the units of* $\mathbf{Z}[\sqrt{-5}]$.

Solution: Suppose $a + \sqrt{-5}b$ is a unit in $\mathbf{Z}[\sqrt{-5}]$.

Then $(a + \sqrt{-5}b)(c + \sqrt{-5}d) = 1 + \sqrt{-5}\,.0$ for some $c, d \in \mathbf{Z}$

So, $(a - \sqrt{-5}b)(c - \sqrt{-5}d) = \bar{1} = 1$

giving $(a^2 + 5b^2)(c^2 + 5b^2) = 1$ in $\mathbf{Z}$

$\Rightarrow \quad a^2 + 5b^2 = 1 \Rightarrow a = \pm 1,\ b = 0$

Thus $a + \sqrt{-5}b = \pm 1$ are the units in $\mathbf{Z}[\sqrt{-5}]$.

The following theorem exhibits the 'closeness' of prime and irreducible elements.

Theorem 9: *In a PID an element is prime if and only if it is irreducible.*

Proof: Let D be a PID and let $p \in D$ be a prime element. We need prove only that if $p = ab$, then a or b is a unit.

So let $p = ab$ then $p \mid ab$

$\Rightarrow \quad p \mid a$ or $p \mid b$ (p is prime)

If $p \mid a$ then $a = px$ for some x

So $p = ab = (px)b$

$\Rightarrow\ p(1 - xb) = 0$

$\Rightarrow\ 1 - xb = 0$ as $p \neq 0$

$\Rightarrow\ xb = 1 \quad \Rightarrow b$ is a unit.

Similarly, if $p \mid b$ then a will be a unit.

Conversely, let p be irreducible element and suppose $p \mid ab$. We show either $p \mid a$ or $p \mid b$.

If $p \mid a$, we have nothing to prove.

Suppose $p \nmid a$

Since p, a are elements of a PID they have a g.c.d., say, d.

We show d is a unit.

Now $d \mid p$ and $d \mid a$

$\Rightarrow \quad \exists\ u, v$ s.t., $p = du$, $a = dv$

If d is not a unit then as p is irreducible and $p = du$, u will be a unit

$\Rightarrow \quad u^{-1}$ exists

$\Rightarrow \quad pu^{-1} = d$

$\therefore \quad a = pu^{-1}v \Rightarrow p \mid a$ which is not so.

Thus d is a unit.

Again, we know that d can be expressed as

$d = \lambda a + \mu p$

which gives $dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p$

$\Rightarrow\ b \,.\, 1 = \lambda d^{-1}ab + \mu d^{-1}bp$

But $p \mid ab,\ p \mid \mu d^{-1}\ bp$

$\therefore \quad p \mid (ab\lambda d^{-1} + \mu d^{-1}bp)$

$\Rightarrow\ p \mid b$

Hence the result follows.

Cor.: In an integral domain with unity, every prime element is irreducible. The converse is not true. See exercises.

Remark: Combining the results of Example 6 and the above theorem, we can say $\mathbf{Z}[\sqrt{-5}]$ is not a PID.

Example 7: Consider the ring $Z_6 = \{0, 1, 2, 3, 4, 5\}$ mod 6.

2 is a prime element in $\mathbf{Z}_6$ but is not irreducible.

2 is, of course, non zero, non unit.

Suppose $2 \mid a \otimes b$

Since $ab = 6q + a \otimes b$ for some q

and as $2 \mid 6q$, $2 \mid a \otimes b$, we find $2 \mid ab$

$\Rightarrow 2 \mid a$ or $2 \mid b$

$\Rightarrow 2 \mid a$ or $2 \mid b$ in $\mathbf{Z}_6$

Hence 2 is a prime element.

Again, as $2 \otimes 4 = 2$, where neither 2 nor 4 is a unit, we find 2 is not irreducible. (Note, $\mathbf{Z}_6$ is not an integral domain.)

Theorem 10: *Let R be a PID which is not a field, then an ideal $A = (a_o)$ is a maximal ideal if and only if a_o is an irreducible element.*

Proof: Let $A = (a_o)$ be a maximal ideal.

(*i*) $a_o \neq 0$.

Suppose $a_o = 0$, then since R is not a field, $\exists$ at least one $0 \neq b \in R$, s.t., b^{-1} does not exist.

Let $B = (b)$ and as $a_o = 0$, $A = (0)$

and $(0) \subseteq B \subseteq R \Rightarrow A \subseteq B \subseteq R$

Now $B \neq A$ as $b \in B$, $b \neq 0$, and $A = (0)$

$B \neq R$ as $1 \in R$, but $1 \notin B$

Note if $1 \in B = (b)$ then $\exists$ some x s.t., $1 = bx$

Showing that b is invertible which is not so

Hence $a_o \neq 0$.

(*ii*) a_o is not a unit.

Suppose a_o is a unit, then $a_o a_o^{-1} = 1$

$a_o \in A$, $a_o^{-1} \in R \Rightarrow a_o a_o^{-1} \in A$

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

which is not possible as A is maximal.

Thus a_o is not a unit.

(*iii*) Let now $a_o = bc$ for some $b, c \in R$. We show either b or c is a unit.

Let $B = (b)$

Since $a_o = bc$, $a_o \in B$

$\Rightarrow$ all multiples of a_o are in B

$\Rightarrow A \subseteq B$

But A is maximal thus either $B = R$ or $B = A$

If $B = R$, then $1 \in B = (b)$ as $1 \in R$

$\Rightarrow$ $1 = xb$ for some x

$\Rightarrow$ b is a unit.

If $B = A$, then $b \in A = (a_o)$

$\Rightarrow b = ya_o$ for some y

$\Rightarrow a_o = bc = ya_oc$

$\Rightarrow a_o - ya_oc = 0$

$\Rightarrow a_o(1 - yc) = 0$

$\Rightarrow 1 - yc = 0$ (as $a_o \neq 0$)

$\Rightarrow c$ is a unit.

Hence the result is proved.

Conversely, let a_o be irreducible element.

We show $A = (a_o)$ is maximal.

Let I be any ideal s.t., $A \subset I \subseteq R$.

Since R is a PID, I is generated by some element, say, x

Now $x \notin A$ as if $x \in A$

then $(x) \subseteq A$.

i.e., $I \subseteq A$ but $A \subseteq I$

means $A = I$ which is not so.

Thus $x \notin A$.

Again, $A = (a_o) \subseteq I$

$\Rightarrow a_o = xy$ for some y

a_o is irreducible $\Rightarrow x$ or y is a unit.

If y is a unit, then $yy^{-1} = 1$

and $a_o = xy$

$\Rightarrow a_oy^{-1} = x$

But $a_o \in A$, $y^{-1} \in R \Rightarrow a_oy^{-1} \in A$

$\Rightarrow x \in A$, which is not true.

Thus y is not a unit.

So x is a unit and $xx^{-1} = 1$.

Now $x \in I$, $x^{-1} \in R$, I is an ideal

$xx^{-1} \in I \Rightarrow 1 \in I \Rightarrow I = R$

$\Rightarrow A$ is maximal ideal of R.

Remark: Recall, a field F has only two ideals F and $\{0\}$. F is not maximal and 0 is not irreducible.

Exercises

1. In a Euclidean domain R with valuation d, show that
- (i) $d(a) = d(-a)$ for all $0 \neq a \in R$
- (ii) if a, b are associates then $d(a) = d(b)$
- (iii) if $a \mid b$ and $d(a) = d(b)$ then a, b are associates
- (iv) if for $0 \neq a \in R$, $d(a) = 0$ then a is a unit
- (v) if $a \mid b$ and a is not an associate of b then $d(a) < d(b)$. $(a, b \neq 0)$.

2. In a commutative ring R with unity, Prove that associate of a prime (irreducible) element is prime (irreducible).

3. If p, q are prime elements in an integral domain with unity such that $p \mid q$ then show that p, q are associates.

4. Show that
- (i) in $\mathbf{Z}_8$, l.c.m. $(3, 6) = 6$ and 2
- (ii) in $\dfrac{\mathbf{Z}}{(20)}$, g.c.d. $(9, 18) = 9$, l.c.m. $(9, 18) = 18$
- (iii) in ring of even integers, l.c.m. $(4, 6)$ does not exist
- (iv) in $\dfrac{\mathbf{Z}}{(12)}$, 6, 8 have no l.c.m.

5. Let R be a PID. Show that
- (i) two non zero elements a, b are co-prime iff $\exists\ x, y \in R$ s.t., $ax + by = 1$
- (ii) if $a \mid bc$ and a, b are co-prime then $a \mid c$

6. Show that every field is a Euclidean domain.

7. Prove that in $\dfrac{\mathbf{Z}}{(8)}$, $\overline{2}$ is a prime element but not irreducible.

8. If A, B, C are ideals in a PID R, prove that
- (i) $A \cap (B + C) = A \cap B + A \cap C$
- (ii) $A + (B \cap C) = (A + B) \cap (A + C)$

9. Show that quotient ring of a PID is a PID and the same is true of the homomorphic image.

10. Show that $\pm 1, \pm i$ are the units in $\mathbf{Z}[i]$ and prove that if $a + ib$ is not a unit in $\mathbf{Z}[i]$ then $a^2 + b^2 > 1$.

11. Prove that $1 + i$ is an irreducible element in the ring $\mathbf{Z}[i]$ of Gaussian integers.

12. In the ring $\mathbf{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbf{Z}\}$, show that $1 + 3\sqrt{-5}$ is irreducible element but is not prime.

13. Show that in $\mathbf{Z}[\sqrt{-3}]$, $1 + \sqrt{-3}$ is irreducible but not prime element.

14. Show that in an integral domain R with unity, any pair of non zero elements has g.c.d. iff it has l.c.m.

15. Show that $\mathbf{Z}[\sqrt{3}] = \{a + \sqrt{3}\, b \mid a, b \in \mathbf{Z}\}$ is a Euclidean domain.

16. Let $A = (a)$, $B = (b)$ be two ideals in an integral domain with unity. Show that $A = B$ iff a and b are associates. Show further that if $(a) + (b) = (d)$, then d = g.c.d. (a, b).

17. Let R be an integral domain with unity. Show that an element $0 \neq p \in R$ is a prime element iff (p) is a prime ideal.

Polynomial rings

Let R be a ring. By a polynomial over R, we mean an expression of the form

$$f(x) = a_o + a_1 x + a_2 x^2 + \ldots + a_m x^m, \qquad a_i \in R$$

What is x? The symbols x, x^2, ... here are not unknown elements or variables from the ring R. These are there only for convenience, say as place indicators for the elements a_o, a_1, a_2, ... of the ring. The idea behind the notation is only our familiarity to polynomials of this type that we are so used to (and there, of course, x does represent a variable). A further justification of this notation follows when we come to defining addition and multiplication of polynomials in the *usual way*.

Alternatively, any infinite sequence $(a_o, a_1, a_2, \ldots)$ of elements of R is called a polynomial over R if all except finite number of its terms a_i are zero. (Thus after a finite number of terms, all members will be zero). The first term a_o is called the constant term of the polynomial. If m is the largest non negative integer such that $a_m \neq 0$, then a_m is called the last (or leading) coefficient of the polynomial.

If
$$f(x) = a_o + a_1 x + \ldots + a_m x^m, \quad a_i \in R$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n, \quad b_j \in R$$

be two polynomials over R, then we say $f(x) = g(x)$ if $m = n$ and $a_i = b_i$ for all i.

Again, addition of polynomials $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + \ldots$$

Product is also defined in the usual way,

$$\begin{aligned} f(x)\, g(x) &= (a_o + a_1 x + \ldots + a_m x^m)\,(b_o + b_1 x + \cdots + b_n x^n) \\ &= a_o b_o + (a_1 b_o + a_o b_1)\, x \ldots \\ &= c_o + c_1 x + c_2 x^2 + \cdots + c_{m+n}\, x^{m+n} \end{aligned}$$

where $c_k = a_o b_k + a_1 b_{k-1} + \ldots + a_k b_o$

Let now $R[x]$ be the set of all polynomials over R. Then $R[x]$ is a non empty set and addition and multiplication as defined above on the members of $R[x]$, clearly are binary compositions. It is easy to see that $R[x]$ forms a ring under these operations. Zero of the ring will be the zero polynomial

$$O(x) = 0 + 0x + 0x^2 + \ldots.$$

Additive inverse of $f(x) = a_o + a_1 x + \ldots.. + a_m x^m$ will be the polynomial $-f(x) = -a_0 - a_1 x + \ldots + (-a_m)\, x^m$. In fact, if R has unity 1 then the polynomial

$$e(x) = 1 + 0x + 0x^2 + \ldots$$

will be unity of $R[x]$. $e(x)$ is also sometimes denoted by 1. Instead of a ring R if we start with a field F we get the corresponding ring $F[x]$ of polynomials.

Remark: Let $R = \mathbf{Z}_3 = \{0, 1, 2\}$ modulo 3. Define

$$f : \mathbf{Z}_3 \to \mathbf{Z}_3, \text{ s.t., } f(x) = x^3 + 2x \text{ and}$$

$$g : \mathbf{Z}_3 \to \mathbf{Z}_3, \text{ s.t., } g(x) = x^5 + 2x$$

Then $f(0) = 0 = g(0),\ f(1) = 1 + 2 = g(1)$

$f(2) = 5 + 1 = 2 + 4 = g(2)$

Hence $f(a) = g(a)\ \forall\ a \in \mathbf{Z}_3$

and thus $f(x) = g(x)$ by our definition of a function.

On the other hand we notice

$$f(x) = (0, 2, 0, 1, 0, 0, ...)$$

$$g(x) = (0, 2, 0, 0, 0, 1, 0, ...)$$

are not equal as polynomials over $\mathbf{Z}_3$. Thus $f(x) \neq g(x)$ in $\mathbf{Z}_3[x]$.

Definition: Let $f(x) = a_o + a_1x + a_2x^2 + \cdots + a_mx^m$ be any non zero polynomial in $R[x]$. We say $f(x)$ has *degree* m if $a_m \neq 0$ and $a_i = 0$ for all $i > m$, and write $\deg f(x) = m$.

We do not define degree of zero polynomial.

We say degree of $f(x)$ is zero if $a_o \neq 0$, $a_i = 0$ for all $i > 0$. In that case it is called a constant polynomial. Also clearly, $\deg(-f(x)) = \deg f(x)$.

Suppose R is any ring and $R[x]$ is the corresponding ring of polynomials over R. If we define a map

$$f : R \to R[x], \text{ s.t.,}$$

$$f(a) = a + 0.x + 0x^2 + ...$$

then it is easy to see that f will be $1 - 1$ homomorphism. Indeed,

$$\begin{aligned} f(a + b) &= (a + b) + 0x + 0x^2 + ... \\ &= (a + 0x + 0x^2 + \cdots) + (b + 0x + 0x^2 + \cdots) \\ &= f(a) + f(b) \\ f(ab) &= ab + 0.x + 0.x^2 + \cdots \\ &= (a + 0x + 0x^2 + \cdots)\ (b + 0x + \cdots) \\ &= f(a)\, f(b) \end{aligned}$$

Hence R can be imbedded into the ring $R[x]$. In other words, R is isomorphic to a subring of $R[x]$.

Thus R can be identified with a subring of $R[x]$ in view of which we sometimes take the liberty of calling R to be a subring of $R[x]$. The following theorem is now easy to prove.

Theorem 11: *Let $R[x]$ be the ring of polynomials over a ring R then*

(*i*) *R is commutative iff $R[x]$ is commutative.*

(*ii*) *R has unity iff $R[x]$ has unity.*

Proof: (*i*) If $R[x]$ is commutative then any subring of $R[x]$ is commutative and as R is isomprphic to a subring of $R[x]$, R will be commutative.

Conversely, if R is commutative

and
$$f(x) = a_o + a_1x + a_2x^2 + \cdots + a_mx^m$$
$$g(x) = b_o + b_1x + b_2x^2 + \cdots + b_nx^n$$

be two members of $R[x]$, then by definition of product

$$\begin{aligned} f(x)g(x) &= a_ob_o + (a_1b_o + a_ob_1)x + \cdots \\ &= b_oa_o + (b_1a_o + b_oa_1)x + \cdots \\ &= g(x)f(x). \end{aligned}$$

(*ii*) If R has unity 1 then the polynomial

$e(x) = 1 + 0x + 0x^2 + \cdots$ is unity of $R[x]$ as $f(x)e(x)$ will be $f(x)$ for any polynomial $f(x)$.

Conversely, let $R[x]$ have unity.

Define a map $\theta : R[x] \to R$, s.t.,

$$\theta(f(x)) = \theta(a_o + a_1x + .. + a_mx^m) = a_o$$

then θ is an onto homomorphism. (See theorem 15).

Thus R is a homomorphic image of $R[x]$ and hence has unity, as homomorphic image of a ring with unity is a ring with unity. It fact, $\theta(e(x))$ will be unity of R where $e(x)$ is unity of $R[x]$.

Theorem 12: *Let $R[x]$ be the ring of polynomial of a ring R and suppose*

$$f(x) = a_o + a_1x + \cdots + a_mx^m$$
$$g(x) = b_o + b_1x + \cdots + b_nx^n$$

are two non zero polynomials of degree m and n respectively, then

(*i*) *If* $f(x) + g(x) \neq 0$, $deg(f(x) + g(x)) \leq max(m, n)$

(*ii*) *If* $f(x)\,g(x) \neq 0$, $deg\,(f(x)\,g(x)) \leq m + n$

(*iii*) *If R is an integral domain*, $deg\,(f(x)\,g(x)) = m + n$

(*iv*) *R is an integral domain iff $R[x]$ is an integral domain.*

(*v*) *If F is a field*, *$F[x]$ is not a field.*

Proof: (*i*) By definition,

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_t + b_t)x^t$$

where $t = \max(m, n)$.

Now $a_k + b_k = 0$ for all $k > t$ as $a_k = 0$, $b_k = 0$

thus degree of $f(x) + g(x)$ is less than or equal to $t = \max(m, n)$. Notice it is possible to have deg $(f(x) + g(x)) < \max(m, n)$. Consider the ring $\mathbf{Z}$ of integers.

Let
$$f(x) = 1 + 2x - 2x^2$$
$$g(x) = 2 + 3x + 2x^2$$

be two members of $\mathbf{Z}[x]$,

then
$$\begin{aligned} f(x) + g(x) &= (1 + 2) + (2x + 3x) + (-2x^2 + 2x^2) \\ &= 3 + 5x \end{aligned}$$

Thus deg $(f(x) + g(x)) = 1$ whereas deg $f(x) = 2 =$ deg $g(x)$

(*ii*) Let $f(x)\, g(x) = c_0 + c_1x + c_2x^2 + \cdots$

where $c_k = (a_kb_0 + a_{k-1}\, b_1 + \ldots + a_0b_k)$.

Here $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_mb_n \ \ldots\ldots + a_{m+n}b_0$

$= a_mb_n$

as all other terms would be zero. ($a_{m+i} = 0$, $b_{n+j} = 0$ for all $i, j > 0$).

Again, $c_{m+n+t} = 0$ for all t > 0 and

thus deg $(f(x)\, g(x)) \leq m + n$ (a_mb_n can be zero even if $a_m \neq 0$ $b_n \neq 0$)

We show that it is possible that deg $(f(x)\, g(x)) < m + n$.

Consider the ring $R = \{0, 1, 2, 3, 4, 5\}$ modulo 6

Take $f(x) = 1 + 2x^3$

$g(x) = 2 + x + 3x^2$

two polynomials in $R[x]$ of degree 3 and 2 respectively.

Here $f(x)g(x) = 2 + x + 3x^2 + 4x^3 + 2x^4$

which is of degree $4 < 5$.

Notice, here R is not an integral domain.

(*iii*) If R is an integral domain then as $a_m \neq 0$, $b_n \neq 0$, therefore, $a_mb_n \neq 0$ and hence $c_{m+n} = a_mb_n \neq 0$ showing that deg $(f(x)g(x)) = m + n$.

(*iv*) If $R[x]$ is an integral domain then since R is isomorphic to a subring of $R[x]$, R will also be an integral domain.

Conversely, suppose R is an integral domain.

Let $f(x)$, $g(x)$ be any two non zero members of $R[x]$ s.t.,

$f(x)g(x) = 0$

where $f(x) = a_o + a_1x + \cdots + a_mx^m$

$g(x) = b_o + b_1x + \cdots + b_nx^n$

Now both $f(x)$ and $g(x)$ cannot be constant polynomials as then $a_o \neq 0$, $b_o \neq 0$ (so $c_o = a_ob_o \neq 0$)

$\therefore \quad f(x)g(x) \neq 0$

Since at least one of $f(x)$, $g(x)$ is non constant polynomial, its degree is ≥ 1.

R being an integral domain

deg $(f(x)g(x)) =$ deg $f(x) +$ deg $g(x) \geq 1$

which is a contradiction as it implies then $c_k \neq 0$ for some $k > 0$

whereas $f(x)g(x) = 0$.

Hence $f(x)g(x) = 0 \Rightarrow f(x) = 0$ or $g(x) = 0$

$\Rightarrow$ $R[x]$ is an integral domain.

(*v*) Let F be a field, then since F is commutative, has unity, by previous results we find $F[x]$ will be a commutative ring with unity. In fact F being an integral domain, $F[x]$ will also be an integral domain. We show, not all non zero elements of $F[x]$ have multiplicative inverse. Consider the non zero polynomial

$$f(x) = 0 + 1x + 0x^2 + 0x^3 + \ldots \; (= a_o + a_1x + a_2x^2 + \ldots\ldots)$$

Suppose $g(x) = b_o + b_1x + b_2x^2 + \ldots$ is its multiplicative inverse

then $f(x)g(x) = c_o + c_1x + c_2x^2 + \ldots$

should be unity $e(x) = 1 + 0x + 0x^2 + \ldots$ of $F[x]$

$\Rightarrow$ $c_o = 1$, $c_i = 0$ for all $i > 0$

where $c_o = a_ob_o = 0 . b_o = 0 \neq 1$.

Hence no $g(x)$ can be multiplicative inverse of $f(x) = x$.

Showing that $F[x]$ is not a field.

If R is a ring, we get $R[x]$ the corresponding ring of polynomials. Since $R[x]$ is a ring, we can similarly get $R[x, y]$ the corresponding ring of polynomials of $R[x]$ and the process can be extended. Elements of $R[x, y]$ will be of the type

$$g = f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_n(x)y^n$$

where $f_i(x) \in R[x], \quad i = 1, 2, \cdots n$

If F is a field then $F[x]$ is a ring with unity and similarly $F[x, y]$ will be a ring with unity. We shall use it a little later when we come to factorisation domains.

Problem 12: *Let R and S be two isomorphic rings. Show that R[x] and S[x] are also isomorphic.*

Solution: Let $\phi : R \to S$ be the given isomorphism.

Define a mapping

$$f : R[x] \to S[x], \text{ s.t.,}$$
$$f(a_o + a_1x + \ldots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$

It should now be a routine exercise for the reader to show that this f is an isomorphism.

Problem 13: *(i) Show that the mapping*

$$\sigma : \mathbf{Q}[x] \to \mathbf{Q}[x], \text{ s.t.,}$$
$$\sigma(f(x)) = f(ax + b), \; a, b \in \mathbf{Q}, \; a \neq 0 \text{ is an automorphism.}$$

(*ii*) Prove that any automorphism of $\mathbf{Q}[x]$ is of the form as in (*i*)

Solution: (i) We show σ as defined above is a ring automorphism

Since $\sigma(f(x) + g(x)) = \sigma(h(x))$ where $h(x) = f(x) + g(x)$

$= h(ax + b)$

$= f(ax + b) + g(ax + b)$

$= \sigma(f(x)) + \sigma(h(x))$

and $\sigma(f(x)g(x)) = \sigma(r(x))$, where $r(x) = f(x)g(x)$

$= r(ax + b) = f(ax + b)g(x + b)$

σ is a homomorphism.

Let $f(x) \in \text{Ker } \sigma$ be any member, then

$\sigma(f(x)) = 0$ i.e., $f(ax + b) = 0$

Suppose $f(x) = a_0 + a_1x + \cdots + a_nx^n$

then $f(ax + b) = a_0 + a_1(ax + b) + \cdots + a_n(ax + b)^n$

Since $f(ax + b) = 0$, we'll get $a_n a^n = 0$

and as $a \neq 0$, $a_n = 0$

So $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$

Proceeding as above, we find $a_i = 0$, $\forall i$

$\Rightarrow f(x) = 0 \Rightarrow \text{Ker}\sigma = \{0\}$

$\Rightarrow \sigma$ is one one

Again, for any $f(x) \in \mathbf{Q}[x]$, Since $f(a^{-1}x - a^{-1}b) \in \mathbf{Q}[x]$

and as $\sigma(f(a^{-1}x - a^{-1}b)) = f(a^{-1}(ax + b) - a^{-1}b) = f(x)$

σ is onto and hence it is an automorphism.

(*ii*) Let now $\sigma: \mathbf{Q}[x] \to \mathbf{Q}[x]$ be a ring automorphism, then

$$\sigma(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1\sigma(x) + a_2(\sigma(x))^2 + \cdots + a_n(\sigma(x))^n$$
$$= a_0 + a_1\sigma(x) + \cdots + a_n\sigma(x^n)$$

Notice that $\sigma\left(\frac{m}{n}\right) = \frac{m}{n} \quad \forall \frac{m}{n} \in \mathbf{Q}$

as $\sigma(1) = 1 \Rightarrow \sigma\left(\frac{n}{n}\right) = 1$ i.e, $\sigma\left(\frac{1}{n}\right) = \frac{1}{n}$

So $\sigma\left(\frac{m}{n}\right) = m\sigma\left(\frac{1}{n}\right) = \frac{m}{n}$

Now σ is completely known if $\sigma(x)$ is known

Suppose $\sigma(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$

$= c_0 + x(c_1 + c_2 x + \cdots + c_n x^{n-1})$

Thus $\sigma(x)$ can be put in the form

$\sigma(x) = xg(x) + b$, where $g(x) \in \mathbf{Q}[x]$, $b \in \mathbf{Q}$

Since σ is onto, both $g(x)$ and x have pre images in $\mathbf{Q}[x]$.

Let $g(x) = \sigma(h(x))$, $\quad x = \sigma(p(x))$

Then $\sigma(x) = \sigma(h(x))\sigma(p(x)) + b = \sigma(h(x)\,p(x) + b)$ as $\sigma(b) = b$

As σ is 1-1, we get

$x = h(x)p(x) + b$

$\Rightarrow$ deg x = deg $(h(x)p(x) + b)$ = deg $h(x)$ + deg $p(x)$

i.e., 1 = deg $h(x)$ + deg $p(x)$

$\Rightarrow$ either deg $h(x) = 1$ and deg $p(x) = 0$

or deg $h(x) = 0$ and deg $p(x) = 1$

If deg $p(x) = 0$, then $p(x)$ is constant poly, say $c \in \mathbf{Q}$ and so $x = \sigma p(x) = \sigma(c) = c$ a contradiction.

Thus deg $p(x) = 1$ and deg $h(x) = 0$,

Let $h(x) = a$, then $a \in \mathbf{Q}$, $a \neq 0$, as $h(x)$ is not a zero polynomial

otherwise also $a = 0 \Rightarrow x = b$ which is not true.

Now $\sigma(x) = \sigma(h(x)p(x) + b)$

gives $\sigma(x) = \sigma(h(x)\sigma(p(x)) + \sigma(b)$

$\sigma(x) = \sigma(a)x + b = ax + b, \qquad a, b \in \mathbf{Q}, \ a \neq 0$

Hence for any $f(x) \in \mathbf{Q}[x]$

$\sigma(f(x)) = f(ax + b), \qquad a, b \in \mathbf{Q}, \ a \neq 0$

or that any automorphism σ of the ring $\mathbf{Q}[x]$ is of the form $\sigma(f(x)) = f(ax + b), \quad a, b \in \mathbf{Q}, a \neq 0$

Remark: If we are in $\mathbf{Z}[x]$, then $a = \pm 1$ as a is invertible. Thus only ring automorphism of $\mathbf{Z}[x]$ would be $\sigma(f(x)) = f(\pm x + b)$, $b \in \mathbf{Z}$.

Theorem 13: *If F is a field, then $F[x]$ is a Euclidean domain.*

Proof: We have seen that $F[x]$ is an integral domain with unity.

For any $f(x) \in F[x], f(x) \neq 0$, define

$d(f(x)) = \deg f(x)$ which is non – ve integer

Since, for any $f(x), g(x) \in F[x], f(x), g(x) \neq 0$

$\deg (f(x)\ g(x)) = \deg f(x) + \deg g(x)$

we get $\deg (f(x)) \leq \deg (f(x)g(x))$, as $\deg (g(x)) \geq 0$

$\therefore \quad d(f(x)) \leq d(f(x)g(x))$

Lastly, we show for any non zero $f(x)$, $g(x)$ in $F[x]$, $\exists$ $t(x)$ and $r(x)$ in $F[x]$ such that

$f(x) = t(x)g(x) + r(x)$

where either $r(x)$ is zero or $\deg r(x) < \deg g(x)$

If $\deg f(x) < \deg g(x)$

then $f(x) = 0.\ g(x) + f(x)$ gives the result.

Assume now the result is true for all (non zero) polynomials in $F[x]$ of deg. less than $\deg f(x)$.

Let $f(x) = a_0 + a_1 + \cdots + a_m x^m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

Suppose $\deg f(x) \geq \deg g(x)$

Define $f_1(x) = f(x) - a_m b_n^{-1}\ x^{m-n}\ g(x)$

then coefficient of x^m in $f_1(x)$ is

$a_m - a_m b_n^{-1}.\ b_n = a_m - a_m = 0$

either $f_1(x) = 0$ (zero polynomial) or $\deg f_1(x) < m$

If $f_1(x) = 0$, then

$0 = f(x) - a_m b_n^{-1} x^{m-n}\ g(x)$

gives $f(x) = a_m b_n^{-1} x^{m-n}\ g(x) + 0$

So by taking $t(x) = a_m b_n^{-1} x^{m-n}$ and $r(x) = 0$ we get the required result.

Suppose $f_1(x) \neq 0$,

then $\deg f_1(x) < m$

i.e., $\deg f_1(x) < \deg f(x)$

By induction hypothesis

$$f_1(x) = t_1(x)\, g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$$\therefore \quad f(x) - a_m b_n^{-1}\, x^{m-n}\, g(x) = t_1(x)\, g(x) + r(x)$$

or
$$f(x) = [\, a_m b_n^{-1}\, x^{m-n} + t_1(x)]\, g(x) + r(x)$$
$$= t(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

and hence $F[x]$ is a Euclidean domain (and also, therefore, a PID)

Remarks: (*i*) Thus $\mathbf{Q}[x]$ is a Euclidean domain which is not a field.

(*ii*) One can show that the above defined $t(x)$ and $r(x)$ are unique.

Suppose $f(x) = t(x)\, g(x) + r(x)$ where either $r(x) = 0$ or $\deg r < \deg g$

and $f(x) = t'(x)\, g(x) + r'(x)$ where either $r'(x) = 0$ or $\deg r' < \deg g$

then $t(x)\, g(x) + r(x) = t'(x)\, g(x) + r(x)$

$\Rightarrow \quad g(t - t') = r' - r$ ...(1)

Suppose $t(x) \neq t'(x)$

then $t - t' \neq 0$ and thus has degree ≥ 0

(1) $\Rightarrow$ $\deg (g(t - t')) = \deg (r' - r)$

$\Rightarrow$ $\deg g + \deg (t - t') = \deg (r' - r)$ ...(2)

Also since $g(t - t')$ has positive degree ($\geq n$), $r' - r$ cannot be zero, otherwise $g(t - t')$ would be a constant polynomial, so its degree cannot be $\geq n$.

$r' - r$ cannot be zero $\Rightarrow$ both r and r' cannot be zero together.

Now L.H.S. of (2) is greater than or equal to deg g

whereas R.H.S. of (2) is $\leq \max (\deg r', \deg r) < \deg g$

as if both r, r' are non zero then $\deg r < \deg g$

$$\deg r' < \deg g$$

$\Rightarrow$ $\max (\deg r, \deg r') < \deg g$

If one of r, r' is zero, the other has deg less than deg g. In any case R.H.S. $< \deg g$, which is a contradiction.

Thus $t - t' = 0 \Rightarrow t = t'$

$\therefore$ (1) $\Rightarrow$ $r = r'$.

Hence the uniqueness is established.

If F is a field then $F[x]$ being a Euclidean domain will be a PID. Hence we can state

Theorem 14: *If F is a field, every ideal in $F[x]$ is principal.*

Problem 14: *Let F be a field and I a non zero ideal in F[x] and g(x) ∈ F[x]. Then I = < g(x) > iff g(x) is non zero polynomial of minimal degree in I.*

Solution: Let $g(x) \in I$ be of minimal degree then $< g(x) > \subseteq I$ (def. of ideal)

Let $f(x) \in F[x]$ be any element, since $F[x]$ is a Euclidean domain, for $f(x), g(x) \in F[x]$, $\exists\ q(x), r(x) \in F[x]$, s.t.,

$$f(x) = q(x)g(x) + r(x), \text{ where either } r(x) = 0 \text{ or deg } r(x) < \text{deg } g(x)$$

If $r(x) \neq 0$, then deg $r <$ deg g and as $r(x) = f(x) - g(x)q(x) \in I$.

we get a contradiction as $g(x)$ is of minimal degree in I.

Hence $r(x) = 0$

$$\Rightarrow f(x) = g(x)q(x) \Rightarrow f(x) \in < g(x) >$$

or that $I \subseteq < g(x) >$

and thus $I = < g(x) >$.

Conversely, Let $I = < g(x) >$

If $f(x) \in I$ be any member then $f(x) = g(x)h(x)$

$$\Rightarrow \text{deg } f(x) = \text{deg } g(x) + \text{deg } h(x)$$

$$\Rightarrow \text{deg } g(x) \leq \text{deg } f(x) \quad \text{as deg } h(x) \geq 0$$

or that $g(x)$ is of minimal degree.

Problem 15: *If R is the field of reals show that* $\dfrac{\mathbf{R}[x]}{< x^2 + 1 >} \cong \mathbf{C}$, *the ring of complex numbers.*

Solution: Define a mapping

$$\varphi : \mathbf{R}[x] \to \mathbf{C}, \text{ st.,}$$

$$\varphi : (f(x)) = f(i),$$

Then φ is easily seen to be an onto homomorphism and thus by Fundamental theorem of ring homomorphism,

$$\mathbf{C} \cong \frac{\mathbf{R}[x]}{\text{Ker } \varphi}$$

Let $f(x) \in$ Ker φ be any member

where $f(x) = a_0 + a_1x + \cdots + a_nx^n$

Then $\varphi(f(x)) = 0$

i.e., $a_0 + a_1i + \cdots + a_ni^n = 0$

If $f(x)$ is a polynomial of 1st degree then it is of the type $ax + b$, where $a \neq 0$

thus in that case $\varphi(f(x)) = ai + b \neq 0$ as $a \neq 0$

So polynomial of first degree is not in the Kernel.

Consider the second degree polynomial $x^2 + 1$,

$$\begin{aligned}\varphi(x^2 + 1) &= \varphi(0 + 0x + 1.x^2 + 0x^3 + \cdots) + \varphi(1 + 0.x + \cdots)\\ &= (0 + 0.i + i^2 + 0.i^3 + \cdots) + (1 + 0i + \cdots)\\ &= -1 + 1 = 0\end{aligned}$$

So $x^2 + 1 \in \text{Ker } \varphi$ and is of minimial degree. Since Ker φ is an ideal of $\mathbf{R}[x]$, by above problem, Ker $\varphi = \langle x^2 + 1\rangle$ proving our cliam.

Example 8: Let $R = \{0, 1\}$ mod 2, then $R[x]$ is an infinite integral domain. If $f(x) \in R[x]$ be any member and if,

$$\begin{aligned}f(x) &= a_o + a_1x + \cdots + a_mx^m \quad \text{then we have}\\ 2f(x) &= f(x) + f(x)\\ &= (a_o \oplus a_o) + (a_1 \oplus a_1)\, x + \cdots + (a_m \oplus a_m)\, x^m\\ &= 0 + 0.x + 0.x^2 + \cdots\\ &= O(x), \text{ zero of } R[x]\end{aligned}$$

Thus $2f(x) = 0\ \forall\ f \in R[x]$, showing that $R[x]$ is of finite characteristic (although it is infinite). Note also that ch R = ch $R[x]$. Here $R[x] = \mathbf{Z}_2[x]$ which is infinite integral domain having finite characteristic. The quotient field $\mathbf{Z}_2(x)$ of $\mathbf{Z}_2[x]$ will be an infinite field with characteristic 2.

Problem 16: *Let R be a commutative ring with unity. Let A be an ideal of R. Show that*

$$\frac{R[x]}{A[x]} \cong \frac{R}{A}[x].$$

Show that

A is prime ideal of $R \Rightarrow A[x]$ is prime ideal of $R[x]$.

Solution: Define a mapping

$$\begin{aligned}&\theta : R[x] \to \frac{R}{A}[x] \text{ s.t.,}\\ &\theta(f(x)) = \theta(a_o + a_1x + \cdots + a_nx^n)\\ &\qquad = (a_o + A) + (a_1 + A)\, x + \cdots + (a_n + A)x^n\end{aligned}$$

then θ is clearly well defined.

If
$$\begin{aligned}f(x) &= a_o + a_1x + a_2x^2 + \cdots\\ g(x) &= b_o + b_1x + b_2x^2 + \cdots\\ f(x)g(x) &= c_o + c_1x + c_2x^2 + \cdots\end{aligned}$$

$$\begin{aligned}\text{then } \theta(f(x) + g(x)) &= \theta((a_o + b_o) + (a_1 + b_1)\, x + \cdots)\\ &= [(a_o + b_o) + A] + [(a_1 + b_1) + A]\, x + \cdots\\ &= (a_o + A) + (b_o + A) + (a_1 + A)x + (b_1 + A)\, x + \cdots\\ &= ((a_o + A) + (a_1 + A)x + ...) + ((b_o + A) + (b_1 + A)x + \cdots)\end{aligned}$$

$$= \theta(f(x)) + \theta(g(x))$$

$$\theta(f(x)g(x)) = \theta(c_o + c_1x + c_2x^2 + ...)$$

$$= (c_o + A) + (c_1 + A)x + ...$$

$$= (a_ob_o + A) + (a_1b_o + a_ob_1 + A)x + ...$$

$$= (a_o + A)\ (b_o + A) + [(a_1b_o + A) + (a_ob_1 + A)]x + ...$$

$$= (a_o + A)\ (b_o + A) + [(a_1 + A)\ (b_o + A) + (a_o + A)\ (b_1 + A)]x + ...$$

Also $\theta(f(x))\ \theta(g(x)) = [(a_o + A) + (a_1 + A)x + ...]\ [(b_o + A) + ...]$

$= (a_o + A)\ (b_o + A) + [(a_1 + A)\ (b_o + A) + (a_o + A)\ (b_1 + A)]x + ...$

$\Rightarrow \theta$ is a homomorphism.

That θ is onto is evident from the definition of θ and hence by Fundamental theorem

$$\frac{R[x]}{\text{Ker } \theta} \cong \frac{R}{A}[x].$$

Now $f(x) \in \text{Ker } \theta \Leftrightarrow \theta(f(x)) = (0 + A) + (0 + A)\ x + ...$

$\Leftrightarrow (a_0 + A) + (a_1 + A)\ x + ... = (0 + A) + (0 + A)\ x + ...$

$\Leftrightarrow a_i + A = A$ for all i

$\Leftrightarrow a_i \in A$ for all i

$\Leftrightarrow f(x) \in A[x]$

Hence $$\frac{R[x]}{A[x]} \cong \frac{R}{A}[x]$$

Finally, let A be a prime ideal of R.

Then $\frac{R}{A}$ is an integral domain

$\Rightarrow \frac{R}{A}[x]$ is an integral domain

$\Rightarrow \frac{R[x]}{A[x]}$ is an integral domal, because of the isomorphism

$\Rightarrow A[x]$ is a prime ideal of $R[x]$.

Remarks: (*i*) It is clear then if A is an ideal of a ring R then $A[x]$ is an deal of $R[x]$ (Kernels are ideals).

(*ii*) If A is maximial ideal of R then R/A is a field $\Rightarrow \frac{R}{A}[x]$ is not a field $\Rightarrow \frac{R[x]}{A[x]}$ is not a field $\Rightarrow A[x]$ is not maximal ideal of $R[x]$. (See exercise 20 on page 471).

Problem 17: *Show that* $\frac{\mathbf{Z}_3[x]}{I}$ *where* $I = < x^2 + x + 1 >$ *is not an integral domain.*

Solution: $(x + 2) + I \in \frac{\mathbf{Z}_3[x]}{I}$

and $((x + 2) + I)^2 = (x + 2)^2 + I = (x^2 + 1.\ x + 1) + I$

$= I =$ zero of $\dfrac{\mathbf{Z}_3[x]}{I}$

but $(x + 2) + I$ is not zero of $\dfrac{\mathbf{Z}_3[x]}{I}$

Hence $\dfrac{\mathbf{Z}_3[x]}{I}$ is not an integral domain.

Notice 3 being prime, $\mathbf{Z}_3$ is an integral domain and thus $\mathbf{Z}_3[x]$ is also an integral domain. So quotient ring of an integral domain may not be an integral domain, a result we discussed earlier also. (See page 356).

Theorem 15: *For any commutative ring R with unity,* $\dfrac{R[x]}{< x >} \cong R$.

Proof: Define a map $\theta : R[x] \to R$, s.t.,

$$\theta(a_o + a_1x + \cdots + a_nx^n) = a_o$$

then θ is clearly well defined. Also

$$\theta[(a_o + a_1x + \cdots + a_nx^n) + (b_o + b_1x + \cdots + b_mx^m)]$$
$$= \theta[(a_o + b_o) + (a_1 + b_1)x + \cdots\ ]$$
$$= a_o + b_o = \theta(a_o + a_1x + \cdots + a_nx^n) + \theta(b_o + b_1x + \cdots + b_mx^m)$$

Similarly the result for product follows.

Thus θ is a homomorphism which is clearly onto. By Fundamental theorem, we get

$$\frac{R[x]}{\text{Ker } \theta} \cong R$$

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \text{Ker } \theta$

$\Leftrightarrow\ \theta(a_0 + a_1x + \cdots + a_nx^n) = 0$

$\Leftrightarrow\ a_0 = 0$

$\Leftrightarrow\ f(x) = x\,[a_1 + a_2x + \cdots + a_nx^{n-1}] = xh(x)$

$\Leftrightarrow\ f(x) \in < x >$

Hence Ker $\theta = < x >$ which proves our result.

Remark: If $\mathbf{Z}$ be the ring of integers then $< x >$ is a prime but not maximal ideal of $\mathbf{Z}[x]$.

By theorem 15, $\dfrac{\mathbf{Z}[x]}{< x >} \cong \mathbf{Z}$

Since $\mathbf{Z}$ is an integral domain, so would be $\dfrac{\mathbf{Z}[x]}{< x >}$ and thus $< x >$ is a prime ideal.

If $< x >$ is maximal ideal of $\mathbf{Z}[x]$ then $\dfrac{\mathbf{Z}[x]}{< x >}$ will be a field implying that $\mathbf{Z}$ is a field which is not true. Hence $< x >$ is not maximal. See also problems 20 and 21 ahead.

Theorem 16: *Let R be a commutative ring with unity such that $R[x]$ is a PID, then R is a field.*

Proof: By previous theorem,

$$\frac{R[x]}{< x >} \cong R.$$

We claim $< x >$ is a maximal ideal of $R[x]$.

Suppose I is any ideal s.t. $< x > \subseteq I \subseteq R[x]$.

Since $R[x]$ is a PID, $I = < f(x) >$ for some $f(x) = a_0 + a_1x + \cdots + a_nx_n$

Now $x \in < x > \subseteq I = < f(x) >$

$\Rightarrow x = f(x)g(x)$ for some $g(x) \in R[x]$

which implies either $f(x) = x, \quad g(x) = 1.$ (unity of $R[x]$)

or $f(x) = \alpha x, \; g(x) = \alpha^{-1}, \; \alpha \in R$

or $f(x) = 1, \quad g(x) = x$

(Second case being conditional to the existence of α^{-1})

If $f(x) = x, \quad I = < f(x) > \Rightarrow I = < x >$

if $f(x) = \alpha x, \; I = < f(x) > \Rightarrow I = < \alpha x > = < x >$

if $f(x) = 1, \quad I = < f(x) > \Rightarrow I = < 1 > = R[x]$

Hence $< x >$ is a maximal ideal.

$\therefore \quad \frac{R[x]}{< x >}$ is a field.

Hence R is a field.

Theorem 17: *An integral domain R with unity is a field iff $R[x]$ is a PID.*

Proof: If $R[x]$ is a PID, we've proved then R is a field (previous theorem).

Conversely, let R be a field.

Then $R[x]$ is a Euclidean domain (Theorem 13)

$\Rightarrow$ $R[x]$ is a PID. (Theorem 5)

The above theorem can be restated as

If R is an integral domain with unity, which is not a field then $R[x]$ is not a PID.

Cor. 1: $\mathbf{Z}[x]$ is not a PID as $\mathbf{Z}$ is not a field.

For another proof see problem 22.

Cor. 2: If F is a field then $F[x, y]$ is not a PID.

Proof: If $F[x, y]$ is a PID then $F[x]$ is a field which is not true as x is not invertible. See theorem 12 earlier.

Problem 18: *Show that $< x^2 + 1 >$ is not a prime ideal of $\mathbf{Z}_2[x]$.*

Solution: We notice that

$$(x + 1)^2 = x^2 + 2x + 1$$
$$= x^2 + 1 \quad \text{in } \mathbf{Z}_2[x]$$

Thus $x^2 + 1 = (x + 1)^2 = (x + 1)(x + 1) \in < x^2 + 1 >$

but $(x + 1) \notin < x^2 + 1 >$.

Problem 19: *Let* $I = \{f(x) \in \mathbf{Z}[x] \mid f(0) = 0\}$. *Show that* I *is an ideal of* $\mathbf{Z}[x]$ *and is* $< x >$.

Solution: I contains those polynomials in $\mathbf{Z}[x]$ whose constant term is zero, i.e., polynomials of the type $0 + a_1x + a_2x^2 + ... + a_nx^n$ where $a_i \in \mathbf{Z}$. Clearly $I \neq \varphi$ and difference of any two polynomials of this type has zero as its constant term.

If $f(x) = 0 + a_1x + a_2x^2 + \cdots + a_nx^n \in I$

and $g(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbf{Z}[x]$

be any members then

$f(x)g(x) = c_0 + c_1x + c_2x^2 + ...$

where $c_0 = a_0b_0 = 0.b_0 = 0$

and thus $f(x)g(x) \in I$ and so I is an ideal of $\mathbf{Z}[x]$

Let $f(x) \in I$ be any member

$\Rightarrow f(0) = 0$

i.e., $f(x) = 0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad a_i \in \mathbf{Z}$

$= x(a_1 + a_2x + \cdots + a_nx^{n-1}) \in < x >$

or that $I \subseteq < x >$

Again if $f(x) \in < x >$ be any member then

$f(x) = xg(x) = x(b_0 + b_1x + ...b_mx^m) \quad b_i \in \mathbf{Z}$

$= b_0x + b_1x^2 + ...$

$= 0 + b_0x + b_1x^2 + ... \in I$

or that $< x > \subseteq I$

and hence $I = < x >$.

Problem 20: *Prove that the ideal* $< x >$ *of* $\mathbf{Z}[x]$ *is a prime ideal but not maximal.*

Solution: Let $f(x) = a_0 + a_1x + \cdots + a_mx^m$

$g(x) = b_0 + b_1x + \cdots + b_nx^n$

be two polynomials of $\mathbf{Z}[x]$ such that $f(x)g(x) \in < x >$

then $(a_o + a_1x + \cdots + a_mx^m)(b_o + b_1x + b_2x^2 + \cdots + b_nx^n) \in < x >$

$\Rightarrow c_o + c_1x + c_2x^2 + \cdots \in < x >$, where $c_k = a_ob_k + a_1b_{k-1} + \cdots + a_kb_o$

$\Rightarrow c_o + c_1x + c_2x^2 + \cdots = x[d_o + d_1x + d_2x^2 + \cdots + d_tx^t]$

Comparing coefficients, we get

$c_o = a_ob_o = 0$

$\Rightarrow a_o = 0$ or $b_o = 0$

If $a_o = 0$ then $f(x) = a_1x + a_2x^2 + \cdots + a_mx^m$

$= x(a_1 + a_2x + \cdots + a_mx^{m-1}) \in < x >$

If $b_0 = 0$ then $g(x) \in < x >$

thus $< x >$ is prime ideal of $\mathbf{Z}[x]$.

We show $< x >$ is not maximal.

Consider $A = \{x f(x) + 2g(x)] \mid f(x), g(x) \in \mathbf{Z}[x]\}$

then A is an ideal of $\mathbf{Z}[x]$ as

$$[x f(x) + 2g(x)] - [x f'(x) + 2g'(x)]$$
$$= x[f(x) - f'(x)] + 2[g(x) - g'(x)] \in A$$

and for $h(x) \in \mathbf{Z}[x]$

$$[x f(x) + 2g(x)] h(x) = xf(x) h(x) + 2g(x) h(x) \in A$$

Now $2 \in A$, $2 \notin < x >$

As $2 = x(0 + 0.x + \cdots) + 2(1 + 0.x + 0.x^2 + \cdots)$

Thus $< x > \subset A$. Notice $< x > \subseteq A$ by definition of A.

Again, $A \neq \mathbf{Z}[x]$, because if $A = \mathbf{Z}[x]$ then as $1 \in \mathbf{Z}[x]$

$1 \in A \Rightarrow 1 = xf(x) + 2g(x)$

$\Rightarrow 1 = x(a_0 + a_1 x + \cdots + a_m x^m) + 2(b_0 + b_1 x + \cdots + b_n x^n)$

$\Rightarrow 1 = 2b_0, \; b_0 \in \mathbf{Z}$

a contradiction

Hence $A \neq \mathbf{Z}[x]$

or that $< x > \subset A \subset \mathbf{Z}[x]$

showing thereby that $< x >$ is not maximal.

Note: (*i*) $< x >$ will be maximal in $\mathbf{Q}[x]$. See also remark after theorem 15.

(*ii*) The above ideal A is also denoted by $< x, 2 >$ and it is the ideal

$$J = \{f(x) \in \mathbf{Z}[x] \mid f(0) = \text{even integer}\}.$$

Problem 21: *Let R be a commutative ring with unity and $< x >$ be a prime ideal of $R[x]$. Show that R must be an integral domain.*

Solution: Let $a, b \in R$ be such that $ab = 0$

Then the polynomials

$$(0 + 1x + 0x^2 + \cdots) + (a + 0x + 0x^2 + \cdots) \text{ and}$$
$$(0 + 1x + 0x^2 + \cdots) + (b + 0x + 0x^2 + \cdots) \text{ belong to } R[x]$$

$\Rightarrow x + a, x + b \in R[x]$

$\Rightarrow (x + a)(x + b) \in R[x]$

$\Rightarrow x^2 + x(a + b) + ab \in R[x]$

Since $ab = 0$, $x^2 + x(a + b) = x[x + a + b] \in < x >$

thus $(x + a)(x + b) \in < x >$

$\Rightarrow (x + a) \in < x >$ or $(x + b) \in < x >$ as $< x >$ is prime ideal

Now $(x + a) \in < x > \Rightarrow x + a = xf(x)$ for some $f(x) \in R[x]$

$$= x(a_0 + a_1 x + \cdots)$$

$\Rightarrow a = 0$

Similarly if $(x + b) \in \langle x \rangle$ then $b = 0$

Hence R is an integral domain.

Problem 22: *Show that the ideal*

$A = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbf{Z}[x]\}$ of $\mathbf{Z}[x]$ *is not a principal ideal.*

Solution: Suppose A is a principal ideal generated by $k(x)$, $k(x) \in \mathbf{Z}[x]$

Since $x = x(1 + 0x + 0x^2 + \cdots) + 2(0 + 0x^2 + \cdots) \in A = \langle k(x) \rangle$

$x = k(x)\, h(x)$

Also $2 \in \langle k(x) \rangle \Rightarrow 2 = k(x)t(x)$ ...(1)

Thus $xk(x)t(x) = 2k(x)h(x)$

$\Rightarrow 2h(x) = xt(x)$

$\Rightarrow$ each coefficient of $t(x)$ is an even integer.

i.e., $t(x) = 2r(x)$ for some $r(x) \in \mathbf{Z}[x]$

$\Rightarrow 2 = 2k(x)r(x)$

$\Rightarrow r(x)k(x) = 1$

$\Rightarrow 1 \in \langle k(x) \rangle$

$\Rightarrow \langle k(x) \rangle = \mathbf{Z}[x]$ [ideal with unity]

$\Rightarrow A = \mathbf{Z}[x]$

which is not true as A is proper ideal of $\mathbf{Z}[x]$ as seen in problem 20.

Remark: The above problem shows us that $\mathbf{Z}[x]$ is not a PID, a result we proved earlier also.

Problem 23: *Show that the above ideal A is maximal ideal in* $\mathbf{Z}[x]$.

Solution: Let I be an ideal such that $A \subset I \subseteq \mathbf{Z}[x]$.

Since $A \neq I$, $\exists$ $h(x) \in I$, s.t., $h(x) \notin A$.

Let $h(x) = b_o + b_1x + b_2x^2 + \cdots + b_mx^m$

then b_o is odd as if b_o is even then $h(x) \in A$.

$h(x) = 2k + b_1x + b_2x^2 + \cdots + b_mx^m = g(x) + xf(x)$ type

Thus $h(x) = (2a + 1) + b_1x + b_2x^2 + \cdots + b_mx^m$

$h(x) = g(x) + 1$

$\Rightarrow 1 = h(x) - g(x)$

$\Rightarrow 1 \in I$ as $h(x) \in I$, $g(x) \in A \subseteq I$

$\Rightarrow I = \mathbf{Z}[x]$

$\Rightarrow A$ is maximal.

Problem 24: *Let R be a commutative ring. If* $f(x) = a_o + a_1x + \cdots + a_mx^m \in R[x]$ *is a zero divisor, show that there exists an element* $b \neq 0$ *in R such that* $ba_o = ba_1 = \cdots = ba_m = 0$.

Solution: Since $f(x)$ is a zero divisor, $\exists$ some $g(x) \neq 0$ s.t.,

$f(x)\, g(x) = 0$

Let $g(x)$ be such polynomial with least degree

and suppose $g(x) = b_o + b_1x + ... + b_nx^n$

Let $f(x)\, g(x) = c_o + c_1x + c_2x^2 + ...$ .....(1)

Since $f(x)\, g(x) = 0$, we get $c_o = c_1 = c_2 = ... = 0$

Now $0 = c_{m+n} = a_{m+n}b_o + a_{m+n-1}\, b_1 + ... + a_mb_n + ...$

$\Rightarrow a_mb_n = 0$ as each $a_ib_j = 0$ when $i > m$

or when $j > n$

Consider $a_mg(x) = a_mb_o + a_mb_1x + ... + a_mb_nx^n$

Since $a_mb_n = 0$

$\deg (a_mg) < n = \deg g$

Now if $a_mg \neq 0$ then since

$f . a_mg = a_mfg = 0$ as $fg = 0$

we find a_mg is a polynomial such that $f(a_mg) = 0$

with $\deg (a_mg) < \deg g$

a contradiction to the choice of g.

Hence $a_mg = 0$

We claim now $a_{m-r}g = 0$. for all r, $0 \leq r \leq m$.

Result is true (proved) for $r = 0$. Suppose it is true for $r - 1$, we show it holds for r.

So we are given that $a_{m-(r-1)}\, g = 0$

we show $a_{m-r}\, g = 0$

Consider, coefficient of x^{m+n-r} in (1), it is c_{m+n-r} which is, of course, zero. So

$0 = c_{m+n-r} = a_{m+n-r}\, b_o + a_{m+n-r+1}\, b_1 + ... + ...$

$\Rightarrow 0 = a_mb_{n-r} + a_{m-1}\, b_{n-r+1} + ... + a_{m-r}b_n$

(rest of the terms being zero)

Since result $a_{m-i}g = 0$ holds when $i < r$

we find $a_mb_{n-r} = a_{m-1}\, b_{n-r+1} = ... = 0$

Note $a_{m-i}g = a_{m-i}b_o + a_{m-i}\, b_1x + ... + a_{m-i}\, b_nx^n = 0$

$\Rightarrow a_{m-i}\, b_o = 0, a_{m-i}\, b_i = 0, ... , a_{m-i}\, b_n = 0$

Hence $a_{m-r}\, b_n = 0 \Rightarrow \deg (a_{m-r}\, g) < n = \deg g$

$a_{m-r}\, g = a_{m-r}\, b_o + a_{m-r}\, b_1x + ... + a_{m-r}\, b_nx^n$

Also $f . a_{m-r}\, g = a_{m-r}\, fg = 0$

Since $\deg a_{m-r}\, g < \deg g$

we find $a_{m-r}\, g = 0$ for all $r = 0, 1, 2, ...$

Thus $a_og = 0, a_1g = 0, ..., a_mg = 0$

$\Rightarrow a_ob_n = 0, a_1b_n = 0, a_2b_n = 0, ..., a_mb_n = 0$

$b_n \neq 0$ in R.

Problem 25: *We have seen earlier* (*exercises on page 351*) *that for ideals A, B, C of a ring R,*

$$(A + C)(B + C) \subseteq AB + C, \quad (A \cap B)(A + B) \subseteq AB \text{ hold.}$$

Show by an example that equality may not hold in either case.

Solution: Consider the ideals

$$A = \langle 3x \rangle,\ B = \langle 2 \rangle,\ C = \langle x^2 \rangle \text{ in } \mathbf{Z}[x]$$

Then $AB = \langle bx \rangle,\ A + C = \langle 3x, x^2 \rangle,\ B + C = \langle 2, x^2 \rangle$

$$AB + C = \langle bx, x^2 \rangle,\ (A + C)(B + C) = \langle 6x, 3x^3, 2x^2, x^4 \rangle$$

Now $x^2 \in AB + C$ and if $x^2 \in (A + C)(B + C)$, then

$$x^2 = f(x)\ 6x + g(x)\ 3x^2 + h(x)\ 2x^2 + r(x)x^4$$

for $f, g, h, r \in \mathbf{Z}[x]$

Suppose $f(x) = \alpha_0 + \alpha_1 x + \ldots\ldots$

$h(x) = \beta_0 + \beta_1 x + \ldots\ldots \quad \alpha_i, \beta_i \in \mathbf{Z}$

Then comparing coefficients of x^2 on both sides

we get

$1 = 6\alpha_1 + 2\beta_0$ which is not possible and hence equality cannot hold in first case.

Again, $A \cap B = \langle 6x \rangle = AB, \quad A + B = \langle 3x, 2 \rangle$

$$(A \cap B)(A + B) = \langle 18x^2, 12x \rangle$$

Now $6x \in AB$ and if $6x \in (A \cap B)(A + B)$, then

$$6x = f(x)\ 2x + g(x)\ 18x^2, \quad f, g \in \mathbf{Z}[x]$$

If $f = \alpha_0 + \alpha_1 x + \ldots\ldots, \qquad \alpha_i \in \mathbf{Z}$

Then comparing coefficients of x we get

$6 = 12\alpha_0$ *i.e.*, $1 = 2\alpha_0$, $\alpha_0 \in \mathbf{Z}$, which is not possible. Hence equality cannot hold in second case also.

Greatest Common Divisor

Let us see how we calculate g.c.d. of any two elements in a Euclidean domain. (See page 29 also) Let a, b be two non zero elements of a Euclidean domain R. By repeated use of the Euclidean division algorithm we get

$$\begin{aligned}
a &= t_1\, b + r_1 && \text{where } d(r_1) < d(b) && (\text{or } r_1 = 0)\\
b &= t_2\, r_1 + r_2 && \text{where } d(r_2) < d(r_1) && (\text{or } r_2 = 0)\\
r_1 &= t_3 r_2 + r_3 && \text{where } d(r_3) < d(r_2)\\
&\cdots\cdots\cdots\\
&\cdots\cdots\cdots\\
r_{k-2} &= t_k r_{k-1} + r_k && \text{where } d(r_k) < d(r_{k-1})\\
r_{k-1} &= t_{k+1}\, r_k + 0
\end{aligned}$$

Then if $r_1 = 0$, g.c.d.$(a, b) = b$ otherwise g.c.d.$(a, b) = r_k$

One may notice here, the adove process must finish as $d(b)$, $d(r_1)$, $d(r_2)$, ... is a decreasing sequence of non – ve integers and hence $r_i = 0$ for some i.

Let us prove the result for, say, $k = 3$.

We have

$$a = t_1\, b + r_1 \qquad ...(1)$$

$$b = t_2\, r_1 + r_2 \qquad ...(2)$$

$$r_1 = t_3 r_2 + r_3 \qquad ...(3)$$

$$r_2 = t_4 r_3 + 0 \qquad ...(4)$$

To show that g.c.d.$(a, b) = r_3$ we prove that $r_3 | a$, $r_3 | b$ and whenever $r | a$ *and* $r | b$ then $r | r_3$.

Now $(4) \Rightarrow r_3 \mid r_2 \Rightarrow r_3 \mid t_3 r_2$ and as $r_3 \mid r_3$

we find $r_3 \mid (t_3 r_2 + r_3) \Rightarrow r_3 \mid r_1$ using (3)

Similarly, $r_3 \mid r_1, r_3 \mid r_2 \Rightarrow r_3 \mid b$ by (2)

and $r_3 \mid b, r_3 \mid r_1 \Rightarrow r_3 \mid a$ by (1)

Let now $r | a$ and $r | b$, then $r | r_1$ using (1)

Also $r \mid b,\ r \mid r_1 \Rightarrow r \mid r_2$ using (2)

$r \mid r_1,\ r \mid r_2 \Rightarrow r \mid r_3$ using (3)

Hence g.c.d.$(a, b) = r_3$, proving our assertion.

Again we know that g.c.d. (a, b) can be put in the form $\lambda a + \mu b$, for some $\lambda, \mu \in R$. We can get this expression from above equation $r_{k-2} = t_k\, r_{k-1} + r_k$ as here $r_k = r_{k-2} - t_k\, r_{k-1}$ and by successively going up the above equations we get the desired form.

We now discuss how to find g.c.d. of any two members of $F[x]$.

Let $f_1, f_2 \in F[x]$ be any two members.

Divide f_1 by f_2 to get $f_1 = f_2 q_1 + f_3$, $\deg f_3 < \deg f_2$

Divide f_2 by f_3 to get $f_2 = f_3 q_2 + f_4$, $\deg f_4 < \deg f_3$

Continuing like this, we'll finally reach

$$f_{n-1} = f_n q_{n-1} + 0$$

then we claim f_n = g.c.d.(f_1, f_2)

Consider the ideal (f_1, f_2) generated by f_1 & f_2.

$$(f_1, f_2) = \{g\, f_1 + h\, f_2 \mid g, h \in F[x]\}$$

Let $g\, f_1 + h\, f_2$ be any member of this ideal, then

$$g\, f_1 + h\, f_2 = g(f_2 q_1 + f_3) + h\, f_2$$

$$= f_2\, (g q_1 + h) + g f_3 \in (f_2, f_3)$$

giving that $(f_1, f_2) \subseteq (f_2, f_3)$

Similarly we can show $(f_2, f_3) \subseteq (f_1, f_2)$ and hence $(f_1, f_2) = (f_2, f_3)$

which would finally lead us to the result

$$(f_1, f_2) = (f_2, f_3) = ... = (f_n, 0) = (f_n)$$

That f_n is g.c.d.(f_1, f_2) now follows from exercise 16 page 416.

We illustrate through the following :

Problem 26: *Find g.c.d. of*

(*i*) 9, 15; 7, 10 *in* $\mathbf{Z}$

(*ii*) $11 + 7i$, $18 - i$ *in* $\mathbf{Z}[i]$

(*iii*) $x^4 + x^3 + 2x^2 + x + 1$, $x^3 - 1$; $x^2 + 1$, $x^6 + x^3 + x + 1$ *in* $\mathbf{Q}[x]$

Solution: (*i*) We have

$$\begin{aligned} 15 &= 9\times1 + 6 & 10 &= 7\times1 + 3 \\ 9 &= 6\times1 + 3 & 7 &= 3\times2 + 1 \\ 6 &= 3\times2 + 0 & 3 &= 1\times3 + 0 \end{aligned}$$

i.e., g.c.d. (9, 15) = 3 and g.c.d.(7, 10) = 1

(*ii*) Dividing $18 - i$ by $11 + 7i$, we get

$$\frac{18-i}{11+7i} = \frac{(18-i)(11-7i)}{(11+7i)(11-7i)} = \frac{191}{170} - \frac{137}{170}\,i$$

$$= \left(1+\frac{21}{170}\right) - \left(1-\frac{33}{170}\right) i = (1 - i) + \left(\frac{21}{170} + \frac{33i}{170}\right)$$

Thus $18 - i = (11 + 7i)(1 - i) + 3i$ ...(1)

Dividing $11 + 7i$ by $3i$, we get

$$\frac{11+7i}{3i} = \frac{(11+7i)(-3i)}{3i(-3i)} = \frac{21}{9} - \frac{33}{9}\,i = \frac{7}{3} - \frac{11}{3}\,i = (2 - 3i) + \left(\frac{1}{3} - \frac{2i}{3}\right)$$

Giving $11 + 7i = 3i(2 - 3i) + (2 + i)$ ...(2)

Again $$\frac{3i}{2+i} = \frac{3i(2-i)}{(2+i)(2-i)} = i + \left(\frac{3}{5} + \frac{1}{5}i\right)$$

or $$3i = i(2 + i) + \left(\frac{3}{5} + \frac{1}{5}i\right)(2 + i)$$

$$3i = i(2 + i) + (1 + i) \quad ...(3)$$

Dividing $(2 + i)$ by $(1 + i)$, we get

$$\frac{2+i}{1+i} = \frac{2+i}{1+i}\cdot\frac{1-i}{1-i} = \frac{3}{2} - \frac{1}{2}i = 1 + \left(\frac{1}{2} - \frac{1}{2}i\right)$$

$$2 + i = (1 + i) \,.\, 1 + 1 \quad ...(4)$$

Dividing $1 + i$ by 1 we have $(1 + i) = 1\cdot(1 + i) + 0$

Hence g.c.d.$(11 + 7i, 18 - i) = 1$.

If we retrace the steps backwards from (4) to (1) we get

$$1 = (11 + 7i)(6 - 6i) - (6 - 6i)(18 - i)$$

i.e., we can express the g.c.d. in the form $\lambda a + \mu b$.

(*iii*) By actual division

$$x^3 - 1 \overline{)\, x^4 + x^3 + 2x^2 + x + 1} \quad (x + 1)$$

$$x^4 - x$$

$$x^3 + 2x^2 + 2x + 1$$

$$x^3 - 1$$

$$2x^2 + 2x + 2$$

we find $x^4 + x^3 + 2x^2 + x + 1 = (x^3 - 1)(x + 1) + (2x^2 + 2x + 2)$

Similarly, $x^3 - 1 = (2x^2 + 2x + 2)\left(\frac{x}{2} - \frac{1}{2}\right) + 0$

Hence required g.c.d. is $2x^2 + 2x + 2$.

One can similarly tackle the second part. We notice

$x^6 + x^3 + x + 1 = (x^2 + 1)\, x^2 + (x + 1)$ (Dividing $x^6 + x^3 + x + 1$ by $x^2 + 1$)

$x^2 + 1 = (x + 1)(x - 1) + 2$ (Dividing $x^2 + 1$ by $x + 1$)

$x + 1 = 2\left(\frac{1}{2}x\right) + 1$ (Dividing $x + 1$ by 2)

$2 = 1 \times 2 + 0$ (Dividing 2 by 1)

Thus g.c.d. is 1

Unique Factorization Domains

Definition: Let R be an integral domain with unity then R is called a *unique factorization domain* (UFD) if

(*i*) every non zero, non unit element a of R can be expressed as a product of finite number of irreducible elements of R and

(*ii*) if $a = p_1 p_2 \ldots p_m$

$a = q_1 q_2 \ldots q_n$

where p_i and q_j are irreducible in R then $m = n$ and each p_i is an associate of some q_j.

(It would, of course, be possible to write q_is in such a manner that each p_i will be an associate of q_i.)

Example 9: The ring $< \mathbf{Z}, +, \cdot >$ of integers is a UFD. We know it is an integral domain with unity. If $n \in \mathbf{Z}$ be any non zero, non unit element (*i.e.*, $n \neq 0, \pm 1$) of $\mathbf{Z}$ then if $n > 0$, we can write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} \text{ where } p_i \text{ are primes}$$

$$\Rightarrow n = (p_1 p_1 \ldots p_1)(p_2 p_2 \ldots p_2) \ldots (p_r p_r \ldots p_r)$$

or that n is a product of prime (and thus irreducible) elements of $\mathbf{Z}$. Again this representation of n is unique (by Fundamental theorem of Arithmetic).

In case $n < 0$, let $n = (-m)$ where $m > 0$ then we can express m as product of primes (therefore, irreducibles) in $\mathbf{Z}$

say, $m = q_1 q_2 \ldots q_k$

then $(-m) = n = (-q_1)\ (q_2) \ldots (q_k)$

Example 10: A field $< F, +, \cdot >$ is always a UFD as it contains no non zero, non unit elements.

Example 11: $\mathbf{Z}[\sqrt{-5}]$ is an integral domain which is not a UFD.

$46 \in \mathbf{Z}[\sqrt{-5}]$ is a non unit, non zero element and we can express it as product of irreducibles in two ways

$$46 = 2 \cdot 23$$

$$46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$$

But 2 is not an associate of $1+3\sqrt{-5}$ or $1-3\sqrt{-5}$. Hence $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

To prove that 2 is irreducible, mimic the proof of example 6.

In fact, $6 = 3.2$

$$6 = (1-\sqrt{-5})(1+\sqrt{-5})$$

is another example of two distinet factorizations of 6 into irreducibles.

Remark: As in example 6 on page 410 we can show that 2 is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$ and thus by using next theorem, $\mathbf{Z}[\sqrt{-5}]$ cannot be a UFD.

Theorem 18: *In a UFD R an element is prime iff it is irreducible.*

Proof : Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible. (See Cor. after theorem 9).

Conversely, let $a \in R$ be irreducible. Then a is non zero, non unit. Let $a \mid bc$

then $bc = ak$ for some k

Case (*i*): b is a unit

then $c = akb^{-1} = a\ (kb^{-1}) \Rightarrow a \mid c.$

Case (*ii*): c is a unit then similarly, $a \mid b.$

Case (*iii*): b, c are non units

If k is a unit, then $bc = ak$

$$\Rightarrow a = b(ck^{-1})$$

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit. Thus ck^{-1} is a unit.

But that implies c is a unit, which is again not true. Hence k is not a unit.

We can thus express

$$b = p_1 p_2 \ldots p_m.$$

$$c = q_1 q_2 \ldots q_n$$

$$k = r_1 r_2 \ldots r_t$$

as product of irreducibles (by def. of UFD).

So $bc = ak$ becomes

$$p_1p_2 \ldots\ldots p_m\, q_1q_2 \ldots\ldots q_n = ar_1\, r_2 \ldots\ldots r_t = x \text{ (say)}$$

Then x is an element having two representations as product of irreducible elements. By Def. of UFD each element in one representation is an associate of some element in the other.

$\Rightarrow$ a is an associate of some p_i or some q_j

$\Rightarrow$ $ua = p_i$ or $ua = q_j$ for some unit u

$\Rightarrow$ $a \mid p_i$ or $a \mid q_j$

$\Rightarrow$ $a \mid b$ or $a \mid c$ $\qquad (p_i \mid b,\ q_j \mid c)$

$\Rightarrow$ a is prime element.

Theorem 19: *If R is an integral domain with unity in which every non zero, non unit element is a finite product of irreducible elements and every irreducible element is prime, then R is a UFD.*

Proof: To show that R is a UFD we need prove that if $a \in R$ be a non zero, non unit element and

$$a = p_1p_2 \ldots\ldots p_m = q_1q_2 \ldots\ldots q_n$$

where p_i and q_j are irreducible elements then $m = n$ and each p_i is an associate of some q_j.

We use induction on n.

Let $n = 1$, then $a = p_1p_2 \ldots\ldots p_m = q_1$ and as q_1 is irreducible some p_i is a unit. But each p_i being irreducible cannot be a unit. Thus $m = 1$.

$\therefore$ $a = p_1 = q_1$ or that the result is true for $n = 1$. Let it be true for $n - 1$.

Let now $a = p_1p_2 \ldots\ldots p_m = q_1q_2 \ldots\ldots q_n$

Then $p_1p_2 \ldots\ldots p_m = q_1(q_2 \ldots\ldots q_n)$

$\Rightarrow$ $q_1 \mid p_1p_2 \ldots\ldots p_m$

Since q_1 is irreducible, it is prime (given)

$\Rightarrow$ $q_1 \mid p_i$ for some i

Without loss of generality, we can take $i = 1$

then $\Rightarrow$ $q_1 \mid p_1 \Rightarrow p_1 = q_1u_1$

But p_1 irreducible $\Rightarrow$ q_1 or u_1 is a unit.

As q_1 is not a unit (being irrducible), u_1 will be a unit and thus p_1, q_1 are associates.

Now $(q_1u_1)p_2p_3 \ldots\ldots p_m = q_1q_2 \ldots\ldots q_n$

or $(u_1p_2)p_3 \ldots\ldots p_m = q_2q_3 \ldots\ldots q_n$

$\Rightarrow$ $p_2'p_3 \ldots\ldots p_m = q_2q_3 \ldots\ldots q_n$, $p_2' = u_1p_2$ is irreducible.

R.H.S. contains $n - 1$ elements and result being true for $n - 1$, we find $m - 1 = n - 1 \Rightarrow m = n$.

Also, just as we showed that q_1 is an associate or p_1, we can show that q_2 is an associate of p_2, by considering $p_1p_2 \ldots\ldots p_m = q_2(q_1q_3 \ldots\ldots q_n)$

Thus q_i will be an associate of p_i.

Hence R is a UFD

Since we've already proved that in a UFD every irreducible element is prime, we have proved

Theorem 20: *An integral domain R with unity is a UFD if and only if every non zero, non unit element is a finite product of irreducible elements and every irreducible element is prime.*

Which could be taken as a second definition of a UFD.

Theorem 21: *An integral domain R with unity is a UFD iff every non zero, non unit element is finite product of primes.*

Proof: If R is a UFD then every non zero, non unit element is a finite product of irreducibles (by def.) and also every irreducible element is prime, hence the result follows.

Conversely, let $a \in R$ be a non zero, non unit element. Then $a = p_1 p_2 \ldots p_n$, where p_i are prime elements $\forall\ i$. Since R is an integral domain, prime elements are irreducible and so each p_i is irreducible. We now show that every irreducible element of R is a prime element. Let $x \in R$ be any irreducible element. Then $x \neq 0$, non unit. Thus $x = q_1 q_2 \ldots q_m$ where q_i are prime. Suppose $m > 1$. Since x is irreducible, either q_1 or $(q_2 q_3 \ldots q_m)$ is a unit. But q_1 is prime and thus cannot be a unit. So $(q_2 q_3 \ldots q_m)$ is a unit which implies q_2 is a unit but that is not true as q_2 is a prime. Hence $m = 1$ or that x is prime. By theorem 20 then, R is a UFD. Summing up the above results we have proved

Theorem 22: *If R is an integral domain with unity then the following are equivalent:*

(*i*) *R is a UFD.*

(*ii*) *Every non zero, non unit element of R is a finite product of irreducible elements and every irreducible element is prime.*

(*iii*) *Every non zero, non unit element of R is finite product of prime elements.*

Theorem 23: *In a UFD R any two non zero elements have a g.c.d.*

Proof : Let a, b be any two non zero elements of R.

Suppose one of them (say a) is a unit then $aa^{-1} = 1$

$\therefore \quad b = (aa^{-1})b = a(a^{-1}\ b)$

$\Rightarrow a \mid b$

Also $a = 1.\ a \Rightarrow a \mid a$

Now if $c \mid a$ and $c \mid b$ then as it means $c \mid a$

we get $a = \text{g.c.d.}(a, b)$.

Similarly if b is a unit, $b = \text{g.c.d.}(a, b)$.

Let now a & b be non units. Since R is a UFD we can express

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$$

as product of irreducibles (Note it is possible to express both a, b as product of same irreducibles by suitably choosing the powers).

Let $s_i = \min(\alpha_i, \beta_i)$

we show $d = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$ is g.c.d.(a, b)

Now $a = (p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n})(p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots p_n^{\alpha_n - s_n})$

$= d(p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots p_n^{\alpha_n - s_n})$

$\Rightarrow d \mid a$

Similarly $d \mid b$

Let now $c \mid a$ and $c \mid b$

If c is a unit, $d = (cc^{-1})d \Rightarrow c \mid d$

If c is not a unit, we can write

$c = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$

Since $c \mid a$, $r_i \leq \alpha_i$ for all i

$c \mid b$, $r_i \leq \beta_i$ for all i

$\Rightarrow$ $r_i \leq \min(\alpha_i, \beta_i) = s_i$ for all i

Thus $d = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n} = (p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n})(p_1^{s_1 - r_1} \ldots p_n^{s_n - r_n})$

$\Rightarrow$ $c \mid d$

Hence $d =$ g.c.d.(a, b)

which proves our result.

As seen earlier, if d_1 and d_2 are two g.c.d.s of a, b then d_1 and d_2 are associates.

It should now be a simple exercise for the reader to prove

Theorem 24: *Any two non zero elements in a UFD have an l.c.m.*

Problem 27: *If in a UFD R, a, b are relatively prime then* $a \mid bc \Rightarrow a \mid c$.

Solution: Let $a \mid bc$ then $\exists$ r such that $bc = ar$

If a is a unit

$c = (aa^{-1})c = a(a^{-1}c) \Rightarrow a \mid c$

If b is a unit

$ba = ar \Rightarrow c = b^{-1} ar$

$\Rightarrow c = a(b^{-1} r) \Rightarrow a \mid c$

If c is a unit $bc = ar$

$\Rightarrow b = arc^{-1} \Rightarrow a \mid b$

$\Rightarrow$ g.c.d.$(a, b) = a$

But a, b being relatively prime

g.c.d.(a, b) will be a unit

$\Rightarrow$ a is a unit

$\Rightarrow a \mid c$ as before.

If r is a unit

then $bc = ar$

$\Rightarrow bcr^{-1} = a \Rightarrow a \mid b$

$\Rightarrow$ g.c.d.$(a, b) = b \Rightarrow b$ is a unit

$\Rightarrow a \mid c$ as before.

Suppose now none of a, b, c, r are units.

If $b = 0$, g.c.d.$(a, b) = a$, a unit which is not true

$\therefore \quad b \neq 0.$

If $c = 0$, then $c = a \cdot 0 \Rightarrow a \mid c$

So assuming that $b \neq 0$, $c \neq 0$, we'll get $a \neq 0$, $r \neq 0$ (as $bc = ar$)

Now a, b, c, r being non zero, non units in a UFD we can express

$$a = a_1 a_2 \ldots\ldots a_m$$
$$b = b_1 b_2 \ldots\ldots b_n$$
$$c = c_1 c_2 \ldots\ldots c_t$$
$$r = r_1 r_2 \ldots\ldots r_k$$

as product of irreducible elements.

Thus $(b_1 b_2 \ldots\ldots b_n)(c_1 c_2 \ldots\ldots c_t) = (a_1 a_2 \ldots\ldots a_m)(r_1 r_2 \ldots\ldots r_k) = x$ (say)

then x has two representations as product of irreducible elements. Therefore, by def. of a UFD these representations should have same number of elements and each element on one side will be associate of an element on the other. So $n + t = m + k$ and each a_i is an associate of some b_i or c_i.

If a_i is an associate of some b_i then

$b_i = a_i u$ for a unit u

$\Rightarrow a_i \mid b_i$ and as $b_i \mid b$

we get $a_i \mid b$

$\Rightarrow a_i \mid$ g.c.d.$(a, b) = 1$ as $a_i \mid a$

$\Rightarrow a_i$ is a unit, which is not true as a_i is irreducible

Hence each a_i has to be an associate of some c_i

$\Rightarrow a_i = c_i u_i$ for unit u_i

which gives $(b_1 b_2 \ldots\ldots b_n)(c_1 c_2 \ldots\ldots c_t) = (c_1 u_1 c_2 u_2 \ldots\ldots c_m u_m)(r_1 r_2 \ldots\ldots r_k)$

$\Rightarrow b(c_{m+1} c_{m+2} \ldots\ldots c_t) = (u_1 u_2 \ldots\ldots u_m) r$

$\Rightarrow b(c_{m+1} c_{m+2} \ldots\ldots c_t)(u_1 u_2 \ldots\ldots u_m)^{-1} = r$

$\Rightarrow b \mid r \Rightarrow r = bd$ for some d

$\Rightarrow bc = ar = abd$

$\Rightarrow b(c - ad) = 0 \Rightarrow c = ad. \Rightarrow a \mid c.$

We come now to the proof of a very important theorem that every PID is a UFD, but before that a bit of warming up by proving a few lemmas would be of great help.

Lemma 1: *In a ring R, the union of an ascending chain of ideals* $A_1 \subseteq A_2 \subseteq A_3 \subseteq$ ..... *is an ideal of R.*

Proof: Let $A = \cup A_i$

$x, y \in A \quad \Rightarrow x \in A_i, y \in A_j$ for some i, j

Without loss of generality we take $i \leq j$ then $A_i \subseteq A_j$

$\therefore \quad x, y \in A_j = x - y \in A_j \subseteq A.$

Again $x \in A$, $r \in R$ would imply, similarly that $xr, rx \in A$. Hence the lemma.

Lemma 2: (Ascending Chain Condition): *In a PID R every ascending chain of ideals must terminate after finite number of steps.*

Proof: Let $A_1 \subseteq A_2 \subseteq A_3 \subseteq$ ..... be the given chain.

Let $A = \cup A_i$

Then A is an ideal of R, which being a PID means A is a principal ideal.

Let $A = (a)$.

Then $a \in (a) = A = \cup A_i$

$\Rightarrow a \in A_i$ for some i

$\Rightarrow$ all multiples of a are in $A_i \Rightarrow (a) \subseteq A_i$

$\Rightarrow \quad A \subseteq A_i \subseteq A_{i+1} \subseteq$ .....

i.e., $\quad A \subseteq A_t$ for each $t \geq i$

i.e., $\quad A \subseteq A_i \subseteq A_t \subseteq A$

$\Rightarrow \quad A_i = A_t$

which proves our assertion.

Lemma 3: *Every non zero, non unit element in a PID R is divisible by an irreducible element.*

Proof: Let $a \in R$ be a non zero, non unit element.

Let $I_1 = (a)$.

If I_1 is maximal ideal, then a is irreducible and as $a \mid a$, our lemma stands proved. Suppose I_1 is not maximal, then $\exists$ some ideal $I_2 \neq R$, s.t., $I_1 \subset I_2 \subset R$.

Let $I_2 = (p_2)$.

If I_2 is maximal then p_2 will be irreducible and as $p_2 \mid a$, the lemma is proved. ($a \in I_1 \subset I_2 = (p_2) \Rightarrow a = tp_2$).

Suppose I_2 is not maximal, then $\exists$ an ideal I_3 such that $I_1 \subset I_2 \subset I_3 \subset R$ and proceeding like this we get an ascending chain of ideals in R which by lemma 2 must terminate after a finite number of steps, say at $I_n = (p_n)$ which will then be maximal and p_n will be irreducible with $p_n \mid a$.

We are now ready to prove

Theorem 25: *A PID R is a UFD.*

Proof: Let $a \in R$ be any non zero, non unit element. If a is irreducible then as $a = a$, we can express a as finite product of irreducibles. If a is not irreducible then by lemma 3,

a is divisible by some irreducible element p_1.

$$p_1 | a \Rightarrow a = a_1 p_1 \text{ for some } a_1$$

If a_1 is irreducible we've been able to express a as a product of finite number of irreducible elements.

Suppose a_1 is not irreducible.

Then a_1 is a non zero, non unit element as $a_1 = 0 \Rightarrow a = 0$, which is not so. Again if a_1 is a unit then as $a = a_1 p_1$, we find a and p_1 are associates and so a is irreducible as p_1 is irreducible (see exercises). But a_1 is not irreducible.

Thus again by lemma 3, $\exists$ an irreducible element p_2 such that $p_2 \mid a_1$

$$\Rightarrow \qquad a_1 = p_2 a_2 \text{ for some } a_2$$

If a_2 is irreducible, then as

$$a = a_1 p_1 = p_2 p_1 a_2$$

We are done. If a_2 is not irreducible, we continue like this.

Consider the ideals (a), (a_1), (a_2), ...

Then $$(a) \subseteq (a_1) \subseteq (a_2) \subseteq .....$$

as $$x \in (a) \Rightarrow x = ar = p_1 a_1 r \in (a_1) \text{ etc.}$$

Thus we get an ascending chain of ideals which must terminate after a finite number of steps (by lemma 2). Hence we'll get some irreducible element a_n so that

$$a = p_1 p_2 ..... p_n a_n$$

i.e., a is expressed as a product of finite number of irreducible elements.

We need show now that if a has more than two such representations then the number of elements is same in both and each element in one representation is an associate of an element in the other.

Let $$a = p_1 p_2 ..... p_m = q_1 q_2 ..... q_n$$

and proceed exactly as in theorem 19 and our result is proved.

Remark: For example of a UFD which is not a PID, see examples 16, 17 page 455.

Problem 28: *Show that in any PID every non zero ideal is a unique product of prime ideals*.

Solution: Let $I \neq 0$ be any ideal in a *PID R*.

Suppose $I \neq R$.

Since R is a PID, $I = < a >$ for some a, where a will not be a unit otherwise $I = R$.

Thus a is non zero, non unit element of R.

Now R being a PID is a UFD and, therefore, we can express

$$a = p_1 p_2 ..... p_r \text{ where } p_i \text{ are irreducible.}$$

Let $P_i = < p_i >$ then each P_i is a maximal ideal

$\Rightarrow$ each P_i is a prime ideal. (See problem 28, page 390)

Now $$a = p_1 p_2 ..... p_r \in P_1 P_2 ..... P_r$$

$\Rightarrow$ multiples of a are in $P_1 P_2 ..... P_r$

$$\Rightarrow < a > \subseteq P_1 P_2 ..... P_r$$

$\Rightarrow I \subseteq P_1P_2 \ldots\ldots P_r$

Again let $b \in P_1P_2 \ldots\ldots P_r$ be any element, then

$b = (x_1x_2 \ldots\ldots x_r) + (y_1y_2 \ldots\ldots y_r) + \ldots\ldots$ (finite sum)

$x_i, y_i, \ldots\ldots \in P_i$

Now $x_1 \in P_1 = \langle p_1 \rangle \Rightarrow x_1 = p_1k_1$

Similalry $x_2 = p_2k_2$

$\ldots\ldots\ldots$

$x_r = p_rk_r$

$\Rightarrow x_1x_2 \ldots\ldots x_r = p_1p_2 \ldots\ldots p_rk_1k_2 \ldots\ldots k_r = a(k_1k_2 \ldots\ldots k_r) \in \langle a \rangle = I$

Similaly, $y_1 y_2 \ldots\ldots y_r \in I$ and others are also in I

$\Rightarrow b \in I$

$\Rightarrow P_1P_2 \ldots\ldots P_r \subseteq I$

$\Rightarrow I = P_1P_2 \ldots\ldots P_r$

uniqueness follows from the fact that each p_i is uniquely determined.

Definition: Let R be a UFD and let

$f(x) = a_o + a_1x + \ldots\ldots + a_nx^n \in R[x]$ be a non zero polynomial.

Then d = g.c.d.$(a_0, a_1, \ldots\ldots, a_n)$ is called the *content* of $f(x)$ and is denoted by $c(f)$.

A polynomial $f(x)$ is called *primitive* if $c(f)$ is a unit.

Since g.c.d. is not essentially unique, one may have more than one content of a polynomial. Two contents would, however, be associates.

Example 12: $f(x) = 8x^3 + 6x + 1 \in \mathbf{Z}[x]$ is primitive

whereas $g(x) = 8x^3 + 6x + 2 \in \mathbf{Z}[x]$ is not primitive

as $c(f)$ = g.c.d.$(8, 6, 1) = 1$ whereas $c(g) = 2$

Since $g(x) = 2\,(4x^3 - 3x - 1) = 2g_1(x)$ where $c(g_1) = 1$

we find it is pcssible to write

$g(x) = 2g_1(x)$ where $g_1(x) =$ is primitive

In fact, we can prove

Theorem 26: *If $f(x)$ be a non zero polynomial in $R[x]$ where R is a UFD, then $f(x) = df_1(x)$ where f_1 is primitive and $d = c(f)$.*

Proof: Let $f(x) = a_o + a_1x + \ldots\ldots + a_nx^n$

and let $c(f) = d$ = g.c.d.$(a_o, a_1, \ldots\ldots a_n)$

Then $d \mid a_i$ for all i

$\Rightarrow a_i = du_i$ for some u_i

$f(x) = du_o + du_1x + \ldots\ldots + du_nx^n$

$= d(u_o + u_1x + \ldots\ldots + u_nx^n) = df_1(x)$ where $f_1(x)$ will be primitive.

Note: If t = g.c.d.$(u_o, u_1, \ldots\ldots, u_n)$

then $t \mid u_i \ \forall\ i \ \Rightarrow td \mid du_i \ \ \forall\ i$

$\Rightarrow$ $td \mid a_i \ \forall\ i$ and thus $td \mid d$

$\Rightarrow$ $t \mid 1$ or that t is a unit.

Theorem 27: (Gauss' Lemma): *Let R be a UFD, then in $R[x]$ the product of two primitive polynomials is a primitive polynomial.*

Proof: Let $f(x) = a_o + a_1x + ... + a_mx^m$

$g(x) = b_o + b_1x + ... + b_nx^n$

be two primitive polynomials in $R[x]$, then $f(x)$ and $g(x)$ are non zero (by definition). Thus

$f(x)g(x) = c_o + c_1x + c_2x^2 + ...$ is also non zero.

Let d = g.c.d.$(c_o, c_1, c_2, ...)$

We show d is a unit. Suppose it is not, then there exists an irreducible element p s.t., $p|d$.

[Recall that in a UFD, a non unit element a can be expressed as a product of irreducibles, $a = p_1p_2 ..... p_n \Rightarrow p_1 \mid a$]

Thus $p \mid d \Rightarrow p \mid c_i$ for all i ...(1)

Now if $p \mid a_i$ for all i then $p \mid$ g.c.d.$(a_o, a_1, ..., a_m)$, which is a unit, say, u.

Now $p \mid u \Rightarrow u = pk \Rightarrow 1 = p(ku^{-1})$

$\Rightarrow p$ is a unit,

which is not true as p is irreducible.

$\therefore$ $p \nmid a_i$ for some i

Let i be such least +ve integer, then

$p \mid a_o, p \mid a_1, ..., p \mid a_{i-1}, p \nmid a_i$

Similarly $\exists$ some integer j, s.t.,

$p \mid b_o, p \mid b_1, ..., p \mid b_{j-1}, p \nmid b_j$

Now $c_{i+j} = (a_ob_{i+j} + a_1b_{i+j-1} + ... + a_{i-1}\, b_{j+1})$

$+ a_ib_j + (a_{i+1}\, b_{j-1} + ... + a_{i+j}\, b_o)$

Since $p \mid c_{i+j}$ by (1) and also

$p \mid (a_ob_{i+j} + a_1b_{i+j-1} + ... + a_{i-1}\, b_{j+1})$,

$p \mid (a_{i+1}\, b_{j-1} + ... + a_{i+j}\, b_0)$

we find $p \mid a_ib_j$, but p being irreducible in a UFD is prime

$\Rightarrow p \mid a_i$ or $p \mid b_j$, a contradiction. Hence the result.

Cor.: If R is a UFD and $f(x), g(x) \in R[x]$, then

$c(fg) = c(f)\ c(g)$ (up to units)

Since we can write $f(x) = df_1(x)$, $d = c(f)$

$g(x) = d'g_1(x)$, $d' = c(g)$

$f(x)g(x) = dd'f_1(x)\ g_1(x)$

where f_1, g_1 being primite give f_1g_1 to be primitive

$c(f_1 g_1) = 1$ (or a unit)

$\therefore \quad c(fg) = dd' = c(f)\ c(g)$

Converse of Gauss' Lemma is also true as we can prove

Theorem 28: *If $f(x)g(x)$ is primitive polynomial in $R[x]$, R being a UFD then so are $f(x)$ and $g(x)$.*

Proof: fg is primitive

$\Rightarrow$ $c(fg)$ is a unit

$\Rightarrow$ $\exists$ an element $r \in R$ s.t., $c(fg)r = 1$

$\Rightarrow$ $c(f)\ c(g)\ r = 1$

$\Rightarrow$ $c(f)\ [c(g)\ .\ r] = 1$

$\Rightarrow$ $c(f)$ is a unit $\Rightarrow f$ is primitive.

Similarly $c(g)$ is a unit $\Rightarrow g$ is primitive.

Theorem 29: *If R is an integral domain with unity, then units of R and $R[x]$ are same.*

Proof: Let a_o be a unit of R.

Then $\exists\ b_o \in R$ s.t., $a_o b_o = 1$

Let $f(x) = a_o + 0.x + 0.x^2 + ...$

$g(x) = b_o + 0.x + 0.x^2 + ...$

then $f(x)g(x) = a_o b_o + 0.x + 0.x^2 + ...$

$= 1 = 1 + 0.x + 0.x^2 + ...$

$\Rightarrow f(x)$ is a unit in $R[x]$

i.e., a_o is a unit in $R[x]$.

Conversely, let $f(x)$ be any unit of $R[x]$

Then $\exists\ g(x) \in R[x]$ s.t.,

$f(x)g(x) = 1\ (= 1 + 0.x + 0.x^2 + ...)$

$\Rightarrow$ deg (fg) = deg 1

$\Rightarrow$ deg f + deg $g = 0$

$\Rightarrow$ deg f = deg $g = 0$

$\Rightarrow$ f and g are constant polynomials

i.e., $f(x) = a_o + 0x + 0x^2 + ...\ \ a_o \in R$

$g(x) = b_o + 0x + 0x^2 + ...\ \ b_o \in R$

Since $fg = a_o b_o = 1$

we find, $a_o = f(x)$ is a unit of R

Hence the result.

Problem 29: *Show that $2x + 1$ is a unit in $\mathbf{Z}_4[x]$.*

Solution: Since $(2x + 1)\ (2x + 1) = 0x^2 + 0x + 1 = 1$

$[4 = 0$ in $\mathbf{Z}_4]$

we find $2x + 1$ is a unit in $\mathbf{Z}_4[x]$.

Remark: Notice $2x + 1$ is a non constant polynomial and therefore, does not belong to $\mathbf{Z}_4$ and thus cannot be a unit in $\mathbf{Z}_4$. But then $\mathbf{Z}_4$ is not an integral domain. In fact, 1 and 3 are units of $\mathbf{Z}_4$. [$3 \otimes 3 = 1$].

Theorem 30: *If R is an integral domain with unity and a is an irreducible element of R then a is irreducible element of $R[x]$.*

Proof: Suppose a is not irreducible element of $R[x]$ then $\exists\ p(x), q(x) \in R[x]$ s.t., $a = p(x)\ q(x)$

where $p(x)$ and $q(x)$ are non units.

Now $a = pq$

$\Rightarrow$ deg a = deg p + deg q

$\Rightarrow$ 0 = deg p + deg q

$\Rightarrow$ deg p = deg q = 0

$\Rightarrow p, q$ are constant polynomials $\Rightarrow p, q \in R$

Thus $a = pq, p, q \in R$ and p, q are non units [units of R and $R[x]$ are same], a contradiction to the fact that a is irreducible in R.

Hence the result follows. (See theorem 32 also).

Definition: Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree (*i.e.*, of deg ≥ 1) is said to be an *irreducible polynomial* over R if it cannot be expressed as product of two polynomials of positive degree.

In other words, if whenever $f(x) = g(x)h(x)$,

then deg $g = 0$ or deg $h = 0$

A polynomial of positive degree which is not irreducible is called *reducible* over R.

Example 13: $x^2 + 1 \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Z}$.

whereas it is reducible over $\mathbf{C}$

as $x^2 + 1 = (x - i)\ (x + i)$

Again $x^2 - 2$ is irreducible over $\mathbf{Z}$, but reducible over $\mathbf{R}$, the reals as

$$x^2 - 2 = (x - \sqrt{2})\ (x + \sqrt{2})$$

Remarks: (*a*) Any polynomial of degree 1 is irreducible over a field F.

(*b*) If $f(x) \in F[x]$ is any polynomial of degree > 1 and $f(a) = 0$ for some $a \in F$ then $f(x)$ is reducible over F.

By division algorithm, for $f(x)$, $g(x) = (x - a)$, we can find t and r such that $f(x) = (x - a)t(x) + r$, where, either $r = 0$ or deg $r <$ deg $(x - a)$, *i.e.*, either $r = 0$ or is a constant polynomial.

Since $f(a) = 0$, we get $0 = f(a) = r$

$\Rightarrow f(x) = (x - a)\ t(x)$

$\Rightarrow$ deg f = deg $(x - a)$ + deg $t(x)$

$\Rightarrow$ deg $t(x) \geq 1$ as deg $f > 1$, deg $(x - a) = 1$

thus f is reducible.

(c) Let $f(x) \in F[x]$ be a polynomial of degree 2 or 3 then $f(x)$ is reducible implies $\exists\ a \in F$; s.t., $f(a) = 0$

$f(x)$ is reducible $\Rightarrow f(x) = g(x)h(x)$ where deg g, deg $h \geq 1$

Now $\deg f = \deg g + \deg h$

$\Rightarrow 2, 3 = \deg g + \deg h$

$\Rightarrow$ one of deg g or deg h is 1

Let deg $g = 1$ and suppose $g(x) = a_o + a_1 x$, $(a_1 \neq 0)$

then $g(-a_o a_1^{-1}) = 0$

$\Rightarrow f(-a_o a_1^{-1}) = 0$. Take $a = -a_o a_1^{-1}$.

(d) $f(x) \in F[x]$ a polynomial of degree 2 or 3 is reducible iff $\exists\ a \in F$ such that $f(a) = 0$

Follows by (b) and (c).

(e) The fact that $f(a) = 0$ is also expressed by saying that a is a *root* or a *zero* of the polynomial $f(x)$.

(f) Polynomials of degrees greater than 3 may be reducible over a field even though they have no root in the field.

For instance, the polynomial $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1) \in \mathbf{Q}[x]$, but has no root in $\mathbf{Q}$.

We should be careful while talking about irreducible elements and irreducible polynomials as the following example shows us the difference between the two.

Example 14: Consider the polynomial $2x^2 + 2$

Since it cannot be expressed as product of two positive degree polynomials in $\mathbf{Z}[x]$, we notice it is irreducible polynomial over $\mathbf{Z}$.

Again $2x^2 + 2 = 2(x^2 + 1)$

$=$ product of two polynomials

$= gh$ (say)

Since g and h are non units in $\mathbf{Z}[x]$ as 1, – 1 are the only units of $\mathbf{Z}$ and, therefore, of $\mathbf{Z}[x]$ we find $2x^2 + 2$ can be expressed as product of two non units and thus $2x^2 + 2$ is *not* an irreducible element in $\mathbf{Z}[x]$. Hence an *irreducible polynomial need not be an irreducible element*.

The converse, however, follows by

Theorem 31: *Every irreducible element in $R[x]$ is an irreducible polynomial, R being an integral domain with unity.*

Proof: Let $f(x) \in R[x]$ be any irreducible element.

Suppose $f(x)$ is reducible polynomial,

then $f(x) = g(x)h(x)$, $g, h \in R[x]$, with deg $g > 0$, deg $h > 0$

Since degree of g and h is positive, g and h are not constant polynomials

$\therefore$ $g, h \notin R$

$\Rightarrow$ g, h cannot be units in R

$\Rightarrow$ g, h cannot be units in $R[x]$

$\Rightarrow$ f is not irreducible element.

a contradiction which proves our result. (See remark on page 450)

Example 15: The polynomial $f(x) = x^2 - 2x - 15$

is both primitive as well as reducible over $\mathbf{Z}$ as

$$c(f) = \text{g.c.d.}(1, -2, -15) = 1$$

and $$x^2 - 2x - 15 = (x - 5)(x + 3)$$

However, the polynomial $x^2 - 2$ is primitive as well as irreducible over $\mathbf{Z}$.

Theorem 32: *If R is a UFD then any $f(x) \in R[x]$ is an irreducible element of $R[x]$ iff either f is an irreducible element of R or f is an irreducible primitive polynomial of $R[x]$.*

Proof: Let $f(x) \in R[x]$ be an irreducible element of $R[x]$. If $f \in R$ then f will be irreducible element of R as well. [Units of R and $R[x]$ are same.]

Suppose $f \notin R$, we show f is then irreducible primitive polynomial of $R[x]$.

Suppose $f = gh$ for some $g, h \in R[x]$.

Since f is irreducible element of $R[x]$, one of g or h must be a unit of $R[x]$.

$\Rightarrow$ one of g or h must be in R (as units of $R[x]$ and R are same).

$\Rightarrow$ deg $g = 0$ or deg $h = 0$

thus f is not reducible or that f is irreducible polynomial of $R[x]$.

(In fact, it follows by theorem 31).

Again since any polynomial $f(x)$ can be written as a product of $c(f)$ and a primitive polynomial we can write $f = df_1$ where $c(f) = d \in R$ and f_1 is primitive.

Since $d \in R$, deg f_1 = deg f

$\Rightarrow$ deg $f_1 \geq 1$

$\Rightarrow f_1 \notin R$

$\Rightarrow f_1$ cannot be a unit of $R[x]$.

Thus $f = df_1$, f_1 is not a unit, f is irreducible element.

$\Rightarrow$ d is a unit

$\Rightarrow$ $c(f)$ = unit

$\Rightarrow$ f is primitive polynomial.

Conversely, if f is an irreducible element of R then f is an irreducible element of $R[x]$, (see theorem 30).

Suppose now f is an irreducible primitive polynomial of $R[x]$. We show f is irrdeucible element of $R[x]$.

Since f is irreducible polynomial, deg $f \geq 1$

and so $f \notin R$

$\Rightarrow f$ cannot be a unit [as units of R and $R[x]$ are same]. Also, of course, f is non zero.

Suppose now $f(x) = g(x)h(x)$ for some $g, h \in R[x]$.

Since f is irreducible polynomial

either deg $g = 0$ or deg $h = 0$

Without any loss of generality, we can take deg $g = 0$.

$\Rightarrow$ g is a constant polynomial say, $b_o + 0x + 0x^2 + ...$

$\Rightarrow$ $g \in R$

Now $c(f) = c(gh) = c(g)\ c(h)$

f being primitive, $c(f)$ = unit u

$c(g)\ c(h) = u \Rightarrow c(g) \mid u$

$\Rightarrow$ $c(g)$ is a unit

or that g is a unit of $R[x]$.

(Unit = $c(g)$ = g.c.d.$(b_o) = b_o = g$)

Hence $f(x)$ is irreducible element of $R[x]$.

Remark: If F is a field then every irreducible polynomial of $F[x]$ is irrdeducible element of $F[x]$ and conversely.

Let $f(x)$ be irreducible polynomial in $F[x]$ and suppose $f = gh$.

Since f is irreducible polynomial,

either deg $g = 0$, or deg $h = 0$.

Suppose deg $g = 0$, then g is a constant polynomial, say,

$g(x) = b_o + 0.x + 0x^2 + ...$

where $b_o \in F$, $b_o \neq 0$, $\therefore b_o^{-1} \in F$

i.e., $b_o = g$ is a unit in F and, therefore, a unit in $F[x]$.

Thus f is irreducible element of $F[x]$.

Notice, since f is irreducible polynomial, deg $f \geq 1$ and so f is non zero, non unit element of $F[x]$.

Converse follows by theorem 31.

Theorem 33: *If F is a field then an ideal $< p(x) > \neq \{0\}$ in $F[x]$ is maximal iff $p(x)$ is irreducible in $F[x]$.*

Proof: If $p(x)$ is irreducible polynomial over F, then it is irreducible element of $F[x]$ and also since F is a field, $F[x]$ is a PID which is not a field. (See page 423). The result now follows by theorem 10 on page 413.

Problem 30: *Show that* $\dfrac{\mathbf{Q}[x]}{I}$ *where* $I = < x^2 - 5x + 6 >$ *is not a field.*

Solution: Since $x^2 - 5x + 6 = (x - 2)\ (x - 3)$ we find it is not irreducible polynomial over **Q.**

Thus $I = < x^2 - 5x + 6 >$ is not a maximal ideal of $\mathbf{Q}[x]$ and hence $\dfrac{\mathbf{Q}[x]}{I}$ is not a field.

Problem 31: *Show that $f(x) = x^3 - 9$ is reducible in* $\mathbf{Z}_{11}$.

Solution: Since $4 \otimes 4 \otimes 4 = 9$ in $\mathbf{Z}_{11}$, we find $(x - 4)$ is a factor of $x^3 - 9$. By actual division we find

$$x^3 - 9 = (x - 4)\ (x^2 + 4x + 5) \text{ in } \mathbf{Z}_{11}.$$

Hence $x^3 - 9$ is reducible.

Problem 32: *Show that* $\mathbf{Z}_5[x]$ *is a UFD. Is* $x^2 + 2x + 3$ *reducible over* $\mathbf{Z}_5[x]$?

Solution: Since 5 is a prime, $\mathbf{Z}_5$ is a field

$\Rightarrow$ $\mathbf{Z}_5$ is a UFD

$\Rightarrow$ $\mathbf{Z}_5[x]$ is a UFD. (See theorem 34 on page 455)

Again $x^2 + 2x + 3$ will be reducible over $\mathbf{Z}_5$ if it has a root in $\mathbf{Z}_5$, but none of the elements in $\mathbf{Z}_5$ is a root of $x^2 + 2x + 3$, hence it is an irreducible polynomial over $\mathbf{Z}_5$.

Problem 33: *Show that the polynomial* $x^2 + x + 2$ *is irreducible over* $F = \{0, 1, 2\}$ *mod* 3. *Use it to construct a field of* 9 *elements.*

Solution: Let $f(x) = x^2 + x + 2$. If it is reducible over F, we should be able to find some $\alpha \in F$ s.t., $f(\alpha) = 0$. [See remark (*c*) on page 448.]

But for no $\alpha \in F$, $f(\alpha) = 0$. [For example, for $\alpha = 1$, $1^2 + 1 + 2 = 1 \neq 0$ etc.]

Thus $f(x)$ is irreducible polynomial over F and as F is a field, $f(x)$ is irreducible element of $F[x]$. Hence $< f(x) >$ is a maximal ideal of $F[x]$ proving thereby that $\frac{F[x]}{< f(x) >}$ is a field.

Any element of this field is of the type

$$p(x) + < f(x) >, \text{ where } p(x) \in F[x].$$

Since $F[x]$ is a Euclidean domain,

for $f(x)$, $p(x) \in F[x]$, $\exists$ $t(x)$, $r(x)$ s.t.,

$$p(x) = f(x)t(x) + r(x), \text{ where either}$$

$r(x) = 0$ or $\deg r(x) < \deg f(x) = 2$

In either case $r(x)$ is of the type $ax + b$, $a, b \in F$

So $p(x) - r(x) = f(x)\ t(x) \in < f(x) >$

i.e., $p - r \in I$, where $I = < f(x) >$

$\Rightarrow$ $p - r + I = I$

i.e., $p + I = r + I = ax + b + < f(x) >$

Hence any member $p + < f(x) >$ of $\frac{F[x]}{< f(x) >}$ is of the type $ax + b + < f(x) >$.

Thus $$\frac{F[x]}{< f(x) >} = \{ax + b + < f(x) > \mid a, b \in F\}$$

Since $a \in F = \{0, 1, 2\}$ can be chosen in three ways and for each choice of a, b can be selected in three ways, we find the number of elements of $\frac{F[x]}{< f(x) >}$ will be $3 \times 3 = 9$. Thus $\frac{F[x]}{< f(x) >}$ is the required field of nine elements.

Remark: Theorem 33 also implies that if F is a field and $<p(x)>$ is an ideal of $F[x]$ then, $\frac{F[x]}{<p(x)>}$ is a field iff $p(x)$ is irreducible over F.

Problem 34: *Show that the polynomial* $x^3 + 2x + 1$ *is irreducible in* $\mathbf{Z}_3[x]$ *and use it to construct a field with* 27 *elements. Find the inverse of* $x^2 + I$ *in that field* [*where* $I = < x^3 + 2x + 1 >$].

Solution: It is easily seen that there doesn't exist any $\alpha \in \mathbf{Z}_3 = \{0, 1, 2\}$ mod 3 s.t., $\alpha^3 + 2\alpha + 1 = 0$. Hence $f(x) = x^3 + 2x + 1$ is irreducible over $\mathbf{Z}_3$ and as in previous problem $\frac{\mathbf{Z}_3[x]}{<f(x)>}$ is a field. Also this field is given by

$$\frac{\mathbf{Z}_3[x]}{<f(x)>} = \{a_0 + a_1x + a_2x^2 + <f(x)> \mid a_i \in \mathbf{Z}_3\}$$

Let $<f(x)> = I$

Then $\frac{\mathbf{Z}_3[x]}{I} = \{a_0 + a_1x + a_2x^2 + I \mid a_i \in \mathbf{Z}_3\}$

Clearly since a_i vary in $\mathbf{Z}_3 = \{0, 1, 2\}$, $\frac{\mathbf{Z}_3[x]}{I}$ has $3 \times 3 \times 3 = 27$ elements.

Suppose now $p(x) + I$ is inverse of $x^2 + I$ in $\frac{\mathbf{Z}_3[x]}{I}$.

Then $(p(x) + I)(x^2 + I) = 1 + I$

$\Rightarrow p(x)\,x^2 + I = 1 + I \quad \Rightarrow p(x)\,x^2 - 1 \in I = <f(x)>$

i.e., $p(x)x^2 - 1$ is a multiple of $f(x)$. Thus $\exists$ some $t(x)$ s.t.,

$$p(x)x^2 + t(x)\,f(x) = 1$$

To find $p(x)$ we use Euclidean algorithm

$$x^2\overline{)x^3 + 2x + 1}\ \Big|\ x$$
$$\underline{x^3}$$
$$2x + 1$$

$$2x + 1\overline{)x^2}\ \Big|\ 2x + 2$$
$$\underline{x^2 + 2x}$$
$$x$$
$$\underline{x + 2}$$
$$1$$

Notice operations are in $\mathbf{Z}_3$

Thus

$$x^3 + 2x + 1 = x(x^2) + (2x + 1)$$
$$x^2 = (2x + 2)(2x + 1) + 1$$

giving
$$1 = x^2 - (2x + 2)(2x + 1)$$
$$= x^2 - [(2x + 2)\{(x^3 + 2x + 1) - x(x^2)\}]$$
$$= x^2 - (2x + 2)(x^3 + 2x + 1) + x(x^2)(2x + 2)$$
$$= x^2[1 + x(2x + 2)] - (2x + 2)(x^3 + 2x + 1)$$
$$1 = x^2(2x^2 + 2x + 1) - (2x + 2)(x^3 + 2x + 1)$$

Hence $p(x) = 2x^2 + 2x + 1$ and thus inverse of $x^2 + I$ in $\frac{\boldsymbol{Z}_3[x]}{I}$ is $(2x^2 + 2x + 1) + I$.

Problem 35: *Let F be a field and $p(x), f(x), g(x) \in F[x]$ where $p(x)$ is irreducible over F. Show that if $p(x) \mid f(x)g(x)$* then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Solution: Since $p(x)$ is irreducible $\frac{F[x]}{< p(x) >}$ is a field and therefore an integral domain. Let $I = < p(x) >$ and suppose $\varphi : F[x] \to \frac{F[x]}{I}$ is the natural homomorphism, then

$$\varphi(f(x)) = f(x) + I,\ \varphi(g(x)) = g(x) + I$$

Now $p(x) \mid f(x)g(x) \Rightarrow f(x)g(x) \in < p(x) > = I$

$\Rightarrow fg + I = I$

$\Rightarrow (f + I)(g + I) = 0 + I$

$\Rightarrow$ either $f + I = I$ or $g + I = I$

$\Rightarrow f \in I$ or $g \in I$, $I = < p(x) >$

$\Rightarrow p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Lemma: *If R is a UFD and $p(x)$ is primitive polynomials in $R[x]$ then it can be factored in a unique way as a product of irreducible elements of $R[x]$.*

Proof: Let K be the field of quotients of R, then $K[x]$ is a Euclidean domain and hence a PID and thus a UFD.

Now $p(x) \in R[x] \Rightarrow p(x) \in K[x]$ and as $K[x]$ is a UFD we can express $p(x) = p_1(x)\ p_2(x)\ .....\ p_k(x)$.

as product of irreducible elements $p_i(x)$ of $K[x]$.

Again $p_i(x) \in K[x] \Rightarrow p_i(x) = \frac{1}{a_i} f_i(x)$

where $a_i \in R,\ f_i \in R[x]$

Since $p_i(x) \in K[x] \Rightarrow p_i(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + ...$

where $\alpha_i \in K$, which being field of quotients of R, means each α_i can be expressed as $\frac{b_i}{a_i}$ $a_i, b_i \in R,\ a_i \neq 0$

or that $p_i(x) = \frac{b_o}{a_o} + \frac{b_1}{a_1} x + \frac{b_2}{a_2} x^2 + ...$

$$= \frac{1}{a}\ [c_o + c_1 x + c_2 x^2 + ...] = \frac{1}{a}\ f(x), \qquad f \in R[x]$$

Again $p_i(x)$ is irreducible element in $K[x]$.

$f_i(x)$ will be irreducible element in $K[x]$ because if it is not so then we can write it as $f_i = g_i\ h_i$ where g_i, h_i are non units.

$\Rightarrow p_i = \dfrac{1}{a_i}\, g_i\, h_i$, where g_i, h_i are non units

$\Rightarrow p_i$ is not irreducible element

Again $f_1(x) \in R[x] \Rightarrow f_i = d_i f_i^*(x)$ where $f_i^*(x)$ is primitive and $d_i = c(f_i)$

$$\therefore \qquad p_i = \frac{d_i}{a_i}\, f_i^*,\ i = 1, 2, \ldots, k$$

$$\Rightarrow p_1 p_2 \ldots p_k = \frac{d_1 d_2 \ldots d_k}{a_1 a_2 \ldots a_k}\, f_1^* f_2^* \ldots f_k^*$$

$$\Rightarrow p = \frac{d_1 d_2 \ldots d_k}{a_1 a_2 \ldots a_k}\, f_1^* f_2^* \ldots f_k^*$$

$$\Rightarrow (a_1 a_2 \ldots a_k)p = (d_1 d_2 \ldots d_k)(f_1^* f_2^* \ldots f_k^*) \qquad \ldots(1)$$

Now as $p_i = \dfrac{d_i}{a_i} f_i^*$ and p_i is irreducible element we find f_i^* will also be irreducible element of $K[x]$ otherwise p_i will not remain irreducible element (as seen earlier).

Content of L.H.S. of (1) is $(a_1 a_2 \ldots a_k)u$ for some unit u as p is primitive and content of R.H.S. of (1) is $(d_1 d_2 \ldots d_k)v$, for some unit v as f_i^* are primitive.

Equating the contents of both sides we get

$$a_1 a_2 \ldots a_k = (d_1 d_2 \ldots d_k)w \quad \text{where } w = vu^{-1} \text{ is a unit.}$$

Thus $\qquad p(x) = (w^{-1} f_1^*)\ (f_2^* f_3^* \ldots f_k^*)$

which is a product of irreducible elements in $K[x]$. Again f_i^* being primitive and irreducible elements in $K[x]$, we find f_i^* will be irreducible elements in $R[x]$. To show uniqueness

Let $p(x) = r_1(x)\ r_2(x) \ldots r_k(x)$, where $r_i(x)$ are irreducible in $R[x]$.

(Notice the number of elements in the product remain same as k as we are in a UFD)

Now $p(x)$ primitive $\Rightarrow$ each r_i is primitive

because $\qquad p = r_1 r_2 \ldots r_k \ \Rightarrow c(p) = c(a_1)\ c(a_2) \ldots c(a_k)$

$\Rightarrow d = d_1 d_2 \ldots d_k$

$\Rightarrow$ each d_i is a unit

$\Rightarrow$ each a_i is primitive

Hence each a_i is primitive and irreducible element in $R[x]$

$\Rightarrow r_i(x)$ is irreducible in $K[x]$ for all i.

But $K[x]$ being a UFD, each r_i is uniquely determined upto associates in $K[x]$.

$\Rightarrow r_i$ & f_i^* are associates for all i

$\Rightarrow r_i = u_i f_i^*$

where u_i is a unit in $K[x]$ and thus in $K \Rightarrow u_i$ is of the form $\dfrac{a_i}{b_i}$

Hence $\qquad r_i = \dfrac{a_i}{b_i}\, f_i^*$

$$\Rightarrow b_i r_i = a_i f_i^*$$

Equating contents on both sides, we get

$b_i = ua_i$ for some unit u in R or $\frac{a_i}{b_i} = u^{-1}$ a unit in R or that r_i is associate of f_i^* in $R[x]$.

Theorem 34: *R is a UFD $\Rightarrow R[x]$ is a UFD.*

Proof: Let $f \in R[x]$ be non zero, non unit element.

Let $f = d f^*(x)$ where $d = c(f)$, f^* is primitive.

By lemma

$f^* = f_1^* f_2^* \ldots . f_x^*$ where f_i^* are irreducible elements of $R[x]$ and this representation is unique upto associates.

Also $d \in R$ and R is a UFD, thus either d is a unit or it can be written as

$$d = d_1 d_2 \ldots . d_r$$

where d_i are irreducible elements in R.

If d is a unit

$$f = d f^* \text{ gives}$$

$$f = (df_1^*) f_2^* \ldots . f_k^*, \quad df_1^*, f_2^*, \ldots . f_x^* \text{ are irreducible,}$$

which gives us the result.

If d is not a unit, let $d = d_1 d_2 \ldots . d_r$

Since each d_i is irreducible element of R each d_i will be irreducible element of $R[x]$, thus f = finite product of irreducible elements in $R[x]$ and representation is unique upto associates thereby proving our theorem.

Remark: $a, b \in R$ are associates in R iff a, b are associates in $R[x]$. The result follows as units of R and $R[x]$ are same.

Example 16: Let F be a field then we've already seen that $F[x, y]$ is not a PID.

Now F being a field is a UFD and therefore by above theorem $F[x, y]$ will be a UFD. Thus $F[x, y]$ is an example of a UFD which is not a PID.

Example 17: $\mathbf{Z}$ is a PID and thus a UFD $\Rightarrow \mathbf{Z}[x]$ is UFD.

But $\mathbf{Z}[x]$ is not a PID otherwise $\mathbf{Z}$ has to be a field, which it is not and hence $\mathbf{Z}[x]$ is a UFD but not PID. (See Cor. 1 page 428).

Theorem 35: *Let R be a UFD and $f(x) \in R[x]$ be primitive polynomial. If $f(x)$ is irreducible element of $K[x]$ then $f(x)$ is an irreducible element of $R[x]$.*

Proof: Suppose $f(x)$ is not irreducible element of $R[x]$

Then $f = gh$, $g, h \in R[x]$ are non units

Also we can write

$$g = dg^*(x)$$

$$h = d'h^*(x), \text{ where } g^* \text{ and } h^* \text{ are primitive}$$

$\Rightarrow f = dd'g^*h^*$

Equating contents on both sides, we get

$u = dd'vw$ as f is primitive and so are g^*, h^*

where u, v, w are units

Thus $1 = dd'vwu^{-1}$

$\Rightarrow d$ is a unit

Similarly d' is a unit

$\Rightarrow g = dg^*$

$\Rightarrow c(g) = c(dg^*) = dc(g^*) =$ unit $\times$ unit = unit

$\Rightarrow g$ is primitive

Similarly h is primitive

Again $g, h \in R[x] \Rightarrow g, h \in K[x]$

Now $f = gh$, f is irreducible element of $K[x]$

$\Rightarrow g$ or h is a unit of $K[x]$

Without any loss of generality let g be a unit in $K[x]$

Then $\exists\ r \in K[x]$, s.t., $gr = 1$

$\Rightarrow \deg g + \deg r = 0$

$\Rightarrow \deg g = \deg r = 0$

$\Rightarrow g, r \in K$

Let $g = \dfrac{\alpha}{\beta}, \quad \alpha, \beta \in R$

Then $f = \dfrac{\alpha}{\beta} h$ or that $\beta f = \alpha h$

$\Rightarrow c(\beta f) = c(\alpha h)$

$\Rightarrow \beta u = \alpha v, \quad u, v$ being units, (f, g primitive)

$\Rightarrow \dfrac{\alpha}{\beta} = uv'$

$\Rightarrow g = \dfrac{\alpha}{\beta} = uv' =$ unit in R

$\Rightarrow g$ is a unit in $R[x]$

a contradiction giving us the result.

We now prove the converse in

Theorem 36: *If $f(x) \in R[x]$ is both primitive and irreducible element of $R[x]$ then $f(x)$ is irreducible element of $K[x]$.*

Proof: Suppose $f(x)$ is not irreducible element of $K[x]$

Then $f = gh$, where f, g are non units in $K[x]$

Thus f, g are non units of K.

i.e., $f, g \notin K$

Note if $g \in K$ then as $g \neq 0$, it will have multiplicative inverse being an element of a field and hence will be a unit.

Thus $\deg g, \quad \deg h > 0$

Now $g(x) = \frac{1}{d}\ g_o(x)$

$\Rightarrow g_o(x) = dg(x) \in R[x]$

Similarly $h_o(x) = d'h(x) \in R[x]$

Again $g_o(x) = \alpha g^*(x)$

$h_o(x) = \beta h^*(x)$ where g^*, h^* are primitive

and α, β are g.c.d. of coeffs. of g_o and h_o

$\therefore \quad c(g_o) = \alpha,\ c(h_o) = \beta$

$\therefore \quad f(x) = \frac{1}{dd'}\ \alpha\beta g^* h^*$

$\Rightarrow dd'f = \alpha\beta g^* h^*$

Since g^*, h^* are primitive, by Gauss Lemma g^*h^* will be primitive.

$\Rightarrow c(dd'f) = c(\alpha\beta g^* h^*) = \alpha\beta$

$\Rightarrow dd' = u\alpha\beta$ as f is primitive

$\Rightarrow f(x) = u^{-1}g^*(x)\ h^*(x), \qquad g^*, h^* \in R[x],\ u \in R$

$\deg u^{-1}g^* = \deg g^* = \deg \alpha g^*$

$= \deg g_0 = \deg \frac{1}{d} g_0 = \deg g > 0$

Also $\deg h^* = \deg h > 0$

$\therefore \quad u^{-1}g^*,\ h^*$ are non units in $R[x]$

Note $\deg h^* > 0 \Rightarrow h^*$ is not a member of R

i.e., h^* cannot be a unit of R and therefore, a unit of $R[x]$

Hence $f = (u^{-1}g^*)\ h^*$

where $u^{-1}g^*$ & h^* are non units in $R[x]$.

$\Rightarrow f$ is not irreducible in $R[x]$

a contradiction, proving our result.

Problem 36: *Find g.c.d.*$(2, x)$ *in* $\mathbf{Z}[x]$ *and show that it cannot be put in the form* $2r(x) + xs(x)$, *for any* $r(x), s(x) \in \mathbf{Z}[x]$.

Solution: We have

$2 = 2 + 0.x + 0.x^2 + ...$

$x = 0 + 1.x + 0.x^2 + ...$

Now $1 \mid 2$ and $1 \mid x$ is obvious by definition as 1 is unity.

Suppose $f \mid 2$ and $f \mid x$. We show that $f \mid 1$

Now $f \mid 2 \Rightarrow 2 = fg$ for some g

$\Rightarrow \deg 2 = \deg f + \deg g$

$\Rightarrow 0 = \deg f + \deg g$

$\Rightarrow \deg f = 0$ or that f is a constant polynomial

Let $f = a_o + 0.x + 0.x^2 + ...$

Again, $f \mid x \Rightarrow a_o \mid x \Rightarrow x = a_o h(x)$

Thus deg x = 0 + deg h which gives deg h = 1

Let $h(x) = b_o + b_1 x + 0 \,.\, x^2 + 0 \,.\, x^3 + ...$

Then $x = a_o h = a_o(b_o + b_1 x) = a_o b_o + a_o b_1 x$

$\Rightarrow 1 = a_o b_1 = f(x)\, b_1$

or that $f \mid 1$

Hence 1 = g.c.d.(2, x)

In view of theorem 1 page 398, any other g.c.d.(2, x) will be an associate of 1. Thus 1, – 1 are the g.c.d. of 2 and x in **Z**[x]. (Recall units of **Z** and **Z**[x] are same and also associate of a unit will be a unit.)

Now suppose it is possible to express any g.c.d. f of (2, x) as $f = 2r + xs$, then

$$1 = (2r + xs)\, b_1 = 2b_1\, (c_o + c_1 x + c_2 x^2 + ...) + b_1 xs(x)$$

where $r(x) = c_o + c_1 x + c_2 x^2 + ...$

i.e., $1 = 2b_1 c_o$, showing that 2 is a unit in **Z**, which is not true. Hence the result follows.

Note: **Z**[x] is a UFD but not a PID. See example 17 page 455.

We now give a test for the irreducibility of a polynomial in **Z**[x] over **Q** the ring of rationals.

Theorem 37: (Eisenstein's Criterion): *Let $f(x) = a_o + a_1 x + a_2 x^2 + ... + a_n x^n$ be a polynomial with integer coefficients (i.e., $f(x) \in \mathbf{Z}[x]$). Suppose that for some prime number p,*

$$p \mid a_o,\ p \mid a_1,\ p \mid a_2\ ...,\ p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_o$$

then $f(x)$ is irreducible polynomial over **Q**, *the ring of rationals.*

We first prove.

Lemma: *If $f(x) \in \mathbf{Z}[x]$ is primitive and $f(x)$ is irreducible over* **Z** *then f is irreducible over* **Q**.

Proof: Suppose f is not irreducible over **Q**,

then we can write $f = gh$, $g, h \in \mathbf{Q}[x]$

with deg g, deg $h > 0$

Then $g(x) \in \mathbf{Q}[x] \Rightarrow g = \dfrac{1}{\alpha} g_1(x)$ where $g_1(x) \in \mathbf{Z}[x]$

$h(x) \in \mathbf{Q}[x] \Rightarrow h = \dfrac{1}{\beta} h_1(x)$ where $h_1(x) \in \mathbf{Z}[x]$

(For instance, if $g(x) = \dfrac{2}{3}x^2 + \dfrac{1}{2}x + 1 \in \mathbf{Q}[x]$ then $g(x) = \dfrac{1}{6}\,(4x^2 + 3x + 6)$, where then $g_1(x) = 4x^2 + 3x + 6 \in \mathbf{Z}[x]$).

Again $g_1(x) \in \mathbf{Z}[x] \Rightarrow g_1 = dg_1^*$ where g_1^* is primitive

$h_1(x) \in \mathbf{Z}[x] \Rightarrow h_1 = d'h_1^*$ where h_1^* is primitive

Thus $$f = gh = \frac{1}{\alpha\beta}\, dd' g_1^* h_1^*$$

$$\Rightarrow \alpha\beta f = dd' g_1^* h_1^*$$

$$\Rightarrow c(\alpha\beta f) = c(dd' g_1^* h_1^*)$$

Since f is primitive polynomial in $\mathbf{Z}[x]$, its content is a unit in $\mathbf{Z}$ and as units in $\mathbf{Z}$ are 1 or -1, $c(f) = \pm 1$. Similarly, $c(g_1^*)$, $c(h_1^*)$ can be ± 1.

Equating the contents on both sides we get

$$\pm\alpha\beta = \pm\, dd'$$

i.e., $$\alpha\beta = \pm\, dd'$$

and hence the equation $\alpha\beta f = dd' g_1^* h_1^*$ reduces to $f = \pm g_1^* h_1^*$

Now $\deg(\pm g_1^*) = \deg g_1^* = \deg dg_1^* = \deg g_1$

$$= \deg \frac{1}{\alpha} g_1 = \deg g > 0$$

Similarly, $\deg(h_1^*) > 0$.

Thus we can write $f = \pm g_1^* h_1^*$ where $\pm g_1^*, h_1^*$ are polynomials in $\mathbf{Z}[x]$ and have positive degree

$\Rightarrow f$ is reducible over $\mathbf{Z}$, a contradiction

hence the lemma is proved.

We now come to the *proof of the main theorem*.

We show f is irreducible over $\mathbf{Z}$.

Suppose it is not irreducible over $\mathbf{Z}$, then $\exists\ g, h \in \mathbf{Z}[x]$ s.t., $f = gh$

with $\deg g, \deg h > 0$

Let $g(x) = b_o + b_1 x + \ldots\ldots + b_s x^s$

$h(x) = c_o + c_1 x + \ldots\ldots + c_t x^t$

then $g(x)\, h(x) = b_o c_o + (b_1 c_o + b_o c_1)x + \ldots\ldots$

So $f = gh$

$\Rightarrow a_o + a_1 x + \ldots\ldots = b_o c_o + (b_1 c_o + b_o c_1)\, x + \ldots$

$\Rightarrow a_o = b_o c_o$

Now $p \mid a_o \Rightarrow p \mid b_o c_o \Rightarrow p \mid b_o$ or $p \mid c_o$ as p is prime

Suppose $p \mid b_0$ then $p \nmid c_0$ as $p^2 \nmid a_o$

$[p \mid b_0, p \mid c_0 \Rightarrow p^2 \mid b_0 c_0 \Rightarrow p^2 \mid a_0]$

Again, p cannot divide all of $b_0, b_1, b_2, \ldots\ldots, b_s$ as if it does

then p divides each term of the type

$$b_0 c_0,\ b_1 c_0 + b_0 c_1,\ \ldots\ldots$$

i.e., p divides all of $a_0, a_1, \ldots\ldots, a_n$

But $p \nmid a_n$

Let k be the smallest integer such that $p \nmid b_k$, $k \leq s < n$

So $p \mid b_0, p \mid b_1, \ldots\ldots, p \mid b_{k-1}, p \nmid b_k$

Now $a_k = b_k c_0 + b_{k-1} c_1 + \ldots\ldots + b_o c_k$

$p \mid a_k$ by given condition as $k < n$

Also $p \mid (b_{k-1} c_1 + b_{k-2} c_2 + \ldots\ldots + b_0 c_k)$

$\Rightarrow p \mid b_k c_0 \Rightarrow p \mid b_k$ or $p \mid c_0$

both leading to a contradiction. Hence $f(x)$ is irreducible over $\mathbf{Z}$.

If $f(x)$ is primitive, it will be irreducible over $\mathbf{Q}$ by lemma. If $f(x)$ is not primitive we can write $f = d f_1$ where f_1 is primitive and $d = c(f)$

Then f irreducible over $\mathbf{Z} \Rightarrow d f_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow f_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow f_1$ is irreducible over $\mathbf{Q}$ (as f_1 is primitive)

$\Rightarrow d f_1$ is irreducible over $\mathbf{Q}$

$\Rightarrow f$ is irreducible over $\mathbf{Q}$

Hence the theorem is proved.

Remark: Since $f(x) = g(x)h(x) \Leftrightarrow f(x + 1) = g(x + 1)\ h(x + 1)$

We find $f(x)$ will be reducible (irreducible) iff $f(x + 1)$ is reducible (irreducible). In fact one can take any integer in place of 1 above.

Example 18: The polynomial $x^2 - 4x + 2$ is irreducible over $\mathbf{Q}$, as if we take $p = 2$, then $p \mid 4$, $p \mid 2$, $p \nmid 1$, $p^2 \nmid 2$.

Again, consider the polynomial $x^2 + 1 = f(x)$.

Since there is no prime p which divides 1, we cannot apply the Eisenstein's criterion to $f(x)$.

Consider $f(x + 1) = (x + 1)^2 + 1$

$= x^2 + 2x + 2 \qquad (a_o = 2,\ a_1 = 2,\ a_2 = 1)$

Take $p = 2$, then $p \mid 2$, $p \nmid 1$, $p^2 \nmid 2$

Hence $f(x + 1)$ is irreducible.

$\Rightarrow f(x)$ is irreducible (by using above remark)

Again, let $f(x) = x^3 + x^2 - 2x - 1$

Since there is no prime that divides 1, we cannot apply the criterion here

Consider $f(x + 1) = (x + 1)^3 + (x + 1)^2 - 2\ (x + 1) - 1$

$= x^3 + 4x^2 + 3x - 1$

we have the same situation. Let us consider

$f(x - 1) = (x - 1)^3 + (x - 1)^2 - 2\ (x - 1) - 1$

$= x^3 - 2x^2 - x - 1$

Again it is not possible to apply the criterion.

Consider $f(x+2) = x^3 + 7x^2 + 14x + 7$

then $p = 7$ will do as here $a_0 = 7$, $a_1 = 14$, $a_2 = 7$, $a_3 = 1$ and $7 \mid 7$, $7 \mid 14$, $7 \mid 7$, $7 \nmid 1$, $7^2 \nmid 7$.

Thus by criterion $f(x+2)$ and therefore, $f(x)$ is irreducible.

Remark: One may note that Eisenstein's criterion is not necessary for irreducibility of a polynomial as we've seen there does not exist any prime p such that $p \mid 1$ (although the polynomial could be irreducible). $x^3 - x + 1$ is irreducible over **Q**, but Eisenstein's criterion is not applicable.

The polynomial $f(x) = x^3 - x + 1$ is irreducible over **Q**, as suppose it is reducible then it has a root in **Q**.

Let $\frac{m}{n}$ [m, n integers, $n \neq 0$, $(m, n) = 1$] be a root

Then $\frac{m^3}{n^3} - \frac{m}{m} + 1 = 0$

$\Rightarrow m^3 - mn^2 + n^3 = 0$

$\Rightarrow m^3 = n^2 (m - n)$

$\Rightarrow n^2 \mid m^3 \Rightarrow n \mid m^3 . 1 \Rightarrow n \mid 1$ as $(m, n) = 1$

$\Rightarrow n = \pm 1$

$\Rightarrow \frac{m}{n} = \pm m$

or that $m^3 - m + 1 = 0$

$\Rightarrow m(m^2 - 1) = -1$

$\Rightarrow m \mid 1$ or that $m = \pm 1$

$\Rightarrow \frac{m}{n} = \pm 1$ which gives

$1 - 1 + 1 = 0$, which is not possible.

Hence $x^3 - x + 1$ is not reducible over **Q**.

Problem 37: *For any prime p, show that the polynomial*

$$x^{p-1} + x^{p-2} + ... + x^2 + x + 1 \text{ is irreducible over } \mathbf{Q}.$$

Solution: Let $f(x) = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$

$$= \frac{x^p - 1}{x - 1} \text{ (sum of a G.P.)}$$

Now

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + p_{c_1} x^{p-1} + ... + p_{c_r} x^{p-2} + ... + p_{c_p} - 1}{x}$$

$$= \frac{x^p + p_{c_1} x^{p-1} + ... + p_{c_{p-1}} x}{x}$$

$$= x^{p-1} + p_{c_1} x^{p-2} + ... + p_{c_{p-1}}$$

Since p is a prime number $p \mid p_{c_r}$ for all $1 \le r \le p-1$. (See example 3, page 357)

Also $p_{c_{p-1}} = p$ or $p^2 \nmid p_{c_{p-1}}$

Hence by Eisenstein's criterion $f(x+1)$ and, therefore, $f(x)$ is irreducible.

Problem 38: *Let F be the field of quotients of an integral domain R. Define.*

$$\theta : R[x] \to R[x] \text{ s.t.,}$$
$$\theta(a_0 + a_1x + \cdots + a_nx^n) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

then show that

(*i*) $\theta(f(x)) = x^n f\left(\frac{1}{x}\right)$ in $F[x]$

(*ii*) θ is $1-1$, onto

(*iii*) $\theta(fg) = \theta(f)\theta(g)$.

Solution: (*i*) If $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then

$$f\left(\frac{1}{x}\right) = a_0 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n} \text{ and thus}$$

$$x^n f\left(\frac{1}{x}\right) = a_0x^n + a_1x^{n-1} + \cdots + a_n = \theta(f(x))$$

(*ii*) Let $\theta(f(x)) = \theta(g(x))$, where

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

then

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = b_0x^m + b_1x^{m-1} + \cdots + b_m$$
$$\Rightarrow m = n \quad \text{and} \quad a_i = b_i \text{ for all } i$$

or that $f(x) = g(x)$ and so θ is 1-1

Again, for any $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$

$g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ will be the required pre image to show that θ is onto.

(*iii*) Let $f(x)g(x) = h(x)$, where $f(x)$, $g(x)$ are as defined above

Now $\theta(f(x)g(x)) = \theta(h(x))$

$$= x^{n+m} h\left(\frac{1}{x}\right)$$
$$= x^n f\left(\frac{1}{x}\right) x^m g\left(\frac{1}{x}\right)$$
$$= \theta(f(x))\ \theta(g(x))$$

Problem 39: *Let* $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$, $a_n \neq 0$. *Suppose there exists a prime p, such that* $p|a_1$, $p|a_2$,....$p|a_n$, $p \nmid a_0$, $p^2 \nmid a_n$,

Show that f(x) is irreducible over **Q**.

Hence show that $2x^4 - 4x^3 + 6x^2 + 2x + 1$ *is irreducible over* **Q**.

Solution: Define $\theta : \mathbf{Z}[x] \to \mathbf{Z}[x]$ s.t.,

$$\theta(f(x)) = \theta(a_0 + a_1x + \cdots + a_nx^n) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

then $$x^n f(\tfrac{1}{x}) = a_0x^n + a_1x^{n-1} + \cdots a_n$$

$$\theta(f(x)) = a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n = g(x)$$

By Eisenstein's Criterion, $g(x)$ is irreducible over **Q**.

Suppose now $f(x)$ is reducible over **Q**, then $f(x)$ is reducible over **Z**.

Let $f(x) = h(x)k(x)$, $h(x)$, $k(x) \in \mathbf{Z}[x]$

$\deg h(x) = r$, $\deg k(x) = s$, $1 \leq r$, $s < n$

Then $\theta(f(x)) = \theta(h(x))\theta(k(x))$ by previous problem

So $g(x) = \theta(h(x))\theta(k(x))$

But $g(x)$ is irreducible over **Q**, so either $\theta(h(x))$ is constant or $\theta(k(x))$ is constant.

Suppose $\theta(h(x)) = c$ a constant.

Then $h(x) = cx^r$

Thus the constant term in $f(x) = h(x)k(x)$ is zero, contradicting that $p \nmid a_0$

So $f(x)$ is irreducible over **Z** and therefore over **Q**.

For the last part, choose $p = 2$ and the result follows by the problem.

We discuss now another method for finding the irreducibility of a polynomial (with integer coefficients) over **Q**.

Lemma: Let p be a prime. Define

$\theta : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$, s.t.,

$\theta(f(x)) = \overline{f}(x)$

where $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$

and $\overline{f}(x) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n \in \mathbf{Z}_p[x]$

where $a_i \equiv \overline{a}_i \pmod{p}$

Then θ is an onto homorphism.

Proof: Consider $\theta(f(x) + g(x))$

$= \theta(h(x))$, $h(x) = f(x) + g(x)$

$= \overline{h}(x)$

$= \overline{f}(x) + \overline{g}(x) = \theta(f(x)) + \theta(g(x))$

and $\theta(f(x)g(x))$

$= \theta(r(x))$ where $f(x)g(x) = r(x)$

$= \bar{r}(x)$

$= \bar{f}(x)\bar{g}(x) = \theta(f(x))\theta(g(x))$

where suppose

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad \bar{f}(x) = \sum_{i=0}^{n} \bar{a}_i x^i$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad \bar{g}(x) = \sum_{j=0}^{m} \bar{b}_j x^j$$

$$r(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}, \quad \bar{r}(x) = \sum_{s=0}^{n+m} \bar{c}_s x^s$$

Then $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$

So $\bar{c}_k = \bar{a}_0\bar{b}_k + \bar{a}_1\bar{b}_{k-1} + \cdots + \bar{a}_k\bar{b}_0$

$\equiv a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 \pmod{p}$

$\equiv c_k \pmod{p}$

Therefore, $\bar{r}(x) = \bar{f}(x)\bar{g}(x)$

So, θ is a ring homomorphism.

Let $\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n \in \mathbf{Z}_p[x]$

Then $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$

and as $\theta(f(x)) = \bar{f}(x)$, θ is onto

which proves the lemma.

Theorem 38: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$, $a_n \neq 0$.

Let p be a prime such that p does not divide a_n

Consider $\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n \in \mathbf{Z}_p[x]$, where $\bar{a}_i \equiv a_i \pmod{p}$

Then if $\bar{f}(x)$ *is irreducible in* $\mathbf{Z}_p[x]$, *then* $f(x)$ *is irreducible in* $\mathbf{Q}[x]$.

Proof: Suppose $f(x)$ is reducible in $\mathbf{Q}[x]$

Then $f(x)$ is reducible in $\mathbf{Z}[x]$

Let $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbf{Z}[x]$

$1 \leq \deg g(x), h(x) < n$

Since p does not divide a_n, it does not divide the leading coefficients of $g(x)$ and $h(x)$.

So, $\deg \bar{g}(x) = \deg g(x)$, $\deg \bar{h}(x) = \deg h(x)$

By above lemma,

$$\bar{f}(x) = \theta(f(x)) = \theta(g(x))\theta(h(x)) = \bar{g}(x)\bar{h}(x)$$

Contradicting that $\overline{f}(x)$ is irreducible in $\mathbf{Z}_p[x]$

Therefore, $f(x)$ is irreducible in $\mathbf{Q}[x]$.

Sometimes the above result is useful for determining the irreducibility of a polynomial by considering the primes, 2, 3 or 5.

Problem 40: *Show that* $f(x) = 8x^3 - 2x^2 - 5x + 10$ *is irreducible over* $\mathbf{Q}$.

Solution: Let $p = 3$.

Then $\overline{f}(x) = 2x^3 + x^2 + x + 1 \in \mathbf{Z}_3[x]$

Now $\overline{f}(0) = 1,\ \overline{f}(1) = 2,\ \overline{f}(2) = 2$ (Remember it is modulo 3)

So, $\overline{f}(x)$ has no zero in $\mathbf{Z}_3$ implying $\overline{f}(x)$ is irreducible in $\mathbf{Z}_3[x]$.

Therefore, $f(x)$ is irreducible in $\mathbf{Q}[x]$.

The next problems show that there can exist a polynomial $f(x) \in \mathbf{Z}[x]$ for which there is no prime p such that $f(x)$ is irreducible in $\mathbf{Z}_p[x]$. So, we can not use the above theorem.

Problem 41: *Let* p *be an odd prime. Let* $\mathbf{Z}_p^* = \mathbf{Z}_p - \{0\}$

Then $\mathbf{Z}_p^*$ *is a multiplicative group.*

Define: $\theta : \mathbf{Z}_p^* \to \mathbf{Z}_p^*$ *such that* $\theta(x) = x^2$. *Show that* θ *is a homomorphism such that* Ker $\theta = \{1, -1\}$ *and* $H = Im\theta = \theta(\mathbf{Z}_p^*)$ *contains* -1, 2 *or* -2.

Solution: Now $\theta(xy) = (xy)^2 = x^2y^2 = \theta(x)\theta(y)$ as $\mathbf{Z}_p^*$ is an abelian group. So, θ is a homomorphism.

Also, $a \in$ Ker θ implies $\theta(a) = 1$ or $a^2 = 1$. So, $p|(a - 1)(a + 1)$ implies $a = 1 \pmod p$ or $a = -1 \pmod p$.

But $\theta(1) = 1$ and $\theta(-1) = 1$. Therefore, Ker $\theta = \{1, -1\}$.

Now $\dfrac{\mathbf{Z}_p^*}{Ker\,\theta} \cong H$ and $o(\text{Ker } \theta) = 2$ implies H has index 2 in $\mathbf{Z}_p^*$.

Suppose that neither -1 nor $2 \in H$

Since index of H is 2, $(-1)H = 2H$,

Also $o\left(\dfrac{\mathbf{Z}_p^*}{H}\right) = 2$ implies $(xH)^2 = H$ for every $x \in \mathbf{Z}_p^*$.

Therefore, $x^2 \in H$ for all $x \in \mathbf{Z}_p^*$

So, $(-1)H(-1)H = (-1)H2H = -2H = H$.

So, $-2 \in H$.

Similarly if $-1 \notin H$ and $-2 \notin H$,

then $(-1)H = (-2)H$ and $(-1)H\ (-1)H = (-1)H(-2)H = 2H = H$ implies $2 \in H$.

If $2 \notin H, -2 \notin H$

then $(2)H = (-2)H$.

So, $(-2)H(-2)H = (-2)H2H = -4H = H$

implies $-4 \in H$.

Also $4 \in H$ as $x^2 \in H$ for all $x \in \mathbf{Z}_p^*$.

so, $4^{-1} \in H$ and $-4.\ 4^{-1} = -1 \in H$

In any case -1, 2 or $-2 \in H$.

Problem 42: *Show that* $x^4 + 1$ *is not irreducible over* $\mathbf{Z}_p$ *for any prime* p.

Solution: Suppose p is an odd prime. By above problem one of the elements in $\{-1, 2, -2\}$ is in H.

If $-1 \in H$, then $-1 = \theta(a)$, $a \in \mathbf{Z}_p^*$

So $a^2 = -1$.

Then $x^4 + 1 = (x^2 + a)(x^2 - a)$

If $2 \in H$ then $2 = \theta(a)$, $a \in \mathbf{Z}_p^*$

So $a^2 = 2$.

Then $x^4 + 1 = (x^2 + ax + 1)(x - ax + 1)$

If $-2 \in H$, then $-2 = \theta(a)$, $a \in \mathbf{Z}_p^*$

So, $a^2 = -2$. Then $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$

In any case, $x^4 + 1$ is reducible over $\mathbf{Z}_p$.

If $p = 2$, then $x^4 + 1 = (x^2 + 1)(x^2 + 1)$.

so, $x^4 + 1$ is reducible over $\mathbf{Z}_2$.

Noetherian Rings

We'll, briefly, discuss noetherian rings here which are in fact a natural generalisation of PIDs. We begin with

Definition I: A ring R is called a *noetherian* ring if every ideal of R is finitely generated.

Definition II: A ring R is called *noetherain* ring if every ascending chain of ideals in R terminates after finite number of steps.

Before giving any examples let us first show the equivalence of the two definitions.

Definition I $\Rightarrow$ Definition II

Let R be a ring in which every ideal is finitely generated. Let

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \ \ldots$$

be any ascending chain of ideals in R,

Let $A = \bigcup_i A_i$

then A is an ideal of R (See lemma 1 on page 442)

Thus A is finitely generated.

Let $A = < a_1, a_2, ..., a_n >$

Consider any a_j, then $a_j \in A = \cup A_i$

$\Rightarrow a_j \in A_i$ for some i

Suppose $a_1 \in A_{i_1}, a_2 \in A_{i_2} ....., a_n \in A_{i_n}$

Let k be such that $A_{i_j} \subseteq A_k \ \forall j = 1, 2,....., n$

Then $a_1, a_2, ..., a_n \in A_k$

$\Rightarrow$ $A \subseteq A_k \subseteq A$

Hence $A_k = A$ or that the chain terminates at A_k which proves the result.

Definition II $\Rightarrow$ Definition I

Let R be a ring satisfying the condition of def. II.

Let I be any ideal of R. We show I is finitely generated.

Let $a_1 \in I$ be any element.

If $I = < a_1 >$, we are done.

If $I \neq < a_1 >$ then $\exists$ same $a_2 \in I$ s.t., $a_2 \notin < a_1 >$

Consider $< a_1, a_2 >$. If $I = < a_1, a_2 >$ then the result is proved.

If not then $\exists$ $a_3 \in I$ s.t., $a_3 \notin < a_1, a_2 >$ continuing like this we get an ascending chain of ideals

$$< a_1 > \subseteq < a_1, a_2 > \subseteq < a_1, a_2, a_3 > \subseteq \ . \ . \ .$$

which must break off after a finite number of steps, say at $<a_1, a_2, ..., a_n>$. Then

$I = < a_1, a_2, ..., a_n >$ and the result is proved.

Example 19: A PID is a noetherian ring. (See lemma 2 on page 442). Thus in particular, $\mathbf{Z}$, $\mathbf{Z}[i]$, $F[x]$ where F is a field are all noetherian.

Example 20: A finite ring will be noetherian and so would be any field. Remeber a field F has only two ideal $\{0\}$ and F.

Remark: A ring R is defined to be *right noetherian* if every ascending chain of right ideals in R terminates after finite number of steps. Similarly one can talk of a *left noetherian ring* by considering left ideals.

Again the condition of termination of an ascending chain is also referred to as ACC(ascending chain condition). A ring in which ACC holds for right as well as left ideals is called a noetherian ring.

One can have examples of right noetherian rings that are not left noetherian and vice versa.

Theorem 39: *Quotient ring of a noetherian ring is noetherian.*

Proof: Let R/I be any quotient ring of a noetherian ring R.

Let $f : R \rightarrow R/I$ be the the natural homomorphism, where $f(r) = r + I$

Let $\overline{J}$ be any ideal of R/I. We show $\overline{J}$ is finitely generated.

Let $J = \{r \in R \mid f(r) \in \bar{J}\}$

then it is easy to see (and we urge the reader to prove) that J is an ideal of R. Since R is noetherian, J is finitely generated.

Let $J = \langle r_1, r_2, \ldots, r_n \rangle$, then we can show that

$$\bar{J} = \langle f(r_1), f(r_2), \ldots, f(r_n) \rangle$$

Let $f(r) \in \bar{J}$ be any element then $r \in J$ and as J is generated by $r_1, r_2, \ldots, r_n$, we get

$$r = \alpha_1 r_1 + \alpha_2 r_2 + \ldots + \alpha_n r_n \qquad \alpha_i \in R$$

$$\Rightarrow f(r) = f(\alpha_1) f(r_1) + f(\alpha_2) f(r_2) + \ldots + f(\alpha_n) f(r_n), \quad f(\alpha_i) \in R/I$$

Showing that $\bar{J} = \langle f(r_1), f(r_2), \ldots, f(r_n) \rangle$

Hence R/I is noetherian.

Theorem 40: *Homomorphic image of a noetherian ring is noetherian*

Proof: Let $f : R \to R'$ be an onto homomorphism and suppose R is noetherian.

By Fundamental theorem of ring homomorphism

R' is isomorphic to a quotient ring of R, which will be noetherian by above theorem. Hence R' will be noetherian.

Problem 43: *Let R be a noetherian ring. Show that any ideal $I \neq R$ is contained in a maximal ideal of R.*

Solution: If I itself is maximal we have nothing to prove. If I is not maximal then $\exists$ an ideal I_1, s.t., $I \subseteq I_1$. If I_1 is maximal, we are done. If not then $\exists$ another ideal I_2 s.t., $I \subseteq I_1 \subseteq I_2$ and continuing like this we get an ascending chain of ideals which must become stationary after a finite number of steps

i.e., $$I \subseteq I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n = I_{n+1} = I_{n+2} \ldots$$

and thus I_n will be maximal.

Problem 44: *Let R be a commutative ring with unity. Let $R[x]$ be noetherian. Show that R is also noetherian.*

Solution: By Theorem 15, page 427, we know that

$$\frac{R[x]}{\langle x \rangle} \cong R$$

Since $R[x]$ is noetherian, its quotient ring $\dfrac{R[x]}{\langle x \rangle}$ is noetherian and therefore so is R.

We use the famous Hilbert Basis theorem which says that polynomial ring $R[x]$ of a noetherian ring R is noetherian in proving the following

Problem 45: *Show by an example that subring of a noetherian ring may not be noetherian.*

Solution: Let $\mathbf{Q}$ be the field of rational numbers, then $\mathbf{Q}$ is a noetherian ring and thus $\mathbf{Q}[x]$ is noetherian.

Let $S = \{f(x) \in \mathbf{Q}[x] \mid f(x) = a_o + a_1 x + a_2 x^2 + \ldots + a_n x^n,\ a_o \in \mathbf{Z},\ a_i \in \mathbf{Q}\ \forall\ i \geq 1\}$

It is easy to see that S is a subring of $\mathbf{Q}[x]$.

We notice the chain

$$< x > \underset{\neq}{\subset} < \frac{x}{2} > \underset{\neq}{\subset} < \frac{x}{4} > \underset{\neq}{\subset} \ldots$$

is an ascending chain of ideals in S which does not terminate after finite number of steps. Suppose for instance, equality holds at $< x > = < \frac{x}{2} >$, then

$$\frac{x}{2} \in < x > \Rightarrow \frac{x}{2} = h(x)x \quad \text{for some } h(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_m x^m$$

where $\alpha_0 \in \mathbf{Z}$

$$\Rightarrow \quad \frac{x}{2} = \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_m x^{m+1}$$

$$\Rightarrow \quad 0 + \frac{1}{2}x + 0x^2 + \ldots = 0 + \alpha_o x + \alpha_1 x^2 + \ldots + \alpha_m x^{m+1}$$

$$\Rightarrow \quad \frac{1}{2} = \alpha_o \text{ But } \frac{1}{2} \notin \mathbf{Z}$$

Hence $< x > \underset{\neq}{\subset} < \frac{x}{2} >$. Similarly it follows that equality does not hold in the above chain at any step.

Definition: A ring R is called *artinian* ring if every decending chain of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$$

terminates after a finite number of steps (the condition being called DCC or Decending Chain Condition)

It is clear that any finite ring is artinian and so would be a field. The ring $\mathbf{Z}$ of integers is not artinian as the decending chain

$$< n > \underset{\neq}{\supset} < 2n > \underset{\neq}{\supset} < 4n > \underset{\neq}{\supset} \ldots$$

of ideals (for any +ve integer n) is infinite.

This also shows that subring of an artinian ring may not be artinian. Notice $\mathbf{Q}$ the ring of rationals being a field is artinian. One can talk of left and right artinian rings also by considering chain of left (right) ideals. See exercises ahead for more results.

Exercises

1. Find sum and product of the polynomials $f(x) = 4x - 5$ and $g(x) = 2x^2 - 4x + 2$ in $\mathbf{Z}_8[x]$.
2. Find all the units of $\mathbf{Z}[x]$ and $\mathbf{Z}_7[x]$.
3. Show by using the long division process that
$$3x^4 + x^3 + 2x^2 + 1 = (x^2 + 4x + 2)(3x^2 + 4x) + (2x + 1) \text{ in } \mathbf{Z}_5[x].$$

4. If R is a UFD and $f(x) \in R[x]$ then it is possible to write $f(x) = ag(x)$, $a \in R$, $g(x) \in R[x]$ being primitive. Show that if $f(x) = ag(x) = bh(x)$, $a, b \in R$, g, h being primitive then a, b are associates and so are $g(x)$ and $h(x)$.

5. Give example of a polynomial, which is

(*i*) primitive and irreducible.

(*ii*) primitive and reducible.

(*iii*) not primitive but irreducible.

(*iv*) not primitive but reducible.

6. Show that $4x^2 + 6x + 2$ is not a primitive polynomial in $\mathbf{Z}[x]$. Is it primitive over $\mathbf{Q}$? Justify.

7. If R is a commutative ring, show that ch $R[x]$ is same as ch R.

8. Let R be a commutative ring and let $f(x) = a_0 + a_1x + ... + a_nx_n \in R[x]$. Show that $f(x)$ is nilpotent in $R[x]$ if and only if $a_0, a_1, ..., a_n$ are nilpotent in R.

9. Show that the following polynomials are irreducible over $\mathbf{Q}$, (the rationals)

(*i*) $8x^3 - 6x - 1$

(*ii*) $x^4 + x^3 + x^2 + x + 1$

(*iii*) $2x^{10} - 25x^3 + 10x^2 - 30$. ($p = 5$).

(*iv*) $3x^4 + 9x^3 - 7x^2 + 15x + 25$. by using the modulo p method. Take $p = 2$.

10. Find g.c.d. of (*i*) $3 + 4i$ and $4 - 3i$ *in* $\mathbf{Z}[i]$. Are these associates?

(*i*) $2x^2 + x^3 - 6x^2 + 7x - 2$, $2x^3 - 7x^2 + 8x - 4$ in $\mathbf{Q}[x]$.

(*ii*) $11 + 7i$ and $3 + 7i$ in $\mathbf{Z}[i]$

(*iii*) $10 + 11i$ and $8 + i$ in $\mathbf{Z}[i]$

(*iv*) 2 and $3 + 5i$ in $\mathbf{Z}[i]$

(*v*) $2x^4 + 2$ and $x^5 + 2$ in $\mathbf{Z}_3[x]$

11. (*i*) Show that the ideal $< x^2 + 1 >$ is maximal ideal in $\mathbf{R}[x]$.

(*ii*) Show that $\frac{\mathbf{Q}[x]}{I}$, where $I = < x^2 - 6x + 6 >$ is a field.

(*iii*) Show that $x^3 + 3x + 1$ is irreducible over $\mathbf{Q}$. Hence prove that $\frac{\mathbf{Q}[x]}{I}$ is a field where $I = < x^3 + 3x + 1 >$. Write an element of $\frac{\mathbf{Q}[x]}{I}$.

(*iv*) Show that $\frac{\mathbf{Z}_2[x]}{I}$, $I = < x^2 + x + 1 >$ is a field with 4 elements. Show that $x + I$ is inverse of $(x + 1) + I$ in this field.

(*v*) Show that $\frac{\mathbf{Q}[x]}{I}$, $I = < x^3 - 5 >$ is a field. Find inverse of $(x + 1) + I$.

12. Show that in a PID, every ideal is contained in a maximal ideal.

13. Show that $x^2 + 1$ and $x^2 + x + 4$ are irreducible over F the field of integers modulo 11. Prove also that $\frac{F[x]}{< x^2 + 1 >}$ and $\frac{F[x]}{< x^2 + x + 4 >}$ are isomorphic fields each having 121 elements.

14. If P is a prime ideal of $R[x]$ then show that $P \cap R$ is a prime ideal of R.

15. Let I be an ideal of $R[x]$ and let A_n be the set of all leading coefficients of polynomials in I together with 0. *i.e.*,

$$A_n = \{0 \neq a \in R \mid \exists\, f(x) = \alpha_o + \alpha_1 x + \ldots\ldots + \alpha_{n-1}x^{n-1} + ax^n \in I\} \cup \{0\}.$$

Show that A_n is an ideal of R. (For some fixed n)

16. Let K be the field of quotients of a UFD R then show that primitive polynomials $f, g \in R[x]$ are associates in $R[x]$ iff f, g are associates in $K[x]$.

17. If F is a field and $f(x) \mid g(x)$ in $F[x]$ then show that f is either a unit, an associate of g or $\deg f < \deg g$.

18. Show that $I = \{ f(x) \in \mathbf{Z}[x] \mid f(0) = \text{even integer}\}$ is the ideal $< x, 2 >$ of $\mathbf{Z}[x]$.

19. Show that the ideal $< x >$ is maximal ideal in $\mathbf{Q}[x]$. See note on page 430.

20. If $A = (2)$, show that $A[x]$ is not a maximal ideal of $\mathbf{Z}[x]$. [See remark (*ii*) on page 426]

21. If R is a Euclidean domain, show that every element of R is either a unit or can be uniquely expressed (upto associates) as product of primes.

22. Show that the set of all polynomials with even coefficients is a prime ideal in $\mathbf{Z}[x]$.

23. Show that $\boldsymbol{Z}[\sqrt{-3}]$ is not a UFD. (See exercise 13 page 415).

24. If F is a field, show that every non zero prime ideal of $F[x]$ is a maximal ideal.

25. Show that in a UFD R, every non zero prime ideal ($\neq R$) contains a prime element.

26. Factorize $x^2 + x + 5$ in $F[x]$, where F is the field of integers mod 11.

27 Let R be an integral domain with unity. Show that a prime element in R is a prime element in $R[x]$.

28. Let A be the set of all polynomials $f(x) \in \mathbf{R}[x]$ s.t., $f(0) = 0 = f(1)$. Show that A is an ideal of $\mathbf{R}[x]$ but is not a prime ideal.

29. Show that any ring which is a quotient ring of a polynomial ring over $\mathbf{Z}$ (or a field F) is noetherian.

30. Show that

(*a*) Homomorphic image of an artinian ring is artinian.

(*b*) An artinian ring which is an integral domain is a field.

A Quick Look at what's been done

- Definitions and existence of g.c.d., and l.c.m., in rings. In an integral domain with unity if there exist more than one g.c.ds (l.c.ms) then they are associates and conversely.
- Every ideal in a Euclidean Domain is a principal ideal.
- The ring of Gaussian integers is a Euclidean Domain and hence a PID.
- Any two non-zero elements in a PID (Euclidean Domain) have g.c.d., and l.c.m.
- Any non-zero, non-unit element p in a commutative ring is called a **prime element** if whenever $p|ab$ then either $p|a$ or $p|b$. It is called **irreducible element** if whenever $p = ab$ then either a is a unit or b is a unit.
- If F is a field then the ring of polynomials $F[x]$ is a Euclidean Domain.
- An integral domain R with unity is a field iff $R[x]$ is a PID.
- $\mathbf{Z}[x]$ is not a PID as $\mathbf{Z}$ is not a field.
- If R is an integral domain with unity then the following are equivalent:
  (i) R is a UFD.
  (ii) Every non-zero, non-unit element of R is a finite product of irreducible elements and every irreducible element is prime.
  (iii) Every non-zero, non-unit element of R is a finite productof prime elements.
- A PID is a UFD.$\mathbf{Z}[x]$ is a UFD but not a PID.
- Gauss Lemma says that if R is a UFD then product of two primitive polynomials over R is primitive.
- An irreducible element is irreducible polynomial, but converse is not always true.
- If R is a UFD then any $f(x)$ in $R[x]$ is an irreducible element of $R[x]$ iff either f is an irreducible element of R or f is an irreducible primitive polynomial of $R[x]$.
- R is a UFD $\Rightarrow R[x]$ is a UFD.
- **Eisenstein's criterion** gives us a method to check irreducibility of a polynomial over rationals.
- A ring is called **Noetherian** if every ideal of it is finitely generated or if every ascending chain of ideals in it terminates after finite number of steps.

10

Vector Spaces

Introduction

The motivating factor in rings was set of integers and in groups the set of all permutations of a set. A vector space originates from the notion of a vector that we are familiar with in mechanics or geometry. Our aim in this volume is not to go into details of that. Reader would recall that a vector is defined as a directed line segment, which in algebraic terms is defined as an ordered pair (a, b), being coordinates of the terminal point relative to a fixed coordinate system. Addition of vectors is given by the rule

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

One can easily verify that set of vectors under this forms an abelian group. Also scalar multiplication is defined by the rule $\alpha\,(a, b) = (\alpha a, \alpha b)$ which satisfies certain properties. This concept is extended similarly to three dimensions. We generalise the whole idea through definition of a vector space and vary the scalars not only in the set of reals but in any field F. A vector space thus differs from groups and rings in as much as it also *involves* elements from outside itself.

Definition: Let $< V, + >$ be an abelian group and $< F, +, \cdot >$ be a field. Define a function $\cdot$ (called scalar multiplication) from $F \times V \to V$, s.t., for all $\alpha \in F$, $v \in V$, $\alpha \cdot v \in V$. Then V is said to form a *vector space* over F if for all $x, y \in V$, $\alpha, \beta \in F$, the following hold

(*i*) $(\alpha + \beta)\, x = \alpha x + \beta x$

(*ii*) $\alpha\,(x + y) = \alpha x + \alpha y$

(*iii*) $(\alpha\beta)\, x = \alpha\,(\beta x)$

(*iv*) $1 \cdot x = x$, 1 being unity of F.

Also then, members of F are called *scalars* and those of V are called *vectors*.

Remark: We have used the same symbol + for the two different binary compositions of V and F, for convenience. Similarly same symbol . is used for scalar multiplication and product of the field F.

Since $< V, + >$ is a group, its identity element is denoted by 0. Similarly the field F would also have zero element which will also be represented by 0. In case of doubt one can use different symbols like 0_v and 0_F etc.

Since we generally work with a fixed field we shall only be writing V is a vector space (or sometimes $V(F)$ or V_F). It would always be understood that it is a vector space over F (unless stated otherwise).

We defined the scalar multiplication from $F \times V \to V$. One can also define it from $V \times F \to V$ and have a similar definition. The first one is called a left vector space and the second a right vector space. It is easy to show that if V is a left vector space over F then it is a right vector space over F and conversely. In view of this result it becomes redundant to talk about left or right vector spaces. We shall thus talk of only vector spaces over F.

One can also talk about the above system when the scalars are allowed to take values in a ring instead of a field, which leads us to the definition of modules.

Theorem 1: *In any vector space $V(F)$ the following results hold*

(i) $0.x = 0$

(ii) $\alpha.0 = 0$

(iii) $(-\alpha)x = -(\alpha x) = \alpha(-x)$

(iv) $(\alpha - \beta)x = \alpha x - \beta x$, $\alpha, \beta \in F$, $x \in V$

Proof: (i) $0.x = (0 + 0).x = 0.x + 0.x$

$\Rightarrow 0 + 0.x = 0.x + 0.x$

$\Rightarrow 0 = 0.x$ (cancellation in V)

(ii) $\alpha.0 = \alpha.(0 + 0) = \alpha.0 + \alpha.0 \Rightarrow \alpha.0 = 0$

(iii) $(-\alpha)x + \alpha x = [(-\alpha) + \alpha]x = 0 \ . \ x = 0$

$\Rightarrow (-\alpha x) = -\alpha x$

(iv) follows from above.

Example 1: If $< F, +, . >$ be a field, then F is a vector space over F as $< F, + > = < V, + >$ is an additive abelian group. Scalar multiplication can be taken as the product of F. All properties are seen to hold. Thus $F(F)$ is a vector space.

Example 2: Let $< F, +, . >$ be a field

Let $V = \{(\alpha_1, \alpha_2) \mid \alpha_1, \alpha_2 \in F\}$

Define + and . (scalar multiplication) by

$$(\alpha_1, \alpha_2) + (\beta_1, \beta_2) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$

$$\alpha(\alpha_1, \alpha_2) = (\alpha\alpha_1, \alpha\alpha_2)$$

One can check that all conditions in the definition are satisfied. Here $V = F \times F = F^2$

One can extend this to F^3 and so on. In general we can take n–tuples $(\alpha_1, \alpha_2, ..., \alpha_n)$, $\alpha_i \in F$ and define F^n or $F^{(n)} = \{(\alpha_1, \alpha_2, ..., \alpha_n) \mid \alpha_i \in F\}$ as a Vector space over F.

Example 3: If $F \subseteq K$ be two fields then $K(F)$ will form a vector space, where addition of $K(F)$ is + of K and for any $\alpha \in F$, $x \in K$, $\alpha \ . \ x$ is taken as product of α and x in K.

Thus $\mathbf{C}(\mathbf{R})$, $\mathbf{C}(\mathbf{C})$, $\mathbf{R}(\mathbf{Q})$ would be some examples of vector spaces, where $\mathbf{C}$ = complex nos., $\mathbf{R}$ = reals and $\mathbf{Q}$ = rationals.

Example 4: Let V = set of all real valued continuous functions defined on [0, 1]. Then V forms a vector space over the field **R** of reals under addition and scalar multiplication defined by

$$(f + g)x = f(x) + g(x) \quad f, g \in V$$
$$(\alpha f)x = \alpha f(x) \qquad \alpha \in \mathbf{R}$$
$$\text{for all } x \in [0, 1]$$

It may be recalled here that sum of two continuous functions is continuous and scalar multiple of a continuous function is continuous.

Example 5: The set $F[x]$ of all polynomials over a field F in an indeterminate x forms a vector space over F w.r.t., the usual addition of polynomials and the scalar multiplication defined by:

For $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x], \quad \alpha \in F$

$$\alpha.(f(x)) = \alpha a_0 + \alpha a_1x + \ldots + \alpha a_nx^n.$$

Example 6: $M_{m \times n}(F)$, the set of all $m \times n$ matrices with entries from a field F forms a vector space under addition and scalar multiplication of matrices.

We use the notation $M_n(F)$ for $M_{n \times n}(F)$.

Example 7: Let F be a field and X a non empty set.

Let $F^X = \{f \mid f : X \to F\}$, the set of all mappings from X to F. Then F^X forms a vector space over F under addition and scalar multiplication defined as follows:

For $f, g \in F^X, \alpha \in F$

Define $f + g : X \to F, \alpha F : X \to, F$ such that

$$(f + g)(x) = f(x) + g(x)$$
$$(\alpha f)(x) = \alpha f(x) \qquad \forall\, x \in X$$

Example 8: Let V be the set of all vectors in three dimensional space. Addition in V is taken as the usual addition of vectors in geometry and scalar multiplication is defined as:

$\alpha \in \mathbf{R}$, $\vec{v} \in V \Rightarrow \alpha\vec{v}$ is a vector in V with magnitude $|\alpha|$ times that of V. Then V forms a vector space over **R**.

Subspaces

Definition: *A* non empty subset W of a vector space $V(F)$ is said to form a *subspace* of V if W forms a vector space under the operations of V.

Theorem 2: *A necessary and sufficient condition for a non empty subset W of a vector space V(F) to be a subspace is that W is closed under addition and scalar multiplication.*

Proof: If W is a subspace, the result follows by definition.

Conversely, let W be closed under addition and scalar multiplication.

Let $x, y, \in W$ since $1 \in F, -1 \in F$

$$\therefore -1.y \in W \Rightarrow -y \in W$$
$$x, -y \in W \Rightarrow x - y \in W$$
$$\Rightarrow < W, + > \text{ forms a subgroup of } < V, + >.$$

Rest of the conditions in the definition follow trivially.

Theorem 3: *A non empty subset W of a vector space $V(F)$ is a subspace of V iff $\alpha x + \beta y \in W$ for $\alpha, \beta \in F$, $x, y \in W$.*

Proof: If W is a subspace, result follows by definition.

Conversely, let given condition hold in W.

Let $x, y \in W$ be any elements. Since $1 \in F$

$$1 \cdot x + 1 \cdot y = x + y \in W$$

$\Rightarrow$ W is closed under addition.

Again, $x \in W$, $\alpha \in F$ then

$$\alpha x = \alpha x + 0.y \quad \text{for any } y \in W, 0 \in F$$

which is in W. (Note here 0 may not be in W)

Hence W is closed under scalar multiplication.

The result thus follows by previous theorem.

Remark: V and $\{0\}$ will be trivial subspaces of any vector space $V(F)$.

Example 9: Consider the vector space $\mathbf{R}^2(\mathbf{R})$

then $W_1 = \{(a, 0) \mid a \in \mathbf{R}\}$

$W_2 = \{(0, b) \mid b \in \mathbf{R}\}$

are subspaces of $\mathbf{R}^2$

As for any $\alpha, \beta \in \mathbf{R}$, $(a_1, 0), (a_2, 0) \in W_1$, we find

$$\alpha(a_1, 0) + \beta(a_2, 0) = (\alpha a_1, 0) + (\beta a_2, 0)$$
$$= (\alpha a_1 + \beta a_2, 0) \in W_1$$

Hence W_1 is a subspace. Similarly we can show W_2 is a subspace of $\mathbf{R}^2$.

Problem 1: *Show that union of two subspaces may not be a subspace.*

Solution: Consider the previous example.

$W_1 \cup W_2$ will be the set containing all pairs of the type $(a, 0), (0, b)$

In particular $(1, 0), (0, 1) \in W_1 \cup W_2$

But $(1, 0) + (0, 1) = (1, 1) \notin W_1 \cup W_2$.

Hence $W_1 \cup W_2$ is not a subspace.

Reader is referred to exercises for more results pertaining to intersection and union of subspaces.

We take up few more examples of subspaces.

Example 10: Let $V = \mathbf{R}[x]$ and suppose $W = \{f(x) \in V \mid f(x) = f(1 - x)\}$

Then W is a subspace of V as

$W \neq \phi$ since $0 \in W$ as $f(x) = 0 = f(1 - x)$

Again, if $f(x), g(x) \in W$, then $f(x) = f(1 - x)$, $g(x) = g(1 - x)$

Let $f(x) + g(x) = h(x)$

Then $h(1 - x) = f(1 - x) + g(1 - x)$

$= f(x) + g(x) = h(x)$

$\Rightarrow h(x) \in W$ or that $f(x) + g(x) \in W$

Again, for $\alpha \in \mathbf{R}$, let $\alpha f(x) = r(x)$

Then $r(1 - x) = \alpha f(1 - x) = \alpha f(x) = r(x)$

$\Rightarrow r(x) \in W \Rightarrow \alpha f(x) \in W$

Hence W is a subspace.

Example 11: Let $V = F^X$ (see example 7) and suppose $Y \subseteq X$

Then $W = \{f \in V \mid f(y) = 0 \ \forall \ y \in Y\}$ is a subspace of V

Clearly $0 \in W$ and for $f, g \in W, f(y) = 0 = g(y) \quad \forall \ y \in Y$

So $(f + g)(y) = f(y) + g(y) = 0 \quad \forall \ y \in Y$

$\Rightarrow f + g \in W$

Again, if $\alpha \in F$, then $(\alpha f)y = \alpha(f(y)) = 0 \quad \forall \ y \in Y$

$\Rightarrow \alpha f \in W.$

Example 12: If $V = \mathbf{R}^n$, then

$W = \{(x_1, x_2, ..., x_n) \mid x_1 + x_2 + ... + x_n = 1\}$ will not be a subspace of V.

Notice, $(1, 0, 0, ..., 0) + (0, 1, 0, ..., 0) = (1, 1, 0, ..., 0) \notin W$.

Example 13: Let $V = M_{2 \times 1}(F)$. Let A be a 2×2 matrix over F.

Then $$W = \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in V \mid A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0 \right\}$$ forms a subspace of V

$$W \neq \phi \text{ as } \begin{bmatrix} 0 \\ 0 \end{bmatrix} \in W$$

For $$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \text{ in } W, \text{ we have}$$

$$A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0 = A \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

$$\Rightarrow A \left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \right) = 0$$

$$\Rightarrow \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in W$$

Also $$A \left(\alpha \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \right) = \alpha A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0 \Rightarrow \alpha \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in W$$

Hence W is a subspace of V.

Example 14: Let $V = F_2^2$, where $F_2 = \{0, 1\}$ mod 2.

If $W_1 = \{(0, 0), (1, 0)\}$

$W_2 = \{(0, 0), (0, 1)\}$

$W_3 = \{(0, 0), (1, 1)\}$

Then $W_1 \cup W_2 \cup W_3 = \{(0, 0), (1, 0), (0, 1), (1, 1)\} = V$

Thus we notice that here V is union of finite number of proper subspaces.

This result may, however, not hold if V happens to be a vector space over an infinite field. (See Exercise 11, page 484)

Problem 2: *Let V be a vector space over a finite field F. Suppose $V = W_1 \cup W_2 \cup \ldots \cup W_k$, W_i being subspaces of V $\forall$ i. If $o(F) \geq k$ then, show that $V = W_i$ for some i.*

Solution: Suppose $V \neq W_i$ for any i

Now $W_k \not\subseteq W_1 \cup W_2 \cup \ldots\ldots \cup W_{k-1}$

and $W_1 \cup W_2 \cup \ldots\ldots \cup W_{k-1} \not\subseteq W_k$

$\Rightarrow$ $\exists\, x \in W_k$ s.t., $x \notin W_1 \cup W_2 \cup \ldots\ldots \cup W_{k-1}$

and $\exists\, y \in W_1 \cup \ldots\ldots \cup W_{k-1}$ s.t., $y \notin W_k$

Let $S = \{ax + y \mid a \in F\}$

Then no element of S can belong to W_k, as

$ax + y \in W_k \Rightarrow ax + y - ax = y \in W_k$, a contradiction

So $ax + y \notin W_k \quad \forall\, a \in F$

$\Rightarrow$ $ax + y \in W_1 \cup W_2 \cup \ldots\ldots \cup W_{k-1} \quad \forall\, a \in F$

So $\exists\, \alpha, \beta \in F$, $\alpha \neq \beta$ such that

$\alpha x + y \in W_j$, $\beta x + y \in W_j$ for some j, $1 \leq j \leq k - 1$

$\therefore$ $(\alpha x + y) - (\beta x + y) \in W_j$

$\Rightarrow$ $(\alpha - \beta)x \in W_j$

$\Rightarrow$ $x \in W_j \Rightarrow x \in W_1 \cup \ldots\ldots \cup W_{k-1}$, a contradiction

$\therefore$ $V = W_i$ for some i

(One may notice here that in previous example $o(F) = 2$ and we could write $V = W_1 \cup W_2 \cup W_3$, $V \neq W_i$ for any i)

Sum of Subspaces

If W_1 and W_2 be two subspaces of a vector space $V(F)$ then we define

$W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$

$W_1 + W_2 \neq \varphi$ as $0 = 0 + 0 \in W_1 + W_2$

Again, $x, y \in W_1 + W_2$, $\alpha, \beta \in F$ implies

$x = w_1 + w_2$

$y = w'_1 + w'_2 \qquad w_1, w'_1 \in W_1, w_2, w'_2 \in W_2$

$\alpha x + \beta y = \alpha (w_1 + w_2) + \beta(w'_1 + w'_2)$

$= (\alpha w_1 + \beta w'_1) + (\alpha w_2 + \beta w'_2) \in W_1 + W_2$

Showing thereby that sum of two subspaces is a subspace.

One can extend the definition, similarly, to the sum of n subspaces $W_1, W_2, ..., W_n$, which would also be a subspace and we write $W_1 + W_2 + ... + W_n = \sum_{i=1}^{n} W_i$

Definition: Let $W_1, W_2, ..., W_n$ be subspaces of V then $W_1 + W_2 + ... + W_n$ is called the direct sum if each $x \in W_1 + W_2 + ... + W_n$ can be expressed uniquely as $x = w_1 + w_2 + ... + w_n$, $w_i \in W_i$ and in that case we write

$$W_1 + W_2 + ... + W_n = W_1 \oplus W_2 \oplus ... \oplus W_n$$

We say, a vector space V is the direct sum of its subspaces $W_1, W_2, ..., W_n$ if $V = W_1 \oplus W_2 \oplus ... \oplus W_n$, *i.e.*, if

$$V = W_1 + W_2 + ... + W_n$$

and each $v \in V$ can be expressed uniquely as $v = w_1 + w_2 + ... + w_n$, $w_i \in W_i$.

Theorem 4: $V = W_1 \oplus W_2 \Leftrightarrow V = W_1 + W_2, W_1 \cap W_2 = (0)$.

Proof: Let $V = W_1 \oplus W_2$

We need to prove $W_1 \cap W_2 = (0)$

Let $x \in W_1 \cap W_2$, then $x \in W_1$ and $x \in W_2$

$$\Rightarrow x = 0 + x \in W_1 + W_2 = V$$

$$\Rightarrow x = x + 0 \in W_1 + W_2 = V$$

Since x has been expressed as $x = x + 0$ and $0 + x$ and the representation has to be unique, we get $x = 0$

$$\Rightarrow W_1 \cap W_2 = (0).$$

Conversely, let $v \in V$ be any element and suppose

$$v = w_1 + w_2$$

$$v = w'_1 + w'_2$$

are two representations of v

then $w_1 + w_2 = w'_1 + w'_2 \ (= v)$

$$\Rightarrow w_1 - w'_1 = w'_2 - w_2$$

Now L.H.S. is in W_1 and R.H.S. belongs to W_2

i.e., each belongs to $W_1 \cap W_2 = (0)$

$$\Rightarrow w_1 - w'_1 = w'_2 - w_2 = 0$$

$$\Rightarrow w_1 = w'_1, w_2 = w'_2.$$

Hence the result.

Remark: The above theorem can also be stated as

$$W_1 + W_2 = W_1 \oplus W_2 \Leftrightarrow W_1 \cap W_2 = \{0\}.$$

Example 15: Consider the space $V(F) = F^2(F)$ where F is a field

Let $W_1 = \{(a, 0) \mid a \in F\}$

$W_2 = \{(0, b) \mid b \in F\}$

then V is direct sum of W_1 and W_2

$v \in V \Rightarrow v = (a, b) = (a, 0) + (0, b) \in W_1 + W_2$

thus $V \subseteq W_1 + W_2$

or that $V = W_1 + W_2$

Again if $(x, y) \in W_1 \cap W_2$ be any element then

$(x, y) \in W_1$ and $(x, y) \in W_2$

$\Rightarrow y = 0$ and $x = 0$

$\Rightarrow (x, y) = (0, 0)$

$\Rightarrow W_1 \cap W_2 = (0)$

Hence $V = W_1 \oplus W_2$.

Problem 3: *Let V be the vector space of all functions from* $\mathbf{R} \to \mathbf{R}$. *Let $V_e = \{f \in V \mid f \text{ is even}\}$, $V_0 = \{f \in V \mid f \text{ is odd}\}$. Then V_e and V_0 are subspaces of V and $V = V_e \oplus V_0$.*

Solution: Addition and scalar multiplication in V are given by the rule $(f + g)\, x = f(x) + g(x)$; $(\alpha f)\, x = \alpha f(x)$

Now $V_e \neq \varphi$ as $0(x) = 0 \Rightarrow 0(x) = 0(-x)$

$\Rightarrow 0 \in V_e$

Again for $\alpha, \beta \in \mathbf{R}$, $f, g \in V_e$, we have

$$(\alpha f + \beta g)(-x) = (\alpha f)(-x) + (\beta g)(-x) = \alpha(f(-x)) + \beta(g(-x))$$
$$= \alpha f(x) + \beta g(x)$$
$$= (\alpha f + \beta g)x$$

$\Rightarrow \alpha f + \beta g \in V_e$

$\Rightarrow V_e$ is a subspace of V

Similarly, V_0 is a subspace of V.

Thus $V_e + V_0$ is a subspace of V. We show $V \subseteq V_e + V_0$

Let $f \in V$ be any member

Let $g : \mathbf{R} \to \mathbf{R}$ be such that $g(x) = f(-x)$, then $g \in V$

Also then $$f = \left(\frac{1}{2}f + \frac{1}{2}g\right) + \left(\frac{1}{2}f - \frac{1}{2}g\right)$$

Since $$\left(\frac{1}{2}f + \frac{1}{2}g\right)(-x) = \frac{1}{2}f(-x) + \frac{1}{2}g(-x) = \frac{1}{2}g(x) + \frac{1}{2}f(x)$$
$$= \left(\frac{1}{2}f + \frac{1}{2}g\right)x$$

we find $$\frac{1}{2}f + \frac{1}{2}g \in V_e$$

Similarly, $\frac{1}{2}f - \frac{1}{2}g \in V_0$

$\Rightarrow f \in V_e + V_0 \Rightarrow V \subseteq V_e + V_0$

or that $V = V_e + V_0$

Finally, $f \in V_e \cap V_0 \Rightarrow f \in V_e, f \in V_0$

$\Rightarrow f(-x) = f(x)$ and $f(-x) = -f(x)$

$\Rightarrow f(x) = -f(x) \Rightarrow f(x) + f(x) = 0 = 0(x)$

$\Rightarrow 2f(x) = 0\ (x)$ for all x

$\Rightarrow 2f = 0 \Rightarrow f = 0 \Rightarrow V_e \cap V_0 = (0)$.

Hence the result.

Problem 4: *If L, M, N are three subspaces of a vector space V, such that* $M \subseteq L$ *then show that* $L \cap (M + N) = (L \cap M) + (L \cap N) = M + (L \cap N)$.

Also give an example, where the result fails to hold when $M \not\subseteq L$.

Solution: We leave the first part for the reader to try. Recall a similar result was proved for ideals in rings. The equality is called modular equality.

Consider now the vector space $V = \mathbf{R}^2$

Let $L = \{(a, a) \mid a \in \mathbf{R}\}$

$M = \{(a, 0) \mid a \in \mathbf{R}\}$

$N = \{(0, b) \mid b \in \mathbf{R}\}$

It is a routine matter to cheek that L, M, N are subspaces of V. Indeed

$\alpha(a, a) + \beta(a', a') = (\alpha a, \alpha a) + (\beta a', \beta a')$

$= (\alpha a + \beta a', \alpha a + \beta a') \in L$ etc.

Now $(x, y) \in L \cap M \Rightarrow (x, y) \in L$ and $(x, y) \in M$

$\Rightarrow y = x$ and $y = 0$

$\Rightarrow x = 0 = y \Rightarrow (x, y) = (0, 0)$

Similarly, $L \cap N = \{(0, 0)\}$

$\Rightarrow L \cap M + L \cap N = \{(0, 0)\}$

Again, $M + N = \{(a, b) \mid a, b \in \mathbf{R}\}$ and as $(1, 1) \in M + N$

$(1, 1) \in L$

we find $(1, 1) \in L \cap (M + N)$, but $(1, 1) \notin L \cap M + L \cap N$

Hence $L \cap (M + N) \neq (L \cap M) + (L \cap N)$, when $M \not\subseteq L$.

Problem 5: *Let* $V = \mathbf{R}^X$ (*See example* 7) *and fix* $x_0 \in X$. *Define*

$W = \{f \in V \mid f(x_0) = 0\}$

$W' = \{g \in V \mid g(x) = 0\ \forall\ x \in X - \{x_0\}\}$

then show that W, W' are subspaces of V and $V = W \oplus W'$.

Solution: We leave it for the reader to show that W, W' are subspaces.

Let $f \in W \cap W'$ then $f \in W$ and $f \in W'$

$\Rightarrow f(x_0) = 0, f(x) = 0 \quad \forall\ x \in X, x \neq x_0$

$\Rightarrow f(x) = 0, \forall\ x \in X,$

$\Rightarrow f = 0$ and thus $W \cap W' = \{0\}$.

Let $f \in V$ and let $f(x_0) = r$

Then $(f - r\ \delta x_0) \in W, \quad r\ \delta x_0 \in W'$

and $f = (f - r\ \delta x_0) + r\ \delta x_0 \in W + W'$

$\therefore \quad V = W + W'$

i.e., $V = W \oplus W'$

Notice here δx_0 denotes the Kronecker delta *i.e.*, $\delta x_0\ (x_0) = 1$, $\delta x_0\ (x) = 0\ \forall\ x \neq x_0$.

Quotient Spaces

If W be a subspace of a vector space $V(F)$ then since $< W, + >$ forms an abelian group of $< V, + >$, we can talk of cosets of W in V. Let $\frac{V}{W}$ be the set of all cosets $W + v$, $v \in V$, then we show that $\frac{V}{W}$ also forms a vector space over F, under the operations defined by

$$(W + x) + (W + y) = W + (x + y) \qquad x, y \in V$$

$$\alpha(W + x) = W + \alpha x \qquad \alpha \in F$$

Addition is well defined, since,

$W + x = W + x'$

$W + y = W + y'$

$\Rightarrow x - x' \in W, y - y' \in W$

$\Rightarrow (x - x') + (y - y') \in W$

$\Rightarrow (x + y) - (x' + y') \in W$

$\Rightarrow W + (x + y) = W + (x' + y')$

Again, $W + x = W + x'$

$\Rightarrow x - x' \in W,$

$\Rightarrow \alpha(x - x') \in W \qquad \alpha \in F$

$\Rightarrow \alpha x - \alpha x' \in W$

$\Rightarrow W + \alpha x = W + \alpha x'$

$\Rightarrow \alpha(W + x) = \alpha(W + x')$

Thus, scalar multiplication is also well defined. It should now be a routine exercise to check that all conditions in the definition of a vector space are satisfied.

$W + 0$ will be zero of $\frac{V}{W}$

$W - x$ will be inverse of $W + x$

Also

$$\alpha((W + x) + (W + y)) = \alpha(W + (x + y)) = W + \alpha(x + y) = W + (\alpha x + \alpha y)$$
$$= (W + \alpha x) + (W + \alpha y) = \alpha(W + x) + \alpha(W + y) \text{ etc.}$$

Hence, V/W forms a vector space over F, called the quotient space of V by W.

Exercises

1. Show that in a vector space $V(F)$

(*i*) $\alpha v = \beta v \Rightarrow \alpha = \beta \quad (v \neq 0)$

(*ii*) $\alpha v_1 = \alpha v_2 \Rightarrow v_1 = v_2 \quad (\alpha \neq 0)$

(*iii*) $\alpha v = 0,\ v \neq 0 \Rightarrow \alpha = 0$

(*iv*) $\alpha v = 0,\ \alpha \neq 0 \Rightarrow v = 0$

(*v*) $\alpha v = v \Rightarrow \alpha = 1$ or $v = 0$. where $\alpha, \beta \in F$; $v, v_1, v_2 \in V$.

2. Is the set of all 2×2 Skew-Hermitian matrices a vector space over $\mathbf{C}$ w.r.t., matrix addition and multiplication of a matrix by a scalar?

3. Let V be the set of all the +ve real numbers. Define addition in V by $v_1 + v_2 = v_1 v_2$, the multiplication of real nos. v_1 & v_2. Define scalar multiplication in V by $\alpha v = v^{\alpha}$, $v \in V$, $\alpha \in \mathbf{R}$. Show that V forms a vector space over $\mathbf{R}$ w.r.t. these operations. [**Hint:** Zero will be 1 and $-v = \frac{1}{v}$].

4. Let $V(F)$ be a vector space, where char $F = p$, a prime. Define scalar multiplication in V by

$$\alpha o v = \alpha^p v,\ \alpha \in F,\ v \in V$$

Show that V forms a vector space over F, w.r.t., the original addition and new scalar multiplication.

5. Let V be a vector space over $\mathbf{C}$. Define scalar multiplication on V by $\alpha o v = \bar{\alpha} v$, $\alpha \in \mathbf{C}$, $v \in V$. Show that V also forms a vector space over $\mathbf{C}$ w.r.t. this new scalar multiplication.

6. Let $V = \{(z_1, z_2, z_3) \mid z_1, z_2, z_3 \in \mathbf{C}\} = \mathbf{C}^3$ be the vector space over $\mathbf{C}$. Check whether

(*i*) $W_1 = \{(z_1, z_2, z_3) \mid z_1 \text{ is a real number}\}$

(*ii*) $W_2 = \{(z_1, z_2, z_3) \mid z_1 + z_2 = 0\}$

(*iii*) $W_3 = \{(z_1, z_2, z_3) \mid z_1 + z_2 = 1\}$

are subspaces of V or not.

7. Which of the following are subspaces of $\mathbf{R}^3$?

(*i*) $W = \{(x_1, x_2, 1) \mid x_1, x_2 \in \mathbf{R}\}$

(*ii*) $W = \{(x_1, x_2, x_3) \in \mathbf{R}^3 \mid x_1 + x_2 + x_3 = 0\}$

(*iii*) $W = \{(x_1, x_2, x_3) \in \mathbf{R}^3 \mid x_1 - 2x_2 + 3x_3 = 0\}$

8. Which of the following are subspaces of $\mathbf{R}[x]$?

(*i*) $W = \{f(x) \in \mathbf{R}[x] \mid f(2) = 0\}$

(*ii*) $W = \{f(x) \in \mathbf{R}[x] \mid f(1) \geq 0\}$

(*iii*) $W = \{f(x) \in \mathbf{R}[x] \mid f(x) = f(-x)\}$

9. Show that intersection of two subspaces is a subspace.

10. Prove that union of two subspaces is a subspace iff one of them is contained in the other.

11. If V is a vector space over an infinite field F then show that it is not possible to write V as union of a finite number of proper subspaces.

12. Which of the following are subspaces of $M_n(F)$?

(*i*) $W = \{A \in M_n(F) \mid A \text{ is diagonal matrix}\}$

(*ii*) $W = \{A \in M_n(F) \mid \text{Trace } A = 0\}$

(*iii*) $W = \{A \in M_n(F) \mid A \text{ is upper triangular matrix}\}$

(*iv*) $W = \{A \in M_n(F) \mid A \text{ is symmetric}\}$

13. Let $V = \mathbf{R}^4$. Show that

$$W_1 = \{(a, b, c, d) \mid a = b + c + d\}$$

$$W_2 = \{(a, b, c, d) \mid a = 3c, b = 4d\}$$

are subspaces of V.

14. Give an example of a vector space having (*i*) two elements (*ii*) four elements.

[**Hint:** Take $F = \{0, 1\}$ mod 2 and $V = \{(\alpha, \beta) \mid \alpha, \beta \in F\}$].

15. Let V be an abelian group under addition with at least two elements. Define scalar multiplication by $\alpha \cdot v = 0 \ \forall \ \alpha \in F, v \in V$ where F is a field. Is V a vector space over F?

16. Let G be an abelian group such that $px = 0 \ \forall \ x \in G$, where p is a fixed prime. Define scalar multiplication by $\bar{a}x = ax$, $\bar{a} \in \mathbf{Z}_p$, $x \in G$. Show that this multiplication is well defined and G forms a vector space over $\mathbf{Z}_p$.

17. Let W_1 & W_2 be proper subspaces of V. Show that there exists $v \in V$ s.t., $v \notin W_1$, $v \notin W_2$.

18. Let $W_1, W_2, \ldots, W_n$ be subspaces of V. Show that

$W_1 + W_2 + \ldots + W_n = W_1 \oplus W_2 \oplus \ldots \oplus W_n$ if and only if $W_k \cap \sum_{\substack{j=1 \\ j \neq k}}^{n} W_j = \{0\}$

19. Let V be the set of all sequences of real numbers $a = (a_1, a_2, \ldots, a_n, \ldots)$ s.t., $\sum_1^\infty a_i^2 < \infty$.

Show that V forms a vector space over $\mathbf{R}$ with component-wise addition and multiplication.

[**Hint:** $\sum_1^n a_i b_i \leq \left(\sum_1^n a_i^2\right)\left(\sum_1^n b_i^2\right) \leq \left(\sum_1^\infty a_i^2\right)\left(\sum_1^\infty b_i^2\right) < \infty$

$\Rightarrow \quad \sum_1^\infty a_i b_i < \infty \Rightarrow \sum_1^\infty (a_i + b_i)^2 < \infty$].

20. Let $V = \{a_0 + a_1x + a_2x^2 \mid a_i \in F\}$ and
$W_1 = \{f(x) \in V \mid f(0) = 0\}$, $W_2 = \{f(x) \in V \mid f(1) = 0\}$
Show that W_1 and W_2 are subspaces of V and $W_1 \cup W_2$ is not a subspace of V. Find also $W_1 \cap W_2$ and $W_1 + W_2$.

21. Let V be the vector space of all $n \times n$ matrices over **R**. Let W_1 be the set of all symmetric matrices in V and W_2 be the set of all skew symmetric matrices in V. Show that W_1 and W_2 are subspaces of V and $V = W_1 \oplus W_2$.

Homomorphisms or Linear Transformations

We are already familiar with the concept of a homomorphism in case of groups and rings. We introduce the same in vector spaces.

Definition: Let V and U be two vector spaces over the same field F, then a mapping $T : V \to U$ is called a homomorphism or a linear transformation if

$$T(x + y) = T(x) + T(y) \quad \text{for all } x, y \in V$$
$$T(\alpha x) = \alpha T(x) \quad \alpha \in F$$

One can combine the two conditions to get a single condition

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) \quad x, y \in V; \alpha, \beta \in F$$

It is easy to see that both are equivalent. If a homomorphism happens to be one-one onto also we call it an *isomorphism*, and say the two spaces are isomorphic. (Notation $V \cong U$).

Example 16: Identity map $I : V \to V$, s.t.,

$$I(v) = v$$

and the zero map $O : V \to V$, s.t.,

$$O(v) = 0$$

are clearly linear transformations.

Example 17: For a field F, consider the vector spaces F^2 and F^3. Define a map $T : F^3 \to F^2$, by

$$T(\alpha, \beta, \gamma) = (\alpha, \beta)$$

then T is a linear transformation as

for any $x, y \in F^3$, if $x = (\alpha_1, \beta_1, \gamma_1)$

$$y = (\alpha_2, \beta_2, \gamma_2)$$

then
$$T(x + y) = T(\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$
$$= (\alpha_1, \beta_1) + (\alpha_2, \beta_2) = T(x) + T(y)$$

and
$$T(\alpha x) = T(\alpha(\alpha_1, \beta_1, \gamma_1)) = T((\alpha\alpha_1, \alpha\beta_1, \alpha\gamma_1)$$
$$= (\alpha\alpha_1, \alpha\beta_1) = \alpha(\alpha_1, \beta_1) = \alpha T(x)$$

Example 18: Let V be the vector space of all polynomials in x over a field F. Define

$$T : V \to V, \text{ s.t.,}$$

$$T(f(x)) = \frac{d}{dx} f(x)$$

then
$$T(f + g) = \frac{d}{dx}(f + g) = \frac{d}{dx} f + \frac{d}{dx} g = T(f) + T(g)$$

$$T(\alpha f) = \frac{d}{dx}(\alpha f) = \alpha \frac{d}{dx} f = \alpha T(f)$$

shows that T is a linear transformation.

In fact, if $\theta : V \to V$ be defined such that

$$\theta(f) = \int_0^x f(t)\ dt$$

then θ will also be a linear transformation.

Example 19: Consider the mapping

$T : \mathbf{R}^3 \to \mathbf{R}$, s.t.,

$$T(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$$

then T is not a linear transformation.

Consider, for instance,

$$T((1, 0, 0) + (1, 0, 0)) = T(2, 0, 0) = 4$$
$$T(1, 0, 0) + T(1, 0, 0) = 1 + 1 = 2.$$

Exercises

Check which of the following are linear transformations

1. $T : \mathbf{R}^2 \to \mathbf{R}^2$, s.t., $T(x_1, x_2) = (1 + x_1, x_2)$
2. $T : \mathbf{R}^2 \to \mathbf{R}^2$, s.t., $T(x_1, x_2) = (x_2, x_1)$
3. $T : \mathbf{C} \to \mathbf{C}$, s.t., $T(z) = \bar{z}$, where $\mathbf{C}$ is vector space of complex numbers over reals.
4. $T : \mathbf{C} \to \mathbf{C}$, s.t., $T(x + iy) = x$
5. $T : \mathbf{R}^3 \to \mathbf{R}^4$, s.t., $T(x_1, x_2, x_3) = (x_1,\ x_1 + x_2,\ x_1 + x_2 + x_3,\ x_3)$
6. $T : \mathbf{R}^2 \to \mathbf{R}^3$, s.t., $T(x_1, x_2) = (x_1,\ x_1 + x_2,\ x_2)$
7. $T : \mathbf{R} \to \mathbf{R}^3$, s.t., $T(x) = (x, x^2, x^3)$
8. Show that $T : M_n(F) \to F$, s.t., $T(A)$ = Trace A = Sum of diagonal elements of A is an onto linear transformation which is not 1–1.
9. Let $T : M_{m \times n}(F) \to M_{n \times m}(F)$ s.t.,
   $T(A) = A'$ = Transpose of A
   Show that T is a linear transformation. Is it 1–1? Is it onto?
10. Show that $T : F[x] \to F$, s.t.,
    $$T(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1 \alpha + \ldots + a_n \alpha^n, \quad \alpha \in F$$
    is an onto linear transformation but is not 1–1.
11. Show that any linear transformation $T : \mathbf{R} \to \mathbf{R}$ is of the form $T(x) = \alpha x$ for some $\alpha \in \mathbf{R}$.

In the theorems that follow, we take V and U to be vector spaces over the same field F.

Theorem 5: *Under a homomorphism* $T : V \to U$,

(*i*) $T(0) = 0$ (*ii*) $T(-x) = -T(x)$.

Proof: $T(0) = T(0 + 0) = T(0) + T(0)$

$\Rightarrow T(0) = 0$

Again $T(-x) + T(x) = T(-x + x) = T(0) = 0$

$\Rightarrow -T(x) = T(-x)$.

Definition: Let $T : V \to U$ be a homomorphism, then *kernel of* T is defined by

$$\text{Ker } T = \{x \in V \mid T(x) = 0\}$$

It is also called the *null space* of T.

Theorem 6: *Let* $T : V \to U$ *be a homomorphism, then Ker* T *is a subspace of* V.

Proof: Ker $T \neq \varphi$ as $0 \in$ Ker T

Let $\alpha, \beta \in F$, $x, y \in$ Ker T be any elements

then $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$

$= \alpha \cdot 0 + \beta \cdot 0 = 0 + 0 = 0$

$\Rightarrow \alpha x + \beta y \in$ Ker T.

Theorem 7: *Let* $T : V \to U$ *be a homomorphism, then*

Ker $T = \{0\}$ *iff* T is *one-one*.

Proof: Let Ker T = $\{0\}$. If $T(x) = T(y)$

then $T(x) - T(y) = 0$

$\Rightarrow T(x - y) = 0$

$\Rightarrow (x - y) \in$ Ker $T = \{0\}$

$\Rightarrow x - y = 0$

$\Rightarrow x = y \Rightarrow T$ is 1–1.

Conversely, let T be one-one

if $x \in$ Ker T be any element, then $T(x) = 0$

$\Rightarrow T(x) = T(0)$

$\Rightarrow x = 0$

$\Rightarrow$ Ker $T = \{0\}$.

Definition: Let $T : V \to U$ be a linear transformation then range of T is defined to be

$$T(V) = \{T(x) \mid x \in V\} = \text{Range } T = R_T$$
$$= \{u \in U \mid u = T(v),\ v \in V\}$$

Theorem 8: *Let* $T : V \to U$ *be a L.T.* (*linear transformation*) *then range of* T *is subspace of* U.

Proof: Since $T(0) = 0$, $0 \in V$

$\therefore$ $T(0) \in$ Range T

i.e., Range $T \neq \varphi$

Let $\alpha, \beta \in F$, $T(x), T(y) \in T(V)$ be any elements

then $x, y \in V$

Now $\alpha T(x) + \beta T(y) = T(\alpha x + \beta y) \in T(V)$

as $\alpha x + \beta y \in V$

Hence the result.

Note: $T(V) = U$ iff T is onto.

Theorem 9: *Let $T : V \to U$ be a L.T. then*

$$\frac{V}{Ker\ T} \cong Range\ T = T(V).$$

Proof: Let $T : V \to U$ and put Ker $T = K$, then K being a subspace of V, we can talk of V/K.

Define a mapping $\theta : V/K \to T(V)$, s.t.,

$$\theta(K + x) = T(x), \quad x \in V$$

Then θ is well defined, one-one map as

$$\begin{aligned} & K + x = K + y \\ \Leftrightarrow\ & x - y \in K = \text{Ker } T \\ \Leftrightarrow\ & T(x - y) = 0 \\ \Leftrightarrow\ & T(x) = T(y) \\ \Leftrightarrow\ & \theta(K + x) = \theta(K + y) \end{aligned}$$

If $T(x) \in T(V)$ be any element, then $x \in V$ and $\theta(K + x) = T(x)$, showing that θ is onto.

Finally, $\theta((K + x) + (K + y)) = \theta(K + (x + y))$

$$= T(x + y)$$
$$= T(x) + T(y)$$
$$= \theta(K + x) + \theta(K + y)$$

and $\theta(\alpha(K + x)) = \theta(K + \alpha x) = T(\alpha x) = \alpha T(x) = \alpha\, \theta(K + x)$

shows θ is a *L.T.* and hence an isomorphism.

Note: The above is called the *Fundamental Theorem of homomorphism* for vector spaces.

If the map T is also onto, then we have proved $\frac{V}{\text{Ker } T} \cong U$.

Theorem 10: *If A and B be two subspaces of a vector space $V(F)$, then*

$$\frac{A + B}{A} \cong \frac{B}{A \cap B}.$$

Proof: A being a subspace of $A + B$ and $A \cap B$ being a subspace of B, we can talk of $\frac{A + B}{A}$ and $\frac{B}{A \cap B}$.

Define a map $\theta : B \to \frac{A + B}{A}$ s.t.,

$$\theta(b) = A + b, \quad b \in B$$

Since $b_1 = b_2 \Rightarrow A + b_1 = A + b_2$, we find θ is well defined.

Again, as
$$\begin{aligned}\theta(\alpha b_1 + \beta b_2) &= A + (\alpha b_1 + \beta b_2)\\ &= (A + \alpha b_1) + (A + \beta b_2)\\ &= \alpha(A + b_1) + \beta(A + b_2)\\ &= \alpha\theta(b_1) + \beta\theta(b_2)\end{aligned}$$

θ is a *L.T.*

For any $A + x \in \dfrac{A+B}{A}$, we find $x \in A + B$

$$\Rightarrow x = a + b, \quad a \in A, b \in B$$
$$\begin{aligned}A + x &= A + (a + b)\\ &= (A + a) + (A + b) = A + (A + b)\\ &= A + b = \theta(b).\end{aligned}$$

Showing that b is the required pre image of $A + x$ under θ and thus θ is onto.

Hence by Fundamental theorem

$$\frac{A+B}{A} \cong \frac{B}{\text{Ker}\,\theta}.$$

We claim Ker $\theta = A \cap B$

Indeed
$$\begin{aligned}x \in \text{Ker}\,\theta &\Leftrightarrow \theta(x) = A\\ &\Leftrightarrow A + x = A\\ &\Leftrightarrow x \in A, \text{ also } x \in \text{Ker}\,\theta \subseteq B\\ &\Leftrightarrow x \in A \cap B\end{aligned}$$

Hence $$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

Note: By interchanging A and B, we get $\dfrac{B+A}{B} \cong \dfrac{A}{B \cap A}$

i.e., $$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

Cor.: If $A + B$ is the direct sum then as $A \cap B = \{0\}$

we get $$\frac{A}{(0)} \cong \frac{A \oplus B}{B}$$

But $\dfrac{A}{(0)} \cong A$ (*see remark below after theorem* 11) gives us $A \cong \dfrac{A \oplus B}{B}$.

Theorem 11: *Let W be a subspace of V, then $\exists$ an onto L.T. $\theta : V \to \dfrac{V}{W}$ such that Ker $\theta = W$.*

Proof: Define $\theta: V \to \frac{V}{W}$ s.t.,

$$\theta(x) = W + x$$

then θ is clearly well defined.

Also $\theta(\alpha x + \beta y) = W + (\alpha x + \beta y)$

$$= (W + \alpha x) + (W + \beta y)$$

$$= \alpha(W + x) + \beta(W + y) = \alpha\theta(x) + \beta\theta(y)$$

Shows θ is a *L.T.*

θ is clearly onto.

Again, $x \in \text{Ker } \theta \Leftrightarrow \theta(x) = W$

$$\Leftrightarrow W + x = W$$

$$\Leftrightarrow x \in W$$

Hence $\text{Ker } \theta = W$.

θ is called the *natural homomorphism* or the *quotient map*.

Remark: In case $W = (0)$ in the above we find θ will be 1–1 also as

$$\theta(a) = \theta(b)$$

$$\Rightarrow W + a = W + b$$

$$\Rightarrow a - b \in W = (0)$$

$$\Rightarrow a - b = 0$$

$$\Rightarrow a = b.$$

Hence in that case $V \cong \frac{V}{W}$ or $V \cong \frac{V}{(0)}$.

Note $W = (0) \Rightarrow \text{Ker } \theta = (0) \Rightarrow \theta$ is one-one.

Problem 6: *Let W and U be subspaces of $V(F)$ such that $W \subset U \subset V$. Let $f: V \to V/W$ be the quotient map. Show that $f(U)$ is a proper subspace of V/W.*

Solution: Since f is a *L.T.*, $f(U)$ is a subspace of V/W.

If $f(U) = 0$ then $f(x) = 0$ for all $x \in U$

$$\Rightarrow W + x = W \quad \text{for all } x \in U$$

$$\Rightarrow x \in W \quad \text{for all } x \in U$$

$$\Rightarrow U \subseteq W, \text{ a contradiction}$$

Again since $U \neq V$, $\exists\ v_0 \in V$ s.t., $v_0 \notin U$.

If $f(v_0) \in f(U)$ then $f(v_0) = f(x)$ for some $x \in U$

$$\Rightarrow f(v_0 - x) = 0$$

$$\Rightarrow W + (v_0 - x) = W$$

$$\Rightarrow v_0 - x \in W$$

$$\Rightarrow v_0 = x + w \quad \text{for some } w \in W$$

$$\Rightarrow v_0 \in U, \text{ a contradiction}$$

Hence $f(v_0) \notin f(U) \Rightarrow f(U) \neq \frac{V}{W}$

or that $f(U)$ is a proper subspace of $\frac{V}{W}$.

Theorem 12: *Let $T : V \to U$ be an onto homomorphism with Ker $T = W$. Then there exists a one-one onto mapping between the subspaces of U and the subspaces of V which contain W.*

Proof: Let $\mathscr{A}$ = set of all subspaces of V, which contain W

$\mathscr{B}$ = set of all subspaces of U

Define a mapping $\theta : \mathscr{A} \to \mathscr{B}$, s.t.,

$$\theta(W_1) = T(W_1)$$

Since $T : V \to U$, $T(W_1)$ will be a subspace of U as

for any $T(x)$, $T(y) \in T(W_1)$ and $\alpha, \beta \in F$.

$\alpha T(x) + \beta T(y) = T(\alpha x + \beta y) \in T(W_1)$, as $x, y \in W_1$

Again $W_1 = W_1'$

$\Rightarrow T(W_1) = T(W_1')$

$\Rightarrow \theta$ is well defined.

Now if $\theta(W_1) = \theta(W_1')$

Then $T(W_1) = T(W_1') \Rightarrow W_1 = W_1'$

as $x \in W_1$ $\Rightarrow T(x) \in T(W_1) = T(W_1')$

$\Rightarrow T(x) \in T(W_1')$

$\Rightarrow T(x) = T(y), \quad y \in W_1'$

$\Rightarrow T(x - y) = 0$

$\Rightarrow x - y \in$ Ker $T = W \subseteq W_1'$

$\Rightarrow x \in W_1'$ as $y \in W_1'$

$\Rightarrow W_1 \subseteq W_1'$. Similarly $W_1' \subseteq W_1$

Hence θ is 1–1.

Let $U_1 \in \mathscr{B}$ be any member.

Define $T^{-1}(U_1) = \{x \in V \mid T(x) \in U_1\}$

Then $0 \in T^{-1}(U_1)$ as $T(0) = 0 \in U_1$

$\Rightarrow T^{-1}(U_1) \neq \varphi$

For $\alpha, \beta \in F$, $x, y \in T^{-1}(U_1)$, we have

$T(x) \in U_1$, $T(y) \in U_1$

$\Rightarrow \alpha T(x) + \beta T(y) \in U_1$

$\Rightarrow T(\alpha x + \beta y) \in U_1$

$\Rightarrow \alpha x + \beta y \in T^{-1}(U_1)$

or that $T^{-1}(U_1)$ is a subspace of V.

Let $x \in W$ then $x \in \text{Ker } T$

$\Rightarrow T(x) = 0 \in U_1$

$\Rightarrow x \in T^{-1}(U_1)$

$\Rightarrow W \subseteq T^{-1}(U_1)$

$\Rightarrow T^{-1}(U_1) \in \mathscr{A}$

Also $T(T^{-1}(U_1)) = \{T(x) \in V \mid T(x) \in U_1\} \subseteq U_1$.

Let $y \in U_1 \Rightarrow y \in U \Rightarrow \exists\, x \in V$, s.t., $T(x) = y$

as T is onto, $x \in T^{-1}(U_1)$

$\Rightarrow y = T(x) \in (T(T^{-1})\ (U_1))$

$\Rightarrow T(T^{-1})(U_1)) = U_1$

$\Rightarrow \theta(T^{-1}(U_1)) = U_1$

$\Rightarrow \theta$ is onto.

Hence the theorem is proved.

Linear Span

Definition: Let $V(F)$ be a vector space, $v_i \in V$, $\alpha_i \in F$ be elements of V and F respectively. Then elements of the type $\sum_{i=1}^{n} \alpha_i v_i$ are called *linear combinations* of $v_1, v_2, \ldots, v_n$ over F.

Let S be a non empty subset of V, then the set

$$L(S) = \left\{ \sum_{i=1}^{n} \alpha_i v_i \mid \alpha_i \in F, v_i \in S, n \text{ finite} \right\}$$

i.e., the set of all linear combinations of finite sets of elements of S is called *linear span* of S. It is also denoted by $< S >$. If $S = \varphi$, define $L(S) = \{0\}$.

Theorem 13: *$L(S)$ is the smallest subspace of V, containing S.*

Proof: $L(S) \neq \varphi$ as $v \in S \Rightarrow v = 1 \,.\, v$, $1 \in F$

$\Rightarrow v \in L(S)$

thus, in fact, $S \subseteq L(S)$.

Let $x, y \in L(S)$, $\alpha, \beta \in F$ be any elements

then $x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$

$y = \beta_1 v_1' + \beta_2 v_2' + \ldots + \beta_m v_m' \qquad v_i, v_j' \in S, \quad \alpha_i, \beta_j \in F$

Thus $\alpha x + \beta y = \alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + \ldots + \alpha\alpha_n v_n + \beta\beta_1 v_1' + \ldots + \beta\beta_m v_m'$.

R.H.S. being a linear combination belongs to $L(S)$

Hence $L(S)$ is a subspace of V, containing S.

Let now W be any subspace of V, containing S

We show $L(S) \subseteq W$

$x \in L(S) \Rightarrow x = \Sigma\alpha_i v_i \qquad v_i \in S,\ \alpha_i \in F$

$v_i \in S \subseteq W$ for all i and W is a subspace

$\Rightarrow \Sigma\alpha_i v_i \in W \Rightarrow x \in W$

$\Rightarrow L(S) \subseteq W$

Hence the result follows.

Theorem 14: *If S_1 and S_2 are subsets of V, then*

(*i*) $S_1 \subseteq S_2 \Rightarrow L(S_1) \subseteq L(S_2)$

(*ii*) $L(S_1 \cup S_2) = L(S_1) + L(S_2)$

(*iii*) $L(L(S_1)) = L(S_1)$.

Proof: (*i*) $x \in L(S_1) \Rightarrow x = \Sigma\alpha_i v_i \quad v_i \in S_1,\ \alpha_i \in F$

thus $v_i \in S_1 \subseteq S_2$ for all i

$\Rightarrow \quad \Sigma\alpha_i v_i \in S_2 \Rightarrow x \in L(S_2)$

$\Rightarrow \quad L(S_1) \subseteq L(S_2)$.

(*ii*) $\quad S_1 \subseteq S_1 \cup S_2 \Rightarrow L(S_1) \subseteq L(S_1 \cup S_2)$

$\quad S_2 \subseteq S_1 \cup S_2 \Rightarrow L(S_2) \subseteq L(S_1 \cup S_2)$

$\Rightarrow \quad L(S_1) + L(S_2) \subseteq L(S_1 \cup S_2)$

Again, $\quad S_1 \subseteq L(S_1) \subseteq L(S_1) + L(S_2)$

$\quad S_2 \subseteq L(S_2) \subseteq L(S_1) + L(S_2)$

$\Rightarrow \quad S_1 \cup S_2 \subseteq L(S_1) + L(S_2)$.

Hence $\quad L(S_1 \cup S_2) \subseteq L(S_1) + L(S_2)$

as $L(S_1 \cup S_2)$ is the smallest subspace containing $S_1 \cup S_2$ and $L(S_1) + L(S_2)$ is a subspace, being sum of two subspaces (and contains $S_1 \cup S_2$).

Thus $\quad L(S_1 \cup S_2) = L(S_1) + L(S_2)$.

(*iii*) $\quad$ Let $L(S_1) = K$ then we show $L(K) = L(S_1)$

Now $K \subseteq L(K) \ \therefore\ L(S_1) \subseteq L(L(S_1))$

Again $x \in L(L(S_1)) \Rightarrow x$ is linear combination of members of $L(S_1)$ which are linear combinations of members of S_1.

So x is a linear combination of members of S_1

$\Rightarrow \quad x \in L(S_1)$

Thus $\quad L(L(S_1)) \subseteq L(S_1)$

Hence $\quad L(L(S_1)) = L(S_1)$.

Theorem 15: *If W is a subspace of V, then $L(W) = W$ and conversely.*

Proof: $W \subseteq L(W)$ by definition and since $L(W)$ is the smallest subspace of V containing W and W is itself a subspace

$L(W) \subseteq W$

Hence $\quad L(W) = W$.

Conversely, let $L(W) = W$

Let $x, y \in W, \alpha, \beta \in F$

Then $x, y \in L(W)$

$\Rightarrow x, y$ are linear combinations of members of W.

$\Rightarrow \alpha x + \beta y$ is a linear combination of members of W

$\Rightarrow \alpha x + \beta y \in L(W)$

$\Rightarrow \alpha x + \beta y \in W$

$\Rightarrow W$ is a subspace.

Definition: If $V = L(S)$, we say S spans (or generates) V. The vector space V is said to be *finite-dimensional* (over F) if there exists a finite subset S of V such that $V = L(S)$. We use notation *F.D.V.S.* for a finite dimensional vector space.

It now follows, from the results we've proved that

If S_1 and S_2 are two subspaces of V, then $S_1 + S_2$ is the subspace spanned by $S_1 \cup S_2$

Indeed, $L(S_1 \cup S_2) = L(S_1) + L(S_2) = S_1 + S_2$.

Problem 7: *Let $S = \{(1, 4), (0, 3)\}$ be a subset of $\mathbf{R}^2(\mathbf{R})$. Show that $(2, 3)$ belongs to $L(S)$.*

Solution: $(2, 3) \in L(S)$ if it can be put as a linear combination of $(1, 4)$ and $(0, 3)$.

Now $(2, 3) = \alpha(1, 4) + \beta(0, 3)$

$\Rightarrow (2, 3) = (\alpha + 0, 4\alpha + 3\beta)$

$\Rightarrow 2 = \alpha, 4\alpha + 3\beta = 3$

$\Rightarrow \alpha = 2, \beta = -\frac{5}{3}$

Hence $(2, 3) = 2\ (1, 4) - \frac{5}{3}\ (0, 3)$

Showing that $(2, 3) \in L(S)$.

Problem 8: *Let $V = \mathbf{R}^4(\mathbf{R})$ and let $S = \{(2, 0, 0, 1), (-1, 0, 1, 0)\}$. Find $L(S)$.*

Solution: Any element $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in L(S)$ is a linear combination of members of S.

Let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha(2, 0, 0\ 1) + \beta(-1, 0, 1, 0), \quad \alpha, \beta \in \mathbf{R}$

then $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (2\alpha - \beta, 0, \beta, \alpha)$

i.e., $L(S) = \{(2\alpha - \beta, 0, \beta, \alpha) \mid \alpha, \beta \in \mathbf{R}\}$

Problem 9: *Show that the vector space $F[x]$ is not finite dimensional.*

Solution: Let $V = F[x]$ and suppose it is finite dimensional.

Then $\exists\ S \subseteq V$, s.t., $V = L(S)$ and S is finite.

Suppose $S = \{p_1, p_2, ..., p_k\}$. We can assume $p_i \neq 0 \quad \forall i$

Let deg $p_i = r_i$ and let $t = \text{Max } \{r_1, r_2, ..., r_k\}$

Now $x^{t+1} \in V$ and since $V = L(S)$,

$x^{t+1} = \alpha_1 p_1 + \alpha_2 p_2 + ... + \alpha_k p_k, \quad \alpha_i \in F$

So $0 = (-1)\ x^{t+1} + \alpha_1 p_1 + ... + \alpha_k p_k$

Since x^{t+1} does not appear in $p_1, p_2, ..., p_k$

we get $-1 = 0$, a contradiction. Hence V is not *FDVS* over F.

Note if $S = \{1, x, ..., x^n, ...\}$ then $V = L(S)$.

Problem 10: *Let* $V = F^S$ *and* $W = \{f \in V \mid f(s) = 0$, for almost all $s \in S\}$.

Show that W *is a subspace of* V *and it is FDVS if* S *is finite*.

Solution: It is easy to check that W is a subspace of V.

Define $\psi_s : S \to F$, s.t., $(s \in S)$

$\psi_s(t) = 1$ if $s = t$

$= 0$ if $s \neq t$

Then $\psi_s \in W \quad \forall\, s \in S$

Let $T = \{\psi_s \mid s \in S\} \subseteq W$.

We show $W = L(T)$

Let $f \in W$ and let $f(s_1) = \alpha_{s_1}, f(s_2) = \alpha_{s_2}, ..., f(s_n) = \alpha_{s_n}$

Such that $\alpha_{s_i} \neq 0 \quad \forall i$

and $f(s) = 0 \quad \forall\, s \neq s_i$ in S

Then $f = \alpha_{s_1}\psi_{s_1} + ... + \alpha_{s_n}\psi_{s_n}$

and so $W = L(T)$.

If S is finite then T is also finite.

$\therefore$ W is a *FDVS* if S is finite.

Linear Dependence and Independence

Let $V(F)$ be a vector space. Elements $v_1, v_2, ..., v_n$ in V are said to be linearly dependent (over F) if $\exists$ scalars $\alpha_1, \alpha_2, ... \alpha_n \in F$, (not all zero) such that

$$\alpha_1 v_1 + \alpha_2 v_2 + ... \alpha_n v_n = 0$$

($v_1, v_2, ..., v_n$ are finite in number, not essentially distinct).

Thus for linear dependence $\Sigma \alpha_i v_i = 0$ and at least one $\alpha_i \neq 0$.

If $v_1, v_2 ... v_n$ are not linearly dependent (*L.D.*) these are called linearly independent (*L.I.*)

In other words, $v_1, v_2, .., v_n$ are *L.I.* if

$$\Sigma \alpha_i v_i = 0 \Rightarrow \alpha_i = 0 \text{ for all } i$$

A finite set $X = \{x_1, x_2, ..., x_n\}$ is said to be *L.D.* or *L.I.* according as its n members are *L.D.* or *L.I.*

In general any subset Y of $V(F)$ is called *L.I.* if every finite non empty subset of Y is *L.I.*, *otherwise* it is called *L.D.*

So, if some subsets are *L.I.* and some are *L.D.* then Y is called *L.D.*

Observations: (*i*) A non zero vector is always *L.I.* as $v \neq 0$, $\alpha v = 0$ would mean $\alpha = 0$.

(*ii*) Zero vector is always *L.D.*

$1 \cdot 0 = 0 \qquad 1 \neq 0,\ 1 \in F$

Thus any collection of vectors to which zero belongs is always *L.D.*

In other words, if $v_1, v_2, ..., v_n$ are *L.I.* then none of these can be zero. (But not conversely, see example ahead).

(*iii*) v is *L.I.* iff $v \neq 0$.

(*iv*) Any subset of a *L.I.* set is *L.I.*

(*v*) Any super set of a *L.D.* set is *L.D.*

(*vi*) Empty set φ is *L.I.* since it has no non empty finite subset and consequently it satisfies the condition for linear independence. In other words, whenever $\Sigma\alpha_i v_i = 0$ in φ then as there is no i for which $\alpha_i \neq 0$, set φ is *L.I.* We sometimes express it by saying that empty set is *L.I.* vacuously.

(*vii*) A set of vector is *L.I.* if and only if every finite subset of it is *L.I.*

Example 20: Consider $\mathbf{R}^2(\mathbf{R})$, $\mathbf{R}$ = reals.

$v_1 = (1, 0),\ v_2 = (0, 1) \in \mathbf{R}^2$ are *L.I.*

as $\alpha_1 v_1 + \alpha_2 v_2 = 0$ for $\alpha_1, \alpha_2 \in \mathbf{R}$

$\Rightarrow \alpha_1(1, 0) + \alpha_2(0, 1) = (0, 0)$

$\Rightarrow (\alpha_1, \alpha_2) = (0, 0) \Rightarrow \alpha_1 = \alpha_2 = 0.$

Example 21: Consider the subset

$S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (2, 3, 4)\}$

in the vector space $\mathbf{R}^3(\mathbf{R})$.

Since $2(1, 0, 0) + 3(0, 1, 0) + 4(0, 0, 1) - 1(2, 3, 4) = (0, 0, 0)$

we find S is *L.D.*

Example 22: In the vector space $F[x]$ of polynomials the vectors $f(x) = 1 - x$, $g(x) = x - x^2$, $h(x) = 1 - x^2$ are *L.D.* since $f(x) + g(x) - h(x) = 0$.

Problem 11: *Show that the vectors* $v_1 = (0, 1, -2),\ v_2 = (1, -1, 1),\ v_3 = (1, 2, 1)$ *are L.I. in* $\mathbf{R}^3(\mathbf{R})$.

Solution: Let $\Sigma\alpha_i v_i = 0$ for $\alpha_i \in \mathbf{R}$

Then $\alpha_1(0, 1, -2) + \alpha_2(1, -1, 1) + \alpha_3(1, 2, 1) = (0, 0, 0)$

$\Rightarrow (0, \alpha_1, -2\alpha_1) + (\alpha_2, -\alpha_2, \alpha_2) + (\alpha_3, 2\alpha_3, \alpha_3) = (0, 0, 0)$

$\Rightarrow 0 + \alpha_2 + \alpha_3 = 0$

$\alpha_1 - \alpha_2 + 2\alpha_3 = 0$

$-2\alpha_1 + \alpha_2 + \alpha_3 = 0$

Since the coefficient determinant $\begin{vmatrix} 0 & 1 & 1 \\ 1 & -1 & 2 \\ -2 & 1 & 1 \end{vmatrix}$ is $-6 \neq 0$ the above equations have only the zero common solution

$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0 \Rightarrow v_1, v_2, v_3$ are *L.I.*

Problem 12: *Show that* $\{f(x), g(x), h(x)\}$ *is L.I. in* $F[x]$, *whenever. deg* $f(x)$, *deg* $g(x)$, *deg* $h(x)$ *are distinct*.

Solution: Let $f(x) = a_0 + a_1x + ... + a_mx^m, \quad a_m \neq 0$

$g(x) = b_0 + b_1x + ... + b_nx^n, \quad b_n \neq 0$

$h(x) = c_0 + c_1x + ... + c_tx^t, \quad c_t \neq 0$

Let $\alpha f(x) + \beta g(x) + \gamma h(x) = 0, \quad \alpha, \beta, \gamma \in F$

Let $m < n < t$ (without any loss of generality)

then $\gamma c_t = 0 \Rightarrow \gamma = 0$ as $c_t \neq 0$

$\therefore \quad \alpha f(x) + \beta g(x) = 0$

and so $\beta b_n = 0 \Rightarrow \beta = 0$ as $b_n \neq 0$

$\Rightarrow \alpha f(x) = 0 \Rightarrow \alpha a_m = 0 \Rightarrow \alpha = 0$ as $a_m \neq 0$

Hence $\{f(x), g(x), h(x)\}$ is *L.I.* in $F[x]$ over F.

Problem 13: *Show that the vectors*

$v_1 = (1, 1, 2, 4)$, $v_2 = (2, -1, -5, 2)$, $v_3 = (1, -1, -4, 0)$ *and* $v_4 = (2, 1, 1, 6)$ *are L.D. in* $\mathbf{R}^4(\mathbf{R})$.

Solution: Suppose $av_1 + bv_2 + cv_3 + dv_4 = 0, \quad a, b, c, d \in \mathbf{R}$

then $a(1, 1, 2, 4) + b(2, -1, -5, 2)$

$+ c(1, -1, -4, 0) + d(2, 1, 1, 6) = (0, 0, 0, 0)$

or $(a, a, 2a, 4a) + (2b, -b, -5b, 2b) + (c, -c, -4c, 0)$

$+ (2d, d, d, 6d) = (0, 0, 0, 0)$

$\Rightarrow a + 2b + c + 2d = 0$

$a - b - c + d = 0$

$2a - 5b - 4c + d = 0$

$4a + 2b + 0c + 6d = 0$

$$\Rightarrow \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & -1 & -1 & 1 \\ 2 & -5 & -4 & 1 \\ 4 & 2 & 0 & 6 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_2 \to R_2 - R_1, \; R_3 \to R_3 - 2R_1, \; R_4 \to R_4 - 4R_1$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to \frac{1}{2}R_4, \; R_3 \to \frac{1}{3}R_3$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -1 & -2/3 & -1/3 \\ 0 & -3/4 & -1 & -1/2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to R_4 - R_2,\ R_3 \to R_3 - R_2$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow a + 2b + c + 2d = 0$

$-3b - 2c + d = 0$

$3b + 2c + d = 0$

$a = -1,\ b = -1,\ c = 1,\ d = 1$ satisfy the equations.

Since coefficients are non zero, the given vectors are *L.D.*

Problem 14: *Show that*

(*i*) $\{1, \sqrt{2}\}$ *is L.I. in* **R** *over* **Q**.

(*ii*) $\{1, \sqrt{2}, \sqrt{3}\}$ *is L.I. in* **R** *over* **Q**.

(*iii*) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *is L.I. in* **R** *over* **Q**.

Solution: (*i*) Suppose $a + b\sqrt{2} = 0,\ a, b \in \mathbf{Q}$

Suppose $b \neq 0$, then $\sqrt{2} = -\frac{a}{b} \in \mathbf{Q}$, a contradiction

Hence $b = 0$ and so $a = 0$. Thus $\{1, \sqrt{2}\}$ is *L.I.* in **R** over **Q**.

(*ii*) Let $a + b\sqrt{2} + c\sqrt{3} = 0,\ a, b, c \in \mathbf{Q}$

Let $c \neq 0$, then

$$\sqrt{3} = -\frac{a}{c} - \frac{b}{c}\sqrt{2} = \alpha + \beta\sqrt{2},\quad \alpha, \beta \in \mathbf{Q}$$

$\Rightarrow 3 = \alpha^2 + 2\beta^2 + 2\alpha\beta\sqrt{2}$

$\Rightarrow \alpha\beta\sqrt{2} \in \mathbf{Q} \Rightarrow \alpha\beta = 0$

Let $\alpha = 0$ then $\beta = \sqrt{\frac{3}{2}}$, a contradiction

So, $c = 0$ giving $a + b\sqrt{2} = 0 \Rightarrow a = b = 0$ by (*i*)

Hence the result follows.

(*iii*) Let $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0,\ a, b, c, d \in \mathbf{Q}$

Then $(a + b\sqrt{2}) + \sqrt{3}(c + d\sqrt{2}) = 0$

Let $c + d\sqrt{2} \neq 0$

Then $\sqrt{3} = \dfrac{-(a+b\sqrt{2})}{(c+d\sqrt{2})} = \dfrac{-(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2}$

$= \alpha + \beta\sqrt{2}, \quad \alpha, \beta \in \mathbf{Q}$

$\Rightarrow \quad \alpha.1 + \beta\sqrt{2} + (-1)\sqrt{3} = 0$

$\Rightarrow \quad -1 = 0$ by (*ii*), a contradiction

$\therefore \quad c + d\sqrt{2} = 0 \Rightarrow c = d = 0 \Rightarrow a + b\sqrt{2} = 0$

$\Rightarrow \quad a = b = 0$

Hence the result follows.

Problem 15: *If two vectors are L.D. then one of them is scalar multiple of the other.*

Solution: Suppose v_1, v_2 are *L.D.* then $\exists\ \alpha_i \in F$, s.t.,

$$\alpha_1 v_1 + \alpha_2 v_2 = 0 \text{ for some } \alpha_i \neq 0$$

without loss of generality we can take $\alpha_1 \neq 0$, then α_1^{-1} exists and $\alpha_1 v_1 = (-\alpha_2 v_2)$

$$\Rightarrow v_1 = (-\alpha_1^{-1}\alpha_2)v_2 = \beta v_2$$

which proves the result.

Problem 16: *If x, y, z are L.I. over the field* **C** *of complex nos. then so are x + y, y + z and z + x over* **C**.

Solution: Suppose $\alpha_1(x+y) + \alpha_2(y+z) + \alpha_3(z+x) = 0$, $\alpha_i \in \mathbf{C}$

Then $$(\alpha_1 + \alpha_3)x + (\alpha_1 + \alpha_2)y + (\alpha_2 + \alpha_3)z = 0$$

$$\Rightarrow \alpha_1 + \alpha_3 = \alpha_1 + \alpha_2 = \alpha_2 + \alpha_3 = 0 \text{ as } x, y, z, \text{ are } L.I.$$

Solving we find

$$\alpha_1 = \alpha_2 = \alpha_3 = 0.$$

Hence the result.

Problem 17: *If* $v_1, v_2, v_3 \in V(F)$ *s.t.,* $v_1 + v_2 + v_3 = 0$ *then show that* $\{v_1, v_2\}$ *spans the same subspace as* $\{v_2, v_3\}$ *i.e., show that*

$$L(\{v_1, v_2\}) = L(\{v_2, v_3\}).$$

Solution: Let $x \in L(\{v_1, v_2\})$ then $x = \alpha v_1 + \beta v_2 \qquad \alpha, \beta \in F$

$$\Rightarrow x = \alpha(-v_2 - v_3) + \beta v_2 \text{ as } v_1 + v_2 + v_3 = 0$$

$$= (\beta - \alpha)v_2 + (-\alpha)v_3 \in L(\{v_2, v_3\})$$

Showing that $L(\{v_1, v_2\}) \subseteq L(\{v_2, v_3\})$

Similarly we can show that $L(\{v_2, v_3\}) \subseteq L(\{v_1, v_2\})$

Hence the result follows.

Note (*i*): Linear dependence depends not only upon the vector space, but the field as well. Consider, for instance, **C**(**C**), **C**(**R**), **C** = complex, **R** = reals.

Take $1, i \in \mathbf{C}$, if $a, \beta \in \mathbf{R}$

then $\alpha \cdot 1 + \beta \cdot i = 0 = 0 + i\,0$

$\Rightarrow \alpha = 0, \beta = 0$

$\Rightarrow 1, i$ are *L.I.* in $\mathbf{C}(\mathbf{R})$

Now if we take α, β in $\mathbf{C}$, then as we can take $\alpha = i$, $\beta = -1$, so that

$i \cdot 1 + (-1)i = 0$, we find $\exists\ \alpha, \beta \neq 0$

s.t., sums of the type $\Sigma\alpha_i v_i = 0$

i.e., $1, i$ are *L.D.* in $\mathbf{C}(\mathbf{C})$

Note (*ii*): In example 20 above, we showed that (1, 0) and (0, 1) are *L.I.* in $\mathbf{R}^2$ $(\mathbf{R})$

if $v = (a, b) \in \mathbf{R}^2$ be *any* element

then since $(a, b) = a(1, 0) + b(0, 1),\ \ a, b \in \mathbf{R}$

We find any element of $\mathbf{R}^2$ can be written as a linear combination of $\{(1, 0), (0, 1)\} = S$

i.e., $v \in \mathbf{R}^2 \Rightarrow v \in L(S)$

$\Rightarrow \mathbf{R}^2 \subseteq L(S)$

But $L(S) \subseteq \mathbf{R}^2$

i.e., $\mathbf{R}^2 = L(S)$

or that S spans $\mathbf{R}^2$.

We generalise this through

Definition: Let $V(F)$ be a vector space. A subset S of V is called a *basis* of V if S consists of *L.I.* elements (*i.e.*, any finite number of elements in S are *L.I.*) and $V = L(S)$, *i.e.*, S spans V.

Thus in example 20, $S = \{(1, 0), (0, 1)\}$ is a basis of $\mathbf{R}^2$ $(\mathbf{R})$. It is rather easy to see then that $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ will form basis of $\mathbf{R}^3$ $(\mathbf{R})$, and one can trivially extend this to $\mathbf{R}^{(n)}$

Again $\{(1, 1, 0), (1, 0, 0), (0, 1, 1)\}$ also forms a basis of $\mathbf{R}^3$ $(\mathbf{R})$. (Show!) Thus a vector space may have more than one basis.

If the elements in a basis are written in a certain specific order, we call it *ordered basis*. Also $\{(1, 0), (0, 1)\}$ $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ etc. are called *standard basis* of $\mathbf{R}^2$, $\mathbf{R}^3$ etc. Also ϕ is a basis for $V = \{0\}$.

Problem 18: *Show that the set* $S = \{(1, 2, 1), (2, 1, 0), (1, -1, 2)\}$ *forms a basis of* $\mathbf{R}^3$ $(\mathbf{R})$.

Solution: Let

$$\alpha_1(1, 2, 1) + \alpha_2(2, 1, 0) + \alpha_3(1, -1, 2) = (0, 0, 0) \quad \alpha_i \in \mathbf{R}$$

$$\Rightarrow (\alpha_1 + 2\alpha_2 + \alpha_3, 2\alpha_1 + \alpha_2 - \alpha_3, \alpha_1 + 0 + 2\alpha_3) = (0, 0, 0)$$

$$\Rightarrow \alpha_1 + 2\alpha_2 + \alpha_3 = 0$$

$$2\alpha_1 + \alpha_2 - \alpha_3 = 0$$

$$\alpha_1 + 0 + 2\alpha_3 = 0$$

In matrix form, we get $\begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

i.e., $AX = O$

where $|A| = -9 \neq 0$.

So A is a non singular matrix and thus $AX = O$ has the unique zero solution $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

Hence S is *L.I.* set.

Again, to show that $L(S) = \mathbf{R}^3$, let $(a, b, c) \in \mathbf{R}^3$ be any element. We want that

$(a, b, c) = \beta_1 (1, 2, 1) + \beta_2 (2, 1, 0) + \beta_3 (1, -1, 2)$ for some $\beta_1, \beta_2, \beta_3 \in \mathbf{R}$

i.e., we want some $\beta_i \in \mathbf{R}$ s.t., the equations

$$\beta_1 + 2\beta_2 + \beta_3 = a$$
$$2\beta_1 + \beta_2 - \beta_3 = b$$
$$\beta_1 + 0\beta_2 + 2\beta_2 = c$$

are satisfied. *i.e.*, in matrix form

$$AX = B \text{ where } A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 1 & 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Since $|A| = -9 \neq 0$, $AX = B$ has a unique solution *i.e.*, $\exists$ some β_i s.t., above equations are satisfied or that it is possible to express any $(a, b, c) \in \mathbf{R}^3$ as a linear combination of members of S. *i.e.*, $L(S) = \mathbf{R}^3$

Hence S forms a basis of $\mathbf{R}^3(\mathbf{R})$.

The next few theorems give a concrete shape to the concept of a basis of a vector space.

Theorem 16: *If $S = \{v_1, v_2, \ldots v_n\}$ is a basis of V, then every element of V can be expressed uniquely as a linear combination of $v_1, v_2, \ldots, v_n$.*

Proof: Since, by definition of basis, $V = L(S)$, each element $v \in V$ can be expressed as linear combination of $v_1, v_2, \ldots, v_n$.

Suppose $v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \quad \alpha_i \in F$

$v = \beta_1 v_1 + \beta_2 v_2 + \ldots + \beta_n v_n, \quad \beta_i \in F$

then $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = \beta_1 v_2 + \beta_2 v_2 + \ldots + \beta_n v_n$

$\Rightarrow (\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \ldots + (\alpha_n - \beta_n) v_n = 0$

$\Rightarrow \alpha_i - \beta_i = 0$ for all i ($v_1, v_2, \ldots v_n$ are *L.I.*)

$\Rightarrow \alpha_i = \beta_i$ for all i.

Theorem 17: *Suppose S is a finite subset of a vector space V such that $V = L(S)$ [i.e., V is a F.D.V.S.] then there exists a subset of S which is a basis of V.*

Proof: If S consists of *L.I.* elements then S itself forms basis of V and we've nothing to prove.

Let now T be a subset of S, such that T spans V and T is such minimal subset of S. (Existence of T is ensured as S is finite).

Suppose $T = \{v_1, v_2, \ldots, v_n\}$

we show T is *L.I.*

Let $\Sigma\alpha_i v_i = 0, \quad \alpha_i \in F$

Suppose $\alpha_i \neq 0$ for some i. Without any loss of generality we can take $\alpha_1 \neq 0$. Then α_1^{-1} exists.

Now $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$

$\Rightarrow \alpha_1^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n) = 0$

$\Rightarrow v_1 = (-\alpha_1^{-1}\alpha_2)v_2 + (-\alpha_1^{-1}\alpha_3)v_3 + \ldots + (-\alpha_1^{-1}\alpha_n)v_n$

$= \beta_2 v_2 + \beta_3 v_3 + \ldots + \beta_n v_n \quad \beta_i \in F$

If $v \in V$ be any element then

$v = \gamma_1 v_1 + \gamma_2 v_2 + \ldots \gamma_n v_n \quad \gamma_i \in F$ as $V = L(T)$

$\Rightarrow v = \gamma_1(\beta_2 v_2 + \ldots + \beta_n v_n) + \gamma_2 v_2 + \ldots + \gamma_n v_n$

i.e., any element of V is a linear combination of $v_2, v_3, \ldots, v_n$

$\Rightarrow \{v_2, v_3, \ldots v_n\}$ spans V, which contradicts our choice of T (as T was such minimal)

Hence $\alpha_1 = 0$

or that $\alpha_i = 0$ for all i

$\Rightarrow v_1, v_2, \ldots v_n$ are *L.I.*

and thus T is a basis of V.

Cor : A *F.D.V.S.* has a basis.

In fact, one can prove this result for any vector space. (i.e. any vector space has a basis)

Theorem 18: *Let V be a F.D.V.S. Suppose S and T are two finite subsets of V such that S spans V and T is L.I. Then* $o(T) \leq o(S)$.

Proof: Suppose $S = \{v_1, v_2, \ldots, v_n\}$

$T = \{w_1, w_2, \ldots, w_m\}$

Suppose $m > n$.

Since S spans V, we have

$$w_1 = a_{11} v_1 + a_{12} v_2 + \ldots + a_{1n} v_n$$
$$w_2 = a_{21} v_1 + a_{22} v_2 + \ldots + a_{2n} v_n$$
$$\ldots \qquad \ldots \qquad \ldots$$
$$w_m = a_{m1} v_1 + a_{m2} v_2 + \ldots + a_{mn} v_n \qquad \text{where } a_{ij} \in F$$

Consider the system of equations

$$a_{11} x_1 + a_{21} x_2 + \ldots + a_{m1} x_m = 0$$
$$a_{12} x_1 + a_{22} x_2 + \ldots + a_{m2} x_m = 0$$
$$\ldots \qquad \ldots \qquad \ldots$$
$$a_{1n} x_1 + a_{2n} x_2 + \ldots + a_{mn} x_m = 0$$

where $x_1, x_2, \ldots, x_m \in F$ are unknowns.

Since the number of equations is less than the number of unknowns, $\exists$ a non zero solution $\alpha_1, \alpha_2, \ldots, \alpha_m$ (some $\alpha_i \neq 0$) in F s.t.,

$$a_{11}\,\alpha_1 + \ldots + a_{m1}\,\alpha_m = 0$$
$$\ldots \qquad \ldots \qquad \ldots$$
$$a_{1n}\,\alpha_1 + \ldots + a_{mn}\,\alpha_m = 0$$

Thus $\alpha_1 (a_{11} v_1 + \ldots + a_{1n} v_n) + \ldots + \alpha_m (a_{m1} v_1 + \ldots + a_{mn} v_n) = 0$

$\Rightarrow \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_m w_m = 0$

$\Rightarrow \alpha_i = 0 \ \forall i$ as $w_1, w_2, \ldots, w_m$ are *L.I.*

which is a contradiction and thus $m \leq n$

i.e., $o(T) \leq o(S)$.

Cor. 1: Any basis of a *F.D.V.S.* is finite.

Proof: Let S be a basis of a *F.D.V.S* V and suppose S is not finite.

Since V is finite dimensional, $\exists$ a finite subset T of V s.t., $V = L(T)$. Suppose $o(T) = m$

Let S_1 be a *L.I.* subset of S s.t., $o(S_1) = m + 1$

By above theorem then $o(T) \geq o(S_1)$ giving $m \geq m + 1$, a contradiction.

Hence S must be finite.

Cor. 2: Any two bases of a *F.D.V.S.* have same number of elements.

Proof: Let S and T be two bases of a *F.D.V.S.* V

By above cor., S and T are finite and by the theorem $o(T) \leq o(S)$ and $o(S) \leq o(T)$

Hence $o(T) = o(S)$.

With the result of cor.2 in our mind we make

Definition: A *F.D.V.S.* V is said to have dimension n if n is the number of elements in any basis of V.

We use the notation $\dim_F V = n$ or simply $\dim V = n$ and say V is n-dimensional vector space.

In view of an example done earlier

$\dim \mathbf{R}^2 = 2$. In fact $\dim \mathbf{R}^n = n$

Cor. 3: If $\dim V = n$, then any $n + 1$ vectors in V are linearly dependent.

Proof: Let $T \subseteq V$ be a *L.I.* set s.t., $o(T) = n + 1$

Let S be a basis of V. Then S spans V and $o(S) = n$.

By theorem, 18. $o(T) \leq o(S)$

giving $n + 1 \leq n$ a contradiction

Thus any $n + 1$ vectors in V are *L.D.*

Theorem 19: *A basis of a vector space is maximal linearly independent set and conversely, every maximal linearly independent set in a vector space is its basis.*

Proof: Let S be a basis of a vector space V, then S is linearly independent set in V. Let T be a linearly independent set in V such that $S \subseteq T$. If $S \neq T$ then $\exists$ some $t \in T$ s.t., $t \notin S$.

Now $t \in T \Rightarrow t \in V \Rightarrow t = \alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n$, $\alpha_i \in F$, $s_i \in S$ as S spans V

$\Rightarrow (-1)\, t + \alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n = 0$, where $t \neq s_i$ for any i

$\Rightarrow -1 = 0$

as $\{t, s_1, s_2, ..., s_n\} \subseteq T$ is a linearly independent set. So we get a contradiction.

Hence S is a maximal linearly independent set.

Conversely, let $S \subseteq V$ be a maximal linearly independent set. Let $v \in V$, and suppose $v \notin L(S)$

Then $S \subset S \cup \{v\}$ as $v \notin L(S) \Rightarrow v \notin S$

and so $S \cup \{v\}$ is a *L.D.* set and thus $\exists$ a finite subset of $S \cup \{v\}$ which is a *L.D.* set.

i.e., $\exists\ s_1, s_2, ... s_n \in S$ s.t., $\{v, s_1, s_2, ..., s_n\}$ is a *L.D.* set.

i.e., $\alpha v + \alpha_1 s_1 + ... + \alpha_n s_n = 0$, $\alpha \in F$, $\alpha_i \in F$

where α or some α_i is not zero.

If $\alpha = 0$ then $\alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n = 0$

$\Rightarrow \alpha_i = 0\ \forall\ i$.

Thus $\alpha \neq 0$

So $v = (-\alpha^{-1}\alpha_1)s_1 + ... + (-\alpha^{-1}\alpha_n)\, s_n$

$\Rightarrow v \in L(S)$, (a contradiction)

Thus $V = L(S)$ and so S is a basis of V**.**

Cor.: Suppose n is the maximum number of *L.I.* vectors in any subset of a vector space V. Then dim $V = n$.

Proof: Let S be a *L.I.* subset of V such that $o(S) = n$

Then S is a maximal *L.I.* set in V. By above theorem then S is a basis of V. Hence dim $V = o(S) = n$.

Theorem 20: *Let $V(F)$ be a vector space. A minimal generating set of V is a basis of V and conversely, every basis of V is a minimal generating set of V.*

Proof: Let S be a minimal generating set of V

Then $V = L(S)$ and no proper subset of S generates V. We show S is *L.I.* set. Suppose it is not, then there exists a finite subset S_1, of S such that S_1 is not *L.I.* Thus $\exists\ s \in S_1$ s.t., s is linear combination of elements of S_1, and so of S.

Let $T = S - \{s\}$

then $V = L(T)$ and $T \subsetneq S$, a contradiction as S is minimal generating set of V.

Hence S is a basis of V.

Conversely, let B be a basis of V. We show no proper subset of B generates V. Let $B' \subsetneq B$ and $V = L(B')$. Then $\exists\ b \in B$, s.t., $b \notin B'$

Now $b \in B \Rightarrow b \in V = L(B') \Rightarrow b = \sum_1^n \alpha_i b_i'$, $b_i' \in B'$

$\Rightarrow 0 = (-1)\, b + \sum_1^n \alpha_i b'_i$, $b \neq b'_i$ for any i

$\Rightarrow -1 = 0$ as $\{b, b'_1,..., b'_n\} \subseteq B$ is a *L.I.* set, a contradiction.

Thus B is minimal generating set of V.

Theorem 21: *If V is a F.D.V.S. and $\{v_1, v_2,..., v_r\}$ is a L.I. subset of V, then it can be extended to form a basis of V.*

Proof: If $\{v_1, v_2,... v_r\}$ spans V, then it itself forms a basis of V and there is nothing to prove.

Let $S = \{v_1, v_2,... v_r, v_{r+1},... v_n\}$ be the maximal *L.I.* subset of V, containing $\{v_1, v_2, ..., v_r\}$.

We show S is a basis of V, for which it is enough to prove that S spans V. Let $v \in V$ be any element

then $T = \{v_1, v_2,...v_n, v\}$ is *L.D.* by choice of S

$\Rightarrow \exists\ \alpha_1, \alpha_2,..., \alpha_n, \alpha \in F$ (not all zero) such that

$$\alpha_1 v_1 + ... + \alpha_n v_n + \alpha v = 0$$

We claim $\alpha \neq 0$. Suppose $\alpha = 0$

then $\alpha_1 v_1 + ... + \alpha_n v_n = 0$

$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2,..., v_n$ are *L.I.*

$\therefore \alpha = \alpha_i = 0$ for all i which is not true.

Hence $\alpha \neq 0$ and so α^{-1} exists.

Since $v = (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + ... + (-\alpha^{-1}\alpha_n)v_n$

v is a linear combination of $v_1, v_2,..., v_n$

which proves our assertion.

Aliter: Let dim $V = n$ and $S = \{v_1, v_2,..., v_r\}$. If S is maximal *L.I.* set in V then by theorem 19, it is a basis of V. If S is not maximal *L.I.* set in V then $\exists$ a set $T \supsetneq S$ such that T is *L.I.* set in V. Since a *L.I.* set cannot have more than n vectors, after finite number of steps, there would be a maximal *L.I.* set $B \supseteq S$ in V. By theorem 19, B would be a basis of V. Hence S can be extended to form a basis B of V.

Remark: This result can be proved even if the vector space is not finite dimensional.

Theorem 22: *If dim $V = n$ and $S = \{v_1, v_2,..., v_n\}$ spans V then S is a basis of V.*

Proof: Since dim $V = n$, any basis of V has n elements. By theorem 17, a subset of S will be a basis of V but as S contains n elements, it will itself form basis of V.

Theorem 23: *If dim $V = n$ and $S = \{v_1, v_2,...,v_n\}$ is L.I. subset of V then S is a basis of V.*

Proof: Since $\{v_1, v_2,..., v_n\} = S$ is *L.I.* it can be extended to form a basis of V, but dim V being n it will itself be a basis of V.

Aliter: Let $v \in V$, then

$v, v_1, v_2,..., v_n$ will be *L.D.* by cor. 3 on page 503. Thus $\exists\ \alpha, \alpha_1, \alpha_2,..., \alpha_n \in F$ s.t.,

$$\alpha v + \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$$

where some α_i or α is not zero.

If $\alpha = 0$, then

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$$
$$\Rightarrow \alpha_i = 0 \ \forall i \text{ as } v_1, v_2 \ldots, v_n \text{ are } L.I.$$

Thus $\alpha \neq 0$ and so

$$v = (-\alpha^{-1}\alpha_1)v_1 + \ldots\ldots + (-\alpha^{-1}\alpha_n)v_n \in L(S)$$
$$\Rightarrow V \subseteq L(S)$$
$$\Rightarrow V = L(S) \text{ and as } S \text{ is } L.I., S \text{ is a basis of } V.$$

Remark: In view of these theorems the proof of problem 18 on page 500 can be shortened as we know dim $\mathbf{R}^3 = 3$.

Problem 19: *If* $\{v_1, v_2, \ldots, v_n\}$ *is a basis of F.D.V.S.* V *of dim* n *and* $v = \Sigma\alpha_i v_i$, $\alpha_r \neq 0$ *then prove that* $\{v_1, v_2, \ldots, v_{r-1}, v, v_{r+1} \ldots, v_n\}$ *is also a basis of* V.

Solution: We have

$$v = \alpha_1 v_1 + \ldots + \alpha_r v_r + \ldots + \alpha_n v_n \quad \alpha_r \neq 0, \ \therefore \alpha_r^{-1} \text{ exists}$$
$$\Rightarrow v_r = (-\alpha_r^{-1}\alpha_1)\, v_1 + \ldots + (-\alpha_r^{-1}\, \alpha_{r-1})\, v_{r-1} + \alpha_r^{-1} v + \ldots + (-\alpha_r^{-1}\alpha_n)v_n$$
$$= \beta_1 v_1 + \ldots + \beta_{r-1} v_{r-1} + \beta_r v + \beta_{r+1}\, v_{r+1} + \ldots + \beta_n v_n.$$

If $x \in V$ be any element, then

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n \quad \alpha_i \in F$$
$$\Rightarrow x = a_1 v_1 + \ldots + a_{r-1} v_{r-1} + a_r(\beta_1 v_1 + \ldots + \beta_n v_n) + \ldots + a_n v_n$$

or that x is a linear combination of

$$v_1, \ldots, v_{r-1}, v, v_{r+1}, \ldots, v_n$$

and x being any element, we find V is spanned by $\{v_1, \ldots, v_{r-1}, v, v_{r+1}, \ldots v_n\}$ and it forms a basis of V, using theorem done above.

Theorem 24: *Two finite dimensional vector spaces over F are isomorphic iff they have the same dimension.*

Proof: Let V and W be two isomorphic vector spaces over F and let $\theta : V \to W$ be the isomorphism.

Let dim $V = n$ and $\{v_1, v_2, .., v_n\}$ be a basis of V.

We claim $\{\theta(v_1), \theta(v_2), \ldots, \theta(v_n)\}$ is a basis of W.

Now $\sum_{i=1}^{n} \alpha_i \ \theta(v_i) = 0 \quad \alpha_i \in F,$

$$\Rightarrow \sum \theta(\alpha_i v_i) = 0 = \theta(0)$$
$$\Rightarrow \sum \alpha_i v_i = 0 \quad (\theta \text{ is } 1\text{–}1)$$
$$\Rightarrow \alpha_i = 0 \text{ for all } i \text{ as } v_1, v_2, \ldots, v_n \text{ are } L.I.$$
$$\Rightarrow \theta(v_1), \theta(v_2), \ldots, \theta(v_n) \text{ are } L.I.$$

Again, if $w \in W$ is any element, then as θ is onto, $\exists$ some $v \in V$ s.t., $\theta(v) = w$

Now $v \in V \Rightarrow v = \sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$

$$\Rightarrow w = \theta(v) = \theta\left(\sum \alpha_i v_i\right)$$

$$\Rightarrow w = \sum \theta(\alpha_i v_i) = \alpha_1\theta(v_1) + \alpha_1\theta(v_2) + \ldots + \alpha_n\theta(v_n)$$

or that w is a linear combination of $\theta(v_1)$, $\theta(v_2)$, ..., $\theta(v_n)$

Hence $\theta(v_1)$, $\theta(v_2)$,..., $\theta(v_n)$ span W and therefore, form a basis of W showing that dim $W = n$.

Conversely, let dim V = dim $W = n$ and suppose. $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$ are basis of V and W respectively.

Define a map $\theta : V \to W$ s.t.,

$$\theta(v) = \theta(\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n)$$
$$= \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_n w_n$$

then θ is easily seen to be well defined. (Indeed any $v \in V$ is unique linear combination of members of basis).

If $v, v' \in V$ be any elements then

$$v = \sum \alpha_i v_i,\ v' = \sum \beta_i v_i \quad \alpha_i, \beta_i \in F$$

$$\theta(v + v') = \theta\left(\sum \alpha_i v_i + \sum \beta_i v_i\right)$$
$$= \theta\left(\sum (\alpha_i + \beta_i) v_i\right)$$
$$= \sum (\alpha_i + \beta_i) w_i$$
$$= \sum \alpha_i w_i + \sum \beta_i w_i = \theta(v) + \theta(v')$$

Also $\theta(\alpha v) = \theta\left(\alpha \sum \alpha_i v_i\right) = \theta\left(\sum \alpha\alpha_i v_i\right) = \sum (\alpha\alpha_i) w_i$

$$= \alpha \sum \alpha_i w_i = \alpha\theta(v)$$

Thus θ is a homomorphism.

Now if $v \in$ Ker θ

then $\theta(v) = 0$

$$\Rightarrow \theta\left(\sum \alpha_i v_i\right) = 0$$

$$\Rightarrow \sum \alpha_i w_i = 0$$

$\Rightarrow \alpha_i = 0$ for all i $w_1, w_2, \ldots, w_n$ being *L.I.*

$\Rightarrow v = 0$

$\Rightarrow$ Ker $\theta = \{0\}$

$\Rightarrow \theta$ is one–one.

That θ is onto is obvious. Hence θ is an isomorphism.

Cor.: Under an isomorphism, a basis is mapped onto a basis.

Follows by first part of the theorem.

Problem 20: *Show that the set of all real valued continuous functions $y = f(x)$ satisfying the differential equation* $\frac{d^3y}{dx^3} + 6\frac{d^2y}{dx^2} + 11\frac{dy}{dx} + 6y = 0$ *is a vector space over* **R**. *Find a basis of this.*

Solution: One can check that $V = \{f \mid f : \mathbf{R} \to \mathbf{R}, f \text{ cont.}\}$ is a vector space over **R**, under

$$(f + g)x = f(x) + g(x)$$
$$(\alpha f)x = \alpha(f(x))$$

Let $W = \{f \in V \mid f$ is a solution of given differential equation$\}$

The given differential equation is

$$(D^3 + 6D^2 + 11D + 6)\, y = 0$$
$$(D + 1)\,(D + 2)\,(D + 3)\, y = 0$$
$$\Rightarrow \quad D = -1, -2, -3$$

and the general solution is

$$y = Ae^{-x} + be^{-2x} + Ce^{-3x}$$

If $S = \{e^{-x}, e^{-2x}, e^{-3x}\}$ then clearly S spans W

Let $Ae^{-x} + Be^{-2x} + Ce^{-3x} = 0$

Then $-Ae^{-x} + (-2)\, Be^{-2x} + (-3C)\, e^{-3x} = 0$

$$Ae^{-x} + (4B)\, e^{-2x} + (9C)\, e^{-3x} = 0 \quad \forall\, x$$

Put $x = 0$

$$\begin{bmatrix} 1 & 1 & 1 \\ -1 & -2 & -3 \\ 1 & 4 & 9 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0 \quad \Rightarrow M \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0$$

where $\det M = 1(-18 + 12) - 1\,(-9 + 3) + 1\,(-4 + 2) = -2 \neq 0$

thus M^{-1} exists and so $A = B = C = 0$

$\Rightarrow S$ is *L.I.* and hence a basis of W.

Note: W is a vector space as it is a subspace of V. [$y_1, y_2 \in W \Rightarrow \alpha_1 y_1 + \alpha_2 y_2$ is a solution of the given differential equation $\Rightarrow \alpha_1 y_1 + \alpha_2 y_2 \in W$].

Problem 21: *If $S = \{v_1, v_2, \ldots, v_r\}$ is a L.I. subset of V and $v \in V$ be such that $v \notin L(S)$, then show that $S \cup \{v\}$ is a L.I. subset of V.*

Solution: $S \cup \{v\} = \{v_1, v_2, \ldots, v_r, v\}$

Let $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_r v_r + \alpha v = 0 \quad \alpha_i \in F, \alpha \in F$

If $\alpha \neq 0$ then α^{-1} exists and we get

$$\alpha^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_r v_r + \alpha v) = 0$$
$$\Rightarrow v = (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + \ldots + (\alpha^{-1}\alpha_r)v_r$$
$$\Rightarrow v \in L(S), \text{ a contradiction}$$

thus $\alpha = 0$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_r v_r = 0$

$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2, \ldots, v_r$ are *L.I.*

$\Rightarrow \alpha = \alpha_i = 0$ for all i

$\Rightarrow v_1, v_2, \ldots, v_r, v$ are *L.I.*

Hence the result follows.

Problem 22: (1, 1, 1) *is L.I. vector in* $\mathbf{R}^3(\mathbf{R})$ *Extend it to form a basis of* $\mathbf{R}^3$.

Solution: (1, 1, 1) is non zero vector and is therefore *L.I.* in $\mathbf{R}^3$.

Let $S = \{(1, 1, 1)\}$, then $L(S) = \{\alpha(1, 1, 1) \mid \alpha \in \mathbf{R}\}$

Now $(1, 0, 0) \in \mathbf{R}^3$, but $(1, 0, 0) \notin L(S)$

thus by above problem $S_1 = \{(1, 1, 1), (1, 0, 0)\}$ is *L.I.*

Now $L(S_1) = \{\alpha(1, 1, 1) + \beta(1, 0, 0) \mid \alpha, \beta \in \mathbf{R}\}$

$= \{(\alpha + \beta, \alpha, \alpha) \mid \alpha, \beta \in \mathbf{R}\}$

Again $(0, 1, 0) \notin L(S_1)$ and by above problem

$S_2 = \{(1, 1, 1), (1, 0, 0), (0, 1, 0)\}$ is *L.I.* subset of $\mathbf{R}^3$.

Since dim $\mathbf{R}^3 = 3$, we find S_2 will be a basis of $\mathbf{R}^3$.

Problem 23: *A finite set of non zero vectors* $\{v_1, v_2, \ldots, v_n\}$ *in a vector space* $V(F)$ *is L.D. iff* $\exists\ v_k$, $2 \le k \le n$, *s.t.,* v_k *is a linear combination of* $v_1, v_2, \ldots, v_{k-1}$.

Solution: Let $v_1, v_2, \ldots, v_n$ be *L.D.* Then $\exists\ \alpha_i \in F$, not all zero s.t., $\sum_{i=1}^{n} \alpha_i v_i = 0$.

Let k be the largest integer s.t., $\alpha_k \neq 0$ and $\alpha_i = 0\ \forall\ i > k$.

then $k \neq 1$ as if $k = 1$,

then $\alpha_1 v_1 = 0$, $\alpha_1 \neq 0$ ($\alpha_i = 0$ for all $i \ge 2$)

$\Rightarrow v_1 = 0$, not true as v_i are non zero

Hence $2 \le k \le n$

Thus $\alpha_k \neq 0$ and $\alpha_i = 0$ for all $i \ge k + 1$. Also then α_k^{-1} exists

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k = 0$

$\Rightarrow \alpha_k^{-1} (\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k) = 0$

$\Rightarrow v_k = (-\alpha_k^{-1}\alpha_1)v_1 + (-\alpha_k^{-1}\alpha_2)\ v_2 + \ldots + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$

which proves the result.

Conversely, suppose $\exists\ k$, $2 \le k \le n$ s.t., v_k is a linear combination of $v_1, v_2, \ldots, v_{k-1}$

Let $v_k = a_1 v_1 + a_2 v_2 + \cdots + a_{k-1} v_{k-1} \quad a_i \in F$

Then $a_1 v_1 + a_2 v_2 + \cdots + a_{k-1} v_{k-1} - 1.\ v_k = 0$

$\Rightarrow v_1, v_2, \ldots, v_k$ are *L.D.* as $(-1) \neq 0$

$\Rightarrow v_1, v_2, \ldots, v_k, v_{k+1}, \ldots, v_n$ are *L.D.*

as any super set of a *L.D.* set is *L.D.*

Hence the result follows.

Remark: If $v_1, v_2, ..., v_n$ be in V then either these are *L.I.* or some v_k is a linear combination of the preceeding ones $v_1, v_2, ..., v_{k-1}$.

All this time we've been talking about basis of a *F.D.V.S. V.* What about a subspace of V. Would it also be finite dimensional? The answer is a natural yes. We formalise it through

Theorem 25: *Let W be a subspace of a F.D.V.S. V, then W is finite dimensional and dim $W \leq$ dim V. In fact, dim V = dim W iff $V = W$.*

Proof: Let dim $V = n$, then n is the maximum number of *L.I.* elements in any subset of V. Since any subset of W will be a subset of V, n is the maximum number of *L.I.* elements in W.

Let $w_1, w_2, ..., w_m$ be the maximum number of *L.I.* elements in W then $m \leq n$.

We show $\{w_1, w_2, ..., w_m\}$ is a basis of W. These are already *L.I.* If $w \in W$ be any element then the set $\{w_1, w_2, ..., w_m, w\}$ is *L.D.*

$\Rightarrow \exists\ \alpha_1, \alpha_2, ..., \alpha_m, \alpha$ in F (not all zero) s.t.,

$\alpha_1 w_1 + ... + \alpha_m w_m + \alpha w = 0$.

If $\alpha = 0$, we get $\alpha_i = 0$ for all i as $w_1, ..., w_m$ are *L.I.* which is not true. Thus $\alpha \neq 0$ and so α^{-1} exists.

The above equation then gives us

$$w = (-\alpha^{-1}\alpha_1)w_1 + ... + (-\alpha^{-1}\ \alpha_m)\ w_m$$

Showing that $\{w_1, w_2, ..., w_m\}$ spans W (and thus W is finite dimensional)

$\Rightarrow$ $\{w_1, w_2, ..., w_m\}$ is a basis of W

$\Rightarrow$ dim $W = m \leq n =$ dim V

Finally, if dim V = dim $W = n$

and $\{w_1, w_2, ..., w_n\}$ be a basis of W then as $\{w_1, w_2, ..., w_n\}$ is *L.I.* in W it will be *L.I.* in V. and as dim $V = n$, $\{w_1, w_2, ..., w_n\}$ is a basis of V.

Now if $v \in V$ be any element then

$$v = \alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_n w_n \in W$$

$\Rightarrow V \subseteq W \Rightarrow V = W$.

Conversely, of course, $V = W \Rightarrow$ dim V = dim W.

Remarks:

(*i*) If W is a subspace of V where $W = (0)$ then dimension of W is taken to be zero.

(*ii*) $\mathbf{C}$ ($\mathbf{Q}$) is not finite dimensional as if it is then its subspace $\mathbf{R}(\mathbf{Q})$ will also be finite dimensional, which is not true, as suppose dim $\mathbf{R}(\mathbf{Q}) = n$. Let $x_1, x_2, ..., x_n$ be a basis of $\mathbf{R}(\mathbf{Q})$, then

$$\mathbf{R} = \{\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n \mid \alpha_i \in \mathbf{Q}\}$$

Since $\mathbf{Q}$ is a countable set, each α_i has countable choices. So $\mathbf{R}$ should be countable, which is not true. Hence dim $\mathbf{R}(\mathbf{Q})$ is not finite.

Aliter: Suppose $[\mathbf{R}: \mathbf{Q}] = n$ and let $f(x) = x^{n+1} - 2 \in \mathbf{Q}[x]$. Then $f(x)$ is irreducible

over **Q**. Let $\alpha = \sqrt[n+1]{2}$ be a real root of $f(x)$, then $[\mathbf{Q}(\alpha): \mathbf{Q}] = \deg f(x) = n + 1$. Also $\mathbf{Q}(\alpha)/\mathbf{Q}$ is a subspace of $\mathbf{R}/\mathbf{Q}$. But dimension of $\mathbf{Q}(\alpha)/\mathbf{Q}$ is $n + 1$ which is more than the dimension n of $\mathbf{R}/\mathbf{Q}$, a contradiction. So $\mathbf{R}/\mathbf{Q}$ is not finite dimensional.

(*iii*) The result of theorem may not hold if V is not finite dimensional. Consider $V = F[x]$ and take $W = F[x^2]$, then W is a subspace of V, $W \neq V$ as $x \in V, x \notin W$. Here $S = \{1, x, x^2,..., x^n,...\}$ is a basis of V and $T = \{1, x^2,..., x^{2n},...\}$ is a basis of W. The map $\theta : S \to T$, s.t., $\theta(x^i) = x^{2i}$ is 1–1 onto and thus S & T have same cardinality $\Rightarrow$ dim V = dim W.

Theorem 26: *Let W be a subspace of a F.D.V.S. V. Then*

$$dim\ \frac{V}{W} = dim\ V - dim\ W.$$

Proof: Let dim $W = m$ and let $\{w_1, w_2, ..., w_m\}$ be a basis of W.

$w_1, w_2,..., w_m$ being *L.I.* in W will be *L.I.* in V and thus $\{w_1, w_2,..., w_m\}$ can be extended to form a basis of V.

Let $\{w_1, w_2,..., w_m, v_1, v_2,..., v_n\}$ be this extended basis of V.

then dim $V = n + m$

Consider the set $S = \{W + v_1, W + v_2,..., W + v_n\}$, we show it forms a basis of $\frac{V}{W}$.

Let $\alpha_1(W + v_1) + ... + \alpha_n(W + v_n) = W, \quad \alpha_i \in F$

Then $W + (\alpha_1 v_1 + ... + \alpha_n v_n) = W$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n \in W$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n$ is a linear combination of $w_1,..., w_m$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = \beta_1 w_1 + ... + \beta_m w_m \quad \beta_j \in F$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n - \beta_1 w_1 - ..... - \beta_m w_m = 0$

$\Rightarrow \alpha_i = \beta_j = 0$ for all i, j.

$\Rightarrow \{W + v_1, W + v_2,....., W + v_n\}$ is *L.I.*

Again, for any $W + v \in \frac{V}{W}$, $v \in V$ means v is a linear combination of $w_1,..., w_m, v_1,..., v_n$.

i.e., $v = \alpha_1 w_1 + ... + \alpha_m w_m + \beta_1 v_1 + ... + \beta_n v_n \quad \alpha_i, \beta_j \in F$

giving $W + v = W + (\alpha_1 w_1 + \cdots + \alpha_m w_m) + (\beta_1 v_1 + \cdots + \beta_n v_n)$

$= W + (\beta_1 v_1 + \cdots + \beta_n v_n)$

$= (W + \beta_1 v_1) + \cdots + (W + \beta_n v_n)$

$= \beta_1(W + v_1) + \beta_2(W + v_2) + \cdots + \beta_n(W + v_n).$

Hence S spans $\frac{V}{W}$ and is therefore a basis.

$\therefore$ dim $\frac{V}{W} = n$

Thus $\dim \frac{V}{W} = \dim V - \dim W$.

Remark: Thus we notice that if V is a *F.D.V.S.* then so is $\frac{V}{W}$. Converse of this may not be true. Consider

$$V = F[x], \quad W = \{x^2 f(x) \mid f(x) \in V\}$$

Then W is a subspace of V and

$\frac{V}{W} = \{W + a_0 + a_1 x \mid a_i \in F\}$ which

is spanned by $\{W + 1, W + x\}$ and thus $\frac{V}{W}$ is finite dimensional, whereas V is not.

Theorem 27: *If A and B are two subspaces of a F.D.V.S. V then*

$$dim\ (A + B) = dim\ A + dim\ B - dim\ (A \cap B).$$

Proof: We've already proved that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

$$\therefore \quad \dim \frac{A+B}{A} = \dim \frac{B}{A \cap B}$$

$$\Rightarrow \dim (A + B) - \dim A = \dim B - \dim (A \cap B)$$

or that $\dim (A + B) = \dim A + \dim B - \dim (A \cap B)$.

Remark: The reader should try to give an independent proof of the above theorem as an exercise.

Cor.: If $A \cap B = (0)$ then $\dim (A + B) = \dim A + \dim B$

i.e., $\dim (A \oplus B) = \dim A + \dim B$.

Problem 24: *Let W_1, W_2, W_3 be subspaces of a F.D.V.S. Show that*

$$dim\ (W_1 + W_2 + W_3) \leq \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_1 \cap W_2) - \dim (W_1 \cap W_3) - \dim (W_2 \cap W_3) + \dim (W_1 \cap W_2 \cap W_3).$$

Solution: We have

$$\begin{aligned}\dim (W_1 + W_2 + W_3) &= \dim W_1 + \dim (W_2 + W_3) - \dim (W_1 \cap (W_2 + W_3)) \\ &= \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_2 \cap W_3) \\ &\qquad - \dim (W_1 \cap (W_2 + W_3)) \\ &\leq \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_2 \cap W_3) \\ &\quad - \dim (W_1 \cap W_2) - \dim (W_1 \cap W_3) + \dim (W_1 \cap W_2 \cap W_3)\end{aligned}$$

as $(W_1 \cap W_2) + (W_1 \cap W_3) \subseteq W_1 \cap (W_2 + W_3)$.

Problem 25: *Let P_n be the vector space of all polynomials of degree $\leq n$ over* **R**. *Exhibit a basis of P_4/P_2. Hence verify that dim $\frac{P_4}{P_2}$ = dim P_4 – dim P_2.*

Solution: It is easy to see that $\{1, x, x^2, x^3, x^4\}$ is a basis of P_4 and thus dim $P_4 = 5$. Similarly dim $P_2 = 3$ as $\{1, x, x^2\}$ will be a basis of P_2.

Let $S = \{P_2 + x^3, P_2 + x^4\}$ then S is a basis of $\frac{P_4}{P_2}$ as

$$P_2 + f \in \frac{P_4}{P_2} \Rightarrow P_2 + \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \alpha_4 x^4 = P_2 + f$$

$$\Rightarrow P_2 + f = \alpha_3(P_2 + x^3) + \alpha_4(P_2 + x^4)$$

$$\Rightarrow S \text{ spans } \frac{P_4}{P_2}.$$

Again, $\alpha(P_2 + x^3) + \beta(P_2 + x^4) = \text{zero} = P_2$

$$\Rightarrow P_2 + \alpha x^3 + \beta x^4 = P_2$$

$$\Rightarrow \alpha x^3 + \beta x^4 = a + bx + cx^2 \in P_2$$

$\Rightarrow a = b = c = \alpha = \beta = 0$ as polynomial is zero, if each coefficient is zero.

Thus S is a basis of $\frac{P_4}{P_2}$.

Hence $\dim \frac{P_4}{P_2} = 2 = 5 - 3 = \dim P_4 - \dim P_2$.

Problem 26: *Let $V = M_2(\mathbf{R})$ and let $W = \{A \in V | A = A'\}$ be a subspace of V. Find a basis of W.*

Solution: Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be in W, then

$$A = a_{11} E_{11} + a_{12} E_{12} + a_{12} E_{21} + a_{22} E_{22}$$

where $E_{ij} = (a_{ij})$ s.t., $a_{ij} = 1$ and 0 elsewhere

Thus $A = a_{11} E_{11} + a_{12} (E_{12} + E_{21}) + a_{22} E_{22}$

$\therefore$ $S = \{E_{11}, E_{12} + E_{21}, E_{22}\} \subseteq W$ spans W

Also S is *L.I.* and hence forms a basis of W and dim $W = o(S) = 3$.

Problem 27: *Let $V = \mathbf{R}^{(n)}$, then $W = \{(x_1, x_2,..., x_n) \mid \sum_1^n x_i = 0\}$ is a subspace of V. Find a basis for* W.

Solution: Let $(x_1, x_2,..., x_n) \in W$, then $x_1 + x_2 +...+ x_n = 0$

$\Rightarrow x_n = - x_1 - x_2 \ldots\ldots - x_{n-1}$

$\Rightarrow (x_1, x_2,..., x_n) = (x_1, x_2,..., x_{n-1}, - x_1 - x_2,..., - x_{n-1})$

$= x_1 (1, 0, 0,..., 0, -1) + x_2 (0, 1,..., 0, - 1) + ...$

$x_{n-1}(0, 0, ..., 1, -1)$

$\Rightarrow S = \{(1, 0, 0,..., 0, - 1), (0, 1,..., 0, - 1),...(0, 0,..., 1, -1)\} \subseteq W$ spans W.

Again, let $\alpha_1(1, 0,..., 0, - 1) +...+ \alpha_{n-1} (0, 0,..., 1, -1) = (0, 0,..., 0)$

Then $(\alpha_1, \alpha_2,..., \alpha_{n-1}, -\alpha_1,..., -\alpha_{n-1}) = (0, 0,..., 0)$

$\Rightarrow \alpha_i = 0 \ \forall i = 1, 2, ..., n-1$

Hence S is a basis of W and dim $W = 0(S) = n - 1$.

Theorem 28: *Let W be a subspace of a F.D.V.S. V, then there exists a subspace W' of V such that $V = W \oplus W'$.*

Proof: Let $\{w_1, w_2, ..., w_m\}$ be a basis of W, then $w_1, w_2, ..., w_m$ being *L.I.* in W will be *L.I.* in V. We extend these *L.I.* elements to form a basis of V, say $\{w_1, ..., w_m, v_1, ..., v_n\}$

Let $W' = L(\{v_1, v_2, ..., v_n\})$, *i.e.*, W' be the subspace spanned by $\{v_1, v_2, ..., v_n\}$.

We show $W \oplus W' = V$

Let $v \in V$ be any element, then

$$v = (\alpha_1 w_1 + ... + \alpha_m w_m) + (\beta_1 v_1 + ... + \beta_n v_n), \quad \alpha_i, \beta_j \in F$$

where the first bracket term belongs to W and the second to W'

$\therefore \quad v \in W + W'$ and thus $V \subseteq W + W'$

$$\Rightarrow V = W + W'$$

Again, if $x \in W \cap W'$ be any element

then $x \in W$ and $x \in W'$

$$\Rightarrow x = a_1 w_1 + ... + a_m w_m \qquad a_i, b_j \in F$$

$$x = b_1 v_1 + ... + b_n v_n$$

$$\Rightarrow a_1 w_1 + ... + a_m w_m + (-b_1) v_1 + ... + (-b_n) v_n = 0$$

$$\Rightarrow a_i = b_j = 0 \text{ for all } i, j \qquad w_1, ..., w_m, v_1, ..., v_n \text{ being } L.I.$$

Hence $x = 0$

$$\Rightarrow W \cap W' = (0)$$

or that $V = W \oplus W'$

Remarks:

(*i*) W' is called complement of W. Thus we have proved that *every subspace of a F.D.V.S. has a complement.*

(*ii*) The above throrem can also be proved in any vector space (not essentially finite dimensional).

Cor.: If W' is any complement of W in V then dim W' = dim V – dim W.

Since $V = W \oplus W' \Rightarrow$ dim V = dim $(W \oplus W')$ = dim W + dim W'

$$\Rightarrow \text{dim } W' = \text{dim } V - \text{dim } W.$$

Although every complement of a subspace has same dimension it does not mean that a subspace has a unique complement. Consider

Example 23: Let $V = \mathbf{R}^2(\mathbf{R})$ and let

$$W = \{(a, 0) \mid a \in \mathbf{R}\}$$

$$W_1 = \{(0, b) \mid b \in \mathbf{R}\}$$

$$W_2 = \{(c, c) \mid c \in \mathbf{R}\}$$

It is easy to see that W, W_1, W_2 are subspaces of V.

We show $V = W \oplus W_1$ and $V = W \oplus W_2$

Now $v \in V \Rightarrow v = (x, y) = (x, 0) + (0, y) \in W + W_1$

$\Rightarrow V \subseteq W + W_1 \Rightarrow V = W + W_1$

Again $x \in W \cap W_1 \Rightarrow x \in W$ and $x \in W_1$

$\Rightarrow x = (a, 0), x = (0, b)$

$\Rightarrow (a, 0) = (0, b) \Rightarrow a = b = 0 \Rightarrow x = 0$

Hence $W \cap W_1 = 0$

or that $V = W \oplus W_1$.

Also $v \in V \Rightarrow v = (x, y) = (x - y, 0) + (y, y) \in W + W_2$

$\Rightarrow V \subseteq W + W_2 \Rightarrow V = W + W_2$

Now $x \in W \cap W_2 \Rightarrow x \in W$ and $x \in W_2$

$\Rightarrow x = (a, 0), x = (c, c)$

$\Rightarrow (a, 0) = (c, c)$

$\Rightarrow c = 0, a = 0$

$\Rightarrow x = (0, 0)$

thus $W \cap W_2 = (0)$

or that $V = W \oplus W_2$

Notice that W, W_1, W_2 are spanned by $\{(1, 0)\}$, $\{(0, 1)\}$, $\{(1, 1)\}$ respectively and as each of these is *L.I.* (they are non zero). These subsets form bases of W, W_1, W_2 respectively.

Hence $\dim W = \dim W_1 = \dim W_2 = 1$.

Definition: Let $V(F)$ be a vector space. Subspaces $W_1, W_2, ..., W_m$ of V are said to be independent if

$$w_1 + w_2 + ... + w_m = 0 \Rightarrow w_i = 0 \quad \forall i, \ w_i \in W_i$$

Theorem 29: *Let V be a F.D.V.S. Let $W_1, W_2, \ldots, W_m$ be subspaces of V, where $W = W_1 + W_2 + ... + W_m$, then the following are equivalent*

(*i*) $W_1, W_2, ..., W_m$ are independent

(*ii*) $W_j \cap (W_1 + W_2 + ... + W_{j-1}) = \{0\}, \quad \forall j, \ 2 \le j \le m$

(*iii*) If β_i is an ordered basis of W_i, $1 \le i \le m$, then $\beta = \{\beta_1, \beta_2, ..., \beta_m\}$ is an ordered basis of W.

Proof: (*i*) $\Rightarrow$ (*ii*)

Let $x \in W_j \cap (W_1 + W_2 + ... + W_{j-1})$ be any element

$\Rightarrow x \in W_j$ and $x \in W_1 + W_2 + ... + W_{j-1}$

$\Rightarrow x = w_j, \quad x = w_1 + w_2 + ... + w_{j-1} \quad w_i \in W_i$

$\Rightarrow w_1 + w_2 + ... + w_{j-1} = w_i$

or that $w_1 + w_2 + ... + w_{j-1} + (-1) w_j + 0 + 0 ... + 0 = 0$

$\Rightarrow w_i = 0 \quad \forall i$ using (*i*)

$\Rightarrow x = 0 \Rightarrow$ result.

(*ii*) $\Rightarrow$ (*iii*)

Let $\beta_i = \{x_{i_1}, ..., x_{i_{d_i}}\}$ be basis of W_i.

Let $\sum_{i=1}^{k} a_{i1}x_{i1} + a_{i2}x_{i2} + ... + a_{id_1}x_{id_i} = 0$

Then $\sum_{i=1}^{k} w_i = 0 \Rightarrow w_i = 0$ for all i (since, if j is the largest integer s.t., $w_j \neq 0$, then $w_1 + ... + w_j = 0 \Rightarrow w_j \in W_j \cap (W_1 + ... + W_{j-1}) = \{0\} \Rightarrow w_j = 0$, a contradiction).

$\therefore$ $\beta = \{\beta_1, ..., \beta_k\}$ is an independent set in W. Since β_i spans W_i for all i, β spans W.

$\therefore$ β is a basis of W.

$(iii) \Rightarrow (i)$

Let $x_1 + ... + x_m = 0$, $x_i \in W_i$

Then $\alpha_{1_1}x_{1_1} + ... + \alpha_{1d_1}x_{1_{d_1}} + ... + \alpha_{k_1}x_{k_1} + ... + x_{k_{d_k}} = 0$

$\Rightarrow$ each coefficient $\alpha_{ij} = 0$ as β is linearly independent

$\Rightarrow$ each $x_i = 0$

$\Rightarrow$ $W_1, ..., W_m$ are independent.

Problem 28: *Let V be a finite dimensional space and $W_1, ..., W_m$ be subspaces of V s.t. $V = W_1 + ... + W_m$ and dim V = dim W_1 + ... + dim W_m*

Prove that $V = W_1 \oplus ... \oplus W_m$.

Solution: Let β_i be an ordered basis of W_i for all i. Let dim $W_i = d_i$. Let $x \in V$. Then $x = x_1 + ... + x_m$, $x_i \in W_i$, $x_i \in W_i \Rightarrow x_i$ is a linear combination of vectors in β_i.

$\Rightarrow$ x is a linear combination of vectors in $\beta = \{\beta_1, ..., \beta_m\}$

$\Rightarrow$ β spans V

$\Rightarrow$ β is a basis of V (for if β is not a basis of V, then some subset of β is a basis of $V \Rightarrow$ dim $V < o(\beta_1) + ... + o(\beta_m)$ = dim W_1 + ... + dim W_k = dim V, a contradiction)

$\Rightarrow$ $W_1, ..., W_m$ are independent by Theorem 29

$\Rightarrow$ $W_j \cap (W_1 + ... + W_{j-1}) = \{0\}$ for all j, $2 \leq j \leq m$ by theorem 29

$\Rightarrow$ $V = W_1 \oplus W_2 + ... + \oplus W_m$. (by exercise 18 on page 484).

Exercises

1. Show that the following vectors are *L.I.*

(*i*) (1, 0, 0), (1, 1, 1), (1, 2, 3), in $\mathbf{R}^3(\mathbf{R})$

(*ii*) (1, 1, 0), (1, 0, 1), (0, 1, 1) in $\mathbf{R}^3(\mathbf{R})$

(*iii*) (1, 2, –1), (2, 2, 1), (1, –2, 3) in $\mathbf{R}^3(\mathbf{R})$

(*iv*) (1, 0, 0, 0), (1, 1, 0, 0), (0, 0, 1, 1), (1, 1, 1, 1) in $\mathbf{R}^4(\mathbf{R})$.

2. Show that the following vectors are *L.D.*

(*i*) (1, – 1, 2, 0), (3, 0, 0, 1), (2, 1, – 1, 0), (1, – 1, 2, 0) in $\mathbf{R}^4(\mathbf{R})$

(*ii*) (1, 1, 2), (– 3, 1, 0), (1, – 1, 1), (1, 2, – 3) in $\mathbf{R}^3(\mathbf{R})$

(*iii*) (1, 2, 3, 4), (0, 1, – 1, 2,), (1, 5, 1, 8), (3, 7, 8, 14) in $\mathbf{R}^4(\mathbf{R})$

(*iv*) (1, 1, 2,), (1, 2, 5), (5, 3, 4) in $\mathbf{R}^3(\mathbf{R})$.

3. Show that vectors (v_1, v_2) and (w_1, w_2) in **C** are *L.D.* iff $v_1 w_2 = v_2 w_1$.

4. Prove that every subset of a *L.I.* set is *L.I.* whereas every super set of a *L.D.* set is *L.D.* Hence show that in **C** the vector space of complex numbers, every set with more than one element is *L.D.* set.

5. Let $\alpha_1 = (1, 1, – 2, 1)$, $\alpha_2 = (3, 0, 4, – 1)$, $\alpha_3 = (– 1, 2, 5, 2)$. Show that the vector $(4, – 5, 9, – 7)$ is spanned by $\alpha_1, \alpha_2, \alpha_3$.

6. If S spans V then show that every super set of S spans V.

7. Let $v_1, v_2, \ldots, v_n \in V(F)$, a vector space. Show that $L(\{v_1, v_2, \ldots, v_n\}) = L_1(\{a_1 v_1, a_2 v_2, \ldots, a_n v_n\})$, $a_i \neq 0$ in F and $L(\{v_1, v_2\}) = L(\{v_1 – v_2, v_1 + v_2\})$.

8. Show that $\{1, i\}$ forms a basis of $\mathbf{C}(\mathbf{R})$.

9. Show that $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$, $\{(1, – 1, 1), (0, 1, 1), (1, 1, 1)\}$ and $\{(1, 2, 1), (1, 0, – 1), (0, – 3, 2)\}$ form basis of $\mathbf{R}^3(\mathbf{R})$.

10. Show that the identity map $i : V \to V$ s.t., $i(x) = x$ and zero map $O : V \to V$ s.t., $O(x) = 0$ are linear transformations.

11. Show that every set of three vectors in $\mathbf{R}^2(\mathbf{R})$ is *L.D.*

12. Find a basis and dimension of the following subspaces of $\mathbf{R}^n$:

(*i*) $W = \{(x_1, x_2, \ldots, x_n) \in \mathbf{R}^n \mid x_1 = x_n\}$

(*ii*) $W = \{(x_1, x_2, \ldots, x_n) \in \mathbf{R}^n \mid x_k = 0$ if k is even$\}$

(*iii*) $W = \{(x_1, x_2, \ldots, x_n) \in \mathbf{R}^n \mid x_k$ *s* are equal when k is even$\}$.

13. Find a basis and dimension of the following subspaces of $M_n(\mathbf{R}) = V$

(*i*) $W = \{A \in V \mid A = A'$, the transpose of $A\}$

(*ii*) $W = \{A \in V \mid A = – A'\}$

(*iii*) $W = \{A \in V \mid$ Trace $A = 0\}$.

14. Show that $W_1 = \{(a, b, 0, 0) \mid a, b \in F\}$, $W_2 = \{(0, 0, c, d) \mid c, d \in F\}$ are subspaces of $F^4(F)$, F a field such that $F^4 = W_1 \oplus W_2$.

15. Let W be a subspace of a vector space $V(F)$. For $a, b \in V$, define $a \equiv b \bmod W$ (a is congruent to b modulo W) iff $a – b \in W$ and $\alpha(a – b) \in W$, for all $\alpha \in F$. Show that this relation is an equivalence relation on V and for any $a \in W$, $cl(a) = W + a$.

16. Extend the set $S = \{(1, 1, 0)\}$ to form two different bases of $\mathbf{R}^3(\mathbf{R})$.

17. Let S be a finite subset of a vector space V such that S is *L.I.* and every proper superset of S in V is *L.D.* Show that S is a basis of V.

18. If W_1 and W_2 are subspaces of $\mathbf{R}^4$ and $\{(1, 0, 0, 0), (1, 1, 0, 0), (1, 1, 1, 0)\}$, $\{(0, 0, 0, 1), (0, 0, 1, 1), (0, 1, 1, 1)\}$ are bases of W_1 and W_2 respectively, find a basis of $W_1 \cap W_2$.

[**Hint:** $W_1 \cap W_2 = \{(0, a, b, 0) \mid a, b \in \mathbf{R}\}$]

19. Find two subspaces A and B of $\mathbf{R}^4(\mathbf{R})$ such that dim $A = 2$, dim $B = 3$ and dim $(A \cap B) = 1$.

20. Let F be a field. Let $A = \{(x, y, 0) \mid x, y, \in F\}$, $B = \{(0, y, z) \mid y, z \in F\}$ be subspaces of $F^3(F)$. Find dimension of the subspace $A + B$.

21. Let W be the subspace of $\mathbf{R}^3(\mathbf{R})$, spanned by $\{(1, 0, 0), (0, 1, 0)\}$. Find a complement of W.

22. Let S be a set of four vectors such that any three of them are *L.I.* Does it follow that the four vectors are *L.I.*?

[No. consider (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)]

23. Let V be a vector space over F. Assume that every linearly independent set in V can be extended to a basis of V. Deduce that V has a basis.

24. If W_1, W_2, and W_3 are subspaces of a *F.D.V.S.* V then show that

$$\dim (W_1 \oplus W_2 \oplus W_3) = \dim W_1 + \dim W_2 + \dim W_3$$

25. Let W_1 and W_2 be subspaces of $\mathbf{R}^n$ such that every vector in $\mathbf{R}^n$ is the sum of a vector in W_1 and a vector in W_2. Let B_1 and B_2 be basis for W_1 and W_2 respectively. Under what condition is $B_1 \cup B_2$ a basis of $\mathbf{R}^n$?

$[W_1 \cap W_2 = (0)]$

26. If W is a finite dimensional subspaces of a vector space V such that $\frac{V}{W}$ is finite dimensional then show that V is also finite dimensional.

27. Prove that if $S = \{v_1, v_2, \ldots, v_n\}$ is a basis of a vector space $V(F)$ and $S' = \{w_1, w_2, \ldots, w_m\}$ is a *L.I.* subset of V then $m \leq n$.

28. Give an example of a vector space V and its subspace W such that V, W and $\frac{V}{W}$ are infinite dimensional and

$$\dim V = \dim W = \dim \frac{V}{W}.$$

[**Hint:** Take $V = F[x]$, $W = F[x^2]$]

Inner Product Spaces

In general a vector space is defined over an arbitrary field F and this is what we did earlier. In this section we restrict F to the field of real or complex numbers. In the first case, the vector space is called real vector space and in the second case it is called a complex vector space. We study real vector spaces in analytical geometry and vector analysis. There we discuss the concept of length and orthogonality. We also have dot or scalar product of two vectors which among other things satisfies the following:

(i) $\vec{v} \cdot \vec{v} \geq 0$ and $(\vec{v} \cdot \vec{v}) = 0 \Leftrightarrow \vec{v} = 0$

(ii) $\vec{v} \cdot \vec{w} = \vec{w} \cdot \vec{v}$

(iii) $\vec{u} \cdot (\alpha\vec{v} + \beta\vec{w}) = \alpha(\vec{u} \cdot \vec{v}) + \beta(\vec{u} \cdot \vec{w})$

where $\vec{u}, \vec{v}, \vec{w}$ are vectors and α, β real numbers.

We wish to extend the concept of dot product to complex vector spaces also. We define a map on $V \times V$ to F (where V = vector space over F) with same property as dot product, called inner product and study the concept of length and orthogonality.

Definition: Let V be a vector space over field F (where F = field of real or complex numbers). Suppose for any two vectors $u, v \in V$ $\exists$ an element $(u, v) \in F$ s.t., [(u, v) here is just an element of F and should not be confused with the ordered pair.]

(*i*) $(u, v) = \overline{(v, u)}$ (*i.e.*, complex conjugate of (v, u))

(*ii*) $(u, u) \geq 0$ and $(u, u) = 0 \Leftrightarrow u = 0$

(*iii*) $(\alpha u + \beta v, w) = \alpha(u, w) + \beta(v, w)$

for any $u, v, w \in V$ and $\alpha, \beta \in F$.

Then V is called an *inner product space* and the function satisfying (*i*), (*ii*) and (*iii*) is called an *inner product*.

Thus inner product space is a vector space over the field of real or complex numbers with an inner product function.

Remarks:

1. Property (*ii*) in the definition of inner product space makes sense in as much as $(u, u) = \overline{(u, u)}$ by $(i) \Rightarrow (u, u)$ = real.
2. Property (*iii*) can also be described by saying that inner product is a linear map in 1st variable.
3. Can we say that inner product is linear in 2nd variable?
   Let's evaluate
   $$(u, \alpha v + \beta w) = \overline{(\alpha v + \beta w, u)} \text{ by } (i)$$
   $$= \bar{\alpha}\,\overline{(v, u)} + \bar{\beta}\,\overline{(w, u)}$$
   $$= \bar{\alpha}\,(u, v) + \bar{\beta}\,(u, w)$$
   So, it need not be linear in 2nd variable.
4. If F = field of real numbers, then the function inner product satisfies same properties as dot product seen earlier.
5. Inner product space over real field is called *Euclidean space* and over complex field is called *Unitary space*.
6. In the vector space of all vectors in 3-dimensional space over reals, the inner product will be the usual dot product of two vectors, *i.e.*,
   $$\langle \vec{u}, \vec{v} \rangle = |\vec{u}||\vec{v}| \cos\theta.$$

Example 24: Let $V = F^{(n)}$, F = field of complex numbers.

Let $u = (\alpha_1, \alpha_2, \ldots, \alpha_n)$
$v = (\beta_1, \beta_2, \ldots, \beta_n)$ in $F^{(n)}$

Define $(u, v) = \alpha_1\overline{\beta_1} + \ldots + \alpha_n\overline{\beta_n}$

It can be easily shown that (u, v) defines an inner product, called standard inner product.

Example 25: Let $V = \mathbf{R}^{(2)}$, $u = (\alpha_1, \alpha_2)$, $v = (\beta_1, \beta_2)$

Define $(u, v) = \alpha_1\beta_1 - \alpha_2\beta_1 - \alpha_1\beta_2 + 4\,\alpha_2\beta_2$

Then

(i) $(u, v) = (v, u) = \overline{(v, u)}$

(ii) $(u, u) = (\alpha_1 - \alpha_2)^2 + 3\alpha_2^2 \geq 0$

$(u, u) = 0 \Leftrightarrow \alpha_1 = \alpha_2,\ \alpha_2 = 0$

$\Leftrightarrow \alpha_1 = 0 = \alpha_2$

$\Leftrightarrow u = (\alpha_1, \alpha_2) = (0, 0) = 0$

(iii) $(\alpha u + \beta u, w) = \alpha(u, w) + \beta(v, w)$

can be easily verified.

Thus (u, v) defines an inner product.

Example 26: One may construct a new inner product from a given one. Let V, W be vector spaces over F and T, a one–one linear transformation from V into W.

Suppose $(\ ,\ )$ is an inner product on W. Then

$$< u, v > = (T(u), T(v))$$

defines an inner product on V as

(i) $< \overline{v, u} > = \overline{(T(v), T(u))}$

$= (T(u), T(v))$

$= < u, v >$

(ii) $< u, v > = (T(u), T(u)) \geq 0$

and $< u, u > = 0 \Leftrightarrow (T(u), T(u)) = 0$

$\Leftrightarrow T(u) = 0 \Leftrightarrow u = 0$ as T is 1–1

(iii) $< \alpha u + \beta v, w > = (T(\alpha u + \beta v), T(w))$

$= (\alpha T(u) + \beta T(v), T(w))$

$= \alpha(T(u), T(w)) + \beta(T(v), T(w))$

$= \alpha < u, w > + \beta < v, w >$

Example 27: Let $V = M_{m\times n}$ $(\mathbf{C})$. Then $< A, B > =$ Trace (AB^*) where $B^* = \overline{B'}$, defines an inner product on V as

(i) $< \overline{B, A} > = \overline{\text{Trace } BA^*}$

Let $A = (a_{ij})$, $B = (b_{ij})$, $AB^* = C = (c_{ij})$

$B^* = (d_{ij})$, where $d_{ij} = \overline{b}_{ji}$

$\therefore\ c_{ik} = \Sigma a_{ij} d_{jk} = \Sigma a_{ij}\, \overline{b}_{kj}$

$\Rightarrow\ c_{ii} = \Sigma a_{ij}\, \overline{b}_{kj}$

$\Rightarrow$ Trace $AB^* = \Sigma c_{ii} = \Sigma(\Sigma a_{ij}\, \overline{b}_{ij})$

Let $A^* = (e_{ij})$, where $e_{ij} = \overline{a}_{ji}$

Let $BA^* = F = (f_{ij})$, then

$$f_{ik} = \Sigma b_{ij}\overline{a}_{kj}$$

$$\Rightarrow \text{Trace } BA^* = \Sigma f_{ii} = \Sigma(\Sigma b_{ij}\overline{a}_{ij})$$

$$\Rightarrow \overline{\text{Trace } BA^*} = \Sigma\Sigma a_{ij}\overline{b}_{ij} = \text{Trace } AB^*$$

$$\Rightarrow \quad \langle \overline{B, A} \rangle = \langle A, B \rangle$$

(ii) $\langle A, B \rangle = \text{Trace } AB^* = \Sigma(\Sigma a_{ij}\overline{b}_{ij})$

$$\therefore \langle A, A \rangle = \sum\sum a_{ij}\overline{a}_{ij} = \sum\sum |a_{ij}|^2 \geq 0$$

and $\langle A, A \rangle = 0 \Leftrightarrow |a_{ij}| = 0 \quad \forall\ i, j$

$$\Leftrightarrow a_{ij} = 0 \quad \forall\ i, j$$

$$\Leftrightarrow A = 0$$

Similarly axiom (iii) can be verified.

Problem 29: *Let V be an inner product space. Show that*

(i) $(0, v) = 0$ *for all* $v \in V$

(ii) $(u, v) = 0$ *for all* $v \in V \Rightarrow u = 0$

Solution: (i) $(0, v) = (0, 0, v)$

$$= 0\,(0, v) = 0$$

(ii) $(u, v) = 0$ for all $v \in V$

$\Rightarrow (u, u) = 0 \Rightarrow u = 0.$

Problem 30: *Let W_1, W_2 be two subspaces of a vector space V. If W_1, W_2 are inner product spaces, show that $W_1 + W_2$ is also an inner product space.*

Solution: Let $x, y \in W_1 + W_2$.

Then $x = u_1 + u_2$

$y = v_1 + v_2 \quad u_1, v_1 \in W_1;\ u_2, v_2 \in W_2$

Define $\langle x, y \rangle = (u_1, v_1) + (u_2, v_2)$

Then

(i) $$\overline{\langle y, x \rangle} = \overline{(v_1, u_1) + (v_2, u_2)}$$

$$= \overline{(v_1, u_1)} + \overline{(v_2, u_2)}$$

$$= (u_1, v_1) + (u_2, v_2)$$

$$= \langle x, y \rangle$$

(ii) $\langle x, x \rangle = (u_1, u_1) + (u_2, u_2) \geq 0$

and $\langle x, x \rangle = 0 \Leftrightarrow (u_1, u_1) = 0 = (u_2, u_2)$

$$\Leftrightarrow u_1 = 0 = u_2$$

$$\Leftrightarrow x = 0$$

(*iii*) $< \alpha x + \beta y, z > = \alpha < x, z > + \beta < y, z >$
can be easily verified.

$\therefore$ $< x, y >$ defines an inner product on $W_1 + W_2$

So, $W_1 + W_2$ is an inner product space.

Norm of a Vector

Let V be an inner product space. Let $v \in V$. Then *norm* of v (or length of v) is defined as $\sqrt{(v, v)}$ and is denoted by $\| v \|$.

In the vector space of all vectors in 3-dimensional space,

$$\| \vec{u} \| = \sqrt{< \vec{u}, \vec{u} >} = | \vec{u} | = \text{length of } \vec{u} .$$

For this reason, norm of vector in general is also called length of vector.

Problem 31: $\| \alpha v \| = | \alpha | \, \| v \|$ *for all* $\alpha \in F$, $v \in V$

Solution:
$$\| \alpha v \|^2 = (\alpha v, \alpha v)$$
$$= \alpha \bar{\alpha} \, (v, v)$$
$$= | \alpha |^2 \, \| v \|^2$$
$$\Rightarrow \| \alpha v \| = | \alpha | \, \| v \|$$

We now prove an important inequality known as *Cauchy-Schwarz inequality*.

Theorem 30: *Let V be an inner product space.*
Then $| (u, v) | \leq \| u \| \, \| v \|$ *for all* $u, v \in V$.

Proof: If $u = 0$, then $(u, v) = (0, v) = 0$

and $\| u \| = \sqrt{(u,u)} = \sqrt{(0,0)} = 0$

$\therefore$ L.H.S. = R.H.S.

Let $u \neq 0$. Then $\| u \| \neq 0$

(as $\| u \| = 0 \Rightarrow \sqrt{(0,0)} = 0$
$\Rightarrow (u, u) = 0 \Rightarrow u = 0$)

Let $w = v - \dfrac{(v, u)}{\| u \|^2} u$

Then
$$(w, w) = \left(v - \frac{(v, u)}{\| u \|^2} u, \, v - \frac{(v, u)}{\| u \|^2} u \right)$$
$$= (v, v) - \frac{(v, u)}{\| u \|^2} \, (u, v)$$
$$= \| v \|^2 - \frac{\overline{(u, v)} \, (u, v)}{\| u \|^2} = \| v \|^2 - \frac{| (u, v) |^2}{\| u \|^2}$$
$$= \frac{\| u \|^2 \, \| v \|^2 - | (u, v) |^2}{\| u \|^2}$$

Since $(w, w) \geq 0$,

$$|(u, v)|^2 \leq \|u\|^2 \|v\|^2$$

$$\Rightarrow |(u, v)| \leq \|u\| \|v\|.$$

Remarks:

(*i*) The above inequality will be an equality if and only if u, v are linearly dependent.

Proof: Suppose $|(u, v)| = \|u\| \|v\|$

If $u = 0$, then $u = 0.v \Rightarrow u$, v are linearly dependent.

Let $u \neq 0$. Then from above

$$(w, w) = 0 \Rightarrow w = 0$$

$$\therefore \quad v - \frac{(v, u)}{\|u\|^2} u = 0$$

$$\Rightarrow v = v - \frac{(v, u)}{\|u\|^2} u \Rightarrow u, v \text{ are linearly dependent.}$$

Conversely, let $u = \alpha v$, $\alpha \in F$

Then $|(u, v)| = |\alpha (v, v)| = |\alpha| \|v\|^2$

$$\|u\| \|v\| = |\alpha| \|v\| \|v\| = |\alpha| \|v\|^2$$

$$|(u, v)| = \|u\| \|v\|.$$

(*ii*) In the vector space of all vectors in 3-dimensional space, since

$$|\langle \vec{u}, \vec{v} \rangle| = |\vec{u}| \, |\vec{v}| \, |\cos\theta|$$

$$\leq \|\vec{u}\| \|\vec{v}\| \quad \text{as } |\cos\theta| \leq 1$$

we find that Cauchy-Schwarz inequality holds.

Theorem 31: *Let V be an inner product space.*

Then (*i*) $\|x + y\| \leq \|x\| + \|y\|$ *for all* $x, y \in V$

(*Triangle inequality*)

(*ii*) $\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$

(*Parallelogram Law*)

Proof: (*i*) $\|x + y\|^2 = (x + y, x + y)$

$$= (x, x) + (y, x) + (x, y) + (y, y)$$

$$= \|x\|^2 + \overline{(x, y)} + (x, y) + \|y\|^2$$

$$= \|x\|^2 + 2Re\,(x, y) + \|y\|^2$$

$$\leq \|x\|^2 + 2\,|(x, y)| + \|y\|^2$$

$$\leq \|x\|^2 + 2\,\|x\| \|y\| + \|y\|^2$$

$$= (\|x\| + \|y\|)^2$$

Hence, $\|x + y\| \leq \|x\| + \|y\|$

This is called triangle inequality as

$\| x \| + \| y \|$ = sum of the lengths of two sides of a triangle

$\| x + y \|$ = length of the third side of the triangle showing that sum of two side of a triangle is less than its third side.

(*ii*) $\| x + y \|^2 + \| x - y \|^2$

$= (x + y, x + y) + (x - y, x - y)$

$= \| x \|^2 + \| y \|^2 + (x, y) + (y, x) + \| x \|^2 + \| y \|^2 - (x, y) - (y, x)$

$= 2 (\| x \|^2 + \| y \|^2)$.

Note: $\| x + y \|^2 + \| x - y \|^2$ = sum of squares of lengths of diagonals of a parallelogram

$2 (\| x \|^2 + \| y \|^2)$ = sum of squares of sides of a parallelogram.

$\therefore$ sum of squares of lengths of diagonals of a parallelogram is equal to sum of squares of lengths of its sides. For this reason (*ii*) is called parallelogram law.

Problem 32: *Show that* $\| x + y \| = \| x \| + \| y \|$ if and only if one of the vectors x, y is a non negative scalar multiple of the other, where x, y are in an inner product space.

Solution: Let $\| x + y \| = \| x \| + \| y \|$

Therefore, $< x + y, x + y > = \| x \|^2 + \| y \|^2 + 2\| x \| \| y \|$

or $\| x \|^2 + \| y \|^2 + < x, y > + < y, x > = \| x \|^2 + \| y \|^2 + 2\| x \| \| y \|$

So $2 \text{ Re} < x, y > = 2\| x \| \| y \|$

or $\text{Re} < x, y > = \| x \| \| y \|$

Let $z = y - \dfrac{\| y \|}{\| x \|} x$

Then $< z, z > = \left(y - \dfrac{\| y \|}{\| x \|} x,\ y - \dfrac{\| y \|}{\| x \|} x \right)$

$= \| y \|^2 - \dfrac{\| y \|}{\| x \|} < y,\ x > - \dfrac{\| y \|}{\| x \|} < x, y > + \| y \|^2$

$= 2 \| y \|^2 - \dfrac{\| y \|}{\| x \|} (2 \text{Re}(x, y))$

$= 2\| y \|^2 - 2\| y \|^2 = 0$

So, $z = 0$ implies $y = \dfrac{\| y \|}{\| x \|} x = cx, \quad c = \dfrac{\| y \|}{\| x \|}$ is a non negative real number.

If $x = 0$, then $x = 0y$

Conversely, let $y = cx$, c, a non negtive real number.

Then $\| x + y \| = \| x + cx \| = |(1 + c)| \ \| x \| = (1 + c) \ \|x\|$

and $\| x \| + \| y \| = \| x \|(1 + |c|) = (1 + c) \ \|x\|$

Hence $\| x + y \| = \| x \| + \| y \|$

Problem 33: *Using Cauchy-Schwarz inequality, prove that cosine of an angle is of absolute vale at most* 1.

Solution: Let F = Field of real numbers and $V = F^{(3)}$

Consider standard inner product on V.

Let $u = (x_1, y_1, z_1)$, $v = (x_2, y_2, z_2) \in V$

Let $O = (0, 0, 0)$

Let θ be an angle between OU and OV.

Then $$\cos\theta = \frac{x_1x_2 + y_1y_2 + z_1z_2}{\sqrt{x_1^2 + y_1^2 + z_1^2}\sqrt{x_2^2 + y_2^2 + z_2^2}} = \frac{(u, v)}{\|u\|\,\|v\|}$$

$$\therefore \quad |\cos\theta| = \frac{|(u, v)|}{\|u\|\,\|v\|} \leq \frac{\|u\|\,\|v\|}{\|u\|\,\|v\|} = 1$$

Orthogonality

Let V be an inner product space. Two vectors $u, v \in V$ are said to be *orthogonal* if $(u, v) = 0 \Leftrightarrow (v, u) = 0$. So, u is orthogonal to v iff v is orthogonal to u. Since $(0, v) = 0$ for all $v \in V$, 0 is orthogonal to every vector in V.

Conversely, if $u \in V$ is orthogonal to every vector in V, then $(u, u) = 0 \Rightarrow u = 0$.

Let W be a subspace of V.

Define $W^\perp = \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}$ ($W^\perp$ is read as W perpendicular). Then $W^\perp$ is a subspace of V as $0 \in W^\perp \Rightarrow W^\perp \neq \varphi$ and $v_1, v_2 \in W^\perp$, $\alpha, \beta \in F$

$\Rightarrow (\alpha v_1 + \beta v_2, w) = \alpha(v_1, w) + \beta(v_2, w) = 0$ for all $w \in W$

$\Rightarrow \alpha v_1 + \beta v_2 \in W^\perp$.

$W^\perp$ is called *orthogonal complement* of W. The reason for calling it thus is because we shall prove later that $V = W \oplus W^\perp$.

Problem 34: *Let V be an inner product space. Let $x, y \in V$ s.t., $x \perp y$*

Then show that $\|x + y\|^2 = \|x\|^2 + \|y\|^2$. (This is Pythagoras Theorem when $F = \mathbf{R}$ as in triangle ABC with $AB \perp BC$, $AB^2 = \|x\|^2$, $BC^2 = \|y\|^2$, $AC^2 = \|x + y\|^2$)

Solution: $$\begin{aligned}\|x + y\|^2 &= (x + y, x + y)\\ &= (x, x) + (y, y) + (x, y) + (y, x)\\ &= \|x\|^2 + \|y\|^2 \quad \text{as } (x, y) = 0 = (y, x).\end{aligned}$$

Orthonormal Set

A set $\{u_i\}_i$ of vectors in an inner product space V is said to be orthogonal if $(u_i, u_j) = 0$ for $i \neq j$. If further $(u_i, u_i) = 1$ for all i, then the set $\{u_i\}$ is called an *orthonormal set*.

Example 28: Let V be the real vector space of real polynomials of degree less than or equal to n. Define an inner product on V by

$$\left(\sum_{i=0}^{n} a_i x^i, \sum_{j=1}^{n} b_j x^j\right) = \sum_{1}^{n} a_i b_i$$

Then $\{1, x, ..., x^n\}$ is an orthonormal subset of V.

Theorem 32: *Let S be an orthogonal set of non zero vectors in an inner product space V. Then S is a linearly independent set.*

Proof: To show S is linearly independent, we have to show that every finite subset of S is linearly independent.

Let $\{v_1, ..., v_n\}$ be a finite subset of S.

Let $\alpha_1 v_1 + ... + \alpha_n v_n = 0, \quad \alpha_i \in F$

$$(\alpha_1 v_1 + ... + \alpha_n v_n, \alpha_1 v_1 + ... + \alpha_n v_n) = 0$$

$$\Rightarrow |\alpha_1|^2 \| v_1 \|^2 + ... + |\alpha_n|^2 \| v_n \|^2 = 0$$

$$\Rightarrow |\alpha_i|^2 \| v_i \|^2 = 0 \quad \text{for all } i = 1, ..., n$$

$$\Rightarrow |\alpha_i|^2 = 0 \text{ for all } i \text{ as } \| v_i \|^2 = 0 \Rightarrow \| v_i \| = 0 \Rightarrow v_i = 0$$

which is not true

$$\Rightarrow \alpha_i = 0 \quad \text{for all } i = 1, ..., n$$

$\Rightarrow S$ is linearly independent.

Cor.: An orthonormal set in an inner product space is linearly independent.

Proof: Let S be an orthonormal set in an inner product space V. Let $v \in S$. Then $v \neq 0$ as $v = 0 \Rightarrow (v, v) = 0 \neq 1$, a contradiction. Therefore, S is an orthogonal set of non zero vectors and so linearly independent.

Theorem 33: (Gram-Schmidt Orthogonalisation process)

Let V be a non zero inner product space of dimension n. Then V has an orthonormal basis.

Proof: It is enough to construct an orthogonal basis of V. For let $S \subseteq V$ be an orthogonal set.

Then $T = \left\{ \frac{x}{\| x \|} \mid x \in S \right\}$ is an orthonormal set.

Let $\{v_1, ..., v_n\}$ be a basis of V.

Let $w_1 = v_1$. Define $w_2 = v_2 - \frac{(v_2, w_1)}{(w_1, w_1)} w_1$

$$= v_2 - \frac{(v_2, v_1)}{(v_1, v_1)} v_1$$

Then $(w_2, w_1) = (w_2, v_1)$

$$= (v_2, v_1) - \frac{(v_2, v_1)}{(v_1, v_1)} (v_1, v_1) = 0$$

Also $v_2 = \alpha_1 v_1 + w_2 = \alpha_1 w_1 + w_2$

where $\alpha_1 = \frac{(v_2, v_1)}{(v_1, v_1)} \in F$.

(Note v_1 is linearly independent $\Rightarrow v_1 \neq 0 \Rightarrow (v_1, v_1) \neq 0$)

Define $w_3 = v_3 - \frac{(v_3, w_2)}{(w_2, w_2)} w_2 - \frac{(v_3, w_1)}{(w_1, w_1)} w_1$

Then $(w_3, w_2) = 0 = (w_3, w_1)$

Also $v_3 = \alpha_1 w_1 + \alpha_2 w_2 + w_3$, where $\alpha_1, \alpha_2 \in F$.

In this way, we can construct an orthogonal set $\{w_1, ..., w_n\}$ where each $v_i = \alpha_1 w_1 + ... + w_i, \quad \alpha_i \in F$

$\therefore \left\{ \frac{w_1}{\| w_1 \|}, ..., \frac{w_n}{\| w_n \|} \right\}$ is an orthonormal set which is linearly independent by Cor. to Theorem 32 and hence forms a basis of V as dim $V = n$.

Aliter: Let dim $V = n$. We use induction on n.

Let $n = 1$. Let $0 \neq x \in V$, then $v = \frac{x}{\| x \|} \in V$ s.t., $\| v \| = 1$.

So, $\{v\}$ is an orthonormal basis of V.

Suppose now that the result holds for any inner product space of dimension less than or equal to $n - 1$.

Let V be an inner product space of dimension n

Let $0 \neq v \in V$ be such that $\| v \| = 1$.

Define $T_v : V \to \mathbf{C}$ s.t.,

$T_v(v') = < v', v >$

Then T_v is a linear transformation.

Let $\alpha \in \mathbf{C}$, then $\alpha = \alpha \| v \|^2 = \alpha < v, v > = < \alpha v, v > = T_v(\alpha v)$

and so T_v is onto. *i.e.*, Range $T_v = \mathbf{C}$.

By Sylvester's law

$$\dim V = \dim \text{Ker } T_v + \dim \text{Range } T_v$$

$$\Rightarrow n = \dim \text{Ker } T_v + \dim \mathbf{C}$$

$$= \dim \text{Ker } T_v + 1$$

$$\Rightarrow \dim W = n - 1, \text{ where } W = \text{Ker } T_v$$

$$= \{x \in V \mid T_u(x) = 0\}$$

$$= \{x \in V \mid < v, x > = 0\}$$

By induction hypothesis, W has an orthonormal basis $\{w_1, w_2, ..., w_{n-1}\}$

Now $w_i \in W \Rightarrow < v, w_i > = 0 \quad \forall i = 1, 2, ..., n - 1$

Also $< v, v > = \| v \|^2 = 1$

So $\{w_1, w_2, ..., w_{n-1}, v\}$ is an orthonormal set.

i.e., $\{w_1, w_2, ..., w_{n-1}, v\}$ is L.I. set by cor. to theorem 32.

Since dim $V = n$, $\{w_1, w_2, ..., w_{n-1}, v\}$ is a basis of V and hence is an orthonormal basis of V. So, result follows by induction.

Problem 35: *Obtain an orthonormal basis, w.r.t. the standard inner product for the subspace of* $\mathbf{R}^3$ *generated by* (1, 0, 3) *and* (2, 1, 1).

Solution: Let $v_1 = (1, 0, 3)$, $v_2 = (2, 1, 1)$

Then $w_1 = v_1,\ w_2 = v_2 - \dfrac{(v_2, w_1)}{(w_1, w_1)}\ w_1$

Now $(v_2, w_1) = (v_2, v_1) = 2 + 0 + 3 = 5$

$(w_1, w_1) = (v_1, v_1) = 1 + 0 + 9 = 10$

$\therefore \quad \| w_1 \| = \sqrt{10}$

So, $w_2 = (2, 1, 1) - \dfrac{5}{10}\ (1, 0, 3) = \left(\dfrac{3}{2}, 1, -\dfrac{1}{2}\right)$

$\therefore \quad \| w_2 \| = \sqrt{\dfrac{9}{4} + 1 + \dfrac{1}{4}} = \sqrt{\dfrac{7}{2}}$

$\therefore$ required orthonormal basis is

$$\left\{\frac{w_1}{\| w_1 \|}, \frac{w_2}{\| w_2 \|}\right\} = \left\{\frac{1}{\sqrt{10}}(1, 0, 3),\ \frac{\sqrt{2}}{7}\left(\frac{\sqrt{3}}{2}, 1, -\frac{1}{2}\right)\right\}$$

Problem 36: *Let V be an inner product space over $\boldsymbol{R}$. Let $\{v_1, v_2, ..., v_n\}$ be a basis of V s.t., whenever $v = \Sigma\alpha_i v_i$ then $\| v \|^2 = \Sigma\alpha_i^2$. Show that $\{v_1, v_2, ..., v_n\}$ is an orthonormal basis.*

Solution: We have $v_i = 1.v_i \Rightarrow \| v_i \|^2 = 1 \qquad \forall i$ by hypothesis

Consider $v_i + v_j$, $i \neq j$, then

$$\| v_i + v_j \|^2 = 2$$

$$\Rightarrow < v_i, v_i > + < v_j, v_j > + < v_i, v_j > + < v_j, v_i > = 2$$

$$\Rightarrow < v_i, v_j > + < v_j, v_i > = 0$$

$$\Rightarrow < v_i, v_j > + < v_i, v_j > = 0 \text{ as } V \text{ is an inner product space over } \mathbf{R}$$

$$\Rightarrow < v_i, v_j > = 0 \quad \forall i \neq j$$

Hence $\{v_1, v_2, ..., v_n\}$ is an orthonormal basis.

Theorem 34: (Bessel's inequality)

If $\{w_1, ..., w_m\}$ is an orthonormal set in V, then

$$\sum_{i=1}^{m} |(w_i, v)|^2 \leq \| v \|^2 \text{ for all } v \in V.$$

Proof: Let $x = v - \sum_{i=1}^{m} (v, w_i)\, w_i$

$\therefore \quad (x, w_j) = (v, w_j) - (v, w_j) = 0$ for all $j = 1, ..., m$

Let $w = \sum_{i=1}^{m} (v, w_i)\, w_i = \sum_{i=1}^{m} \alpha_i w_i,\ \alpha_i = (v, w_i)$

$\therefore \quad v = x + w$

Also $(w, x) = (\alpha_1 w_1 + ... + \alpha_m w_m, x)$

$= \alpha_1(w_1, x) + ... + \alpha_m(w_m, x) = 0$

Now $\| v \|^2 = (v, v)$

$$= (w + x,\ w + x)$$
$$= (w,\ w) + (x,\ x)$$
$$= \| w \|^2 + \| x \|^2 \geq \| w \|^2$$

But $\| w \|^2 = (w,\ w)$
$$= (\alpha_1 w_1 + ... + \alpha_m w_m,\ \alpha_1 w_1 + ... + \alpha_m w_m)$$
$$= \alpha_1 \overline{\alpha_1}\ (w_1,\ w_1) + ... + \alpha_m \overline{\alpha_m}\ (w_m,\ w_m)$$
$$= | \alpha_1 |^2 + ... + | \alpha_m |^2$$

as $\{w_1,....., w_m\}$ is an orthonormal set

$$= \sum_{i=1}^{m} | \alpha_i |^2 = \sum_{i=1}^{m} | (v_i, w_i) |^2 = \sum_{i=1}^{m} | \overline{(w_i, v)} |^2 = \sum_{i=1}^{m} | (w_i, v) |^2$$

$\therefore$ $\sum_{i=1}^{m} | (w_i, v) |^2 \leq \| v \|^2$ for all $v \in V$.

Cor.: Equality holds if and only if $v = w$.

Proof: Suppose $v = w$

Then $\| v \|^2 = \| w \|^2 = \sum_{i=1}^{m} | (w_i, v) |^2$

Conversely, suppose equality holds

Then $\| v \|^2 = \| w \|^2$

$\Rightarrow \| x \|^2 = 0 \Rightarrow (x,\ x) = 0 \Rightarrow x = 0$

$\Rightarrow v = w + x = w.$

Theorem 35: *If V is a finite dimensional inner product space and W is a subspace of V, then $V = W \oplus W^{\perp}$.*

Proof: Since V is an inner product space, so is W. By theorem 33, W has an orthonormal basis $\{w_1,..., w_m\}$.

Let $v \in V$.

Let $w = \sum_{i=1}^{m} (v, w_i) w_i$, $w_i \in W$ and $x = v - w$

Then $(x,\ w_j) = 0$ as in theorem 34, for all $j = 1,..., m$

$\therefore$ $(x,\ w) = (x,\ \beta_1 w_1 + ... + \beta_m w_m)$
$$= \overline{\beta_1}\ (x,\ w_1) + ... + \overline{\beta_m}\ (x,\ w_m)$$
$$= 0 \text{ for all } w \in W$$

$\therefore$ $x \in W^{\perp}$

So, $v = w + x \in W + W^{\perp}$

$V \subseteq W + W^{\perp}$

$\Rightarrow V = W + W^{\perp}$

Let $y \in W \cap W^{\perp} \Rightarrow (y, w) = 0$ for all $w \in W, y \in W$

$\Rightarrow (y, y) = 0$ as $y \in W$

$\Rightarrow y = 0$

$\therefore \quad W \cap W^{\perp} = \{0\}$

Hence $V = W \oplus W^{\perp}$.

Cor. 1: If W is a subspace of a finite dimensional inner product space V, then $(W^{\perp})^{\perp} = W$.

By above theorem, $V = W \oplus W^{\perp}$

Let $w \in W, x \in W^{\perp}$

Then $x \in W^{\perp} \Rightarrow < x, y > = 0 \quad \forall\, y \in W$

$\Rightarrow < x, w) = 0 \quad \forall\, x \in W^{\perp}$

$\Rightarrow w \in (W^{\perp})^{\perp}$

i.e., $W^{\perp} \subseteq (W^{\perp})^{\perp}$

Let $v \in (W^{\perp})^{\perp}$ then $v = w + w'$, $w \in W$, $w' \in W^{\perp}$

$\Rightarrow 0 = < w', v > = < w', w + w') = < w', w > + < w', w' > = < w', w' >$

So $w' = 0 \Rightarrow v = w \in W$

i.e., $(W^{\perp})^{\perp} \subseteq W$ giving $W = (W^{\perp})^{\perp}$.

Cor. 2: If $S = \{x_1, x_2, ..., x_r\}$ is a basis of W and $T = \{y_1, y_2, ..., y_s\}$ is a basis of $W^{\perp}$ then $\{x_1, x_2, ..., x_r, y_1, y_2, ..., y_s\}$ is an orthonormal basis of V.

By above theorem $V = W \oplus W^{\perp}$

thus $S \cup T$ is a basis of V

Also $< x_i, y_j > = 0 \quad \forall\, i, j$ as $y_j \in W^{\perp}\ \forall j$

proving the result.

Remark: Theorem 35 on page 529 need not hold in case of infinite dimensional vector space. For instance, take

$$V = \{(a_n) \mid (a_n) \text{ is a sequence of complex nos. s.t., } \sum_{1}^{\infty} |a_n|^2 < \infty\}.$$

Then V is a vector space w.r.t. componentwise addition and scalar multiplication

Take $a = (a_n), b = (b_n) \in V$

Define $< a, b > = \sum_{1}^{\infty} a_n \overline{b_n}$

Since $(|a_n| - |b_n|)^2 \geq 0$

$|a_n|^2 + |b_n|^2 \geq 2 |a_n| |b_n|$

Now $2 |\Sigma a_n \bar{b}_n| \leq 2\Sigma |a_n| |\bar{b}_n|$

$\Rightarrow 2 |\Sigma a_n \bar{b}_n| \leq 2 \Sigma |a_n| |b_n|$ as $|b_n| = |\bar{b}_n|$

$\leq \Sigma |a_n|^2 + \Sigma |b_n|^2 < \infty$

Thus $< a, b >$ is well defined inner product on V.

Let $A_k \in V$ s.t., k^{th} entry is 1 and zero elsewhere

Let $S = \{| A_k | k = 1, 2,..., \} \subseteq V$

Then $< A_i, A_j > = \delta_{lj}$.

Let $W = L(S)$, then $W \neq V$ as $v = \left\{\frac{1}{n^2}\right\} \in V$ and $v \notin L(S)$.

[In fact $L(S)$, is the set of those sequences whose only finite number of entries are non zero].

Also $x \in W^{\perp} \Rightarrow < x, w > = 0 \quad \forall\, w \in W$

$\Rightarrow < x, A_k > = 0 \quad \forall\, k = 1, 2, ...$

$\Rightarrow x_k = 0 \ \forall k$ where $x = (x_n)$

$\Rightarrow x = 0$ or that $W^{\perp} = \{0\}$

So $V \neq W \oplus W^{\perp} = W$.

Notice V is not *F.D.V.S.* by theorem 35.

Problem 37: *If W is a subspace of V and $v \in V$ satisfies*

$$(v, w) + (w, v) \leq (w, w) \text{ for all } w \in W$$

prove that $(v, w) = 0$ for all $w \in W$, where V is an inner product space over F.

Solution: Let n be a +ve integer

Then $w \in W \Rightarrow \frac{w}{n} \in W$

$$\therefore \quad \left(v, \frac{w}{n}\right) + \left(\frac{w}{n}, v\right) \leq \left(\frac{w}{n}, \frac{w}{n}\right)$$

$$\therefore \quad (v, w) + (w, v) \leq \frac{1}{n}\ (w, w)$$

Let $n \to \infty$

Then $(v, w) + (w, v) \leq 0$ for all $w \in W$

$(v, -w) + (-w, v) \leq 0$ for all $w \in W$

$\Rightarrow -[(v, w) + (w, v)] \leq 0$ for all $w \in W$

$\Rightarrow (v, w) + (w, v) \geq 0$ for all $w \in W$

$\Rightarrow (v, w) + (w, v) = 0$ for all $w \in W$

If $F \subseteq \mathbf{R}$, then $(w, v) = (v, w)$

$\Rightarrow (v, w) + (v, w) = 0$

$\Rightarrow 2(v, w) = 0$ for all $w \in W$

$\Rightarrow (v, w) = 0$ for all $w \in W$

If $F \subseteq \mathbf{C}$, then $(v, iw) + (iw, v) = 0$ for all $w \in W$

$\Rightarrow -i\,(v, w) + i\,(w, \bar{z}) = 0$ for all $w \in W$

$\Rightarrow -i\,[z - \bar{z}] = 0,\ z = (v, w) = x + iy$

$\Rightarrow -i(2iy) = 0$
$\Rightarrow y = 0$
$\Rightarrow z = (v, w) = \text{real} \quad \text{for all } w \in W$
$\Rightarrow (v, w) + (v, w) = 0$
$\Rightarrow 2(v, w) = 0$
$\Rightarrow (v, w) = 0 \quad \text{for all } w \in W.$

Problem 38: *If V is a finite dimensional inner product space and $f \in V$, prove that $\exists\ u_0 \in V$ s.t., $f(v) = (v, u_0)$ for all $v \in V$. Also show that u_0 is uniquely determined.*

Solution: Let $\{v_1, ..., v_n\}$ be an orthonormal basis for V. Let $v \in V$.

Then $v = \alpha_1 v_1 + ... + \alpha_n v_n, \quad \alpha_i \in F$

Let $f(v_i) = \beta_i, \quad i = 1, 2, ..., n$

Define $u_0 = \overline{\beta_1}\, v_1 + ... + \overline{\beta_n}\, v_n \in V$

Then $(v, u_0) = (\alpha_1 v_1 + ... + \alpha_n v_n, \overline{\beta_1}\, v_1 + ... + \overline{\beta_n}\, v_n)$
$= \alpha_1\beta_1 + ... + \alpha_n\beta_n \quad \text{as } (v_i, v_j) = \delta_{ij}$
$= f(v) \quad \text{for all } v \in V$

Suppose $\exists\ u_0' \in V \text{ s.t. } f(v) = (v, u_0')$

Then $(v, u_0) = (v, u_0') \text{ for all } v \in V$
$\Rightarrow (v, u_0 - u_0') = 0 \text{ for all } v \in V$
$\Rightarrow (u_0 - u_0', u_0 - u_0') = 0$
$\Rightarrow u_0 = u_0'$

$\therefore\ u_0$ is uniquely determined.

Problem 39: *Let A be an $n \times n$ symmetric matrix and suppose that $\mathbf{R}^n$ has the standard inner product. Prove that if $(u, uA) = (u, u)$ for all u in $\mathbf{R}^n$, then $A = I$.*

Solution: Let $A = (a_{ij})$. Take $u = \in_1 = (1, 0, ..., 0)$

Then $(\in_1, \in_1 A) = (\in_1, \in_1)$

Therefore $(\in_1 (a_{11}, a_{21}, ..., a_{n1})) = 1$

implies $a_{11} = 1$

Similarly, Take $\in_i = u$, then $a_{ii} = 1$ for all i.

So, the diagonal elements of A are 1.

Now take $u = \in_1 - \in_2 = (1, -1, 0, ... 0)$

Then $(u, u) = 2$

and $(\in_1 - \in_2, (\in_1 - \in_2)A)$
$= (\in_1 - \in_2, (a_{11} - a_{12}, a_{12} - a_{22}, ..., a_{1n} - a_{2n}))$
$= 1 - a_{12} - a_{12} + 1$

So, $a_{12} = 0$

Similarly $a_{13} = 0, ..., a_{1n} = 0$

In this way, all entries other than diagonal would be 0.

Hence $A = I$.

Problem 40: *Let* $\mathbf{R}^n$ *be an inner product space with the standard inner product. Let T be a linear operator on* $\mathbf{R}^n$. *Show that for any vector u in* $\mathbf{R}^n$, $\| T(u) \| = \| u \|$ *if and only if* $(T(u), T(v)) = (u, v)$ *for all u, v in* $\mathbf{R}^n$. *Such a linear operator is said to preserve inner products.*

Solution: Let $\| T(u) \| = \| u \|$ for all u in $\mathbf{R}^n$

Then $\| T(u + v) \| = \| u + v \|$ for all u, v in $\mathbf{R}^n$

So $(T(u) + T(v), T(u) + T(v)) = (u + v, u + v)$

which implies $(T(u), T(u)) + ((T(u), T(v)) + (T(u), T(v)) + (T(v), T(u))$

$= (u, u) + (v, v) + (u, v) + (v, u)$

So, $(T(u), T(v)) = (u, v)$ for all u, v in $\mathbf{R}^n$

Conversely, let $(T(u), T(v)) = (u, u)$ for all u, v in $\mathbf{R}^n$

Then $(T(u), T(u)) = (u, v)$ for all u in $\mathbf{R}^n$

So, $\| T(u) \|^2 = \| u \|^2$

or $\| T(u) \| = \| u \|$ for all u in $\mathbf{R}^n$

Exercises

Throughout these exercises V stands for inner product space with inner product (,).

1. Show that $(x, z) = (y, z)$ for all $z \in V \Rightarrow x = y$.

2. Consider standard inner product on $\mathbf{R}^2$.

Suppose $\alpha = (1, 2)$, $\beta = (-1, 1) \in \mathbf{R}^2$. If $\gamma \in \mathbf{R}^2$ be s.t., $(\alpha, \gamma) = -1$ and $(\beta, \gamma) = 3$, find γ.

3. Show that for any $\alpha \in \mathbf{R}^2$

$$\alpha = (\alpha, \in_1)\in_1 + (\alpha, \in_2)\in_2$$

where $\in_1 = (1, 0)$, $\in_2 = (0, 1)$.

4. Let $u = (x_1, x_2)$ and $v = (y_1, y_2) \in R^2$

(*i*) Verify that the following is an inner product on $\mathbf{R}^2$

$$(u, v) = x_1y_1 - 2x_1y_2 - 2x_2y_1 + 5x_2y_2$$

(*ii*) For what values of k is the following an inner product on $\mathbf{R}^2$

$$(u, v) = x_1y_1 - 3x_1y_2 - 3x_2y_1 + kx_2y_2.$$ (**Ans**. $k > 9$)

(*iii*) For what values of $a, b, c, d \in \mathbf{R}$ is the following an inner product on $\mathbf{R}^2$.

$$(u, v) = ax_1y_1 + cx_1y_2 + dx_2y_1 + bx_2y_2$$

(**Ans**. $c^2 < ab$, $a \geq 0$, $b \geq 0$, $c = d$)

5. Show that $| \| x \| - \| y \| | \leq \| x - y \|$ for all $x, y \in V$.

[**Hint:** $\| x \| = \| x - y + y \|$]

6. Let W_1 and W_2 be subspaces of a finite dimensional inner product space V. Show that

(*i*) $(W_1 + W_2)^{\perp} = W_1^{\perp} \cap W_2^{\perp}$ (*ii*) $(W_1 \cap W_2)^{\perp} = W_1^{\perp} + W_2^{\perp}$

7. Obtain an orthonormal basis w.r.t. standard inner product for the subspace of $\mathbf{R}^4$ generated by (1, 0, 2, 0) and (1, 2, 3, 1).

$$\left(\textbf{Ans.}\left\{\left(\frac{1}{\sqrt{5}}, 0, \frac{2}{\sqrt{5}}, 0\right), \left(\frac{-2\sqrt{26}}{5\sqrt{5}}, \frac{2\sqrt{26}}{\sqrt{5}}, \frac{\sqrt{26}}{5\sqrt{5}}, \frac{\sqrt{26}}{\sqrt{5}}\right)\right\}\right)$$

8. Obtain an orthonormal basis for V, the space of all real polynomials of degree at most 2, the inner product defined by

$$(f, g) = \int_0^1 f(x)\, g(x)\, dx$$

$$\left(\textbf{Ans.}\left\{1, \sqrt{12}\ x - \frac{1}{2}\right), 180\left\{x^2 - x + \frac{1}{6}\right\}\right\}\right)$$

9. Let $\theta_1, \theta_2, \ldots, \theta_n$ and $\lambda_1, \lambda_2, \ldots, \lambda_n$ be positive real members such that $\theta_1 + \theta_2 + \ldots + \theta_n = 1$. Show that

$$\left(\sum_1^n \theta_i \lambda_i\right) \left(\sum \theta_i \lambda_i^{-1}\right) \geq 1$$

[**Hint**: let $\theta = (\sqrt{\theta_1\lambda_1}, \ldots, \sqrt{\theta_n\lambda_n}) \in \mathbf{R}^n$

$$\lambda = (\sqrt{\theta_1\lambda_1^{-1}}, \ldots, \sqrt{\theta_n\lambda_n^{-1}}) \in \mathbf{R}^n$$

and use Cauchy-Schwarz inequality]

10. Let $\{u_1, \ldots, u_r\}$ be an orthonormal set in V. Show that for any $v \in V$, the vector

$$w = v - (v, u_1)\, u_1 - \ldots - (v, u_r)\, u_r$$

is orthogonal to each of the u_i.

11. Let W be the set of real valued functions $y = f(x)$ satisfying $\dfrac{d^2y}{dx^2} + 4y = 0$. Prove that W is two dimensional real vector space.

Define $(y, z) = \int_0^\pi yzdz$ in W. Find an orthonormal basis of W.

$$\left(\textbf{Ans.}\left\{\frac{\sqrt{2}}{\pi}\sin 2x, \frac{\sqrt{2}}{\pi}\cos 2x\right\}\right)$$

12. Let V be the vector space of real valued functions $y = f(x)$ satisfying

$$\frac{d^3y}{dx^3} - \frac{6d^2y}{dx^2} + 11\frac{dy}{dx} - 6y = 0$$

Prove that V is a dimensional vector space over R. Define

$$(f, g) = \int_{-\infty}^0 fgdx \text{ in } V$$

Find an orthonormal basis of V over R.

(**Ans.** $\sqrt{2}\, e^x$, $2\,(3e^{2x} - 2e^x)$, $(3e^x - 12e^{2x} - 10e^{3x})\sqrt{6}$)

A Quick Look at what's been done

- Definition, examples and elementary properties of vector spaces over a field discussed.
- A non-empty subset of a vector space is said to form a **subspace** if it forms a vector space under the operations of the parent space. A non-empty subset W of $V(F)$ is a subspace iff $\alpha x + \beta y \in W$ for all $x, y \in W$ and $\alpha, \beta \in F$.
- Intersection(sum) of subspaces is a subspace but union is not.
- If W is a subspace of $V(F)$ then the set of all cosets of W in V forms a vector space called the **quotient space**of V by W and is denoted by V/W.
- If V and$U$ be two vector spaces over the same field F then a mapping T: $V \to U$ is called a **homomorphism** or a **linear transformation** (L.T.) if $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)\ \forall\ x, y \in V$ and $\alpha, \beta \in F$.
- **Kernel** of a homomorphism T contains all those members that are mapped to 0; and it is called the **null space** of T. Ker $T = \{0\}$ iff T is one-one. Range of T is defined to be $\{ T(x) \mid x \in V \} = R_T$.
- **Fundamental theorem of homomorphism** for vector spaces states that if $T : V \to U$ be a L.T., then $V/\text{Ker } T \cong R_T$.
- Elements of the type $\Sigma a_i v_i$, where $a_i \in F$, $v_i \in V$ are called *linear combinations* of v_i over F. The set of all linear combinations of finite sets of elements of S is called **linear span** of S, where S is a non-empty subset of V and is denoted by $L(S)$.
- If $V = L(S)$, we say S spans (or generates) V. A vector space V is said to be **finite-dimensional** (over F) if there exists a finite subset S of V such that $V = L(S)$. We use the notation *F.D.V.S.* for a finite-dimensional vector space.
- **Linearly dependent** and **linearly independent** elements are defined, followed by some results satisfied by them. A subset S of a vector space $V(F)$ is called a **basis** of V if S consists of L.I. elements and S spans V.
- Any basis of a *F.D.V.S.* is finite, and any two bases have the same number of elements. A *F.D.V.S.* V is said to have **dimension** n if n is the number of elements in any basis of V.
- Two finite-dimensional vector spaces over F are isomorphic iff they have same dimension.
- If W is a subspace of a *F.D.V.S.* V, then dim V/W =dim V – dim W.
- If A, B are two subspaces of a *F.D.V.S.* V, then
  $\dim(A + B) = \dim A + \dim B - \dim(A \cap B)$.
- **Inner product spaces**, **norm** of a vector, **orthogonality** and **orthonormal vectors** are defined and discussed in later part of the chapter.
- **Gram-Schmidt** orthogonalization process says that every finite dimensional inner product space has an orthonormal basis.
- **Cauchy-Schwarz** inequality and **Bessel's** inequality are proved.

11

Linear Transformations

Introduction

We defined a linear transformation (homomorphism) in the previous chapter and proved a few results pertaining to it, including a few on isomorphisms. We now come back to it and study it in a little more detail. To recall the definition, by a linear transformation (*L.T.*) we mean a map $T : V \to W$, s.t., $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ where $x, y \in V$, $\alpha, \beta \in F$ and V, W are vector spaces over the field F. We urge the reader to go through the definitions and results done earlier, especially on kernel and range of a *L.T.* Also, we'll be dealing with vector spaces that are finite dimensional, unless mentioned otherwise.

Theorem 1: *A L.T.* $T : V \to V$ *is one-one iff* T *is onto.*

Proof: Let $T : V \to V$ be one-one. Let dim $V = n$.

Let $\{v_1, v_2, ..., v_n\}$ be a basis of V, then $\{T(v_1), ..., T(v_n)\}$ will also be a basis of V as

$$\alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0$$

$$\Rightarrow \quad T(\alpha_1 v_1 + ... + \alpha_n v_n) = T(0) \quad (T \text{ a } L.T.)$$

$$\Rightarrow \quad \alpha_1 v_1 + ... + \alpha_n v_n = 0 \quad (T \text{ is 1-1})$$

$$\Rightarrow \quad \alpha_i = 0 \text{ for all } i$$

thus $T(v_1)$, ... $T(v_n)$ are *L.I.* and as dim $V = n$ the result follows (Theorem done earlier).

Let now $v \in V$ be any element

then $v = a_1 T(v_1) + a_2 T(v_2) + ... + a_n T(v_n) \quad a_i \in F$

$= T(a_1 v_1 + ... + a_n v_n)$

$= T(v')$ for some v'

Hence T is onto.

Conversely, let T be onto.

Here again we show that if $\{v_1, v_2, ... v_n\}$ is a basis of V then so also is $\{T(v_1), T(v_2), ..., T(v_n)\}$

For any $v \in V$, since T is onto, $\exists$ some $v' \in V$ s.t.,

$$T(v') = v$$

Again $v' \in V$ means $v' = \sum \alpha_i v_i \quad \alpha_i \in F$

$\therefore \quad v = T(v') = T(\sum \alpha_i v_i) = \sum \alpha_i T(v_i)$

$\Rightarrow \quad T(v_1), T(v_2), ..., T(v_n)$ span V

and as dim $V = n$, $\{T(v_1), ..., T(v_n)\}$ forms a basis of V.

Now if $v \in$ Ker T be any element

then $T(v) = 0$

$\Rightarrow \quad T(\Sigma \alpha_i v_i) = 0$

$\Rightarrow \quad \Sigma \alpha_i T(v_i) = 0$

$\Rightarrow \quad \alpha_i = 0$ for all i as $T(v_1), ..., T(v_n)$ are *L.I.*

$\Rightarrow \quad v = \Sigma \alpha_i v_i = 0$

$\Rightarrow$ Ker $T = \{0\} \Rightarrow T$ is 1-1.

Theorem 2: *Let V and W be two vector spaces over F. Let $\{v_1, v_2, ..., v_n\}$ be a basis of V and $w_1, w_2, ..., w_n$ be any vectors in W (not essentially distinct). Then there exists a unique L.T*

$$T : V \to W \text{ s.t., } T(v_i) = w_i \quad i = 1, 2, ..., n.$$

Proof: Let $v \in V$ be any element, then $v = \sum_{i=1}^{n} \alpha_i v_i , \quad \alpha_i \in F$

as $\{v_1, v_2, ..., v_n\}$ is a basis of V.

Define $T : V \to W$ s.t.,

$$T(v) = \Sigma \alpha_i w_i$$

Then T is a linear transformation (verify!).

Clearly here, $T(v_i) = T(ov_1 + ... + 1 . v_i + ... + ov_n) = 1w_i$ for all i

To show uniqueness let T' be any other *L.T.* from $V \to W$ s.t.

$$T'(v_i) = w_i$$

Let $v \in V$ be any element, then $v = \Sigma \alpha_i v_i$

$$T'(v) = T'(\Sigma \alpha_i v_i) = \Sigma \alpha_i T'(v_i) = \Sigma \alpha_i w_i = T(v)$$

Hence $T' = T$.

Thus we notice that a linear transformation is completely determined by its values on the elements of a basis.

Definition: Let $T : V \to W$ be a *L.T.*

then we define Rank of T = dim Range $T = r(T)$

Nullity of T = dim Ker $T = \nu(T)$.

Theorem 3: (Sylvester's Law) : *Let $T : V \to W$ be a L.T., then*

$$\textit{Rank } T + \textit{Nullity } T = \dim V.$$

Proof: Let $\{x_1, x_2, ..., x_m\}$ be a basis of Ker T then $\{x_1, x_2, ..., x_m\}$ being *L.I.* in Ker T will be *L.I.* in V. Thus it can be extended to form a basis of V.

Let $\{x_1, x_2, ..., x_m, v_1, v_2, ..., v_n\}$ be the extended basis of V.

Then dim Ker T = nullity of $T = m$

dim $V = m + n$

we show $\{T(v_1), T(v_2), ..., T(v_n)\}$ is a basis of Range T

Now $\alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0$

$\Rightarrow T(\alpha_1 v_1 + ... + \alpha_n v_n) = 0$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 ... + \alpha_n v_n \in$ Ker T

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = \beta_1 x_1 + ... + \beta_m x_m$

or $\alpha_1 v_1 + ... + \alpha_n v_n + (-\beta_1) x_1 + ... + (-\beta_m) x_m = 0$

$\Rightarrow \alpha_1 = \alpha_2 = ... = \beta_1 = ... = \beta_m = 0$

$\Rightarrow \alpha_i = 0$ for all i

i.e., $\{T(v_1), T(v_2), ..., T(v_n)\}$ is *L.I.*

Now if $T(v) \in$ Range T be any element then as $v \in V$

$v = a_1 x_1 + ... + a_m x_m + b_1 v_1 + ... + b_n v_n \quad a_i, b_j \in F$

$\therefore \quad T(v) = a_1 T(x_1) + ... + a_m T(x_m) + b_1 T(v_1) + ... + b_n T(v_n)$

$= 0 + ... + 0 + b_1 T(v_1) + ... + b_n T(v_n)$ [as $x_i \in$ Ker T]

or that $T(v)$ is a linear combination of $T(v_1), ..., T(v_n)$

which, therefore, form a basis of Range T.

$\therefore$ dim Range $T = n =$ rank T

which proves the theorem.

Theorem 4: *If $T : V \to V$ be a L.T. Show that the following statements are equivalent.*

(*i*) *Range $T \cap$ Ker $T = \{0\}$*

(*ii*) *If $T(T(v)) = 0$ then $T(v) = 0$, $v \in V$*

Proof: (*i*) $\Rightarrow$ (*ii*)

$T(T(v)) = 0 \Rightarrow T(v) \in$ Ker T

Also $T(v) \in$ Range T (by definition)

$\Rightarrow T(v) = 0$

(*ii*) $\Rightarrow$ (*i*)

Let $x \in$ Range $T \cap$ Ker T

$\Rightarrow x \in$ Range T and $x \in$ Ker T

$\Rightarrow x = T(v)$ for some $v \in V$

and $T(x) = 0$

$x = T(v) \Rightarrow T(x) = T(T(v))$

$\Rightarrow 0 = T(T(v))$

$\Rightarrow T(v) = 0$ (given condition)

$\Rightarrow v = 0.$

Algebra of Linear Transformations

Let V and W be two vector spaces over the same field F. Let $T : V \to W$ and $S : V \to W$ be two linear transformations. We define $T + S$, the sum of T and S by

$T + S : V \to W$, s.t.

$(T + S)v = T(v) + S(v), \quad v \in V$

Then $T + S$ is also a *L.T.* from $V \to W$ as

$$\begin{aligned}(T + S)(\alpha x + \beta y) &= T(\alpha x + \beta y) + S(\alpha x + \beta y)\\ &= \alpha T(x) + \beta T(y) + \alpha S(x) + \beta S(y)\\ &= \alpha(T + S)x + \beta(T + S)y\end{aligned}$$

Again for $\alpha \in F$, we define the product of a *L.T.* $T : V \to W$ with α, by $(\alpha T) : V \to W$ s.t., $(\alpha T)v = \alpha(T(v))$.

It is easy to see that αT is a also a *L.T.* from $V \to W$. Let Hom (V, W) be the set of all linear transformations from $V \to W$. Then we show Hom (V, W) forms a vector space over F under the addition and scalar multiplication as defined above.

We have already seen that when $T, S \in$ Hom (V, W), $\alpha \in F$ then $T + S$, $\alpha T \in$ Hom (V, W), thus closure holds for these operations. We verify some of the other conditions in the definition.

$$(T + S)v = T(v) + S(v) = S(v) + T(v) = (S + T)v \text{ for all } v \in V$$

$$\Rightarrow \quad T + S = S + T \text{ for all } S, T \in \text{Hom } (V, W)$$

The map $O : V \to W$, s.t.,$O(v) = 0$ is a *L.T.* and

$$(T + O)v = T(v) + O(v) = T(v) = (O + T)v \text{ for all } v$$

thus O is zero of Hom (V, W)

For any $T \in$ Hom (V, W), the map $(-T) : V \to W$, s.t.,

$$(-T)v = -T(v)$$

will be additive inverse of T.

$$\begin{aligned}\text{Again,} \quad [\alpha(T + S)]v &= \alpha[(T + S)v] = \alpha[T(v) + S(v)] = \alpha T(v) + \alpha S(v)\\ &= (\alpha T)v + (\alpha S)v = (\alpha T + \alpha S)v \quad \text{for all } v \in V\end{aligned}$$

$$\Rightarrow \quad \alpha(T + S) = \alpha T + \alpha S$$

$$[(\alpha\beta)T]v = (\alpha\beta)T(v) = \alpha[\beta T(v)] = [\alpha(\beta T)]v \quad \text{for all } v$$

$$\Rightarrow \quad (\alpha\beta)T = \alpha(\beta T)$$

$$(1T)v = 1 \,.\, T(v) = T(v) \quad \text{for all } v$$

$$\Rightarrow \quad 1 \,.\, T = T$$

Hence one notices that Hom (V, W) forms a vector space over F.

Note: The notation $L(V, W)$ is also used for denoting Hom (V, W).

Definition: Product (composition) of two linear transformations

Let V, W, Z be three vector spaces over a field F

Let $T : V \to W$, $S : W \to Z$ be *L.T.*

We define $ST : V \to Z$, s.t.,

$(ST)v = S(T(v))$

then ST is a linear transformation (verify!), called product of S and T.

Note: TS may not be defined and even if it is defined it may not equal ST.

Definition: A *L.T.* $T : V \to V$ is called a *linear operator* on V, whereas a *L.T.* $T : V \to F$ is called a *linear functional*. We use notation T^2 for $T.T$ and $T^n = T^{n-1}T$ etc.

Theorem 5: *Let T, T_1, T_2 be linear operators on V, and let $I : V \to V$ be the identity map $I(v) = v$ for all v (which is clearly a L.T.) then*

(*i*) $IT = TI = T$

(*ii*) $T(T_1 + T_2) = TT_1 + TT_2$

$(T_1 + T_2)T = T_1T + T_2T$

(*iii*) $\alpha(T_1T_2) = (\alpha T_1)T_2 = T_1(\alpha T_2) \quad \alpha \in F$

(*iv*) $T_1(T_2T_3) = (T_1T_2)T_3$.

Proof: (*i*) Obvious.

(*ii*) $[T(T_1 + T_2)]x = T[(T_1 + T_2)x] = T[T_1(x) + T_2(x)]$

$= T(T_1(x)) + T(T_2(x)) = TT_1(x) + TT_2(x)$

$= (TT_1 + TT_2)x$

$\Rightarrow \quad T(T_1 + T_2) = TT_1 + TT_2$

Other result follows similarly.

(*iii*) $[\alpha(T_1T_2)]x = \alpha[(T_1T_2)x] = \alpha[T_1(T_2(x))]$

$[(\alpha T_1)T_2]x = (\alpha T_1)\ [T_2(x)] = \alpha[T_1(T_2(x)]$

$[T_1(\alpha T_2)]x = T_1(\alpha T_2)x = T_1(\alpha T_2(x)) = \alpha T_1(T_2(x))]$

Hence the result follows.

(*iv*) Follows easily by definition.

See exercises for the generalised version of above theorem.

Theorem 6: *Let V and W be two vector spaces (over F) of dim m and n respectively. Then Hom (V, W) has dim mn.*

Proof: Let $\{v_1, v_2, ..., v_m\}$ and $\{w_1, w_2, ..., w_n\}$ be basis of V and W respectively.

Define mappings $T_{ij} : V \to W$, s.t.

$$T_{ij}(v) = \alpha_i w_j \quad 1 \le i \le m, \quad 1 \le j \le n$$

where $v \in V$ is any element and therefore,

$v = \alpha_1 v_1 + \alpha_2 v_2 + ... \ \alpha_m v_m$ for some $\alpha_i \in F$

Note also that $T_{ij}(v_k) = 0$ if $k \neq i$

$= w_j$ if $k = i$

We show T_{ij} are *L.T.*

Let $x, y \in V$ then $x = \sum_1^m \alpha_i v_i, \quad y = \sum_1^m \beta_i v_i \quad \alpha_i, \beta_i \in F$

Now $T_{ij}(x + y) = T_{ij}[(\alpha_1 v_1 + ... + \alpha_m v_m) + (\beta_1 v_1 + ... + \beta_m v_m)]$

$= T_{ij}[(\alpha_1 + \beta_1)v_1 + ... + (\alpha_m + \beta_m)v_m]$

$$= T_{ij}(\gamma_1 v_1 + \ldots + \gamma_m v_m)$$
$$= \gamma_i w_j$$
$$= (\alpha_i + \beta_i) w_j = \alpha_i w_j + \beta_i w_j = T_{ij}(x) + T_{ij}(y)$$

Also, $T_{ij}(\lambda x) = T_{ij}(\lambda(\alpha_1 v_1 + \ldots + \alpha_m v_m))$
$$= T_{ij}(\lambda\alpha_1 v_1 + \ldots + \lambda\alpha_m v_m)$$
$$= (\lambda\alpha_i) w_j = \lambda(\alpha_i w_j) = \lambda T_{ij}(\Sigma\alpha_i v_i)$$
$$= \lambda T_{ij}(x)$$

Hence $T_{ij} \in$ Hom (V, W). We claim $S = \{T_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ forms a basis of Hom (V, W)

Suppose

$\beta_{11}T_{11} + \beta_{12}T_{12} + \ldots + \beta_{1n}T_{1n} + \beta_{21}T_{21} + \beta_{22}T_{22} + \ldots + \beta_{2n}T_{2n} + \ldots + \beta_{m1}T_{m1} + \beta_{m2}T_{m2} + \ldots + \beta_{mn}T_{mn} = 0$, $\beta_{ij} \in F$

[where 0 is, of course, zero of Hom (V, W)]

By operating on v_1, we get

$\beta_{11}T_{11}(v_1) + \beta_{12}T_{12}(v_1) + \ldots + \beta_{1n}T_{1n}(v_1) + \beta_{21}T_{21}(v_1) + \ldots = 0$

$\Rightarrow \beta_{11}w_1 + \beta_{12}w_2 + \ldots + \beta_{1n}w_n + 0 + \ldots + 0 + \ldots = 0$

But $w_1, w_2 \ldots, w_n$ are *L.I.*

$\Rightarrow \beta_{11} = \beta_{12} = \ldots \beta_{1n} = 0$

Similarly, by operating on v_2 we'll get $\beta_{21} = \beta_{22} = \ldots \beta_{2n} = 0$

Thus by operating on $v_3, v_4 \ldots$ we find that all the coefficients are zero and hence S is *L.I.*. So, $o(S) = mn$.

Let Now $T \in$ Hom (V, W) be any element, then

$T : V \to W$ is a *L.T.*

We show T is a linear combination of T_{ij}

Consider v_1, then $T(v_1) \in W$ and thus is a linear combination of $w_1, w_2, \ldots w_n$

Let $T(v_1) = \alpha_{11}w_1 + \alpha_{12}w_2 + \ldots + \alpha_{1n}w_n$

Put $T_0 = \alpha_{11}T_{11} + \alpha_{12}T_{12} + \ldots + \alpha_{1n}T_{1n} + \alpha_{21}T_{21} + \alpha_{22}T_{22} + \ldots + a_{mn}T_{mn}$

(where $\alpha_{11}, \alpha_{12} \ldots$ are, of course, the same as before)

Then $T_0(v_1) = \alpha_{11}T_{11}(v_1) + \alpha_{12}T_{12}(v_1) + \ldots$
$$= \alpha_{11}w_1 + \alpha_{12}w_2 + \alpha_{2n}w_n + 0 + 0 + \ldots + 0$$
$$\Rightarrow T_0(v_1) = T(v_1)$$

Similarly proceeding with $v_2, v_3, \ldots v_m$ we get

$$T_0(v_2) = T(v_2)$$
$$\ldots\ldots\ldots$$
$$T_0(v_m) = T(v_m)$$

Thus T_0 and T agree on all elements of the basis of V.

$\Rightarrow T_0$ and T agree on all elements of $V \Rightarrow T_0 = T$

But T_0 is a linear combination of members of S

$\Rightarrow T$ is a linear combination of members of S

$\Rightarrow S$ spansHom (V, W)

or that S forms a basis of Hom (V, W)

Hence dim Hom $(V, W) = mn$.

Cor.: Obviously dim Hom $(V, V) = m^2$ where dim $V = m$ and

dim Hom $(V, F) = m \cdot 1 = m$ as dim $F(F) = 1$ as F is generated by 1 and thus $\{1\}$ is a basis of $F(F)$.

Problem 1: *Find the range, Rank, Ker and nullity of the linear transformation*

$T : \mathbf{R}^3 \to \mathbf{R}^3$, *s.t.*,

$T(x, y, z) = (x + z, \quad x + y + 2z, \quad 2x + y + 3z)$

Solution: Let $(x, y, z) \in$ Ker T be any element, then

$$T(x, y, z) = (0, 0, 0)$$

$$\Rightarrow (x + z, \ x + y + 2z, \ 2x + y + 3z) = (0, 0, 0)$$

$$\Rightarrow x + 0 + z = 0$$

$$x + y + 2z = 0$$

$$2x + y + 3z = 0$$

Giving $x = -z, \ -z + y + 2z = 0$ *i.e.*, $y = -z$

Thus Ker T consists of all elements of the type $(x, x, -x) = x(1, 1, -1)$ where x is any real no. *i.e.*, Ker T is spanned by $(1, 1, -1)$ which is *L.I.* Note $(1, 1, -1) \in$ Ker T

Hence dim (Ker T) = 1 = nullity of T

Again, from def. of T, we notice elements of the types $(x + z, \ x + y + 2z, \ 2x + y + 3z)$ are in Range T

Now $(x + z, \ x + y + 2z, \ 2x + y + 3z) = (x + 0 + z, \ x + y + 2z, \ 2x + y + 3z)$

$$= (x, x, 2x) + (0, y, y) + (z, 2z, 3z)$$

$$= x(1, 1, 2) + y(0, 1, 1) + z(1, 2, 3)$$

Thus Range T is spanned by $\{(1, 1, 2), (0, 1, 1), (1, 2, 3)\}$

Since $(1, 1, 2) + (0, 1, 1) = (1, 2, 3)$ we find these vectors are *L.D.* So dim Range $T \leq 2$

Again as $(1, 1, 2)$ and $(0, 1, 1)$ are *L.I.* we find

dim Range $T = 2 =$ Rank T.

Problem 2: *Find the range, rank, Ker and nullity of the following linear transformations*

(*a*) $T : \mathbf{R}^2 \to \mathbf{R}^3$ s.t., $T(x_1, x_2) = (x_1, x_1 + x_2, x_2)$

(*b*) $T : \mathbf{R}^4 \to \mathbf{R}^3$ s.t., $T(x_1, x_2, x_3, x_4) = (x_1 - x_4, x_2 + x_3, x_3 - x_4)$

Solution: (*a*) From definition of T, we notice elements of the type $(x_1, x_1 + x_2, x_2)$ will have pre images in $\mathbf{R}^2$ *i.e.*, elements of this type are in Range T.

Now $(x_1, x_1 + x_2, x_2) = (x_1 + 0, x_1 + x_2, 0 + x_2)$

$$= (x_1, x_1, 0) + (0, x_2, x_2)$$

$$= x_1(1, 1, 0) + x_2(0, 1, 1)$$

or that Range T is spanned by $\{(1, 1, 0), (0, 1, 1)\}$ and since

$$\alpha_1(1, 1, 0) + \alpha_2(0, 1, 1) = (0, 0, 0)$$

$$\Rightarrow \alpha_1 = \alpha_2 = 0$$

these are *L.I.* and thus form a basis of Range T

$$\Rightarrow \text{Rank } T = \dim \text{Range } T = 2.$$

Again $(x_1, x_2) \in \text{Ker } T \Rightarrow T(x_1, x_2) = (0, 0, 0)$

$$\Rightarrow (x_1, x_1 + x_2, x_2) = (0, 0, 0)$$

$$\Rightarrow x_1 = 0, x_1 + x_2 = 0, x_2 = 0$$

$$\Rightarrow x_1 = x_2 = 0$$

$$\Rightarrow \text{Ker } T = \{(0, 0)\}$$

Also then nullity $T = \dim \text{Ker } T = 0$.

(*b*) From defintion of T, we find elements of the type $(x_1 - x_4, x_2 + x_3, x_3 - x_4)$ have pre image in $\mathbf{R}^4$.

Now

$$(x_1 - x_4,\ x_2 + x_3,\ x_3 - x_4) = (x_1 + 0 + 0 - x_4,\ 0 + x_2 + x_3 + 0,\ 0 + 0 + x_3 - x_4)$$

$$= x_1(1, 0, 0) + x_2(0, 1, 0) + x_3(0, 1, 1) + x_4(-1, 0, -1)$$

or that Range T is spanned by

$\{(1, 0, 0), (0, 1, 0), (0, 1, 1), (-1, 0, -1)\}$

Since Range T is a subspace of $\mathbf{R}^3$ which has dim 3 these four elements cannot form basis of Range T.

In fact these are *L.D.*, elements as

$$(-1, 0, -1) + (1, 0, 0) + (0, 1, 0) + (0, 1, 1) = (0, 0, 0)$$

If we consider three members

$$(1, 0, 0), (0, 1, 0), (0, 1, 1)$$

we notice $\alpha_1(1, 0, 0) + \alpha_2(0, 1, 0) + \alpha_3(0, 1, 1) = (0, 0, 0)$

$$\Rightarrow \alpha_i = 0 \text{ for all } i$$

or that (1, 0, 0), (0, 1, 0) (0, 1, 1) are *L.I.*, and hence form basis of Range T

$\Rightarrow$ dim Range $T = 3$ = rank of T

one might notice here that as

$$(-1, 0, -1) = -1(1, 0, 0) - 1(0, 1, 0) - 1(0, 1, 1)$$

the elements (1, 0, 0), (0, 1, 0), (0, 1, 1) span Range T

Also then Range $T = \mathbf{R}^3$

Again $(x_1,\ x_2,\ x_3,\ x_4) \in \text{Ker } T \Rightarrow T(x_1,\ x_2,\ x_3,\ x_4) = (0, 0, 0)$

$$\Rightarrow x_1 - x_4 = 0$$

$$x_2 + x_3 = 0$$

$$x_3 - x_4 = 0$$

if we fix x_4, we get $x_1 = x_4,\ x_2 = -x_3 = -x_4,\ x_3 = x_4$

or that elements of the type $(x_4,\ -x_4,\ x_4,\ x_4)$ are in the Ker T

i.e., Ker T is spanned by (1, –1, 1, 1) (Note (1, – 1, 1, 1) $\in$ Ker T)

this being *L.I.* forms basis of Ker T

$\Rightarrow$ dim Ker $T = 1$

$\Rightarrow$ nullity of $T = 1$.

Problem 3: *Let F be a subfield of complex numbers and T a function from* $F^3 \to F^3$ *defined by*

$$T(x_1, x_2, x_3) = (x_1 - x_2 + 2x_3, \; 2x_1 + x_2, \; -x_1 - 2x_2 + 2x_3)$$

(*i*) *Show that T is a L.T.*

(*ii*) *What are the conditions on a, b, c such that* (*a, b, c*) *be in the null space of T? Find nullity of T.*

Solution: $T[(x_1, x_2, x_3) + (y_1, y_2, y_3)] = T(x_1 + y_1, x_2 + y_2, x_3 + y_3)$

$= (x_1 + y_1 - x_2 - y_2 + 2x_3 + 2y_3, \; 2x_1 + 2y_1 + x_2 + y_2,$

$-x_1 - y_1 - 2x_2 - y_2 + 2x_3 + 2y_3)$

Also $T(x_1, x_2, x_3) + T(y_1, y_2, y_3) = (x_1 - x_2 + 2x_3, \; 2x_1 + x_2, \; -x_1 - 2x_2 + 2x_3)$

$+ (y_1 - y_2 + 2y_3, \; 2y_1 + y_2, \; -y_1 - 2y_2 + 2y_3)$

$= (x_1 - x_2 + 2x_3 + y_1 - y_2 + 2y_3, \; 2x_1 + x_2 + 2y_1 + y_2$

$-x_1 - 2x_2 + 2x_3 - y_1 - 2y_2 + 2y_3)$

$= (x_1 + y_1 - x_2 - y_2 + 2x_3 + 2y_3, \; 2x_1 + 2y_1 + x_2 + y_2,$

$-x_1 - y_1 - 2x_2 - y_2 + 2y_3 + 2y_3)$

Thus $T((x_1, x_2, x_3) + (y_1, y_2, y_3)) = T(x_1, x_2, x_3) + T(y_1, y_2, y_3)$

It is easy to see that for any α

$$T(\alpha(x_1, x_2, x_3)) = \alpha T(x_1, x_2, x_3)$$

Thus T is a *L.T.*

Now if $(a, b, c) \in$ Ker T then $T(a, b, c) = (0, 0, 0)$

$\Rightarrow (a - b + 2c, \; 2a + b, \; -a - 2b + 2c) = (0, 0, 0)$

$\Rightarrow a - b + 2c = 0$

$2a + b = 0$

$-a - 2b + 2c = 0$

Since $\begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & 0 \\ -1 & -2 & 2 \end{vmatrix} = 0$

The above equations have a non zero solution.

Solving the equiations, we find

$$\begin{bmatrix} 1 & -1 & 2 \\ 2 & 1 & 0 \\ -1 & -2 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_2 \to R_2 - 2R_1, \; R_3 \to R_3 + R_1$

$$\begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -4 \\ 0 & -3 & 4 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_3 \to R_3 + R_2$

$$\begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -4 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow a - b + 2c = 0$

$3b - 4c = 0$

Since rank of coeficient matrix is 2, the number of *L.I.* solutions is $3 - 2 = 1$.

If we take $c = k$, we get $a = -\frac{2k}{3}$, $b = \frac{4k}{3}$, $c = k$ as solution of the given equations.

In other words a, b, c should satisfy the relation $\frac{a}{-2} = \frac{b}{4} = \frac{c}{4}$ for (a, b, c) to be in Ker T.

Now $(-2, 4, 3)$ is one member of Ker T and all other members would be multiples of this, *i.e.*, $\{(-2, 4, 3)\}$ generates ker T. Since $(-2, 4, 3)$ being non zero is *L.I.* $\{(-2, 4, 3)\}$ forms a basis of Ker T or that dim Ker T = nullity $T = 1$.

In fact, the result dim V = dim Range T + dim Ker T will then give us dim Range T = Rank $T = 2$ as dim V = dim $F^3 = 3$. (See exercises).

Problem 4: *If $T_1, T_2 \in$ Hom (V, W) then show that*

(*i*) $r(\alpha T_1) = r(T_1)$ *for all* $\alpha \in F$, $\alpha \neq 0$

(*ii*) $|r(T_1) - r(T_2)| \leq r(T_1 + T_2) \leq r(T_1) + r(T_2)$

where $r(T)$ means rank of T.

Solution: (*i*) $T_1 : V \to W$

thus $T_1(V)$ = range T_1, is a subspace of W

Now $(\alpha T_1)v = \alpha(T_1(v)) \in T_1(V)$ for all $v \in V$

$\Rightarrow (\alpha T_1)V \subseteq T_1(V)$ ...(1)

Again as $\alpha \neq 0$, α^{-1} exists and thus

$(\alpha^{-1}T_1)\ V \subseteq T_1(V)$

$\alpha(\alpha^{-1}T_1)V \subseteq \alpha T_1(V)$

$\Rightarrow T_1(V) \subseteq \alpha T_1(V) \Rightarrow T_1(V) = \alpha T_1(V)$ by (1)

$\Rightarrow$ dim $T_1(V)$ = dim $\alpha T_1(V)$

or $r(T_1) = r(\alpha T_1)$.

(*ii*) Since $(T_1 + T_2)x = T_1(x) + T_2(x)$ for all $x \in V$

$(T_1 + T_2)V \subseteq T_1(V) + T_2(V)$

$\Rightarrow$ dim $[(T_1 + T_2)V] \leq$ dim $[T_1(V) + T_2(V)]$

$\leq$ dim $T_1(V)$ + dim $T_2(V)$

$\Rightarrow r(T_1 + T_2) \leq r(T_1) + r(T_2)$

Again $T_1 = (T_1 + T_2) - T_2 = (T_1 + T_2) + (-T_2)$

$\Rightarrow r(T_1) = r[(T_1 + T_2) + (-T_2)]$

$\leq r(T_1 + T_2) + r(-T_2) = r(T_1 + T_2) + r(T_2)$

(using (1) $\alpha = -1$)

$\Rightarrow r(T_1) - r(T_2) \leq r(T_1 + T_2)$

Similarly $r(T_2) - r(T_1) \leq r(T_1 + T_2)$

$\Rightarrow |r(T_1) - r(T_2)| \leq r(T_1 + T_2) \leq r(T_1) + r(T_2)$.

Problem 5: *Let T be a linear operator on V. If $T^2 = 0$, what can you say about the relation of the range of T to the null space of T? Give an example of linear operator T of $\mathbf{R}^2$ such that $T^2 = 0$, but $T \neq 0$.*

Solution: $T^2 = 0 \Rightarrow T^2(v) = 0$ for all $v \in V$

$\Rightarrow T(T(V)) = 0$

$\Rightarrow T(v) \in$ Ker T for all $v \in V$

$\Rightarrow$ range $T \subseteq$ Ker T.

Define $T : \mathbf{R}^2 \to \mathbf{R}^2$, such that

$T(x_1, x_2) = (x_2, 0)$

then T is a linear operator (Verify!)

Since $T(2, 2) = (2, 0) \neq (0, 0)$

$T \neq 0$

But $T^2(x_1, x_2) = T(T(x_1, x_2)) = T(x_2, 0) = (0, 0)$

$\Rightarrow T^2 = 0$.

Problem 6: *Let T be a linear operator on V and let Rank T^2 =* Rank *T then show that Range $T \cap$ Ker $T = \{0\}$.*

Solution: $T : V \to V$, $T^2 : V \to V$

Rank $T^2 =$ dim $V -$ dim Ker T^2

$\Rightarrow$ dim Ker $T =$ dim Ker T^2

We claim Ker $T =$ Ker T^2

$x \in$ Ker $T \Rightarrow T(x) = 0 \Rightarrow T^2(x) = T(0) = 0$

$\Rightarrow x \in$ Ker $T^2 \Rightarrow$ Ker $T \subseteq$ Ker T^2

$\Rightarrow$ Ker $T =$ Ker T^2 (as they have same dim)

Now $x \in$ Range $T \cap$ Ker $T \Rightarrow x \in$ Range T and $x \in$ Ker T

$\Rightarrow T(x) = 0$, $x = T(y)$ for some $y \in V$

$\Rightarrow T(T(y)) = 0$

$\Rightarrow T^2(y) = 0$

$\Rightarrow y \in \text{Ker } T^2 = \text{Ker } T$
$\Rightarrow T(y) = 0 \Rightarrow x = 0$
$\Rightarrow \text{Ker } T \cap \text{Range } T = \{0\}$.

Invertible Linear Transformations

We recall that a map $T : V \to W$ is invertible iff it is 1-1 onto, and inverse of T is the map T^{-1}: $W \to V$ such that

$$T^{-1}(y) = x \Leftrightarrow T(x) = y$$

We show that inverse of a (1–1 onto) *L.T.* is also a *L.T.* Let $T : V \to W$ be a 1-1 onto *L.T.* and T^{-1}: $W \to V$ be its inverse.

We have to prove

$$T^{-1}(\alpha w_1 + \beta w_2) = \alpha T^{-1}(w_1) + \beta T^{-1}(w_2) \quad \alpha, \beta \in F, w_1, w_2 \in W$$

Since T is onto, for $w_1, w_2 \in W$, $\exists\ v_1, v_2 \in V$ such that $T(v_1) = w_1$, $T(v_2) = w_2$

$\Leftrightarrow v_1 = T^{-1}(w_1)$, $v_2 = T^{-1}(w_2)$

Now $T^{-1}(\alpha w_1 + \beta w_2) = T^{-1}(\alpha T(v_1) + \beta T(v_2))$
$= T^{-1}(T(\alpha v_1) + T(\beta v_2))$
$= T^{-1}(T(\alpha v_1 + \beta v_2))$
$= \alpha v_1 + \beta v_2$
$= \alpha T^{-1}(w_1) + \beta T^{-1}(w_2)$.

Definition: A *L.T.* $T : V \to W$ is called *non-singular* if Ker $T = \{0\}$ *i.e.* if T is 1-1.

Theorem 7: *A linear transformation $T : V \to W$ is non singular iff T carries each L.I. subset of V onto a L.I. subset of W.*

Proof: Let T be non-singular and $\{v_1, v_2 \ldots, v_n\}$ be a *L.I.* subset of V. we show $\{T(v_1), T(v_2) \ldots, T(v_n)\}$ is *L.I.* subset of W.

Now $\alpha_1 T(v_1) + \alpha_2 T(v_2) + \ldots + \alpha_n T(v_n) = 0 \quad \alpha_i \in F$
$\Rightarrow T(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0$
$\Rightarrow \alpha_1 v_1 + \ldots \alpha_n v_n \in \text{Ker } T = \{0\}$
$\Rightarrow \alpha_1 v_1 + \ldots \alpha_n v_n = 0$
$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2 \ldots, v_n$ are *L.I.*
Conversely, let $v \in \text{Ker } T$ be any element

Then $T(v) = 0$
$\Rightarrow \{T(v)\}$ is not *L.I.* in W
$\Rightarrow v$ is not *L.I.* in V. (by hypothesis)
$\Rightarrow v = 0 \Rightarrow \text{Ker } T = \{0\}$
$\Rightarrow T$ is non singular.

Theorem 8: *Let $T : V \to W$ be a L.T. where V and W are two F.D.V.S. with same dimension. Then the following are equivalent*

(*i*) *T is invertible*

(*ii*) *T is non singular* (*i.e.*, *T is* 1-1)

(*iii*) *T is onto* (*i.e., Range T = W*)

(*iv*) *If* $\{v_1, v_2, ..., v_n\}$ *is a basis of V then* $\{T(v_1), T(v_2), ..., T(v_n)\}$ *is a basis of W.*

Proof: (*i*) $\Rightarrow$ (*ii*) follows by definition.

(*ii*) $\Rightarrow$ (*iii*) T is non-singular

$\Rightarrow$ Ker $T = \{0\}$

$\Rightarrow$ dim Ker $T = 0$

Since dim Range T + dim Ker T = dim V, we get

dim Range T = dim V

$\Rightarrow$ dim Range T = dim W (given condition)

But Range T being a subspace of W, we find

Range $T = W$

(*iii*) $\Rightarrow$ (*i*) T onto means Range $T = W$

$\Rightarrow$ dim Range T = dim W = dim V

and as dim Range T + dim Ker T = dim V, we get

dim Ker $T = 0$

$\Rightarrow$ Ker $T = \{0\}$

or that T is 1-1 and as it is onto T will be invertible.

(*i*) $\Rightarrow$ (*iv*) T is invertible $\Rightarrow$ T is 1-1 onto

i.e., T is an isomorphism, so result follows as done in theorem 24, chapter 10.

(*iv*) $\Rightarrow$ (*i*)

Let $\{T(v_1), ..., T(v_n)\}$ be basis of W where $\{v_1, ...v_n\}$ is basis of V. Any $w \in W$ can be put as

$w = \alpha_1 T(v_1) + ... + \alpha_n T(v_n)$

$= T(\alpha_1 v_1 + ... + \alpha_n v_n) = T(v)$ for some $v \in V$

$\therefore$ T is onto. Thus (*iii*) holds.

Hence (*i*) holds.

Problem 7: *Let T be a linear operator on* $\mathbf{R}^3$, *defined by*

$$T(x_1, x_2, x_3) = (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3)$$

show that T is invertible and find the rule by which T^{-1} *is defined.*

Solution: $T : \mathbf{R}^3 \to \mathbf{R}^3$

Let $(x_1, x_2, x_3) \in$ Ker T be any element

Then $T(x_1, x_2, x_3) = (0, 0, 0)$

$\Rightarrow (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3) = (0, 0, 0)$

$\Rightarrow 3x_1 = 0, \; x_1 - x_2 = 0, \; 2x_1 + x_2 + x_3 = 0$

$\Rightarrow x_1 = x_2 = x_3 = 0$ or that Ker $T = \{(0, 0, 0)\}$

$\Rightarrow T$ is non singular and thus invertible (See theorem 8)

Now if (z_1, z_2, z_3) be any element of $\mathbf{R}^3$, then (x_1, x_2, x_3) will be its image under T if

$$T(x_1, x_2, x_3) = (z_1, z_2, z_3)$$
$$\Rightarrow \quad 2x_1 = z_1$$
$$x_1 - x_2 = z_2$$
$$2x_1 + x_2 + x_3 = z_3$$

which give $x_1 = \frac{z_1}{3}$, $x_2 = \frac{z_1}{3} - z_2$, $z_3 = z_3 - z_1 + z_2$

Hence $T^{-1} : \mathbf{R}^3 \to \mathbf{R}^3$ is defined by

$$T^{-1}(z_1, z_2, z_3) = \left(\frac{z_1}{3}, \frac{z_1}{3} - z_2, z_3 - z_1 + z_2 \right)$$

Problem 8: *If $T : V \to V$ is a L.T., such that T is not onto, then show that there exists some $0 \neq v$ in V s.t., $T(v) = 0$.*

Solution: Since T is not onto, it is not 1-1 (theorem done)

Suppose $\exists$ no $0 \neq v \in V$ s.t. $T(v) = 0$

Then $T(v) = 0$ only when $v = 0$

$\Rightarrow$ Ker $T = \{0\} \Rightarrow T$ is 1-1, a contradiction.

Theorem 9: *Let $T : V \to W$ and $S : W \to U$ be two linear transformations. Then*

(*i*) *If S and T are one-one onto then ST is one-one onto and $(ST)^{-1} = T^{-1} S^{-1}$.*

(*ii*) *If ST is one-one then T is one-one*

(*iii*) *If ST is onto then S is onto.*

Proof: (*i*) Since S and T are 1-1 onto, S^{-1} and T^{-1} exist.

Let $ST(x) = ST(y)$

Then $S(T(x)) = S(T(y))$

$\Rightarrow T(x) = T(y)$ as S is 1-1

$\Rightarrow x = y$ as T is 1-1

$\Rightarrow ST$ is 1-1.

Again $ST : V \to U$, let $u \in$ U be any element then as S in onto, $\exists\ w \in W$ s.t., $S(w) = u$ and as $T : V \to W$ is onto $\exists\ v \in V$ s.t., $T(v) = w$

Now $T(v) = w \Rightarrow S(T(v)) = S(w) \Rightarrow ST(v) = u$

or that ST is onto.

Also $(ST)(T^{-1}S^{-1}) = S(T(T^{-1}S^{-1})) = S(TT^{-1})S^{-1} = S(IS^{-1}) = SS^{-1} = I$

Similarly $(T^{-1}S^{-1})(ST) = T^{-1}(S^{-1}(ST)) = T^{-1}(S^{-1}S)T = T^{-1}(IT) = T^{-1}T = I$

Showing that $(ST)^{-1} = T^{-1}S^{-1}$.

(*ii*) Let $v \in$ Ker T be any element

Then $T(v) = 0$

$\Rightarrow S(T(v)) = S(0)$

$\Rightarrow ST(v) = 0$

$\Rightarrow v \in \text{Ker } ST$ and $\text{Ker } ST = (0)$ as ST is 1-1

$\Rightarrow v = 0 \Rightarrow \text{Ker } T = (0) \Rightarrow T$ is 1-1.

(*iii*) Let $u \in U$ be any element. Since $ST : V \to U$ is onto, $\exists$ some $v \in V$ s.t., $ST(v) = u$

i.e., $S(T(v)) = u$

Let $T(v) = w$ and $w \in W$ such that

$S(w) = u$

Then S is onto.

Problem 9: *In the above theorem show that if ST is 1-1 onto then T is 1-1 and S is onto. Again, if V, W, U are of same dimension and ST is one-one onto then so are S and T.*

Solution: First part of the problem follows by (*ii*) and (*iii*) of theorem 9.

Let now $\dim V = \dim W = \dim U$

The result then follows by using theorem 8 we proved earlier that if $T : V \to W$ is a *L.T.* where $\dim V = \dim W$ then T is 1-1 iff T is onto.

Problem 10: *Let T be a linear operator on F.D.V.S. V. Suppose there is a linear operator U on V such that TU = I. Show that T is invertible and* $T^{-1} = U$.

Solution: We have $T : V \to V$, $U : V \to V$ s.t., $TU = I$ we claim U is 1-1.

Let $U(x) = U(y)$

Then $T(U(x)) = T(U(y))$

$\Rightarrow I(x) = I(y)$ $(TU = I)$

$\Rightarrow x = y$

or that U is 1-1 and, therefore, onto also.

Hence U is invertible.

Now $U^{-1} : V \to V$ s.t., $UU^{-1} = 1$

Thus $UT = (UT)I = UT(UU^{-1}) = U(TU)U^{-1} = UU^{-1} = I$

$\Rightarrow UT = I = TU$

$\Rightarrow T$ is invertible and $T^{-1} = U$.

Problem 11: *Show that the conclusion of the previous problem fails if V is not finite dimensional.*

Solution: Let V be the vector space of all polynomials in x over a filed F.

Let T = differential operator on V.

i.e., $T : V \to V$, s.t.,

$$T(f(x)) = \frac{d}{dx} f(x)$$

Notice this T is a linear transformation (example 18, chapter 10).

Let $U : V \to V$ s.t.,

$$U(f) = \int_0^x f(t)\,dt$$

Then U is a linear transformation.

Again $TU(f) = T\int_0^x f(t)\,dt = f = I(f)$

$\Rightarrow TU = I$

Now $T(2x) = 2,\ T(2x + 3) = 2$

and as $2x \neq 2x + 3$, T is not 1-1 and hence T is not invertible. Thus $UT \neq I$.

Problem 12: *Let V_1 and V_2 be vector spaces over F. Show that $V_1 \times V_2$ is F.D.V.S. if and only if V_1 and V_2 are F.D.V.S.*

Solution: Let $V_1' = \{(v_1, 0) \mid v_1 \in V_1\}$

$V_2' = \{(0, v_2) \mid v_2 \in V_2\}$

then V_1' and V_2' are subspaces of $V_1 \times V_2$

Define $\theta_1 : V_1 \to V_1'$ s.t.,

$\theta_1(v_1) = (v_1, 0)$

Then θ_1 is an isomorphism (Prove!)

Similarly $\theta_2 : V_2 \to V_2'$ s.t.,

$\theta_2(v_2) = (0, v_2)$

will be an isomorphism.

So $V_1 \cong V_1',\ V_2 \cong V_2'$

Suppose $V_1 \times V_2$ is *F.D.V.S.*, then V_1' and V_2' are *F.D.V.S.* (being subspaces of $V_1 \times V_2$)

$\Rightarrow V_1$ and V_2 are *F.D.V.S.*

Conversely, if V_1 and V_2 are *F.D.V.S.* then $V_1 \times V_2$ is *F.D.V.S.* and dim $(V_1 \times V_2)$ = dim V_1 + dim V_2. (Note: If $\{e_1, e_2, ..., e_m\}$ and $\{f_1, f_2, ..., f_n\}$ are basis of V_1 and V_2 resp., then $\{(e_1, 0), ..., (e_m, 0), (0, f_1), ..., (0, f_n)\}$ is a basis of $V_1 \times V_2$.)

Problem 13: *Let W_1 and W_2 be subspaces of V such that $\frac{V}{W_1}$ and $\frac{V}{W_2}$ are F.D.V.S. Show that $\frac{V}{W_1 \cap W_2}$ is also a F.D.V.S.*

Solution: Define $\theta : V \to \frac{V}{W_1} \times \frac{V}{W_2}$ s.t.,

$$\theta(v) = (W_1 + v,\ W_2 + v)$$

It is easy to see that θ is a linear transformation where Ker $\theta = W_1 \cap W_2$.

Hence $\frac{V}{\text{Ker } \theta} \cong \theta(V)$

Again, since $\frac{V}{W_1}$ and $\frac{V}{W_2}$ are *F.D.V.S.*, so will be $\frac{V}{W_1} \times \frac{V}{W_2}$. In fact $\dim\left(\frac{V}{W_1} \times \frac{V}{W_2}\right) = \dim \frac{V}{W_1} + \dim \frac{V}{W_2}$. (See Problem 12).

Also $\theta(V)$ is a subspace of $\frac{V}{W_1} \times \frac{V}{W_2}$ and is therefore, finite dimensional.

Hence $\frac{V}{W_1 \cap W_2}$ is *F.D.V.S.*

Exercises

1. Let $T : F^3 \to F^3$ be defined by

$T(x_1, x_2, x_3) = (x_1 - x_2 + 2x_3, 2x_1 + x_2, -x_1 - 2x_2 + 2x_3)$

then T is a *L.T.* Find the conditions on a, b, c such that (a, b, c) is in Range T. Show that rank T is 2. $[a = b + c]$

2. Show that image of a *L.I.* set by a *L.T.*, need not be *L.I.* (consider zero *L.T.*).

3. Let dim $V = n$, $T : V \to V$ be a *L.T.* such that Range T = Ker T. Show that n is even. Prove that $T : \mathbf{R}^2 \to \mathbf{R}^2$, s.t., $T(x_1, x_2) = (x_2, 0)$ is such a *L.T.*

4. Find a *L.T.* $T : \mathbf{R}^3 \to \mathbf{R}^3$ such that the set of all vectors (x_1, x_2, x_3) satisfying the equation $4x_1 - 3x_2 + x_3 = 0$ is Ker T.

$[T(x_1, x_2, x_3) = (4x_1 - 3x_2 + x_3, 8x_1 - 6x_2 + 2x_3, 0)]$

5. Show that $f : \mathbf{R}^4 \to \mathbf{R}^4$, s.t., $f(x, y, z, t) = (2x, 3y, 0, 0)$ is a *L.T.* Find its rank and nullity.

6. Find range, rank, Ker and nullity of the *L.T.* defined by

(*i*) $T : \mathbf{R}^2 \to \mathbf{R}^2$ s.t., $T(x_1, x_2) = (x_1 + x_2, x_1)$ $[\mathbf{R}^2, 2, (0), 0]$

(*ii*) $T : \mathbf{R}^2 \to \mathbf{R}^3$ s.t., $T(x_1, x_2) = (x_1 + x_2, x_1 - x_2, x_2)$

(*iii*) $T : \mathbf{R}^3 \to \mathbf{R}^2$ s.t., $T(x_1, x_2, x_3) = (x_1 - x_2, x_1 + x_3)$

$[(1, 1, 0)\ (1, -1, 1), 2, (0), 0]$

(*iv*) The zero and the identity linear transformations

(*v*) $T : \mathbf{R}^3 \to \mathbf{R}^2$, s.t., $T(x_1, x_2, x_3) = (x_1 + x_2, 2x_3 - x_1)$.

7. Find the *L.T.* from $\mathbf{R}^3 \to \mathbf{R}^3$ which has its range the subspace spanned by $(1, 0, -1)$, $(1, 2, 2)$.

8. Let G be the set of all invertible linear transformations from $V \to V$ then show that G forms a group under product of linear transformations.

9. Let T, T_1, T_2 be linear transformations from $V \to W$, S, S_1, S_2 from $W \to U$ and K, K_1, K_2 from $U \to Z$ where V, W, U, Z are vector spaces over a field F then show that

(*i*) $S(T_1 + T_2) = ST_1 + ST_2$

(*ii*) $(S_1 + S_2)T = S_1T + S_2T$

(*iii*) $K(ST) = (KS)T$

(*iv*) $(\alpha S)T = \alpha(ST) = S(\alpha T)$ $\alpha \in F$.

10. Let $T : \mathbf{R}^3 \to \mathbf{R}^2$, $S : \mathbf{R}^2 \to \mathbf{R}^2$ be linear transformations. Show that ST is not invertible.

11. Show that it is possible to find two linear operators T, U on $\mathbf{R}^2$ such that $TU = 0$ but $UT \neq 0$.

(Consider $(x_1, x_2) \to (x_1, 0)$ and $(x_1, x_2) \to (0, x_1)$).

12. A linear transformation $T : V \to V$ is called *idempotent* or a *projection* if $T^2 = T$. Show that if S, T are idempotent and $ST = TS$ then ST and $S + T - ST$ are idempotent and if $ST + TS = 0$ then $S + T$ is idempotent.

13. Let V be the real vector space and E an idempotent linear operator. Show that $I + E$ is invertible. [Hint: consider $I - 1/2E$].

14. A linear transformation $T : V \to V$ is called *nilpotent* on V if $T^n = 0$ for some integer $n > 1$. The smallest integer n (> 1) for which $T^n = 0$ is called degree of nilpotency of T. Show that $T : \mathbf{R}^4 \to \mathbf{R}^4$, defined by $T(x_1, x_2, x_3, x_4) = (0, 2x_1, 3x_1 + 2x_2, x_2 + 4x_3)$ is nilpotent of degree 4.

15. Show that a necessary and sufficient condition for the map $T : F^2 \to F^2$ s.t., $T(x_1, x_2) = (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$, $[(\alpha, \beta, \gamma, \delta)$ some fixed elements of $F)]$ to be an isomorphism is that $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0$.

16. If $O \neq T \in$ Hom (V, V) then show that there exists some $S \in$ Hom (V, V) such that TS is an idempotent.

17. Show that the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ defined by $T(x_1, x_2, x_3) = (2x_1, x_1 - x_2, 5x_1 + 4x_2 + x_3)$ is invertible.

18. If the *L.T.* $T : \mathbf{R}^7 \to \mathbf{R}^3$ has a four dimensional Kernel, show that range of T has dimension three.

19. Let T be a *L.T.* from $\mathbf{R}^7$ onto a 3-dimensional subspace of $\mathbf{R}^5$. Show that dim Ker $T = 4$.

Matrix of a Linear Transformation

Let $U(F)$, $V(F)$ be vector spaces of dimension n and m respectively. Let $\beta = \{u_1, ..., u_n\}$, $\beta' = \{v_1, ..., v_m\}$ be their ordered basis respectively. Suppose $T : U \to V$ is a linear transformation. Since $T(u_1)$, ..., $T(u_n) \in V$ and $\{v_1, ..., v_m\}$ spans V, each $T(u_i)$ is a linear combination of vectors v_1, ..., v_m.

Let
$$T(u_1) = \alpha_{11}v_1 + ... \ \alpha_{m1}v_m$$
$$T(u_2) = \alpha_{12}v_1 + ... + \alpha_{m2}v_m$$
$$.....$$
$$T(u_n) = \alpha_{1n}v_1 + ... + \alpha_{mn}v_m$$

where each $\alpha_{ij} \in F$. Then the $m \times n$ matrix

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & ... & ... & \alpha_{1n} \\ : & : & ... & ... & : \\ : & : & ... & ... & : \\ : & : & ... & ... & : \\ \alpha_{m1} & \alpha_{m2} & ... & ... & \alpha_{mn} \end{bmatrix}$$

is called matrix of T with repsect to ordered basis β, β' respectively. A is uniquely determined by T as each $\alpha_{ij} \in F$ is uniquely determined. We write

$$A = [T]_{\beta, \beta'}$$

The word *ordered basis is very significant, for as the order of basis is changed, the entries α_{ij} will change their positions and so the corresponding matrix will be different.*

In particular if $U = V$, $\beta = \beta'$, then instead of writing $[T]_{\beta, \beta'}$, we write $[T]_{\beta}$.

Let $M_{m\times n}(F)$ denote the vector space of all $m \times n$ matrices over F. Let Hom (U, V) denote the vector space of all linear transformations from $U(F)$ into $V(F)$. We prove

Theorem 10: *Hom* $(U, V) \cong M_{m\times n}(F)$.

Proof: Define θ : Hom $(U, V) \to M_{m\times n}(F)$, s.t.,

$$\theta(T) = [T]_{\beta, \beta'}$$

Where $\beta = \{u_1, \ldots u_n\}$, $\beta' = \{v_1, \ldots v_m\}$ are ordered basis of U, V respectively. θ is well defined as $[T]_{\beta, \beta'}$ is uniquely determined by T

It is not difficult to verify that θ is a linear transformation.

Let $\theta(S) = \theta(T)$, $S, T \in$ Hom (U, V)

Then $[S]_{\beta, \beta'} = [T]_{\beta, \beta'}$

$\Rightarrow$ $(a_{ij}) = (b_{ij})$

$\Rightarrow$ $a_{ij} = b_{ij}$ for all i, j

$\Rightarrow$ $S(u_j) = \sum_{i=1}^{m} a_{ij}v_i = \sum_{i=1}^{m} b_{ij}v_i = T(u_j)$ for all $j = 1, \ldots n$

$\Rightarrow$ $S = T \Rightarrow \theta$ is 1-1.

Let $A = (a_{ij})_{m\times n} \in M_{m\times n}(F)$. Then $\exists$ a linear transformation $T \in$ Hom (U, V) s.t.,

$$T(u_j) = \sum_{i=1}^{m} a_{ij}v_i \quad \text{for } j = 1, \ldots, n$$

$\therefore$ $A = [T]_{\beta, \beta'} = \theta(T) \Rightarrow \theta$ is onto.

Hence θ is an isomorphism and so Hom $(U, V) \cong M_{m\times n}(F)$.

Cor.: dim Hom $(U, V) = mn$.

Proof: S = set of all $m \times n$ matrices with only one entry 1 and all other entries zero, is a basis of $M_{m\times n}(F)$.

Clealy, $o(S) = mn \Rightarrow$ dim $M_{m\times n}(F) = mn$

dim Hom $(U, V) = mn$.

Theorem 11: *Let S, T be two linear transformations from V(F) into V(F). Let* β *be an ordered basis of V. Then*

$$[ST]_\beta = [S]_\beta[T]_\beta.$$

Proof: Let $\beta = \{v_1, \ldots v_n\}$

Let $S(v_1) = a_{11}v_1 + \ldots a_{n1}v_1$

.....

$S(v_n) = a_{1n}v_1 + \ldots + a_{nn}v_n$

where $a_{ij} \in F$

In general, $S(v_j) = \sum_{i=1}^{n} a_{ij}v_i$ for all $j = 1, \ldots, n$

$\therefore$ $[S]_\beta = (a_{ij})$

Similarly,

$$T(v_1) = b_{11}v_1 + \ldots + b_{n1}v_n$$
$$\ldots\ldots\ldots$$
$$T(v_n) = b_{1n}v_1 + \ldots + b_{nn}v_n \quad \text{where } b_{ij} \in F$$

In general $T(v_k) = \sum_{j=1}^{n} b_{jk} v_j$, for all $k = 1, \ldots, n$

$\therefore \quad [T]_\beta = (b_{jk})$

$$\therefore \quad ST(v_k) = S\left(\sum_{j=1}^{n} b_{jk} v_j\right) = \sum_{j=1}^{n} b_{jk} S(v_j)$$
$$= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{jk}\right) v_i$$

$$[ST]_\beta = (c_{ik}), \text{ where } c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

Also, (i, k)th entry in $[S]_\beta [T]_\beta$

$$= \sum_{j=1}^{n} a_{ij} b_{jk} = c_{ik} = (i, k)\text{th entry in } [ST]_\beta$$

$\therefore \quad [ST]_\beta = [S]_\beta [T]_\beta$

Cor.: If S is an invertible linear transformation from $V(F)$ into $V(F)$, then so is $[S]_\beta$ with respect to any basis β of V and conversely.

Proof: Since S is invertaible, $\exists\ T : V \to V$ s.t., $ST = I = TS$. Let β be an ordered basis of V. Then by above theorem,

$$[ST]_\beta = [I]_\beta = I, \text{ where } T = S^{-1}$$
$$\Rightarrow \quad [S]_\beta [T]_\beta = I$$
$$\Rightarrow \quad [S]_\beta [S^{-1}]_\beta = I$$
$$\Rightarrow \quad [S^{-1}]_\beta = [S]^{-1}_\beta \text{ for any basis } \beta \text{ of } V$$

Conversely, let $[S]_\beta$ be invertible. Then $\exists$ a matrix $A = (a_{ij})$ over F s.t., $[S]_\beta A = I$

Let $T : V \to V$ be a linear transformation s.t.,

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i \quad \text{for all } j = 1, \ldots n$$

$\therefore \quad [T]_\beta = A$

$\therefore \quad [S]_\beta [T]_\beta = I$

$$\Rightarrow \quad [ST]_\beta = I$$
$$\Rightarrow \quad (ST)(v_j) = v_j \quad \text{for all } j = 1, \ldots, n$$
$$\Rightarrow \quad (ST)(x) = (ST)(\alpha_1 v_1 + \ldots + \alpha_n v_n)$$

$$= \alpha_1 v_1 + \ldots + \alpha_n v_n$$
$$= x \quad \text{for all } x \in V$$

$\Rightarrow \quad ST = I \Rightarrow S$ is invertible.

We give a more general result of above theorem 11.

Theorem 11(a): *Let $T : V \to W$ and $S : W \to Z$ be linear transformations. Let* β, γ and δ *be ordered basis for V, W and Z respetively. Then*

$$[ST]_{\beta,\delta} = [S]_{\gamma,\delta}\,[T]_{\beta,\gamma}$$

Proof: Let $\beta = \{v_1, \ldots, v_n\}$, $\gamma = \{w_1, \ldots, w_m\}$, and $\delta = \{z_1, \ldots, z_p\}$,

Let $[T]_{\beta,\gamma} = A = (a_{ij})_{m \times n}$, $[S]_{\gamma,\delta} = B = (b_{ij})_{p \times m}$

Then, $T(v_k) = a_{1k}w_1 + \ldots + a_{mk}w_m$

$S(w_j) = b_{1j}z_1 + \ldots + b_{pj}z_p$

$\therefore \quad (ST)(v_k) = S(T(v_k))$

$= S(a_{1k}w_1 + \ldots + a_{mk}w_m)$

$= a_{1k}S(w_1) + \ldots + a_{mk}S(w_m)$

$= a_{1k}(b_{11}z_1 + \ldots + b_{m1}z_p) + \ldots + a_{mk}(b_{1m}z_1 + \ldots + b_{pm}z_p)$

$= (a_{1k}b_{11} + \ldots + a_{mk}b_{1m})z_1 + \ldots + (a_{1k}b_{m1} + \ldots + a_{mk}b_{pm}z_p)$

$$= \sum_{i=1}^{p}\left(\sum_{j=1}^{m} b_{ij}a_{jk}\right) z_i$$

$$= \sum_{i=1}^{p} c_{ik}z_i, \text{ where } c_{ik} = \sum_{j=1}^{m} b_{ij}a_{jk}$$

$\therefore \quad [ST]_{\beta,\delta} = (c_{ik}) = C$

Also, (i, k)th entry of $BA = \sum_{j=1}^{m} b_{ij}a_{jk}$

$= c_{ik}$

$= (i, k)$th entry of $[T]_{\beta,\delta}$

$\therefore \quad [ST]_{\beta,\delta} = BA = [S]_{\gamma,\delta}\,[T]_{\beta,\gamma}$

In particular, if $V = W = Z$ and $\beta = \gamma = \delta$, then

$$[ST]_{\beta,\beta} = [S]_{\beta,\beta}\,[T]_{\beta,\beta}$$

or

$$[ST]_{\beta} = [S]_{\beta}\,[T]_{\beta}$$

So, theorem 11 is a special case of above thorem 11(a).

Cor: Let $T : V \to W$ be a linear transformation. Then T is invertible if and only if $[T]_{\beta,\gamma}$ is invertible where β and γ are bases of V and W respectively.

Proof: Let T be invertible. Then there exists a linear transformation $T^{-1} : V \to W$ such that $T^{-1}T = I_V$, $TT^{-1} = I_W$.

$\therefore$ $I = [I_V]_\beta = [T^{-1}T]_\beta = [T^{-1}]_{\gamma,\beta}\,[T]_{\beta,\gamma}$

So, $[T]_{\beta,\gamma}$ is invertible.

Conversely, let $[T]_{\beta,\gamma}$ be invertible. There exists a matrix B such that $[T]_{\beta,\gamma} = I = [T]_{\beta,\gamma}B$.

Let $\beta = \{v_1, \ldots, v_n\}$ and $\gamma = \{w_1, \ldots, w_m\}$ be bases for V and W respectively.

Then there exists a linear transformation S: $W \to V$ such that $S(w_k) = \sum_{i=1}^{n} b_{ik} v_i$.

Here $[S]_{\gamma,\beta} = B = (b_{ij})_{n \times m}$

$\therefore$ $[S]_{\gamma,\beta}\,[T]_{\beta,\gamma} = I$. By above theorem $[ST]_\beta = I$.

So, $ST = I_V$.

Similarly, $TS = I_W$.

Thus, T is invertible.

In particular, if $V = W$, $\beta = \gamma$. Then T: $V \to V$ is invertible if and only if $[T]_\beta$ is invertible. So, Cor. to theorem 11 is a special case of above theorem.

We now give a relation between matrices of a linear transformation with respect to two different basis of a vector space.

Theorem 12: *Let $T : V(F) \to V(F)$ be a linear transformation. Let $\beta = \{u_1, \ldots, u_n\}$, $\beta' = \{v_1, \ldots, v_n\}$ be two ordered basis of V. Then $\exists$ a non singular matrix P over F such that*

$$[T]_{\beta'} = P^{-1}[T]_\beta P.$$

Proof: Let $S : V \to V$ be a linear transformation such that $S(u_i) = v_i$ for all $i = 1, \ldots n$.

Now $x \in \text{Ker } S \Rightarrow S(x) = 0$, $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$, $\alpha_i \in F$

$\Rightarrow$ $S(\alpha_1 u_1 + \ldots + \alpha_n u_n) = 0$

$\Rightarrow$ $\alpha_1 S(u_1) + \ldots + \alpha_n S(u_n) = 0$

$\Rightarrow$ $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$

$\Rightarrow$ $\alpha_i = 0$ for all i

$\Rightarrow$ $x = 0$

$\Rightarrow$ Ker $S = \{0\}$

$\Rightarrow$ S is 1-1 and so onto.

$\therefore$ S is an isomorphism. Let $[T]_\beta = (a_{ij})$

Then $T(u_j) = \sum_{i=1}^{n} a_{ij} u_i$

$\therefore$ $(STS^{-1})(v_j) = ST(u_j)$

$$= S\left(\sum_{i=1}^{n} a_{ij} u_i\right) = \sum_{i=1}^{n} a_{ij} v_i$$

$$\therefore \quad [STS^{-1}]_{\beta'} = (a_{ij}) = [T]_{\beta}$$
$$\Rightarrow \quad [S]_{\beta'}[T]_{\beta'}[S^{-1}]_{\beta'} = [T]_{\beta}$$
$$\Rightarrow \quad [S]_{\beta'}[T]_{\beta'}[S]_{\beta}^{-1} = [T]_{\beta}$$
$$\Rightarrow \quad [T]_{\beta'} = [S]_{\beta'}^{-1}[T]_{\beta}[S]_{\beta'}$$
$$= P^{-1}[T]_{\beta} P, \text{ where } P = [S]_{\beta'}.$$

As in theorem 11, we give a more general result of above theorem 12.

Theorem 12(a): Let $T : V(F) \to W(F)$ *be a linear transformation. Let* β, β' *and* γ, γ' *be ordered basis for V and W respectively. Then*

$$[T]_{\beta',\gamma'} = S^{-1}[T]_{\beta,\gamma} P$$

where P is the matrix of β' relative to β and S is the matrix of γ' relative to γ.

Proof: Let $\beta = \{v_1, \ldots, v_n\}$, $\beta' = \{v'_1, \ldots, v'_n\}$
$\gamma = \{w_1, \ldots, w_m\}$, $\gamma' = \{w'_1, \ldots, w'_m\}$

Let $P = (p_{ij})_{n \times n}$, $S = (s_{ij})_{m \times m}$

Then $$v'_j = \sum_{k=1}^{n} p_{kj} v_k, \qquad 1 \le j \le n$$

$$w'_r = \sum_{k=1}^{m} s_{kr} w_k, \qquad 1 \le r \le m$$

Let $\theta : W \to W$ be the linear transformation
$\theta(W_i) = w'_i$ for all i.

Then θ is an isomorphism as θ takes basis of W into basis of W.

Also $[\theta]_{\gamma,\gamma} = S$

Since θ is invertible, so is S.

Also, $S^{-1} = [\theta^{-1}]_{\gamma',\gamma'}$

Let $$w_r = \sum_{l=1}^{m} s'_{lr} w'_l, \qquad 1 \le r \le m$$

Then S^{-1} = matrix of γ relative to γ'

Let $[T]_{\beta,\gamma} = A = (a_{ij})_{m \times n}$
$[T]_{\beta',\gamma'} = B = (b_{ij})_{m \times n}$

$$\therefore \quad T(v_k) = \sum_{i=1}^{m} a_{ik} w_i, \qquad T(v'_j) = \sum_{l=1}^{m} b_{lj} w'_l,$$

$$\therefore \quad T(v'_j) = \sum_{k=1}^{n} p_{kj} T(v_k)$$
$$= \sum_{k=1}^{n} p_{kj} \left[\sum_{i=1}^{m} a_{ik} w_i \right]$$

$$= \sum_{i=1}^{m}\left[\sum_{k=1}^{n} a_{ik}\, p_{kj}\right] w_i$$

$$= \sum_{i=1}^{m}\left[\sum_{k=1}^{n} a_{ik}\, p_{kj}\right]\left[\sum_{l=1}^{m} s'_{li} w'_l\right]$$

$$= \sum_{l=1}^{m}\left[\sum_{k=1}^{n}\sum_{i=1}^{m} s'_{li}\, a_{ik}\, p_{kj}\right] w'_l = \sum_{l=1}^{m} b_{lj} w'_l$$

$\therefore \quad b_{lj} = \sum_{k=1}^{n}\sum_{i=1}^{m} s'_{li}\, a_{ik}\, p_{kj}$

$\therefore \quad [T]_{\beta',\gamma'} = S^{-1}[T]_{\beta,\gamma}\, P$

In particular, if $V = W$, $\beta = \gamma$, $\beta' = \gamma'$, then

$$[T]_{\beta'} = S^{-1}[T]_{\beta}\, P, \qquad S = P$$
$$= P^{-1}[T]_{\beta}\, P$$

So, theorem 12 is a special case of the above theorem 12(a).

The converse of theorem 12 is also true, as is seen in

Theorem 13: *Let A and B be $n \times n$ matrices over F. Suppose A and B are similar. Then A and B represent the same linear transformation with respect to two ordered basis for some vector space over F.*

Proof: Let $V = F^{(n)}$. Since A and B are similar there exists a non singular matrix $P = (p_{ij})$ over F such that $B = P^{-1}AP$.

Let $\beta = \{v_1, v_2,....,v_n\}$ be an ordered basis for V.

Let $A = (a_{ij})$. Then there exists a linear transformation. $T : V \to V$ such that

$$T(v_j) = a_{1j}v_1 + a_{2j}v_2 + \ldots + a_{nj}v_n \quad \text{for all } j = 1, 2, \ldots, n$$

Also $[T]_{\beta} = A$

Let $w_j = \sum_{i=1}^{n} p_{ij} v_i, \quad j = 1, 2, \ldots, n.$

Let $\beta' = \{w_1, w_2,....,w_n\}$. We show that β' is a basis of V.

Let $a_1w_1 + a_2w_2 + \ldots + a_nw_n = 0$

Then $a_1(p_{11}v_1 + \ldots + p_{n1}v_n) + \ldots + a_n(p_{1n}v_1 + \ldots + p_{nn}v_n) = 0$

or $(a_1p_{11} + \ldots + a_np_{1n})v_1 + \ldots + (a_1p_{n1} + \ldots + a_np_{nn})v_n = 0$

Since β is a linearly independent set,

$$a_1p_{11} + \ldots + a_np_{1n} = 0$$
$$\ldots$$
$$a_1p_{n1} + \ldots + a_np_{nn} = 0$$

or $$P\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = 0$$

So, $$P^{-1}P\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = 0$$

Therefore, $a_i = 0$ for all i

Hence β' is a linearly independent set and so forms a basis for V as dim $V = n$

Define: $\theta : V \to V$ such that

$$\theta(v_i) = w_i \text{ for all } i$$

Then θ is an isomorphism.

Now
$$\begin{aligned}(\theta T\theta^{-1})\ (w_j) &= (\theta T)(\theta^{-1}(w_j)) \\ &= (\theta T)(v_j) \\ &= \theta(T(v_j)) \\ &= \theta(a_{1j}v_1 + \ldots + a_{nj}v_n) \\ &= a_{1j}w_1 + \ldots + a_{nj}w_n \\ &= \sum_{i=1}^{n} a_{ij}w_i\end{aligned}$$

So, $$[\theta T\theta^{-1}]_{\beta'} = (a_{ij}) = A$$

Now
$$\begin{aligned}\theta(w_j) &= \theta(p_{1j}v_1 + \ldots + p_{nj}v_n) \\ &= p_{1j}w_1 + \ldots + p_{nj}w_n \\ &= \sum_{i=1}^{n} p_{ij}w_i\end{aligned}$$

So, $$[\theta]_{\beta'} = (p_{ij}) = P$$

Since
$$[\theta T\theta^{-1}]_{\beta'} = A,$$
$$[\theta]_{\beta'}\,[T]_{\beta'}\,[\theta^{-1}]_{\beta'} = A$$
$$P[T]_{\beta'}\,[\theta]_{\beta'}^{-1} = A$$
$$P[T]_{\beta'}\,P^{-1} = A$$

or $$[T]_{\beta'} = P^{-1}AP = B$$

Hence, A and B represent same linear transformation T with respect to ordered basis β and β' respectively.

Problem 14: *Let T be a linear operator on $\mathbf{C}^2$ defined by $T(x_1, x_2) = (x_1, 0)$ Let $\beta = \{\in_1 = (1, 0), \in_2 = (0, 1)\}$, $\beta' = \{\alpha_1 = (1, i), \alpha_2 = (-i, 2)\}$ be ordered basis for $\mathbf{C}^2$. What is the matrix of T relative to the pair β, β'?*

Solution: Now $T(\in_1) = T(1, 0)$

$= (1, 0)$

$= a(1, i) + b(-i, 2)$

$\Rightarrow \quad a - bi = 1$ where $a, b \in \mathbf{C}$

$ai + 2b = 0$

$\Rightarrow \quad a = 2, b = -i$

$\Rightarrow \quad T(\in_1) = 2\alpha_1 - i\alpha_2$

Also $T(\in_2) = T(0, 1) = (0, 0) = 0\alpha_1 + 0\alpha_2$

$$\therefore \qquad [T]_{\beta\beta'} = \begin{bmatrix} 2 & 0 \\ -i & 0 \end{bmatrix}.$$

Problem 15: *Let T be the linear operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (-x_2, x_1)$*

(*i*) *Prove that for all real numbers c, the operator $(T - cI)$ is invertible.*

(*ii*) *Prove that if β is any ordered basis for $\mathbf{R}^2$ and $[T]_\beta = A$, then $a_{12}a_{21} \neq 0$, where $A = (a_{ij})$.*

Solution: (*i*) Let $\beta = \{\in_1 = (1, 0), \in_2 = (0, 1)\}$ be an ordered basis for $\mathbf{R}^2$.

Then $\quad T(\in_1) = T(1, 0) = (0, 1) = 0\in_1 + 1\in_2$

$T(\in_2) = T(0, 1) = (-1, 0) = -1\in_1 + 0\in_2$

$$\therefore \qquad [T]_\beta = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \; [cI]_\beta = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$$

$$\therefore \qquad [T - cI]_\beta = \begin{bmatrix} -c & -1 \\ 1 & -c \end{bmatrix}$$

$\det [T - cI]_\beta = c^2 + 1 \neq 0$ for all real numbers c

$\therefore \quad [T - cI]_\beta$ is invertible.

$\Rightarrow \quad T - cI$ is invertible for all real numbers c.

(*ii*) Let β be any ordered basis for $\mathbf{R}^2$ s.t.,

$$[T]_\beta = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = A, \quad a_{ij} \in \mathbf{R}$$

By (*i*) $T - a_{11}I$ is Invertible

$\Rightarrow \quad [T - a_{11}I]_\beta$ is invertible

$$\Rightarrow \qquad \begin{bmatrix} 0 & a_{12} \\ a_{21} & a_{22} - a_{11} \end{bmatrix} \text{ is invertible}$$

$\Rightarrow \quad -a_{12}a_{21} \neq 0$ as det of abve matrix $\neq 0$

$\Rightarrow \quad a_{12}a_{21} \neq 0.$

Problem 16: *Let T be the linear operator on $\mathbf{R}^3$ defined by*

$$T(x_1, x_2, x_3) = (3x_1 + x_3, -2x_1 + x_2, -x_1 + 2x_2 + 4x_3)$$

Show that T is invertible.

Solution: Let $\beta = \{\in_1 = (1, 0, 0), \in_2 = (0, 1, 0), \in_3 = (0, 0, 1)\}$ be an ordered basis of $\mathbf{R}^3$.

Then $[T]_\beta = \begin{bmatrix} 3 & 0 & 1 \\ -2 & 1 & 0 \\ -1 & 2 & 4 \end{bmatrix} = A.$

$$\det A = 3(4) + 1\ (-4 + 1) = 12 - 3 = 9 \neq 0$$

So, A is invertible

$\Rightarrow T$ is invertible.

Problem 17: *Let A be an $n \times n$ matrix over F. Show that A is invertible if and only if columns of A are linearly independent over F.*

Solution: Let $V(F)$ be a vector space of dimension n. Let $\beta = \{v_1,..., v_n\}$ be an ordered basis of V. Let $A = (a_{ij})$. Then $\exists$ a linear transformation $T : V \to V$ such that

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i$$

$\therefore \quad [T]_\beta = A.$

Let $M_n(F)$ denote the vector space of all $n \times n$ matrices over F.

Let $A \in M_n(F)$ be invertible. Then T is also invertible (by Cor. to Theorem 11) and so T is 1-1, onto.

Let $$\alpha_1 \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \ldots + \alpha_n \begin{bmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{bmatrix} = 0,\ \alpha_i \in F$$

$$\Rightarrow \begin{bmatrix} \alpha_1 a_{11} & \cdots & +\alpha_n a_{1n} \\ \cdots & \cdots & \cdots \\ \alpha_1 a_{n1} + & \cdots & +\alpha_n a_{nn} \end{bmatrix} = 0$$

$$\Rightarrow \quad \alpha_1 a_{11} + \ldots + \alpha_n a_{1n} = 0$$

$$\cdots \qquad \cdots$$

$$\alpha_1 a_{n1} + \ldots + \alpha_n a_{nn} = 0$$

$$\Rightarrow \quad \alpha_1 a_{11} v_1 + \ldots + \alpha_n a_{1n} v_1 = 0$$

$$\cdots \qquad \cdots$$

$$\alpha_1 a_{n1} v_n + \ldots + \alpha_n a_{nn} v_n = 0$$

$$\Rightarrow \quad \alpha_1(a_{11}v_1 + \ldots + a_{n1}v_n) + \ldots + \alpha_n(a_{1n}v_1 + \ldots + \alpha_{nn}v_n) = 0$$

$$\Rightarrow \quad \alpha_1 T(v_1) + \ldots + \alpha_n T(v_n) = 0$$

$$\Rightarrow \quad T(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0$$

$$\Rightarrow \quad \alpha_1 v_1 + \ldots + \alpha_n v_n = 0 \text{ as } T \text{ is 1-1}$$

$\Rightarrow \quad \alpha_i = 0$ for all i

$\Rightarrow$ columns of A are linearly independent.

Conversely, let columns of A be linearly independent over F.

Now $x \in \text{Ker } T$

$\Rightarrow T(x) = 0, x \in V$

$\Rightarrow T(\alpha_1 v_1 + ... + \alpha_n v_n, = 0$

$\Rightarrow \alpha_1 T(v_1) + ... + \alpha_n T(v_n) = 0$

$$\Rightarrow \sum_{j=1}^{n} \alpha_j T(v_j) = 0 \Rightarrow \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{n} a_{ij} v_i \right) = 0$$

$$\Rightarrow \sum_{i=1}^{n} \left(\sum_{j=1}^{n} (\alpha_j a_{ij}) \right) v_i = 0$$

$$\Rightarrow \sum_{j=1}^{n} \alpha_j a_{ij} = 0 \text{ for all } i = 1, ..., n$$

$$\Rightarrow \alpha_1 \begin{bmatrix} a_{11} \\ : \\ a_{n1} \end{bmatrix} + ... + \alpha_n \begin{bmatrix} a_{1n} \\ : \\ a_{nn} \end{bmatrix} = 0$$

$\Rightarrow$ each $\alpha_i = 0$ as columns are linearly independent

$\Rightarrow x = 0 \quad \Rightarrow \text{Ker } T = \{0\}$

$\Rightarrow T$ is 1-1 and so onto

$\Rightarrow T$ is invertible.

Problem 18: *Let T be the linear operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (-x_2, x_1)$.*

Let $\beta = \{\in_1 = (1, 0), \in_2 = (0, 1)\}$

$\beta' = \{\alpha_1 = (1, 2), \alpha_2 = (1, -1)\}$

be ordered basis for $\mathbf{R}^2$. Find a matrix P such that

$$[T]_{\beta'} = P^{-1}[T]_{\beta} P.$$

Proof: $T(\in_1) = T(1, 0) = (0, 1) = 0\in_1 + 1\in_2$

$T(\in_2) = T(0, 1) = (-1, 0) = -1\in_1 + 0\in_2$

$$\therefore \quad [T]_{\beta} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Define $S : \mathbf{R}^2 \to \mathbf{R}^2$ s.t.,

$S(\in_i) = \alpha_i \quad i = 1, 2$

Now $\alpha_1 = (1, 2) = 1\in_1 + 2\in_2$

$\alpha_2 = (1, -1) = 1\in_1 + (-1)\in_2$

$\Rightarrow \quad S(\alpha_1) = 1\alpha_1 + 2\alpha_2$

$S(\alpha_2) = 1\alpha_1 + (-1)\alpha_2$

$$\Rightarrow \qquad [S]_{\beta'} = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}$$

$$\Rightarrow \qquad P = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix} \text{ and } P^{-1} = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{bmatrix}$$

$$\Rightarrow \qquad P^{-1}\,[T]_{\beta}\,P = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{2}{3} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ -\frac{5}{3} & -\frac{1}{3} \end{bmatrix}$$

$$= [T]_{\beta'}$$

Problem 19: *Let T be linear operator on* $\mathbf{R}^3$*, the matrix of which in the standard ordered basis is*

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ -1 & 3 & 4 \end{bmatrix}$$

Find a basis for the range of T and a basis for the null space of T.

Solution: Det $A = 1(4 - 3) - 2\,(1) + 1(1)$

$= 1 - 2 + 1 = 0$

$\therefore$ A is not invertible and so T is not invertible.

Let $\{\in_1 = (1, 0, 0), \in_2 = (0, 1, 0), \in_3 = (0, 0, 1)\}$

be standard ordered basis of $\mathbf{R}^3$.

Let $(x_1, x_2, x_3) \in \text{Ker } T$

Then $T(x_1, x_2, x_3) = 0$

$\Rightarrow T(x_1(1, 0, 0) + x_2(0, 1, 0) + x_3(0, 0, 1)) = 0$

$\Rightarrow T(x_1 \in_1 + x_2 \in_2 + x_3 \in_3) = 0$

$\Rightarrow x_1 T(\in_1) + x_2 T(\in_2) + x_3 T(\in_3) = 0$

$\Rightarrow x_1(1, 0, -1) + x_2(2, 1, 3) + x_3(1, 1, 4) = 0$

$\Rightarrow (x_1 + 2x_2 + x_3, x_2 + x_3, -x_1 + 3x_2 + 4x_3) = 0$

$\Rightarrow x_1 + 2x_2 + x_3 = 0, x_2 + x_3 = 0, -x_1 + 3x_2 + 4x_3 = 0$

$\Rightarrow x_1 + x_2 = 0, x_2 + x_3 = 0$

$\Rightarrow (x_1, x_2, x_3) = (-x_2, x_2, -x_3)$

$= x_2(-1, 1, -1)$

$\Rightarrow$ every element in Ker T is multiple of $(-1, 1, -1)$

$\Rightarrow$ Ker T is spanned by $(-1, 1, -1)$

Since $(-1, 1, -1) \neq 0$, $\{(-1, 1, -1)\}$ is a basis of Ker T.

$\therefore$ dim Ker $T = 1 \Rightarrow$ dim Range $T = 2$

Since $T\in_1 = (1, 0, -1)$

$T\in_2 = (2, 1, 3)$

belong to Range T and $aT\in_1 + bT\in_2 = 0$

we find $a(1, 0, -1) + b(2, 1, 3) = 0$

$\Rightarrow b = 0, a = 0$

$\Rightarrow \{T\in_1, T\in_2\}$ is a linearly independent set in Range T. As dim Range $T = 2$, $\{(1, 0, -1), (2, 1, 3)\}$ is a basis of Range T.

Problem 20: *Let T be a linear operator on F^n and let A be the matrix of T in the standard ordered basis for F^n. Let W be the subspace of F^n spanned by the column vectors of A. Find a relation between W and T.*

Solution: $T : F^n \to F^n$

Let $\beta = \{e_1 = (1, 0, 0, \ldots 0), \ldots, e_n = (0, 0, \ldots, 1)\}$ be the standard ordered basis of F^n and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

thus $T(e_1) = a_{11}e_1 + a_{21}e_2 + \ldots + a_{n1}e_n$

$T(e_2) = a_{12}e_1 + a_{22}e_2 + \ldots + a_{n2}e_2$

$\ldots \quad \ldots \quad \ldots$

$T(e_n) = a_{1n}e_1 + a_{2n}e_2 + \ldots + a_{nn}e_n$

and also W is spanned by

$\{(a_{11}, a_{21}, \ldots, a_{n1}), (a_{12}, a_{22}, \ldots, a_{n2}), \ldots, (a_{1n}, a_{2n}, \ldots, a_{nn})\}$

We claim $T : F^n \to W$ is onto *L.T.*

For any $x \in F^n$, $x = \alpha_1e_1 + \alpha_2e_2 + \ldots + \alpha_ne_n$

$\Rightarrow T(x) = \alpha_1T(e_1) + \alpha_2T(e_2) + \ldots + \alpha_nT(e_n)$

$\Rightarrow T(x) \in W$ as $T(e_1), T(e_2), \ldots, T(e_n) \in W$

Again, for any $w \in W$, $w = \beta_1T(e_1) + \beta_2T(e_2) + \ldots + \beta_nT(e_n)$

$= T(\beta_1e_1 + \beta_2e_2 + \ldots + \beta_ne_n)$

showing that T is onto.

$\Rightarrow$ Range $T = W \Rightarrow$ dim Range $T =$ dim W

or that rank of $T =$ dim W

which is the required relation between T and W.

Exercises

1. Let V be the space of all polynomial functions from $\mathbf{R}$ into $\mathbf{R}$ of the form

$$f(x) = c_o + c_1x + c_2x^2 + c_2x^3$$

Let $\beta = \{1, x, x^2, x^3\}$ be an ordered basis of V. Let D be the differential operator on V. Show

$$[D]_\beta = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

2. Let T be the operator on $\mathbf{C}^2$ defined by $T(x_1, x_2) = (x_1, 0)$. Let β be the standard ordered basis of $\mathbf{C}^2$ and $\beta' = \{\alpha_1 = (1, i), \alpha_2 = (-i, 2)\}$ be an ordered basis for $\mathbf{C}^2$.

(i) what is $[T]_{\beta', \beta}$?

(ii) what is $[T]_{\beta'}$? Find P such that $[T]_{\beta'} = P^{-1}[T]_\beta P$.

3. Let T be the linear transformation from $\mathbf{R}^3$ into $\mathbf{R}^2$ defined by

$$T(x_1, x_2, x_3) = (x_1 + x_2, 2x_3 - x_1)$$

(i) If β, β' are standard ordered basis for $\mathbf{R}^3$ and $\mathbf{R}^2$ respectively, find $[T]_{\beta, \beta'}$.

(ii) If $\beta = \{\alpha_1 = (1, 0, -1), \alpha_2 = (1, 1, 1), \alpha_3 = (1, 0, 0)\}$

$\beta' = \{\beta_1 = (0, 1), \beta_2 = (1, 0)\}$

are ordered basis for $\mathbf{R}^3$ and $\mathbf{R}^2$ respectively, find $[T]_{\beta, \beta'}$

4. Let V be a two dimensional vector spacer over the field F and β be an ordered basis for V. If T is a linear operator on V and $[T]_\beta = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, prove that

$$T^2 - (a + b)T + (ad - bc)I = 0.$$

5. Let T be the operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (x_1, 0)$. Let β be the standard ordered basis for $\mathbf{R}^2$ and $\beta' = \{\alpha_1 = (1, 1), \alpha_2 = (2, 1)\}$ be an ordered basis for $\mathbf{R}^2$. Find P s.t.,

$$[T]\beta' = P^{-1}[T]_\beta P.$$

6. Let A be $n \times n$ matrix over F. Show that A is invertible if and only if rows of A are linearly independent over F.

7. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2×2 matrix over F. Show that A is invertible if and only $\{(a, b), (c, d)\}$ is a basis of F^2.

8. Let T be the linear operator on $\boldsymbol{R}^3$, the matrix of which in the standard ordered basis is $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

Find a basis of Range T and Ker T.

9. Show that $T : \mathbf{R}^3 \to \mathbf{R}^2$ s.t., $T(x, y, z) = (y, x)$ is a *L.T.* Find the matrix representation of T for the standard ordered basis of $\mathbf{R}^3$ and $\{(0, 1), (2, 3)\}$ of $\mathbf{R}^2$.

10. Let dim $V = 2$. Let T be a linear operator on V. Suppose matrix of T w.r.t. all bases of V is same. Show that $T = \alpha I$ for some $\alpha \in F$.

[Hint: Let $\beta = \{v_1, v_2\}$ be an ordered basis of V.

Then $\beta' = \{v_2, v_1\}$, $\beta'' = \{v_1 + v_2, v_2\}$ are also bases of V

By hypothesis, $[T]_\beta = [T]_{\beta'} = [T]_{\beta''}$]

Dual Spaces

Earlier we saw that Hom (V, W), the set of all linear transformations from vector space V over F into vector space W over F, is also a vector space over F. Further, if dim $V = m$, dim $W = n$, then dim How $(V, W) = mn$. In particular, if $W = F$, then

Hom (V, F) is called dual space of V over F. It is denoted by $\hat{V}$ and read as V dual. In this section we study these dual spaces.

Our first job will be to construct a basis of $\hat{V}$, from a given basis of V.

Theorem 14: *Let* $\{v_1, ..., v_n\}$ *be a basis of* V.

Define $\hat{v}_i : V \to F$ *s.t.,*

$$\hat{v}_i (\alpha_1 v_1 + ... + \alpha_n v_n) = \alpha_i \quad i = 1, 2, ..., n$$

Then $\hat{v}_i$ *is a linear transformation for all* $i = 1, ..., n$ *and* $\{\hat{v}_1, ..., \hat{v}_n\}$ *is a basis of* $\hat{V}$. *Hence dim* V = *dim* $\hat{V}$.

Proof: Let $v, v' \in V$

Suppose $v = \alpha_1 v_1 + ... + \alpha_n v_n$

$v' = \beta_1 v_1 + ... + \beta_n v_n, \quad \alpha_i, \beta_i \in F$

If $v = v'$, then $\alpha_j = \beta_j$ for all $j = 1, ..., n$

$\therefore \quad \hat{v}_i(v) = \alpha_i = \hat{v}_i (v')$

$\therefore \hat{v}_i$ is well defined for all $i = 1, ..., n$

Also $\hat{v}_i(v + v') = \hat{v}_i(\overline{\alpha_1 + \beta_1} v_1 + ... + \overline{\alpha_n + \beta_n} v_n)$

$= \alpha_i + \beta_i$

$= \hat{v}_i(v) + \hat{v}_i(v')$

and $\hat{v}_i(\alpha v) = \hat{v}_i(\alpha\alpha_1 v_1 + ... + \alpha\alpha_n v_n)$

$= \alpha\alpha_i = \alpha \hat{v}_i(v)$

$\therefore \hat{v}_i$ is a *L.T.* for all $i = 1, ..., n$

By def., $\hat{v}_i(v_j) = (0v_1 + ... + 1v_j + ... + 0v_n) = 0$ if $j \neq i$

$= 1$ if $j = i$

$\therefore \quad \hat{v}_i(v_j) = \delta_{ij}$ for all $i, j = 1, ..., n$

Let $\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n = 0 \quad \alpha_i \in F$

Then $(\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n)(v_j) = 0(v_j) = 0$

$\Rightarrow \quad \alpha_j \hat{v}_j(v_j) = 0$

$\Rightarrow \quad \alpha_j = 0 \quad$ for all $j = 1, ..., n$

$\therefore$ $\{\hat{v}_1, ..., \hat{v}_n\}$ is *L.I.* over F.

Let $f \in \hat{V}$. Let $f(v_i) = \alpha_i \quad i = 1, ..., n$

Then $(\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n)\ (v_i)$

$= \alpha_i \hat{v}_i(v_i)$

$= \alpha_i \quad i = 1, ..., n$

$\therefore$ f and $\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n$ agree on all bases elements of V.

So, $f = \alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n$

$\therefore$ $\{\hat{v}_1, ..., \hat{v}_n\}$ spans $\hat{V}$.

Hence, $\{\hat{v}_1, ..., \hat{v}_n\}$ is a basis of $\hat{V}$, called *dual basis* of $\{v_1, ..., v_n\}$ s.t., $\hat{v}_i(v_j) = \delta_{ij}$.

Cor.: Let V be a finite dimensional vector space over F. Let $0 \neq v \in V$. Then $\exists$ $f \in \hat{V}$ s.t., $f(v) \neq 0$.

Proof: Since $v \neq 0$, $\{v\}$ is *L.I.* set. So, it can be extended to form a basis of V.

Let $\{v = v_1, v_2, ..., v_n\}$ be a basis of V.

Let $\{\hat{v}_1, ..., \hat{v}_n\}$ be corresponding dual basis. Then $\hat{v}_i(v_j) = \delta_{ij}$

$\therefore \quad \hat{v}_1(v_1) = 1$

Let $\quad f = \hat{v}_1 \in \hat{V}$

Then $\quad f(v) = f(v_1) = \hat{v}_1(v_1) = 1 \neq 0.$

Theorem 15: *Let V be a finite dimensional vector space over F.*

Define $\quad \theta : V \to \hat{\hat{V}}$ *s.t.,*

$\theta(v) = T_v$ *for all* $v \in V$

where $\quad T_v : \hat{V} \to F$ *s.t.,*

$T_v(f) = f(v)$ for all $f \in \hat{V}$

Then θ is an isomorphism from V onto $\hat{\hat{V}}$. (Here $\hat{\hat{V}}$ = dual of $\hat{V}$, called double dual of V).

Proof: Let $f, g \in \hat{V}$

Then $\quad T_v(f + g) = (f + g)\ (v)$

$= f(v) + g(v)$

$= T_v(f) + T_v(g)$

Let $\alpha \in F$

Then $\quad T_v(\alpha f) = (\alpha f)\ (v)$

$= \alpha f(v)$

$= \alpha T_v(f)$

$\therefore \quad T_v \in \hat{\hat{V}}$

θ is well defined as $v = v' \Rightarrow T_v(f) = f(v)$

$= f(v') = T_{v'}(f)$ for all $f \in \hat{V} \Rightarrow T_v = T_{v'}$

θ is a *L.T.* as

$$\theta(v + v') = T_{v+v'} = T_v + T_{v'} = \theta(v) + \theta(v')$$

as $T_{v+v'}(f) = f(v + v')$

$= f(v) + f(v')$

$= T_v(f) + T_{v'}(f)$

$= (T_v + T_{v'})(f)$ for all $f \in \hat{V}$

$T_{v+v'} = T_v + T_{v'}$

Also $\theta(\alpha v) = T_{\alpha v} = \alpha T_v = \alpha\theta(v)$

as $T_{\alpha v}(f) = f(\alpha v)$

$= \alpha f(v)$

$= \alpha T_v(f)$ for all $f \in \hat{V}$

$\therefore \quad T_{\alpha v} = \alpha T_v$

Let $0 \neq v \in \text{Ker } \theta \Rightarrow \theta(v) = 0 \Rightarrow T_v = 0$

By Cor. to Theorem 13 $\exists f \in \hat{V}$ s.t., $f(v) \neq 0$

$\therefore \quad T_v(f) \neq 0$

a contradiction as $T_v = 0 \Rightarrow T_v(f) = 0$

$\therefore \quad \text{Ker } \theta = \{0\} \Rightarrow \theta$ is 1-1

$\therefore \quad V \cong \theta(V) \subseteq \hat{\hat{V}}$

$\Rightarrow \quad \dim \theta(V) = \dim V = \dim \hat{V} = \dim \hat{\hat{V}}$ (by Theorem 14)

$\therefore \quad \theta(V) = \hat{\hat{V}}$ as $\theta(V)$ is a subspace of $\hat{\hat{V}}$

$\therefore$ θ is onto from V to $\hat{\hat{V}}$.

Thus θ is an isomorphism.

Cor. 1: Let V be a finite dimensional vector space over F. If L is a linear functional on $\hat{V}$, then $\exists$ a unique $v \in V$ s.t., $L(f) = f(v)$ for all $f \in \hat{V}$.

Proof: L is a linear functional on $\hat{V}$

$\Rightarrow L \in \hat{\hat{V}} \Rightarrow \exists$ unique $v \in V$ s.t.,

$\theta(v) = L$ as θ is 1-1 onto

$\therefore \quad T_v = L$

$\Rightarrow L(f) = T_v(f) = f(v)$ for all $f \in \hat{V}$.

Cor. 2: Let V be a finite dimensional vector space over the field F. Then each basis for $\hat{V}$ is the dual of some basis for V.

Proof: Let $\{f_1, ..., f_n\}$ be a basis for $\hat{V}$.

By theorem 13, $\exists$ a basis $\{L_1, ..., L_n\}$ for $\hat{\hat{V}}$ s.t., $L_i(f_j) = \delta_{ij}$. As in Cor. 1 $\exists$ unique $v_i \in V$ for each i

s.t., $L_i = T_{v_i} = \theta(v_i)$

Since $\{L_1, L_2, ..., L_n\}$ is a basis for $\hat{\hat{V}}$, $\{\theta^{-1} L_1, ..., \theta^{-1} L_n\} = \{v_1, ..., v_n\}$ is basis for V as θ is an isomorphism.

Also $\delta_{ij} = L_i(f_j) = T_{v_i}(f_j) = f_j(v_i)$

$\{f_1, ..., f_n\}$ is dual of basis $\{v_1, ..., v_n\}$ for V.

Problem 21: *Let V be the vector space of all polynomial functions from* **R** *to* **R** *which have degree less than or equal to* 2, *Let t_1, t_2, t_3 be three distinct real numbers and let $L_i : V \to F$ be s.t., $L_i(p(x)) = p(t_i)$, $i = 1, 2, 3$. Show that $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$. Determine a basis for V s.t., $\{L_1, L_2, L_3\}$ is its dual.*

Solution: $L_i\ (p(x) + q(x))$

$= L_i(r(x)),\quad r(x) = p(x) + q(x)$

$= r(t_i) = p(t_i) + q(t_i)$

$= L_i(p(x)) + L_i(q(x))$

Also $L_i(\alpha p(x)),\quad \alpha \in F$

$= L_i(q(x)),\ q(x) = \alpha p(x)$

$= q(t_i)$

$= \alpha p(t_i) = \alpha\ L_i(p(x))$ for all $i = 1, 2, 3$

$L_i \in \hat{V}$ for all $i = 1, 2, 3$

Let $\alpha_1 L_1 + \alpha_2 L_2 + \alpha_3 L_3 = 0$

Apply it on polynomials $1, x, x^2$ to get

$\alpha_1 + \alpha_2 + \alpha_3 = 0$

$\alpha_1 t_1 + \alpha_2 t_2 + \alpha_3 t_3 = 0$

$a_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 = 0$

$$\begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0,\ A = \begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix}$$

$\det A = (t_1 - t_2)\ (t_2 - t_3)\ (t_3 - t_1)$

$\neq 0$ as t_1, t_2, t_3 are distinct

Thus A^{-1} exists

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

Hence $\{L_1, L_2, L_3\}$ is a *L.I.* set.

Since dim $V = 3$, $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$.

Let $\{p_1(x), p_2(x), p_3(x)\}$ be a basis of V s.t., $\{L_1, L_2, L_3\}$ is its dual basis.

Then $L_1(p_1) = 1,\ L_2(p_1) = 0,\ L_3(p_1) = 0$

$L_2(p_1) = 0 \Rightarrow p_1(t_2) = 0$

$\Rightarrow t_2$ is a root of $p_1(x)$

$L_3(p_1) = 0 \Rightarrow p_1(t_3) = 0$

$\Rightarrow t_3$ is a root of $p_1(x)$

Since $\deg p_1(x) \le 2,$

$p_1(x) = \alpha(x - t_2)\ (x - t_3), \quad \alpha =$ constant

$L_1\ (p_1) = 1 \Rightarrow p_1(t_1) = 1$

$\Rightarrow \alpha(t_1 - t_2)\ (t_1 - t_3) = 1$

$$\Rightarrow \alpha = \frac{1}{(t_1 - t_2)\,(t_1 - t_3)}$$

$\therefore$ $$p_1(x) = \frac{(x - t_2)\,(x - t_3)}{(t_1 - t_2)\,(t_1 - t_3)}$$

Similarly, $$p_2(x) = \frac{(x - t_1)\,(x - t_3)}{(t_2 - t_1)\,(t_2 - t_3)},\ p_3(x) = \frac{(x - t_1)\,(x - t_2)}{(t_3 - t_1)\,(t_3 - t_2)}.$$

Problem 22: *Let V be the vector space of all polynomial functions p from* **R** *into* **R** *which have degree 2 or less. Define three linear functionals on V by*

$$f_1(p) = \int_0^1 p(x)\,dx,\ f_2(p) = \int_0^1 p(x)\,dx,$$

$$f_3(p) = \int_0^{-1} p(x)\,dx$$

Show that $\{f_1, f_2, f_3\}$ is basis of $\hat{V}$. Determine a basis for V s.t., $\{f_1, f_2, f_3\}$ is its dual basis.

Solution: It can be easily seen that $f_1, f_2, f_3 \in \hat{V}$.

Let $\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 = 0, \quad \alpha_i \in$ **R**

Apply it on $1, x, x^2$ to get

$$\alpha_1 + 2\alpha_2 - \alpha_3 = 0$$

$$\frac{\alpha_1}{2} + \frac{4}{2}\alpha_2 + \frac{\alpha_3}{2} = 0$$

$$\frac{\alpha_1}{3} + \frac{8}{3}\alpha_2 - \frac{\alpha_3}{3} = 0$$

Let $$A = \begin{bmatrix} 1 & 2 & -1 \\ 1 & 4 & 1 \\ 1 & 8 & -1 \end{bmatrix}$$

Then $$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0,\ \det A \neq 0$$

$$\therefore \qquad A^{-1}A\begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

$\therefore$ $\{f_1, f_2, f_3\}$ is a *L.I.* set.

Since dim $V = 3$, $\{f_1, f_2, f_3\}$ is a basis of $\hat{V}$.

Let $\{p_1(x), p_2(x), p_3(x)\}$, be a basis of V s.t., $\{f_1, f_2, f_3\}$ is its dual basis.

$\therefore$ $f_1(p_1) = 1, f_2(p_1) = 0, f_3(p_1) = 0$

Let $p_1(x) = c_o + c_1x + c_2x^2$

$$f_2(p_1) = 0 \Rightarrow c_o x + c_1\frac{x^2}{2} + c_2\frac{x^3}{3}\Big|_0^2 = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 0 \text{ when } x = 2$$

$$f_3(p_1) = 0 \Rightarrow c_o x + c_1\frac{x^2}{2} + c_2\frac{x^3}{3}\Big|_0^{-1} = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 0 \text{ when } x = -1$$

$\therefore$ $$c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = \alpha x(x-2)(x+1)$$

$$f_1(p_1) = 1 \Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 1 \text{ when } x = 1$$

$$\Rightarrow \alpha \cdot 1\,(-1)\,(2) = 1 \Rightarrow \alpha = -\frac{1}{2}$$

$$c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = -\frac{1}{2}x(x-2)(x+1)$$

$$= -\frac{1}{2}x^3 + \frac{1}{2}x^2 + x$$

$\therefore$ $$\frac{c_2}{3} = -\frac{1}{2},\ \frac{c_1}{2} = \frac{1}{2},\ c_o = 1$$

$\therefore$ $$c_o = 1,\ c_1 = 1,\ c_2 = -\frac{3}{2}$$

$\therefore$ $$p_1(x) = 1 + x - \frac{3}{2}x^2$$

Similarly, we can find $p_2(x)$, $p_3(x)$.

Definition: Let W be a sub-set of V.

Define $A(W) = \{f \in \hat{V} \mid f(w) = 0 \quad \text{for all } w \in W\}$

Then $A(W)$ is a sub-space of $\hat{V}$ as $\alpha, \beta \in F$,

$$\begin{aligned} f, g \in A(W) &\Rightarrow f(w) = 0 = g(w) \quad \text{for all } w \in W \\ &\Rightarrow \alpha f(w) + \beta g(w) = 0 \text{ for all } w \in W \\ &\Rightarrow (\alpha f + \beta g)(w) = 0 \quad \text{for all } w \in W \\ &\Rightarrow \alpha f + \beta g \in A(W) \end{aligned}$$

$A(W)$ is called *annihilator* of W.

Problem 23: *Let U, W be sub-sets of V. If $U \subseteq W$, show that $A(U) \subseteq A(W)$.*

Solution: Let $f \in A(W)$ then, $f(w) = 0$ for all $w \in W$

$$\begin{aligned} &\Rightarrow f(u) = 0 \quad \text{for all } u \in U \text{ as } U \subseteq W \\ &\Rightarrow f \in A(U). \end{aligned}$$

Theorem 16: *Let V be a finite dimensional vector space and W, a subspace of V. Then dim $A(W)$ = dim V – dim W.*

Proof: Let $\{w_1, ..., w_m\}$ be a basis of W.

It can be extended to form a basis of V.

Let $\{w_1, ..., w_m, v_{m+1}, ..., v_n\}$ be a basis of V.

Let $\{f_1, ..., f_m, f_{m+1}, ..., f_n\}$ be corresponding dual basis.

Then $f_i(w_j) = 0 \quad i = m+1, ..., n$

$$j = 1, ..., m$$

$\therefore$ $f_i \in A(W)$ for all $i = m+1, ..., n$

We show $\{f_{m+1}, ..., f_n\}$ is a basis of $A(W)$.

Let $\alpha_{m+1} f_{m+1} + ... + \alpha_n f_n = 0$

$\therefore$ $(\alpha_{m+1} f_{m+1} + ... + \alpha_n f_n)(v_k) = 0$ for all $k = m+1, .., n$

$\therefore$ $\alpha_k f_k (v_k) = 0$

$\therefore$ $\alpha_k = 0$ for all $k = m+1, ..., n$

So, $\{f_{m+1}, ..., f_n\}$ is a *L.I.* set.

Let $f \in A(W)$ then $f(w) = 0$ for all $w \in W$, $f \in \hat{V}$

$$\begin{aligned} f \in \hat{V} &\Rightarrow f = \beta_1 f_1 + ... + \beta_m f_m + ... + \beta_n f_n \\ &\Rightarrow 0 = f(w_j) = \beta_j f_j(w_j) = \beta_j \quad \text{for all } j = 1, ..., m \\ &\Rightarrow f = \beta_{m+1} f_{m+1} ... + \beta_n f_n \\ &\Rightarrow \{f_{m+1}, ..., f_n\} \text{ spans } A(W) \end{aligned}$$

$\therefore$ $\{f_{m+1}, ..., f_n\}$ is a basis of $A(W)$.

Hence dim $A(W) = n - m$ = dim V – dim W.

Cor. 1: $\dfrac{\hat{V}}{A(W)} \cong \hat{W}$

Proof: Since dim $\dfrac{\hat{V}}{A(W)}$ = dim $\hat{V}$ – dim $A(W)$

$$= \dim V - \dim V + \dim W$$

$$= \dim W = \dim \hat{W}$$

Hence $\dfrac{\hat{V}}{A(W)} \cong \hat{W}$.

Cor. 2: If V is a finite dimensional vector space and W, a subspace of V, then

$$A(A(W)) \cong W.$$

Proof: Define $\theta : W \to A(A(W))$ s.t.,

$$\theta(w) = T_w$$

where $T_w : \hat{W} \to F$ s.t.,

$$T_w(f) \to f(w)$$

$$T_w \in A(A(W)) \text{ as } T_w(f) = f(w) = 0 \quad \text{for all } f \in A(W)$$

Then as in Theorem 14, θ is well defined 1-1 linear transformation.

$\therefore$ $W \cong \theta(W) \subseteq A(A(W))$

Since $\dim A(A(W)) = \dim \hat{V} - \dim A(W)$

$$= \dim V - \dim A(W)$$

$$= \dim W \qquad \text{by Theorem 16}$$

and $\dim \theta(W) = \dim W$

$$A(A(W)) = \theta(W)$$

$\therefore$ θ is onto from W to $A(A(W))$

Hence $W \cong A(A(W))$.

For sake of convenience, we shall write $A(A(W)) = W$.

Consider for example, $V = \mathbf{R}^2$, $W = \{(x, 0) \mid x \in R\}$

Then $A(W)$ is a subspace of $\hat{V}$ spanned by f

where $f(x_1, x_2) = x_2$

In fact, $\{f\}$ is a basis of $A(W)$ as $\dim W = 1$.

Also, $A(A(W))$ is spanned by T_w where $w = (1, 0)$

Since $\dim A(A(W)) = 1$, $\{T_w\}$ is a basis of $A(A(W))$

Then $\theta : W \to A(A(W))$ s.t.,

$$\theta(w) = T_w$$

is an isomorphism as basis of W is mapped to basis of $A(A(W))$.

Problem 24: *Let W_1, W_2 be subspaces of finite dimensional vector space V. Determine $A(W_1 + W_2)$.*

Solution: $f \in A(W_1 + W_2)$

$\Leftrightarrow$ $f(x) = 0$ for all $x \in W_1 + W_2$

$\Leftrightarrow$ $f(w_1) = 0 = f(w_2)$ for all $w_1 \in W_1$, $w_2 \in W_2$

$\Leftrightarrow$ $f \in A(W_1) \cap A(W_2)$

$\therefore$ $A(W_1 + W_2) = A(W_1) \cap A(W_2)$.

Problem 25: *Let* f_1, f_2, f_3 *be three linear functionals on* $\mathbf{R}^4$ *defined as follows:*

$$f_1(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 2x_3 + x_4$$
$$f_2(x_1, x_2, x_3, x_4) = 2x_2 + x_4$$
$$f_3(x_1, x_2, x_3, x_4) = -2x_1 - 4x_3 + 3x_4$$

Determine the subspace W *of* $\mathbf{R}^4$ *s.t.,*

$$f_i(w) = 0,\ w \in W \quad i = 1, 2, 3.$$

Solution: Let $(x_1, x_2, x_3, x_4) \in W$

Then $f_i(x_1, x_2, x_3, x_4) = 0 \qquad i = 1, 2, 3$

$\therefore$ $x_1 + 2x_2 + 2x_3 + x_4 = 0$

$2x_2 = x_4 = 0$

$-2x_1 - 4x_3 + 3x_4 = 0$

$\therefore$
$$\begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ -2 & 0 & -4 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0$$

By elementary row transformations, we get

$$\begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0$$

$\therefore$ $x_1 + 2x_3 = 0,\ x_2 = 0,\ x_4 = 0$

$\therefore$ $(x_1, x_2, x_3, x_4) = (-2x_3, 0, x_3, 0) = x_3(-2, 0, 1, 0)$

$\therefore$ W is spanned by $(-2, 0, 1, 0)$.

Problem 26: *Let* W *be the subspace of* $\mathbf{R}^5$ *spanned by the vectors*

$$\alpha_1 = (2, -2, 3, 4, -1),\ \alpha_3 = (0, 0, -1, -2, 3)$$
$$\alpha_2 = (-1, 1, 2, 5, 2),\ \alpha_4 = (1, -1, 2, 3, 0)$$

Describe $A(W)$.

Solution: Let $f \in A(W)$

Then $f(w) = 0$ for all $w \in W$

$\Rightarrow f(\alpha_i) = 0$ for all $i = 1, 2, 3, 4$

Let $f(x_1, x_2, x_3, x_4, x_5) = c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$

(Note $v_1 = (1, 0, 0, 0, 0)$, $v_2 = (0, 1, 0, 0, 0)$, $v_3 = (0, 0, 1, 0, 0)$, $v_4 = (0, 0, 0, 1, 0)$, $v_5 = (0, 0, 0, 0, 1)$ form a basis of $\mathbf{R}^5$).

Let $\{\hat{v}_1, \hat{v}_2, \hat{v}_3, \hat{v}_4, \hat{v}_5\}$ be its dual basis.

Then $f = c_1\hat{v}_1 + c_2\hat{v}_2 + c_3\hat{v}_3 + c_4\hat{v}_4 + c_5\hat{v}_5$

$$\Rightarrow f(x_1, x_2, x_3, x_4, x_5) = \sum_{1}^{5} c_i\hat{v}_i\,(x_1, x_2, x_3, x_4, x_5)$$

$$= \sum_{1}^{5} c_i \hat{v}_i\,(x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4 + x_5v_5)$$

$$= c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$$

as $\hat{v}_i\,(v_j) = \delta_{ij}$

$\therefore$ $f(\alpha_i) = 0$ for all $i = 1, 2, 3, 4$

$$\Rightarrow \begin{bmatrix} 2 & -2 & 3 & 4 & -1 \\ -1 & 1 & 2 & 5 & 2 \\ 0 & 0 & 1 & -2 & 3 \\ 1 & -1 & 2 & 3 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 0$$

By elementary row transformations, we get

$$\begin{bmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 0$$

$\Rightarrow c_1 - c_2 - c_4 = 0,\ c_3 + 2c_4 = 0,\ c_5 = 0$

$\Rightarrow 2c_1 - 2c_2 + c_3 = 0,\ c_5 = 0,\ c_3 = -2c_4$

Let $c_2 = a,\ c_4 = b$

Then $c_3 = -2b$

$2c_1 - 2a - 2b = 0 \Rightarrow c_1 = a + b$

$\Rightarrow f(x_1, x_2, x_3, x_4, x_5) = (a + b)\,x_1 + ax_2 - 2bx_3 + bx_4$

Take $a = 1,\ b = 0$

Then $f_1(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2$

Take $a = 0,\ b = 1$

Then $f_2(x_1, x_2, x_3, x_4, x_5) = x_1 - 2x_3 + x_4$

$\therefore$ $f = af_1 + bf_2$

$\therefore$ $\{f_1, f_2\}$ spans $A(W)$

Let $\alpha f_1 + \beta f_2 = 0$. Apply it on v_1, v_2 respectively. We get $\alpha + \beta = 0,\ \alpha = 0 \Rightarrow \beta = 0$.

$\therefore$ $\{f_1, f_2\}$ is *L.I.* So, $\{f_1, f_2\}$ is a basis of $A(W)$

Hence $\dim A(W) = 2$.

Problem 27: *Let V be a finite dimensional vector space. Suppose $V = W_1 \oplus W_2$, where W_1, W_2 are subspaces of V. Show that $\hat{V} = A(W_1) \oplus A(W_2)$.*

Solution: $\dim V = \dim (W_1 \oplus W_2)$

$= \dim W_1 + \dim W_2$

Also dim $(A(W_1) \oplus A(W_2))$

$= \dim A(W_1) + \dim A(W_2)$

$= \dim V - \dim W_1 + \dim V - \dim W_2$

$= 2 \dim V - (\dim W_1 + \dim W_2)$

$= 2 \dim V - \dim V = \dim V = \dim \hat{V}$

Since $A(W_1) \oplus A(W_2)$ is a subspace of $\hat{V}$

and dim $\hat{V}$ = dim $(A(W_1) \oplus A(W_2))$,

$\hat{V} = A(W_1) \oplus A(W_2)$.

Problem 28: *If f and g are in $\hat{V}$ s.t., $f(v) = 0$ implies $g(v) = 0$, prove that $g = cf$ for some $c \in F$.*

Solution: If $f = 0$, then $g = 0 = cf$ where $c = 0 \in F$.

Let $f \neq 0$ then $\exists\ v \neq 0$ in V s.t., $f(v) \neq 0$

Let $c = \dfrac{g(v)}{f(v)}$

$h = g - cf$ and $x \in V$

and $\alpha = \dfrac{f(x)}{f(v)}$.

Then $f(x - \alpha v) = f(x) - \alpha f(v) = 0$

$\Rightarrow x - \alpha v \in \text{Ker } f$

$\Rightarrow x - \alpha v = y \in \text{Ker } f$

$\Rightarrow x = y + \alpha v$

$\therefore\ h(x) = g(x) - cf(x)$

$= g(y) + \alpha g(v) - cf(y) - c\alpha f(v)$

$= \alpha g(v) - c\alpha f(v)$ as $y \in \text{Ker } f \Rightarrow y \in \text{Ker } g$

$= \alpha g(v) - \alpha g(v) = 0$ for all $x \in V$

$\therefore\ h = 0 \Rightarrow g = cf$

Hence the result follows.

Definition: Consider the system of m equations

$a_{11}x_1 + \ldots + a_{1n}x_n = 0$

$\ldots \quad \ldots \quad \ldots$

$a_{m1}x_1 + \ldots + a_{mn}x_n = 0$, where $a_{ij} \in F$

in n unknowns.

Let U be the subspace of $F^{(n)}$ generated by m vectors

$u_1 = (a_{11}, \ldots, a_{1n}), \ldots, u_m = (a_{m1}, \ldots, a_{mn})$

If dim $U = r$, we say the system of equations has rank r.

We determine the number of linearly independent solutions to the system of equations in $F^{(n)}$. Consider

Theorem 17: *If the system of homogeneous linear equations*

$$a_{11}x_1 + \ldots + a_{1n}x_n = 0$$
$$\ldots \quad .. \quad \ldots$$
$$a_{m1}x_1 + \ldots + a_{mn}x_n = 0,$$

where $a_{ij} \in F$ *is of rank r, then there are* $n - r$ *linearly independent solutions in* $F^{(n)}$.

Proof: Let S be the set of solutions of the given system of equations

$S = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in F^n \mid \sum a_{ij}\,\alpha_j = 0, \quad i = 1, 2, .., m\}$

Then S is a subspace of $F^n = V$

Let $\{v_1, v_2, \ldots, v_n\}$ be the standard basis of V

and $\{f_1, f_2, \ldots, f_n\}$ be its dual basis

Let U be the subspace of V as described above

Define $\theta : S \to A(U)$, s.t.,

$$\theta((\alpha_1, \alpha_2, \ldots, \alpha_n)) = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$$

Let $f = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$

Then $f(u_1) = (\alpha_1 f_1 + \ldots + \alpha_n f_n)\,(a_{11}v_1 + \ldots + a_{1n}v_n)$

$= \alpha_1 a_{11} + \ldots \alpha_n a_{1n}$

$= 0$ as $(\alpha_1, \ldots, \alpha_n) \in S$

Similarly $f(u_2) = \ldots = f(u_m) = 0$

So $f \in A(U)$

It can be easily shown that θ is a linear transformation.

If $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in$ Ker θ then $\sum_1^n \alpha_i f_i = 0$

$\Rightarrow \alpha_i = 0 \quad \forall\ i$

$\Rightarrow$ Ker $\theta = \{0\}$ or that θ is 1–1.

Let now $f \in A(U) \subseteq \hat{V}$

and suppose $f = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$

Then $0 = f(u_1) = \alpha_1 a_{11} + \ldots + \alpha_n a_{1n}$

$\ldots \quad \ldots \quad \ldots$

$0 = f(u_m) = \alpha_1 a_{m1} + \ldots + \alpha_n a_{mn}$

$\therefore (\alpha_1, \alpha_2, \ldots, \alpha_n) \in S$

and $\theta((\alpha_1, \alpha_2, \ldots, \alpha_n)) = \alpha_1 f_1 + \ldots + \alpha_n f_n = f$

or that θ is onto.

Hence $S \cong A(U)$

$\Rightarrow$ dim S = dim $A(U)$ = dim V – dim U

$= n - r$

Hence there are $n - r$ linearly independent solutions of the given system of equations.

Cor.: If $n > m$, that is, if the number of unknowns exceed the number of equations, then the system of equations has a non zero solution.

Proof: Since U is generated by m vectors, $r = \dim U \leq m < n \Rightarrow n - r > 0 \Rightarrow$ system of equations has a linearly independent solution, which is non zero (as zero vector is not linearly independent).

Problem 28: *Let m and n be positive integers. Let* $f_1, ..., f_m$ *be linear functionals on* $F^{(n)}$. *For* α *in* $F^{(n)}$ *define* $T(\alpha) = (f_1(\alpha), ..., f_m(\alpha))$.

Show that T is a linear transformation from $F^{(n)}$ *into* $F^{(m)}$. *Then show that every linear transformation from* $F^{(n)}$ *into* $F^{(m)}$ *is of the above form, for some* $f_1, ..., f_m$.

Solution: Since $f_1, ..., f_m$ are linear transformations, so is T. Let $\{e_1, ..., e_n\}$ be the standard basis of $F^{(n)}$.

Then $T(e_i) \in F^{(m)} \quad \forall\, i = 1, ..., n.$

So, $T(e_i) = (\beta_{i1}, ..., \beta_{im}) \quad \forall\, i = 1, ..., n.$

$\therefore$ $T(\alpha) = T(\alpha_1 e_1 + ... + \alpha_n e_n),\ \alpha = \alpha_1 e_1 + ... + \alpha_n e_n$

$= \alpha_1 T(e_1) + ... + \alpha_n T(e_n)$

$= \alpha_1(\beta_{11}, ..., \beta_{1m}) + ... + \alpha_n(\beta_{n1}, ..., \beta_{nm})$

$= (\alpha_1\beta_{11} + ... + \alpha_n\beta_{n1}, ..., \alpha_1\beta_{1m} + ... + \alpha_n\beta_{nm})$

For each $i (1 \leq i \leq m)$, $\exists$ a linear transformation

$f_i : F^{(n)} \to F$ s.t.,

$f_i(e_1) = \beta_{1i}, ..., f_i(e_n) = \beta_{ni}$

$\therefore$ $f_1(\alpha) = f_1(\alpha_1 e_1 + ... + \alpha_n e_n)$

$= \alpha_1\beta_{11} + ... + \alpha_n\beta_{n1}$

.....

$f_m(\alpha) = f_m(\alpha_1 e_1 + ... + \alpha_n e_n)$

$= \alpha_1\beta_{1m} + ... + \alpha_n\beta_{nm}$

So, $T(\alpha) = (f_1(\alpha), ..., f_m(\alpha))$.

Problem 29: *Let V be the vector space of all* 2×2 *matrices over the field of real numbers, and let*

$$B = \begin{bmatrix} 2 & -2 \\ -1 & 1 \end{bmatrix}$$

Let W be the subspace of V consisting of all A such that $AB = 0$. *Let f be a linear functional on V which is in the annihilator of W. Suppose that* $f(I) = 0$ *and* $f(C) = 3$, *where I is the* 2×2 *identity matrix and*

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Find $f(B)$.

Solution: Now $W = \{A \mid AB = 0\}$

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in V$

Then $A = a_{11}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{12}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{21}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{22}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$\therefore \quad f(A) = a_{11}f\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{12}f\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{21}f\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{22}f\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$= a_{11}\alpha + a_{12}\beta + a_{21}\gamma + a_{22}\delta$ (say).

$\therefore \quad 0 = f(I) = \alpha + \delta$

$3 = f(C) = \delta$

So, $\alpha = -3, \delta = 3$

Let $D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$. Then $DB = 0$

So, $D \in W$

$\Rightarrow f(D) = 0$ as $f \in A(W)$.

$\therefore \quad 0 = \alpha + 2\beta \Rightarrow \beta = \frac{3}{2}$

Also, let $E = \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix}$.

Then $EB = 0$.

So, $E \in W$.

$\Rightarrow f(E) = 0$ as $f \in A(W)$

$\therefore \quad \gamma + 2\delta = 0 \Rightarrow \gamma = -6$

So, $f(B) = 2 \times (-3) + (-2)\left(\frac{3}{2}\right) + (-1)(-6) + (3)(1)$

$= -6 - 3 + 6 + 3 = 0.$

Problem 30: *Let F be a subfield of complex numbers. We define n linear functionals on* $F^{(n)}$ $(n \geq 2)$ *by*

$$f_k(x_1, \ldots, x_n) = \sum_{j=1}^{n} (k - j)x_j, \quad 1 \leq k \leq m.$$

What is the dimension of the subspace annihilated by $f_1, \ldots, f_n$?

Solution: Now $f_1(x_1, \ldots, x_n) = ox_1 - x_2 - 2x_3 \ldots - (n-1)x_n$

$f_2(x_1, \ldots, x_n) = x_1 + ox_2 - x_3 \ldots - (n-2)x_n$

$f_3(x_1, \ldots, x_n) = 2x_1 + x_2 + ox_3 \ldots - (n-3)x_n$

.....

$f_n(x_1, \ldots, x_n) = (n-1)x_1 + (n-2)x_2 + (n-3)x_3 + \ldots + 1\, x_{n-1} + ox_n$

Let W be the subspace of $F^{(n)}$ annihilated by $f_1, \ldots, f_n$.

Then $(x_1, \ldots, x_n) \in W$

$\Rightarrow f_k(x_1, \ldots, x_n) = 0 \quad \forall\ k = 1, 2, \ldots, n.$

$$\begin{bmatrix} 0 & -1 & -2 & \ldots & \ldots & -(n-1) \\ 1 & 0 & -1 & \ldots & \ldots & -(n-2) \\ 2 & 1 & 0 & \ldots & \ldots & -(n-3) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ n-1 & n-2 & n-3 & \ldots & \ldots & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = 0$$

i.e., $AX = 0$, where A is the matrix on the left and $X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$.

It can be easily seen that Rank $A = 2$.

$\therefore$ number of linear independent solutions in W is $n - 2$.

$\therefore$ dim $W = n - 2$.

Problem 31: *Let V be a finite dimensional vector space and W_1 and W_2 be subspaces of V such that $A(W_1) = A(W_2)$. Show that $W_1 = W_2$.*

Solution: Let $W_1 \neq W_2$. Suppose $W_1 \subsetneq W_2$. Then there exists $x \in W_1$ such that $x \notin W_2$.

Let $\{x_1, x_2, \ldots x_r\} = S$ be a basis of W_2.

Then $L(S) = W_2$.

Now $x \notin L(S)$ and S is a linearly independent set in V, $S \cup \{x\}$ is a linearly independent set. It can be extended to a basis of V.

Let $\{x_1, x_2, \ldots x_r, x = x_{r+1}, \ldots, x_n\}$ be a basis of V.

Let $\{f_1, f_2, \ldots, f_r, f_{r+1}, \ldots f_n\}$ be its dual basis

Then $f_{r+1}(x_1) = f_{r+1}(x_2) = \ldots = f_{r+1}(x_r) = 0$

So, $f_{r+1} \in A(W_2)$

Since $A(W_2) = A(W_1),\ f_{r+1} \in A(W_1)$

Now $x = x_{r+1} \in W_1$ and $f_{r+1}(x) = f_{r+1}(x_{r+1}) = 1 \neq 0$

contradicting $f_{r+1} \in A(W_1)$

So, $W_1 = W_2$.

Transpose of a Linear Transformation

Let V, W be vector spaces over F.

Let T be a linear transformation from V into W.

Define $T^t : \hat{W} \to \hat{V}$ s.t.,

$T^t(g) = gT$

Then T^t is a linear transformation called the *transpose* of T.

It can be easily shown that

(*i*) $(T_1 + T_2)^t = T_1^t + T_2^t$, where T_1, T_2 are linear transformations from V into W.

(*ii*) $(T_1T_2)^t = T_2^t T_1^t$, where $T_1 : W \to V$ and $T_2 : V \to W$ are linear transformations

(*iii*) $(\alpha T)^t = \alpha T^t$, $\alpha \in F$, $T : V \to W$ is a linear trasnsformation

(*iv*) $I^t = I$, $I : V \to V$ is the identity map.

Theorem 18: *Let $T : V \to W$ be a linear transformation. Then*

(*a*) *The null space of T^t = the annihilator of range of T.*

(*b*) *If V, W are finite dimensional, then*

(*i*) *rank of T = rank of T^t*

(*ii*) *range of T^t = annihilator of the null space of T.*

Proof: (*a*) Now $g \in$ Null space of T^t

$\Leftrightarrow T^t(g) = 0$

$\Leftrightarrow gT = 0 \Leftrightarrow gTV = 0 \Leftrightarrow g(\text{Range } T) = 0$

$\Leftrightarrow g \in A(R_T)$

Where $A(R_T)$ denotes the annihilator of range T.

(*b*) Let dim $V = n$, dim $W = m$,

Let r = rank of T = dim R_T = dim $T(V)$

where R_T denotes the range of T.

Now dim $A(R_T)$ = dim $A(TV)$

= dim W – dim $T(V) = m - r$

Nullity of T^t = dimension of the null space of T^t

= dim $A(R_T) = m - r$

But nullity of T^t = dim W – rank T^t

= dim W – rank T^t

$\Rightarrow \quad m - r = m -$ rank T^t

$\Rightarrow \quad$ rank $T^t = r =$ rank T

This proves (*i*).

Let N denote the null space of T.

Then $A(N) = \{f \in \hat{V} \mid f(n) = 0 \ \forall \ n \in N\}$ = Annihilator of the null space of T.

Now $f \in$ Range T^t

$\Rightarrow \quad f = T^t g, \quad g \in W$

$= gT$

$\Rightarrow \quad f(n) = gT(n) = g(0) = 0 \quad \forall \ n \in N$

$\Rightarrow \quad f \in A(N)$

$\Rightarrow$ Range $T^t \subseteq A(N)$

So, dim $A(N)$ = dim V – dim N

= dim V – nullity T = rank T

= rank T^t = dim Range T^t

Therefore, $A(N)$ = Range T^t

This proves (*ii*).

Lemma: *Let $T : V \to W$ be a linear transformation. Let $\beta = \{v_1, \ldots, v_n\}$, $\beta' = \{w_1, \ldots, w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, \ldots, f_n\}$ be the dual basis of V such that $f_i(v_j) = \delta_{ij}$. Let $F \in \hat{V}$.*

Then

$$f = \sum_1^n f(v_i)\, f_i$$

Proof: Sppose $f = \sum_1^n c_i\, f_i,\ c_i \in F$

Then $$f(v_j) = \sum c_i f_i(v_j) = \sum c_i\, \delta_{ij} = c_j$$

So, $$f = \sum_1^n f(v_i)\, f_i.$$

Theorem 19: *Let $T : V \to W$ be a linear transformation. Let $\beta = \{v_1, \ldots, v_n\}$, $\beta' = \{w_1, \ldots, w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, \ldots, f_n\}$, $\hat{\beta}' = \{g_1, \ldots, g_m\}$ be the dual basis of V, W respectively.*

Let $A = (a_{ij})$ be the matrix of T w.r.t. β, β' and $B = (b_{ij})$ be the matrix of T^t w.r.t., $\hat{\beta}'\ \hat{\beta}$.

Then $a_{ij} = b_{ji}\ \forall\ i, j.$

(This shows that the matrix of T^t is the transpose of the matrix of T. For this reason T^t is called the transpose of T.)

Proof: Now $T^t : \hat{W} \to \hat{V}$ s.t.,

$$T^t(g_j) = g_j T = f \text{ (say)}$$

Then
$$\begin{aligned} f(v_i) &= (T^t g_j)\ (v_i) \\ &= (g_j T)\ (v_i) \\ &= (g_j T)\ (v_i) = g_j \left(\sum_1^m a_{ki}\ w_k \right) \\ &= \sum a_{ki}\, g_j(w_k) = \sum a_{ki}\, \delta_{jk} = a_{ji} \end{aligned}$$

By above lemma,

$$f = \sum_1^n f(v_j) f_i = \sum_1^n a_{ji} f_i$$

But $$f = T^t g_j = \sum_1^n b_{ij} f_i$$

So, $\sum_1^n b_{ij} f_i = \sum_1^n a_{ji} f_i$

$\Rightarrow \sum_1^n (b_{ij} - a_{ji}) f_i = 0$

$\Rightarrow b_{ij} = a_{ji} \ \forall\ i, j$. This proves the theorem.

Let $A = (a_{ij})$ be the $m \times n$ matrix over F. Then *row rank* of A is defined as the dimension of the subspace of $F^{(n)}$ spanned by $(a_{11}, ..., a_{1n})$, ..., $(a_{m1}, ..., a_{mn})$.

Similarly, *column rank* of A is defined as the dimension of the subspace of $F^{(m)}$ spanned by $(a_{11}, a_{21}, ..., a_{m1})$, ..., $(a_{1n}, ..., a_{mn})$.

Theorem 20: *Let A be an $m \times n$ matrix over F. Then*
Row rank of A = column rank of A.

Proof: Define $T : F^{(n)} \to F^{(m)}$ s.t.,

$T((x_1, ..., x_n)) = (y_1, ..., y_m)$

where $y_i = \sum_{j=1}^n a_{ij} x_j$

Then T is a linear transformation.

Range $T = \{T(x_1, ..., x_n) \mid x_i \in F\}$

$= \{T(x_1 (1, ..., 0) + ... + x_n(0, -0, 1)) \mid x_i \in F\}$

$= \{x_1 T(e_1) + ... + x_n\ T(e_n) \mid x_i \in F\}$

e_i = nth-tuple with ith co-ordinate 1 and zero elesewhere

$=$ {linear combination of columns of A}

$\subseteq$ subspace generated by columns of A and vice-versa

Thus, Range T = subspace of $F^{(n)}$ generated by columns of A

So, Rank T = column rank of A

Also, Rank T^t = column rank of A^t

= dimension of subspace of $F^{(m)}$ generated by columns of A^t

= dimension of subspace generated by rows of A

= Row rank of A

Thus, column rank of A

= Row rank of A (as Rank T^t = Rank T)

= Rank T.

Problem 32: *Let V be a finite dimensional vector space over F. Let T be a linear operator on V. Let $c \in F$. Suppose $\exists\ 0 \neq v \in V$ such that $T(v) = cv$. Prove that there is a non zero linear functional f on V s.t., $T^t f = cf$.*

Solution: Now $(T - cI)v = 0$, $v \neq 0$

$\Rightarrow v \in$ Ker $(T - cI)$

$\Rightarrow$ Ker $(T - cI) \neq \{0\}$
$\Rightarrow$ dim Ker $(T - cI) \geq 1$
$\Rightarrow$ nullity of $(T - cI) \geq 1$
$\Rightarrow$ rank of $(T - cI) < n$
$\Rightarrow$ rank of $(T - cI)^t < n$
$\Rightarrow$ nulity of $(T - cI)^t \geq 1$
$\Rightarrow \exists f \in \hat{V}$ such that $f \neq 0$ and $(T - cI)^t f = 0$
$\Rightarrow T^t f = cf, f \neq 0.$

Problem 33: *Let A be $m \times n$ matrix with real entries. Prove that $A = 0 \Leftrightarrow$ Trace $(A^tA) = 0$.*

Solution: Let $A^t = B = (b_{ij})_{n \times m}$
$A = (a_{jk})_{m \times n}$

$$A^tA = BA = C = (c_{ik}), \quad c_{ik} = \sum_{j=1}^{m} b_{ij}\, a_{jk}$$

Trace $(A^tA) = 0$

$$\Rightarrow \sum_{1}^{n} c_{ii} = 0$$

$$\Rightarrow c_{11} + \ldots + c_{nn} = 0$$

$$\Rightarrow \sum_{1}^{m} b_{ij}a_{ji} + \ldots + \sum_{1}^{m} b_{nj}a_{jn} = 0$$

$$\Rightarrow \sum (a_{ji})^2 + \ldots + \sum (a_{jn})^2 = 0$$

$\Rightarrow a_{ji} = 0 \quad \forall\ i, j$
$\Rightarrow A = 0.$

Converse is obvious.

Exercises

1. Let $S = \{\alpha_1, \alpha_2, \alpha_3\}$ be the basis of $\mathbf{C}^3$ defined by
$\alpha_1 = (1, 0, -1), \alpha_2 = (1, 1, 1), \alpha_3 = (2, 2, 0)$
Find the dual basis of S,

$$\{f_1(\alpha) = a - b, f_2(\alpha) = a - b + c, f_3(\alpha) = -\frac{a}{2} + b - \frac{c}{2}, \alpha = (a, b, c)\}$$

2. Let $\{e_1, \ldots, e_n\}$ be the standard basis of $F^{(n)}$ (F = field). Define
$\pi_i : F^{(n)} \to F$ s.t.,
$\pi_i (a_1, \ldots, a_n) = a_i$
Show that π_i is a linear functional for all i and $\{\pi_1, \ldots, \pi_n\}$ is dual basis of $\{e_1, \ldots, e_n\}$.

3. Let F be a subfield of the field of complex numbers and V a vector space over F. Suppose that f and g are linear functionals on V such that the function h defined by $h(v) = f(v)\, g(v)$ is also a linear functional on V. Prove that

(i) $h(v) = 0$ for all $v \in V$

(ii) $f = 0$ or $g = 0$

(Hint: (ii) suppose $g \neq 0$, $\exists\ v \in V$ s.t., $g(v) \neq 0 \Rightarrow f(v) = 0$

$\therefore f(x - v)\, g(x - v) = 0$ for all $x \in V \Rightarrow f(x)\, g(v) = 0$ for all $x \in V$).

4. Let V be the vector space of polynomials over $\mathbf{R}$ of degree ≤ 1. Let $\varphi_1 : V \to \mathbf{R}$, $\varphi_2 : V \to \mathbf{R}$ be defined by

$$\varphi_1(f(x)) = \int_0^1 f(x)dx, \quad \varphi_2(f(x)) = \int_0^1 f(x)dx$$

Show that $\{\varphi_1, \varphi_2\}$ is a basis of $\hat{V}$. Find a basis $\{v_1, v_2\}$ of V which is dual to $\{\varphi_1, \varphi_2\}$. $\left[\{2 - 2x, -\frac{1}{2} + x\}\right]$.

5. Suppose $u, v \in V$ and that $\varphi(u) = 0 \Rightarrow \varphi(v) = 0$ for all $\varphi \in \hat{V}$. Show that $v = \alpha u$ for some scalar α.

6. Let W be the subspace of $\mathbf{R}^3$ spanned by (1, 1, 0) and (0, 1, 1). Find a basis of the annihilator of W. $[\varphi(x, y, z) = x - y + z]$

7. Let W be the subspace of $\mathbf{R}^4$ spanned by (1, 2, – 3, 4), (1, 3, – 2, 6) and (1, 4, –1, 8). Find a basis of the annihilator of W.

$[\varphi_1(x, y, z, t) = 5x - y + z,\ \varphi_2(x, y, z, t) = 2y - t]$

8. Let W_1, W_2 be subspaces of a finite dimensonal vector space. Show that

$$A(W_1 \cap W_2) = A(W_1) + A(W_2)$$

(Hint: apply problem (24) on $A(W_1)$ and $A(W_2)$).

9. Let n be a +ve integer and F, a field. Let

$$W = \{(x_1, \ldots, x_n) \in F^{(n)} \mid x_1 + \ldots + x_n = 0\}$$

Prove that $\mathrm{A(W)} = \{f \mid f(x_1, \ldots, x_n) = c \sum_{j=1}^{n} x_j\}$

10. Let W be a subspace of a finite dimensional vector space. Define

$$\theta : \hat{V} \to \hat{W} \text{ s.t.,}$$

$$\theta(f) = f \mid W = \bar{f}\ (\bar{f}(w) = f(w) \quad \text{for all } w \in W)$$

Show that θ is onto linear transformation and Ker $\theta = A(W)$.

(Thus $\frac{\hat{V}}{A(W)} \cong \hat{W}$).

A Quick Look at what's been done

- A *L.T.* $T: V \to V$ is one-one iff T is onto.
- **Sylvester's law** says that if $T: V \to W$ is a linear transformation then *Rank* T + *Nullity* T = *dim* V.
- Under algebra of linear transformations, sums, products (composition) and scalar multiples of linear transformations are discussed.
- A *L.T.* $T: V \to V$ is called a **linear operator** on V, whereas a *L.T.* $T: V \to F$ is called a **linear function**.
- If V and W be two vector spaces over F of dim m and n respectively then dim Hom(V, W) = mn.
- A *L.T.* is called **non-singular** if its Ker is {0}, i.e., it is one-one. A *L.T.* $T: V \to W$ is non-singular iff T carries each *L.I.* subset of V onto a *L.I.* subset of W.
- Matrix of a linear transformation is defined. If $M_{m\times n}(F)$ denotes the vector space of all $m \times n$ matrices over F then Hom $(U,V) \cong M_{m\times n}(F)$ and dim Hom(U, V) = mn.
- Hom (V, F) is called **dual space** of V over F. Dimension of the dual space is same as dimension of the vector space.
- If W be a subspace of V then $A(W)$, the **annihilator** of W, is defined to be the set containing those members of dual of V that map all w in W to 0. Also, dim$A(W)$= dim V – dim W.
- If W is a subspace of a *F.D.V.S.* V then $A(A(W)) \cong W$.
- Using dual spaces, we have shown that if the number of unknowns exceeds the number of equations in a system of equations then the system has a non-zero solution.
- If T^t denotes the **transpose** of the *L.T.* T then matrix of T^t is the transpose of the matrix of T.

12

Eigen Values and Eigen Vectors

Introduction

In this chapter we will be dealing with linear operators T on a finite dimensional vector space V. The main idea is to find an ordered basis β of V s.t., matrix of T w.r.t. β is a diagonal matrix. We can know a lot about T through this. The question that arises is "Can we find such an ordered basis for all linear operators?" and if not then for which operators such a basis would exist? We shall attempt to answer it in this chapter. If $\beta = \{v_1, ..., v_n\}$ s.t. $[T]_\beta = \text{diag}\ (c_1, ..., c_n)$, then $T(v_i) = c_i v_i$, $i = 1, ..., n$. This leads us to the concept of eigen values c_i and eigen vectors v_i of T.

Definition: Let V be a vector space over F. Let T be a linear operator on V. If $\exists\ 0 \neq v \in V$ s.t., $T(v) = cv$ for some $c \in F$, then v is called an *eigen vector* or *characteristic vector* of T and c is called an *eigen value* or *characteristic value* or *characteristic root* of T.

Example 1: Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be a linear operator defined by $T(x, y) = (x, 0)$. If $c \in \mathbf{R}$ is an eigen value of T, then $\exists\ (x, y) \neq (0, 0)$ in $\mathbf{R}^2$ s.t. $T(x, y) = c(x, y)$

$$\therefore \quad (x, 0) = c(x, y) = (cx, cy) \Rightarrow cx = x,\ cy = 0$$

$$\Rightarrow x(c - 1) = 0,\ cy = 0$$

Now $\quad x(c - 1) = 0 \Rightarrow x = 0$ or $c = 1$

If $x = 0$, then $y \neq 0$. $\therefore\ cy = 0 \Rightarrow c = 0$

If $c = 0$, then $(0, 1)$ is an eigen value of T as $T(0, 1) = (0, 0) = c(0, 1)$.

$\therefore$ 0 is an eigen value of T. If $c \neq 0$, then $y = 0$ and $c = 1$.

$\therefore\ T(1, 0) = (1, 0) = 1\ (1, 0) \Rightarrow (1, 0)$ is an eigen vector of T and 1 is an eigen value of T.

Example 2: Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be a linear operator defined by $T(x, y) = (x + y, x + y)$.

Then $T(1, -1) = (0, 0) = 0(1, -1) \Rightarrow 0$ is an eigen value of T and $(1, -1)$ is an eigen value of T.

Also $T(1, 1) = (2, 2) = 2(1, 1) \Rightarrow 2$ is an eigen value of T and $(1, 1)$ is an eigen vector of T.

Problem 1: *Let v and w be eigen vectors of T corresponding to two distinct eigen values of T(a linear operator on V). Show that v + w cannot be an eigen vector of T.*

Solution: Let $T(v) = \alpha v$

$T(w) = \beta w, \quad \alpha \neq \beta$

We first show that $\{v, w\}$ is a linearly independent set.

Let $av + bw = 0$

Then $T(av + bw) = 0$

$\Rightarrow aT(v) + bT(w) = 0$

$\Rightarrow a\alpha\, v + b\beta\, w = 0$

$\Rightarrow -b\alpha\, w + b\beta\, w = 0$

$\Rightarrow (b\beta - b\alpha)w = 0$

$\Rightarrow b\beta - b\alpha = 0$, as $w \neq 0$

$\Rightarrow b(\beta - \alpha) = 0$

$\Rightarrow b = 0$, as $\beta - \alpha \neq 0$

$\Rightarrow a = 0$

So, $\{v, w\}$ is a linearly independent set.

Suppose $v + w$ is an eigen vector of T.

Let $T(v + w) = c(v + w)$

Then $T(v) + T(w) = cv + cw$

$\Rightarrow \alpha v + \beta w = cv + cw$

$\Rightarrow (\alpha - c)v + (\beta - c)w = 0$

$\Rightarrow \alpha - c = 0 = \beta - c$, as $\{v, w\}$ is a linearly independent set.

$\Rightarrow \alpha = \beta$, a contriadiction.

Hence $v + w$ is not an eigen vector of T.

Problem 2: *Suppose every non zero vector of a FDVS is an eigen vector of a linear operator T on V. Show that T is a scalar multiple of I.*

Solution: Let $0 \neq v \in V$.

By hypothesis $T(v) = cv$.

Let $w \in \langle v \rangle$

Then $w = av$

$\Rightarrow T(w) = aT(v) = acv = c\, w$

Let $w \notin \langle v \rangle$

Then $w \neq 0$

and $T(w) = dw$. Let $d \neq c$

By problem 1, $v + w$ can not be an eigen vector of T. However, by hypothesis $v + w$ is an eigen vector of T (as $w \notin \langle v \rangle \Rightarrow v + w \neq 0$)

$\therefore \quad d = c$

$\therefore \quad T(w) = cw \quad \forall\, w \in V$

$\therefore \quad T = cI.$

Problem 3: *If T is a linear operator on V and α is an eigen value of T, show that $f(\alpha)$ is an eigen value of $f(T)$ if $f(x) \in F[x]$.*

Solution Let $f(x) = a_n x^n + ... + a_1 x + a_0$

Then $f(T) = a_n T^n + ... + a_1 T + a_0 I$

$$\Rightarrow f(T)(v) = a_n T^n (v) + ... + a_1 T(v) + a_0 v$$
$$= a_n \alpha^n v + ... + a_1 \alpha v + a_0 v$$
$$= (a_n \alpha^n + ... + a_1 \alpha + a_0) v$$
$$= f(\alpha) v$$

where $T(v) = \alpha v$, v is an eigen vector of T w.r.t. eigen value α of T.

Definition: Let c be an eigen value of T.

Let $W_c = \{v \in V \mid T(v) = cv\}$

Then $0 \in W_c$ as $T(0) = 0 = c \cdot 0 \Rightarrow W_c \neq \varphi$

Let $\alpha, \beta \in F$, $v_1, v_2 \in V$. Then

$$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$$
$$= \alpha c v_1 + \beta c v_2$$
$$= c(\alpha v_1 + \beta v_2)$$

$\therefore$ $\alpha v_1 + \beta v_2 \in W_c$

$\therefore$ W_c is a subspace of V.

W_c is called *eigen space* of T associated with eigen value c of T.

Example 3: Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be defined by $T(x, y) = (x, 0)$.

As seen before, 1 is an eigen value of T.

$\therefore$ Eigen space of T associated with eigen value 1 is given by

$$W_1 = \{(x, y) \mid T(x, y) = (x, y)\}$$
$$= \{(x, y) \mid (x, 0) = (x, y)\}$$
$$= \{(x, 0) \in \mathbf{R}^2 \mid x \in \mathbf{R}\}$$
i.e., the x-axis

Note: Eigen space $W_c = \{v \in V \mid T(v) = cv\}$

$$= \{v \in V \mid (T - cI)v = 0\}$$
$$= \text{Ker}\,(T - cI)$$

i.e., W_c is the null space of $T - cI$.

Theorem 1: *Let T be a linear operator on a finite dimensional vector space V over F. Then $c \in F$ is an eigen value of T if and only if $T - cI$ is singular* (*not invertible*).

Proof: Let c be an eigen value of T.

Then $\exists\ 0 \neq v \in V$ s.t. $T(v) = cv$

$\therefore$ $(T - cI)v = 0$

$\Rightarrow 0 \neq v \in \text{Ker}(T - cI)$

$\Rightarrow T - cI$ is not one-one

$\Rightarrow T - cI$ is singular.

Conversely, $T - cI$ is singular $\Rightarrow$ $T - cI$ is not one–one (as dim V = finite $\Rightarrow$ $T - cI$ is one-one if and only if $T - cI$ is onto)

$\Rightarrow \exists\ 0 \neq v \in \text{Ker}\ (T - cI)$

$\Rightarrow (T - cI)v = 0,\ v \neq 0 \Rightarrow T(v) = cv,\ v \neq 0$

$\Rightarrow$ c is eigen value of T.

Cor.: Let V be a *FDVS* and T a linear operator on V then T is invertible if and only if 0 is not an eigen value of T.

Problem 4: *Let dim $V = n$. Let T be a linear operator on V. Let $v_1, ..., v_k$ be eigen vectors of T, corresponding to distinct eigen values $c_1, ..., c_k$ of T. Show that $v_1, ..., v_k$ are linearly independent.*

Solution: Let $T(v_i) = c_i v_i$

Then $T^r(v_i) = c_i^r v_i\ \forall\ r \geq 1$

Let $\alpha_1 v_1 + ... + \alpha_k v_k = 0$

Apply $T, T^2, ..., T^{k-1}$ on above.

Thus $\alpha_1 c_1 v_1 + ... + \alpha_k c_k v_k = 0$

.....

.....

$\alpha_1 c_1^{k-1} v_1 + ... + \alpha_k c_k^{k-1} v_k = 0$

$$\Rightarrow \begin{bmatrix} 1 & 1 & \cdots & 1 \\ c_1 & c_2 & \cdots & c_k \\ \cdots & \cdots & \cdots & \cdots \\ c_1^{k-1} & c_2^{k-1} & \cdots & c_k^{k-1} \end{bmatrix} \begin{bmatrix} \alpha_1 v_1 \\ \vdots \\ \alpha_k v_k \end{bmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} \alpha_1 v_1 \\ \vdots \\ \alpha_k v_k \end{bmatrix} = 0 \text{ as } c_1, ..., c_k \text{ are distinct}$$

$\Rightarrow \alpha_i v_i = 0\ \forall i$

$\Rightarrow \alpha_i = 0\ \forall i$

$\therefore$ $v_1, ..., v_k$ are linearly independent.

Problem 5: *Let V be a two dimensional vector space over the field* **R** *of real numbers. Let T be a linear operator on V such that*

$T(v_1) = \alpha v_1 + \beta v_2$

$T(v_2) = \gamma v_1 + \delta v_2, \quad \alpha, \beta, \gamma, \delta \in \mathbf{R}$

where $\{v_1, v_2\}$ is a basis of V.

Find necessary and sufficient condition that 0 be a characteristic root of T.

Solution: Let 0 be a characteristic root of T.

Then there exists $0 \neq v \in V$ such that

$$T(v) = 0$$

$\therefore$ $T(av_1 + bv_2) = 0$

$\Rightarrow$ $a(\alpha v_1 + \beta v_2) + b(\gamma v_1 + \delta v_2) = 0$

$\Rightarrow$ $a\alpha + b\gamma = 0,\ a\beta + b\delta = 0$

If $\alpha\delta \neq \beta\gamma$, then $a = 0 = b \Rightarrow v = 0$, a contradiction.

$\therefore$ $\alpha\ \delta = \beta\ \gamma$

Conversely, let $\alpha\delta = \beta\gamma$

Then $T(v_1) = \alpha v_1 + \beta v_2$

$\Rightarrow$ $T(\delta v_1) = \alpha\delta v_1 + \beta\delta v_2$

$T(v_2) = \gamma v_1 + \delta v_2$

$\Rightarrow$ $T(\beta v_2) = \beta\gamma v_1 + \beta\delta v_2$

$\therefore$ $T(\delta v_1 - \beta v_2) = (\alpha\delta - \beta\gamma)v_1 = 0$

If $\delta v_1 - \beta v_2 = 0$, then $\delta = 0 = \beta$

$\Rightarrow$ $T(v_1) = \alpha v_1$ and $T(v_2) = \gamma v_1$

$\Rightarrow$ $T(\gamma v_1 - \alpha v_2) = 0$

If $\gamma v_1 - \alpha v_2 = 0$, then $\gamma = 0 = \alpha$

$\Rightarrow$ $T(v_1) = 0$

$\Rightarrow$ 0 is a characteristic root of T.

If $\delta v_1 - \beta v_2 \neq 0$, then 0 is a characteristic root of T.

If $\gamma v_1 - \alpha v_2 \neq 0$, then 0 is a characteristic root of T.

So, necessary and sufficient condition for 0 to be a characteristic root of T is $\alpha\delta = \beta\gamma$.

Characteristic Polynomials

Let A be an $n \times n$ matrix over a field F. $c \in F$ is called an eigen value of A if $A - cI$ is singular (not invertible), *i.e.* det $(A - cI) = 0$.

Now, det $(A - cI) = 0 \Leftrightarrow$ det $(cI - A) = 0$.

Let $f(x) = \det(xI - A)$

Then c is an eigen value of A if and only if $f(c) = 0$. For this reason $f(x)$ is called *characteristic polynomial* of A. Clearly deg $f(x) = n$ and coefficient of highest degree term x^n in $f(x)$ is 1 (*i.e.* $f(x)$ is monic).

Theorem 2: *Similar matrices have same characteristic polynomial.*

Proof: Let A, B be similar matrices.

Then $\exists$ non singular matrix P s.t.

$$B = P^{-1}AP$$

$\therefore$ Characteristic polynomial of B = det $(xI - B)$

$= \det(xI - P^{-1}AP)$

$= \det(P^{-1}\ (xI - A)P)$

$$= \det (xI - A) = \text{characteristic polynomial of } A.$$

However, the converse of above theorem need not be true. Consider

Example 4: Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Then the characteristic polynomial of A is $|xI - A| = (x - 1)^2$

and that of B is $|xI - B| = (x - 1)^2$

But A and B are not similar matrices as $A = P^{-1}BP \Rightarrow A = I$.

Characteristic Polynomial of a Linear Operator

If β, β' are two ordered basis of V s.t. $[T]_\beta = A$, $[T]_{\beta'} = B$, then $B = P^{-1}AP$ for some matrix P.

$c \in F$ is an eigen value of operator T on a finite dimensional vector space V

$\Leftrightarrow$ $T - cI$ is singular by Theorem 1

$\Leftrightarrow$ $\det [T - cI]_\beta = 0$

$\Leftrightarrow$ $\det \{[T]_\beta - cI\} = 0$

$\Leftrightarrow$ $\det (A - cI) = 0$

$\Leftrightarrow$ c is an eigen value of A.

By theorem 2, A and B have same characteristic polynomial. So, c is an eigen value of A $\Leftrightarrow$ c is an eigen value of B.

Hence $c \in F$ is an eigen value of T if and only if c is an eigen value of corresponding matrix of T w.r.t. any basis of V.

If $[T]_\beta = A$, we say characteristic polynomial of T is $\det xI - A$, which does not depend on the basis of V by theorem 2.

Remarks:

1. If $T : V \to V$ is a linear operator s.t. dim $V = n$, then $[T]_\beta$ is $n \times n$ matrix. Let $A = [T]_\beta$. Then $\det (A - xI)$ is a polynomial of degree n. So, A (or T) can't have more than n distinct eigen values.
2. T may not have any eigen value (See Problem 8).
3. Let $A = (a_{ij})$. Then

   $\det (xI - A) = x^n - (a_{11} + a_{12} + ... + a_{nn})x^{n-1} + ...$

   $\Rightarrow$ sum of eigen values of A (or T) is sum of diagonal elements of A

   $\Rightarrow$ sum of eigen values of A (or T) is trace of A.
4. Put $x = 0$ in

   $\det (xI - A) = x^n - (a_{11} + ... + a_{nn})\, x^{n-1} ... +$ constant term then $\det (-A)$ = constant term

   $\Rightarrow (-1)^n \det A$ = constant term of characteristic polynomial of A or T.
5. If A is a matrix over **C**, the field of complex numbers, then by fundamental theorem of algebra, characteristic polynomial of A must have a root in **C**. In other words A (or T) has at least one eigen value in **C**.

6. Let $c \in F$ be an eigen value of $n \times n$ matrix A over F.
   Then $\det(cI - A) = 0$.
   So, columns of $cI - A$ are linearly dependent over F.
   $\therefore \exists\ \alpha_1, \alpha_2, ..., \alpha_n \in F$ such that $\alpha_1 c_1 + ... + \alpha_n c_n = 0$, $\alpha_i \neq 0$ for some i, where c_1, ..., c_n are columns of $cI - A$.

   Thus, $[c_1, c_2, ..., c_n] \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$

   $\therefore \quad (cI - A) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$

   So, $\quad A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = c \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$.

   Hence $AX = cX$, where $X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \neq 0$

   X is called an eigen vector of A.
   Conversely, let $AX = cX$, $X \neq 0$ is an $n \times 1$ matrix over F.
   $\therefore (cI - A)X = 0$
   So, $\det(cI - A) = 0$ as $X \neq 0$.
   Thus, c is an eigen value of A.
7. We now give a method of determining eigen vector of $A = [T]_\beta$, given an eigen vector of T and conversely.
   Let $\{v_1, v_2, ..., v_n\} = \beta$ be an ordered basis of V. Let $A = (a_{ij}) = [T]_\beta$.
   Now $0 \neq v \in V$ is an eigen vector of T
   $\Leftrightarrow T(v) = cv$, for some $c \in F$
   $\Leftrightarrow T(\alpha_1 v_1 + ... + \alpha_n v_n) = c(\alpha_1 v_1 + ... + \alpha_n v_n)$, $\alpha_i \in F$
   $\Leftrightarrow \alpha_1 T(v_1) + ... + \alpha_n T(v_n) = c\alpha_1 v_1 + ... + c\alpha_n v_n$
   $\Leftrightarrow \alpha_1(a_{11}v_1 + ... + a_{n1}v_n) + ... + \alpha_n(a_{1n}v_1 + ... + a_{nn}v_n) = c\alpha_1 v_1 + ... + c\alpha_n v_n$
   $\Leftrightarrow \alpha_1 a_{11} + ... + \alpha_n a_{1n} = c\alpha_1$
   . . . . . .
   $\alpha_1 a_{n1} + ... + \alpha_n a_{nn} = c\alpha_n$

   $\Leftrightarrow A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = c \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$

$\Leftrightarrow AX = cX$, where $X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \neq 0$.

So, if $v = \alpha_1 v_1 + ... + \alpha_n v_n$ is an eigen vector of T, then $X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$

is an eigen vector of A and conversely.

8. Let c be an eigen value of $n \times n$ matrix A over F.
   Then $W_c' = \{X \mid X = n \times 1$ matrix over F, $AX = cX\}$, is a subspace of $n \times 1$ matrices over F. W_c' is called an eigen space of A w.r.t. eigen value c of A.
   Let $A = [T]_\beta$, where T is a linear operator on V and β, an ordered basis of V. We show that dim W_c' = dim W_c, where W_c = eigen space of T w.r.t. eigen value c of T.
   Define $\theta : W_c \to W_c'$ s.t.,

$$\theta(v) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \text{ where } v = \alpha_1 v_1 + ... + \alpha_n v_n$$

   Then θ is an isomorphism. (Verify!)
   So, dim W_c = dim W_c'

9. Let $[T]_\beta = A$ = diagonal matrix

$$= \begin{bmatrix} c_1 & \cdots & O \\ \vdots & \ddots & \vdots \\ O & \cdots & c_n \end{bmatrix}$$

   Suppose Rank $A = r$. So, r entries in diagonal of A are non-zeros and all other entries are zeros. Let first r entries $c_1, ..., c_r$ be all non-zero and $c_{r+1} = ... = c_n = 0$. Let $\beta = \{v_1, ..., v_r, v_{r+1}, ..., v_n\}$ = ordered basis of V. Then, $T(v_i) = c_i v_i$, $i = 1, 2, ..., r$. Now $\{T(v_1), ..., T(v_r)\} \subseteq$ Range T. Let $\alpha_1 T(v_1) + ... + \alpha_r T(v_r) = 0$, $\alpha_i \in F$.
   Then $\alpha_1 c_1 v_1 + ... + \alpha_r c_r v_r = 0$
   $\Rightarrow \alpha_i c_i = 0 \ \forall \ i = 1, 2, ..., r$
   $\Rightarrow \alpha_i = 0 \ \forall \ i = 1, 2, ..., r$ as $c_i \neq 0$
   $\therefore S = \{T(v_1), ..., T(v_r)\}$ is a *L.I.* set.
   Let $T(v) \in$ Range T.
   Now $v \in V \Rightarrow v = \beta_1 v_1 + ... + \beta_r v_r + \beta_{r+1} v_{r+1} + ... + \beta_n v_n$
   $\Rightarrow T(v) = \beta_1 T(v_1) + ... + \beta_r T(v_r)$
   $\Rightarrow S$ spans Range T
   $\Rightarrow S$ = basis of Range T
   $\Rightarrow$ dim Range $T = r$
   $\Rightarrow$ Rank $T = r$

So, Rank A = Rank T, where $[T]_\beta = A$ = diagonal matrix.

In fact, Rank A = Rank T, even when A is not diagonal matrix.

Problem 6: *Let* $A = (a_{ij})_{n \times n}$ *be such that*

(*i*) $\sum_j a_{ij} = 1$ *for each* i

(*ii*) $\sum_i a_{ij} = 1$ *for each* j

Prove that 1 *is characteristic value of* A.

Solution: (*i*) Let dim $V = n$. Let T be the linear operator on V s.t., $[T]_\beta = A$, where $\beta = \{v_1, v_2, ..., v_n\}$ is an ordered basis of V. Then

$$T(v_1) = a_{11}v_1 + ... + a_{n1}v_n$$
$$. . . . . .$$
$$T(v_n) = a_{1n}v_1 + ... + a_{nn}v_n$$

Then $T(v_1 + v_2 + ... + v_n) = v_1 + v_2 + ... + v_n$

as $\sum_j a_{ij} = 1$ for each i

Hence 1 is a characteristic value of A.

(*ii*) Let A' denote the transpose of A. By (*i*) 1 is the characteristic value of A'

Thus $\det (I - A') = 0$

$\Rightarrow \det (I - A')' = 0$

$\Rightarrow \det (I - A) = 0$

$\Rightarrow$ 1 is characteristic value of A.

Problem 7: *Prove that it is impossible to find a* 2×2 *matrix* C *over* F *such that*

$$C \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} C^{-1} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}, \alpha, \beta \in F.$$

Solution: Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$.

Suppose there exists 2×2 matrix C over F such that

$$CAC^{-1} = B.$$

Since 1 is the only eigen value of A, 1 is also the only eigen value of B as the characteristic polynomials of A and B are same. So, $\alpha = \beta = 1$. $\therefore B = I$

$\Rightarrow CAC^{-1} = I \Rightarrow A = I$, a contradiction.

So, there does not exist any 2×2 matrix C over F such that $CAC^{-1} = B$.

Problem 8: *Let* T *be a linear operator on* $\mathbf{R}^2$ *which is represented in the standard ordered basis by the matrix*

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Show that T *has no eigen values in* $\mathbf{R}$.

Solution: The characteristic polynomial of A (or T) is given by

$$\det(xI - A) = \begin{vmatrix} x & 1 \\ -1 & x \end{vmatrix} = x^2 + 1$$

which has no real roots. So T has no eigen values in $\mathbf{R}$. However $\pm i$ are eigen values of T in $\mathbf{C}$.

Problem 9: *Let $c \neq 0$ be an eigen value of an invertible operator T. Show that c^{-1} is an eigen value of T^{-1}.*

Solution: Since c is an eigen value of T, $\exists\ 0 \neq v \in V$ s.t.

$$T(v) = cv$$
$$\Rightarrow v = T^{-1}(cv) = c(T^{-1}(v))$$
$$\Rightarrow c^{-1}v = T^{-1}(v)$$
$$\Rightarrow c^{-1} \text{ is an eigen value of } T^{-1}.$$

Problem 10: *Obtain the eigen values, eigen vectors and eigen spaces of*

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Solution: The characteristic polynomial of A is

$$\det(xI - A) = \begin{vmatrix} x & -1 & 0 \\ -1 & x & 0 \\ 0 & 0 & x-1 \end{vmatrix} = (x + 1)(x - 1)^2$$

$\therefore$ eigen values of A are $1, -1$.

The eigen vector corresponding to eigen value 1 is given by

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

giving $\quad x_2 = x_1,\ x_1 = x_2,\ x_3 = x_3$

Thus eigen vectors are

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

So, eigen space W_1 corresponding to eigen value 1 is spanned by $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ which is linerly independent.

$\therefore \quad \dim W_1 = 2$

Also eigen vectors corresponding to eigen value –1 are given by

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = (-1) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

giving $x_2 = -x_1,\ x_1 = -x_2, \quad x_3 = -x_3$

$$\therefore \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_1 \\ 0 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$$

i.e., eigen space W_{-1} corresponding to eigen value –1 is spanned by $\begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$

Thus $\dim W_{-1} = 1$

Hence eigen values are ± 1 and eigen vectors are $\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$.

Problem 11: *Show that eigen values of an $n \times n$ triangular matrix A are the diagonal elements of A.*

Solution: Let

$$A = \begin{bmatrix} a_{11} & & & \\ & a_{22} & & \\ & & \cdots & \\ 0 & & & a_{nn} \end{bmatrix},\ a_{ij} = 0 \text{ for all } i > j$$

Characteristic polynomial of A is

$$(x - a_{11}) \ldots (x - a_{nn})$$

$\therefore\ a_{11}, \ldots, a_{nn}$ are eigen values of A.

Problem 12: *Let A be a real $n \times n$ matrix. Let λ be a real eigen value of A. Show that there exists an eigen vector X of A corresponding to eigen value λ such that X is also real.*

Solution: Suppose $Ay = \lambda y,\ y \neq 0$. Then y is eigen vector of A corresponding to eigen value λ of A. If y is real, then result follows. Suppose y is not real. Let $y = u + iv$ where u and v real column matrices.

Then $Ay = \lambda y$

$\Rightarrow A(u + iv) = \lambda(u + iv)$

$\Rightarrow Au + iAv = \lambda u + i\lambda v$

$\Rightarrow Au = \lambda u,\ Av = \lambda v$

Since $y \neq 0$, either $u \neq 0$ or $v \neq 0$. If $u \neq 0$, then u is real eigen vector of A and $v \neq 0 \Rightarrow v$ is real eigen vector of A corresponding to eigen value λ of A.

Problem 13: *Let A be $n \times n$ matrix given by*

$$A = \begin{bmatrix} k & 1 & 0 & \cdots & \cdots & 0 \\ 1 & k & 1 & \cdots & \cdots & 0 \\ 0 & 1 & k & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \cdots & k \end{bmatrix}$$

(*i.e. diagonal entries of A are k and entries above and below the diagonal are* 1 *and zero elsewhere*).

Show that $X_i (i = 1, ..., n)$ where X_is are column matrices with jth entry $\left\{ \sin \frac{ij\pi}{n+1} \right\}$ are eigen vectors of A. Find corresponding eigen values of A.

Solution: Now

$$AX_i = \begin{bmatrix} k & 1 & 0 & \cdots & \cdots & 0 \\ 1 & k & 1 & \cdots & \cdots & 0 \\ 0 & 1 & k & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \cdots & k \end{bmatrix} \begin{bmatrix} \sin \frac{i\pi}{n+1} \\ \sin \frac{2i\pi}{n+1} \\ \sin \frac{3i\pi}{n+1} \\ \cdots\cdots\cdots \\ \sin \frac{ni\pi}{n+1} \end{bmatrix} = \begin{bmatrix} k \sin \frac{i\pi}{n+1} + \sin \frac{2i\pi}{n+1} \\ \sin \frac{i\pi}{n+1} + k \sin \frac{2i\pi}{n+1} + \sin \frac{3i\pi}{n+1} \\ \sin \frac{2i\pi}{n+1} + k \sin \frac{3i\pi}{n+1} + \sin \frac{4i\pi}{n+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \sin \frac{(n-1)i\pi}{n+1} + k \sin \frac{ni\pi}{n+1} \end{bmatrix}$$

$$= \begin{bmatrix} k \sin \frac{i\pi}{n+1} + 2 \sin \frac{i\pi}{n+1} \cos \frac{i\pi}{n+1} \\ k \sin \frac{2i\pi}{n+1} + 2 \sin \frac{2i\pi}{n+1} \cos \frac{i\pi}{n+1} \\ k \sin \frac{3i\pi}{n+1} + 2 \sin \frac{3i\pi}{n+1} \cos \frac{i\pi}{n+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ k \sin \frac{ni\pi}{n+1} + 2 \sin \frac{ni\pi}{n+1} \cos \frac{i\pi}{n+1} \end{bmatrix}$$

$$= \begin{bmatrix} \left(k + 2\cos\frac{i\pi}{n+1}\right)\sin\frac{i\pi}{n+1} \\ \left(k + 2\cos\frac{i\pi}{n+1}\right)\sin\frac{2i\pi}{n+1} \\ \left(k + 2\cos\frac{i\pi}{n+1}\right)\sin\frac{3\pi}{n+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \left(k + 2\cos\frac{i\pi}{n+1}\right)\sin\frac{n\pi}{n+1} \end{bmatrix}$$

$$= \left(k + 2\cos\frac{i\pi}{n+1}\right)\begin{bmatrix} \sin\frac{i\pi}{n+1} \\ \sin\frac{2i\pi}{n+1} \\ \sin\frac{3i\pi}{n+1} \\ \ldots\ldots\ldots \\ \sin\frac{ni\pi}{n+1} \end{bmatrix}$$

$$= \left(k + 2\cos\frac{i\pi}{n+1}\right)X_i$$

$\therefore X_i$ are eigen vectors of A for each $i = 1, ..., n$ and $k + 2\cos\frac{i\pi}{n+1}$ are corresponding eigen values of A.

Problem 14: *Let V be the space of all real valued continuous functions. Define*

$$T : V \to V \text{ by } (Tf)(x) = \int_0^x f(t)\,dt$$

Show that T has no eigen values.

Solution: Let c be an eigen value of T.

$\therefore$ $\exists\ 0 \neq f \in V$ s.t.

$Tf = cf$

$\therefore$ $Tf(x) = cf(x)$

$\therefore$ $\int_0^x f(t)\,dt = cf(x)$

$f(x) = cf'(x)$

$y = c\frac{dy}{dx}$

$c \neq 0$ (as $c = 0 \Rightarrow y = 0 \Rightarrow f(x) = 0 \Rightarrow f = 0$)

$$\therefore \quad \frac{dy}{y} = \frac{dx}{c}$$

$$\Rightarrow \log y = \frac{x}{c} + \log a \Rightarrow y = ae^{x/c}$$

$$\Rightarrow y(0) = a$$

$$\Rightarrow f(x) = y = f(0)\ e^{x/c}$$

$$\Rightarrow \int_0^x f(0)e^{t/c}dt = \int_0^x f(t)\,dt = cf(x) = cf(0)e^{x/c}$$

$f(0) \neq 0$ (as $f(0) = 0 \Rightarrow a = 0 \Rightarrow y = 0 \Rightarrow f(x) = 0 \Rightarrow f = 0$)

$$\therefore \quad f(0)\left[ce^{t/c}\right]_0^x = cf(0)\ e^{x/c}$$

$$\therefore \quad c(e^{x/c} - 1) = ce^{x/c}$$

$$\Rightarrow e^{x/c} - 1 = e^{x/c}$$

$\Rightarrow 1 = 0$, a contradiction

$\therefore$ T has no eigen value.

Remark: Let D be the differential operator on V in the above problem.

Let c be any real number.

Define $f : \mathbf{R} \to \mathbf{R}$, s.t.,

$$f(x) = e^{cx}$$

Then $f \in V$ and $Df = cf$.

So, every real number is an eigen value of D.

In the above problem, linear operator T on V has no eigen value whereas here every real number is an eigen value of the linear operator D.

Minimal Polynomials

In order to determine a linear operator T, it is very useful to determine the class of polynomials which annihilate T.

If T is a linear operator on the n - dimensional space V, then dim Hom $(V, V) = n^2$

$\Rightarrow$ any $n^2 + 1$ vectors in Hom (V, V) are linearly dependent.

$\Rightarrow I, T, T^2, ..., T^{n^2}$ are linearly dependent.

$\Rightarrow \exists\ c_o, c_1, c_2, ..., c_{n^2} \in F$ s.t.

$c_oI + c_1T + ... + c_{n^2}T^{n^2} = 0$ where some $c_i \neq 0$

i.e., T satisfies a polynomial $p(x) \in F[x]$, where

$p(x) = c_o + c_1x + ... + c_{n^2}T^{n^2}$, $p(x) \neq 0$ s.t. $p(T) = 0$

Among all such polynomials satisfied by T, choose a polynomial of least degree.

Definition: Let T be a linear operator on a finite dimensional space V over F. The *minimal polynomial* for T is defined to be the unique polynomial $p(x) \in F[x]$ s.t.

(*i*) $p(x)$ is monic polynomial

(*ii*) $p(T) = 0$

(*iii*) No polynomial over F which annihilates T has smaller degree than $p(x)$.

Note that $p(x)$ is uniquely determined by (*i*).

We have similar definition for minimal polynomial for a square matrix A.

Theorem 3: *Let T be a linear operator on an n-dimensional space V. The characteristic and minimal polynomials for T have the same roots.*

Proof: Let $p(x)$ be the minimal polynomial for T. Let c be a root of $p(x)$ *i.e.*, $p(c) = 0$.

Then $p(x) = (x - c)\, q(x)$ for some $q(x) \in F[x]$.

Since deg $q(x) <$ deg $p(x)$, $q(T) \neq 0$

$\exists\ v \in V$ s.t. $q(T)\, v \neq 0$, $v \neq 0$

Let $x = q(T)\, v \neq 0$

Then $0 = p(T)\, v$

$= (T - cI)\, q(T)\, v$

$= T(x) - cx$

$\Rightarrow\ T(x) = cx,\ x \neq 0$

$\Rightarrow c$ is an eigen value of T.

Conversely, let c be an eigen value of T.

Then $\exists\ 0 \neq v \in V$ s.t. $Tv = cv$

$\therefore\ p(T)\, v = p(c)\, v$

Since $p(T) = 0$, $p(c)\, v = 0$, $v \neq 0$

$p(c) = 0$

$\therefore\ c$ is a root of minimal polynomial for T.

Example 5: Although minimal polynomial and characteristic polynomial have same roots, they may not be same. For example, the characteristic polynomial of

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$ is $(x - 1)\,(x - 2)^2$ while $(A - I)\,(A - 2I) = 0 \Rightarrow$ minimal polynomial of A is $(x - 1)\,(x - 2)$.

A natural question arises. When would these two polynomials be same? If eigen values of linear operator T are all distinct, the characteristic polynomial of T is $f(x) = (x - c_1) \ldots (x - c_n)$. Since roots of minimal polynomial $p(x)$ of T are same as of $f(x)$ and deg $p(x) \leq$ deg $f(x) = n$

$$p(x) = (x - c_1) \ldots (x - c_n) = f(x)$$

There is that well known result in matrices called ''*Cayley Hamilton Theorem*'' which says ''Every square matrix satisfies its characteristic polynomial''. Since characteristic polynomial of a linear operator T is same as characteristic polynomial of $[T]_\beta$ w.r.t. any basis β of V, Cayley Hamilton Theorem is true for linear operators also *i.e.* if $f(x)$ is the characteristic polynomial of T, then $f(T) = 0$.

A simple consequence of the above is

Theorem 4: *The minimal polynomial of a linear operator T divides its characteristic polynomial.*

Proof: Let $p(x)$, $f(x)$ be the minimal and characteristic polynomials respectively of T.

Then $f(x) = g(x)\ p(x) + q(x)$ where either $q(x) = 0$ or deg $q(x)$ < deg $p(x)$

Let $q(x) \neq 0$. Now $0 = f(T) = g(T)\ p(T) + q(T)$

$\Rightarrow q(T) = 0\ (f(T)) = 0$ (by Cayley Hamilton Theorem)

$\therefore$ $q(x)$ is a non zero monic polynomial of degree less than deg $p(x)$ and $q(T) = 0$, contradicting $p(x)$ is minimal. $\therefore$ $q(x) = 0$

$\therefore$ $p(x)$ divides $f(x)$.

Remarks (1): Let $A = [T]_\beta$ and $p(x)$ = minimal polynomial of T. Then $p(x)$ is also minimal polynomial of A.

Proof: Now $[T^r]_\beta = [T]_\beta \ldots [T]_\beta = A^r$

$\therefore$ $[p(T)]_\beta = p(A)$

$\therefore$ $p(A) = 0$ as $p(T) = 0$

Let $q(x)$ = minimal polynomial of A.

Let $p(x) = q(x)\ r(x) + s(x)$, where

$s(x) = 0$ or deg $s(x)$ < deg $q(x)$

Now $0 = p(A) = q(A)\ r(A) + s(A)$

$\Rightarrow s(A) = 0$

If $s(x) \neq 0$, then A satisfies a non-zero polynomial of degree less than deg $q(x)$, a contradiction.

$\therefore$ $s(x) = 0$. So, $q(x) \mid p(x)$

Again $[q(T)]_\beta = q(A) = 0 \Rightarrow q(T) = 0$

Let $q(x) = p(x)\ g(x) + h(x)$

where $h(x) = 0$ or deg $h(x)$ < deg $p(x)$.

$\therefore$ $q(T) = p(T)\ g(T) + h(T)$

$\Rightarrow 0 = h(T)$

If $h(x) \neq 0$, then T satisfies a non-zero polynomial of degree less than deg $p(x)$, a contradiction.

$\therefore$ $h(x) = 0 \Rightarrow p(x) \mid q(x)$

Hence $p(x) = q(x)$ = minimal polynomial of A.

(2) Similar matrices have same minimal polynomial.

Proof: Let A, B be similar matrices

Then $B = P^{-1}AP$

Let $p(x)$ = minimal polynomial of A.

$q(x)$ = minimal polynomial of B.

Now $0 = q(B) = q(P^{-1}AP) = P^{-1}q(A)P$

$\therefore$ $q(A) = 0$

As before $p(x) \mid q(x)$

Similarly, $0 = p(A) = p(PBP^{-1}) = Pp(B)P^{-1}$

$\therefore$ $p(B) = 0$

So, $q(x) \mid p(x)$

Thus, $p(x) = q(x)$.

However, the converse need not be true. Consider

Example 6: Let $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$

Then the minimal polynomial of A(and B) is $(x - 1)(x - 2)$

Since Trace $A = 4$, Trace $B = 5$, A and B are not similar.

Problem 15: *For two matrices A and B show that AB and BA need not have the same minimal polynomial.*

Solution: Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Then $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $BA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

$\therefore$ $AB = 0 = (BA)^2$

$\Rightarrow$ Minimal polynomial of AB is x whereas the minimal polynomial of BA is x^2.

Problem 16: *Let* $A = \begin{bmatrix} B & O \\ O & C \end{bmatrix}$, *where B and C are square matrices. Show that the minimal polynomial* $p(x)$ *of A is the l.c.m. of the minimal polynomials* $q(x)$ *and* $r(x)$ *of B and C.*

Solution : Now $p(A) = \begin{bmatrix} p(B) & O \\ O & p(C) \end{bmatrix}$.

Since $p(A) = 0$, $p(B) = 0 = p(C)$

we find $q(x) \mid p(x)$, $r(x) \mid p(x)$

Suppose $q(x) \mid f(x)$, $r(x) \mid f(x)$

Then $f(A) = \begin{bmatrix} f(B) & O \\ O & f(C) \end{bmatrix}$

Now $q(x) \mid f(x) \Rightarrow f(B) = 0$

$r(x) \mid f(x) \Rightarrow f(C) = 0$

$\therefore$ $f(A) = 0$

$\therefore$ $p(x) \mid f(x)$.

So, $p(x)$ is the l.c.m. of $q(x)$ and $r(x)$.

Problem 17: *Let V be a F.D.V.S. Let T be a linear operator on V. Let $T^t : \hat{V} \to \hat{V}$ be the transpose of T, defined by $T^t(f) = fT$. Show that T and T^t have the same minimal polynomial.*

Solution: Let $\beta = \{v_1, ..., v_n\}$ be a basis of V and $\beta_1 = \{f_1, ..., f_n\}$ be the dual basis of β.

Let $[T]_\beta = A$, $[T^t]_{\beta_1} = B$

Then $B = A^t$ = transpose of A.

(See theorem 19, page 853)

Let $p(x) = \sum_{o}^{r} a_i x^i$ be the minimal polynomial of A (or T).

Let $q(x)$ be the minimal polynomial of A^t (or T^t).

Then $0 = p(A) = a_o I + a_1 A + ... + a_r A^r$ ...(i)

$0 = a_o I + a_1 A^t + ... + a_r (A^t)^r$

(by taking transpose on both sides of (i)).

$\Rightarrow 0 = p(A^t)$.

So, $q(x) \mid p(x)$.

Similarly, $p(x) \mid q(x)$.

$\therefore$ $p(x) = q(x)$.

$\therefore$ The minimal polynomials of T and T^t are same.

Problem 18: *Let a, b, c be elements of a field F and*

$$A = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$$

Prove that the characteristic polynomial of A is same as its minimal polynomial.

Solution: The characteristic polynomial of A is given by

$$f(x) = |xI - A| = x^3 - ax^2 - bx - c$$

Let $p(x)$ be its minimal polynomial.

Then deg $p(x) \leq$ deg $f(x) = 3$.

If deg $p(x) = 1$, then $p(x) = x - \alpha$, $\alpha \in F$

$$\therefore \quad O = p(A) = A - \alpha I = \begin{bmatrix} -\alpha & 0 & c \\ 1 & -\alpha & b \\ 0 & 1 & a-\alpha \end{bmatrix}$$

which is not true as $1 \neq 0$.

If deg $p(x) = 2$, then $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$

$$\Rightarrow O = p(A) = A^2 + \alpha A + \beta I$$

$$\Rightarrow \begin{bmatrix} - & - & - \\ - & - & - \\ 1 & - & - \end{bmatrix} + \begin{bmatrix} - & - & - \\ - & - & - \\ 0 & - & - \end{bmatrix} + \begin{bmatrix} - & - & - \\ - & - & - \\ 0 & - & - \end{bmatrix} = 0$$

$\Rightarrow$ 1 = 0 which is not true.

So deg $p(x) = 3$ and hence $p(x) = f(x)$.

Problem 19: *Let T be a linear operator on a finite dimensional vector space V(F). Show that T is invertible if and only if the constant term of the minimal polynomial of T is not zero.*

Solution: Let $p(x)$ be the minimal polynomial of T.

Let T be invertible.

Suppose the constant term of $p(x)$ is 0.

Then $p(x) = \alpha_1 x + ... + \alpha_k x^k$

$\Rightarrow p(o) = 0$

$\Rightarrow$ 0 is a root of $p(x)$.

$\Rightarrow$ 0 is an eigen value of T, a contradiction by cor. to theorem 1.

$\therefore$ The constant term of $p(x)$ is not zero.

Conversely: let $p(x) = \alpha_o + \alpha_1 x + ... + \alpha_k x^k$, $\alpha_o \neq 0$.

Then $p(o) = \alpha_o \neq 0$

$\Rightarrow$ 0 is not a root of $p(x)$

$\Rightarrow$ 0 is not an eigen value of T

$\Rightarrow$ T is invertible, by Cor. to theorem 1.

Problem 20: *If T is a linear operator on a finite dimensional vector space V over F and T is right invertible, show that T is invertible.*

Solution: Let $TU = I$. If T is not invertible, then by above problem, the constant term of the minimal polynomial $p(x)$ of T is 0.

Let $p(x) = \alpha_1 x + ... + \alpha_m x^m$.

Then $0 = p(T) = \alpha_1 T + ... + \alpha_m T^m$.

Let $S = \alpha_1 I + \alpha_2 T + ... + \alpha_m T^{m-1}$.

Then $S \neq 0$ as $p(x)$ is of least degree satisfied by T.

Also $ST = TS = 0$.

Now $0 = (ST)U = S(TU) = SI = S$, a contradiction.

So, T is invertible.

Problem 21: *Let V be the space of n × n matrices over F. Let A be n × n matrix in V. Define $T : V \to V$ s.t. $T(B) = AB$ for all $B \in V$. Show that the minimal polynomial of T is the minimal polynomial of A.*

Solution : Let $p(x) = x^n + ... + \alpha_{n-1} x + \alpha_n$

$q(x) = x^m + ... + \beta_{m-1} x + \beta_m$

be minimal polynomials of T and A respectively

Now $0 = p(T)I$

$= (T^n + ... + \alpha_n I)I$

$= A^n + ... + \alpha_n I$ as $T(I) = A \Rightarrow T^r(I) = A^r$

$= p(A)$.

$\therefore$ A satisfies $p(x)$.

Let $p(x) = (x - c)\, q(x) + r(x)$, $r(x) = 0$ or deg $r(x) <$ deg $q(x)$, c is root of $p(x)$.

Then $0 = p(A) = (A - cI)\, q(A) + r(A)$

$\Rightarrow r(A) = 0$

If $r(x) \neq 0$, then $r(x)$ is non zero monic polynomial of degree less than deg $q(x)$ s.t. $r(A) = 0$, a contradiction.

$\therefore$ $r(x) = 0$.

$\therefore$ $q(x)$ divides $p(x)$

Also $0 = q(A)B$

$= (A^m + ... + \beta_m I)B$

$= A^m B + ... + \beta_m B$

$= T^m B + ... + \beta_m B$

$= (T^m + ... + \beta_m I)B$

$= q(T)B$ for all $B \in V$

$\Rightarrow q(T) = 0$

As before, $p(x)$ divides $q(x)$ and thus $p(x) = q(x)$.

Diagonalizable Operators

Definition: A linear operator T on a finite dimensional vector space V is called diagonalizable if $\exists$ an ordered basis $\beta = \{v_1, ..., v_n\}$ of V s.t. matrix of T w.r.t. β is a diagonal matrix.

i.e.,
$$[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & c_2 & \\ & & \cdots \\ 0 & & c_n \end{bmatrix}$$

Equivalently *A linear operator T on the finite dimensional vector space V is diagonalisable if and only if $\exists$ a basis β of V consisting of eigen vectors of T.*

Proof: Let T be diagonisable.

Then $\exists$ a basis $\beta = \{v_1, ..., v_n\}$ of V s.t.,

$$[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & c_2 & \\ & & \cdots \\ 0 & & c_n \end{bmatrix}$$

i.e. $T(v_i) = c_i v_i$ for all $i = 1, ..., n$.

$\therefore$ $v_1, ..., v_n$ are eigen vectors of T.

Conversely, let $\beta = \{v_1, ..., v_n\}$ be a basis of V s.t. each v_i is an eigen vector of T.

Then $$[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ \cdots & & \cdots \\ 0 & & c_n \end{bmatrix}$$ is a diagonal matrix

$\therefore$ T is diagonalizable.

Theorem 5: *Let T be a linear operator on a finite dimensional vector space V(F). Let* $c_1, c_2, ..., c_k \in F$ *be distinct eigen values of T and let* W_i *be the eigen space corresponding to eigen value* c_i, $i = 1, 2, ..., k$. *Suppose* $\beta_1, ..., \beta_k$ *are basis of* $W_1, ..., W_k$ *respectively. Then* $\beta = \{\beta_1, ..., \beta_k\}$ *is a basis of* $W = W_1 + ... + W_k$ *and dim* W = *dim* W_1 + ... + *dim* W_k. *Hence* $W = W_1 \oplus ... \oplus W_k$.

Proof: We first show that whenever

$$x_1 + ... + x_k = 0, \; x_i \in w_i \qquad ...(i)$$

then $x_i = 0 \; \forall \; i$.

Apply $T, T^2, ..., T^{k-1}$ in (i) to get

$$c_1 x_1 + ... + c_k x_k = 0$$
$$\cdots$$
$$c_1^{k-1} x_1 + ... + c_1^{k-1} x_k = 0$$

(Note that $T(x_i) = c_i x_i \Rightarrow T^r(x_i) = c_{c_i}^{r_i} x_i$)

$\therefore$
$$\begin{bmatrix} 1 & \cdots & 1 \\ c_1 & & c_k \\ \vdots & & \vdots \\ c_1^{k-1} & & c_k^{k-1} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = 0$$

$$C \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = 0, \text{ where } C = \begin{bmatrix} 1 & \cdots & 1 \\ c_1 & & c_k \\ \vdots & & \vdots \\ c_1^{k-1} & & c_k^{k-1} \end{bmatrix}$$

$\Rightarrow \det C \neq 0$, as $c_i, ..., c_k$ are distinct.

$\therefore$
$$C^{-1} C \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = 0$$

$$\Rightarrow \quad \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = 0 \Rightarrow x_i = 0 \ \forall \ i$$

Hence our assertion follows.

Let now $x \in W$. Then $x = x_1 + ... + x_k$, $x_i \in W_i$ as $W = W_1 + ... + W_k$

Also $\beta_1 = \{v_1, ..., v_{d_1}\}$ spans W_1 (assuming dim $W_k = d_k$)

In this way, since $\beta_k = \{v_1', ..., v_{d_k}'\}$ spans W_k

we find $x_k = \beta_1 v_1' + ... + \beta_{d_k} v_{d_k}'$

So, $x = \alpha_1 v_1 + ... + \alpha_{d_1} v_{d_1} + ... + \beta_1 v_1' + ... + \beta_{d_k} v_{d_k}'$

$= $ linear combination of $v_1, ..., v_{d_1}, ..., v_{d_1}', ... v_{d_k}'$

$\Rightarrow \{\beta_1, \beta_2, ..., \beta_k\} = \beta$ spans W.

Suppose $(\alpha_1 v_1 + ... + \alpha_{d_1} v_{d_1}) + ... + (\beta_1 v_1' + ... + \beta_{d_k} v_{d_k}') = 0$

$\Rightarrow x_1 + ... + x_k = 0$

where $x_1 = \alpha_1 v_1 + ... + \alpha_{d_1} \quad v_{d_1} \in W_1$

. . . . . .

$x_k = \beta_1 v_1' + ... + \beta_{d_k} \quad v_{d_k}' \in W_k$

Then $x_i = 0$ for all i (as shown above)

$\Rightarrow \alpha_1 = ... = \alpha_{d_1} = ... = \beta_1 = ... = \beta_{d_k} = 0$

as each β_i is basis of W_i

$\Rightarrow \beta = \{\beta_1, ..., \beta_k\}$ is linearly independent and so forms a basis of W.

Now dim $W = o(\beta_1) + ... + o(\beta_k)$

i.e., dim W = dim W_1 + ... + dim W_k

proving the theorem.

We now give conditions under which an operator T is diagonalisable.

Theorem 6: *Let T be a linear operator on a finite dimensional vector space $V(F)$. Then T is diagonalisable if and only if dim V = dim W_1 + ... + dim W_k.*

Proof: Let T be diagonalisable. Then $\exists$ a basis β of V such that each vector of β is an eigen vector of T. Suppose first r_1 vectors $x_1, ..., x_{r_1} \in W_1$, second r_2 vectors belong to W_2 and in this way last r_k vectors $y_1, ..., y_{r_k}$ belong to W_k.

as $W_1 + W_2 + ... + W_k = W_1 \oplus W_2 \oplus ... \oplus W_k$

Then v = linear combination of $x_1, ..., x_{r_1}$ + ... + linear combination of $y_1, ..., y_{r_k}$.

$\therefore \quad v \in W_1 + ... + W_k$

$\Rightarrow V = W_1 + ... + W_k$

$\Rightarrow$ dim V = dim $(W_1 + ...$ + dim $W_k)$

= dim W_1 + ... + dim W_k

(by above theorem)

Conversely, let dim V= dim W_1 + ... + dim W_k = dim W

$\therefore$ $\dim W = \dim V$

$\Rightarrow$ $W = V$

If β_i is a basis of W_i $\forall$ i, by above theorem $\beta = \{\beta_1, ..., \beta_k\}$ is a basis of $W = V$

Since each β_i consists of eigen vectors only, β is a basis of V consisting of eigen vectors only.

$\therefore$ T is diagonalisable.

Theorem 7: *Let T be a linear operator on a finite dimensional vector space $V(F)$. Then T is diagonalisable if and only if the characteristic polynomial $f(x)$ of T is*

$$f(x) = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k},$$

where $d_i = \dim W_i$

and $d_1 + \ldots + d_k = \dim V = n$

Proof: Since T is diagonalisable, $\exists$ an ordered basis $\beta = \{v_1, ..., v_n\}$ s.t. $[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_n \end{bmatrix}$.

Suppose c_1 appears d_1 times, ..., c_k appears d_k times, then

$$[T]_\beta = \begin{bmatrix} c_1 & & & & & O \\ & \ddots & & & & \\ & & c_1 & & & \\ & & & \cdots & & \\ & & & & c_k & \\ & & & & & \ddots \\ O & & & & & c_k \end{bmatrix}$$

$\therefore$ characteristic polynomial for T is given by

$$f(x) = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k},\ d_1 + \ldots + d_k = n$$

$\therefore$ $[T - c_i I]_\beta$ has only d_i zeros on the diagonal for all $i = 1, ..., k$

$\therefore$ Rank $[T - c_i I] = n - d_i$ for all $i = 1, ..., k$ (See Remark 9 on page 595)

$\Rightarrow$ nullity $(T - c_i I) = d_i$ for all $i = 1, ..., k$

$\Rightarrow$ $\dim W_i = d_i$ for all $i = 1, ..., k$. ($W_i = \text{Ker}\ (T - c_i I)$)

Conversely, since $d_1 + d_2 + \ldots + d_k = \dim V$

$\dim W_1 + \dim W_2 + \ldots + \dim W_k = \dim V$

By theorem 6 then T is diagonalisable.

Definition: Let T be a linear operator on a *F.D.V.S.* V. Let $c \in F$ be an eigen value of T. The dimension of eigen space W_c is called the *geometric multiplicity* of c. Also the multiplicity of c as a root of the characteristic polynomial of T is called the *algebraic multiplicity* of c.

If we denote the geometric multiplicity of c by *G.M.* and the algebraic multiplicity of c by *A.M.* we can prove

Theorem 8: *G.M.* $\leq$ *A.M.*

Proof: Let dim $W_c = g$ = *G.M.* and *A.M.* = m

Let $\{x_1, x_2, \ldots, x_g\}$ be a basis of W_c then it can be extended to a basis $\beta = \{x_1, x_2, \ldots, x_g, y_1, \ldots, y_n\}$ of V.

Now $T(x_1) = cx_1 = cx_1 + ox_2 + \ldots + ox_g + oy_1 + \ldots + oy_n$

. . . .

. . . .

$T(x_g) = cx_g = ox_1 + \ldots + ox_{g-1} + cx_g + oy_1 + \ldots + oy_n$

Let $A = [T]_\beta$, then $A = \begin{bmatrix} cI_g & - \\ O & B \end{bmatrix}$

where I_g denotes $g \times g$ identity matrix and B is $n \times n$ matrix.

Let $f(x)$ be the characteristic polynomial of T (or A), then

$$f(x) = |xI - A| = \begin{bmatrix} (x-c)I_g & - \\ O & xI_n - B \end{bmatrix}$$

$$= (x - c)^g \, |x\, I_n - B|$$

$\Rightarrow$ algebraic multiplicity of c is at least g.

Hence *G.M.* $\leq$ *A.M.*

Example 7: Let $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Then characteristic polynomial of A is $(x + 1)(x - 1)^2$

Let $c = 1$, then eigen space $W_c = \left\langle \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\rangle$

(See Problem 10)

Thus, geometric multiplicity of c is 2 and algebraic multiplicity of c is 2.

Theorem 9: *Let T be a linear operator on a finite dimensional vector space V(F). Then T is diagonalisable if and only if algebraic multiplicity of* c_i *is same as geometric multiplicity of* $c_i \ \forall \ i$.

Proof: Suppose T is diagonalisable.

By theorem 7, the characteristic polynomial $f(x)$ of T is

$$f(x) = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k}.$$

where $d_i = \dim W_i$, $d_1 + \ldots + d_k = n$.

$\therefore$ algebraic multiplicity of $c_i = d_i = \dim W_i$ = geometric multiplicity of $c_i \ \forall \ i$.

Conversely, let $f(x)$ be the characteristic polynomial of T. Let d_i be the algebraic multiplicity of $c_i \ \forall \ i$.

Then $f(x) = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k}$,

$d_i = \dim W_i \ \forall\ i$ by hypothesis

By theorem 7, T is diagonalisable.

Theorem 10: *Let T be a linear operator on a finite dimensional vector space $V(F)$. Let $p(x)$ be the minimal polynomial of T. Then T is diagonalisable if and only if*

$p(x) = (x - c_1) \ldots (x - c_k)$, where $c_1, c_2, \ldots, c_k \in F$ are distinct.

Proof: Let $p(x) = (x - c_1) \ldots (x - c_k)$

Let $f_i(x) = \dfrac{p(x)}{(x - c_i)}$, $i = 1, 2, \ldots, k$.

Then g.c.d. $(f_1, f_2, \ldots, f_R) = 1$

$\Rightarrow \exists\ g_1, g_2, \ldots, g_k \in F[x]$ such that

$g_1 f_1 + \ldots + g_k f_k = 1$

$\therefore \quad g_1(T) f_1(T) + \ldots + g_k f_k(T) = I$

Let $v \in V$

Then $v = g_1(T) f_1(T)v + \ldots + g_k(T) f_k(T)\ (v)$

$f_1(T)v = (T - c_2 I) \ldots (T - c_k I)(v)$

$\Rightarrow (T - c_1 I) f_1(T)(v) = (T - c_1 I)(T - c_2 I) \ldots (T - c_k I)(v)$

$= p(T)(v)$

$= 0$

$\Rightarrow f_1(T)(v) \in \text{Ker}\ (T - c_1 I) = W_1$

$\Rightarrow g_1(T) f_1(T)(v) \in W_1$

(as $w_1 \in W_1 \Rightarrow T(w_1) = c_1 w_1$

$\Rightarrow T^r(w_1) = c_1^r w_1 \in W_1$)

Similarly, $g_i(T) f_i(T)\ (v) \in W_i \ \forall\ i$

$\therefore v \in W_1 + \ldots + W_k$

$\Rightarrow V = W_1 + \ldots + W_k$

$\Rightarrow \dim V = \dim W_1 + \ldots + \dim W_k$ (by theorem 5)

$\Rightarrow T$ is diagonalisable.

Conversely, let T be diagonalisable then $\exists$ a basis $\beta = \{v_1, \ldots, v_n\}$ of V such that each v_i is an eigen vector of T.

Now $(T - c_1 I) \ldots (T - c_k I)\ (v_i) = 0 \ \forall\ i$

as each v_i belongs to some eigen space.

$W_j = \text{Ker}\ (T - c_j I)$.

$\therefore\ p(x) = (x - c_1) \ldots (x - c_k)$ is the minimal polynomial of T.

Theorem 11: *Let T be a linear operator on an n-dimensional vector space V, and suppose that T has n distinct characteristic values. Then T is diagonalisable.*

Proof: Let $c_1, \ldots, c_n$ be distinct eigen values of T and $v_1, \ldots, v_n$ be corresponding eigen vectors of T.

$\therefore \quad T(v_i) = c_i v_i$ for all $i = 1, \ldots, n$

$\Rightarrow (T - cI)v_i = 0$ for all i, $v_i \neq 0$

$\Rightarrow 0 \neq v_i \in \text{Ker } (T - c_iI)$

$\Rightarrow \dim (\text{Ker } (T - c_iI) \geq 1$

$\Rightarrow \dim W_i \geq 1$, where $W_i = \text{Ker } (T - c_i I)$ = eigen space of T

$\Rightarrow \dim W_1 + ... + \dim W_n \geq n = \dim V$

$\Rightarrow \dim (W_1 + ... + W_n) \geq \dim V$

$\Rightarrow \dim (W_1 + ... + W_n) = \dim V$ as $W_1 + ... + W_n \subseteq V$

$\Rightarrow \dim W_1 + ... + \dim W_n = \dim V$

$\Rightarrow T$ is diagonalisable by Theorem 6.

However the converse of above theorem need not be true. Consider

Example 8: Let T be a linear operator on $\boldsymbol{R}^3$ such that matrix of T w.r.t. standard basis of $\mathbf{R}^3$ is $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Then eigen values of A (or T) are 1, –1, –1.

(See problem 10) dim $W_1 = 2$, dim $W_{-1} = 1$

$\therefore$ dim W_1 + dim $W_{-1} = 3 = \dim \mathbf{R}^3$

$\therefore$ T is diagonalisable but eigen values of T are not distinct.

Theorem 12: *Let T be a linear operator on a finite dimensional vector space V over F. Let $c_1, ..., c_k$ be distinct eigen values of T and $v_1, ..., v_k$ be corresponding eigen vectors of T. Then $v_1, ..., v_k$ are linearly independent.* (*See problem* 4).

Proof: Let $\alpha_1 v_1 + ... + \alpha_k v_k = 0$

Then $w_1 + ... + w_k = 0$

where $w_i = \alpha_i v_i \in W_i$ = eigen space of T w.r.t. c_i

Since $W_1 + ... + W_k$ is direct sum, $w_i = 0 \ \forall \ i$

$\therefore \alpha_i v_i = 0 \ \forall \ i$, $v_i \neq 0$

$\Rightarrow \alpha_i = 0 \ \forall \ i$

$\therefore$ $v_1, ..., v_k$ are linearly independent.

Note: If T is diagonalisable operator, then $\exists$ a basis β of V s.t. $[T]_\beta$ = diagonal matrix = A. If β' is any other basis of V, then $\exists$ matrix P s.t. $[T]_{\beta'} = P^{-1}AP$. We say that $[T]_{\beta'}$ is similar to diagonal matrix. So if T is diagonalisable, then matrix of T w.r.t. any basis is similar to a diagonal matrix. This leads us to the following definition:

Let A be $n \times n$ matrix. We say A is diagonalisable if A is similar to a diagonal matrix, i.e. $A = P^{-1}BP$, B = diagonal matrix.

One may notice that we can have a non diagonal matrix which is similar to a diagonal matrix. For instance, $A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ has distinct eigen values 1 and 2 and so is similar to a diagonal matrix although A itself is not a diagonal matrix.

Remarks: (1) Let $A = [T]_\beta$. Suppose A is diagonalisable. Then T is diagonalisable.

Proof: Since A is diagonalisable, $\exists$ matrix P s.t. $A = P^{-1} BP$, where B = diagonal matrix $(c_1, ..., c_1, ..., c_k, ..., c_k)$.

$\therefore$ $f(x)$ = characteristic polynomial of T

$= (x - c_1)^{d_1} ... (x - c_k)^{d_k}$, where c_i's are distinct and $d_1 + ... + d_k = n = \dim V$.

Now $$B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

$\therefore$ $$X_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \text{eigen vector of } B \text{ w.r.t. eigen value } c_1 \text{ of } B$$

So, $$\begin{aligned} A(P^{-1}X_1) &= (P^{-1}BP)\ (P^{-1}X_1) \\ &= P^{-1}\ BX_1 \\ &= P^{-1}\ c_1X_1 \\ &= c_1(P^{-1}X_1) \end{aligned}$$

$\therefore$ $P^{-1}X_1$ = eigen vector of A w.r.t. eigen value c_1 of A. Similarly,

$$X_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \text{eigen vector of } B.$$

$\Rightarrow$ $P^{-1}X_2$ = eigen vector of A.

In this way, $X_1, X_2, ..., X_{d_1}$ are eigen vectors of B.

$\Rightarrow$ $P^{-1}X_1, P^{-1}X_2, ..., P^{-1}X_{d_1}$ are eigen vectors of A w.r.t. eigen value c_1.

Let $$\sum_{i=1}^{d_1} \alpha_i P^{-1}X_i = 0,\ \alpha_i \in F$$

Then $$P^{-1} \sum_{i=1}^{d_1} \alpha_i\ X_i = 0 \Rightarrow \sum_{i=1}^{d_1} \alpha_i X_i = 0 \Rightarrow \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{d_1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$$

$\therefore \quad \alpha_i = 0 \quad \forall\ i = 1, ..., d_1$

So, $P^{-1}X_1, ..., P^{-1}X_{d_1}$ are *L.I.* vectors.

$\therefore$ dim $W'_{c_1} \geq d_1$, where W'_{c_1} = eigen space of A w.r.t. eigen value c_1 of A.

So, dim $W_{c_1} \geq d_1$, where W_{c_1} = eigen space of T w.r.t. eigen value c_1 of T.

Similarly, dim $W_{c_i} \geq d_i \quad \forall\ i = 1, 2, ..., k$.

Suppose dim $W_{c_i} > d_i$ for some i. Let $W = W_{c_1} + ... + W_{c_k}$.

Then dim $W = \sum_{i=1}^{k}$ dim $W_{c_i} > d_1 + ... + d_i + ... + d_k = n$.

$\therefore$ dim $W >$ dim V, a contradiction.

So, dim $W_{c_i} = d_i \ \forall\ i$.

Hence T is diagonalisable by theorem 7.

(2) Let $X_1, ..., X_k$ be eigen vectors corresponding to eigen values $c_1, c_2, ..., c_k$ of an $n \times n$ matrix A over F. Then $\{X_1, ..., X_k\}$ is a *L.I.* set.

Let $$X_1 = \begin{bmatrix} \alpha_{11} \\ \cdots \\ \cdots \\ \alpha_{n1} \end{bmatrix}, ..., X_k = \begin{bmatrix} \alpha_{1k} \\ \cdots \\ \cdots \\ \alpha_{nk} \end{bmatrix}$$

Then $AX_i = c_i X_i$

Let $\beta = \{e_1, e_2, ..., e_n\}$ be a basis of some vector space V, then $\exists$ a linear transformation $T : V \to V$, s.t.,

$$T(e_1) = a_{11}e_1 + ... + a_{n1}e_n$$
$$. \ . \ . \ . \ . \ . \ . \ . \ . \ .$$
$$T(e_n) = a_{1n}e_1 + ... + a_{nn}e_n$$

where $A = (a_{ij})$.

Then $A = [T]_\beta$

Let $$v_1 = \alpha_{11}e_1 + ... + a_{n1}e_n$$
$$. \ . \ . \ . \ . \ . \ . \ . \ . \ .$$
$$v_k = \alpha_{1k}e_1 + ... + a_{nk}e_n$$

Then $v_1, ..., v_k$ are eigen vectors of T s.t.,

$T(v_i) = c_i v_i$, $i = 1, 2, ..., k$ (See Remark 7, page 594)

$\therefore$ By theorem 12, $\{v_1, v_2 ..., v_k\}$ is *L.I.*

Let $\beta_1 X_1 + ... + \beta_k X_k = 0$, $\beta_i \in F$

Then $$\beta_1 \begin{bmatrix} \alpha_{11} \\ \cdots \\ \cdots \\ \alpha_{n1} \end{bmatrix} + ... + \beta_k \begin{bmatrix} \alpha_{1k} \\ \cdots \\ \cdots \\ \alpha_{nk} \end{bmatrix} = 0$$

Thus $\beta_1\alpha_{11} + ... + \beta_k\alpha_{1k} = 0$

. . . . . .

$\beta_1\alpha_{n1} + ... + \beta_k\alpha_{nk} = 0$

So $\beta_1(\alpha_{11}e_1 + ... + a_{n1}e_n) + ... + \beta_k(\alpha_{1k}e_1 + ... + a_{nk}e_k) = 0$

$\Rightarrow \beta_1 v_1 + \beta_2 v_2 + ... + \beta_k v_k = 0$

$\Rightarrow \beta_i = 0 \quad \forall\ i$

$\Rightarrow \{X_1, X_2, ..., X_k\}$ is a *L.I.* set.

Theorem 13: *Let A be an n × n matrix. Then A is diagonalisable if and only if A has n linearly independent eigen vectors.*

Proof: Suppose A is diagonalisable, then $\exists$ a non-singular matrix P s.t.,

$P^{-1}AP = D = \text{diag}\ (c_1, c_2, ..., c_n)$

or $AP = PD$

Let $P = [X_1, X_2, ..., X_n]$

Then $AP = [AX_1, AX_2, ..., AX_n]$

$PD = [c_1X_1, c_2X_2, ..., c_nX_n]$

Thus $AX_i = c_iX_i \quad i = 1, 2, ..., n$

Since P is invertible, X_is are *L.I.* eigen vectors. So $X_i \neq 0 \quad \forall\ i$

Hence $X_1, X_2, ..., X_n$ are eigen vectors of A.

Conversely, let $X_1, X_2, ..., X_n$ be *L. I.* eigen vectors of A, corresponding to eigen values $c_1, c_2, ..., c_n$ of A

Then $AX_i = c_i X_i \quad \forall\ i$

Let $P = [X_1, X_2, ..., X_n]$

Since X_i are linearly independent, P is invertible

Thus $AP = [AX_1, AX_2, ..., AX_n]$

$= [c_1X_1, c_2X_2, ..., c_nX_n]$

$= PD$, where $D = \text{diag}\ (c_1, c_2, ..., c_n)$.

i.e., $A = PDP^{-1}$

Hence A is diagonalisable.

Problem 22: *Show that* $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ *and* $B = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$ *are not diagonalisable.*

Solution: Since A is a triangular matrix, entries on diagonal are eigen values of A and thus 0 is the only eigen value of A.

If A is diagonalisable then A is similar to a diagonal matrix D.

$\therefore \quad A = P^{-1}\begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix} P$

$\Rightarrow c_1 = c_2 = 0$

i.e., $A = 0$, a contradiction and so A is not diagonalisable.

Again, λ will be the only eigen value of B and if B is diagonalisable then

$$B = P^{-1}\begin{bmatrix} c_1 & 0 & 0 \\ 0 & c_2 & 0 \\ 0 & 0 & c_3 \end{bmatrix} P$$

$\Rightarrow c_1 = c_2 = c_3 = \lambda$ and so $B = \lambda I$, a contradiction.

Problem 23: *Construct a diagonalisable* 3×3 *matrix* A *whose eigen values are* $-2, -2, 6$ *and corresponding eigen vectors are* $\begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$.

Solution: Let $D = \begin{bmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 6 \end{bmatrix}$, $P = \begin{bmatrix} 1 & 0 & 2 \\ -2 & 3 & 1 \\ 0 & 1 & -1 \end{bmatrix}$

then $A = P^{-1}DP = \begin{bmatrix} -2 & 6 & -6 \\ 0 & 3 & -5 \\ 0 & -3 & 1 \end{bmatrix}$.

Problem 24: *Find* A^{100} *where* $A = \begin{bmatrix} -1 & 2 \\ 3 & 4 \end{bmatrix}$.

Solution: 5 and -2 will be eigen values of A and so it is diagonalisable.

$$X_1 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}, X_2 = \begin{bmatrix} -2 \\ 1 \end{bmatrix} \text{ are corresponding eigen values}$$

Let $P = \begin{bmatrix} 1 & -2 \\ 3 & 1 \end{bmatrix}$

Then $A = P^{-1}\begin{bmatrix} 5 & 0 \\ 0 & -2 \end{bmatrix} P \Rightarrow A^{100} = P^{-1}\begin{bmatrix} 5^{100} & 0 \\ 0 & 2^{100} \end{bmatrix} P$

$$A^{100} = \frac{1}{7}\begin{bmatrix} 1 & 2 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 5^{100} & 0 \\ 0 & 2^{100} \end{bmatrix}\begin{bmatrix} 1 & -2 \\ 3 & 1 \end{bmatrix}$$

$$= \frac{1}{7}\begin{bmatrix} 1 & 2 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 5^{100} & -2.5^{100} \\ 3.2^{100} & 2^{100} \end{bmatrix}$$

$$= \frac{1}{7}\begin{bmatrix} 5^{100} + 6.2^{100} & -2.5^{100} + 2.2^{100} \\ -3.5^{100} + 3.2^{100} & 6.5^{100} + 2^{100} \end{bmatrix}$$

Problem 25: *If* $A = \begin{bmatrix} -2 & 6 & -6 \\ 0 & 3 & -5 \\ 0 & -3 & 1 \end{bmatrix}$, *find eigen values of* $A^4 + A^2 + 5A$.

Solution: Eigen values of A are $-2, -2, 6$

Let $f(x) = x^4 + x^2 + 5x$. If $c \in F$ is an eigen value of A then $f(c)$ is an eigen value of $f(A)$.

Now $f(-2) = (-2)^4 + (-2)^2 + 5(-2) = 10$

$f(6) = 6^4 + 6^2 + 5.6 \quad = 1362$

Thus eigen values of $A^3 + A^2 + 5A$ are 10, 10, 1362.

Example 9: *Let* $A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.

Then the characteristic polynomial of A is $f(x) = (x + 1)^2 (x - 2)$.

Also $\left\{ \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \right\}$ is a basis of eigen space W_{-1} w.r.t. eigen value -1 and $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$ is a basis of eigen space W_2 w.r.t. eigen value 2.

$$\therefore \qquad P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } P^{-1} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix}.$$

$$\text{So,} \qquad P^{-1} A P = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

This provides a method of diagonalising a matrix.

Problem 26: *Let A be an* $n \times n$ *matrix over F such that its diagonal elements are* 'a' *and other elements are* 'b' *where a and b are in F. Show that A is diagonalisable, if char F = 0 or char F does not divide n.*

Solution: Let $f(x)$ be the characteristic polynomial of A.

Then $\quad f(x) = |xI - A|$

$$= \begin{vmatrix} x-a & -b & \cdots & -b \\ -b & x-a & \cdots & -b \\ \vdots & & \ddots & \\ -b & \cdots & -b & x-a \end{vmatrix}$$

Apply $C_1 \to C_1 + C_2 + \ldots + C_n$

$$= \begin{vmatrix} x-a-(n-1)b & -b & \cdots & -b \\ x-a-(n-1)b & x-a & \cdots & -b \\ \vdots & & \ddots & \\ x-a-(n-1)b & \cdots & & x-a \end{vmatrix}$$

$$= (x-a-(n-1)b)\begin{vmatrix} 1 & -b & \cdots & -b \\ 1 & x-a & \cdots & -b \\ \vdots & & \ddots & \\ 1 & \cdots & & x-a \end{vmatrix}$$

Apply $R_2 \to R_2 - R_1$, $R_3 \to R_3 - R_1$, . . . $R_n \to R_n - R_1$

$$= (x-a-(n-1)b)\begin{vmatrix} 1 & -b & \cdots & -b \\ 0 & x-a+b & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & \cdots & & x-a+b \end{vmatrix}$$

$$= (x-(a+(n-1)b))\,(x-(a-b))^{n-1}$$

Let $p(x)$ be the minimal polynomial of A.

Then $p(x) = (x-(a+(n-1)b))\,(x-(a-b))$

Since $p(x)$ is the product of linear factors in $F[x]$, A is diagonalisable.

Problem 27: *In above problem, find P such that $P^{-1}AP$ is diagonal.*

Solution: $A = \begin{bmatrix} a & b & \cdots & b \\ b & a & \cdots & b \\ \vdots & \vdots & \ddots & \vdots \\ b & b & \cdots & a \end{bmatrix}$

Then $A \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} a+(n-1)b \\ a+(n-1)b \\ \vdots \\ a+(n-1)b \end{bmatrix} = a+(n-1)b \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$

So, $\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$ is an eigen vector of A with respect to eigen value $a + (n-1)b$.

Also $A\begin{bmatrix}1\\-1\\0\\\vdots\\0\end{bmatrix} = \begin{bmatrix}a-b\\a-b\\0\\\vdots\\0\end{bmatrix} = (a-b)\begin{bmatrix}1\\-1\\0\\\vdots\\0\end{bmatrix}$

So, $\begin{bmatrix}1\\-1\\0\\\vdots\\0\end{bmatrix}$ is an eigen vector of A with respect to eigen value $a - b$.

In this way, we get all $n - 1$ eigen vectors of A with respect of eigen value $a - b$.

Therefore, $P = \begin{bmatrix}1 & 1 & 1 & \cdots & 1\\1 & -1 & 0 & & 0\\\vdots & 0 & -1 & & 0\\\vdots & \vdots & 0 & & \vdots\\\vdots & \vdots & \vdots & & 0\\1 & 0 & 0 & \cdots & -1\end{bmatrix}$

Such that $P^{-1}AP = \begin{bmatrix}a+(n-1)b & 0 & \cdots & 0\\0 & a-b & \ddots & 0\\\vdots & \vdots & \ddots & \\0 & 0 & \cdots & a-b\end{bmatrix}$

$= \text{diag}\ (a + (n - 1)b, a - b, \ldots, a - b).$

Problem 28: *Let* $A = \begin{bmatrix}6 & -3 & -2\\4 & -1 & -2\\10 & -5 & -3\end{bmatrix}$.

Show that A is not similar over **R** *to a diagonal matrix whereas A is similar over* **C** *to a diagonal matrix.*

Solution: Characteristic polynomial of A is $(x - 2)(x^2 + 1)$

If A is similar to a diagonal matrix over **R**, then $\exists$ matrix P s.t.

$P^{-1}AP = \text{diag}\ (a, b, c)$, a, b, c are real. Eigen values of $P^{-1}AP$ are eigen values of $A = 2, \pm i$. But eigen values of diag (a, b, c) are a, b, c by (problem 11) where a, b, c are all real, a contradiction.

$\therefore$ A is not similar over **R** to a diagonal matrix.

Since eigen values of A are distinct, by Theorem 11, A is similar over **C** to a diagonal matrix.

Problem 29: *Let V be the vector space of $n \times n$ matrices over F. Let A be a fixed $n \times n$ matrix over F. Let T be the linear operator "left multiplication by A" on V. Show that T and A have the same eigen values.*

Solution: Let c be an eigen value of A.

Then $AX = cX$ for some $0 \neq X$ ($X = n \times 1$ matrix).

Now $T(XX^t) = AXX^t = cXX^t$ (X^t means transpose of X)

If $XX^t = 0$, then

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} [x_1, \ldots, x_n] = 0$$

$$\Rightarrow x_1^2 = x_2^2 = \ldots = x_n^2 = 0$$

$$\Rightarrow x_i = 0 \text{ for all } i \Rightarrow X = 0, \text{ a contradiction}$$

$$\therefore \quad XX^t \neq 0$$

So, c is also an eigen value of T.

Conversely, let c be an eigen value of T.

Then $\exists\ 0 \neq B \in V$ s.t. $T(B) = cB$

$$\Rightarrow AB = cB$$

$$\Rightarrow ABX = cBX \text{ for all column matrices } X$$

If $BX = 0$ for all X, then $B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$

$\Rightarrow$ 1st column of B is zero.

Similarly, $B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0 \Rightarrow$ 2nd column of B is zero.

In this way, all columns of B are zero.

$\therefore\ BX \neq 0$ for some X

$\therefore\ c$ is also an eigen value of A.

Thus T and A have same eigen values.

Problem 30: *Let A and B be $n \times n$ matrices over F. Show that AB and BA have same characteristic polynomial.*

Solution: Let $C = \begin{bmatrix} I_n & A \\ 0 & I_n \end{bmatrix}$ be $2n \times 2n$ matrix over F.

Then $C^{-1} = \begin{bmatrix} I_n & -A \\ 0 & I_n \end{bmatrix}$

Let $D = \begin{bmatrix} AB & 0 \\ B & 0 \end{bmatrix}$ be $2n \times 2n$ matrix over F.

Then $C^{-1}DC = \begin{bmatrix} 0 & 0 \\ B & BA \end{bmatrix} = E$

Since D and E are similar matrices.

Characteristic polynomial of D and E are same

$$\begin{vmatrix} xI_n & 0 \\ -B & xI_n - BA \end{vmatrix} = \begin{vmatrix} xI_n - AB & 0 \\ -B & xI_n \end{vmatrix}$$

$\Rightarrow x^n \mid xI_n - BA \mid = x^n \mid xI_n - AB \mid$

$\Rightarrow \mid xI_n - BA \mid = \mid xI_n - AB \mid$

$\Rightarrow$ charactersitic polynomial of BA = characteristic polynomial of AB.

Primary Decomposition Theorem

Theorem 14: *Let T be a liner operator on a finite dimensional space V over F. Let $p(x)$ be the minimal polynomial for T s.t.*

$$p(x) = p_1(x)^{r_1} \ldots\ldots p_k(x)^{r_k}$$

where the $p_i(x)$ are distinct irreducible monic polynomials over F and r_i are +ve integers. Let W_i be the null spaces of $p_i(T)^{r_i}$, $i = 1, \ldots, k$. Then

(*i*) $V = W_1 \oplus \ldots \oplus W_k$

(*ii*) *each W_i is invariant under T (i.e., $T(W_i) \subseteq W_i \ \forall\ i$)*

(*iii*) *if T_i is operator induced on W_i by T, then the minimal polynomial $q_i(x)$ for T_i is $p_i(x)^{r_i}$.*

Proof: Let $f_i(x) = \dfrac{p(x)}{p_i(x)^{r_i}}$, $i = 1, 2, \ldots, k$

Then g.c.d. $(f_1(x), \ldots, f_k(x)) = 1$

$\therefore\ \exists\ g_1(x), \ldots, g_k(x) \in F[x]$ such that

$$g_1(x) f_1(x) + \ldots + g_k(x) f_k(x) = 1$$

$$\Rightarrow g_1(T) f_1(T) + \ldots + g_k(T) f_k(T) = I$$

Let $v \in V$, then

$$v = g_1(T) f_1(T)(v) + \ldots + g_k(T) f_k(T)(v)$$

Now $p_i(T)^{r_i} f_i(T) g_i(T) = p(T) g_i(T) = 0$

$\therefore$ $g_i(T) f_i(T)(v) = f_i(T) g_i(T)(v)$

$\Rightarrow p_i(T)^{r_i} g_i(T) f_i(T)(v) = 0$

$\Rightarrow g_i(T) f_i(T)(v) \in \text{Ker } p_i(T)^{r_i} = W_i$

$\Rightarrow v \in W_1 + \ldots + W_k$

$\Rightarrow V = W_1 + \ldots + W_k$

or that $V = W_1 \oplus ... \oplus W_k$

For let $x_1 + ... + x_k = 0, \quad x_i \in W_i$

then $x_1 = -(x_2 + ... + x_k)$

$\Rightarrow f_1(T)\, x_1 = 0$ as $\forall\ i \neq 1, f_1(T)\, x_i = 0$

Now g.c.d. $(f_1(x), p_1(x)^{r_1}) = 1$

So $\exists\ q_1(x), r_1(x) \in F[x]$ such that

$$f_1(x)\, q_1(x) + p_1(x)^{r_1}\, r_1(x) = 1$$

$$\Rightarrow I = q_1(T)\, f_1(T) + r_1(T)\, p_1(T)^{r_1}$$

$$\Rightarrow x_1 = 0$$

Similarly $x_i = 0\ \forall\ i$

This proves (*i*).

Let $x_i \in W_i = \text{Ker}\ p_i(T)^{r_i}$

Then $p_i(T)^{r_i}\ (x_i) = 0$

$$\Rightarrow Tp_i(T)^{r_i}\ (x_i) = 0$$

$$\Rightarrow p_i(T)^{r_i}\ (T(x_i)) = 0$$

$$\Rightarrow T(x_i) \in W_i\ \forall\ i$$

$\Rightarrow W_i$ is T-invariant $\forall\ i$

which proves (*ii*).

Again, since $p_i(T)^{r_i}\ (x_i) = 0 \quad \forall\ x_i \in W_i$

$$p_i(T)^{r_i} = 0 \text{ on } W_i$$

$\Rightarrow p_i(T_i)^{r_i} = 0$ as T restricted to W_i is T_i.

$\Rightarrow q_i(x) \mid p_i(x)^{r_i} \Rightarrow q_i(x) = p_i(x)^{s_i},\ s_i \leq r_i$

Let $f(x) = f_i(x)p_i(x)^{si}$

and let $v \in V$ then $v = w_1 + ... + w_k, \quad w_i \in W_i$

$\therefore f(T)(v) = f_i(T)\ p_i(T)^{s_i} w_i$

$\because \quad f_i(T)\ w_j = 0 \quad \forall\ j \neq i$

$\therefore \quad f(T)(v) = f_i(T) q_i(T) w_i$

$$= f_i(T)\ q_i(T_i)\ w_i$$

$$= 0 \text{ as } q_i(T_i) = 0$$

$\Rightarrow f(T) = 0$

$\therefore \quad p(x) \mid f(x)$

$$\Rightarrow p_i(x)^{r_i} \mid p_i(x)^{s_i}$$

$$\Rightarrow r_i \leq s_i$$

$\therefore \quad r_i = s_i$

So, $q_i(x) = p_i(x)^{r_i}$

which proves (*iii*).

Cor.: If T is a linear operator on a finite dimensional space V over F and minimal polynomial $p(x)$ of T is a product of distinct linear factors, then T is diagonalisable.

Proof: Let $p(x) = (x - c_1) \ldots (x - c_r)$, where c_i are distinct roots of $p(x)$ in F. By primary decomposition theorem

$V = W_1 \oplus \ldots \oplus W_r$, where each W_i = Null space of $(T - c_i I)$

$\therefore \quad v \in W_i \Rightarrow (T - c_i I)v = 0$

$\Rightarrow T(v) = c_i v$

$\therefore$ every non zero vector in W_i is an eigen vector of T corresponding to eigen value c_i of T. If β_i is a basis of W_i, then $\{\beta_i, \ldots, \beta_r\}$ is a basis of V. β_i consists of eigen vectors of $T \Rightarrow \{\beta_1, \ldots, \beta_r\} = \beta$ consists of eigen vectors of T and is a basis of $V \Rightarrow T$ is a diagonalisable.

Problem 31: *Let T and S be linear operators on $V(F)$, each having all its eigen values in F such that $TS = ST$.*

Show that they have a common eigen vector.

Solution: Let c be an eigen value of T. Let $W_c = \{v \in V \mid T(v) = cv\}$ be the eigen space w.r.t. eigen value c.

Let $v \in W_c$.

Then $T(S(v)) = (TS)(v)$

$= (ST)(v)$

$= S(T(v))$

$= S(cv)$

$= cS(v)$

$\therefore S(v) \in W_c \ \forall \ v \in W_c \Rightarrow S : W_c \to W_c$.

$\therefore S$ is a linear operator on W_c.

Let $\alpha \in F$ be an eigen value of S as linear operator on W_c.

$\therefore \exists \ w \in W_c$ such that

$S(w) = \alpha w, \ w \neq 0$

$w \in W_c \Rightarrow T(w) = cw$

$\therefore w$ is a common eigen vector of T and S.

Problem 32: *Let N be 2×2 complex matrix such that $N^2 = 0$. Prove that either $N = 0$ or N is similar over* $\mathbf{C}$ *to* $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

Solution: Let $T : V \to V$ be a linear operator such that

$[T]_\beta = N$, $\beta = \{v_1, v_2\}$ is a basis of V.

Now $\quad 0 = N^2 = N \,.\, N = [T]_\beta \, [T]_\beta = [T^2]_\beta$

$\Rightarrow \ T^2 = 0$.

Suppose $N \neq 0$, *i.e.*, $T \neq 0$.

Let λ be an eigen value of T.

Then there exists $0 \neq v \in V$ s.t.

$$T(v) = \lambda v$$

$$\Rightarrow T^2(v) = \lambda(T(v)) = \lambda^2 v$$

$$\Rightarrow 0 = \lambda^2 v$$

$$\Rightarrow \lambda^2 = 0 \text{ as } v \neq 0$$

$$\Rightarrow \lambda = 0$$

$\Rightarrow$ 0 is the only eigen value of T.

Let W_o be the eigen space of T w.r.t. eigen value 0.

Then $W_o = \{x \in V \mid T(x) = 0\} = \text{Ker } T$

Since $0 \neq v \in W_o$, $W_o \neq \{0\}$

So, dim $W_o = 1$ or 2.

If dim $W_o = 2$, then dim $W_o = \dim V$

$\Rightarrow W_o = V \Rightarrow$ Ker $T = V \Rightarrow T = 0$, which is not true.

Therefore, dim $W_o = 1$.

Let $W_o = < w_2 >$

There exists a subspace W' of V s.t.

$$V = W' \oplus W_o$$

Since dim $V = 2$, dim $W_o = 1$, dim $W' = 1$.

Let $W' = < w_1 >$

Then $\{w_1, w_2\}$ is a basis of V.

Let $T(w_1) = \alpha_1 w_1 + \alpha_2 w_2$

$T(w_2) = 0w_1 + 0w_2$ as $w_2 \in$ Ker T.

But $T^2 = 0 \Rightarrow 0 = T^2(w_1)$

$$= \alpha_1 T(w_1) + \alpha_2 T(w_2)$$

$$= \alpha_1 T(w_1)$$

$$= \alpha_1(\alpha_1 w_1 + \alpha_2 w_2)$$

$$= \alpha_1^2 w_1 + \alpha_1 \alpha_2 w_2$$

$\Rightarrow \alpha_1 = 0$ ($\alpha_2 \neq 0$ as $\alpha_2 = 0 \Rightarrow w_1 \in$ Ker T

$\Rightarrow w_1 \in W_o \cap W' = \{0\}$

$\Rightarrow w_1 = 0$ which is not true).

So, $T(w_1) = \alpha_2 w_2$.

Now $\{\alpha_2^{-1} w_1, w_2\} = \beta'$ is also a basis of V

as $a\alpha_2^{-1} w_1 + bw_2 = 0$

$\Rightarrow a\alpha_2^{-1} = 0, b = 0$

$\Rightarrow a = 0 = b$.

$\Rightarrow \{\alpha_2^{-1} w_1, w_2\} = \beta'$ is a *L.I.* set

$\Rightarrow \beta'$ is a basis of V as dim $V = 2$

Therefore, $T(\alpha_2^{-1} w_1) = \alpha_2^{-1} T(w_1)$

$= \alpha_2^{-1} \alpha_2 w_2 = w_2$

$= 0\alpha_2^{-1} w_1 + 1 w_2$

$\Rightarrow [T]_{\beta'} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

Also $[T]_{\beta} = N$

$\Rightarrow N$ is similar to $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ over $\mathbf{C}$.

Problem 33: *Show that if A is a 2×2 matrix over $\mathbf{C}$ then A is similar to a matrix of the type $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ or $\begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}$ over $\mathbf{C}$.*

Solution: Let $f(x)$ be the characteristic polynomial of A. If the roots of $f(x)$ are distinct, then A is diagonalisable.

So, $A = P^{-1}BP$, $B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ $a, b \in \mathbf{C}$.

$\Rightarrow A$ is similar over $\mathbf{C}$ to $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$

If the roots of $f(x)$ are same, let $f(x) = (x - \alpha)^2$

Then $0 = f(A) = (A - \alpha I)^2$

Let $N = A - \alpha I$

By above problem either $N = 0$ or N is similar over $\mathbf{C}$ to $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

If $N = 0$, then $A = \alpha I = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$

$\Rightarrow A$ is similar over $\mathbf{C}$ to $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$

If $N = Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$

Then $A - \alpha I = Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$

$\Rightarrow A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} + Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$

$= Q^{-1}\left\{\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right\}Q$

$$= Q^{-1}\begin{bmatrix}\alpha & 0\\ 1 & \alpha\end{bmatrix}Q$$

$\Rightarrow A$ is similar over **C** to the matrix of the type $\begin{bmatrix}\alpha & 0\\ 1 & \alpha\end{bmatrix}$.

Problem 34: *Give an example to show that AB is diagonalisable and BA is not diagonalisable, where A and B are n × n matrices over F.*

Solution: Let $A = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$, $B = \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$

Then $AB = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$

So, AB is a diagonal matrix. AB is a diagonalisable matrix.

Now $BA = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ and $(BA)^2 = 0$

$\Rightarrow$ minimal polynomial of BA is x^2.

So, the minimal polynomial of BA is not product of distinct linear factors.

$\therefore$ BA is not diagonalisable.

Problem 35: *If T is an idempotent linear operator* (*i.e.*, $T^2 = T$) *then show that* 0 *or* 1 *are only eigen values of T and T is diagonalisable.*

Solution: Let $f(x) = x\,(x - 1) = x^2 - x$

then $f(T) = T^2 - T = 0$

If $p(x)$ is the minimal polynomial of T, then $p(x) \mid f(x)$.

$p(x) = x$ or $x - 1$ or $x(x - 1)$

The eigen values of T are the roots of the minimal polynomial of T.

$\therefore$ 0 or 1 are only eigen values of T.

In each case $p(x) = x$ or $x - 1$ or $x(x - 1)$,

$p(x)$ is product of distinct linear factors. So, T is diagonalisable.

Problem 36: *Give an example of a linear operator T having eigen values 0 and 1 but T is not idempotent.*

Solution: Let T be a linear operator on V where dim $V = 3$ such that matrix of T w.r.t. a basis of V is

$$A = \begin{bmatrix}0 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix}$$

Then eigen values of A (or T) are entries on the diagonal as A is a triangular matrix.

$\therefore$ eigen values of T are 0, 1, 1.

But $$A^2 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \neq A$$

$\therefore$ A is not idempotent.

So, T is not idempotent.

Exercises

1. Find the characteristic polynomial for identity and zero operator on n-dimensional space.

2. Give an example of a 2×2 matrix A such that A and transpose of A do not have same eigen values.

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

3. Show that A is nilpotent if and only if all eigen values of A are zero.

4. Show that any nilpotent matrix has trace zero.

5. Let A, B be $n \times n$ matrices over a field F. Prove that if $(I - AB)$ is invertible then $I - BA$ is invertible and $(I - BA)^{-1} = I + B(I - AB)^{-1}A$.

6. Find the eigen values and bases for the eigen spaces of the matrix

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 4 \end{bmatrix}$$

Is A diagonalisable

$$2,\ 3 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}$$

7. Find eigen values, eigen vectors and eigen spaces of the matrix

$$A = \begin{bmatrix} -2 & 6 & -6 \\ 0 & 3 & -5 \\ 0 & -3 & 1 \end{bmatrix}$$

Show A is diagonalisable

$$-2,\ -2,\ 6,\ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 6 \\ 5 \\ -3 \end{bmatrix}$$

Eigen space corresponding to eigen value –2 is spanned by $\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}$

and corresponding to eigen value 6 is spanned by $\begin{bmatrix}6\\5\\-3\end{bmatrix}$.

8. Let $A = \begin{bmatrix}a & b\\c & d\end{bmatrix}$ and $\Delta = (a-d)^2 + 4bd$. Show that

(i) If $\Delta > 0$ then A is diagonalisable.

(ii) If $\Delta < 0$ then A is not diagonalisable and

(iii) If $\Delta = 0$ then A many or may not be diagonalisable.

9. Find the characteristic roots and characteristic vectors for the matrix

$$A = \begin{bmatrix}2 & 2 & 1\\1 & 3 & 1\\1 & 2 & 2\end{bmatrix}.$$

[1, 1, 5]

10. Let T be a linear operator on a vector space $V(F)$. If $q(x) \in F[x]$ be such that $q(T) = 0$ then is every root of $q(x)$ in F a characteristic root of T? Justify.

11. Let A be an $n \times n$ matrix with characteristic polynomial

$$f(x) = (x - c_1)^{d_1} \ldots (x - c_k)^{d_k}.$$

Show that trace $A = c_1d_1 + c_2d_2 + \ldots + c_kd_k$.

12. Let λ be an eigen value of $n \times n$ matrix A. Prove that

(i) transpose of A has the same eigen value as that of A

(ii) kA has eigen value $k\lambda$ for any scalar k

(iii) A^r(r is a positive integer) has the eigen value λ^r

(iv) If A is invertible, A^{-1} has the eigen value $\frac{1}{\lambda}$.

(v) the matrix $A + kI$ has the eigen value $\lambda + k$.

13. For the matrix $A = \begin{bmatrix}1 & 2 & 0\\2 & 1 & -6\\2 & -2 & 3\end{bmatrix}$ find P such that $P^{-1}AP$ is a diagonal matrix.

$$\begin{bmatrix}1 & 1 & -1\\2 & 1 & 2\\-1 & 0 & 1\end{bmatrix}.$$

14. For the matrix $\begin{bmatrix} 1 & 1 & 2 \\ -1 & 2 & 1 \\ 0 & 1 & 3 \end{bmatrix}$ find P such that $P^{-1}AP$ is a diagonal matrix.

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & 0 \\ -1 & 1 & 1 \end{bmatrix}.$$

15. Let T be a linear operator on a *F.D.V.S.V.* Suppose T is diagonalisable. Show that
$T = \text{Ker } T \oplus ImT$

16. Show that the eigen values of $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ are the fourth roots of unity.

17. Let T be a linear operator on V such that T is diagonalisable. Show that $(T - \lambda I)^n(v) = 0$, $v \in V$, $\lambda \in F \Rightarrow (T - \lambda I)(v) = 0$.

18. Let T be a linear operator on V s.t., $T^m = I$. Let char $F = 0$. Suppose T has all eigen values in F. Show that T is diagonalisable.
[Hint: If g.c.d. $(f, f') = 1$, then roots of f are simple.]

Invariant Subspaces

Definition: Let T be a linear operator on a vector space V. If W is a subspace of V s.t. $T(W) \subseteq W$, we say W is *invariant under T* or is *T-invariant*.

Example 10: Since $T(0) = 0$ and $T(V) = V$, both zero subspace and V are invariant subspaces of V.

Example 11: Let $v \in \text{Ker } T$ then $T(v) = 0 \in \text{Ker } T \Rightarrow \text{Ker } T$ is invariant subspace of V. Also $w \in ImT \Rightarrow w = T(v) \Rightarrow Tw = T(Tv)$, $Tv \in V \Rightarrow Tw \in ImT$.

$\therefore$ ImT is an invariant subspace of V.

Example 12: Let $f(t)$ be any polynomial. Let $v \in \text{Ker } (f(T))$ then $f(T)\, v = 0$

Since $f(t)\ .\ t = tf(t)$

$f(T)T = Tf(T)$

Thus, $f(T)\ Tv = Tf(T)\ v = 0$

$\Rightarrow Tv \in \text{Ker } f(T)$

$\Rightarrow \text{Ker } f(T)$ is invariant under T.

Problem 37: *Let T be a linear operator on* $\mathbf{R}^2$, *the matrix of which in the standard ordered basis is*

$$A = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$$

Prove that the only subspaces of $\mathbf{R}^2$ *invariant under T are* $\mathbf{R}^2$ *and zero subspaces.*

Solution: Characteristic polynomial of A (or T) is $\begin{vmatrix} x-1 & 1 \\ -2 & x-2 \end{vmatrix} = x^2 - 3x + 4$, whose roots are not real. Thus eigen values of A (or T) do not exist in $\mathbf{R}$. If W is an invariant subspace of $\mathbf{R}^2$ s.t. $W \neq 0$, $\mathbf{R}$ then dim $W = 1$. Let W be spanned by v. Then $Tv \in W \Rightarrow Tv = \alpha v$, $v \neq 0$ $\Rightarrow \alpha$ is an eigen value of T ($\alpha \in \mathbf{R}$), a contradiction. Hence O and $\mathbf{R}^2$ are only invariant subspaces of $\mathbf{R}^2$.

Theorem 15: *Let W be an invariant subspace of linear operator T on V. Then T has a matrix representation* $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$, *where A is matrix of restriction* T_w *of T on W.*

Proof: Let $\{w_1, ..., w_r\}$ be a basis of W. Let $\beta = \{w_1, ..., w_r, v_1, ..., v_s\}$ be a basis of V, obtained by extending basis of W.

Since $T(w) \in W$ for all $w \in W$, we define $T_w : W \to W$ by $T_w(x) = T(x)$ for all $x \in W$.

Then T_w is operator in W.

$T_w(w_1) = T(w_1) = a_{11}w_1 + ... + a_{r1}w_r$

.....

$T_w(w_r) = T(w_r) = a_{1r}w_1 + ... + a_{rr}w_r$

$T(v_1) = b_{11}w_1 + ... + b_{r1}w_r + c_{11}v_1 + ... + c_{s1}v_s$

.....

$T(v_s) = b_{1s}w_1 + ... + b_{rs}w_r + c_{1s}v_1 + ... + c_{ss}v_s$

Thus matrix of T w.r.t. basis β is

$$\begin{bmatrix} a_{11} & \cdots & a_{1r} & b_{11} & \cdots & b_{1s} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ a_{r1} & \cdots & a_{rr} & b_{r1} & \cdots & b_{rs} \\ 0 & \cdots & 0 & c_{11} & \cdots & c_{1s} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & c_{s1} & \cdots & c_{ss} \end{bmatrix}$$

$$= \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \text{ where } A = (a_{ij}),\ B = (b_{ij}),\ C = (c_{ij})$$

are of order $r \times r$, $r \times s$, $s \times s$ respectively

Clearly, A is matrix of T_w w.r.t. $\{w_1, ..., w_r\}$ = basis of W. T_w is called restriction of T on W.

We now show that the matrix C obtained in theorem 15 is the matrix of some linear operator on $\frac{V}{W}$ induced by T.

Define $\hat{T} : \frac{V}{W} \to \frac{V}{W}$ s.t.,

$$\hat{T}(W + v) = W + T(v), \quad v \in V$$

Then $\hat{T}$ is well defined as $W + v = W + v'$

$\Rightarrow v - v' \in W$

$\Rightarrow T(v - v') \in W$

$\Rightarrow T(v) - T(v') \in W$

$\Rightarrow W + T(v) = W + T(v')$

Since T is linear transformation, so is $\hat{T}$. Let $\{w_1, ..., w_r\}$ be a basis of W.

Then it can be extended to form a basis of V. Let $\{w_1, ..., w_r, v_1, ..., v_s\}$ be a basis of V. Then $\{W + v_1, ..., W + v_s\}$ is a basis of $\frac{V}{W}$.

Now
$$\begin{aligned}\hat{T}(W + v_1) &= W + T(v_1)\\ &= W + b_{11}w_1 + ... + b_{r1}w_r + c_{11}v_1 + ... + c_{s1}v_s\\ &= W + c_{11}v_1 + ... + c_{s1}v_s\\ &\text{.....}\end{aligned}$$

$$\hat{T}(W + v_s) = W + T(v_s) = W + b_{1s}w_1 + ... + b_{rs}w_r + c_{1s}w_1 + ... + c_{ss}v_s.$$
$$= W + c_{1s}v_1 + ... + c_{ss}v_s \qquad \text{(as in theorem 15)}$$

$\therefore$ matrix of $\hat{T}$ w.r.t. basis $\{W + v_1, ..., W + v_s\}$ of $\frac{V}{W}$ is

$$\begin{bmatrix} c_{11} & \cdots & \cdots & c_{1s} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ c_{s1} & \cdots & \cdots & c_{ss} \end{bmatrix} = C$$

A special situation where $B = 0$ in theorem is obtained when V is a direct sum of two invariant subspaces under T.

Problem 38: *If W and U are invariant subspaces of a linear operator on a F.D.V.S. V over F and $V = U \oplus W$, then $\exists$ a basis β of V such that the matrix of T w.r.t. β is $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$, where A is the matrix of T_w on W and C is the matrix of T_u on U.*

Solution: Let $\{w_1, ..., w_r\}$ be a basis of W and $\{u_1, ..., u_s\}$ be a basis of U. Then $\{w_1, ..., w_r, u_1, ..., u_s\}$ is a basis of $W \oplus U = V$.

Now
$$T_w(w_1) = T(w_1) = a_{11}w_1 + ... + a_{r_1}w_r$$
$$T_w(w_2) = T(w_2) = a_{12}w_1 + ... + a_{r_2}w_2$$
$$\text{.....}$$
$$T_w(w_r) = T(w_r) = a_{1r}w_1 + ... + a_{rr}w_r$$

as $T(w_i) \in W$ for all $i = 1, ..., r$

Similarly,
$$T_u(u_1) = T(u_1) = c_{11}u_1 + ... + c_{s1}u_s$$
$$T_u(u_2) = T(u_2) = c_{12}u_1 + ... + c_{s2}u_s$$
$$\text{.....}$$

$$T_u(u_s) = T(u_s) = c_{1s}u_1 + \ldots + c_{ss}u_s$$

as $T(u_j) \in U$ for all $j = 1, \ldots, s$

So matrix of T w.r.t. $\beta = \{w_1, \ldots, w_r, u_1, \ldots, u_r\}$ of V is given by

$$\begin{bmatrix} a_{11} & \cdots & a_{1r} & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ a_{r1} & \cdots & a_{rr} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & c_{11} & \cdots & c_{1s} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & c_{s1} & \cdots & c_{ss} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$$

where $A = (a_{ij})$, $C = (c_{ij})$ are $r \times r$ and $s \times s$ matrices respectively. Clearly A is the matrix of T_w on W and C is the matrix of T_u on U.

Problem 39: *Let V be the vector space of all polynomials in x over F, of degree ≤ 5. Let T: $V \to V$ be defined by $T(1) = x^2 + x^4$, $T(x) = x + 1$, $T(x^2) = 1$, $T(x^3) = x^3 + x^2 + 1$, $T(x^4) = x^4$, $T(x^5) = 0$. If W is the linear span of $\{1, x^2, x^4\}$,*

(*a*) *Show that W is invariant under T.*

(*b*) *Find the matrix of T_w in a suitable basis of W.*

(*c*) *Find the matrix of $\hat{T}$ in a suitable basis of $\frac{V}{W}$.*

(*d*) *Find the matrix of T in a suitable basis of V.*

Solution (*a*): Let $w \in W$. Then $w = a + bx^2 + cx^4$ where $a, b, c \in F$.

$$\begin{aligned} T(w) &= a \,.\, T(1) + bt(x^2) + cT(x^4) \\ &= a(x^2 + x^4) + b + cx^4 \\ &= b + ax^2 + (a + c)\, x^4 \\ &\in W \text{ for all } w \in W \end{aligned}$$

$\therefore$ W is invariant under T.

(*b*): Notice that $\{1, x^2, x^4\}$ is linearly independent set over F and so forms a basis of W, and it can be extended to form a basis, namely $\{1, x^2, x^4, x, x^3, x^5\}$ of V.

Now
$$\begin{aligned} T_w(1) &= T(1) = x^2 + x^4 = 0 \,.\, 1 + 1 \,.\, x^2 + 1 \,.\, x^4 \\ T_w(x^2) &= T(x^2) = 1 = 1 \,.\, 1 + 0 \,.\, x^2 + 0 \,.\, x^4 \\ T_w(x^4) &= T(x^4) = x^4 = 0 \,.\, 1 + x^2 + 1 \,.\, x^4 \end{aligned}$$

$\therefore$ matrix of T_w w.r.t. basis $\{1, x^2, x^4\}$ of W is given by $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$.

(*c*): Now $\{W + x, W + x^3, W + x^5\}$ is basis of $\frac{V}{W}$.

$\therefore$
$$\begin{aligned} \hat{T}(W + x) &= W + T(x) = W + x + 1 \\ &= W + x = 1 \,.\, (W + x) + 0(W + x^3) + 0(W + x^5) \end{aligned}$$

$$\begin{aligned}\hat{T}(W + x^3) &= W + T(x^3)\\ &= W + x^3 + x^2 + 1\\ &= W + x^3\\ &= 0(W + x) + 1(W + x^3) + 0(W + x^5)\\ \hat{T}(W + x^5) &= W + T(x^5)\\ &= W + 0 = W = \text{zero of } \frac{V}{W}\\ &= 0(W + x) + 0(W + x^3) + 0(W + x^5)\end{aligned}$$

$\therefore$ matrix of $\hat{T}$ w.r.t. basis $\{W + x, W + x^3, W + x^5\}$ of $\frac{V}{W}$ is given by

$$C = \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix}$$

(*d*): $T(x) = x + 1 = 1 \,.\, 1 + 0 \,.\, x^2 + 0 \,.\, x^4 + 1 \,.\, x + 0 \,.\, x^3 + 0 \,.\, x^5$

$T(x^3) = x^3 + x^2 + 1 = 1 \,.\, 1 + 1 \,.\, x^2 + 0 \,.\, x^4 + 0 \,.\, x + 1 \,.\, x^3 + 0 \,.\, x^5$

$T(x^5) = 0 = 0 \,.\, 1 + 0 \,.\, x^2 + 0 \,.\, x^4 + 0 \,.\, x + 0 \,.\, x^3 + 0 \,.\, x^5$

$\therefore$ matrix of T w.r.t. basis $\{1, x^2, x^4, x, x^3, x^5\}$ of V is given by

$$\left[\begin{array}{cccccc}0 & 1 & 0 & 1 & 1 & 0\\ 1 & 0 & 0 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0 & 0\\ \hdots & \hdots & \hdots & \hdots & \hdots & \hdots\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\end{array}\right]$$

$$= \begin{bmatrix}A & B\\ 0 & C\end{bmatrix}, \text{ where } B = \begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix}.$$

Problem 40: *Let T be a linear operator on a F.D.V.S. V over F. Let W be an invariant subspace of T. Show that the characteristic polynomial $p_T(x)$ of T is given by*

$p_T(x) = p_{T_w}(x)\, p_{\hat{T}_w}(x)$, *where* $p_{T_w}(x)$, $p_{\hat{T}_w}(x)$ *are the characteristic polynomials of* T_w *and* $\hat{T}_w$ *respectively.*

Solution: Characteristic polynomial $p_T(x)$ of T is given by

$$\left|\begin{bmatrix}A & B\\ 0 & C\end{bmatrix} - xI\right|$$

$$= \left|\begin{bmatrix}A - xI & B\\ 0 & C - xI\end{bmatrix}\right| \quad \left(\begin{array}{c}\text{Here } A = \text{matrix of } T_w \text{ on } W\\ C = \text{matrix of } \hat{T} \text{ on } \frac{V}{W}\end{array}\right)$$

$$= |A - xI||C - xI|$$
$$= \text{(characteristic polynomial of } T_w\text{)}$$
$$\times \text{(characteristic polynomial of } \hat{T}\text{)}$$
$$= p_{T_w}(x)\ \ p_{\hat{T}}(w).$$

A natural question arises "what is the minimal polynomial for T in terms of minimal polynomial for T_w"? As we saw in above problem that the characteristic polynomial of T_w divides the characteristic polynomial of T, we have a similar result about minimal polynomial of T. We prove

Problem 41: *Let T be a linear operator on a finite dimensional vector space V. Let W be a T-invariant subspace of V. Suppose that* $v_1, v_2, \ldots, v_k$ *are eigen vectors of T corresponding to distinct eigen values. Prove that if* $v_1 + v_2 \ldots + v_k \in W$. *then* $v_i \in W_i$ *for all i.*

Solution: We prove the result by induction on k. For $k = 1$, the result is clearly true. Assume that the result is true for $k - 1$, $k > 1$.

Let $v_1 + v_2 \ldots + v_k \in W$

Then $T(v_1) + T(v_2) + \ldots + T(v_k) \in W$ as $T(W) \subseteq W$

$\therefore$ $\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k \in W$

Also $\lambda_k v_1 + \lambda_k v_2 + \ldots + \lambda_k v_k \in W$

$\therefore$ $(\lambda_1 - \lambda_k)v_1 + (\lambda_2 - \lambda_k)v_2 + \ldots + (\lambda_{k-1} - \lambda_k)v_{k-1} \in W$

By induction hypothesis,

$(\lambda_i - \lambda_k)v_i \in W_i$ for all i, = 1, 2, . . ., $k - 1$

$\therefore$ $v_i \in W_i$ for all i, = 1, 2, . . ., k

$\therefore$ $v_k \in W_i$

So, the result is true for k also.

Hence by induction the result is true for all integers $k > 0$.

Problem 42: *Prove that if T is a diagonalisable linear operator on a finite dimensional vector space V and W is a non-zero T-invariant subspace of V, then* T_w *is also diagonalisable.*

Solution: Since T is a diagonalisable, there exists an ordered basis $\beta = \{v_1, v_2, \ldots, v_k\}$ of V such that each v_i is an eigen vector of T. Let $T(v_i) = \lambda_i v_i$.

Let $V = \{w_1, w_2, \ldots, w_m\}$ be a basis of W.

Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be distinct eigen values of T.

Let $W_1, W_2, \ldots, W_k$ be the corresponding eigen spaces.

Then $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$

Let $\beta_1 = \{x_1, \ldots, x_{r_1}\}, \ldots, \beta_k = \{y_1, \ldots, y_{r_k}\}$ be basis of $W_1, \ldots, W_k$ respectively.

Then $w_1 = (\alpha_1 x_1 + \ldots + \alpha_{r_1} x_{r_1}) + \ldots + (\beta_1 y_1 + \ldots + \beta_{r_k} y_{r_k}) = z_1 + \ldots + z_k$,

where $z_1 = \alpha_1 x_1 + \ldots + \alpha_{r_1} x_{r_1}$

. . . .

$z_k = \beta_1 y_1 + \ldots + \beta_{r_k} y_{r_k}$

Now $z_1 + \ldots + z_k \in W$ and each z_i is an eigen vector of T.

By previous problem, $z_i \in W$ for all i = 1, 2, . . ., k.

In this way, let

$W_m = u_1 + \ldots + u_k$, where each u_i is an eigen vector of T. w.r.t. distinct eigen values of T.

$\therefore$ $\{z_1, z_2, \ldots, z_k, \ldots, u_1, \ldots, u_k\}$ span W.

$\therefore$ Some subset of it is a basis of W consisting of eigen vector of T_w.

$\therefore$ T_w is also diagonalisable.

Theorem 16: *The minimal polynomial of T_w divides the minimal polynomial for T, where W is an invariant subspace of V and T is a linear operator on V.*

Proof: Let $p(x)$ be the minimal polynomial for T.

Let $p(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1} + x^n$

Since $T(w) = T_w(w)$ for all $w \in W$

$T^2(w) = T(T_w(w))$

$= T_w(T_w(w))$ as $T_w(w) \in W$

In this way $T^r(w) = T_w^r(w)$ for all $w \in W$

$\therefore$ $p(T_w)(w) = p(T)(w)$ for all $w \in W$

$= 0$ as $p(T) = 0$ for all $w \in W$

$\therefore$ $p(T_w) = 0$

Let $q(x)$ be the minimal polynomial for T_w. Then $p(x) = q(x)\, r(x) + h(x)$ where $h(x) = 0$ or $\deg h(x) < \deg q(x)$.

$\therefore$ $0 = p(T_w) = q(T_w)\, r(T_w) + h(T_w)$

$\therefore$ $h(T_w) = 0$

If $h(x) \neq 0$, then $h(x)$ is non zero polynomial satisfied by T_w of degree less than $\deg q(x)$, a contradiction as $q(x)$ is minimal.

$\therefore$ $h(x) = 0 \Rightarrow q(x)$ divides $p(x)$.

Definition: A linear operator T on a *F.D.V.S.* $V(F)$ is said to be *triangulable* or *triangularizable* over F if there exists an ordered basis β of V such that $[T]_\beta$ is triangular.

Theorem 17: *Let T be a linear operator on a F.D.V.S. V(F). Then T is triangulable if and only if the characteristic polynomial for T is a product* (*not necessarily distinct*) *of linear factors on F*[*x*]. (*Equivalently, T is triangulable if and only if the eigen values of T are all in F*).

Proof: Let the characteristic polynomial of T be product of linear factors in $F[x]$.

Let $c_1, c_2, \ldots, c_n$ be eigen values of T in F.

We use induction on n.

If $n = 1$, then the result is obvious as 1×1 matrix is always triangular.

Let $n > 1$. Assume that the result is true for all vector spaces over F of dimension less than n.

Let dim $V = n$. Let v_1 be an eigen vector of T w.r.t. c_1, then $T(v_1) = c_1 v_1$

Let $W = \langle v_1 \rangle$.

Then W is T-invariant subspace of V. Consider $\frac{V}{W}$. $\dim \frac{V}{W} = n - 1$

Then $\hat{T} : \frac{V}{W} \to \frac{V}{w}$ s.t.,

$\hat{T}(W + v) = W + T(v)$

is well defined linear operator on $\frac{V}{W}$. Let $f(x)$ be the characteristic polynomial for T and $g(x)$ be the characteristic polynomial for $\hat{T}$. Then $g(x)$ divides $f(x)$ by problem 40.

So, $g(x)$ is also product of linear factors in $F[x]$.

By induction hypothesis $\exists$ a basis $\bar{\beta} = \{W + v_2, ..., W + v_n\}$ of $\frac{V}{W}$ such that

$$\left[\hat{T}\right]_{\bar{\beta}} = \begin{bmatrix} a_{22} & \cdots & \cdots & a_{2n} \\ 0 & \ddots & & \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & a_{nn} \end{bmatrix}, \; a_{ij} \in F$$

$$\therefore \quad \hat{T}(W + v_j) = a_{2j}(W + v_2) + ... + a_{nj}(W + v_n)$$

$$\Rightarrow W + T(v_j) = a_{2j}(W + v_2) + ... + a_{nj}(W + v_n)$$

$$= W + a_{2j} v_2 + ... + a_{nj} v_n$$

$$\Rightarrow T(v_j) = a_{2j} v_2 + ... + a_{nj} v_n + a_{1j} v_1 \quad , \quad a_{1j} \in F$$

Now $\beta = \{v_1, v_2, ..., v_n\}$ is a basis of V

$$\therefore \quad [T]_\beta = \begin{bmatrix} a_{11} & a_{12} & a_{1n} \\ \vdots & a_{22} & a_{2n} \\ \vdots & \vdots & \vdots \\ 0 & 0 & a_{nn} \end{bmatrix}, \text{ where } a_{11} = c_1$$

which is triangular matrix and so T is triangulable. So, result follows by induction.

Conversely, if T is triangulable then $\exists$ a basis β of V such that $[T]_\beta = A$ is triangular and eigen values of T are diagonal entries in A.

$\therefore$ Characteristic polynomial for A or T is product of linear factors in $F[x]$.

Remark: We thus realise that T is triangulable if and only if minimal polynomial for T is product of linear factors in $F[x]$.

Cor.: If A is $n \times n$ matrix over the field of complex numbers, then A is triangulable.

Proof: By fundamental theorem of algebra (*i.e.* Every polynomial over the field **C** of complex numbers has all roots in **C**), the minimal polynomial $p(x)$ of A has the form $p(x) = (x - c_1)^{r1} ... (x - c_k)^{rk}$, where $c_i \in \mathbf{C}$. By above theorem A is triangulable.

Problem 43: *Let T be a linear operator on a finite dimensional vector space V(F). Suppose all eigen values of T are in F. Show that every non zero. T-invariant subspace of V contains*

an eigen vector of T.

Solution: Let W be a non zero T-invariant subspace of V. Then the restriction T_w of T on W is a linear operator on W. Since the characteristic polynomial of T_w divides the characteristic polynomial of T, eigen values of T_w also belong to F. Let $c \in F$ be an eigen value of T_w. Then $\exists\ 0 \neq x \in W$ such that $T_w(x) = cx \Rightarrow T(x) = cx \Rightarrow x$ is also an eigen vector of T.

Problem 44: *Let T be a linear operator on V. If every subspace of V is invariant under T, show that T is a scalar multiple of the identity operator.*

Solution: Let $0 \neq v \in$ V. Let W be a subspace of V spanned by V. Since W is invariant under T, $v \in W \Rightarrow T(v) \in W \Rightarrow T(v) = \alpha v$. $w \in W \Rightarrow w = av \Rightarrow T(w) = aT(v) = a\alpha v = \alpha av = \alpha w$. Let $v' \notin W, v' \in V$. Then, v, v' are linearly independent. Let W' be the subspace spanned by v'. Since W' is invariant under T, $T(v') \in W'$.

$\therefore\ T(v') = \alpha' v'$. Let V' be the subspace spanned by $v - v'$. Then as before $T(v - v') = \beta(v - v')$

$\Rightarrow T(v) - T(v') = \beta v - \beta v' \Rightarrow \alpha v - \alpha' v' = \beta v - \beta v'$

$\Rightarrow (\alpha - \beta)v = (\alpha' - \beta)v' \Rightarrow \alpha = \beta = \alpha'$ as v, v' are linearly independent

$\Rightarrow T(v') = \alpha(v')$.

$\therefore$ for all $v \in V$, $T(v) = \alpha v$

$\Rightarrow T = \alpha I$.

Problem 45: *Let T be a linear operator on* $\mathbf{R}^3$ *which is represented in the standard ordered basis by the matrix* $\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$

Let $W = \text{Ker}\ (T - 2I)$. *Prove that W has no complementary T-invariant subspace.*

Solution: Now $w \in W$ implies that $(T - 2I)\ (w) = 0$

So, $T(w) = 2w$. Let $w = (x, y, z)$

Then $\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 2 \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

Therefore, $x + 2y = 2y, 3z = 2z$.

So, $x = 0 = z$ and $w = (0, y, 0)$

Therefore, $W = <(0, 1, 0)> = <\in_2>$

Suppose $V = W \oplus W'$, $T(W') \subseteq W'$

Let $T' = T - 2I$. Let $v \in N(T') \cap R(T')$

Therefore, $T'(v) = 0$, $v = T'(y) = (T - 2I)(w + w')$, $w \in W$, $w' \in W'$

$= (T - 2I)(w') \in W'$

Also $T'(v) = 0$ means that $v \in N(T') = W$

So, $v \in W \cap W' = \{0\}$.

Therefore, $v = 0$ means that $N(T') \cap R(T') = \{0\}$

Now $(T - 2I)(\in_1) = T(\in_1) - 2\in_1 = 2\in_1 + \in_2 - 2\in_1 = \in_2 \in W = N(T')$

Also $(T - 2I)(\in_1) = T'(\in_1) \in R(T')$

By above, $(T - 2I)(\in_1) \in N(T') \cap R(T') = \{0\}$

So, $\in_2 = 0$, a contradiction.

Thus, W has no complementary T-invariant subspace.

Problem 46: *Let T be a linear operator on a finite dimensional vector space V. Prove that there exists an integer $k > 0$ such that*

$$V = R(T^k) \oplus N(T^k)$$

Solution: Now $V \supseteq R(T) \supseteq R(T^2) \supseteq \ldots$, is a descending chain of subspaces of V.

Since V is finite dimensional, there exists an integer $k > 0$ such that $R(T^k) = N(T^{k+1})$

Since $\dim V = \dim R(T^k) + \dim N(T^k)$

$= \dim R(T^{k+1}) + \dim N(T^{k+1})$

$\dim N(T^k) = \dim N(T^{k+1})$

So, $N(T^k) = N(T^{k+1}) = \ldots$

Now $x \in R(T^k) \cap N(T^k)$

$\Rightarrow T^k(x) = 0, x = T^k(v)$

$\Rightarrow T^{2k}(v) = 0 \Rightarrow v \in N(T^{2k}) = N(T^k)$

$\Rightarrow T^k(v) = 0 \Rightarrow x = 0$

So $R(T^k) \cap N(T^k) = \{0\}$.

Problem 47: *Let T be a linear operator on a finite dimensional vector space and let R be the range of T. Prove that R has a complementary T-invariant subspace if and only if R is independent of the null space of T.*

Solution: Suppose that R has a complementary T-invariant subspace W.

Therefore, $V = R \oplus W$, $T(w) \subseteq W$.

Let $x \in R \cap N$.

Then $x = T(y)$, $T(x) = 0$

Now $y \in V$ means that $y = r + w$, $r \in R$, $w \in W$

So, $x = T(y) = T(r) + T(w) = T(r) + w'$, $w' = T(w) \in W$

Therefore, $w' = x - T(r) \in R$.

So, $w' \in R \cap W = \{0\}$ means that

$w' = 0$ and therefore, $x = T(r)$, $r \in R$.

In this way, $x = T^k(r_1) \in R(T^k)$

Also $x \in N(T)$ means that $x \in N(T^k)$

Therefore, $x \in R(T^k) \cap N(T^k) = \{0\}$

So, $x = 0$ which means that $R \cap N = \{0\}$.

Thus, R is independent of N.

Conversely, Let R be independent of N.

Then $R \cap N = \{0\}$

Since $\dim (N + R) = \dim N + \dim R - \dim (R \cap N)$,

$= \dim N + \dim R = \dim V$

Therefore, $V = R \oplus N$

But $T(N) \subseteq N$

Thus, R has a complementary T-invariant subspace N.

Problem 48: *If T is a linear operator on a finite dimensional vector space V and R, N are independent subspaces of V, then prove that N is the unique T-invairant subspace complementary to R.*

Solution: By above problem, $V = R \oplus N$, $T(N) \subseteq N$

Suppose $V = R \oplus W$, $T(W) \subseteq W$

We show that $W = N$

Now $\dim N = \dim W$.

Let $w \in W$.

Therefore $T(w) \in R \cap W = \{0\}$

which means that $T(w) = 0$.

So, $w \in N$.

Therefore, $W \subseteq N$ and $\dim W = \dim N$.

Hence $W = N$.

Problem 49: *Let T be a linear operator on a finite dimensional vector space over the field of complex numbers. Prove that T is diagonalisable, if and only if T is annihilated by some polynomial over* **C** *which has distinct roots.*

Solution: Suppose T is a diagonalisable. Let $p(x)$ be the minimal polynomial for T. By theorem 10, $p(x)$ has distinct roots and $p(T) = 0$.

Conversely, let $q(x)$ be a polynomial over **C** s.t. $q(T) = 0$ and roots of $q(x)$ are distinct.

$\therefore$ $p(x)$ divides $q(x)$

and thus roots of $p(x)$ are distinct.

By theorem 10 then T is diagonalisable.

Problem 50: *If A is nilpotent, show that A is similar to a triangular matrix whose entries on the diagonal are all zero.*

Solution: A is nilpotent $\Rightarrow A^m = 0 \Rightarrow$ the minimal polynomial $p(x)$ of A is x^r, $r \leq m$. So, 0 is only eigen value of A. Since $0 \in F$, by theorem 17, A is similar to a triangular matrix B.

$\therefore A = P^{-1}BP$

Since eigen value of A is only 0, eigen value of B is only 0 and these are diagonal entries on B.

Cyclic Subspaces

Let T be a linear operator on a vector space V. Let $0 \neq v \in V$.

The subspace W spanned by $\{v, T(v), T^2(v), \ldots\}$ is called the T-cyclic subspace of V generated by v. It is denoted by $W = Z(v, T)$. If $W = V = Z(v, T)$, then v is called a cyclic vector for T.

Let $w \in W$. Then $w = \alpha_i T^i(v) + \alpha_j T^j(v) + \ldots + \alpha_k T^k(v)$

$\therefore$ $T(w) = \alpha_i T^{i+1}(v) + \alpha_j T^{j+1}(v) + \ldots + \alpha_k T^{k+1}(v) \in W$.

So, W is a T-invariant subspace of V.

Let W' be a T-invariant subspace of V containing $v \in V$.

We show that $W \subseteq W'$.

Since $T(W') \subseteq W'$ and $v \in W'$, $T(v) \in W'$. So, $T^r(v) \in W'$ for all integers $r > 0$.

Let $w \in W$. Then $w = \alpha_i T^i(v) + \alpha_j T^j(v) + \ldots + \alpha_k T^k(v)$

$\therefore$ $w \in W'$ as $T^r(v) \in W'$ for all integers $r > 0$.

So, $W \subseteq W'$.

Thus, T-cyclic subspace generated by v is the smallest T-invariant subspace of V containing v.

Problem 51: *Let T: $\mathbf{R}^4 \to \mathbf{R}^4$ be the linear operator defined by $T(a, b, c, d) = (a + b, b - c, a + c, a + d)$. Find an ordered basis for the T-cyclic subspace generated by $\in_1 = (1, 0, 0, 0)$.*

Solution: Now $T(\in_1) = (1, 0, 1, 1)$, $T^2(\in_1) = (1, -1, 2, 2)$, $T^3(\in_1) = (0, -3, 3, 3)$

$= -3T(\in_1) + 3T^2(\in_1)$

$\therefore$ $W = T$-cyclic subspace generated by $\in_1$

$= \langle \in_1, T(\in_1), T^2(\in_1) \rangle$

$= \langle (1, 0, 0, 0), (1, 0, 1, 1), (1, -1, 2, 2) \rangle$

Since these 3 vectors (1, 0, 0, 0), (1, 0, 1, 1), (1, −1, 2, 2) are linearly independent, $\{(1, 0, 0, 0), (1, 0, 1, 1), (1, -1, 2, 2)\}$ is an ordered basis for W.

Problem 52: *Let T be a linear operator on a two-dimensional vector space V. Prove that either V is a T-cyclic subspace of itself or $T = cI$ for some scalar c.*

Solution: If every non-zero vector in V is an eigen vector of T, then $T = cI$ for some scalar c (See Problem 2 on page 589).

Let $0 \neq v \in V$ be not an eigen vector of T.

Let $W = \langle v \rangle$. Let $T(v) = v'$. Then $v' \notin W$ as v is not an eigen vector of T.

Let $W' = \langle v' \rangle$.

Then $W \cap W' = \{0\}$ and $V = W \oplus W'$.

Let $u \in V$.

Then $u = cv + dv'$.

$\therefore$ $(dT + cI)(v) = dT(v) + cv = dv' + cv = u$.

$\therefore$ $u = dT(v) + cv \in Z(v, T)$.

So $V \subseteq Z(v, T) \subseteq V$.

$\therefore$ $V = Z(v, T)$. Thus V is a T-cyclic subspaces of itself.

Problem 53: *Let T be a linear operator on V. Let v be a non zero vector in V and W = Z(v, T). Let w ∈ V. Then prove that w ∈ W if and only if w = g(T)v (for some polynomial g(x)). If dim W = m, show that* $W = \langle v, T(v), \ldots, T^{m-1}(v)\rangle$.

Solution: Let $w \in W$. Then $w = \alpha_i T^i(v) + \alpha_j T^j(v) + \ldots + \alpha_k T^k(v)$.

Then $w = (\alpha_i T^i + \alpha_j T^j + \ldots + \alpha_k T^k)(v) = g(T)v$, where $g(x) = \alpha_i x^i + \alpha_j x^j + \ldots + \alpha_k x^k$

Conversely, let $w = g(T)v$, $g(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_r x^r$

Then $w = (\alpha_0 I + \alpha_1 T + \ldots + \alpha_r T^r)(v)$

$= \alpha_0 v + \alpha_1 T(v) + \ldots + \alpha_r T^r(v) \in z(v, T) = W$

$\therefore$ $w \in W$.

Let $\dim W = m$.

Then any $m + 1$ vectors in W are linearly dependent.

Now, $v, T(v), \ldots, T^m(v)$ are in $W = Z(v, T)$.

$\therefore$ there exist scalars $\alpha_0, \alpha_1, \ldots, \alpha_m$

such that $\alpha_0 v + \alpha_1 T(v) + \ldots + \alpha_m T^m(v) = 0$, some $\alpha_i \neq 0$

If $\alpha_m \neq 0$, then $T^m(v)$ is a linear combination of vectors $v, T(v), \ldots, T^{m-1}(v)$.

$\therefore$ w in W means that w is a linear combination of vectors $v, T(v), \ldots, T^{m-1}(v)$.

If $\alpha_m = 0$, then $\alpha_0 v + \alpha_1 T(v) + \ldots + \alpha_{m-1} T^{m-1}(v) = 0$, some $\alpha_i \neq 0$

Again w in W is a linear combination of vectors $v, T(v), \ldots, T^{m-1}(v)$.

So, $W = \langle v, T(v), \ldots, T^{m-1}(v)\rangle$

By above problem, if $W = Z(v, T)$, then any vector w in W can be written as $w = g(T)v$, for some polynomial $g(x)$ such that either $g(x) = 0$ or $\deg g(x) < \dim W$.

Problem 54: *Let T be a linear operator on* $\mathbf{R}^3$ *which is represented in the standard orderd basis by the matrix* $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}$. *Prove that T has no cyclic vector. What is Z(v, T), v =* $(1, -1, 3)$?.

Solution: Suppose (a, b, c) is a cyclic vector.

Then $\mathbf{R}^3 = Z((a, b, c), T)$

By definition of T, $T(\in_1) = 2\in_1$, $T(\in_2) = 2\in_2$, $T(\in_3) = -\in_3$

$\therefore$ $T(a, b, c) = a2\in_1 + b2\in_2 - c\in_3$

$= (2a, 2b, -c)$

$T^2(a, b, c) = (2^2a, 2^2b, c)$

Now $(0, 1, 0) = g(T)(a, b, c)$

$= (\alpha_2T^2 + \alpha_1T + \alpha_0I)(a, b, c)$

$= (\alpha_2 2^2a + \alpha_1 2a + \alpha_0a, \alpha_2.2^2b + \alpha_1 2b + \alpha_0b, \ldots)$

$\therefore$ $a(2^2\alpha_2 + 2\alpha_1 + \alpha_0) = 0$

$b(2^2\alpha_2 + 2\alpha_1 + \alpha_0) = 1$

So, $a = 0$

$\therefore$ $(1, 0, 0) = (\beta_2T^2 + \beta_1T + \beta_0I)(0, b, c)$

$= \beta_2T^2(0, b, c) + \beta_1T(0, b, c) + \beta_0(0, b, c)$

$= (0, -, -)$ a contradiction.

Thus, T has no cyclic vector.

Now $Z((1, -1, 3), T) = W$

$= \{g(T)\ (1, -1, 3) \mid g(x) \in \mathbf{R}[x], \deg g(x) < 3\}$

$= \{(\alpha_2T^2 + \alpha_1T + \alpha_0I)(1, -1, 3) \mid \alpha_i \in \mathbf{R}\}$

$= \{\alpha_2(4, -4, 3) + \alpha_1(2, -2, -3) + \alpha_0(1, -1, 3) \mid \alpha_i \in \mathbf{R}\}$

$= \{(4\alpha_2 + 2\alpha_1 + \alpha_0, -4\alpha_2 - 2\alpha_1 - \alpha_0, 3\alpha_2 - 3\alpha_1 + 3\alpha_0) \mid \alpha_i \in \mathbf{R}\}$

$= \langle(4, -4, 3), (2, -2, -3), (1, -1, 3)\rangle$

But $(4, -4, 3) = 1(2, -2, -3) + 2(1, -1, 3)$

$\therefore$ $W = \langle(2, -2, -3), (1, -1, 3)\rangle$

Also $\{(2, -2, -3), (1, -1, 3)\}$ is a linearly independent set

$\therefore$ $\dim W = 2$.

Problem 55: *Prove that if T^2 has a cyclic vector, then T also has a cyclic vector. Is the converse true?*

Solution: Let $V = Z(v, T^2)$.

Then $u \in V$ means that $u = \alpha_0v + \alpha_2T^2(v) + \ldots + \alpha_{2m}T^{2m}(v) \in Z(v, T)$

$\therefore$ $V \subseteq Z(v, T) \subseteq V$

So, $V = Z(v, T)$.

Thus v is also a cyclic vector of T.

The converse need not be true.

For, let T be the linear operator on $\mathbf{R}^2$ defined by $T(\in_1) = \in_2$, $T(\in_2) = 0$.

Then $T^2(\in_1) = 0 = T^2(\in_2)$. So, $T^2 = 0$

$\therefore$ $z(v, T^2) = \{0\} \neq \mathbf{R}^2$ for any v in V.

So, T^2 has no cyclic vector.

Let $(a, b) \in \mathbf{R}^2$

Then, $(a, b) = a\in_1 + b\in_2$

$= (a + bT)(\in_1)$

Thus $\mathbf{R}^2 = z(\in_1, T)$

So, T has a cyclic vector $\in_1$.

Problem 56: *Let T be the linear operator on* $\mathbf{R}^2$ *which is represented in the standard basis by the matrix* $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. *Show that* (0, 1) *is not a cyclic vector for T.*

Solution: By definition $T(\in_1) = \in_2$, $T(\in_2) = 0$.

If (0, 1) is a cyclic vector for T,

then $(1, 0) = g(T)\ (0, 1)$

$= (a + bT)\ (0, 1)$

$= (a + bT)\ (\in_2)$

$= a\in_2 = (0, a)$, a contradiction.

So, (0, 1) is not a cyclic vector for T.

Theorem 18: *If V is T-cyclic subspace of dimension n then the characteristic polynomial for T is same as the minimal polynomial for T.*

Proof: Let $V = Z(v, T)$. dim $V = n$.

Then $\beta = \{v, T(v), \ldots, T^{n-1}(v)\}$ spans V.

Since dim $V = n$, β is a basis for V.

Let $g(x) = a_0 + a_1x + \ldots + a_kx^k$ be such that

deg $g(x) = k < n$. Then $a_k \neq 0$

$\therefore$ $g(T)v = (a_0I + a_1T + \ldots + a_kT^k)\ (v)$

$= a_0v + a_1T(v) + \ldots + a_kT^k(v)$

$\neq 0$ (as $g(T)v = 0$ means that $a_k = 0$, a contradiction)

$\therefore$ $g(T) \neq 0$

$\therefore$ T does not satisfy any polynomial of degree less than n.

But T satisfies its characteristic polynomial.

$\therefore$ Minimial polynomial for T is same as the characteristic polynomial for T.

Problem 57: *Using above result, show that the characteristic polynomial for the differential operator D on the vector space V of all polynomials over* $\mathbf{R}$ *of degree less than* 3 *is equal to the minimal polynomial for T.*

Solution: $\beta = \{1, x, x^2\}$ is a basis of V and $[D]_\beta = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = A$. The characteristic polynomial for D is $|xI - A| = x^3$.

Now $V = Z(x^2, T)$ as $\alpha_0 + \alpha_1 x + \alpha_2 x^2 = (\alpha_2 + \frac{\alpha_1}{2} T + \frac{\alpha_0}{2} T^2)(x^2)$

By above theorem, the minimial polynomial for T is also x^3.

One important application of cyclic subspaces is a well known result [Cayley-Hamilton theorem] that we have already stated earlier on page 602.

Theorem 19: *Let T be a linear operator on a finite dimensional vector space V. Let f(x) be the characteristic polynomial for T. Then f(T) = 0.*

Proof: Let $0 \neq v \in V$. Let W be the T-cyclic subspace generated by v. Let dim $W = k$.

Let $\beta = \{v, T(v),. . .,T^{k-1}(v)\}$ be a basis of W.

Then there exist scalars $\alpha_0, \alpha_1, . . .,\alpha_k$ such that

$$\alpha_0 v + \alpha_1 T(v)+. . .+ \alpha_k T^k(v) = 0, \text{ some } \alpha_i \neq 0$$

If $\alpha_k = 0$, then $\alpha_i = 0$ for all i. So, $\alpha_k \neq 0$

$$\therefore \quad \left(\alpha_k^{-1}\alpha_0\right)v + \left(\alpha_k^{-1}\alpha_1\right)T(v) + \cdots + \left(\alpha_k^{-1}\alpha_{k-1}\right)T^{k-1}(v) + T^k(v) = 0$$

$$\therefore \quad a_0 v + a_1 T(v)+. . .+ a_{k-1} T^{k-1}(v) + T^k(v) = 0$$

Now $T_w(v) = T(v) = 0v + 1T(v)+. . .+0T^{k-1}(v)$

$T_w(T(v)) = T^2(v) = 0v + 0T(v)+1T^2(v)+. . .+0T^{k-1}(v)$

. . .

$T_w(T^{k-1}(v)) = T^k(v) = -a_0 v - a_1 v\ T(v)+. . .+(-a_{k-1})T^{k-1}(v)$

$\therefore$ The matrix of T_w with respect to basis β is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{pmatrix} = [T_W]_\beta = A$$

Then the characteristic polynomial of T_w is

$$g(x) = a_0 + a_1 x+ . . .+a_{k-1}x^{k-1} + x^k$$

(Use induction on k and expanding the determinant $|xI - A|$ along the first row to get $g(x)$)

Then $g(T)(v) = a_0 v + a_1 T(v)+ . . .+a_{k-1} T^{k-1}(v) + T^k(v) = 0$

Since the characteristic polynomial $g(x)$ of T_w divides the characteristic polynomial $f(x)$ of T,

$$f(x) = g(x)h(x) = h(x)g(x)$$

$\therefore$ $f(T)v = h(T)g(T)v = 0$ for all $v \neq 0$ in V.

Also $f(T)0 = 0$

$\therefore$ $f(T) = 0$

Cor: Let A be an $n \times n$ matrix over F and let $f(x)$ be the characteristic polynomial for A. Then $f(A) = 0$ = zero matrix.

Proof: Let T be the linear operator on F^n such the matrix of T with respect to the standard ordered basis β of F^n is A.

So, $A = [T]_\beta$.

Let $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$

Then $O = f(T) = a_0I + a_1T + \ldots + a_{n-1}T^{n-1} + T^n$

$\therefore$ $$\begin{aligned} O &= [a_0I + a_1T + \ldots + a_{n-1}T^{n-1} + T^n]_\beta \\ &= a_0[I]_\beta + a_1[T]_\beta + \ldots + a_{n-1}[T^{n-1}]_\beta + [T^n]_\beta \\ &= a_0I + a_1A + \ldots + a_{n-1}A^{n-1} + A^n \\ &= f(A) \end{aligned}$$

Note: The matrix $[T_W]_\beta$ in above theorem is also called the *companion matrix* of the polynomial $g(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1} + x^k$.

Definition: Let T be a linear operator on a finite dimensional vector space $V(F)$. Let $0 \neq v$ be in V.

Let $W = Z(v, T)$, dim $W = m$.

Let $\beta = \{v, T(v), \ldots, T^{m-1}(v)\}$ be a basis for W.

Then $T^m(v)$ is in W as W is T-invariant.

$\therefore$ $T^m(v)$ can be uniquely expressed as

$$T^m(v) = c_0v + c_1T(v) + \ldots + c_{m-1}T^{m-1}(v)$$

or $$(-c_0)v + (-c_1)T(v) + \ldots + (-c_{m-1})T^{m-1}(v) + T^m(v) = 0.$$

or $$a_0v + a_1T(v) + \ldots + a_{m-1}T^{m-1}(v) + T^m(v) = 0.$$

Then a_i's are uniquely determined for each non zero vector v in V.

Let $f_v(x) = a_0 + a_1x + \ldots + a_{m-1}x^{m-1} + x^m$

Then $f_v(T)v = 0$

$f_v(x)$ is called the *T-annihilator* of v or the *T-annihilator* of $Z(v, T)$.

We observe the following:

(*i*) Let T be a linear operator on V. Let $0 \neq v$ be in V. Then the T-annihilator of v is uniquely determined.

(*ii*) The degree of the T-annihilator of v = dimension of $Z(v, T)$

(*iii*) If $W = Z(v, T)$, then the T-annihilator of v is the characteristic polynomial of T_w.

(*iv*) The minimial polynomial of T_w is same as the T-annihilator of v for if

$p(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1} + x^k$ be the minimal polynomial for T_w, $k < m$ = dim W.

Then $0 = p(T_w)$ means that

$$\left(a_oI + a_1T_w + \cdots a_{k-1}T_w^{k-1} + T_w^k\right)v = 0$$

So, $a_0v + a_1T(v) + \ldots + a_{k-1}T^{k-1}(v) + T^k(v) = 0$, $k < m$ means that 1 = 0, a contradiction,

$\therefore$ $k = m$

Thus, degree of the minimial polynomial of T_w = dimension of W = degree of the characterstic polynomial of T_w.

Hence the minimal polynomial of T_w

= The characteristic polynomial of T_w

= The T-annihilator of v.

Problem 58: *If* T: $\mathbf{R}^3 \to \mathbf{R}^3$ *is represented by*

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

with respect to the standard basis, find the T-annihilator of $\in_1 = (1, 0, 0)$.

Solution: $T(\in_1) = \in_2$, $T(\in_2) = \in_3$, $T(\in_3) = 0$.

$W = Z(\in_1, T)$

$= \{\alpha_2 T^2(\in_1) + \alpha_1 T(\in_1) + \alpha_0 \in_1 | \ \alpha_i \in \mathbf{R}\}$

$= \{\alpha_0 \in_1 + \alpha_1 \in_2 + \alpha_2 \in_3 | \ \alpha_i \in \mathbf{R}\}$

$= \mathbf{R}^3$

The characteristic polynomial of $T_w = T|W$

= The characteristic polynomial of T

$= x^3$

$\therefore$ The T-annihilator of $\in_1$ is x^3

Problem 59: *Let T be the linear operator on* $\mathbf{R}^3$ *such that its matrix with respect to the standard basis is*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Determine the T-annihilator of (1, 1, 0)

Solution: $W = Z((1, 1, 0), T)$

$= \{(\alpha_2 T^2 + \alpha_1 T + \alpha_0)(1, 1, 0) \mid \alpha_i \in \mathbf{R}\}$

$= \{(\alpha_2 T^2 + \alpha_1 T + \alpha_0)(\in_1 + \in_2) \mid \alpha_i \in \mathbf{R}\}$

$= \langle \in_1 + \in_2 \rangle$.

Here $T(\in_1) = \in_1$

$T(\in_2) = \in_2$

$T(\in_3) = -\in_3$

dim $W = 1$

Let $v = (1, 1, 0) = \in_1 + \in_2$

Then $\{v\}$ is a basis of W.

$T_w(v) = T(v) = v$

$\therefore [T_w] = I$

$\therefore$ The characteristic polynomial of T_w is $(x-1)^2$

$\therefore$ The T-annihilator of T_w is $(x-1)^2$

Problem 60: *Let T be* a *linear operator on an n-dimensional vector space V. Suppose that T is diagonalisable.*

(*a*) *If T has a cyclic vector, show that T has n distinct eigen values.*

(*b*) *If T has n distinct eigen values and* $\{v_1, v_2, \ldots, v_n\}$ *is a basis of eigen vectors of T,* show that $v = v_1 + v_2 + \ldots + v_n$ is a cyclic vector of T.

Solution: (*a*) Since T has a cyclic vector.

$V = Z(v, T)$ for some v in V.

$\therefore$ $f(x)$ = The characteristic polynomial of T.

= The minimal polynomial of $T = p(x)$

Since T is diagonalisable, $p(x)$ is product of distinct linear factors.

Since deg $f(x) = n$, deg $p(x) = n$.

T has n distinct eigen values.

(*b*) Let $T(v_1) = c_1v_1$, $T(v_2) = c_2v_2, \ldots, T(v_n) = c_nv_n$

where c_i's are distinct eigen values of T.

Let $v = v_1 + v_2 + \ldots + v_n$

Let $S = \{v_1 + v_2 + \ldots + v_n,\ c_1v_1 + \ldots + c_nv_n, \ldots c_1^{n-1}v_1 + \ldots + c_n^{n-1}v_n\}$ then S is a linearly independent set as $c_1, c_2, \ldots c_n$ are distinct.

$\therefore$ S forms a basis of V.

In fact $S = \{v, T(v), \ldots, T^{n-1}(v)\}$

Let $u \in V$

Then $u = a_0v + a_1T(v) + \ldots + a_{n-1}T^{n-1}(v)$

$= (a_0 + a_1T + \ldots + a_{n-1}T^{n-1})(v)$

$= g(T)v$, $g(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$

$\therefore$ v is a cyclic vector of T.

Problem 61: *Let T be a linear operator on a finite dimensional vector space V. Show that T has a cyclic vector if and only if there exists an ordered basis* β *for V such that* $[T]_\beta$ *is the companion matrix of the minimal polynomial for T.*

Solution: Suppose T has a cyclic vector v.

Then $V = Z(v, T)$

Let dim $V = n$

Then v, $T(v)$, . . .,$T^n(v)$ are linearly dependent vectors and as before there exist scalars a_0, a_1,. . .,a_{n-1} on such that

$$a_0 v + a_1 T(v) + \ldots + a_{n-1} T^{n-1}(v) + T^n(v) = 0$$

Let $u \in V$. Then $u = g(T)v$, $g(x) = 0$ or deg $g(x) < n$

$$= (\alpha_0 + \alpha_1 T + \ldots + \alpha_k T^k)(v)$$

$\therefore$ $\beta = \{v, T(v),\ldots,T^{n-1}v\}$ spans V and so forms a basis of V. Then

$$[T]_\beta = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

is companion matrix of T-annihilator

$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ of v

= minimial polynomial for T.

Conversely, let there exist an ordered basis $\beta = \{v_1, v_2,\ldots v_n\}$ for V such that $[T]_\beta$ is the companion matrix of the minimal polynomial for T. Then v_1 is clearly a cyclic vector for T.

Projections

We recall, by a projection E of a vector space V, we mean a linear operator on V s.t., $E^2 = E$.

Let now E be a projection on V, then $E : V \to V$.

We show $V = R \oplus N$, where R = range of E and

N = Null space of E = Ker E.

Let $v \in V$ be any element, then

$$E^2 = E$$

$$\Rightarrow E^2(v) = E(v)$$

$$\Rightarrow E(v - E(v)) = 0$$

$$\Rightarrow v - E(v) \in \text{Ker } E = N$$

Thus $v = E(v) + (v - E(v)) \in R + N$

i.e., $V = R + N$

Again, let $x \in R \cap N$ then $x \in R$ and $x \in N$

$x \in R \Rightarrow \exists\, y \in V$ s.t., $E(y) = x$

$x \in N \Rightarrow E(x) = 0$

So $E^2(y) = E\,E(y) = E(x) = 0$

$\Rightarrow E(y) = 0 \Rightarrow x = 0 \Rightarrow R \cap N = \{0\}$

Hence $V = R \oplus N$.

Suppose now $V = A \oplus B$, where A, B are subspaces of V.

Define $E : V \to V$, s.t.,

$E(v) = a$

where $v \in V \Rightarrow v = a + b$ (uniquely) $a \in A$, $b \in B$

Then E is easily seen to be a linear operator

Also $E^2(v) = EE(v) = E(a) = E(a + 0) = a = E(v) \quad \forall\ v \in V$

shows that $E^2 = E$ and thus E is a projection.

We claim A = range of E and B = Ker E

$v \in$ Ker $E \Rightarrow E(v) = 0 \Rightarrow E(a + b) = 0$ where $v = a + b$

$\Rightarrow a = 0 \Rightarrow v = a + b = b \in B$

Again $b \in B \Rightarrow b = 0 + b \ \Rightarrow E(b) = E(0 + b) = 0 \Rightarrow b \in$ Ker E

So B = Ker E

It is easy to see that A = range of E.

We thus notice that when there is projection E on V, then V is direct sum of range E and Ker E and *conversely*, if V is direct sum of two subspaces then there exists a projection E on V such that these subspaces are range and Ker of E.

If $V = R \oplus N$ corresponding to a projection E, we say E is projection on R along N (R = range E, N = Ker E).

Suppose again that $V = A \oplus B$ and let's define

$F : V \to V$ s.t.,

$F(v) = b$ where $v \in V$ is s.t. $v = a + b$

then as before we can check that F is a projection on V and A = Ker F, B = Range F.

Hence if E was projection on A along B, then F is projection on B along A. Is there a direct relation between E and F?

Consider $(E + F)(v) = E(v) + F(v) = a + b = v,$

$= I(v) \ \forall\ v$

and thus $E + F = I$

or that $E = I - F$

We can sum up and say that E is a projection iff $I - E$ is a projection and if E is a projection on R along N then $I - E$ is a projection on N along R.

We give another 'proof' of this result in problem 43.

Let us now consider the general result through

Theorem 20: *If $V = W_1 \oplus \ldots \oplus W_k$, then $\exists$ k linear operators $E_1, \ldots, E_k$ on V s.t.*

(*i*) *Each E_i is a projection*

(*ii*) *$E_iE_j = 0$ for all $i \neq j$*

(*iii*) *$I = E_1 + \ldots + E_k$*

(*iv*) *the range of E_i is W_i*

and conversely.

Proof: Let $v \in V$ be any element then

$$v = x_1 + x_2 + ... + x_k, \quad x_i \in W_i \text{ being uniquely determined}$$

Define $E_i : V \to V$, s.t.,

$$E_i(x_1 + ... + x_k) = x_i \text{ for all } i$$

Then E_i is linear operator s.t.,

$$E_i^2 (x_1 + ... + x_k) = E_i(x_i) = x_i = E_i(x_1 + ... + x_k)$$

$$\Rightarrow E_i^2 = E_i \text{ for all } i$$

This proves (*i*).

Let $i \neq j$. Then $E_iE_j(x_1 + ... + x_k) = E_i(x_j) = 0$

$$\therefore \quad E_iE_j = 0 \text{ for all } i \neq j.$$

This proves (*ii*).

Let $v \in V$. Then $v = x_1 + ... + x_k$, $x_i \in W_i$

$$\therefore \quad (E_1 + ... + E_k)v = E_1v + ... + E_kv$$
$$= x_1 + ... + x_k$$
$$= v = I(v)$$

$$\therefore \quad E_1 + ... + E_k = I$$

This proves (*iii*).

By definition of E_i, range of E_i is W_i which proves (*iv*).

Conversely, let $v \in V$. By (*iii*) $I = E_1 + ... + E_k$

$$\Rightarrow v = I(v) = E_1(v) + ... + E_k(v) = x_1 + ... + x_k, \; x_i \in W_i \; (x_i = E_iv)$$

$$\therefore \quad V = W_1 + ... + W_k$$

Let $v = y_1 + ... + y_k, \quad y_i \in W_i$ = Range of E_i

$$\Rightarrow y_i = E_i(z_i)$$

$$\therefore \quad E_j(v) = E_j(y_1) + ... + E_j(y_k)$$
$$= E_j\, E_1(z_1) + ... + E_jE_k(z_k)$$
$$= E_j^2 (z_j) = E_j(z_j) = y_j$$

$$\therefore \quad x_j = y_j \text{ for all } j = 1, ..., k$$

$\therefore$ each $v \in V$ can be uniquely written as sum of elements of $W_1, ..., W_k$.

Hence, $V = W_1 \oplus ... \oplus W_k$.

Problem 62: *Prove that if E is the projection on R along N, then I–E is the projection on N along R.*

Solution: Let $x \in R$ then $x = Ey$, $y \in V$

$$\Rightarrow (I - E)\, x = x - Ex = Ey - Ey = 0$$

$$\Rightarrow x \in \text{null space of } I - E$$

Also $x \in N \Rightarrow Ex = 0$

$$\Rightarrow (I - E)\, x = x \text{ for all } x \in N$$

$\therefore \quad v \in V \Rightarrow v = r + n,\ r \in R,\ n \in N$

$\Rightarrow (I - E)\ v = (I - E)\ r + (I - E)\ n$

$= 0 + n = n$

$\therefore$ Range space of $I - E$ is N

Also $(I - E)^2 = I + E^2 - 2E = I - E$

$\therefore$ $I - E$ is the projection on N along R.

Problem 63: *Let $V(F)$ be a vector space. Let E_1 be a projection on R_1 along N_1 and E_2 be a projection on R_2 along N_2. Assuming that $1 + 1 \neq 0$ in F, show that*

(i) $E_1 + E_2$ is projection iff $E_1E_2 = E_2E_1 = 0$.

(ii) $E_1 + E_2$ is a projection on $R_1 \oplus R_2$ along $N_1 \cap N_2$.

Solution: We have $V = R_1 \oplus N_1$ and $V = R_2 \oplus N_2$

Let $E_1 + E_2$ be a projection. Then $(E_1 + E_2)^2 = E_1 + E_2$

$\Rightarrow E_1^2 + E_2^2 + E_1E_2 + E_2E_1 = E_1 + E_2$

$\Rightarrow E_1E_2 + E_2E_1 = 0$ $\quad (i)$

$\Rightarrow E_1E_1E_2 + E_1E_2E_1 = 0 \Rightarrow E_1E_2 = -E_1E_2E_1$

and $E_1E_2E_1 + E_2E_1E_1 = 0 \Rightarrow E_2E_1 = -E_1E_2E_1$

Thus $E_1E_2 = E_2E_1$ and so (i) gives

$(1 + 1)\ E_1E_2 = 0 \Rightarrow E_1E_2 = 0$

Hence $E_1E_2 = E_2E_1 = 0$

Conversely, $E_1E_2 = E_2E_1 = 0$ gives

$E_1E_2 + E_2E_1 = 0$

$\Rightarrow E_1^2 + E_2^2 + E_1E_2 + E_2E_1 = E_1 + E_2$

$\Rightarrow (E_1 + E_2)^2 = E_1 + E_2$.

(ii) We have to show that Range of $E_1 + E_2$ is $R_1 \oplus R_2$ and Ker $(E_1 + E_2) = N_1 \cap N_2$.

Let $x \in \text{Ker}\ (E_1 + E_2) \Rightarrow (E_1 + E_2)x = 0$

$\Rightarrow E_1x + E_2x = 0 \Rightarrow E_1E_1(x) + E_1E_2(x) = 0$

$\Rightarrow E_1(x) + E_1E_2(x) = 0$

$\Rightarrow E_1(x) = 0$ as $E_1E_2(x) = 0$

Similarly we get $E_2(x) = 0$

Hence $x \in \text{Ker}\ E_1 = N_1,\ x \in \text{Ker}\ E_2 = N_2$

and so $x \in N_1 \cap N_2 \Rightarrow \text{Ker}\ (E_1 + E_2) \subseteq N_1 \cap N_2$

Again, $y \in N_1 \cap N_2 \Rightarrow y \in N_1\ \&\ y \in N_2$

$\Rightarrow E_1(y) = 0,\ E_2(y) = 0$

$\Rightarrow (E_1 + E_2)y = 0 \Rightarrow y \in \text{Ker}\ (E_1 + E_2)$

So $N_1 \cap N_2 \subseteq \text{Ker}\ (E_1 \cap E_2)$

or that $\text{Ker}\ (E_1 + E_2) = N_1 \cap N_2$

We leave the rest of the proof for the reader as an exercise.

Theorem 21: *Any projection E on a vector space V is diagonalisable.*

Proof: Suppose $\{v_1, v_2, ..., v_k\}$ is a basis of range space R of E and $\{v_{k+1}, ..., v_n\}$ is a basis of null space N of E.

Then $\{v_1, v_2, ..., v_k, v_{k+1}, ..., v_n\}$ is a basis of $R \oplus N = V$

Now $E(v_1) = E(r_1 + n_1) \quad r_1 \in R, n_1 \in N$

$\Rightarrow E^2(v_1) = E(v_1) = E(r_1 + n_1) = E(r_1) + E(n_1) = E(r_1)$

$\Rightarrow E(v_1) = E(r_1)$

$\Rightarrow E(v_1 - r_1) = 0 \Rightarrow v_1 - r_1 \in \text{Ker } E = N$

Also $v_1 \in R, r_1 \in R \Rightarrow v_1 - r_1 \in R$

and thus $v_1 - r_1 \in R \cap N = \{0\}$

$\Rightarrow v_1 = r_1$

Again $n_1 = v_1 - r_1 = 0$

Thus $E(v_1) = v_1$. Similarly $E(v_i) = v_i \quad \forall\ i = 1, 2, ..., k$

Also $E(v_j) = 0 \quad \forall\ j = k + 1, ..., n.$

Showing matrix of E w.r.t. this basis is $\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$

which is clearly a diagonal matrix.

Hence the result follows.

Problem 64: *If diagonal operator has eigen values 0 and 1 only then show that it is a projection.*

Solution: Since T is diagonal operator, $\exists$ a basis $\beta = \{v_1, ..., v_n\}$ of V s.t. $[T]_\beta$ = diagonal. Since eigen values of T are 0 and 1, let first m entries in diagonal be 1 and others be 0.

Let $v \in V$. Then $v = \alpha_1 v_1 + ... + \alpha_m v_m + \alpha_{m+1} v_{m+1} + ... + \alpha_n v_n$

$\therefore \quad T^2(v) = T(Tv)$

$= T(\alpha_1 v_1 + ... + \alpha_m v_m)$ as $Tv_i = v_i$ for all i, $1 \le i \le m$

$Tv_j = 0$ for all $j > m$

$= T(\alpha_1 v_1 + ... + \alpha_m v_m + \alpha_{m+1} v_{m+1} + ... + \alpha_n v_n)$

$= T(v)$ for all $v \in V$

$\therefore \quad T^2 = T$

Hence T is a projection.

Theorem 22: *Let T be a linear operator on the space V and $V = W_1 \oplus ... \oplus W_k$. Define $E_i(v) = E_i(x_1 + ... + x_k) = x_i \in W_i$. Then each E_i is a projection on V s.t. $E_i E_j = 0$ for all $i \neq j$ and $I = E_1 + ... + E_k$. Also then each W_i is invariant under T iff $TE_i = E_i T$ for all i = 1, 2, ..., k.*

Proof: Let $TE_i = E_i T$

Let $x_i \in W_i$. Then by def., $E_i(x_i) = x_i$

$$\therefore \quad T(x_i) = T(E_i x_i)$$
$$= E_i(Tx_i)$$
$$\Rightarrow T(x_i) \in \text{Range of } E_i = W_i$$

$\therefore$ W_i is invariant under T for all $i = 1, ..., k$

Conversely, let W_i be invariant under T. Then $v \in V$

$$\Rightarrow I(v) = (E_1 + ... + E_k)(v)$$
$$\Rightarrow v = E_1(v) + ... + E_k(v)$$
$$\Rightarrow T(v) = TE_1(v) + ... + TE_k(v)$$

Since $E_i(v) \in W_i$ and W_i is T- invariant $\Rightarrow T(E_i(v)) \in W_i$.

So, $E_j[T(E_i(v)] = T(E_i(v))$ if $j = i$
$= 0$ if $j \neq i$

$\therefore$ $E_j(T(v)) = T(E_j(v)) \quad \forall\ v \in V$

$\Rightarrow E_j T = TE_j \quad \forall\ j.$

Definition: Let V be a vector space and $E_1, E_2, ..., E_k$ be a collection of projections on V, then this collection is called *orthogonal* collection if $E_i E_j = 0\ \forall\ i \neq j$. Consider the space $\mathbf{R}^2$. Define

$E_1 : \mathbf{R}^2 \to \mathbf{R}^2$, s.t., and $E_2 : \mathbf{R}^2 \to \mathbf{R}^2$, s.t.,

$E_1(a, b) = (a, 0)$ $E_2(a, b) = (0, b)$

then clearly E_1, E_2 are projections and

$E_1E_2(a, b) = E_1(0, b) = (0, 0)$

$E_2E_1(a, b) = E_2(a, 0) = (0, 0)$

Shows $E_1E_2 = E_2E_1$ and thus E_1, E_2 is an orthogonal set of projections.

The above theorem could be restated as

Let T be a linear operator on the space V and let $V = W_1 \oplus W_2 \oplus ... \oplus W_k$ be determined by orthogonal projections $E_1, E_2, ..., E_k$ on V. Then each W_i is T-invariant if and only if $E_iT = TE_i$, $i = 1, 2, ..., k$.

Theorem 23: *Let T be a linear operator on a F.D.V.S. V. If T is diagonalisable and $c_1, ..., c_k$ are distinct eigen values of T, then $\exists$ linear operators $E_1, ..., E_k$ on V s.t.*

(*i*) $T = c_1E_1 + ... + c_kE_k$

(*ii*) $I = E_1 + ... + E_k$

(*iii*) $E_iE_j = 0$ *for all* $i \neq j$

(*iv*) $E_i^2 = E_i$

(*v*) *Range of E_i is the eigen space of T associated with eigen value c_i of T.*

Conversely, if $\exists$ distinct scalars $c_1, ..., c_k$ and k non-zero linear operators $E_1, ..., E_k$ satisfying (*i*), (*ii*), (*iii*) *then T is diagonalisable, $c_1, ..., c_k$ are eigen values of T and* (*iv*) *and* (*v*) *are also satisfied.*

Proof: Let T be diagonalisable and $c_1, ..., c_k$ be distinct eigen values of T. Let W_i be eigen spaces of T corresponding to eigen values c_i.

Then dim V = dim W_1 + ... + dim W_k

and $V = W_1 + ... + W_k$

Hence $V = W_1 \oplus ... \oplus W_k$

As in theorm 20, let E_1, ..., E_k be the projections associated with this decomposition. Then (*ii*) to (*v*) are satisfied. Let $v \in V$

Then $I(v) = v = (E_1 + ... + E_k)v$

$= E_1(v) + ... + E_k(v)$

$\Rightarrow T(v) = TE_1(v) + ... + TE_k(v)$

$= c_1E_1(v) + ... + c_kE_k(v)$ as $E_i(v) \in$ Range of $E_i = W_i$

$= (c_1E_1 + ... + c_kE_k)v$

$\Rightarrow T = c_1E_1 + ... + c_kE_k$

This proves (*i*).

Conversely, suppose T along with distinct scalars c_i and non-zero operators E_i satisfy (*i*), (*ii*) and (*iii*). Also $T = c_1E_1 + ... + c_kE_k$

Then $TE_i = c_iE_i$ for all i

$\Rightarrow (T - c_iI)\ E_i = 0$ for all i

Since $E_i \neq 0\ \exists\ v_i \in V$ s.t. $E_i(v_i) \neq 0$

$\therefore$ $(T - c_iI)\ (E_i(v_i)) = 0$ for all i

$\Rightarrow T(E_i(v_i)) = c_i(E_i(v_i)),\ E_i(v_i)) \neq 0$ for all i

$\Rightarrow c_i$ is an eigen value of T for all i, ($E_i v_i$ is an eigen vector).

If c is any scalar, then

$(T - cI) = (c_1E_1 + ... + c_kE_k) - c(E_1 + ... + E_k)$

$= (c_1 - c)E_1 + ... + (c_k - c)E_k$

If c is an eigen value of T, then $\exists\ 0 \neq v \in V$ s.t.

$Tv = cv \Rightarrow (T - cI)v = 0$

$\therefore$ $(c_1 - c)\ E_jE_1(v) + ... + (c_k - c)\ E_jE_k(v) = 0$

$\Rightarrow (c_j - c)\ E_j(v) = 0$ for all $j = 1, ..., k$

If $E_j(v) = 0$ for all j, then $I = E_1 + ... + E_k$

$\Rightarrow v = I(v) = E_1(v) + ... + E_k(v) = 0$

$\therefore$ $E_j(v) \neq 0$ for some j

$\therefore$ $c_j = c$ for some j

$\therefore c_1, ..., c_k$ are only eigen values of T.

Let W_i = range of E_i, $i = 1, ..., k$.

By (*ii*) $I = E_1 + ... + E_k$

$\Rightarrow v = Iv = E_1v + ... + E_kv \in W_1 + ... + W_k$ for all $v \in V$

$\Rightarrow V = W_1 + ... + W_k$

As in theorem 22, $V = W_1 \oplus ... \oplus W_k$

$\therefore$ dim V = dim W_1 + ... + dim W_k

$\Rightarrow$ T is diagonalisable if W_i = eigen space of T corresponding to c_i.

Let $x \in$ eigen space of T. Then $T(x) = c_i x$, $1 \le i \le k$

$\Rightarrow (c_1E_1 + ... + c_kE_k)x = c_iI(x) = c_i(E_1 + ... + E_k)x$

$\Rightarrow c_1E_1(x) + ... + c_kE_k(x) = c_iE_1(x) + ... + c_iE_k(x)$

$\Rightarrow (c_1 - c_i)\, E_1(x) + ... + (c_k - c_i)\, E_k(x) = 0$

$\Rightarrow (c_j - c_i)\, E_j(x) = 0$ for all $j = 1, ..., k$

as $E_j(x) \in$ Range of $E_j = W_j$

and $W_1, ..., W_k$ are independent.

we get $E_j(x) = 0$, $j \ne i$ as $c_j - c_i \ne 0$ for all $j \ne i$

Since $I = E_1 + ... + E_k$,

$x = E_1(x) + ... + E_k(x) = E_i(x)$

$\Rightarrow x \in$ Range of $E_i = W_i$

$\therefore$ eigen space corresponding to c_i is contained in W_i.

Also $0 \ne x \in W_i \Rightarrow x = E_i(y_i) \ne 0$

But $(T - c_iI)E_i = 0$

$\Rightarrow TE_i(y_i) = c_iE_i(y_i)$

$\Rightarrow T(x) = c_ix \Rightarrow x \in$ eigen space corresponding to c_i

$\therefore$ W_i = eigen space corresponding to c_i.

Using above theorem, we give another proof of theorem 10 *i.e.* suppose T is a linear operator with minimal polynomial $p(x) = (x - c_1) ... (x - c_k)$ s.t. $c_1, ..., c_k \in F$ are distinct. To show T is diagonalisable.

Proof: Let $p_j(x) = \prod_{i \ne j} \frac{(x - c_i)}{(c_j - c_i)}$, $j = 1, ..., k$

Then $p_j(c_i) = \delta_{ij}$

Let V = space of all polynomials over F of degree less than k.

Then $p_1, ..., p_k \in V$ and are linearly independent as $\alpha_1p_1 + ... + \alpha_kp_k = 0$

$\Rightarrow \alpha_1p_1(c_i) + ... + \alpha_k p_k(c_i) = 0$

$\Rightarrow \alpha_i = 0$ for all i

Since dim $V = k$, $\{p_1, ..., p_k\}$ is a basis of V.

Now $1 \in V \Rightarrow 1 = \alpha_1p_1 + ... + \alpha_kp_k$

Put $x = c_i$ on both sides to get

$1 = \alpha_i$ for all i

$\Rightarrow 1 = p_1 + ... + p_k$ ...(*i*)

$x \in V \Rightarrow x = \beta_1p_1 + ... + \beta_kp_k$

Put $x = c_i$

Then $c_i = \beta_i$ for all i

$\Rightarrow x = c_1p_1 + ... + c_kp_k$ ...(*ii*)

Let $p_j(T) = E_j$

Put $x = T$ in (*i*) and (*ii*) above to get

$$I = p_1(T) + ... + p_k(T) = E_1 + ... + E_k$$

$$T = c_1E_1 + ... \; c_kE_k$$

Since $p(x)$ divides $p_i(x)p_j(x)$ for all $i \neq j$

$$p_i(T)p_j(T) = p(T)q(T) \text{ for all } i \neq j$$

$\Rightarrow$ $E_iE_j = 0$ for all $i \neq j$

If $E_j = 0$ for some j, then $p_j(T) = 0$ and

degree of $p_j(x) < \deg p(x)$, a contradiction

$\therefore$ $E_j \neq 0$ for all $j = 1, ..., k$

$\therefore$ T is diagonalisable.

Problem 65: *Let E be a projection of V and let T be a linear operator on V. Prove that the range of E is invariant under T if and only if ETE = TE. Prove that both the range and null space of E are invariant under T if and only if ET = TE.*

Solution: Let R = range of E

N = null space of E

Then $V = R \oplus N$

We have shown before that $I - E$ is also a projection. $x \in N \Rightarrow Ex = 0 \Rightarrow (I - E)x = x \Rightarrow x \in$ range of $I - E$. $\therefore$ Range of $E = R$, Range of $(I - E) = N$.

Also $E(I - E) = E - E^2 = E - E = 0$. Suppose R is invariant under T then $\Rightarrow T(EV) \subseteq EV$ $\Rightarrow T(I - E)V = T(V - EV) \subseteq V - EV = (I - E)V \Rightarrow N = (I - E)V$ is invariant under T.

$\therefore$ By Theorem 22, $TE = ET$

$\Rightarrow ETE = E^2T = ET = TE$.

Conversely, suppose $ETE = TE$

Let $E(v) \in R$ = range of E

Then $E\,(TE(v)) \in R$ as $T : V \to V$, $E : V \to V$

$\Rightarrow TE(v) \in R$ since $ETE = TE$

$\Rightarrow R$ is invariant under T.

Further, if both R and N are invariant under T, then by Theorem 22, $TE = ET$.

Conversely, suppose $TE = ET \Rightarrow ETE = TE$

From above then, R is invariant under T.

Also $n \in N \Rightarrow E(n) = 0 \Rightarrow (ET)(n) = (TE)(n)$

$= T(E(n))$

$= T(0) = 0$

$\therefore$ $E(T(n)) = 0$ for all $n \in N$

$\Rightarrow T(n) \in$ null space of E for all $n \in N$

$\Rightarrow N$ is invariant under T.

Problem 66: *Let* $V = \mathbf{R}^2$ *and T be the linear operator on V whose matrix relative to standard ordered basis is* $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ *for some non-zero a,* $b \in \mathbf{R}$. *Show that*

(*i*) W_1 *the subspace generated by* (1, 0) is *T-invariant*

(*ii*) W_2 *the subspace generated by* (0, 1) *is not T-invariant*

(*iii*) $\exists$ *no T-invariant subspace W of* $\mathbf{R}^2$ *s.t.,* $\mathbf{R}^2 = W_1 \oplus W$.

Solution: We have $W_1 = \{(x, 0) \mid x \in \mathbf{R}\}$

$$T(W_1) = \{a(x, 0) \mid x \in \mathbf{R}\} \subseteq W_1$$

and thus W_1 is invariant under T.

Suppose now W is T-invariant subspace of $\mathbf{R}^2$ s.t., $\mathbf{R}^2 = W_1 \oplus W$. Since dim $W_1 = 1$, dim W must also be 1.

Define $E : \mathbf{R}^2 \to \mathbf{R}^2$, s.t.,

$$E(x, y) = (x, 0)$$

then E is a projection of $\mathbf{R}^2$ onto W_1.

By problem 46, we should have $TE = ET$.

But $TE(1, 1) = T(1, 0) = (a, 0)$

$$ET(1, 1) = E(a + b, a) = (a + b, 0)$$

Showing that $ET \neq TE$ and thus there does not exist any T-invariant subspace W s.t., $\mathbf{R}^2 = W_1 \oplus W$. We leave part (*ii*) for the reader to try.

Using projections, we give another proof of the

Primary Decomposition Theorem: *Let T be a linear operator on a finite dimensional vector space V. Let p*(*x*) *be the minimal polynomial for T such that* $p(x) = p_1(x)^{r_1} \ldots p_k(x)^{r_k}$ *where* $p_i(x)$ *are distinct irreducible monic polynomials over F and* r_i*'s are positive integers. Let* W_i *be the null space of* $p_i(T)^{r_i}$, $i = 1, 2, \ldots, k$. *Then* (*i*) $V = W_1 \oplus \ldots \oplus W_k$ (*ii*) $T(W_i) \subseteq W_i$ *for all* $i = 1, 2, \ldots, k$. (*iii*) *If* T_i *is operator induced on* W_i *by T, then the minimial polynomial for* T_i *is* $p_i(x)^{r_i}$.

Proof: Let $f_i(x) = \dfrac{p(x)}{p_i(x)^{r_i}}$, $i = 1, 2, \ldots, k$

Then g.c.d. $f_1(x), \ldots, f_k(x)) = 1$.

Therefore, there exist $g_1(x), \ldots, g_k(x)$ in $F[x]$ such that

$$f_1(x)g_1(x) + \ldots + f_k(x)g_k(x) = 1$$

So, $f_1(T)g_1(T) + \ldots + f_k(T)g_k(T) = I$

Let $E_i = f_i(T)g_i(T)$

Then $E_1 + \ldots + E_k = I$

Also, $f_i(x) f_j(x) = p(x)q(x)$ for all $i \neq j$

Therefore, $f_i(T) f_j(T) = p(T)q(T) = 0$ $q(T) = 0$ for all $i \neq j$

So, $f_i(T)\, g_i(T)\, f_j(T) g_j(T) = 0$ for all $i \neq j$

which means that $E_i E_j = 0$ for all $i \neq j$

Now $I = E_1 + \ldots + E_k$ and $E_i E_j = 0$ for all $i \neq j$ gives that $E_i^2 = E_i$ for all i. So, each E_i is a projection on V.

Let v be in Range E_i. Then $v = E_i(v')$ gives that $E_i(v) = v$.

So, $p_i(T)^{r_i}(v) = p_i(T)^{r_i} E_i(v) = p_i(T)^{r_i} f_i(T) g_i(T) v = p(T) g_i(T) v = 0$.

Therefore, v is in the null space of $p_i(T)^{r_i}$. So, v is in W_i which means that Range $E_i \subseteq W_i$.

Let v be in W_i. Then for all $j \neq i$, $p_i(x)^{r_i}$ divides $f_j(x)$.

So, $f_j(x) = p_i(x)^{r_i}\, q(x)$

Therefore, $f_j(T) v = p_i(T)^{r_i} q(T) v = q(T)\, p_i(T)^{r_i}\, v = 0$

which gives $f_j(T) g_j(T) v = g_j(T) f_j(T) v = 0$ for all $j \neq i$

So, $E_j(v) = 0$ for all $j \neq i$

Now $I = E_1 + \ldots + E_k$ gives $v = I(v) = E_1(v) + \ldots + E_k(v) = E_i(v)$

Therefore, v is in Range E_i

So, W_i = Range E_i

By Theorem 20, $V = W_1 \oplus \ldots \oplus W_k$. This proves (*i*).

Since $TE_i = T f_i(T) g_i(T) = f_i(T) g_i(T) T = E_i T$ for all i, each W_i is invariant under T. This proves (*ii*). The proof of (*iii*) is smae as given earlier.

The advantage of the above proof is that we have shown that each projection E_i on V is a polynomial in T. This we shall use in the next theorem.

Theorem 24: *Let T be a linear operator on the F.D.V.S. V(F). Suppose that the minimal polynomial for T decomposes over F into a product of linear polynomials. Then* $\exists$ *a diagonalisable operator D on V and a nilpotent operator N on V s.t.* (*i*) $T = D + N$ (*ii*) $DN = ND$. *Further, D and N are uniquely determined such that* $T = D + N$ *and* $DN = ND$.

Proof: Let $p(x) = (x - c_1)^{r_1} \ldots (x - c_k)^{r_k}$ be the minimal polynomial for T where $c_1, \ldots, c_k$ are distinct scalars in F.

By Primary decomposition theorem, $V = W_1 \oplus \ldots \oplus W_k$, where W_i = null space of $(T - c_i I)^{r_i}$. Let $E_1, \ldots, E_k$ be the corresponding projections. Then W_i = range of E_i.

Let $D = c_1 E_1 + \ldots + c_k E_k$

By theorem 21, D is diagonalisable.

Since $I = E_1 + \ldots + E_k$

$T = TE_1 + \ldots + TE_k$, $D = c_1 E_1 + \ldots + c_k E_k$

Let $N = T - D = (T - c_1 I) E_1 + \ldots + (T - c_k I) E_k$

Then $N^2 = (T - c_1 I)^2 E_1 + \ldots + (T - c_k I)^2\, E_k$ as $TE_i = E_i T\ \forall\ i$

and in general that $N^r = (T - c_1 I)^r E_1 + \ldots + (T - c_k I)^r\, E_k$

Since $(x - c_i)^{r_i}$ is the minimal polynomial of T on W_i, $(T - c_i I)^{r_i} = 0$ on W_i for all i.

$\Rightarrow$ $(T - c_i I)^r = 0$ on W_i for all $r \geq r_i$

$\therefore$ $N^r = 0$ for all $r \geq r_i$ for each i

$\therefore$ N is nilpotent operator.

$\therefore$ $T = D + N$, D is diagonalisable and N, nilpotent operator.

Now $DT = (c_1E_1 + ... + c_kE_k)(TE_1 + ... + TE_k)$

$= c_1TE_1 + ... + c_kTE_k$

as $W_i s$ are invariant under $T \Rightarrow TE_i = E_iT$ for all i

$= T(c_1E_1) + ... + (c_kE_k)$

$= (TE_1)(c_1E_1) + ... + (TE_k)(c_kE_k)$

$= (TE_1 + ... + TE_k)(c_1E_1 + ... + c_kE_k)$

$= TD$

$\therefore$ $D(D + N) = (D + N)D$

$\Rightarrow DN = ND$.

To show uniqueness, suppose $T = D' + N'$, where D' is diagonalisable and N' is nilpotent and $D'N' = N'D'$.

Then $D'T = D'(D' + N') = D'D' + D'N'$

$= D'D' + N'D' = (D' + N')D'$

$= TD'$

So D' commutes with T.

Since $D = C_1E_1 + \ldots + C_kE_k$ and each E_i is a polynomial in T, D is a polynomial in T.

So $D'D = DD'$

Thus D, D' are simultaneously diagonalisable.

So, $D - D'$ is also a diagonalisable linear operator.

Now $D - D' = N' - N$ and $NN' = (T - D)(T - D') = (T - D')(T - D) = N'N$

So, $N' - N$ is also a nilpotent operator.

Therefore, $D - D'$ is both diagonalisable and nilpotent operator.

Thus $D - D' = 0 = N' - N \Rightarrow D = D'$ and $N = N'$.

Problem 67: *Let T be the linear operator on* $\mathbf{R}^3$ *which represented by the matrix*

$$\begin{bmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{bmatrix}$$

in the standard ordered bases. Show that there exists a diagonal operator D and a nilpotent operator N such that T = D + N and DN = ND. Find the matrices of D and N.

Solution: The characteristic polynomial of T

$= (x - 1)(x - 2)^2$

= The minimimal polynomial of T.

The eigen values of T are 1, 2, 2.

By Theorem 24, there exists a diagnonal operator D and a nilpotent operator N such that $T = D + N$ and $DN = ND$

Here $c_1 = 1, c_2 = 2$

$\therefore$ $D = E_1 + 2E_2$

Now $(x^2 - 4x + 4) - (x - 3)(x - 1) = 1$

$\therefore$ $E_1 = T^2 - 4T + 4I, \; E_2 = -T^2 + 4T - 3I$

$$\therefore \quad D = -T^2 + 4T - 2I = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ -2 & 2 & 2 \end{bmatrix}$$

$$N = T - D = \begin{bmatrix} 2 & 0 & -1 \\ 2 & 0 & -1 \\ 4 & 0 & -2 \end{bmatrix}$$

Then $N^2 = 0$. So, N is nilpotent.

and $$DN = \begin{bmatrix} 4 & 0 & -2 \\ 4 & 0 & -2 \\ 8 & 0 & -4 \end{bmatrix} = ND$$

The characteristic polynomial of D is $(x - 1)(x - 2)^2$

The minimal polynomial of D is $(x - 1)(x - 2)$ which is product of distinct linear factors. So, D is diagonalisable.

Problem 68: *Let V be the space of all polynomials of degree $\leq n$ over a field F. Let T be the differential operator on V. Using theorem 24, show that T is nilpotent.*

Solution: Let $\beta = \{1, x, \ldots, x^n\}$ be an ordered basis for V.

Then $$[T]_\beta = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & n \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

The characteristic polynomials for T is x^{n+1} which is also the minimal polynomial for T. By Theorem 24, there exists a diagonal operator D and a nilpotent operator N

such that $T = D + N$

Since 0 is the only eigen value of T and $D = c_1E_1 + \ldots + c_{n+1} E_{n+1} = 0$

$\therefore$ $T = N$

So, T is nilpotent

Problem 69: *Show that a non zero linear operator on a finite dimensional vector space can not be both diagonal and nilpotent.*

Solution: Let T be a non zero linear operator on a finite dimensional vector space V. If T is nilpotent then $T^r = 0$ for some integer $r > 0$. The minimal polynomial for T would be x^3, $s \leq r$. If T is also diagonalisable, then the minimal polynomial would be a product of distinct linear factors. So, it would be x which means that $T = 0$, a contradiction. Thus T cannot be both diagonal and nilpotent.

Let T and S be linear operators on a finite dimensional vector space V. If there exists a basis β for V such that $[T]_\beta$ and $[S]_\beta$ are diagonal matrices, then T and S are called *simultaneously diagonalisable*. Equivalently, if there exists a bsis $\beta = \{v_1, v_2, \ldots, v_n\}$ for V such that each v_i is an eigen vector of both T and S, then T and S are called simultaneously diagonalisable.

Theorem 25: *Let S and T be diagonalisable operators on a finite dimensional vector space V such ST = TS. Then T and S are simultaneously diagonalisable.*

Proof: Let λ be an eigen value of T.

Let $W = \{v \in V \mid T(v) = \lambda v\}$

Let $v \in W$

Then $T(Sv) = (TS)(v)$

$= (ST)(v)$

$= S(T(v))$

$= S(\lambda v)$

$= \lambda\, Sv$

$\therefore$ $Sv \in W$ for all $v \in W$

$\therefore$ W is S-invariant.

Since S is diagonalisable, $S \mid W$ is diagonalisable.

Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be distinct eigen values of T.

Let $W_1, W_2, \ldots, W_k$ be the corresponding eigen spaces.

Since T is diagonalisable $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$

Now $S \mid W_1 = S_{W1}$is diagonalisable, and so there exists a basis $\beta_1 = \{x_1, x_2, \ldots x_r\}$ of W_1 such that each x_i is an eigen vector of S_{W1}. Now $S_{W1}(x_i) = S(x_i)$ as $x_i \in W_1$. So, each x_i is an eigen vector of S.

In this way, there exist basis $\beta_1, \beta_2, \ldots, \beta_k$ of $W_1, W_2, \ldots, W_k$ respectively, such that β_i consists of eigen vector of S.

Let $\beta = \beta_1 \cup \beta_2 \cup \ldots \cup \beta_k$. Then β is a basis of V.

Also $x_i \in \beta_i \leq W_i$ means that x_i is also an eigen vector of T.

In this way, β consists of eigen vectors of S and T.

Thus, T and S are simultaneously diagonalisable.

Cor: Let S and T be linear operators on a finite dimensional vector space V such that both S and T are diagonalisable and $ST = TS$. Then $S + T$ is also diagonalisable.

Proof: By above theorem S and T are simulataneously diagonalisable. So, there exists an ordered basis of β of V such that $[T]_\beta$ and $[S]_\beta$ are both diagonal matrices.

$\therefore$ $[S + T]_\beta = [S]_\beta + [T]_\beta$ is a diagonal matrix.

Hence $S + T$ is also diagoanlisable.

Problem 70: Let *T be a linear operator on a finite dimensional vector space V such that Rank T = 1. Show that T is either diagonalisable or nilpotent.*

Solution: Since Rank $T = 1$, dim Ker $T = n - 1$

Where $n = \dim V$

Let $\{x_1, x_2, \ldots, x_{n-1}\}$ be a basis of Ker T

Let $\{x_1, x_2, \ldots, x_{n-1}, x_n\} = \beta$ be a basis of V

Then $$[T]_\beta = \begin{bmatrix} 0 & 0 & 0 & c_1 \\ 0 & 0 & 0 & c_2 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & c_{n-1} \\ 0 & 0 & 0 & c \end{bmatrix}$$

If $c \neq 0$, the characteristic polynomial of T is $x^{n-1}(x - c)$ and the minimal polynomial of T would be $x(x - C)$

So, T is diagonalisable

If $c = 0$, then the characteristic polynomial for T is x^n and the minimal polynomial of T would be x^r, $1 \leq r \leq n$.

So, T is nilpotent.

Problem 71: *Let T be a linear operator on a finite dimensional vector space V. Suppose T commutes with every diagonalisable operator on V. Prove that T is scalar multiple of I.*

Solution: Let $D = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ & & \mathrm{O} & \end{bmatrix} = E_{11}$

Then D is diagonalisable

Let $[T]_\beta = (a_{ij}) = A$

Then $AD = DA$ means that 1st row and 1st column of A is zero except a_{11}.

Let $D = E_{22}$. Then D is diagonalisable.

So, $AD = DA$ means that 2nd row and 2nd column of A is zero except a_{22}.

In this way, $A = \begin{bmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{bmatrix}$

Let $D = E_{11} + E_{21} + \ldots + E_{n1}$

Then the characteristic polynomial of D is $x^{n-1}(x-1)$ and the minimal polynomial of D is $x(x-1)$

$\therefore$ $AD = DA$ means that

$a_{22} = a_{33} = \ldots = a_{nn} = a_{11} = c$ (say)

$\therefore$ $$A = \begin{bmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{bmatrix} = cI$$

Hence, $T = cI$.

Exercises

1. Let V be the vector space of all polynomials of degree ≤ 6 over F. Let W be the subspace of V spanned by $\{1, x^2, x^4, x^6\}$. Let D be the differential operator on V. (*i.e.* $D(f(x)) = \frac{d}{dx} f(x)$). Show that W is not invariant under D.

2. In exercise 1, show that W is invariant under D^2 where $D^2(f(x)) = \frac{d^2}{dx^2} f(x)$. Let $T = D^2$. Find

(i) the matrix of T_w in a suitable basis of W.

(ii) the matrix of $\hat{T}$ in a suitable basis of $\frac{V}{W}$

(iii) the matrix of T in a suitable basis of V.

(i) $A = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 30 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ (ii) $C = \begin{bmatrix} 0 & 6 & 0 \\ 0 & 0 & 20 \\ 0 & 0 & 0 \end{bmatrix}$ (iii) $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$

3. Let V be the vector space of all polynomials over the field of real numbers **R**. Let W be the subspace of V spanned by $\{1, x, x^2\}$. Let T be the linear operator on V defined by $T(f(x)) = xf(x)$. Show that W is not invariant under T.

4. Let T be a linear operator on a vector space V over F. If $W_1, \ldots, W_k$ are T-invariant subspaces of V, prove that $\sum_{i=1}^{k} W_i$ and $\bigcap_{i=1}^{k} W_i$ are T-invariant subspaces of V.

5. Let c be a characteristic value of T and W be the space of characteristic vectors associated with the characteristic value c. What is the restriction operator T_w? ($T_w = cI$)

6. Let T be a linear operator on a finite dimensional vector space V. Prove that T is diagonalisable if and only if V is a direct sum of one dimensional T-invariant subspaces.

7. Let T be a linear operator on a finite dimensional vector space V and let W be a T-invariant subspace of V.

(i) Show that if λ is an eigen value of T_w, then λ is an eigen value of T.

(ii) Show that the eigen space of T_w corresponding to eigen value λ of T_w is $W_\lambda \cap W$, where W_λ denotes the eigen space of T corresponding to λ.

(iii) Prove that if T is diagonalisable, then so is T_w.

(**Hint**: T is diagonalisable $\Leftrightarrow V = W_1 + ... + W_k$ where W_i denotes eigen space corresponding to eigen value λ_i of T. Use (ii)).

8. Let W be a proper T-invariant subspace of V, where T is a linear operator on a finite dimensional vector space V.

Let $\eta : V \to \frac{V}{W}$ s.t.,

$\eta(v) = W + v$ be a linear transformation. Show that $\eta T = \hat{T}\eta$ where $\hat{T}$ is a linear operator on $\frac{V}{W}$ defined by $\hat{T}(W + v) = W + T(v)$.

Further, if T is diagonalisable, show that $\hat{T}$ is also diagonalisable.

(**Hint**: T is diagonalisable $\Rightarrow \exists$ a basis $\{x_1, ..., x_n\}$ of V consisting of eigen vectors of T. Also $\eta T = \hat{T}\eta \Rightarrow \{\eta x_1, \ldots, \eta x_n\}$ are eigen vectors of $\hat{T} \Rightarrow \{W + x_1, ..., W + x_n\}$ are eigen vectors of $\hat{T}$. If $\{W + v_1, ..., W + v_r\}$ is a basis of $\frac{V}{W}$, then it can be replaced by $\{W + x_1, ..., W + x_r\}$ such that it forms a basis of $\frac{V}{W}$ consisting of eigen vectors of $\frac{V}{W}$).

9. Let T be a linear operator on a finite dimensional vector space and suppose that $V = W_1 \oplus \ldots \oplus W_k$, where W_i is a T-invariant subspace of V for each $i = 1, ..., k$. If $f(t)$ denotes the characteristic polynomial of T and $f_i(t)$ denotes the characteristic polynomial of T_{w_i} ($1 \le i \le k$), then show that

$$f(t) = f_1(t) \cdot f_2(t) \ldots f_k(t)$$

(**Hint**: Use induction on k).

10. If E_1, E_2 are projections onto independent subspaces, show that $E_1 + E_2$ is also a projection.

11. Let T be a linear operator on a finite dimensional vector space V. Let R be the range of T and let N be the null space of T. Prove that R and N are independent if and only if $V = R \oplus N$.

A Quick Look at what's been done

- If T be a linear operator on a vector space $V(F)$ and there exists a non-zero $v \in V$, s.t., $T(v) = cv$ for some c in F, then v is called an **eigen vector** or **characteristic vector** of T and c is called an **eigen value** or **characteristic value** or **characteristic root** of T.
- Let T be a linear operator on a *F.D.V.S. V(F)*. The **minimal polynomial** for T is defined to be the unique polynomial $p(x) \in F[x]$, s.t., $p(x)$ is monic, $p(T) = 0$ and no polynomial over F which annihilates T has smaller degree than $p(x)$.
- If T be a linear operator on an n-dimensional space V, then the characteristic and minimal polynomials for T have same roots.
- The minimal polynomial of a linear operator T divides its characteristic polynomial.
- A linear operator T on a finite-dimensional vector space V is called **diagonalizable** if there exists an ordered basis β of V such that matrix of T w.r.t. β is a diagonal matrix. Equivalently, T is diagonalizable iff there exists basis of V consisting of eigen vectors of T.
- If T is a linear operator on an n-dimensional vector space V and it has n distinct characteristic values, then T is diagonalizable. The converse does not hold.
- If T is a linear operator on a *F.D.V.S.* $V(F)$, then T is diagonalizable iff algebraic multiplicity of $c_i (\in F)$equals the geometric multiplicity of c_i for all i.
- If W is a subspace of V and T is a linear operator on V, s.t., $T(W) \subseteq W$, we say W is **invariant** under T or is ***T*-invarient**.
- **Primary decomposition theorem** and **projections** have been discussed in the later part of the chapter. If a linear operator T has a minimal polynomial as a product of linear polynomials then $T = D + N$, $DN = ND$, where D is diagonalizable operator and N is a nil operator.

13

Fields

Introduction

In earlier chapters we defined a field, a subfield and proved a few results regarding these. We now come back to fields and study them in some more details. Fields play an important role in algebra with applications to Number Theory, theory of equations and geometry. In this chapter we plan to study different extensions of a field, the presence of roots of a polynomial in an extension and splitting fields.

Definition: Let K be a field and suppose F is a subfield of K, then K is called an *extension* of F.

Suppose S is a non empty subset of K. Let $F(S)$ denote the smallest subfield of K which contains both F and S. (In fact $F(S)$ would be the intersection of all subfields of K that contain F and S). The following theorem is then an easy consequence.

Theorem 1: *If S, T are non empty subsets of a field K and K is an extension of a field F then $F(S \cup T) = F(S)\ (T)$ (where, of course, if $F(S) = E$, then by $F(S)(T)$ we mean $E(T)$).*

Proof: $F(S \cup T)$ is the smallest subfield of K containing $S \cup T$, F

i.e., $S, T, F \subseteq F(S \cup T)$

$\Rightarrow \quad F(S) \subseteq F(S \cup T),\ T \subseteq F(S \cup T)$

$\Rightarrow \quad F(S)(T) \subseteq F(S \cup T)$

Again, $F, S, T \subseteq F(S)(T)$

$\Rightarrow F, S \cup T \subseteq F(S)\ (T)$

$\Rightarrow F(S \cup T) \subseteq F(S)(T)$

or that $F(S \cup T) = F(S)(T)$

Cor.: $F(S \cup T) = F(T \cup S) = F(S)(T)$ follows clearly as $S \cup T = T \cup S$.

Note: If S is a finite subset $\{a_1, a_2, \ldots, a_n\}$ of K we write $F(S) = F(a_1, a_2, \ldots, a_n)$. The order in which a_i appear is immaterial in view of the above corollary as

$$\begin{aligned} F(a_1, a_2, \ldots, a_n) &= F(\{a_1\}\{a_2, a_3, \ldots, a_n\}) \\ &= F(\{a_2, a_3, \ldots, a_n\} \cup \{a_1\}) \\ &= F(a_2, a_3, \ldots, a_n, a_1) \end{aligned}$$

Also then, $F(a)(b) = F(a, b) = F(b, a) = F(b)(a)$

Again, if $K = F(a)$, K is called *simple extension* of F and we say K is obtained by adjoining the element a to F.

Problem 1: *Let* $\mathbf{Q}$ *be the field of rationals then show that* $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Solution: By definition

$$\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

$$\Rightarrow \sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3}) \quad \text{(closure)}$$

$$\Rightarrow \mathbf{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

Now $\sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow (\sqrt{2} + \sqrt{3})^2 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow 2 + 3 + 2\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Also $5 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow 5 + 2\sqrt{2}\sqrt{3} - 5 = 2\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Again, $2 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\therefore \quad 2 \times \frac{1}{2} \sqrt{2}\sqrt{3} = \sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow (\sqrt{2} + \sqrt{3})\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3}) \qquad \ldots(1)$$

Also $\sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow 2(\sqrt{2} + \sqrt{3}) \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow 2\sqrt{2} + 2\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow (2\sqrt{3} + 3\sqrt{2}) - (2\sqrt{2} + 2\sqrt{3}) \in \mathbf{Q}(\sqrt{2} + \sqrt{3}) \text{ by using (1)}$$

$$\Rightarrow \sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Again, $\sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow 3(\sqrt{2} + \sqrt{3}) \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$
and using (1) we get

$$(3\sqrt{2} + 3\sqrt{3}) - (2\sqrt{3} + 3\sqrt{2}) \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

i.e., $\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

Hence $\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow \mathbf{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2} + \sqrt{3})$

or that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

If K is an extension of F, then we know that K can be regarded as a vector space over F. In that case dimension of K over F is called *degree of K over F* and we denote it by $[K : F]$. Our next theorem is about the degree of extension fields. If $[K : F]$ is finite, we say K is finite extension of F.

Theorem 2: *Let K be a finite extension of F and L, a finite extension of K. Then L is a finite extension of F and*

$$[L : F] = [L : K]\,[K : F].$$

Proof: Let $[L : K] = m$, $[K : F] = n$

Let $\{a_1, ..., a_m\}$ be a basis of L over K and $\{b_1, ..., b_n\}$ be a basis of K over F.

We show that $\{a_i b_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ is a basis of L over F.

$$a_i \in L,\ b_j \in K \quad \Rightarrow \quad b_j \in L. \quad \therefore \quad a_i b_j \in L \text{ for all } i, j$$

Let $$\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} a_i b_j = 0, \quad \alpha_{ij} \in F$$

Then $$\sum_{i=1}^{m} \sum_{j=1}^{n} (\alpha_{ij} b_j) a_i = 0, \quad \sum_{j=1}^{n} \alpha_{ij} b_j \in K$$

Since $\{a_1, ..., a_m\}$ are linearly independent over K,

$$\sum_{j=1}^{n} \alpha_{ij} b_j = 0 \quad \text{for all } i = 1, ..., m$$

Also $b_1, ..., b_n$ are linearly independent over F.

$$\alpha_{ij} = 0 \quad \text{for all } i = 1, ..., m \quad j = 1, ..., n$$

$\therefore$ $\{a_i b_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ is a linearly independent subset of L over F. Let $a \in L$. Since $\{a_1, ..., a_m\}$ is a basis of L over K, $a = \alpha_1 a_1 + ... + \alpha_m a_m$, $\alpha_i \in K$ and $\{b_1,..., b_n\}$ is a basis of K over F

$$\Rightarrow \quad \alpha_i = \beta_{i1} b_1 + ... + \beta_{in} b_n, \quad \beta_{ij} \in F$$

$$\therefore \quad a = \sum_{i=1}^{m} \alpha_i a_i = \sum_{i=1}^{m} (\beta_{i1} b_1 ... + \beta_{in} b_n) a_i$$

$$= \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} a_i b_j, \quad \beta_{ij} \in F$$

$\therefore$ $\{a_i b_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ spans L over F and so forms a basis of L over F.

$\therefore$ $$[L : F] = mn = [L : K]\,[K : F]$$

Remark: If $[L : K]$ is infinite, then $[L : F]$ is also infinite because $[L : F] = r \Rightarrow$ every subset of L having $r + 1$ elements is linearly dependent over F. Since $[L : K]$ is infinite, $\exists\, a_1, ..., a_{r+1} \in L$ which are linearly independent over K. Now $1 \in K$ and 1 is linearly independent over F as $1 \ne 0$. As in Theorem 2, $a_1.1$, $a_2.1$, ... $a_{r+1}.1$ are linearly independent over F. We find $a_1, ..., a_{r+1} \in L$ are linearly independent over F, a contradiction.

$\therefore$ $[L : F]$ is infinite. Similarly, $[K : F]$ is infinite.

Cor. 1: If L is a finite extension of F and K is a subfield of L which contains F, then $[K : F]$ divides $[L : F]$.

Proof: By remark above $[K : F]$ is finite as $[L : F]$ = finite. Also $[L : K]$ is finite.

By Theorem 2, $[L : F] = [L : K]\,[K : F]$

$\therefore$ $[K : F]$ divides $[L : F]$

Cor. 2: If K is an extension of F, then $K = F$ if and only if $[K : F] = 1$.

Proof: If $K = F$, then $[K : F] = [K : K] = 1$

If $[K : F] = 1$, let $\{a\}$ be a basis of K over F.

$\therefore$ $1 \in K \Rightarrow 1 = \alpha a,\ \alpha \in F,\ \alpha \neq 0$ as $1 \neq 0$

$\Rightarrow a = \alpha^{-1} \in F$

Let $b \in K \Rightarrow b = \beta a,\ \beta \in F,\ a \in F$

$\Rightarrow b \in F \Rightarrow K \subseteq F \Rightarrow K = F.$

Cor. 3: If L is an extension of F and $[L : F]$ is a prime number p, then there is no field K s.t., $F \subset K \subset L$.

Proof: Suppose $\exists$ a field K s.t., $F \subset K \subset L$.

Then $p = [L : F] = [L : K]\,[K : F]$ by Theorem 2

$\Rightarrow [L : K] = 1$ or $[K : F] = 1$

$\Rightarrow K = L$ or $K = F$ by Cor. 2

a contradiction.

Hence the result.

Trivially then, if K is an extension of F of prime degree then for every $a \in K$, $F(a) = F$ or $F(a) = K$.

Problem 2: *Let D be an integral domain. Let F be a field s.t., $F \subseteq D$. Suppose unity* 1 *of F is also unity of D. Then D can be regarded as a vector space over F. Show that D is a field if* $[D : F]$ = *finite.*

Solution: Let $[D : F] = r$. Let $\{a_1, ..., a_r\}$ be a basis of D over F.

Let $0 \neq a \in D$. We show that a is invertible. Consider $\{aa_1, ..., aa_r\}$.

Let $\alpha_1(aa_1) + ... + \alpha_r(aa_r) = 0,\ \alpha_i \in F.$

Then $a(\alpha_1 a_1 + ... + \alpha_r a_r) = 0$

$\Rightarrow \alpha_1 a_1 + ... + \alpha_r a_r = 0$, as $a \neq 0$ and D is an integral domain.

$\Rightarrow \alpha_i = 0$ for all $i = 1, ..., r$ as $\{a_1, ..., a_r\}$ is linearly independent over F.

$\Rightarrow \{aa_1, ..., aa_r\}$ is linearly independent over F.

But $[D : F] = r \Rightarrow \{aa_1, ..., aa_r\}$ is a basis of D over F.

$\therefore$ $1 \in D \Rightarrow 1 = \beta_1 aa_1 + ... + \beta_r aa_r,\quad \beta_i \in F$

$= a(\beta_1 a_1 + ... \beta_r a_r)$

$= ab,\quad b = \beta_1 a_1 + ... + \beta_r a_r \in D$

$\Rightarrow a$ is invertible.

$\Rightarrow D$ is a field.

Algebraic Extensions

Suppose K is an extension of F and $a \in K$.

Let $F[a] = \{f(a) \mid f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]\}, \quad a_i \in F$

then as $f(a) = a_0 + a_1a + \ldots + a_na^n \in K$, we find $F[a] \subseteq K$

One can show that $F[a]$ is an integral domain.

Let E be its field of quotients. Then E is the smallest field containing $F[a]$. We show

$$F[a] \subseteq F(a) \subseteq E.$$

Now $x = 0 + 1.x + 0.x^2 + \ldots \in F[x]$ and so

$a = 0 + 1.a + 0.a^2 + \ldots \in F[a]$

i.e., $a \in F[a] \subseteq E$

Again if $\alpha \in F$ be any element then

$$\alpha = \alpha + 0x + 0x^2 + \ldots \in F[x]$$

gives $\alpha \in F[a]$ or that $F \subseteq F[a] \subseteq E$

Hence $F(a) \subseteq E$, as $F(a)$ is the smallest field containing F and a.

If $f(a) \in F[a]$ be any member where

$$f(a) = \alpha_0 + \alpha_1a + \ldots + \alpha_na^n, \ \alpha_i \in F$$

then as $a \in F(a)$, $\alpha_i \in F \subseteq F(a)$, we find $f(a) \in F(a)$

Hence $F[a] \subseteq F(a)$ and so

$$F[a] \subseteq F(a) \subseteq E$$

But E is the smallest field containing $F[a]$.

$\therefore E \subseteq F(a)$. Hence $F(a) = E$.

So, we have explicitly determined the field $F(a)$. It is the field of quotients of $F[a]$.

We write, $F(a) = \left\{ \dfrac{f(a)}{g(a)} \middle| g(a) \neq 0, f(x), g(x) \in F[x] \right\}$

In general, one can show that

$$F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \middle| g(a_1, \ldots, a_n) \neq 0, \begin{matrix} f(x_1, \ldots, x_n) \in F[x] \\ g(x_1, \ldots, x_n) \in F[x] \end{matrix} \right\}$$

A natural question arises. When is $F[a] = F(a)$? To answer this, we first define what is an algebraic element. Let K be an extension of F. $a \in K$ is said to be *algebraic* over F if $\exists$ non-zero polynomial $f(x) \in F[x]$ s.t., $f(a) = 0$. Otherwise, it is called transcendental element. For example, $\sqrt{2} \in \mathbf{R}$ = real field, is algebraic over $\mathbf{Q}$ = rational field as $\sqrt{2}$ satisfies non-zero polynomial $f(x) = x^2 - 2 \in \mathbf{Q}[x]$. However, $\pi, e \in \mathbf{R}$ are not algebraic over $\mathbf{Q}$. An extension K of F is called an *algebraic extension* if every $a \in K$ is algebraic over F.

If for some $a \in K$, a is not algebraic over F, then K is called transcendental extension of F. For example, $\mathbf{R}$ is transcendental extension of $\mathbf{Q}$. We shall see in the following theorem that finite extensions are algebraic. So, $\mathbf{C}$ = the field of complex numbers is algebraic over $\mathbf{R}$ as $[\mathbf{C} : \mathbf{R}] = 2$, $\{1, i\}$ being a basis of $\mathbf{C}$ over $\mathbf{R}$.

We sometimes use the notation K/F to express the fact that K is an extension of F. Similarly, K/F is algebraic would mean K is an algebraic extension of F.

Theorem 3: *A finite extension is algebraic.*

Proof: Let K be a finite extension of F. Let $[K : F] = n$. Let $a \in K$. Then $1, a, \ldots, a^n$ are linearly dependent over F. Thus $\exists\ \alpha_0, \alpha_1, \ldots, \alpha_n \in F$ s.t., $\alpha_0.1 + \alpha_1 a + \ldots + \alpha_n a^n = 0$ for some $\alpha_i \neq 0$.

Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$. Then $f(x)$ is non-zero polynomial in $F[x]$ as some $\alpha_i \neq 0$. Also $f(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n = 0$

$\therefore$ a is algebraic over F.

$\therefore$ K is algebraic over F.

Note: Converse of Theorem 3 is not true. We shall give an example later to prove this.

Cor.: $a \in K$ is algebraic over F if $[F(a) : F]$ = finite.

Proof: By theorem 3, $F(a)$ is algebraic over F.

$\therefore$ $a \in F(a)$ is algebraic over F.

Converse of the above corollary is also true. But we'll prove it after the next theorem.

Theorem 4: *Let $a \in K$ be algebraic over F. Then*

(*i*) $\exists$ *a unique monic irreducible polynomial* $p(x) \in F[x]$ *s.t.,* $p(a) = 0$

(*ii*) $\exists$ *non-zero polynomial* $q(x) \in F[x]$ *s.t.,* $q(a) = 0$, *then* $p(x)$ *divides* $q(x)$,

(*iii*) $F(a) = F[a]$.

Proof: (*i*) Since a is algebraic over F, $\exists$ a non-zero polynomial $f(x) \in F[x]$, s.t.,

$$f(a) = 0.$$

Let $t(x)$ be the non-zero polynomial of smallest degree over F s.t., $t(a) = 0$ and suppose

$$t(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad a_i \in F$$

If $t(x)$ is not monic [By monic polynomial, we mean a polynomial in which coefficient of highest degree term is 1], then let

$$p(x) = a_n^{-1} a_0 + a_n^{-1} a_1 x + \ldots + x^n = a_n^{-1} t(x)$$

Now deg $p(x) = n$ = deg $t(x)$ and $p(a) = 0$ and $p(x)$ is a monic polynomial. Thus $\exists$ a monic polynomial $p(x)$ of least degree s.t., $p(a) = 0$.

Suppose $p(x) = p_1(x)p_2(x)$, where p_1 and p_2 are polynomials with lesser degree than deg p.

Then $$0 = p(a) = p_1(a)p_2(a)$$

$\Rightarrow$ $p_1(a) = 0$ or $p_2(a) = 0$ [as $F[a]$ is an Integral Domain]

But that would lead to a contradiction as $p(x)$ is such polynomial with least degree.

Hence $p(x)$ is irreducible polynomial.

To show uniqueness of $p(x)$, suppose $q(x)$ is any irreducible monic polynomial over F s.t., $q(a) = 0$. Since $F[x]$ is a Euclidean domain, $\exists$ $h(x)$ and $r(x)$ s.t., $q(x) = p(x)h(x) + r(x)$

where either $$r(x) = 0 \quad \text{or} \quad \deg r < \deg p$$

Now $0 = q(a) = p(a)h(a) + r(a)$

$\Rightarrow \quad r(a) = 0 \quad$ as $\quad p(a) = 0$

Since $p(x)$ is of least degree s.t., $p(a) = 0$, we find deg $r <$ deg p is not possible. Hence $r(x) = 0$

i.e., $q(x) = p(x)h(x)$ ...(1)

Since $q(x)$ is irreducible, $h(x)$ must be a constant polynomial, say $h(x) = c$

Then $q(x) = cp(x)$

Since $q(x)$ is monic, coefficient of highest degree term in L.H.S. is 1 and therefore it is 1 on R.H.S. also

R.H.S. being $cp(x) = ca_n^{-1}a_0 + ca_n^{-1}a_1x + ... + cx^n$ gives $c = 1$

Hence $q(x) = p(x)$, proving the uniqueness of $p(x)$

(*ii*) Follows by (1)

(*iii*) Define a mapping $\theta : F[x] \to F[a]$, s.t.,

$$\theta(f(x)) = f(a)$$

then θ is onto homomorphism (verify!)

By fundamental theorem then

$$F[a] \cong \frac{F[x]}{\text{Ker}\,\theta}$$

Since $F[a]$ is an integral domain, so would be $\dfrac{F[x]}{\text{Ker}\,\theta}$ which implies Ker θ is a prime ideal. Since a is algebraic over K, $\exists$ a *non-zero polynomial* $f(x) \in F[x]$ s.t. $f(a) = 0$.

$\Rightarrow \theta(f(x)) = f(a) = 0$

$\Rightarrow f(x) \in \text{Ker } \theta \Rightarrow \text{Ker } \theta \neq (0)$

i.e., Ker θ is a non-zero prime ideal of $F[x]$ which being a Euclidean domain is a PID.

Thus Ker θ is a maximal ideal. (See Problem 3 on Page 329)

$\Rightarrow \dfrac{F[x]}{\text{Ker}\,\theta}$ is a field.

$\Rightarrow F[a]$ is a field.

But $F(a)$ is the smallest field containing F and a and thus $F(a) \subseteq F[a]$

Also $F[a] \subseteq F(a)$

Hence $F(a) = F[a]$.

Note $F(a)$ is field of quotients of $F[a]$ and when $F[a]$ is itself a field, $F[a] = F(a)$.

Note: $p(x)$ determined in Theorem 4 is denoted by $p(x) = Irr(F, a)$. It is the unique monic irreducible polynomial over F satisfied by a. Since $p(x)$ is of least degree s.t. $p(a) = 0$, $p(x)$ is called the minimal polynomial for a.

where $$F(x) = \left\{ \frac{f(x)}{g(x)} \middle| f, g \in K[x], \underset{g \neq 0}{} \right\}.$$

Remark: If $a \in K$ is transcendental over F then $F(x) \cong F(a)$.

Proof: Define $\varphi : F(x) \to F(a)$ s.t.,

$$\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(a)}{g(a)},$$

Then φ is well defined onto homomorphism.

Also $\varphi\left(\frac{f(x)}{g(x)}\right) = 0$

$\Rightarrow \frac{f(a)}{g(a)} = 0$

$\Rightarrow f(a) = 0$

$\Rightarrow f(x) = 0$, for otherwise a would be algebraic over F.

$\Rightarrow \frac{f(x)}{g(x)} = 0$

$\Rightarrow \varphi$ is 1–1.

Hence $F(x) \cong F(a)$.

Cor. 1: Let $a \in K$ be algebraic over F. Then $[F(a) : F]$ = finite = deg *Irr* (F, a) and so $F(a)$ is an algebraic extension of F.

Proof: Let $p(x) = Irr\ (F, a)$. Let $n = \deg p(x)$.

We show that $1, a, a^2, ..., a^{n-1}$ form a basis of $F(a)$ over F.

Let $0 \neq f(a) \in F[a] = F(a)$. Then $f(x) \in F[x]$.

Now for $f(x)$, $p(x) \in F[x]$, $\exists\ q(x), r(x) \in F[x]$ s.t., $f(x) = p(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg r < \deg p$.

But $r(x) = 0 \Rightarrow f(x) = p(x)q(x)$

$\Rightarrow f(a) = p(a)q(a) = 0$ as $p(a) = 0$

which is not possible as $f(a) \neq 0$

Thus $r(x) \neq 0$. Hence $\deg r < \deg p$.

Suppose $r(x) = \beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1}$, $\beta_i \in F$, where some β_i could be zero.

Again as $f(a) = p(a)\ q(a) + r(a)$ and $p(a) = 0$

we find $f(a) = r(a)$

Thus $f(a) = \beta_0 + \beta_1 a + \beta_2 a^2 + ... + \beta_{n-1}a^{n-1}$

i.e., $\{1, a, a^2, ..., a^{n-1}\}$ spans $F[a] = F(a)$ over F.

We show these are *L.I.*

Suppose these are *L.D.*, then $\exists\ \gamma_i$, not all zero, s.t.,

$$\gamma_0 + \gamma_1 a + \gamma_2 a^2 + ... + \gamma_{n-1}a^{n-1} = 0$$

$\Rightarrow t(x) = \gamma_0 + \gamma_1 x + ... + \gamma_{n-1}x^{n-1}$ is non zero polynomial (some $\gamma_i \neq 0$) with $t(a) = 0$.

A contradiction to the fact that $p(x)$ is such polynomial with least degree. Hence $1, a, ..., a^{n-1}$ are *L.I.* and thus form a basis of $F(a)$.

Hence $[F(a) : F] = n$.

Remark: Using cor. to theorem 3 we conclude $a \in K$ is algebraic over F iff $[F(a) : F]$ = finite.

Definition: An element $a \in K$ is said to be *algebraic of degree n* over F if it satisfies a polynomial of degree n over F and does not satisfy any polynomial of lesser degree (than n).

Thus a is algebraic of degree n over F if deg $Irr\,(F, a) = n$. Also in that case, $[F(a) : F] = n$ and $\{1, a, a^2, ..., a^{n-1}\}$ is a basis of $F(a)$ over F.

Cor. 2: If $a_1, ..., a_n \in K$ are algebraic over F then $F(a_1, ..., a_n)$ is finite extension of F and so is algebraic over F.

Proof: We prove the result by induction on n. If $n = 1$, result follows from Cor. 1. Assume it to be true for naturals less than n. Let $a_1, ..., a_n \in K$ be algebraic over F. Now a_n is algebraic over $F \Rightarrow a_n$ is algebraic over $F(a_1, \ldots, a_{n-1})$ as $F \subseteq F(a_1, a_2, ..., a_{n-1})$.

$\therefore$ By Cor. 1, $[F(a_1, ..., a_{n-1})\,(a_n) : F(a_1, ..., a_{n-1})]$ is finite. By induction hypothesis, $[F(a_1, ..., a_{n-1}) : \mathrm{F}]$ is finite.

$\therefore$ $[F(a_1, ..., a_n) : F] = [F(a_1, ..., a_n) : F(a_1, ..., a_{n-1})]\ [F(a_1, ..., a_{n-1}) : F]$ = finite

$\therefore$ result is true for n also.

By induction, result is true for all $n \geq 1$.

Cor. 3: If $a, b \in K$ are algebraic over F, then $a \pm b$, ab, ab^{-1} (if $b \neq 0$) are algebraic over F. In other words, the elements of K which are algebraic over F form a subfield of K (and this subfield is called the *algebraic closure* of F over K).

Proof: By Cor. 2, $F(a, b)$ is algebraic over F.

$\therefore$ $a \pm b$, ab, $ab^{-1} \in F(a, b)$ are algebraic over F.

Remarks (1): If K is an extension field of a field F and $S \subseteq K$, then

$$F(S) = \left\{ \frac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)} \,\middle|\, \begin{array}{l} f, g \in F[x_1, ..., x_n] \\ g(u_1, ..., u_n) \neq 0, n \in \mathbf{N} \\ u_1, ..., u_n \in S \end{array} \right\}$$

Proof: Let L denote the R.H.S. We first show that L is a subfield of K.

Let $\quad \dfrac{f(u_1, ..., u_m)}{g(u_1, ..., u_m)} \in L, \ \dfrac{f_1(v_1, ..., v_n)}{g_1(v_1, ..., v_n)} \in L$

Let $\quad Y = \dfrac{f(u_1, ..., u_m)}{g(u_1, ..., u_m)} - \dfrac{f_1(v_1, ..., v_n)}{g_1(v_1, ..., v_n)}$

$$= \frac{f(u_1, ..., u_m)\, g_1(v_1, ..., v_n) - f_1(v_1, ..., v_n)\, g(u_1, ..., u_n)}{g(u_1, ..., u_m)\, g_1(v_1, ..., v_n)}$$

Define $\quad h(x_1, \ldots, x_{m+n})$

$= f(x_1, \ldots, x_m)\, g_1(x_{m+1}, \ldots, x_{m+n}) - g(x_1, \ldots, x_m)\, f_1(x_{m+1}, \ldots, x_{m+n})$

$r(x_1, \ldots, x_{m+n}) = g(x_1, \ldots, x_m)\, g_1(x_{m+1}, \ldots, x_{m+n})$

Then $$Y = \frac{h(u_1, ..., u_m, v_1, ..., v_n)}{r(u_1, ..., u_m, v_1, ..., v_n)} \in L$$

Suppose $$\frac{f_1(v_1, ..., v_n)}{g_1(v_1, ..., v_n)} \neq 0$$

Let $$Z = \frac{f(u_1, ..., u_m)}{g(u_1, ..., u_m)} \cdot \frac{g_1(v_1, ..., v_n)}{f_1(v_1, ..., v_n)}$$

Define $$h_1(x_1, \ldots, x_{m+n}) = f(x_1, \ldots, x_m)\, g_1(x_{m+1}, \ldots, x_{m+n});$$
$$r_1(x_1, \ldots, x_{m+n}) = g(x_1, \ldots, x_m)\, f_1(x_{m+1}, \ldots, x_{m+n}).$$

Then $$Z = \frac{h_1(u_1, ..., u_m, v_1, ..., v_n)}{r_1(u_1, ..., u_m, v_1, ..., v_n)} \in L$$

So, L is subfield of K.

Let $u_1 \in S$. Define $f(x) = x$, $g(x) = 1$.

Then $$f(u_1) = u_1,\ g(u_1) = 1$$

$$\Rightarrow \quad \frac{f(u_1)}{g(u_1)} \in L \quad \Rightarrow \quad \frac{u_1}{1} \in L \quad \Rightarrow \quad u_1 \in L$$

So, $S \subseteq L$.

Let $\alpha \in F$. Define $f(x) = \alpha$, $g(x) = 1$.

Let $u \in S$. Then $f(u) = \alpha$, $g(u) = 1$.

Now $$\frac{f(u)}{g(u)} \in L \quad \Rightarrow \quad \frac{\alpha}{1} = \alpha \in L.$$

So, $F \subseteq L$.

But $F(S)$ is the smallest field containing F and S, $F(S) \subseteq L$.

Let $Y \in L$. Then $Y = \frac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)}$, $u_i \in S$.

Since $u_i \in S$ and coefficients in f, g belong to F, $f(u_1, \ldots, u_n) \in F(S)$ and $g(u_1, \ldots, u_n) \in F(S)$.

So, $$Y \in F(S).$$

then $$L \subseteq F(S).$$

Hence $$F(S) = L.$$

(2) If K is an extension field of F, and K is generated by algebraic elements (*i.e.*, $K = F(S)$, where $S \subseteq K$ is a set of algebraic elements over K), then K is an algebraic extension of F.

Proof: Let $C \in K$, then $C = \frac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)}$, $u_i \in S$.

where $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$.

Clearly $C \in F(u_1, \ldots, u_n)$. But $u_1, \ldots, u_n$ are algebraic over $F \Rightarrow F(u_1, \ldots, u_n)$ is an algebraic extension of $F \Rightarrow C$ is algebraic over F.

Hence K/F is algebraic.

Theorem 5: *If L is an algebraic extension of K and K, an algebraic extension of F, then L is an algebraic extension of F.*

Proof: Let $a \in L$. Since L is algebraic over K, a is algebraic over K.

$\therefore \exists\ 0 \neq f(x) \in K[x]$ s.t., $f(a) = 0$. Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$, $\alpha_i \in K$.

Since K is algebraic over F, each $\alpha_i \in K$ is algebraic over F. By Cor. 2 Theorem 4, $[F(\alpha_0, \alpha_1, \ldots, \alpha_n) : F]$ = finite.

Let $M = F(\alpha_0, \alpha_1, \ldots, \alpha_n)$

Then $[M : F]$ is finite and so M is algebraic over F. Clearly, each $\alpha_i \in M$. Thus, $f(x) \in M[x]$.

i.e., a is algebraic over M.

By Cor. 1, $M(a)$ is finite extension of M.

$\Rightarrow$ $[M(a) : F] = [M(a) : M]\ [M : F]$ = finite.

$\Rightarrow$ $M(a)$ is algebraic over F.

$\Rightarrow$ $a \in M(a)$ is algebraic over F.

Since a is an arbitrary element of L, L is an algebraic extension of F.

Definition: A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

An algebraic number is said to be an *algebraic integer* if it satisfies an equation of the form $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ where $\alpha_1, \ldots, \alpha_n$ are integers (*i.e.* a monic polynomial over integers).

Problem 3: *If a is any algebraic number, prove that $\exists$ a +ve integer n such that na is an algebraic integer.*

Solution: Since a is an algebraic number, a is algebraic over the field of rationals. Thus $\exists$ a non-zero monic polynomial $f(x) \in \mathbf{Q}[x]$ s.t., $f(a) = 0$, where $\mathbf{Q}$ = field of rationals.

Let $f(x) = x^m + \alpha_1 x^{m-1} + \ldots + \alpha_{m-1} x + \alpha_m$, $\alpha_i \in \mathbf{Q}$

Let $\alpha_i = \dfrac{p_i}{q_i}$ where p_i, q_i are integers, $q_i > 0$

$$\therefore \quad a^m + \frac{p_1}{q_1} a^{m-1} + \ldots + \frac{p_{m-1}}{q_{m-1}} a + \frac{p_m}{q_m} = 0$$

Let $n = q_1 \ldots q_m$. Then n is a +ve integer

and $na^m + p_1 q_2 \ldots q_m a^{m-1} + \ldots + p_m q_1 \ldots q_{m-1} = 0$

$\Rightarrow$ $n^m a^m + p_1 q_2 \ldots q_m a^{m-1} n^{m-1} + \ldots + p_m q_1 \ldots q_{m-1} n^{m-1} = 0$

$\Rightarrow$ na satisfies the polynomial

$$x^m + p_1 q_2 \ldots q_m x^{m-1} + \ldots + p_m q_1 \ldots q_{m-1} n^{m-1} = 0$$

where coefficients are integers.

$\therefore$ na is an algebraic integer.

Problem 4: *If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.*

Solution: Let $r = \frac{p}{q}$, where $q > 0$, $(p, q) = 1$

Since r is an algebraic integer

$$r^m + \alpha_1 r^{m-1} + \ldots + \alpha_{m-1} r + \alpha_m = 0$$

α_is are integers.

$$\therefore \quad \frac{p^m}{q^m} + \alpha_1 \frac{p^{m-1}}{q^{m-1}} + \ldots + \alpha_{m-1} \frac{p}{q} + \alpha_m = 0$$

$\therefore p^m + q \times$ an integer $= 0$

$\Rightarrow$ q divides p^m. But $(p, q) = 1$.

$\therefore \quad q \mid 1 \Rightarrow \quad q = 1 \quad \Rightarrow \quad r = p =$ integer.

Problem 5: *Prove that sin m° is an algebraic number for every integer m.*

Solution: Now $e^{\pi mi/180} = \cos\frac{\pi m}{180} + i \sin\frac{\pi m}{180}$

$$\therefore \quad (e^{\pi mi/180})^{180} = \cos m\pi + i \sin m\pi = \pm 1$$

$\therefore e^{\pi mi/180}$ is a root of $x^{180} = \pm 1$

$\therefore e^{\pi mi/180}$ is an algebraic number for all integers m.

$\therefore \cos\frac{m\pi}{180} + i \sin\frac{m\pi}{180}$ is an algebraic number.

Also $\cos\frac{m\pi}{180} - i \sin\frac{m\pi}{180}$ is algebraic number (by putting m as $-m$).

$\therefore 2\cos\frac{m\pi}{180}$ is algebraic number for all integers m.

$\therefore \cos\frac{m\pi}{180}$ is algebraic number for all integers m.

$\therefore \cos m^\circ$ is algebraic number for all integers m.

Also $\cos\frac{m\pi}{180}$ and $\cos\frac{m\pi}{180} + i \sin\frac{m\pi}{180}$ is algebraic number $\Rightarrow i \sin\frac{m\pi}{180}$ is algebraic number

$\Rightarrow \sin\frac{m\pi}{180}$ is algebraic number as i is also algebraic number $\Rightarrow \sin m^\circ$ is algebraic number.

Problem 6: *Find a basis of* $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbf{Q}$.

Solution: We have

$$\begin{aligned}
[\mathbf{Q}(\sqrt{3}, \sqrt{5}) : \mathbf{Q}] &= [\mathbf{Q}(\sqrt{3})(\sqrt{5}) : \mathbf{Q}] \\
&= [\mathbf{Q}(\sqrt{3})(\sqrt{5}) : \mathbf{Q}(\sqrt{3})]\ [\mathbf{Q}\sqrt{3} : \mathbf{Q}] \\
&= [L(\sqrt{5}) : L]\ [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \text{ where } L = \mathbf{Q}(\sqrt{3}) \\
&= \text{deg } Irr\ (L, \sqrt{5}) \times \text{deg } Irr\ (\mathbf{Q}, \sqrt{3})
\end{aligned}$$

$$= \deg (x^2 - 5) \times \deg (x^2 - 3)$$
$$= 2 \times 2 = 4.$$

Thus basis has 4 elements.

Also if $[(F(a) : F)] = n$ then $1, a, a^2, ..., a^{n-1}$ is basis of $F(a)$ over F, and thus

Basis of $L(\sqrt{5})$ over L is $\{1, \sqrt{5}\}$

Basis of $\mathbf{Q}(\sqrt{3})$ over $\mathbf{Q}$ is $\{1, \sqrt{3}\}$

Thus basis of $[L(\sqrt{5}) : L]\ [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = [(\mathbf{Q}(\sqrt{3}, \sqrt{5}) : \mathbf{Q}]$

is $1.1,\ 1.\sqrt{3}\ ,\ 1.\sqrt{5}\ ,\ \sqrt{3}\sqrt{5}$ [see theorem 2]

i.e. $1,\ \sqrt{3}, \sqrt{5}, \sqrt{15}$.

Problem 7: *Find the minimal polynomial for* $\sqrt{2}+\sqrt{3}$ *and use it to show that* $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. *Find a basis for* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Solution: Now $(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$;

$$(\sqrt{2}+\sqrt{3})^4 = 49 + 20\sqrt{6}\ .$$

So, $(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$

Therefore, $a = \sqrt{2}+\sqrt{3}$ satisfies

$f(x) = x^4 - 10x^2 + 1$ over $\mathbf{Q}$.

Let $p(x) = Irr(\mathbf{Q}, a)$

Then $\sqrt{2}-\sqrt{3},\ -\sqrt{2}+\sqrt{3},\ -\sqrt{2}-\sqrt{3}$ are also roots of $p(x)$. So, degree of $p(x)$ is at least 4. But $f(a) = 0$ and $f(x) \in \mathbf{Q}[x]$

$$\Rightarrow p(x) \text{ divides } f(x)$$
$$\Rightarrow p(x) = f(x).$$

So, $f(x)$ is the minimal polynomial for $\sqrt{2}+\sqrt{3}$.

Therefore, $[\mathbf{Q}(\sqrt{2}+\sqrt{3}) : \mathbf{Q}] = 4.$

Also, $[\mathbf{Q}\sqrt{2} : \mathbf{Q}] = \deg\ Irr\ (\mathbf{Q},\ \sqrt{2}\ )$
$= \deg\ (x^2 - 2) = 2.$

Now, $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}\ ) \subseteq \mathbf{Q}(\sqrt{2}\ ,\ \sqrt{3}\ ).$

Consider $g(x) = x^2 - 3 \in \mathbf{Q}(\sqrt{2}\ )\ [x].$

Then $g(\sqrt{3}\ ) = 0$

$\therefore$ $\deg\ Irr\ (\mathbf{Q}(\sqrt{2}\ ),\ \sqrt{3}\ ) \leq \deg\ g(x) = 2$

$\Rightarrow$ $[(\mathbf{Q}(\sqrt{2}\ ,\ \sqrt{3}\ ) : \mathbf{Q}] \leq 2.$

So, $[\mathbf{Q}(\sqrt{2}\ ,\ \sqrt{3}\ ) : \mathbf{Q}] \leq 4.$

Clearly, $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}\ +\ \sqrt{3}\ ) \subseteq \mathbf{Q}(\sqrt{2}\ ,\ \sqrt{3}\ ).$

$\therefore \quad [\mathbf{Q}(\sqrt{2}, \sqrt{3})] : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2} + \sqrt{3})] \times [\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}]$

$\Rightarrow \quad [\mathbf{Q}(\sqrt{2}, \sqrt{3})] : \mathbf{Q}(\sqrt{2} + \sqrt{3})] = 1$

$\Rightarrow \quad \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$

Since $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}] = 4$

$\{1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3\}$ is a basis for $\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$.

Problem 8: *Let $F(x)$ be the field of rational functions in an indeterminate x. Show that every element of $F(x)$ which is not in F is transcendental over F.*

Solution: Let $0 \neq \frac{f}{g} \in F(x), \frac{f}{g} \notin F, \quad (f, g) = 1.$

Suppose $\frac{f}{g}$ is not transcendental over F.

Then $\frac{f}{g}$ is algebraic over F.

So $F\left(\frac{f}{g}\right) = F\left[\frac{f}{g}\right].$

Consider $\frac{g}{f} \in F\left[\frac{f}{g}\right] = F\left(\frac{f}{g}\right).$

(Note $0 \neq \frac{f}{g} \in F\left[\frac{f}{g}\right]$ and $F\left[\frac{f}{g}\right]$ is a field, $\frac{g}{f} \in F\left(\frac{f}{g}\right) = F\left[\frac{f}{g}\right]$)

Therefore, $\frac{g}{f} = \alpha_0 + \alpha_1 \left(\frac{f}{g}\right) + ... + \alpha_n \left(\frac{f}{g}\right)^n, \ \alpha_i \in F.$

So, $g^{n+1} = (\alpha_0 g^n + \alpha_1 f g^{n-1} + ... \ a_n f^n) \ f.$

Since $(f, g) = 1, \ f \mid g^{n+1} \Rightarrow f \mid g \Rightarrow f =$ unit

$\Rightarrow \quad g =$ unit $\Rightarrow \frac{f}{g} =$ unit $\in F$, a contradiction.

So, $\frac{f}{g}$ is transcendental over F.

Problem 9: *Let K be an extension of F and let $a \in K$. Then $F[a]$ can be regarded as a vector space over F. If the dimension of $F[a]$ over F is finite, show that $F[a] = F(a)$.*

Solution: Let $0 \neq c \in F[a]$. Define

$T : F[a] \to F[a]$ s.t.,

$T(b) = bc$

Then T is a linear transformation.

Let $b \in \text{Ker } T$. Then $T(b) = 0 \Rightarrow bc = 0 \Rightarrow b = 0$ as $c \neq 0$ and $F[a]$ is an integeral domain.

Thus Ker $T = \{0\}$ forcing T to be 1–1.

Since $F[a]$ is a FDVS over F, T is also onto.

Now $1 \in F[a] \Rightarrow \exists\ b \in F[a]$ st., $T(b) = 1$

$\Rightarrow bc = 1$ or that c is invertible.

So $F[a]$ is a field containing F and a. But $F(a)$ is the smallest field containing F & a and so $F(a) \subseteq F[a]$, However $F[a] \subseteq F(a)$ giving $F[a] = F(a)$.

Problem 10: *Let K be an extension of F. Show that K/F is algebraic if and only if every ring R, such that $F \subseteq R \subseteq K$ is a field.*

Solution: Let K/F be algebraic and let R be a ring s.t., $F \subseteq R \subseteq K$.

Since $R \subseteq K$, R will be commutative and also unity of K will be unity of R as $F \subseteq R \subseteq K$.

Let $0 \neq a \in R$, then $a \in K \Rightarrow a^{-1} \in K$

K/F algebraic $\Rightarrow$ a is algebraic over F.

$\Rightarrow \exists\ 0 \neq f(x) \in F(x)$ s.t., $f(a) = 0$

Let $f(x) = \alpha_0 + \alpha_1 x + \ldots\ldots + \alpha_n x^n$, $\alpha_i \in F$

Then $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots\ldots + \alpha_n a^n = 0$ with some $\alpha_i \neq 0$. Suppose $\alpha_o \neq 0$

Then $\alpha_0 a^{-1} = -(\alpha_1 + \alpha_2 a + \ldots + \alpha_n a^{n+1}) \in R$

$\Rightarrow \quad a^{-1} \in R$ as $\alpha_0^{-1} \in F \subseteq R$

So, every non zero element is invertible in R.

Conversely, let $a \in K$. Let $R = F[a]$, then R is a ring s.t., $F \subseteq R \subseteq K$. By hypothesis R is a field.

Suppose $a \neq 0$, then $a^{-1} \in R = F[a]$

Thus $a^{-1} = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n, \quad \alpha_i \in F$

Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x]$

Now $1 = \alpha_0 a + \alpha_1 a^2 + \ldots + \alpha_n a^{n+1}$

gives $\alpha_0 a + \alpha_1 a^2 + \ldots + \alpha_n a^{n+1} - 1 = 0$

showing that a satisfies $x f(x) - 1 \in F[x]$.

Clearly $x f(x) - 1$ is a non zero polynomial.

Hence, a is algebraic over F and so K/F is algebraic.

Exercises

1. If $a, b \in K$ are algebraic over F of degrees m and n respectively and if m and n are relatively prime, prove that $F(a, b)$ is of degree mn over F.
2. If $a \in K$ is algebraic over F of odd degree, show that $F(a) = F(a^2)$.

3. Show that degree of $\sqrt{2}+\sqrt{3}$ over $\mathbf{Q}$ is 4 and degree of $\sqrt{2}+\sqrt[3]{5}$ over $\mathbf{Q}$ is 6.

4. If a is an algebraic integer and m is an ordinary integer, prove

(i) $a + m$ is an algebraic integer.

(ii) ma is an algebraic integer.

5. Prove that sum and product of two algebraic integers is an algebraic integer.

6. Find a basis of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$. $[1, \sqrt{2}, \sqrt{3}, \sqrt{6}]$

7. Let K be an extension of F. Suppose E_1, E_2 are contained in K and are extensions of F. If $[E_1 : F]$ and $[E_2 : F]$ are primes, show that either $E_1 \cap E_2 = F$ or $E_1 = E_2$.

8. If K is an extension of F, $c \in K$, $a, b \in F$, $a \neq 0$ then show that $F(c) = F(ac + b)$.

9. Suppose that a field F has finite number of elements q. Show that

(i) $q = p^n$ for some prime p and integer n.

(ii) $a^q = a$ for all $a \in F$.

(iii) If $b \in K$ is algebraic over F, then $b^{q^m} = b$ for some $m > 0$.

10. Let K be a finite extension of F. Suppose if F_1 and F_2 are any two subfields of K s.t., $F \subseteq F_1$ and $F \subseteq F_2$ then either $F_1 \subseteq F_2$ or $F_2 \subseteq F_1$. Show that K will be a simple extension of F.

Roots of Polynomials

Let F be a field and $f(x) \in F[x]$. We ask ourselves whether there exists an extension K of F containing a root (Definition on page 448) of $f(x)$? What is the degree of such an extension? How many roots of $f(x)$ can the extension K of F have? The answers to the above queries are provided by the following results.

Theorem 6: (Remainder theorem). *If $p(x) \in F[x]$ and K is an extension of F, then for any element $a \in K$, $p(x) = (x - a)\, q(x) + p(a)$ where $q(x) \in K[x]$ and deg $q(x)$ = deg $p(x) - 1$.*

Proof: Now $p(x) \in F[x] \Rightarrow p(x) \in K[x]$. Also $a \in K \Rightarrow x - a \in K[x]$. By the division algorithm for polynomials in $K[x]$,

$p(x) = (x - a)\, q(x) + r(x)$ where $q(x) \in K[x]$ and $r(x) \in K[x]$ s.t., $r(x) = 0$ or deg $r(x) <$ deg $(x - a) = 1$. Thus $r(x)$ is a constant. Let $r(x) = c \in K$.

Now $p(x) = (x - a)\, q(x) + c$

$\Rightarrow$ $p(a) = c$

$\Rightarrow$ $p(x) = (x - a)\, q(x) + p(a)$ (where $p(a)$ could be zero).

Clearly deg $q(x)$ = deg $p(x) - 1$

Cor.: If $a \in K$ is a root of $p(x) \in F[x]$ where $F \subseteq K$, then $(x - a) \mid p(x)$ in $K[x]$ and conversely.

Proof: By above theorem,

$$p(x) = (x - a)\, q(x) + r, \quad r \in K$$

$$\Rightarrow \quad 0 = p(a) = r$$

$$\Rightarrow \quad p(x) = (x - a)\, q(x)$$

$(x - a) \mid p(x)$ in $K[x]$ as $q(x) \in K[x]$.

Conversely, if $(x - a) \mid p(x)$ in $K[x]$ then $p(x) = g(x)\,(x - a)$ for some $g(x) \in K[x]$. Thus $p(a) = (a - a)\, g(a) = 0$ and so a is a root of $p(x)$.

Definition: An element $a \in K$ is called a root of $p(x) \in F[x]$ of *multiplicity m* if $(x - a)^m \mid p(x)$ and $(x - a)^{m+1} \nmid p(x)$ in $K[x]$.

If a is a root of $p(x)$ of multiplicity 1 then it is called a *simple root* of $p(x)$. It is called a *multiple root* otherwise (when $m > 1$).

Remark: If a is a root (of multiplicity m) of $p(x)$ then $(x - a)^m \mid p(x) \Rightarrow p(x) = (x - a)^m\, g(x)$, for some $g(x)$.

Now if a is also a root of $g(x)$ then $(x - a) \mid g(x)$

$\Rightarrow \qquad g(x) = (x - a)\, h(x)$

$\Rightarrow \qquad p(x) = (x - a)^{m+1} h(x) \Rightarrow (x - a)^{m+1} \mid p(x)$, a contradiction.

Thus $g(a) \neq 0$.

Indeed, if a is a simple root of $p(x)$, then $p(x) = (x - a)\, g(x)$ where $g(a) \neq 0$.

Theorem 7: *A polynomial of degree n over a field can have at most n roots in any extension field. A root of multiplicity m to be counted m times.*

Proof: Let $p(x) \in F[x]$, degree $p(x) = n$. We prove the result by induction on n. Let K be an extension of F. Let $n = 1$. Then $p(x)$ is of the form $ax + b$, $a, b \in F$, $a \neq 0$. Then $p(\alpha) = 0 \Rightarrow \alpha = -ba^{-1}$. So, $p(x)$ has unique root $-ba^{-1} \in F$. Therefore K also has only one root of $p(x)$. So, result is true for $n = 1$. Assume it to be true for naturals less than n. Let deg $p(x) = n$. If $p(x)$ has no root in K, then result is true. Let α be a root of $p(x)$ in K. Let α be of multiplicity m. Then by definition, $(x - \alpha)^m \mid p(x)$.

$\therefore\ p(x) = (x - \alpha)^m\, q(x)$. Since $(x - \alpha)^{m+1} \nmid p(x)$, $(x - \alpha) \nmid q(x)$. So α is not a root of $q(x)$. If $\beta \neq \alpha$ is a root of $p(x)$ in K, then $0 = (\beta - \alpha)^m\, q(\beta) \Rightarrow q(\beta) = 0 \Rightarrow \beta$ is a root of $q(x)$. So, any root of $p(x)$ different from α in K is also a root of $q(x)$. But deg $q(x) = n - m < n$. By induction hypothesis K has at most $n - m$ roots of $q(x)$. So, K has at most $(n - m) + m = n$ roots of $p(x)$. Therefore, result is true for n. By induction result is true for all $n \geq 1$.

Remark: It must be noted that above theorem may not hold if we consider a polynomial over a ring which is not a field.

For example, $f(x) = x^2 + 1$ has at least 6 roots namely $\pm i, \pm j, \pm k$ in the ring of real quaternions which is not a field.

We now show that a non-constant polynomial over a field has a root in some field extension.

Theorem 8: *Let $p(x)$ be a non constant irreducible polynomial of degree n in $F[x]$. Then there exists an extension K of F s.t., $[K : F] = n$ and K has a root of $p(x)$.*

Proof: Since $p(x)$ is irreducible polynomial in $F[x]$ it will be an irreducible element (See Remark on page 450) and thus the ideal $M = \langle p(x) \rangle$ is maximal ideal of $F[x]$ and $\dfrac{F[x]}{M}$ will be a field.

Take $K = \dfrac{F[x]}{M}$.

Define $\theta : F \to K$, s.t.,

$\theta(\alpha) = \alpha + M$

Then θ is easily seen to be a homomorphism.

Again, $\alpha \in \text{Ker } \theta \Rightarrow \theta(\alpha) = 0 + M$

$\Rightarrow \alpha + M = M \quad \Rightarrow \quad \alpha \in M = < p(x) >$

and so $\alpha = p(x)q(x)$ for some $q(x) \in F[x]$

Since p is irreducible (with deg ≥ 1) and $\alpha \in F$ is either zero or a constant polynomial, we observe that the above relation holds only when $\alpha = 0$

i.e., Ker $\theta = \{0\}$ or that θ is 1–1.

Hence $F \cong \theta(F)$.

Define now $\psi : F[x] \to K$, s.t.,

$$\psi(f(x)) = f(x) + M \quad \left(K = \frac{F[x]}{M} \right)$$

Then ψ is the natural (onto) homomorphism.

Again as $\psi(\alpha) = \alpha + M = \theta(\alpha) \quad \forall\ \alpha \in F$, we notice θ is restriction of ψ over F.

Now $x = 0 + 1 \,.\, x + 0 \,.\, x^2 + \ldots \in F[x]$

Let $a = \psi(x) = x + M = x + <p(x)>, \quad x \in F[x]$ ...(1)

We claim, a is a root of $p(x)$ in K.

Suppose $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n, \quad \alpha_i \in F$

Then $\psi(p(x)) = \psi(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n)$

$= \psi(\alpha_0) + \psi(\alpha_1)\ \psi(x) + \psi(\alpha_2)\psi(x^2)$

$+ \ldots + \psi(\alpha_n)\psi(x^n)$

Also $\psi(p(x)) = p(x) + M = p(x) + <p(x)> = M = \text{Zero of } K$

Thus Zero of $K = \psi(\alpha_0) + \psi(\alpha_1)\psi(x) + \ldots + \psi(\alpha_n)\psi(x^n)$

$= \theta(\alpha_0) + \theta(\alpha_1)\psi(x) + \ldots + \theta(\alpha_n)\psi(x^n)$

Since $F \cong \theta(F)$, F is isomorphic to a subfield of K and we can think of K as containing F by identifying $\alpha \in F$ with $\theta(\alpha)$ and vice versa.

We thus get

Zero of $K = \alpha_0 + \alpha_1 \psi(x) + \alpha_2 \psi(x^2) + \ldots + \alpha_n(\psi(x^n))$

$= \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n$ from (1)

$= p(a)$

Hence a is a root of $p(x)$ in K.

We show now $\{1 + M, x + M, x^2 + M..., x^{n-1} + M\}$ forms a basis of K over F.

Let $\beta_0(1 + M) + \beta_1(x + M) + \ldots + \beta_{n-1}(x^{n-1} + M) = M$ (Zero of K)

As above then $\beta_i = \theta(\beta_i) = \beta_i + M$ and thus

$(\beta_0 + M)(1 + M) + (\beta_1 + M)(x + M) + \ldots + (\beta_{n-1} + M)(x^{n-1} + M) = M$

or $(\beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_{n-1} x^{n-1}) + M = M$

or $q(x) + M = M$ where $q(x) = \beta_0 + \beta_1 x + \ldots + \beta_{n-1} x^{n-1}$

or $q(x) \in M = \langle p(x) \rangle$

$\Rightarrow q(x) = p(x)h(x)$

$\Rightarrow \deg q = \deg p + \deg h$

$\Rightarrow \deg q \geq \deg p$

or that $n - 1 \geq n$, which leads us to a contradiction, unless $q(x) = 0$

i.e., $\beta_i = 0 \quad \forall i$

and hence $1 + M$, $x + M$, ..., $x^{n-1} + M$ are linearly independent.

Let now $f(x) + M \in K$ be any member.

Since $f(x)$, $p(x) \in F[x]$, $\exists\ t(x)$, $r(x)$ s.t.,

$$f(x) = p(x)t(x) + r(x), \text{ where either } r(x) = 0 \text{ or } \deg r(x) < \deg p(x)$$

$$\Rightarrow \quad f + M = (pt + r) + M = (p + M)(t + M) + (r + M)$$
$$= M(t + M) + (r + M) = M + (r + M) = r + M$$

Suppose $r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$ where, of course, some or all r_i could be zero as either $r(x) = 0$ or $\deg r(x) < \deg p(x)$

Thus $f + M = r + M = (r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}) + M$

$= (r_0 + M) + (r_1 x + M) + \ldots + (r_{n-1} x^{n-1} + M)$

$= (r_0 + M)(1 + M) + (r_1 + M)(x + M) + \ldots + (r_{n-1} + M)(x^{n-1} + M)$

$= r_0(1 + M) + r_1(x + M) + \ldots + r_{n-1}(x^{n-1} + M)$

[because of $F \cong \theta(F)$]

or that $1 + M$, $x + M$, ..., $x^{n-1} + M$ span K

Hence $[K : F] = n$.

Cor.: If $f(x) \in F[x]$ is of degree n, then there is a finite extension K of F in which $f(x)$ has a root. Also, $[K : F] \leq \deg f(x)$.

Proof: If $f(x)$ is irreducible polynomial then result follows by above theorem. If not then let $f(x) = p(x)\, q(x)$, where $p(x)$ is irreducible. By above theorem $\exists$ an extension K of F in which $p(x)$ has a root.

$\therefore\ p(\alpha) = 0$ for some $\alpha \in K$. So, $f(\alpha) = p(\alpha)\, q(\alpha) = 0 \Rightarrow \alpha$ is a root of $f(x)$. Also $[K : F] = \deg p(x) \leq \deg f(x)$.

Remark: The construction of an extension of K in which a given polynomial f has a root is not, in general, unique. Let $f = x^4 - 4$ over $\mathbf{Q}$. Then $f = (x^2 - 2)(x^2 + 2)$ and $\exists$ two non-isomorphic extensions $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2i})$ containing a root of f.

For if, σ is an isomorphism from $\mathbf{Q}(\sqrt{2})$ to $\mathbf{Q}(\sqrt{2i})$, then $\sigma(1) = 1 \Rightarrow \sigma(a) = a$ for all $a \in \mathbf{Q}$. So $(\sigma(\sqrt{2}))^2 = \sigma(\sqrt{2})^2 = \sigma(2) = 2$

$$\Rightarrow \sigma(\sqrt{2}) \text{ is a zero of } x^2 - 2$$

$$\Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$$

$$\Rightarrow Im\ \sigma = \mathbf{Q}(\sqrt{2})$$

$$\Rightarrow \mathbf{Q}(\sqrt{2}i) = \mathbf{Q}(\sqrt{2})$$

$$\Rightarrow \sqrt{2}i \in \mathbf{Q}(\sqrt{2})$$

$$\Rightarrow \sqrt{2}i \text{ is a real number, which is not true.}$$

Therefore, $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2}i)$ are non-isomorphic.

In the next result we determine the degree of extension which contains all roots of a given polynomial.

Theorem 9: *Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then $\exists$ an extension K of F s.t. $[K : F] \leq n!$ and K has n roots of $f(x)$.*

Proof: We prove the result by induction on n. If $n = 1$, then $f(x) = \alpha x + \beta$, $\alpha \neq 0$, $\alpha, \beta \in F$ has only one root $-\beta\alpha^{-1} \in F$. Thus $K = F$ and $[K : F] = 1 = n$. So, result is true for $n = 1$. Assume it to be true for naturals less than n. Let $\deg f(x) = n > 1$. Then by above cor. $\exists$ an extension L of F containing a root α of $f(x)$ and $[L : F] \leq n$. Let $f(x) = (x - \alpha)q(x)$, $\deg q(x) = n - 1$, $q(x) \in L[x]$. By induction hypothesis $\exists$ an extension K of L containing all $n - 1$ roots of $q(x)$ and $[K : L] \leq (n - 1)!$

$$\therefore \qquad [K : F] = [K : L][L : F] \leq n\,(n - 1)! = n!$$

Also $\alpha \in L \Rightarrow \alpha \in K \Rightarrow K$ has all n roots of $f(x)$. (The $n - 1$ roots of $q(x)$ are also roots of $f(x)$). So, result is true for n. By induction, result is true for all $n \geq 1$.

In the next section, we shall study the smallest field containing all roots of $f(x)$. This field will be called a splitting field of $f(x)$.

We now give an example of an algebraic extension which is not a finite extension.

Example 1: Let K be the field of complex numbers and F, the field of rationals.

Let K_a be the set of all elements of K which are algebraic over F.

Then K_a is a subfield of K and $F \subseteq K_a$. By def., K_a is an algebraic extension of F. Suppose $[K_a : F] = n$.

Let $$f(x) = x^{n+1} - 3 \in F[x]$$

By Eisenstein criterion, $f(x)$ *is irreducible* over $\mathbf{Q} = F$. Let α be a root of $f(x)$ in K. Then α is algebraic over $F = \mathbf{Q}$. So, $\alpha \in K_a$.

Since $$[F(\alpha) : F] = \deg Irr\ (F, \alpha) = \deg f(x) = n + 1,$$

$$[K_a : F] = [K_a : F(\alpha)]\ [F(\alpha) : F] = [K_a : F(\alpha)]\ (n + 1)$$

$\therefore\ n = [K_a : F(\alpha)]\ (n + 1)$, which is not possible.

Hence $[K_a : F]$ is not finite.

Splitting Fields

Let K be an extension of a field F and suppose $f(x) \in F[x]$ can be expressed as product of linear factors in $K[x]$.

i.e., $f(x) = c(x - a_1)(x - a_2) \ldots (x - a_n)$, $c \in F$, $a_i \in K$ then we say that $f(x)$ splits up in $K[x]$ (or splits over K) and K is called a splitting field of $f(x)$ over F. Further K is called minimal splitting field of $f(x)$ over F if $f(x)$ can be expressed as product of linear factors in $K[x]$ and it cannot be so factored over any proper subfield of K. Thus in above case $F(a_1, a_2, \ldots, a_n)$ is minimal splitting field of $f(x)$ over F.

We will show that splitting fields always exist and the minimal splitting fields are unique upto isomorphism, *i.e.* if $\exists$ more than one minimal splitting field then these are isomorphic. Sometimes (when there is no chance of confusion) the word minimal is dropped and we simply talk of splitting fields.

Note: If $f \in k[x]$ splits in $k[x]$, then k is the only minimal splitting field of f over k. For, let $f = c(x - a_1)(x - a_2) \ldots (x - a_n)$, $a_i \in k$. If f splits in any extension K of k then the roots of f in K will also be $a_1, a_2, \ldots, a_n$. So, $k(a_1, a_2, \ldots, a_n) = k$ is the only minimal splitting field of f over k.

Splitting field of a polynomial over a field depends on both the polynomial as well as the field and that is why it is essential to mention splitting field of $f(x)$ *over* F. Take for instance, $f(x) = x^2 + 1 \in \mathbf{Q}[x]$, then as $x^2 + 1 = (x + i)(x - i)$, we find splitting field of $f(x)$ over $\mathbf{Q}$ will be $\mathbf{Q}(i)$. However if $f(x) = x^2 + 1$ is taken as a polynomial over $\mathbf{R}$ then its splitting field over $\mathbf{R}$ is $\mathbf{R}(i) = \mathbf{C}$ the field of complex numbers.

Theorem 10: *Let k be a field and $f(x)$, a non zero polynomial in $k[x]$. Then there exists a splitting field of f over k. Further if deg $f = n$, then any minimal splitting field E of f over k satisfies $[E : k] \leq n!$*

Proof: We prove the result by induction on deg $f = n$.

Let $n = 1$. Then $f = \alpha x + \beta, \quad \alpha, \beta \in k.$

$$= \alpha(x + \beta\alpha^{-1}).$$

So, f splits in $k[x]$.

Assume that the result is true for all polynomials of degree $< n$. Let deg $f = n$. If $f = gh$, $g, h \in k[x]$, then deg g, $h < n$. By induction hypothesis, $\exists$ an extension K of k s.t., g splits in $K[x]$. Now $h \in k[x] \subseteq K[x]$. Again, by induction hypothesis $\exists$ an extension E of K s.t. h splits in $E[x]$. So, both g and h split in $E[x]$. Thus f splits in $E[x]$ where $E \supseteq K \supseteq k$. If f is irreducible, then $\exists$ an extension K of k s.t., $f(\alpha) = 0$ for some $\alpha \in K$.

Now $f(x) = (x - \alpha)\, g(x), \quad g(x) \in K[x]$.

Since deg $g < n$, by induction hypothesis $\exists$ an extension E of K s.t., $g(x)$ splits in $E[x]$. So $f(x)$ splits in $E[x]$ as $(x - \alpha) \in K[x] \subseteq E[x]$. By induction, the result follows.

For the second part, note that if α is a zero of f, then

$$[k(\alpha) : k] = \deg Irr\ (k, \alpha)$$
$$\leq \deg f = n.$$

Let $f = \alpha_0(x - \alpha_1) \ldots (x - \alpha_n), \quad \alpha_i \in E.$

Then, $E = k(\alpha_1, \ldots, \alpha_n).$

Now, $[k(\alpha_1) : k] \leq n$

$$[k(\alpha_1, \alpha_2) : k(\alpha_1)] = \deg Irr\ (k(\alpha_1), \alpha_2)$$
$$\leq n - 1 \text{ as } f(x) = \alpha_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

$$\Rightarrow \quad f(x) = (x - \alpha_1)\, g(x)$$

where $g(x) = \alpha_0(x - \alpha_2)...(x - \alpha_n) \in k(\alpha_1)[x]$

In this way, $[k(\alpha_1, \alpha_2, ..., \alpha_r) : k(\alpha_1, \alpha_2, ..., \alpha_{r-1})] \leq n - (r - 1)$

Thus
$$[E : k] = [k(\alpha_1, \alpha_2, ..., \alpha_n) : k]$$
$$= [k(\alpha_1, \alpha_2, ..., \alpha_n) : k(\alpha_1, \alpha_2, ..., \alpha_{n-1})] \ ... \ [k(\alpha_1) : k]$$
$$\leq (n - (n + 1)) \ ... \ (n - 1)n = n!$$

which proves the second part.

Definition: Let E and L be two extensions of a field k. An isomorphism $f : E \to L$ is called a *k-isomorphism* if $f(a) = a \ \forall \ a \in k$ and in that case we say E and L are k-isomorphic. Similarly we talk of k-homomorphism or k-automorphism.

Theorem 11: *Let k_1, k_2 be two fields. Suppose $\sigma : k_1 \to k_2$ is an isomorphism and $f_1 \in k_1[x]$ is irreducible over k_1. Then*

$\sigma(f_1(x)) = \sigma(a_0 + a_1x + ... + a_nx^n) = \sigma(a_0) + \sigma(a_1)x + ... + \sigma(a_n)x^n$ *is irreducible over* k_2.

Proof: Suppose $\sigma(f_1(x)) = g_2h_2, \quad g_2, h_2 \in k_2[x]$.

Let
$$g_2 = b_o + b_1x + ... + b_rx^r$$
$$h_2 = c_o + c_1x + ... + c_sx^s, \quad b_i, c_j \in k_2.$$

Since σ is onto, given $b_i \in k_2 \ \exists \ b'_i \in k_1$ s.t., $\sigma(b'_i) = b_i$

Therefore, $g_2 = \sigma(b'_o) + ... + \sigma(b'_r)x^r$

Similarly $h_2 = \sigma(c'_o) + ... + \sigma(c'_s)x^s$.

So,
$$g_2 = \sigma(b'_o + b'_1x + ... + b'_rx^r) = \sigma(g'_2)$$
$$h_2 = \sigma(c'_o + c'_1x + ... + c'_sx^s) = \sigma(h'_2),$$

where g'_2 and $h'_2 \in k_1[x]$.

Thus $\sigma(f_1(x)) = \sigma(g'_2)\ \sigma(h'_2) = \sigma(g'_2h'_2)$.

So, $f_1 = g'_2h'_2$, contradicting the fact that f_1 is irreducible over k_1.

Hence $\sigma(f_1(x))$ is irreducible over k_2.

Theorem 12: *Suppose $\sigma : k_1 \to k_2$ is an isomorphism from a field k_1 to a field k_2.*

Let α_1 be a zero of an irreducible polynomial $f_1(x)$ over k_1 and α_2 be a zero of the corresponding polynomial $f_2(x) = \sigma(f_1(x))$ over k_2. Then there exists a unique isomorphism θ from $k_1(\alpha_1)$ to $k_2(\alpha_2)$ s.t., $\theta(\alpha_1) = \alpha_2$ *and* $\sigma(\alpha) = \alpha \ \forall \ \alpha \in k_1$.

Proof: Now $\varphi_1 : k_1[x] \to k_2[\alpha_1]$

with $\varphi_1(g_1(x)) = g_1(\alpha_1)$

is an onto homomorphism s.t., Ker $\varphi_1 = < f_1 >$.

So, $\theta_1 : \dfrac{k_1[x]}{< f_1 >} \to k_2[\alpha_1]$ is an isomorphism, where

$$\theta_1(< f_1 > + g_1(x)) = \varphi(g_1(x)) = g_1(\alpha_1).$$

Here $\theta_1(< f_1 > + x) = \alpha_1$.

Similarly $\exists$ an isomorphism

$$\theta_2 : \frac{k_2[x]}{< f_2 >} \to k_2[\alpha_2] \text{ s.t.,}$$

$$\theta_2(< f_2 > + g_2(x)) = g_2(\alpha_2).$$

Here $\theta_2(< f_2 > + x) = \alpha_2.$

Also $$\theta_3 : \frac{k_1[x]}{< f_1 >} \to \frac{k_2[x]}{< f_2 >} \text{ s.t.,}$$

$$\theta_3(< f_1 > + g_1) = < f_2 > + \sigma(g_1),$$

is well defined and is an isomorphism.

If $< f_1 > + g_1 = < f_1 > + g'_1,$

then $g_1 - g'_1 \in < f_1 >$

$\Rightarrow g_1 - g'_1 = 0$ or $\deg(g_1 - g'_1) \geq \deg f_1,$

But $\deg g_1 < \deg f_1,\ \deg g'_1 < \deg f_1$

$\Rightarrow \deg(g_1 - g_1') < \deg f_1$

$\Rightarrow g_1 - g'_1 = 0$

$\Rightarrow \sigma(g_1 - g'_1) = 0 \in < f_2 >$

$\Rightarrow \sigma(g_1) - \sigma(g'_1) \in < f_2 >$

$\Rightarrow < f_2 > + \sigma(g_1) = < f_2 > + \sigma(g'_1)$

$\Rightarrow \theta_3$ is well defined.

Here, $\theta_3(< f_1 > + x) = < f_2 > + x,$ as $\sigma(1) = 1.$

Hence, $$\theta_1^{-1} : k_1[\alpha_1] \to \frac{k_1[x]}{< f_1 >}$$

$$\theta_3 : \frac{k_1[x]}{< f_1 >} \to \frac{k_2[x]}{< f_2 >},\ \theta_2 : \frac{k_2[x]}{< f_2 >} \to k_2[\alpha_2]$$

are isomorphisms.

So, $\theta = \theta_2\theta_3\theta_1^{-1}$ is an isomorphism.

In fact, $\theta : k_1[\alpha_1] \to k_2[\alpha_2]$

and
$$\begin{aligned}\theta(\alpha_1) &= \theta_2\theta_3\theta_1^{-1}(\alpha_1)\\ &= \theta_2\theta_3\ (< f_1 > + x)\\ &= \theta_2(< f_2 > + x)\\ &= \alpha_2\end{aligned}$$

$$\begin{aligned}\theta(\alpha) &= \theta_2\theta_3\theta_1^{-1}(\alpha)\\ &= \theta_2\theta_3(< f_1 > + \alpha)\\ &= \theta_2(< f_2 >) + \sigma(\alpha)\\ &= \sigma(\alpha) \quad \forall\ \alpha \in k_1\end{aligned}$$

If $\varphi : k_1[\alpha_1] \to k_2[\alpha_2]$ is another isomorphism s.t., $\varphi(\alpha_1) = \alpha_2,\ \varphi(\alpha) = \sigma(\alpha)$ $\forall\ \alpha \in k_1,$

Then $\varphi(a_o + a_1\alpha_1 + \ldots + a_n\alpha_1^n)$

$= \varphi(a_o) + \varphi(a_1)\ \varphi(\alpha_1) + \ldots + \varphi(a_n)\ \varphi(\alpha_1^n), \quad a_i \in k,$

$= \sigma(a_o) + \sigma(a_1)\alpha_2 + \ldots + \sigma(a_n)\alpha_2^n.$

$= \theta(a_o) + \theta(a_1)\ \theta(\alpha_1) + \ldots + \theta(a_n)\ \theta(\alpha_1^n)$

$= \theta(a_o + a_1\alpha_1 + \ldots + \alpha_n\alpha_1^n)$

i.e. $\theta = \varphi$

and thus φ is uniquely determined.

Cor.: Let k be a field and $f(x) \in k[x]$ be irreducible over k. Let α, β be roots of $f(x)$. Then there exists a k-isomorphism θ from $k(\alpha)$ to $k(\beta)$ s.t., $\theta(\alpha) = \beta$ and θ is uniquely determined.

Follows by taking $k_1 = k_2 = k$ and $\sigma = I$ in the theorem.

Remark: The above result need not hold if $f(x)$ is not irreducible over k. For instance, if $f(x) = (x^2 - 2)(x^2 + 2)$, then $\sqrt{2}$ and $\sqrt{2}\,i$ are roots of $f(x) \in \mathbf{Q}[x]$ and $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{2}\,i)$ are not isomorphic. See remark after theorem 8.

Theorem 13: *Let k' be a field isomorphic to k, f' the polynomial over k' corresponding to f over k. If E, E' are minimal splitting fields of f over k and f' over k' respectively, then the given isomorphism between k and k' can be extended to an isomorphism between E and E'.*

Proof: Let $\sigma : k \to k'$ be an isomorphism. Let $[E : k] = n$. We prove the result by induction on n.

Let $n = 1$. Then $E = k$.

Let $f = \alpha_0(x - \alpha_1)\ldots(x - \alpha_m)$, $\alpha_i \in E$, $\alpha_0 \in k$.

Since $E = k$, $\alpha_i \in k$.

Therefore, $f' = \sigma(f) = \sigma(\alpha_0)\ (x - \sigma(\alpha_1))\ \ldots\ (x - \sigma(\alpha_m))$ splits in $k'[x]$.

So, $E' = k'$

Then, σ is an extension of σ and the result is true in this case.

Let $n > 1$. Let $f = p_1p_2\ldots p_r$, where each p_i is irreducible over k. Since $[E : k] > 1$, some p_i has degree greater than 1, say p_1.

Now $f' = \sigma(f) = \sigma(p_1)\ldots\sigma(p_r)$

$= p'_1\ldots p'_r$, $\sigma(p_i) = p'_i \in k'[x]$.

Let σ be a zero of p_1 in E and α', any zero of p'_1 in E'. Then by previous result, $\exists$ an isomorphism $\theta : k(\alpha) \to k'(\alpha')$ s.t., $\theta(b) = \sigma(b)\ \forall\ b \in k$, $\theta(\alpha) = \alpha'$. Now $p_1 = Irr\ (k, \alpha)$ and $\deg p_1 > 1 \Rightarrow [k(\alpha) : k] = \deg p_1 > 1$.

So, $[E : k] = [E : k(\alpha)]\ [k(\alpha) : k]$

$> [E : k(\alpha)]$.

Now, a minimal splitting field of f over $k(\alpha)$ is $k(\alpha)$ (Zeros of f in E) $= E$.

Also, a minimal splitting field of f' over $k'(\alpha')$ is $k'(\alpha')$ (Zeros of f' in E') $= E'$.

By induction hypothesis (Since $[E : k(\alpha)] < [E : k]$), $\exists$ an isomorphism.

$\psi : E \to E'$ s.t.

$$\psi(a) = \theta(a) \quad \forall\ a \in k(\alpha).$$

Also
$$\psi(b) = \theta(b) \quad \forall\ b \in k.$$
$$= \sigma(b) \qquad b \in k.$$

Therefore, ψ is an extension of σ. So, the result is true in this case. By induction the result is true for all $n \geq 1$.

Cor.: If E and E' are minimal splitting fields of f over k, then E and E' are k-isomorphic.

Proof: Take $k' = k$, σ = identity map I in above result. Then $\exists$ an isomorphism $\psi : E \to E'$ s.t., $\psi(a) = \sigma(a) = I(a) = a$, $a \in k$.

Problem 11: *Describe the splitting field of* $x^3 - 2$ *over* $\mathbf{Q}$, *the field of rationals.*

Solution: Let $f(x) = x^3 - 2$

Then by Eisenstein's criterion, $f(x)$ is irreducible over $\mathbf{Q}$. Since $f(x)$ is of odd degree, it has a real root, say a.

Then
$$x^3 - 2 = (x - a)(x^2 + ax + a^2)$$
$$= (x - a)(x - a\omega)(x - a\omega^2)$$

$$\text{where } \omega = \frac{-1 \pm \sqrt{3}\, i}{2}$$

So, splitting field of $f(x)$ over $\mathbf{Q}$ is
$$K = \mathbf{Q}(a, a\omega, a\omega^2)$$
$$= \mathbf{Q}(a, \omega)$$

w satisfies $g(x) = x^2 + x + 1$, $g(x)$ is irreducible over reals and so over $\mathbf{Q}(a)$.

Now
$$[K : \mathbf{Q}] = [\mathbf{Q}(a, \omega) : \mathbf{Q}(a)]\ [\mathbf{Q}(a) : \mathbf{Q}]$$
$$= [F(\omega) : F]\ [\mathbf{Q}(a) : \mathbf{Q}] \quad \text{where } F = \mathbf{Q}(a)$$
$$= \deg Irr\ (F, \omega) \times \deg Irr\ (\mathbf{Q}, a)$$
$$= \deg g(x) \times \deg f(x)$$
$$= 2 \times 3 = 6.$$

Problem 12: *Let* F *be a field of characteristic* p. *Let* b *be a root of* $f(x) = x^p - x - a \in F[x]$. *Show that splitting field of* $f(x)$ *over* F *is* $F(b)$.

Solution: Since b is a root of $f(x)$,
$$b^p - b = a \in K$$

Also
$$(b + 1)^p - (b + 1) = b^p + 1 - b - 1 = a$$

$\therefore$ $b + 1$ is a root of $f(x)$

Similarly $b + 2, \ldots, b + (p - 1)$ are roots of $f(x)$,

$\therefore$
$$f(x) = (x - b)(x - b - 1) \ldots\ldots (x - b - p + 1)$$

$\therefore$ Splitting field of $f(x)$ over F
$$= F(b, b + 1, \ldots, b + (p - 1)) = F(b).$$

Problem 13: Let $f(x) = x^4 + x^2 + 1 \in \mathbf{Q}[x]$. *Show that the splitting field of* $f(x)$ *over* $\mathbf{Q}$ *is* $\mathbf{Q}(\omega)$ *and* $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$.

Solution: We have

$$\omega^4 + \omega^2 + 1 = \omega + \omega^2 + 1 = 0$$

and $(\omega^2)^4 + (\omega^2)^2 + 1 = \omega^8 + \omega^4 + 1 = \omega^2 + \omega + 1 = 0$

$\Rightarrow \omega, \omega^2$ are roots of $f(x) = x^4 + x^2 + 1$

Also, $-\omega, -\omega^2$ are roots of $f(x)$

So, $f(x) = (x - \omega)(x + \omega)(x - \omega^2)(x + \omega^2)$

and splitting field of $x^4 + x^2 + 1$ over $\mathbf{Q}$ is

$$\mathbf{Q}(\omega, -\omega, \omega^2, -\omega^2) = \mathbf{Q}(\omega)$$

where $[\mathbf{Q}(\omega) : \mathbf{Q}] = \deg Irr(\mathbf{Q}, \omega)$

$= \deg (x^2 + x + 1) = 2.$

Problem 14: *Show that the splitting field of* $x^4 + 1$ *over* $\mathbf{Q}$ *is* $\mathbf{Q}(\sqrt{2}, i)$ *whose degree over* $\mathbf{Q}$ *is* 4.

Solution: Roots of $x^4 + 1$ are given by

$$x = (-1)^{1/4}$$
$$= (\cos(2r + 1)\pi + i \sin(2r + 1)\pi)^{1/4}$$
$$r = 0, 1, 2, 3$$
$$= \alpha, \alpha^3, \alpha^5, \alpha^7$$

where $\alpha = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$

$\therefore$ splitting field K of $x^4 + 1$ over $\mathbf{Q}$ is

$$K = \mathbf{Q}(\alpha, \alpha^3, \alpha^5, \alpha^7) = \mathbf{Q}(\alpha)$$

$\therefore$ $[K : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}]$

$= \deg Irr(\mathbf{Q}, \alpha)$

$= \deg (x^4 + 1) = 4.$

Notice, $f(x) = x^4 + 1$ gives $f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ which is irreducible by Eisenstein's criterion and thus $f(x)$ is irreducible over $\mathbf{Q}$.

Problem 15: *Find necessary and sufficient conditions on* a *and* b *so that the splitting field of irreducible cubic* $x^3 + ax + b$ *has degree* 3 *over* $\mathbf{Q}$.

Solution: Let $f(x) = x^3 + ax + b \in \mathbf{Q}[x]$

Let K be the splitting field of $f(x)$ over $\mathbf{Q}$. Let $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

Then $K = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$

Now $\alpha_1 + \alpha_2 + \alpha_3 = 0, \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = a$

$\alpha_1\alpha_2\alpha_3 = -b$

Let $D = [(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)]^2$

Then $D = -4a^3 - 27b^2$ (Prove it!)

Now $\mathbf{Q}(\sqrt{D}, \alpha_3) \subseteq K$

as $\alpha_1, \alpha_2, \alpha_3 \in K \Rightarrow \alpha_1 - \alpha_2, \alpha_2 - \alpha_3, \alpha_3 - \alpha_1 \in K$

$$\Rightarrow (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in K$$

$$\Rightarrow \sqrt{D} \in K. \text{ Also } \alpha_3 \in K$$

$$\Rightarrow \mathbf{Q}(\sqrt{D}, \alpha_3) \subseteq K$$

Now $\sqrt{D} = (\alpha_1 - \alpha_2)[\alpha_3(\alpha_1 + \alpha_2) - \alpha_3^2 - \alpha_1\alpha_2] \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

Since $\alpha_1\alpha_2 = -\dfrac{b}{\alpha_3} \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

and $\alpha_1 + \alpha_2 = -\alpha_3 \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

$$\alpha_1 - \alpha_2 \in \mathbf{Q}(\sqrt{D}, \alpha_3) \Rightarrow \alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D}, \alpha_3)$$

$\therefore$ $K \subseteq \mathbf{Q}(\sqrt{D}, \alpha_3)$

Suppose $\sqrt{D} \in \mathbf{Q}$. Then $K = \mathbf{Q}(\alpha_3)$

$\therefore$ $[K : \mathbf{Q}] = [\mathbf{Q}(\alpha_3) : \mathbf{Q}]$

$= \deg Irr\ (\mathbf{Q}, \alpha_3)$

$= \deg f(x) = 3$

Conversely, let $[K : \mathbf{Q}] = 3$

Let $\sqrt{D} \notin \mathbf{Q}$

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{D}) \subseteq \mathbf{Q}(\sqrt{D}, \alpha_3) = K$

But $\sqrt{D}$ satisfies $x^2 - D \in \mathbf{Q}[x]$

$\therefore$ $[\mathbf{Q}(\sqrt{D}) : \mathbf{Q}] = 2$ as $x^2 - D$ is irreducible over $\mathbf{Q}$.

$[K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{D})][\mathbf{Q}(\sqrt{D}) : \mathbf{Q}]$

$3 = [K : \mathbf{Q}(\sqrt{D})] = 2$, a contradiction

$\Rightarrow$ $\sqrt{D} \in \mathbf{Q}$

Hence a necessary and sufficient condition for the splitting field of irreducible cubic $x^3 + ax + b$ over $\mathbf{Q}$ to have degree 3 is $\sqrt{D} \in \mathbf{Q}$.

Problem 16: *Find the degree of a minimal splitting field of* $x^6 + 1$ *over* $\mathbf{Q}$.

Solution: Let $f(x) = x^6 + 1$

Then the roots of $f(x)$ are

$$\frac{\sqrt{3}}{2} + \frac{i}{2},\ \frac{-\sqrt{3}}{2} + \frac{i}{2},\ \frac{-\sqrt{3}}{2} - \frac{i}{2},\ \frac{\sqrt{3}}{2} - \frac{i}{2},\ i,\ -i.$$

Let E be a minimal splitting field of $f(x)$ over $\mathbf{Q}$. Then

$$E = \mathbf{Q}(\sqrt{3}, i)$$

and $[E : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}]$

$= [\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})]\ [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$

$$= \deg \mathit{Irr}\ (\mathbf{Q}(\sqrt{3}),\ i) \times \deg \mathit{Irr}\ (\mathbf{Q},\ \sqrt{3})$$
$$\leq 2 \times 2 \text{ as } \deg \mathit{Irr}\ (\mathbf{Q},\ \sqrt{3}) = \deg x^2 - 3 = 2$$

and i satisfies $x^2 + 1$ over $\mathbf{Q}(\sqrt{3})$.

So, $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 1$ or 2.

If $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 1$, then

$\mathbf{Q}(\sqrt{3}) = \mathbf{Q}(\sqrt{3}, i)$ which is not true as i does not belong to $\mathbf{Q}(\sqrt{3})$, the subfield of real numbers.

Therefore, $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 2$

Thus, $[E : \mathbf{Q}] = 4$.

Problem 17: *Find the degree of a minimal splitting of* $x^4 + 2$ *over* $\mathbf{Q}$.

Solution: Let $f(x) = x^4 + 2$.

The roots of $f(x)$ are

$$2^{1/4}\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)$$

If E is a minimal splitting field of $f(x)$ over $\mathbf{Q}$, then

$$E = \mathbf{Q}(2^{1/4}, i), \text{ as } (2^{1/4})^2 = \sqrt{2}.$$

Now
$$[E : \mathbf{Q}] = [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})]\ [\mathbf{Q}(2^{1/4}) : \mathbf{Q}]$$
$$= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})] \deg \mathit{Irr}\ (\mathbf{Q}, 2^{1/4})$$
$$= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})] \deg (x^4 - 2)$$
$$\leq \deg (x^2 + 1) \times \deg (x^4 - 2) = 8$$

$\therefore$ $[E : \mathbf{Q}] = 4$ or 8

If $[E : \mathbf{Q}] = 4$, then $[\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})] = 1$

$\Rightarrow$ $\mathbf{Q}(2^{1/4}, i) = \mathbf{Q}(2^{1/4}) \subseteq \mathbf{R}$, the field of reals

$\Rightarrow$ $i \in \mathbf{R}$ which is not true

Hence $[E : \mathbf{Q}] = 8$.

Problem 18: *Show that there is an irreducible polynomial of degree* 2 *over the field* $F_p = \{0, 1, 2, ..., p - 1\}$ *mod* p, *where* p *is a prime.*

Hence construct a field with p^2 *elements.*

Solution: Define $\theta : F_p \to F_p$, s.t.,

$$\theta(a) = a^2 \quad (p \neq 2)$$

Then $\theta(a) = \theta(-a) \Rightarrow \theta$ is not 1-1 as $a \neq -a$ in F_p.

Thus θ is not onto as F_p is finite.

So, $\exists\ b \in F_p$ s.t., $b \neq a^2 \quad \forall\ a \in F_p$

Then $f(x) = x^2 - b \in F_p[x]$ is irreducible over F_p and degree of $f(x)$ is 2.

Let α be a root of $f(x)$. Then

$$f(x) = Irr\ (F_p, \alpha)$$

and $$[F_p(\alpha) : F_p)] = \deg f(x) = 2$$

i.e., $$o(F_p(\alpha)) = p^2.$$

Suppose now $p = 2$. Then $g(x) = x^2 + x + 1$ is irreducible over F_2. If α is root of $g(x)$ then

$$[F_2(\alpha) : F_2] = \deg\ Irr\ (F_2, \alpha)$$
$$= \deg\ g(x) = 2.$$

i.e. $$o(F_2(\alpha)) = 2^2.$$

(See also theorem 67 on page 756).

Problem 19: *Show that a minimal splitting field over k for a polynomial of degree n is generated over k by any of n – 1 of its zeros.*

Solution: Let $f(x) \in k[x]$, $\deg f(x) = n$.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_o, \quad a_i \in k$

Let $E = k(\alpha_1, ..., \alpha_n)$ be a minimal splitting field of f over k.

Now, $$\sum \alpha_i = -\frac{a_{n-1}}{a_n} \in k \subseteq k(\alpha_1, \alpha_2, ..., \alpha_n) = E.$$

Therefore, $$\alpha_1 + \alpha_2 + ... + \alpha_n \in E \text{ and } \alpha_i \in E.$$

Let $$E' = k(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_n)$$

Now $$\alpha_i = -\frac{a_{n-1}}{a_n} - (\alpha_1 + .. + \alpha_{i-1} + \alpha_{i+1} + ... + \alpha_n)$$
$$\in E'$$

$\Rightarrow$ $E \subseteq E'$. But $E' \subseteq E$.

Therefore, $E = E'$, which is generated by $n - 1$ zeros of $f(x)$ over k.

Exercises

1. Find the degree of splitting field of $x^5 - 3x^3 + x^2 - 3$ over $\mathbf{Q}$. [4]

2. Find the splitting field of $x^p - 1$ over $\mathbf{Q}$, p being a prime number.

3. Find the splitting fields and their degrees of the following polynomials over $\mathbf{Q}$.
(*i*) $x^6 + 1$ (*ii*) $x^4 - 2$ (*iii*) $x^5 - 1$

(*i*) $\mathbf{Q}(\sqrt{3}, i)$, 4 (*ii*) $\mathbf{Q}(2^{1/4}, i)$, 8 (*iii*) $\mathbf{Q}(e^{2\pi i/5})$, 4

4. If E is an extension of F and $f(x) \in F[x]$ and if φ is an automorphism of E leaving every element of F fixed, prove that φ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.

5. Prove that $F(\sqrt[3]{2})$ where F is the field of rationals, has no automorphisms other than the identity automorphism.

6. Using exercise (4), prove that if the complex number α is a root of the polynomial $p(x)$ having real coefficients, then $\bar{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.

7. If F is the field of real numbers, prove that if φ is an automorphism of F then φ leaves every element of F fixed.

8. Find the degree of a minimal splitting field of $x^6 + 1$ over F_2 the field $\{0, 1\}$ mod 2.

(**Hint:** $x^6 + 1 = (x + 1)^2 (x^2 + x + 1)^2$

$= (x + 1)^2 (x + \alpha)^2 (x + \alpha^2)^2$

Let E be a minimal splitting field of $x^6 + 1$ over F_2.

Then $E = F_2(\alpha)$

amd $[E : F_2] = \deg Irr\ (F_2, \alpha) = x^2 + x + 1 = 2$

9. Find the degree of minimal splitting field of $x^6 + 1$ over $F_3 = \{0, 1, 2\}$ mod 3. [2]

10. Find the degree of minimal splitting field of $x^3 + x^2 + 1$ over $F_2 = \{0, 1\}$ mod 2. [3]

[**Hint**: Roots will be α, α^2, $1 + \alpha + \alpha^2$].

A Quick Look at what's been done

- If F is a subfield of a field K, then K is called an **extension** of F. If S is a non-empty subset of K, then $F(S)$ is used to denote the smallest subfield of K containing F and S.
- An extension K of F is called an **algebraic extension** if every $a \in K$ is algebraic over F(i.e., there exists a non-zero polynomial $f(x) \in F[x]$, s.t., $f(a) = 0$). A finite extension is algebraic. Converse is not true.
- A complex number is said to be **algebraic number** if it is algebraic over the field of rationals, and it is called an **algebraic integer** if it satisfies a monic polynomial over integers.
- **Remainder theorem** says that if K is an extension of F and $p(x) \in F[x]$ then for any $a \in K$, $p(x) = (x - a)q(x) + p(a)$ where $q(x) \in K[x]$ and $\deg q(x) = \deg p(x) - 1$.
- If K is an extension of F, then $a \in K$ is a root of $p(x) \in F[x]$ iff $(x - a) \mid p(x)$ in $K[x]$.
- A polynomial of degree n over a field can have at most n roots in any extension field. A root of multiplicity m to be counted m times.
- If $p(x)$ is a non constant irreducible polynomial of degree n in $F[x]$ then there exists an extension K of F, s.t., $[K : F] = n$ and K has a root of $p(x)$.
- If $f(x) \in F[x]$ is of degree $n \geq 1$ then there exists an extension K of F, s.t., $[K : F] \leq n!$ and K has n roots of $f(x)$.
- Suppose K is an extension of F and $f(x) \in F[x]$. We say that $f(x)$ splits in K if it can be expressed as a product of linear factors in $K[x]$ and then K is called a **splitting field** of $f(x)$ over F if $f(x)$ splits in K(but in no proper subfield of K).
- Splitting field of a polynomial over a field always exists and is unique up to isomorphism.

14

More on Fields

Introduction

We continue our discussion on fields in this chapter and take up separable extensions, normal extensions, algebraically closed fields and algebraic closures. We'll study automorphisms of field extensions including Artin's theorem. All these results will lead us to the study of Galois extension and the fundamental theorem of Galois theory. Towards the end of the chapter we take up roots of unity, finite fields and construction by ruler and compass.

Prime Subfields

Definition: Let F be a field. The intersection of all subfields of F is the smallest subfield of F and is called the *prime subfield* of F.

Example 1: Let $F = \mathbf{Z}_p = \{0, 1, 2, ..., p-1\}$ mod p, p being prime. Suppose P is the prime subfield of F. Since $1 \in P$, $2, 3, ..., p-1 \in P$. Therefore, $P = F$.

Example 2: Let $\mathbf{Q}$ be the field of rationals.

Let $\frac{m}{n} \in \mathbf{Q}$, $m > 0$, $n > 0$, $m, n \in \mathbf{Z}$. Then

$$m = 1 + 1 \ldots + 1 \ (m \text{ times})$$
$$n = 1 + 1 + \ldots + 1 \ (n \text{ times})$$

$\Rightarrow m, n \in P$, the prime subfield of $\mathbf{Q}$ (as $1 \in P$). So, $\frac{m}{n} \in P \Rightarrow \frac{-m}{n} \in P$. Therefore, $\mathbf{Q} \subseteq P$. Thus, $P = \mathbf{Q}$.

In both the above examples, the prime subfield of the field turns out to be the field itself. But that is not always the case. Consider

Example 3: Let P_1 and P_2 be the prime subfields of two fields F_1 and F_2 respectively where $F_1 \subseteq F_2$.

Now $\quad P_1 \subseteq F_1 \subseteq F_2 \Rightarrow P_1 \subseteq F_2$.

But P_2 is the smallest subfield of F_2, so, $P_2 \subseteq P_1 \subseteq F_1 \Rightarrow P_2 \subseteq F_1$.

Again, P_1 is the smallest subfield of F_1. So, $P_1 \subseteq P_2$.

Thus, $P_1 = P_2$.

Since, $\mathbf{Q} \subseteq \mathbf{R}$ and $\mathbf{Q}$ is the prime subfield of $\mathbf{Q}$, it follows from above that $\mathbf{Q}$ is the prime subfield of $\mathbf{R}$.

We now tackle the problem in general to determine the prime subfield of any field F. We write char F to denote the characteristic of F.

Theorem 1: *Let P be the prime subfield of a field F. Then either $P \cong \mathbf{Q}$ or $P \cong \frac{\mathbf{Z}}{(p)}$, for some prime p, $\mathbf{Z}$ being the ring of integers.*

Proof: Define $\theta : \mathbf{Z} \to P \subseteq F$ s.t.,

$\theta(n) = ne$, where e denotes the unity of F

(of course, unity is denoted by 1, but here $\mathbf{Z}$ also has unity 1. So, we denote unity of F by e).

Then θ is homomorphism. (verify !)

Case 1: Char $F = 0$

Let $n \in \text{Ker } \theta$. Then $\theta(n) = 0 \Rightarrow ne = 0 \Rightarrow n = 0$ as $e \neq 0$.

So, Ker $\theta = \{0\} \Rightarrow \theta$ is one-one and so $\mathbf{Z} \cong \theta(\mathbf{Z}) \subseteq P$.

Since $\mathbf{Z}$ is an integral domain, so will be $\theta(\mathbf{Z})$.

Let $\mathbf{Q}'$ be the quotient field of $\theta(\mathbf{Z})$. Since $\mathbf{Q}$ is the quotient field of $\mathbf{Z}$, $\mathbf{Q} \cong \mathbf{Q}'$.

Also $\mathbf{Q}'$ is the smallest field containing $\theta(\mathbf{Z})$. But $\theta(\mathbf{Z}) \subseteq P$. Therefore, $\mathbf{Q}' \subseteq P \subseteq F$.

Again P is the smallest subfield of $F \Rightarrow P \subseteq \mathbf{Q}' \Rightarrow P = \mathbf{Q}'$.

Since $\mathbf{Q}' \cong \mathbf{Q}$, we get $P \cong \mathbf{Q}$.

Case 2: Char $F \neq 0$. Let char $F = p$, p being prime.

Let $n \in \text{Ker } \theta$. Then $\theta(n) = 0 \Rightarrow ne = 0 \Rightarrow p \mid n$ as $e \neq 0$

$\Rightarrow n \in (p) \Rightarrow \text{Ker } \theta \subseteq (p)$.

Also, $m \in (p) \Rightarrow m = pr \Rightarrow \theta(m) = \theta(pr) = (pr)e = (pe)\,(re) = 0$

$\Rightarrow m \in \text{Ker } \theta \Rightarrow (p) \subseteq \text{Ker } \theta$.

So, Ker $\theta = (p)$.

But (p) is a maximal ideal of $\mathbf{Z}$

$$\Rightarrow \frac{\mathbf{Z}}{\text{Ker } \theta} = \frac{\mathbf{Z}}{(p)} = \text{field}$$

$$\Rightarrow \theta(\mathbf{Z}) \cong \frac{\mathbf{Z}}{\text{Ker } \theta} \text{ is a field.}$$

Now, $\theta(\mathbf{Z}) \subseteq P \subseteq F$ and P is the smallest subfield of F, $P \subseteq \theta(\mathbf{Z})$. So $\theta(\mathbf{Z}) = P$

Thus $P \cong \frac{\mathbf{Z}}{(p)}$.

Remarks: (*i*) Let F_1, F_2 be fields such that $F_1 \subseteq F_2$. Then F_1, F_2 have the same prime subfield P.

If char $F_2 = 0$, then $P \cong \mathbf{Q}$. So, char $F_1 = 0$.

If char $F_2 = p$, then $P \cong \dfrac{\mathbf{Z}}{(p)}$. So, char $F_1 = p$.

In any case, char F_1 = char F_2.

(*ii*) If F is a finite field, then char $F = p$, for some prime p.

For let, char $F = 0$. Let P denote the prime subfield of F. Then $P \cong \mathbf{Q} \Rightarrow P$ is infinite $\Rightarrow F$ is infinite, a contradiction. Therefore, char $F = p$, for some prime P.

(*iii*) Char $\mathbf{Q} = 0$. For let char $\mathbf{Q} = p$, then the prime subfield $\mathbf{Q}$ of $\mathbf{Q}$ is isomorphic to $\dfrac{\mathbf{Z}}{(p)}$, which is not true as $\mathbf{Q}$ is infinite while $\dfrac{\mathbf{Z}}{(p)}$ is finite. So, char $\mathbf{Q} = 0$.

Example 4: We now give an example of an infinite field which has finite characteristic p.

Let $F = \{0, 1, 2, ..., p - 1\}$ mod p.

Let P be the prime subfield of F.

Then $P = F \cong \dfrac{\mathbf{Z}}{(p)}$. So, char $F = p$.

Now $F[x]$ is an infinite integral domain. Let $F(x)$ denote the quotient field of $F[x]$. Clearly, $F \subseteq F[x] \subseteq F(x)$. So, char F = char $F(x) \Rightarrow$ char $F(x) = p$. Thus, $F(x)$ is an example of an infiite field with finite characteristic p.

Problem 1: *Let char $F = p$. Then*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \textit{for all } n \geq 1,\ a, b \in F.$$

Solution: Let $n = 1$. Then

$$(a + b)^p = a^p + \sum_{r=1}^{p-1} p_{c_r} a^r b^{p-r} + b^p.$$

Since $p \mid p_{c_r}$, for all r, $1 \leq r \leq p - 1$. (See example on page 357)

We find $p_{c_r}\, a^r\, b^{p-r} = 0$

Therefore, $(a + b)^p = a^p + b^p$.

So the result is true for $n = 1$.

Assume that the result is true for $n = m$.

Now
$$\begin{aligned}(a + b)^{p^{m+1}} &= [(a + b)^p]^{p^m} \\ &= (a^p + b^p)^{p^m} \\ &= (a^p)^{p^m} + (b^p)^{p^m} \quad \text{by induction hypothesis} \\ &= a^{p^{m+1}} + b^{p^{m+1}}\end{aligned}$$

Therefore, the result is true for $n = m + 1$. By induction, the result is true for all $n \geq 1$.

Problem 2: *Every automorphism of a field F leaves the prime subfield P of F, elementwise fixed.*

Solution: Let θ be an automorphism of F.

Let $K = \{a \in F \mid \theta(a) = a\}$

Then K is a subfield of F (Prove!)

Since P is the smallest subfield of F, $P \subseteq K$. Let $b \in P$. Then $b \in K \Rightarrow \theta(b) = b \Rightarrow \theta$ fixes each element of P.

Separable Extensions

This section deals with those polynomials which have simple roots and the fields generated by these simple roots.

Recall, a root α of $f(x) \in K[x]$ is called simple if $x - \alpha$ divides $f(x)$ and $(x - \alpha)^2$ does not divide $f(x)$. Similarly, a root α of $f(x) \in K[x]$ is said to be a root with multiplicity m, if $(x - \alpha)^m$ divides $f(x)$ but $(x - \alpha)^{m+1}$ does not divide $f(x)$.

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$.

Define $f'(x) = a_1 + 2a_2 + \ldots + na_nx^{n-1} \in K[x]$.

Then $f'(x)$ or f' is called the *derivative* of f.

If $f, g \in K[x]$, then it can be easily proved that

(*i*) $(f \pm g)' = f' \pm g'$

(*ii*) $(fg)' = f'g + fg'$

(*iii*) $(af)' = af'$, $a \in K$

(*iv*) $x' = 1$.

It can be easily checked that α is a simple root of $f(x) \in K[x]$ iff $f'(\alpha) \neq 0$. In other words, α is not a simple root of $f \in K[x]$ iff $f'(\alpha) = 0$.

Theorem 2: *Suppose all roots of $f(x) \in K[x]$ in a minimal spitting field of f over K are simple. Then the roots of f in any minimal splitting field of f over K are simple.*

Proof: Let $f(x) = \alpha_0(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in E$.

where $E = K(\alpha_1, \ldots, \alpha_n)$ is a minimal splitting field of f over K.

Suppose each α_i is a simple root of f.

Let E' be another minimal splitting field of f over K.

Then $E' = K(\beta_1, \ldots, \beta_n)$ where $\beta_i s$ are roots of f.

Then there exists a K-isomorphism $\sigma : E \to E'$.

Since α_i is a root of f, $\sigma(\alpha_i)$ is also a root of f in E'.

Therefore $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\beta_1, \ldots, \beta_n\}$.

Since σ is 1-1 and $\alpha_i s$ are distinct roots of f, $\sigma(\alpha_i) s$ are all distinct. So $\beta_i s$ are all distinct.

Thus, the roots of f in E' are also simple roots.

Note: By the above arguments, we can also prove that if there is a root of multiplicity m in a minimal splitting field of f over K, then every minimal splitting field of f over K will have a root of f of multiplicity m.

Theorem 3: *Let F be an extension of K. Let $f, g \in K[x]$. Then the g.c.d. of f and g regarded as polynomials in $K[x]$ is same as that of f and g regarded as polynomials in $F[x]$, upto associates.*

Proof: Let d be the g.c.d. of $f, g \in K[x]$ and d_1 be the g.c.d. of $f, g \in F[x]$.

Now $d \mid f, d \mid g$ in $K[x] \Rightarrow d \mid f, d \mid g$ in $F[x]$

$\Rightarrow d \mid d_1$ in $F[x] \Rightarrow d_1 = du, \quad u \in F[x]$.

Also, $d = ff_1 + gg_1, \quad f, f_1 \in K[x]$.

Since $d_1 \mid f, d_1 \mid g, d_1 \mid ff_1, d_1 \mid gg_1$.

Therefore, $d_1 \mid ff_1 + gg_1 = d$ in $F[x]$.

$\Rightarrow d = d_1 v \quad v \in F[x]$.

So, $d = duv \Rightarrow uv = 1 \Rightarrow u, v$ are units in $F \Rightarrow d, d_1$ are associates. Thus d and d_1 are same upto associates.

Theorem 4: *Let F be an extension of K.Then f and g are relatively prime regarded as elements of $K[x]$ iff f and g are relatively prime regarded as elements of $F[x]$.*

Proof: Suppose f and g are relatively prime regarded as elements of $F[x]$.

Then (f, g) = g.c.d. of $f, g \in F[x]$ is a unit $d \in F$.

Let (f, g) = g.c.d. of $f, g \in K[x]$ be d_1

Then d and d_1 are associates

$\Rightarrow \quad d = ud_1$, u = unit in F

$\Rightarrow \quad d_1 = u^{-1} d$ = unit in F

Since $d_1 \in K$, d_1 is a unit in K.

The converse follows similarly.

Theorem 5: *Let F be an extension of K. Let $f(x) \in K[x]$, $\alpha \in F$. Then f can be written as $f = (x - \alpha)^2 g + (x - \alpha) f'(\alpha) + f(\alpha)$ for some $g \in F[x]$.*

Proof: Now $(x - \alpha) \in F[x]$.

Let $f = (x - \alpha)^2 g + h, \quad g, h \in F[x]$

and $h = (x - \alpha) g_1 + h_1, \quad g, h_1 \in F$

So, $f(\alpha) = h(\alpha) = h_1$ (deg $h < 2$)

Also, $f' = 2 (x - \alpha) g + (x - \alpha)^2 g' + h'$

and $h' = g_1$

$\Rightarrow f'(\alpha) = h'(\alpha) = g_1$.

Theorem, $f = (x - \alpha)^2 g + (x - \alpha) f'(\alpha) + f(\alpha)$.

Theorem 6: *Let $f \in K[x]$. Then the roots of f are simple iff f and f' are relatively prime.*

Proof: Suppose the roots of f are simple. Let $(f, f') = d$.

If d is a non-constant polynomial in $K[x]$, then d has a root α in some extension F of K.

Now $f = df_1, f' = dg_1, \quad f_1, g_1 \in K[x]$

$\Rightarrow f(\alpha) = d(\alpha) f_1(\alpha), \quad f'(\alpha) = d(\alpha) g_1(\alpha)$

$\Rightarrow f(\alpha) = 0 = f'(\alpha)$.

Using above result, we get

$$f = (x - \alpha)^2 g + (x - \alpha) f'(\alpha) + f(\alpha)$$
$$= (x - \alpha)^2 g$$

$\Rightarrow \alpha$ is not a simple root of f, a contradiction.

So, d = constant $\in K$.

Since $f \neq 0$, d is a non zero element in K.

Therefore, d is a unit $\Rightarrow f, f'$ are relatively prime.

Conversely, let f and f' be relatively prime. Then $(f, f') = d$ = unit in K.

Let α be a root of f' such that α is not a simple root of f. Let $\alpha \in F \supseteq K$.

Then $f(\alpha) = 0 = f'(\alpha)$

$\Rightarrow x - \alpha$ divides f and f' in $F[x] \supseteq K[x]$

$\Rightarrow x - \alpha$ divides d

But $d \in K \Rightarrow \deg d = 0$ $(d \neq 0)$.

and $x - \alpha$ divides d

$\Rightarrow \deg (x - \alpha) \leq \deg d = 0$, a contradiction.

So all roots of f are simple.

Definition: A polynomial is said to be *separable* if all its roots are simple.

In view of the above theorem, the following result follows.

Theorem 7: *A polynomial $f(x) \in F[x]$ is separable iff f and f' are relatively prime.*

Cor. 1: If $f(x) \in F[x]$ is irreducible over F such that $f' \neq 0$, then f is separable.

Proof: Let g.c.d. $(f, f') = d$ then $\deg d \leq \deg f' < \deg f$.

Since f is irreducible over F and d is a factor of f such that $\deg d < \deg f$, we find d is (non zero) constant and thus a unit. So, f and f' are relatively prime. By above theorem, f is separable.

Cor. 2: Let $f(x) \in F[x]$ be irreducible over F. If characteristic of F is zero, then f is separable. (In other words, an irreducible polynomial over a field of characteristic zero is separable).

Proof: Let $f = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$.

Then $f' = a_1 + 2a_2 + \ldots + n a_n x^{n-1}$.

If $f' = 0$, then $r a_r = 0$ for all $r = 1, 2, \ldots, n$. Since char $F = 0$, $a_r = 0$ for all $r = 1, 2, \ldots, n \Rightarrow f = a_0$, a contradiction as F is irreducible ($\deg f \geq 1$).

Thus, $f' \neq 0$. By Cor. 1, f is separable.

Theorem 8: *Let F be a field of characteristic p. Then for any polynomial $f(x) \in F[x]$, $f' = 0$ iff $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.*

Proof: Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $f' = 0$.

Then $r a_r = 0 \quad \forall\ r = 1, 2, \ldots, n$.

$\Rightarrow a_r = 0$ or p divides r as char $F = p$.

Thus, $f = a_0 + a_p x^p + \ldots + a_{sp} x^{sp}$

$= g(x^p)$, where $g(x) = a_0 + a_p x + \ldots + a_{sp} x^s \in F[x]$.

Conversely, let $f = g(x^p)$, where

$g(x) = b_0 + b_1x + ... + b_nx^n \in F[x]$

Then $f = b_0 + b_1x^p + ... + b_n\, x^{np}$

$\Rightarrow \quad f' = pb_1x^{p-1} + ... + npb_nx^{np-1} = 0 \quad$ as $pa = 0\ \forall\ a \in F$.

Theorem 9: *Let $f(x) \in F[x]$ be irreducible over F. Then all its roots have the same multiplicity.*

Proof: (*i*) Let char $F = 0$. Then by cor. 2 to theorem 7 f is separable. So, all roots of f are simple.

(*ii*) Let char $F = p$. If $f' \neq 0$, then by cor. 1 to theorem 7 f is separable. So, all roots of f are simple.

If $f' = 0$, then $f(x) = g(x^p)$, for some $g \in F[x]$.

Since f is irreducible over F, so is g over F.

If $g' \neq 0$, then g is separable over F. Let α be a root of f.

Then $\quad 0 = f(\alpha) = g(\alpha^p) \Rightarrow g(x) = Irr\ (F, \alpha^p)$.

Now, $\quad g(x) = (x - \alpha^p)\ h(x),\ h(\alpha^p) \neq 0$ as α^p is a simple root of $g(x)$.

So, $\quad f(x) = g(x^p) = (x^p - \alpha^p)\ h(x^p)$

$= (x - \alpha)^p\ h_1(x)$

$[h_1(x) = h(x^p) \Rightarrow h_1(\alpha) = h(\alpha^p) \neq 0]$

$\Rightarrow \quad x - \alpha$ appears exactly p times in $f(x)$.

This is true for all roots of $f(x)$.

If $g' = 0$, then $g(x) = q(x^p)$, $q \in F[x]$

$\Rightarrow \quad f(x) = q(x^{p^2})$.

Proceeding in this way, since, deg f is finite, after finite number of steps we get $f(x) = r(x^{p^e})$, $r' \neq 0$. Then r is separable over F and every root of f appears exactly p^e times.

Hence all roots of f have same multiplicity p^e ($e \geq 0$).

Aliter: Let α be a root of f of multiplicity m.

Then $f(x) = (x - \alpha)^m\ g(x),\ g(\alpha) \neq 0 \quad g(x) \in K[x],\ K = k(\alpha)$

Let β the another root of f. Then $\exists$ an F-isomorphism

$\sigma : F(\alpha) \to F(\beta)$ s.t.,

$\sigma(\alpha) = \beta$

Now $\quad f = \sigma(f) = (x - \beta)^m\ \sigma(g(x))$

Let $\quad g(x) = a_0 + a_1x + ... + a_nx^n,\ a_i \in K$

Then $\quad \sigma(g(x)) = \sigma(a_0) + \sigma(a_1)\ x + ... + \sigma(a_n)\ x^n$

$\Rightarrow \quad \sigma(g(\beta)) = \sigma(a_0) + \sigma(a_1)\beta + ... + \sigma(a_n)\ \beta^n$

$= \alpha(a_0) + \alpha(a_1)\ \sigma(\alpha) + ... + \sigma(a_n)\ \sigma(\alpha^n)$

$= \sigma(a_0 + a_1\alpha_1 + ... + a_n\alpha^n)$

$= \sigma(g(\alpha)) \neq 0$ as $g(\alpha) \neq 0$

$\Rightarrow \quad \beta$ is a root of f of multiplicity m, showing that all roots of f have same multiplicity.

Cor.: If $f \in F_p[x]$ is irreducible over F_p and f is not separable, then p divides n, where $n = \deg f$. (F_p deotes the field $\{0, 1, 2, ..., p-1\} \bmod p$).

Proof: By above theorem, all roots of f have same multiplicity p^e, $e > 0$ as f is not separable.

So, $\deg f = rp^e$

$\Rightarrow p$ divides $n = \deg f$. (Note, char $F_p = p$).

Theorem 10: *Let $x^p - a \in F[x]$, where p = char F. Then either $x^p - a$ is irreducible over F or $x^p - a$ is a p-th power of a linear polynomial in F.*

Proof: Let $f(x) = x^p - a$.

If b is a root of $f(x)$, then $f(b) = 0 \Rightarrow a = b^p$.

$$\Rightarrow f(x) = x^p - b^p = (x - b)^p.$$

If $b \in F$, then $f(x)$ is p-th power of linear polynomial $x - b \in F[x]$.

Suppose $b \notin F$. Let $p(x)$ be a monic irreducible factor of $f(x)$ in $F[x]$.

Since $p(x)$ divides $f(x)$, $p(x) = (x - b)^m$ for some m, $1 \leq m \leq p$.

So, $p(b) = 0$. Thus, $p(x) = Irr\ (F, b)$.

If $q(x)$ is another monic irreducible factor of $f(x)$ in $F[x]$, then

$$q(x) = Irr\ (F, b) = p(x).$$

So, $$f(x) = (p(x))^r.$$

Since $\deg f = p$, $p = rm$.

If $r > 1$, then $m = 1 \Rightarrow p(x) = x - b \in F[x] \Rightarrow b \in F$, a contradiction.

So, $r = 1 \Rightarrow f(x) = p(x)$ is irreducible over F.

Example 5: We saw earlier that any polynomial over a field of characteristic zero is separable. However, this need not be true over a field of characteristic p. We give an example of an irreducible polynomial which does not have distinct roots.

Let $K = F_2(t)$, $F_2 = \{0, 1\} \bmod 2$ and t is an indeterminate over F_2. Let $f(x) = x^2 - t \in K[x]$.

If f is reducible over K, then there would be an element $a \in K$ s.t., $f(a) = 0$.

$\Rightarrow t = a^2$. But $a \in K \Rightarrow a = \dfrac{g(t)}{h(t)}$.

So, $t = \dfrac{(g(t))^2}{(h(t))^2} \Rightarrow \deg (g(t))^2 = \deg\ t(h(t))^2$.

$\Rightarrow 2 \deg g(t) = \deg t + 2 \deg h(t) = 1 + 2 \deg h(t)$, which is not true.

So, f is irreducible over K.

If α is a root of f, then $f'(\alpha) = 0$ (as char K = 2 = char F_2) $\Rightarrow \alpha$ is not a simple root of f.

So, $f = (x - \alpha)^2$.

Thus, f is an irreducible polynomial having no simple roots.

Definition: Let F be an algebraic extension of K. Then $a \in F$ is called separable over K if $Irr\ (K, a)$ is separable.

Thus, $a \in F$ is separable over K iff a is a simple root of $Irr\ (K, a)$. Further, if each $a \in F$ is separable over K, then F is called a separable extension of K. (We write F/K is separable).

In the example above, $x^2 - t = Irr\ (K, \alpha)$ and α is not a simple root of $x^2 - t$.

If F is a minimal splitting field of $f = x^2 - t$ over K, containing α then F/K is algebraic and $\alpha \in F$ is not separable over K.

So, $F = K(\alpha)$ is not separable over F.

However, if char $K = 0$ then every algebraic extension of K is separable by cor.2. to theorem 7.

Theorem 11: *Let char $K = p$. Then every algebraic extension of K is separable iff $K = K^p$.*

Proof: Suppose every algebraic extension of K is separable. Let $a \in K$. Let $f(x) = x^p - a$ and b be a zero of $f(x)$. Then $0 = f(b) = b^p - a \Rightarrow a = b^p \Rightarrow f(x) = x^p - b^p = (x - b)^p$. If $b \notin K$ then $f(x)$ is irreducible over K.

So, $x^p - a = Irr(K, b)$.

But $f(x) = x^p - a$

$\Rightarrow$ $f'(x) = px^{p-1}$

$\Rightarrow$ $f'(b) = 0$ as char $K = p$

$\Rightarrow$ b is not a simple root of $f(x)$

$\Rightarrow K(b)/K$ is not separable, contradicting the given fact that every algebraic extension of K is separable.

So, $b \in K$ and $a = b^p \in K^p \Rightarrow K \subseteq K^p$.

However, $K^p \subseteq K$. So $K = K^p$ (Note, $K^p = \{a^p \mid a \in K\}$).

Conversely, let $K = K^p$. Let F/K be algebraic.

Let $\alpha \in F$, $f(x) = Irr\ (K, \alpha)$. If f is not separable, then $f' = 0$. So, $f = g(x^p)$ for some $g \in K[x]$.

Let $g = a_0 + a_1x + \ldots + a_nx^n,\ a_i \in K.$

Then $f = g(x^p) = a_0 + a_1x^p + \ldots + a_nx^{np}$

Since $K = K^p,\ a_i = b_i^p,\ b_i \in K.$

So, $f = b_0^p + b_1^p x^p + \ldots + b_n^p x^{np}$

$= (b_0 + b_1x + \ldots + b_nx^n)^p,\ b_i \in K$

contradicting that f is irreducible over K.

Thus f is separable $\Rightarrow \alpha$ is separable.

Since α is an arbitrary element of F, F/K is separable.

Definition: *A* field K is called *perfect field* if every algebraic extension of K is separable.

A field of characteristic zero is perfect by cor. 2 to theorem 7. So, **Q**, **R**, **C**, are perfect fields.

Theorem 12: *Let char $K = p$. Then the following are equivalent:*

(*i*) *K is perfect.*

(*ii*) $K = K^p$

(*iii*) *Every element in K is a p-th power of some element in K.*

(*iv*) $\theta : K \to K$ *such that* $\theta(a) = a^p$ *is an automorphism.*

Proof: (*i*) $\Rightarrow$ (*ii*) follows by theorem 11

(*ii*) $\Rightarrow$ (*iii*) obvious

(*iii*) $\Rightarrow$ (*iv*): Since char $K = p$, θ is clearly a homomorphism and is 1-1.

Also, $b \in K \Rightarrow b = a^p$, $a \in K$ by (*iii*).

$\Rightarrow b = \theta(a) \Rightarrow \theta$ is onto. So, θ is an automorphism.

(*iv*) $\Rightarrow$ (*i*): Now $\theta(K) = \{\theta(a) \mid a \in K\}$

$= \{a^p \mid a \in K\}$

$= K^p$.

Since θ is onto, $K = K^p$.

By theorem 11 then K is perfect.

Theorem 13: *Let* $F \subseteq K \subseteq L$ *be a tower of fields. Suppose L/F is separable. Then L/K is separable.*

Proof: Let $a \in L$, $p(x) = Irr\,(K, a)$

$q(x) = Irr(F, a)$

Then $q(x) \in K[x]$ and $q(a) = 0$.

So, $p(x)$ divides $q(x)$ in $K[x]$

$\Rightarrow$ $q(x) = p(x)\, r(x)$, $r(x) \in K[x]$

$\Rightarrow$ $q'(x) = p'(x)\, r(x) + p(x)\, r'(x)$

$\Rightarrow$ $q'(a) = p'(a)\, r(a)$.

Since L/F is separable, a is separable over F.

So a is a simple root of $q(x) \Rightarrow q'(a) \neq 0$

$\Rightarrow$ $p'(a) \neq 0 \Rightarrow a$ is a simple root of $p(x)$

$\Rightarrow$ a is separable over K

$\Rightarrow$ L/K is separable.

Cor.: Every finite extension of a perfect field is perfect.

Proof: Let F be a perfect field. Let K/F be finite extension. Then K/F is algebraic. Let L/K be algebraic. Then L/F is algebraic. Since F is perfect, L/F is separable. From above, L/K is separable. So, K is perfect.

Problem 3: *Let F be a perfect field. Show that the set of elements fixed under all automorphisms of F is a perfect subfield.*

Solution: Let char $F = p$, $K = \{a \in F \mid \sigma(a) = a \ \forall\ \sigma \in G\}$, where G is the group of all automorphisms of F. Then K is subfield of F.

Define $\theta : F \to F$ s.t.,

$\theta(\alpha) = \alpha^p$

Then θ is a homomorphism. Since F is perfect, θ is onto. So, $\theta \in G$.

Let $\alpha \in K$. Then $\sigma(\alpha) = \alpha \quad \forall\ \sigma \in G$

$\Rightarrow \theta(\alpha) = \alpha \Rightarrow \alpha^p = \alpha \Rightarrow \alpha \in K^p \Rightarrow K \subseteq K^p$.

$\Rightarrow K = K^p \Rightarrow K$ is perfect.

Problem 4: Let *K/F be a finite extension and suppose K is perfect then show that F is perfect*.

Solution: Let char $F = p$, then char $K = p$.

Let $[K : F] = n$ and $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a basis of K over F.

Since K is perfect, $K = K^p$. We show $F = F^p$.

Now $F^p \subseteq F \subseteq K$. So we show that

$[K : F^p] = [K : F]$ which would give $F = F^p$.

Let $S = \{\alpha_1^p, \alpha_2^p, ..., \alpha_n^p\} \subseteq K^p = K$

If $a_1^p\alpha_1^p + a_2^p\alpha_2^p + ... + a_n^p\alpha_n^p = 0$, $a_i \in F$

then $(a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n)^p = 0$

$\Rightarrow a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n = 0$

$\Rightarrow a_i = 0 \quad \forall\ i$

$\Rightarrow S$ is L.I. set in K (over F^p)

Let $b \in K$, then $b = a^p$, $a \in K$ as $K = K^p$

Now $a \in K \Rightarrow a = b_1\alpha_1 + b_2\alpha_2 + ... + b_n\alpha_n$, $b_i \in F$

$\Rightarrow \quad b = a^p = b_1^p\ \alpha_1^p + b_2^p\ \alpha_2^p + ... + b_n^p\ \alpha_n^p$

$\Rightarrow \quad S$ spans K over F^p

Hence S is a basis of K over F^p

$\Rightarrow [K : F^p] = o(S) = n = [K : F]$

$\Rightarrow F = F^p$ or that F is perfect.

Normal Extensions

As seen earlier if $f(x) \in K[x]$ is irreducible over K, then $\exists$ an extension E of K containing a root of $f(x)$. In this section we consider those extensions of K which contain all roots of $f(x)$ and study properties of such extensions.

Definition: Let E be an extension of K. E is called *normal extension* of K if (*i*) E/K is algebraic (*ii*) $\alpha \in E \Rightarrow p(x) = Irr\,(K, \alpha)$ splits in $E[x]$ or E.

Example 6: A quadratic extension is a normal extension.

Let E be a quadratic extension of K. Then $[E : K] = 2$.

Since E/K is finite, E/K is algebraic.

Let $\alpha \in E$, $p(x) = Irr\,(K, \alpha)$.

Now $K \subseteq K(\alpha) \subseteq E$. Since $2 = [E : K] = [E : K(\alpha)]\ [K(\alpha) : K]$.

Either $[E : K(\alpha)] = 1$ or $[K(\alpha) : K] = 1$.

If $[K(\alpha) : K] = 1$, then $K(\alpha) = K \Rightarrow \alpha \in K \Rightarrow p(x) = x - \alpha$ splits in $K[x] \subseteq E[x]$.

If $[E : K(\alpha)] = 1$, then $E = K(\alpha)$.

So, $2 = [E : K] = [K(\alpha) : K] = \deg Irr\ (K, \alpha) = \deg p(x)$.

Now α is a root of $p(x) \Rightarrow x - \alpha$ divides $p(x)$ in $E[x]$.

$\Rightarrow p(x) = (x - \alpha)\ q(x), \quad q(x) \in E[x]$.

Since deg $p(x) = 2$, deg $q(x) = 1$. So $q(x) = (x - \beta)$, $\beta \in E$.

Therefore, $p(x) = (x - \alpha)\ (x - \beta)$ splits in $E[x]$.

Thus, E/K is normal.

Example 7: Let $f(x) = x^3 - 2 \in \mathbf{Q}[x]$. Let α be the real root of $f(x)$. Consider $\mathbf{Q}(\alpha)/\mathbf{Q}$. We show that $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Now $f(x)$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion (take $p = 2$). So, $f(x) = Irr\ (\mathbf{Q}, \alpha)$. Since α is algebraic over $\mathbf{Q}$(being root of $f(x) \in \mathbf{Q}[x]$), $\mathbf{Q}(\alpha)/\mathbf{Q}$ is algebraic.

If $f(x)$ splits in $\mathbf{Q}(\alpha)$, then $\mathbf{Q}(\alpha)$ contains a minimal splitting field E of $f(x)$ over $\mathbf{Q}$.

So, $\mathbf{Q} \subseteq E \subseteq \mathbf{Q}(\alpha)$.

But $[E : \mathbf{Q}] = 6$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg Irr\ (\mathbf{Q}, \alpha) = \deg f(x) = 3$.

Since $3 = [\mathbf{Q}(\alpha) : \mathbf{Q}] \geq [E : \mathbf{Q}] = 6$, we get a contradiction.

So, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Similarly, $\mathbf{Q}(\alpha w)/\mathbf{Q}$ and $\mathbf{Q}(\alpha w^2)/\mathbf{Q}$ are not normal extensions.

Remark: We have seen in above example that an extension of degree 3 need not be normal. We can, however, have a normal extension of degree 3. Consider $f(x) = x^3 + x^2 + 1 \in F_2[x]$, where $F_2 = \{0, 1\}$ mod 2. Let α be a root of $f(x)$. Then α^2, $1 + \alpha + \alpha^2$ are also roots of $f(x)$. So $F_2(\alpha)$ is a minimal splitting field of $f(x)$ over F_2. Thus $F_2(\alpha)/F_2$ is normal and $[F_2(\alpha) : F_2] = \deg$ Irr $(F_2, \alpha) = \deg f(x) = 3$.

Theorem 14: *Let $F \subseteq K \subseteq E$ be a tower of fields. If E/F is normal, then so is E/K.*

Proof: Since E/F is normal, E/F is algebraic. So, E/K is algebraic.

Let $\alpha \in E$, $p(x) = Irr\ (K, \alpha)$, $q(x) = Irr(F, \alpha)$. Then $q(x) \in F[x] \subseteq K[x] \Rightarrow q(x) \in K[x]$ and $q(\alpha) = 0$.

So, $p(x)$ divides $q(x)$ in $K[x]$.

Since E/F is normal and $\alpha \in E$, $q(x)$ splits in $E[x]$.

So, $p(x)$ splits in $E[x]$. Thus, E/K is normal.

Remark: In above theorem K/F need not be normal. Consider $f(x) = x^3 - 2 \in \mathbf{Q}[x]$. Let $\alpha \in \mathbf{R}$ be a root of $f(x)$. Then $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal by example 7. However, $\mathbf{Q}(\alpha, w)/\mathbf{Q}$ is normal by theorem 15 and $\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\alpha, w)$. Notice $\mathbf{Q}(\alpha, w)$ is a minimal splitting field of $f(x)$ over $\mathbf{Q}$.

Theorem 15: *A minimal splitting field of a non-constant polynomial $f(x) \in K[x]$ over K is normal extension of K.*

Proof: Let E be a minimal splitting field of $f(x)$ over K. Then E/K is algebraic and finite. Let $f(x) = \alpha_0(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in E$.

Then $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Let $\alpha \in E$, $p(x) = Irr\ (K, \alpha) \in K[x] \subseteq E[x]$.
Then $p(x)$ splits in some extension of E.
Let β be a root of $p(x)$ in some extension of E. We show that $\beta \in E$.
Now α, β are roots of $p(x) \Rightarrow \exists$ a K-isomorphism $\sigma : K(\alpha) \to K(\beta)$ s.t., $\sigma(\alpha) = \beta$.
Then, a minimal splitting field of f over $K(\alpha)$ is $K(\alpha)\ (\alpha_1, \alpha_2, ..., \alpha_n)$

$$= K(\alpha_1, \alpha_2, ..., \alpha_n)\ (\alpha)$$
$$= E(\alpha)$$
$$= E \quad \text{as } \alpha \in E$$

Also, a minimal splitting field of $\sigma(f) = f$ over $K(\beta)$ is

$$K(\beta)\ (\alpha_1, \alpha_2, ..., \alpha_n)$$
$$= K(\alpha_1, \alpha_2, ..., \alpha_n)\ (\beta)$$
$$= E(\beta).$$

So, $\exists$ an isomorphism $\theta : E \to E(\beta)$ s.t., $\theta(a) = \sigma(a)\ \forall\ a \in K(\alpha)$

$$\Rightarrow \qquad \theta(\alpha) = \sigma(\alpha) = \beta.$$

Now $K \subseteq K(\alpha) \subseteq E \subseteq E(\beta)$

$$\Rightarrow \quad [E : K(\alpha)] = [\theta(E) : \theta(K(\alpha)]$$
$$= [E(\beta) : \sigma(K(\alpha)]$$
$$= [E(\beta) : K(\beta)]$$

So, $[E(\beta) : K] = [E(\beta) : K(\beta)]\ [K(\beta) : K]$

$$= [E : K(\alpha)]\ \deg p(x)$$
$$= [E : K(\alpha)]\ [K(\alpha) : K]$$
$$= [E : K].$$

Since $E \subseteq E(\beta)$ and E, $E(\beta)$ as vector spaces over K have same dimension, $E = E(\beta)$. So, $\beta \in E$. Thus, $p(x)$ splits in E. This proves E/K is normal.

Theorem 16: *A finite normal extension is a minimal splitting field of some polynomial.*

Proof: Let E/K be a finite normal extension.
E/K is finite $\Rightarrow E = K(\alpha_1, \alpha_2, ..., \alpha_n)$.
Let $p_i(x) = Irr\ (K, \alpha_i)$. Since $\alpha_i \in E$ and E/K is normal, each $p_i(x)$ splits in E.
Let $f = p_1 p_2 \ ... \ p_n \in K[x]$.
Then, a minimal splitting field of f over K is
$K(\alpha_1, \alpha_2, ..., \alpha_n,$ roots of $p_i s$ in $E) = E$.
So, E is a minimal splitting field of f over K.

Cor.: Let $K \subseteq E_1 \subseteq E$, $K \subseteq E_2 \subseteq E$ be towers of fields s.t., E_1/K, E_2/K are finite normal extensions. Then E_1E_2, the smallest subfield of E containing $E_1 \cup E_2$ is finite normal extension of K.

Proof: Since E_1/K is finite, $E_1 = K(\alpha_1, ..., \alpha_n)$.
So, $\quad E_1E_2 = K(\alpha_1, ..., \alpha_n)E_2$

$= E_2(\alpha_1, ..., \alpha_n)$, as $K \subseteq E_2 \Rightarrow KE_2 = E_2$

Thus $[E_1E_2 : E_2] = [E_2(\alpha_1, ..., \alpha_n) : E_2]$

$= [E_2(\alpha_1, ..., \alpha_n) : E_2(\alpha_1, ..., \alpha_{n-1})]$ ..... $[E_2(\alpha_1) : E_2]$

$\leq [K(\alpha_1, ..., \alpha_n) : K(\alpha_1, ..., \alpha_{n-1})]$ ..... $[K(\alpha_1) : K]$

$= [K(\alpha_1, ..., \alpha_n) : K]$

$= [E_1 : K]$.

Therefore, $[E_1 E_2 : K] = [E_1E_2 : E_2]\,[E_2 : K]$

$\leq [E_1 K]\,[E_2 : K]$ = finite

$\Rightarrow [E_1E_2 : K]$ = finite.

Now E_1/K is finite normal $\Rightarrow E_1$ is a minimal splitting field of f_1 over K

Also, E_2/K is finite normal $\Rightarrow E_2$ is a minimal splitting field of f_2 over K

Let $f = f_1 f_2$, $E_1 = K(a_1, ..., a_r)$, $E_2 = K(b_1, ..., b_s)$. Then, a minimal splitting field of f over K is $K(a_1, ..., a_r, b_1, ..., b_s)$

$= E_1(b_1, ..., b_s)$

$= E_1K(b_1, ..., b_s)$ as $E_1K = E_1$

$= E_1E_2$.

Thus, E_1E_2/K is finite normal extension.

(Note, we have also shown above that E_1/K, E_2/K are finite $\Rightarrow E_1E_2/K$ is finite).

Example 8: We now give an example to show that a normal extension of a normal extension need not be a normal extension.

Consider the tower of fields $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(2^{1/4})$.

Now $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$ = deg *Irr* $(\mathbf{Q}, \sqrt{2})$ = deg$(x^2 - 2)$ = 2

and $[\mathbf{Q}(2^{1/4}) : \mathbf{Q}(2^{1/2})]$ = deg *Irr*$(\mathbf{Q}(\sqrt{2}), 2^{1/4})$ = deg $(x^2 - \sqrt{2})$ = 2

So, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, $\mathbf{Q}(2^{1/4})/\mathbf{Q}(\sqrt{2})$ are normal.

If $\mathbf{Q}(2^{1/4})/\mathbf{Q}$ is normal, then $f(x) = Irr(\mathbf{Q}, 2^{1/4}) = x^4 - 2$ must split in $\mathbf{Q}(2^{1/4})$.

So, $\mathbf{Q}(2^{1/4})$ contains a minimal splitting field E of $f(x)$.

But $[E : \mathbf{Q}] = 8$ and $\mathbf{Q} \subseteq E \subseteq \mathbf{Q}(2^{1/4}) \Rightarrow [\mathbf{Q}(2^{1/4}) : \mathbf{Q}] = 4 \geq [E : \mathbf{Q}] = 8$, a contradiction.

Therefore, $\mathbf{Q}(2^{1/4})/\mathbf{Q}$ is not normal, proving our assertion.

Theorem 17: *Let $K \subseteq F \subseteq E$ be a tower of fields s.t., E/K is finite normal. Then any K-homomorphism of F into E can be extended to K-automorphism of E.*

Proof: Since E/K is finite, $E = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Also E/K is finite normal $\Rightarrow E$ is a minimal splitting field of some $f(x) \in K[x]$ over K. Let σ be a K-homomorphism of F into E. Then σ is a K-isomorphism from F onto $\sigma(F) = F'$. $f = p_1p_2 \ldots p_n$, where $p_i = Irr\ (K, \alpha_i)$ splits in E. So, a minimal splitting field of f over F is

$F(\alpha_1, \alpha_2, ..., \alpha_n$, roots of f in $E)$

$= E$(roots of f in E) $= E$

$(E = K(\alpha_1, \alpha_2, ..., \alpha_n) \subseteq F(\alpha_1, \alpha_2, ..., \alpha_n) \subseteq E \Rightarrow E = F(\alpha_1, \alpha_2, ..., \alpha_n))$

Also, a minimal splitting field of $\sigma(f(x)) = f$ over F' is

$F'(\alpha_1, \alpha_2, ..., \alpha_n,$ roots of f in $E)$

$= E($roots of $f(x)$ in $E)$

$= E$

$[E = K(\alpha_1, \alpha_2, ..., \alpha_n) \subseteq F(\alpha_1, \alpha_2, ..., \alpha_n)$

$\cong F'(\alpha_1, \alpha_2, ..., \alpha_n)$

$\subseteq F(\alpha_1, \alpha_2, ..., \alpha_n) = E$

$\Rightarrow E = F'(\alpha_1, \alpha_2, ..., \alpha_n)]$

Therefore, $\exists$ an isomorphism $\theta : E \to E$ s.t., $\theta(a) = \sigma(a)\ \forall\ a \in F \Rightarrow \theta(\alpha) = \sigma(\alpha) = \alpha\ \forall\ \alpha \in K \Rightarrow \theta$ is a K-automorphism of E extending σ. This proves the result.

Normal Closure: Let E/K be a finite extension. Then $E = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Let $p_i = Irr(K, \alpha_i)$ and $f = p_1 p_2 ... p_n \in K[x]$.

Then E' the minimal splitting field of f over K is

$K(\alpha_1, ..., \alpha_n,$ root of f in some extension of $E)$

$= E($roots of f in some extension of $E)$

$\Rightarrow E \subseteq E'$ and E'/K is finite normal

(as a minimal splitting field of f over K is finite normal extension of K)

Suppose $K \subseteq E \subseteq F$ s.t., F/K is finite normal.

We show that E' can be embedded in F.

$\alpha_i \in E \subseteq F \Rightarrow \alpha_i \in F\ \forall\ i$. Also F/K is normal.

So, $p_i(x)$ splits in $F[x]\ \forall\ i \Rightarrow f$ splits in $F[x]$

$\Rightarrow F$ contains a minimal splitting field E_1 of f over K.

$\Rightarrow E_1 \subseteq F$. But E' is also a minimal splitting field of f over K.

Therefore, $E' \cong E_1 \subseteq F \Rightarrow E'$ can be embedded in F.

Thus, E' is the least finite normal extension of K s.t., $K \subseteq E \subseteq E'$.

E' is called the normal closure of E/K.

Example 9: Let $f(x) = x^3 - 2$

$= (x - \alpha)\ (x - \alpha w)\ (x - \alpha w^2)$

We find the normal closure of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

Now $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg f(x) = 3$.

where $f = Irr\ (\mathbf{Q}, \alpha)$.

Then, a minimal splitting field of f over $\mathbf{Q}$ is $\mathbf{Q}(\alpha, \alpha w, \alpha w^2) = \mathbf{Q}(\alpha, w)$.

So, $\mathbf{Q}(\alpha w)/\mathbf{Q}$ is the normal closure of $\mathbf{Q}$.

Algebraically closed fields and algebraic closure

In this section, we give a characterization of normal extensions. Also, we show that given a tower of fields $k \subseteq F \subseteq K$ such that K/k is normal, any k-homomorphism of F into K can be

extended to a k-automorphism of K. We have already seen this result when K/k is finite normal. We also show that given a field k, there is an algebraic extension $\bar{k}$ of k such that $\bar{k}$ has no algebraic extension other that $\bar{k}$ itself. $\bar{k}$ is called an *algebraic closure* of k. We define the product of two subfields of a field and show that the product and the intersection of two normal extensions of k is again a normal extension of k.

Let S be a set of polynomials over k. Suppose each $f \in S$ splits in a field E containing k. Then E is called a *splitting field of S over k* and k(zeros of $f \in S$ in E) is called a *minimal splitting field of S over k.* For a finite set S, it is very easy to show the existence of a minimal splitting field of S over k. For, let

$$S = \{f_1, f_2, \ldots, f_n \mid f_i \in k[x]\}.$$

Let E_1 be a minimal splitting field of f_1 over k, E_2 be a minimal splitting field of f_2 over E_1 and so on, E_n be a minimal splitting field of f_n over E_{n-1}. Then $E_1 \subseteq E_2 \subseteq \ldots \subseteq E_n$ and each f_i splits in $E_i \subseteq E_n \Rightarrow S$ splits in E_n. So, k(zeros of f_i in E_n) is a minimal splitting field of S over k. It is also a minimal splitting field of $f = f_1 f_2 \ldots f_n$ over k.

Definition: A field k is called *algebraically closed* if every polynomial f over k splits in k.

By fundamental theorem of algebra, every polynomial over **C**, the field of complex numbers splits in **C**. So, **C** is an algebraically closed field. However, **R** the field of reals is not algebraiclly closed as $x^2 + 1 \in \mathbf{R}[x]$ does not split in **R**. We have the following characteriszations of algebraically closed fields.

Theorem 18: *A field k is algebrically closed iff every irreducible polynomial over k has degree one.*

Proof: Suppose k is algebraically closed.

Let f be an irreducible polynomial over k. Since k is algebrically closed, f splits in k.

So, $f = f_1 f_2 \ldots f_n$ where each f_i is linear over k.

Since f is irreducible over k, $f = f_1 \Rightarrow f$ is linear over $k \Rightarrow \deg f = 1$.

Conversely, let $g \in k[x]$.

Then $g = g_1 g_2 \ldots g_m$, where each g_i is irreducible over k.

By hypothesis, $\deg g_i = 1 \Rightarrow g_i$ is linear over k for each i

$\Rightarrow g$ is a product of linear factors over $k \Rightarrow g$ splits in k.

So, k is algebraically closed.

Theorem 19: *A field k is algebraically closed iff every algebraic extension of k is k itself.*

Proof: Let k be algebraically closed. Let K/k be algebraic.

Let $\alpha \in K$, $p(x) = Irr\ (k, \alpha)$.

By above theorem $\deg p(x) = 1 \Rightarrow p(x) = x - \alpha \in k[x] \Rightarrow \alpha \in k \Rightarrow K = k$.

Conversely, let $f \in k[x]$. Let K be a minimal splitting field of f over k.

Then K/k is algebraic. By hypothesis, $K = k$.

So, $f(x)$ splits in $k[x] \Rightarrow k$ is algebraically closed.

Summarising the last two results, we have the following

Theorem 20: *Let k be a field. Then following are equivalent*

(*i*) *k is algebraically closed.*

(*ii*) *Every irreducible polynomial over k has degree one.*

(*iii*) *Every algebraic extension over k is k itself.*

Theorem 21: *A finite field is not algebraically closed.*

Proof: Let k be the finite field $\{a_1, a_2, ..., a_n\}$

Let $f = 1 + (x - a_1)(x - a_2) ... (x - a_n) \in k[x]$.

Since $f(a_i) \neq 0$ for all i, we find f does not split in k.

Hence k is not algebraically closed.

Definition: Let k be a field. An extension E of k is called *algebraic closure* of k if

(*i*) E/k is algebraic.

(*ii*) E is algebraically closed.

The following result is now an immediate consequence of theorem 19.

Theorem 22: *Let E be an algebraic extension of k. Then E is algebraically closed iff E has no algeraic extension other than E itself.*

Example 10: Since $[\mathbf{C} : \mathbf{R}] = 2$, $\mathbf{C}/\mathbf{R}$ is algebraic. Also, $\mathbf{C}$ is algebraically closed, So, $\mathbf{C}$ is an algebraic closure of $\mathbf{R}$. However, $\mathbf{C}$ is not an algebraic closure of $\mathbf{Q}$ as $\mathbf{C}/\mathbf{Q}$ is not algebraic ($\pi \in \mathbf{C}$ is not algebraic over $\mathbf{Q}$).

Theorem 23: *Let K/k be algebraic. Let* $\bar{k}$ *denote an algebraic closure of K. Then* $\bar{k}$ *is an algebraic closure of k such that*

$$k \subseteq K \subseteq \bar{k}.$$

Proof: Since $\bar{k}$ is an algebraic closure of K, $\bar{k}/K$ is algebraic. Also, K/k is algebraic. So, $\bar{k}/k$ is algebraic. But $\bar{k}$ is algebraically closed. Thus $\bar{k}$ is also an algebraic closure of k.

Theorem 24: *Let K be an algebraically closed field such that K is an extension of k. Let* $F = \{a \in K | a \text{ is algebraic over } k\}$.

Then F is an algebraic closure of k.

Proof: We know that

$k \subseteq F \subseteq K$ is a tower of fields.

Also, by definition of F, F/k is algebraic.

Let $f \in F[x]$. Then $f \in K[x]$. Since K is algebraically closed, f splits in K.

Let $f = \alpha(x - \alpha_1) ... (x - \alpha_n)$, $\alpha_i \in K$.

Since α_i is algebraic over F, $F(\alpha_i)/F$ is algebraic for all i.

Also F/k is algebraic. So, $F(\alpha_i)/k$ is algebraic for all i.

$\Rightarrow \alpha_i \in K$ is algebraic over k

$\Rightarrow \alpha_i \in F$

$\Rightarrow f$ splits in F

$\Rightarrow F$ is algebraically closed

$\Rightarrow F$ is an algebraic closure of k.

From above theorem it follows that $F = \{a \in \mathbf{C} \mid a$ is algebraic over $\mathbf{Q}\}$is an algebraic closure of $\mathbf{Q}$.

We now show the existence of a minimal splitting field of a set of polynomials over k.

Theorem 25: *Let S be a set of polynomials over k. Then there is a minimal splitting field of S over k.*

Proof: Suppose $S = \{f_i \mid f_i \in k[x],\ i \in I\}$.

Let $A = \{i_1, i_2, ..., i_n\}$ be a finite subset of I.

Put $f_A = f_{i1}\, f_{i2} \ldots f_{i_n} \in k[x]$.

Let E_A be a minimal splitting field of f_A over k.

Suppose $B \subseteq A$. Then f_B divides f_A. So, f_B splits in E_A.

Let $F_B = k$(zeros of f_B in E_A).

Then F_B is a minimal splitting field of f_B over k. So, $F_B \cong E_B$. But $F_B \subseteq E_A$. Therefore, we can regard $E_B \subseteq E_A$. So, we have $B \subseteq A \Rightarrow E_B \subseteq E_A$.

Let $E = \bigcup_A E_A$. Let $a, b \in E$. Then $a \in E_A$, $b \in E_B$ for some finite sets $A, B \subseteq I$.

Let $C = A \cup B$. Then $A, B \subseteq C$.

So, $E_A, E_B \subseteq E_C \Rightarrow a, b \in E_C$

$\Rightarrow a \pm b, ab, ab^{-1}$, (if $b \neq 0$) are in $E_C \subseteq E$

$\Rightarrow E$ is a field.

Therefore, for each $f_i \in S$, f_i splits in E_A, where $A = \{i\}$.

$\Rightarrow$ each $f_i \in S$ splits in E.

$\Rightarrow E$ is a splitting field of S over k.

$\Rightarrow k$(zero of f_i in E) is a minimal splitting field of S over k.

Using Zorn's lemma or otherwise one can prove the following result. We, however, omit the proof.

Theorem 26: *Any two minimal splitting fields of a set of polynomials over k are isomorphic.*

We can now show the existence of an algebraic closure of a field k.

Theorem 27: *Let S be the set of all polynomials over k. Then a minimal splitting field of S over k is an algebraic closure of k.*

Proof: Let F be a minimal splitting field of S. Since F is generated by zeros of $f \in S$, F is generated by algebraic elements over k. So, F/k is algebraic.

Let $f = a_0 + a_1x + ... + a_nx^n \in F[x]$.

Let $E = k(a_0, a_1, ..., a_n) \subseteq F$.

Then $f \in E[x]$. Let E' be a minimal splitting field of f over E.

Let $f = \alpha(x - \alpha_1) \ldots (x - \alpha_n),\ \alpha_i \in E'$.

Then $E' = E(\alpha_1, ..., \alpha_n)$.

Since each α_i is algebraic over E, E'/E is algebraic. Also, each $a_i \in F$ is algebraic over k $\Rightarrow E/k$ is algebraic. So, E'/k is algebraic.

Let $g_i = Irr(k, \alpha_i)$

Let $g = g_1 g_2 \ldots g_n \in k[x]$

Now $g_i = (x - \alpha_i) f_i,\ f_i \in E'[x]$.

Therefore, $g = (x - \alpha_1) \ldots (x - \alpha_n) f_1 \ldots f_n$

$= \alpha(x - \alpha_1) \ldots (x - \alpha_n)\alpha^{-1} f_1 \ldots f_n$

$= ff',\ f' = \alpha^{-1} f_1 \ldots f_n \in E'[x]$

Let $g = \Sigma c_i x^i,\ f' = \Sigma b_i x^i,\ f = \Sigma a_i x^i$

where $c_i \in k,\ b_i \in E',\ a_i \in F$.

Now $c_r = \sum_i a_i\, b_{r-i}$

Let a_j be the first non zero coefficient in $f(x)$.

Therefore, $c_j = a_j b_0 \Rightarrow b_0 = a_j^{-1} c_j \in F$.

Suppose $b_0, b_1, \ldots, b_r \in F$.

Then $c_{j+r+1} = a_{j+r+1} b_0 + a_{j+r} b_1 + a_{j+1} b_r + a_j b_{r+1}$

$\Rightarrow b_{r+1} = a_j^{-1} (c_{j+r+1} - a_{j+r+1} b_0 \ldots - a_{j+i} b_r) \in F$

By induction, each $b_i \in F \Rightarrow f' \in F[x]$.

By hypothesis, $g \in k[x] \Rightarrow g$ splits in F.

Let $g = (x - \beta_1) \ldots (x - \beta_m)\ \beta_i \in F$

Suppose $f \in F[x]$ splits in some extension F' of F.

Let $f = d(x - d_1) \ldots (x - d_n), \quad d_i \in F' \subseteq F$.

Now $f' \in F[x] \subseteq F'[x] \Rightarrow f'$ splits in some extension F'' of F'.

Let $f' = e(x - e_1) \ldots (x - e_r), \quad e_i \in F'' \supseteq F' \supseteq F$

So, $g = ff' \Rightarrow g(d_i) = 0$ for all i

$\Rightarrow d_i - \beta_j = 0$ for some j depending on i

$\Rightarrow d_i = b_j \in F$

$\Rightarrow d_i \in F$ for all i

$\Rightarrow f$ splits in F.

Thus, F is algebraically closed.

Hence F is an algebraic closure of k.

Converse of above theorem is also true.

Theorem 28: *Let F be an algebraic closure of k. Then F is a minimal splitting field of the set S of all polynomials over k.*

Proof: Now F is an algebraic closure of k

$\Rightarrow F$ is algebraically closed

$\Rightarrow$ each $f \in S$ splits in F.

Let $F' = k$(zeros of $f \in S$ in $F) \subseteq F$.

Let $\alpha \in F'$. Then α is algebraic over k as F/k is algebraic. Let $p(x) = Irr(k, \alpha)$

Then α is a zero of $p(x) \in S$ in F.

So, $\alpha \in F' \Rightarrow F \subseteq F$.

Therefore, $F' = F \Rightarrow F$ is a minimal splitting field of F' of the set of all polynomials over k. The following is then immediate.

Theorem 29: *Any two algebraic closures of a field are isomorphic.*

Proof: Let k be a field and F_1, F_2 be algebraic closures of k. Then F_1, F_2 are minimal splitting fields of the set of all polynomials over k. So, F_1, F_2 are isomorphic by theorem 26.

Theorem 30: *Algebraic closure of a countable field is countable.*

Proof: Let k be a countable field. For each integer $n \geq 1$, there is a countable set of polynomials of degree n over k. Thus, the set S of all polynomials over k is countable.
Let $S = \{f_1, f_2, ..., f_n, ...\}$. Let $E_0 = k$, and E_1 be a minimal splitting field of f_1 over $E_0 = k$. In this way, let E_i be a minimal splitting field of f_i over E_{i-1}. Then $E_{n-1} \subseteq E_n$ for all n.

So, $E = \bigcup_n E_n$ is a field $\Rightarrow$ each f_i splits in E

$\Rightarrow E$ is a splitting field of S over k.

Let $F = k$(zeros of f_i in E) $\subseteq E$.

Then $k \subseteq F \subseteq E$ is a tower of fields and F is a minimal splitting field of S over k. So, F is an algebraic closure of $k \Rightarrow F$ is algebraically closed $\Rightarrow F$ is not finite. Since E is countable, F is also countable. Thus, any algebraic closure F' of k being isomorphic to F is also countable.

Lemma: *Let E be an algebraic extension of k and let* $\sigma : E \to E$ *be a k-homomorphism. Then* σ *is a k-automorphism.*

Proof: Let $\alpha \in E$, $p(x) = Irr\ (k, \alpha)$.

Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_r$ be zeros of $p(x)$ lying in E.

Let $E' = k(\alpha_1, \alpha_2, ..., \alpha_r) \subseteq E$.

Then E'/k is finite.

Let $p(x) = (x - \alpha_i)\ q_i(x), \quad q_i(x) \in k(\alpha_i)[x]$.

Since $\sigma(a) = a$ for all $a \in k$, $\sigma(p(x)) = p(x)$.

Therefore, $p(x) = \sigma(p(x)) = (x - \sigma(\alpha_i))\ \sigma(q_i(x))$

$\Rightarrow \quad \sigma(\alpha_i)$ is a zero of $p(x)$ for all i.

But $\sigma : E \to E \Rightarrow \sigma(\alpha_i) \in E$ for all i.

So, $\sigma(\alpha_i)$ is a zero of $p(x)$ in E for all i.

$\Rightarrow \quad \sigma(\alpha_i) \in E'$ for all i.

$\Rightarrow \quad \sigma : E' \to E'$ is k-homomorphism.

Also E'/k is finite. Since σ is also 1-1, $\sigma : E' \to E'$ must be onto (See below).

Therefore, $E' = \sigma(E') \Rightarrow \alpha = \sigma(\beta)$, for some $\beta \in E' \subseteq E$

$\Rightarrow \sigma : E \to E$ is onto $\Rightarrow \sigma$ is a k-automorphism of E.

That $\sigma : E \to E'$ is onto follows from the result

"If V is a finite dimensional vector space over F and $T : V \to V$ is a linear transformaion, then T is 1-1 iff T is onto". Here $\sigma : E' \to E'$ is a k-homomorphism $\Rightarrow \sigma$ is a linear transformation as $\sigma(a\beta) = \sigma(a)\ \sigma(\beta) = a\sigma(\beta)$ for all $a \in k$, $\beta \in E'$. Also E' as a vector space over k is finite dimensional.

We now give two characterisations of normal extensions. These are very useful in finding whether the given extension is normal or not.

Theorem 31: *Let K be an algebraic extension of k. Let $\bar{k}$ denote an algebraic closure of k such that $k \subseteq K \subseteq \bar{k}$. Then K/k is normal iff every k-homomorphism of K into $\bar{k}$ is a k-automorphism of K.*

Proof: Let K/k be normal. Let $\sigma : K \to \bar{k}$ be a k-homomorphism. Let $a \in K$. Since K/k is algebraic, a is algebraic over k. Let $p(x) = Irr\ (k, \alpha)$. Let $\sigma(a) = b$. Since $\sigma(p(x)) = p(x)$, b is a zero of $p(x)$ in $\bar{k} \supseteq K$.

Since K/k is normal, $p(x)$ splits in $K[x]$. So, $b \in K$.

Therefore, $\sigma : K \to K$ is k-homomorphism.

By above lemma, σ is a k-automorphism of K.

Conversely, let $\alpha \in K$ and $p(x) = Irr(k, \alpha)$.

Since $\bar{k}$ is an algebraic closure of k, $p(x)$ splits in $\bar{k}\,[x]$.

Let β be a zero of $p(x)$ in $\bar{k}$.

Then there exists a k-isomorphism $\sigma : k(\alpha) \to k(\beta)$ such that $\sigma(\alpha) = \beta$.

Since $\beta \in k$, $k(\beta) \subseteq k$. So, σ is a k-homomorphism from $k(\alpha)$ into $\bar{k}$.

Thus σ can be extended to k-homomorphism $\bar{\sigma} : K \to K$.

By hypothesis, $\bar{\sigma}$ is a k-automorphism of K.

So, $\bar{\sigma}(K) = K$. Also $\bar{\sigma}(a) = \sigma(a)$ for all $a \in k(\alpha)$. In particular $\bar{\sigma}(\alpha) = \sigma(\alpha) = \beta$.

Since $\alpha \in K$, $\bar{\sigma}(\alpha) \in \bar{\sigma}(K) = K \Rightarrow \beta \in$ K.

Therefore, $p(x)$ splits in $K[x]$.

Hence K/k is normal.

Theorem 32: *Let K be an algebraic extension of k. Then K/k is normal iff K is a minimal splitting field over k of a set of polynomials in $k[x]$.*

Proof: Let K/k be normal. Let $\alpha \in K$. Let $f_\alpha(x) = Irr\ (k, \alpha)$. Then $f_\alpha(x)$ splits in $K[x]$ for all $\alpha \in K$. Let $S = \{f_\alpha \mid \alpha \in K\}$. Let $F = k(\text{zeros of } f_\alpha \text{ in } K, \alpha \in K)$.

Then F is a minimal splitting field of S over k.

Clearly, $F \subseteq K$. Also $\alpha \in K \Rightarrow \alpha$ is a zero of $f_\alpha \Rightarrow \alpha \in F$. So, $F = K$. Thus K is a minimal splitting field of S over k.

*Converse*ly, let K be a minimal splitting field of a set S of polynomials over k. Let $\bar{k}$ be an algebraic closure of k such that $k \subseteq K \subseteq \bar{k}$.

Let $\sigma : K \to \bar{k}$ be a k-homomorphism.

Let $a \in K$ be a zero of some $f \in k[x]$ in S.

Then $\sigma(a)$ is also a zero of f as σ is a k-homomorphism.

As f splits in $K[x]$, we can write $f = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in K$, $\alpha \in k$.

Since $\sigma(\alpha_i)$ is a zero of f for all i, $\sigma(\alpha_i) \in \bar{k}$, $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ as $\bar{k}$ can't have more than n zeros of f. So, $\sigma(\alpha_i) \in K$ for all i.

Let $T = \{\text{zeros of } f \text{ in } K, f \in S\}$. Then $\sigma : T \to T$. Also $\sigma : T \to T$ is 1-1 as $\sigma : K \to \bar{k}$ is 1-1.

Let $b \in \sigma(K)$. Then $b = \sigma(c)$, $c \in K$.

Now $c \in K \Rightarrow c = \dfrac{f(\beta_1, \ldots, \beta_n)}{g(\beta_1, \ldots, \beta_n)}$, $\beta_i \in T$.

Then $b = \dfrac{f(\sigma(\beta_1), \ldots, \sigma(\beta_n))}{g(\sigma(\beta_1), \ldots, \sigma(\beta_n))} = \dfrac{f(\gamma_1, \ldots, \gamma_n)}{g(\gamma_1, \ldots, \gamma_n)}$, $\gamma_i \in T$

So, $b \in K \Rightarrow \sigma(K) \subseteq K$. Also $d \in K \Rightarrow d = \dfrac{f_1(\delta_1, \ldots, \delta_m)}{g_1(\delta_1, \ldots, \delta m)}$,

$$\delta_i \in T \Rightarrow d = \frac{f_1(\sigma(u_1), \ldots, \sigma(u_m))}{g_1(\sigma(u_1), \ldots, \sigma(u_m))},\ u_i \in T$$

$$\Rightarrow \quad d = \frac{\sigma(f_1(u_1, \ldots, u_m))}{\sigma(g_1(u_1, \ldots, u_m))} = \sigma\left(\frac{f_1(u_1, \ldots, u_m)}{g_1(u_1, \ldots, u_m)}\right),\ u_i \in T$$

$$\Rightarrow \quad d \in \sigma(K) \Rightarrow K \subseteq \sigma(K) \Rightarrow \sigma(K) = K.$$

So, $\sigma : K \to K$ is onto Thus, σ is a k-automorphism of K. By previous result, K/k is normal.

Summarising, the last two theorems we get

Theorem 33: *Let K be an algebraic extension of k. Then following are equivalent:*

(*i*) *K/k is normal.*

(*ii*) *Every k-homomorphism of K into* $\bar{k}$ *is a k-automorphism of K where* $\bar{k}$ *is an algebraic closure of k.*

(*iii*) *K is a minimal splitting field of a set of polynomials over k.*

Theorem 34: *Let F/k be algebraic. If every finite extension of k admis a k-homomorphism into F, then F is an algebraic closure of k.*

Proof: Let $f = a_0 + a_1x + \ldots + a_nx^n \in k[x]$. Let E be a minimal splitting field of f over k. Then E/k is finite.

By hypothesis, there is a k-homomorphism $\sigma : E \to F$.

Let $f = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in E$.

Then $f = \sigma f = \alpha(x - \sigma(\alpha_1)) \ldots (x - \sigma(\alpha_n))$

$\Rightarrow f$ splits in F

$\Rightarrow$ every polynomial over k splits in F.

Let F' be a minimal splitting field of the set of all polynomials over k.

Then $F' = k(\text{zero of } f \in k[x] \text{ in } F) \subseteq F$

Also, $\alpha \in F \Rightarrow \alpha$ is algerbraic over k.

Let $p(x) = Irr(k, \alpha)$. Then $\alpha \in F$ is a zero of $p(x) \in k[x]$

$\Rightarrow \quad \alpha \in F' \Rightarrow F \subseteq F' \Rightarrow F = F'$.

So, F is an algebraic closure of k.

Theorem 35: *Let K/k be an algebraic extension. Let $\bar{k}$ be an algebraic closure of k such that $k \subseteq K \subseteq \bar{k}$. Let F be an algebraically closed field such that $k \subseteq F$. Then any k-homomorphism from K into F can be extended to a k-homomorphism from $\bar{k}$ into F.*

Proof: Let $\alpha : K \to F$ be a k-homomorphism.

Let $$S = \left\{ (E, g) \;\middle|\; \begin{array}{l} E \text{ is a subfield of } \bar{k} \text{ and } K \subseteq E \\ g : E \to F \text{ is a homomorphism extending } \sigma \end{array} \right\}.$$

Define a relation $\leq$ on S as follows:

$(E_1, g_1) \leq (E_2, g_2)$ if $E_1 \subseteq E_2$ and g_2 is an extension of g_1 to E_2.

Then $\leq$ is a partial order on S.

Let $\{(E_i, g_i)\}_i$ be a chain in S. Let $E = \bigcup_i E_i$ and define $g : E \to F$ such that $g(\alpha) = g_i(\alpha)$ if $\alpha \in E_i$.

Then $(E, g) \in S$ and is an upper bound of the chain $\{(E_i, g_i)\}$.

By Zorn's lemma S has a maximal element, say (E_0, g_0).

We show that $E_0 = \bar{k}$. Suppose $E_0 \neq \bar{k}$.

Then we can find $a \in \bar{k}$ such that $a \notin E_0$. Since $\bar{k}/k$ algebraic, a is algebraic over k.

Let $f = Irr(k, a)$. Now $k \subseteq E_0 \Rightarrow f \in E_0[x]$. Since F is algebraically closed, $g_0(f) \in F[x]$ splits in $F[x]$.

Let b be a zero of $g_0(f)$ in F. Then there exists an isomorphism $\theta : E_0(a) \to E_0'(b)$ extending g_0, where $E_0' = g_0(E_0)$.

But $b \in F$, $E_0' \subseteq F \Rightarrow E_0'(b) \subseteq F$. So, $\theta : E_0(a) \to F$ is a homomorphism extending g_0.

Therefore, $(E_0, g_0) \leq (E_0(a), \theta)$ and $E_0 \neq E_0(a) \Rightarrow (E_0, g_0) \neq (E_0(a), \theta)$.This contradicts the maximality of (E_0, g_0).

So, $E_0 = \bar{k}$. Therefore, $g_0 : \bar{k} \to F$ is a homomorphism extending σ.

Cor: Let K/k be algebraic such that $k \subseteq K \subseteq \bar{k}$. Then any k-homomorphism of K into $\bar{k}$ can be extended to a k-homomorphism of $\bar{k}$ into $\bar{k}$.

Proof: Take $F = \bar{k}$ in above theorem.

Cor.: Any two algebraic closures of a field k are k-isomorphic.

Proof: Let K_1, K_2 be algebraic closures of k.

Now $k \subseteq K_1, K_2$. Let $\sigma : k \to K_1$ be the inclusion map *i.e.*, $\sigma(\alpha) = \alpha$ for all $\alpha \in k$.

By taking $K = \bar{k}$, $k = K_2$, $F = k_1$, in above theorem, σ can be extended to a k-homomorphism $\eta : K_2 \to K_1$.

As $K_2 \cong \eta(K_2)$ and K_2 is algebraically closed we find $\eta(K_2)$ is algebraically closed.

Also $k \subseteq K_2 \Rightarrow \eta(K_2)$ can be regarded as an extension of k.

So, we have $k \subseteq \eta(K_2) \subseteq K_1$.

Since K_1/k is algebraic, $K_1/\eta(K_2)$ is also algebraic.

But $\eta(K_2)$ is algebraically closed $\Rightarrow \eta(K_2)$ has no algebraic extension other than itself $\Rightarrow K_1 = \eta(K_2) \Rightarrow \eta$ is onto $\Rightarrow \eta$ is a k-isomorphism.

Hence, K_1, K_2 are k-isomorphic.

Note: This result was proved earlier also.

We now prove the result on normal extensions stated in the beginning of this section.

Theorem 36: *Let k, E, K be fields such that $k \subseteq E \subseteq K$ and K/k is normal. Then any k-homomorphism $\sigma : E \to K$ can be extended to a k-automorphism of K.*

Proof: Since K/k is normal, K is minimal splitting field a set of polynomials over k. Let $\bar{k}$ denote an algebraic closure of k.

Then $\bar{k}$ is a minimal splitting field of the set of all polynomials over k.

So K can be regarded as a subfield of $\bar{k}$.

Now $\sigma : E \to K$ is a k-homomorphism.

Thus $\sigma : E \to \bar{k}$ is a k-homomorphism.

Since K/k is algebraic, so is E/k. Now $k \subseteq E \subseteq \bar{k}$, E/k is algebraic.

By previous theorem, σ can be extended to a k-homomorphism $\tau : \bar{k} \to \bar{k}$. Therefore, $\tau : K \to \bar{k}$ is also a k-homomorphism.

Again, K/k is normal $\Rightarrow \tau$ is a k-automorphism of K.

This proves the result.

Product of Fields: Let M, N be extensions of a field k such that M, N are contained in a field L. Then MN is defined as the smallest subfield of L containing M and N.

Let $$M[N] = \{a_1b_1 + \ldots + a_nb_n \mid a_i \in M,\ b_i \in N\}.$$
$$n = \text{finite}$$

Then $M[N]$ is an integral domain. Let K be field of quotients of $M[N]$. Clearly, $M \subseteq M[N]$, $N \subseteq M[N]$.

So, $$M, N \subseteq M[N] \subseteq K.$$

But MN is the smallest field containing M, N, $MN \subseteq K$.

Also, $$\sum_{i=1}^{n} a_ib_i \in M[N], \text{ for all } a_i \in M,\ b_i \in N$$

$$\Rightarrow \quad \sum_{i=1}^{n} a_ib_i \in MN, \text{ as } \left.\begin{array}{l} a_i \in M \Rightarrow a_i \in MN \\ b_i \in N \Rightarrow b_i \in MN \end{array}\right\}$$

$$\Rightarrow \quad M[N] \subseteq MN.$$

But K is the smallest field containing $M[N] \Rightarrow K \subseteq MN$

$$\Rightarrow \quad K = MN$$

$\Rightarrow MN$ is a quotient field of $M[N]$.

Lemma: *Let K_1, K_2 be extensions of a field k contained in a field K and let σ be a k-homomorphism of K in some field L. Then*

$$\sigma(K_1K_2) = \sigma(K_1)\ \sigma(K_2).$$

Proof:

Let $\alpha = \dfrac{a_1b_1 + ... + a_nb_n}{a_1'b_1' + ... + a_n'b_n'} \in K_1K_2$

where $a_i, a_i' \in K_1,\ b_i, b_i' \in K_2$

Then $\sigma(\alpha) = \dfrac{\sigma(a_1)\sigma(b_1) + ... + \sigma(a_n)\ \sigma(b_n)}{\sigma(a_1')\sigma(b_1') + ... + \sigma(a_n')\ \sigma(b_n')} \in \sigma(K_1)\sigma(K_2)$

$\Rightarrow\ \sigma(K_1K_2) \subseteq \sigma(K_1)\ \sigma(K_2)$

Let $\beta \in \sigma(K_1)\ \sigma(K_2)$.

Then $\beta = \dfrac{\sigma(c_1)\sigma(d_1) + ... + \sigma(c_r)\sigma(d_r)}{\sigma(c_1')\sigma(d_1') + ... + \sigma(c_r')\sigma(d_r')}$

$= \sigma(\alpha)$, where $\alpha = \dfrac{c_1d_1 + ... + c_rd_r}{c_1'd_1' + ... + c_r'd_r'} \in K_1K_2$

$\Rightarrow\ \beta \in \sigma(K_1K_2)$

$\Rightarrow\ \sigma(K_1)\sigma(K_2) \subseteq \sigma(K_1K_2)$

$\Rightarrow\ \sigma(K_1K_2) = \sigma(K_1)\sigma(K_2)$.

Theorem 37: *If E, F are normal extensions of k, then EF and $E \cap F$ are normal over k.*

Proof: (*i*) Let $\bar{k}$ denote an algebraic closure of *k*. Let σ be a *k*-homomorphism from *EF* into $\bar{k}$ such that $k \subseteq EF \subseteq \bar{k}$.

Now $\sigma(EF) = \sigma(E)\sigma(F)$ by above lemma.

Since $E, F \subseteq EF$, σ is also *k*-homomorphism from *E* into $\bar{k}$ and *F* into $\bar{k}$. Also *E*, *F* are normal over $k \Rightarrow \sigma : E \to E$ and $\sigma : F \to F$ are *k*-automorphisms

$\Rightarrow\ \sigma(E) = E,\ \sigma(F) = F$

$\Rightarrow\ \sigma(EF) = EF$

Now $\sigma : EF \to \bar{k}$ is also a *k*-homomorphism from *EF* into *EF*. But $\sigma(EF) = EF$

$\Rightarrow \sigma : EF \to EF$ is onto.

So, $\sigma : EF \to EF$ is a *k*-automorphism.

$\Rightarrow EF/k$ is normal.

(*ii*) Let σ be a *k*-homorphism from $E \cap F$ into $\bar{k}$ such that $k \subseteq E \cap F \subseteq \bar{k}$. Then σ can be extended to $\bar{k}$-homomorphism $\eta : \bar{k} \to \bar{k}$.

Since E/k is normal, *E* is a minimal splitting field of a set of polynomials over *k*. However, $\bar{k}$ is a minimal splitting field of the set of all polynomials over *k*. So, *E* can be regarded as a subfield of $\bar{k}$. Therefore, $k \subseteq E \subseteq \bar{k}$. Similarly $k \subseteq F \subseteq \bar{k}$.

Let $\eta \mid E = \eta_1,\ \eta \mid F = \eta_2$.

Now $\eta_1 : E \to \bar{k}$, $\eta_2 : F \to \bar{k}$ are k-homomorphisms. Since E/k, F/k are normal, η_1 and η_2 are k-automorphism of E and F respectively. So, $\eta_1(E) = E$, $\eta_2(F) = F$. Now $E \cap F \subseteq E$, $F \subseteq \bar{k}$.

Thus, $\eta(E \cap F) = \eta(E) \cap \eta(F)$
$= \eta_1(E) \cap \eta_2(F)$
$= E \cap F$.

But $\eta \mid E \cap F = \sigma$

$\Rightarrow$ $\sigma(E \cap F) = E \cap F$

$\Rightarrow \sigma$ is a k-automorphism of $E \cap F$.

$\Rightarrow E \cap F/k$ is normal.

Automorphisms of Field extensions

The purpose of this section is to find conditions under which a finite extension F/K is separable in terms of k-automorphisms of F. We first show that the number of k-automorphisms of F is at most $n = [F : K]$. We then show that the upper bound n is achieved iff F/K is both normal and separable.

Definition: Let $\sigma_1, \sigma_2, ..., \sigma_n$ be homomorphisms from a field E into a field E'. Then, $\sigma_i s$ are called *linearly independent* over E' if $\alpha_1\sigma_1 + ... + \alpha_n\sigma_n = 0$, $\Rightarrow \alpha_i = 0 \ \forall \ i$ where $\alpha_i \in E'$.

Note, $\alpha_i\sigma_i : E \to E'$ s.t., $(\alpha_i\sigma_i)(a) = \alpha_i(\sigma_i(a)) \quad \forall \ a \in E$.

In the following result, we show that any family of homomorphisms from a field into another field is linearly independent.

Theorem 38: (Dedekind). *Let $(\sigma_i)_i$ be a family of distinct homomorphism from a field E into a field E'. Then $\{\sigma_i\}_i$ is linearly independent over E'.*

Proof: Suppose $\{\sigma_i\}_i$ is not linearly independent over E'. Then $\exists$ finite subset of $\{\sigma_i\}_i$ which is not linearly independent over E'. (*i.e.*, it is linearly dependent over E'.). Let $\{\sigma_1, \sigma_2, ..., \sigma_r\}$ be a minimal linearly dependent subset of $\{\sigma_i\}_i$ over E'.

So, $\exists \ \alpha_1, \alpha_2, ..., \alpha_r \in E'$ s.t.,

$\alpha_1\sigma_1 + ... + \alpha_r\sigma_r = 0$ and some $\alpha_i \neq 0$.

$\Rightarrow (\alpha_1\sigma_1 + ... + \alpha_r\sigma_r)(a) = 0 \quad \forall \ a \in E$

$\Rightarrow \alpha_1\sigma_1(a) + ... + \alpha_r\sigma_r(a) = 0 \quad \forall \ a \in E$

Suppose $\alpha_1 \neq 0$.

Now $\sigma_1(a) = (-\alpha_1^{-1}\alpha_2)\sigma_2(a) + ... + (-\alpha_1^{-1}\alpha_r)\sigma_r(a) \ \forall \ a \in E$

$\sigma_1(a) = \beta_2\sigma_2(a) + ... + \beta_r\sigma_r(a)$, $\beta_i = -\alpha_1^{-1}\alpha_i \in E'$, $\forall \ a \in E \quad (i)$

So, $\sigma_1(ab) = \beta_2\sigma_2(ab) + ... + \beta_r\sigma_r(ab) \quad \forall \ a, b \in E$

$\Rightarrow \sigma_1(a)\sigma_1(b) = \beta_2\sigma_2(a)\sigma_2(b) + ... + \beta_r\sigma_r(a)\sigma_r(b) \quad \forall \ a, b \in E \quad (ii)$

Consider $(ii) - \sigma_1(b)\ (i)$.

Then $0 = \beta_2\sigma_2(a)(\sigma_2(b) - \sigma_1(b)) + ... + \beta_r\sigma_r(a)(\sigma_r(b) - \sigma_1(b))$

$$= \sum_{2}^{r} \beta_i (\sigma_i(b) - \sigma_1(b)) \sigma_i(a) \quad \forall\ a \in E$$

$$\Rightarrow\ 0 = \sum_{2}^{r} \beta_i (\sigma_i(b) - \sigma_1(b)) \sigma_i$$

$$\Rightarrow\ \beta_i(\sigma_i(b) - \sigma_1(b)) = 0 \quad \forall\ i = 2, 3, ..., r, \forall\ b \in E$$

as $\{\sigma_1, \sigma_2, ..., \sigma_r\}$ is a minimal linearly dependent subset of $\{\sigma_i\}_i$.

Since $\sigma_i \neq \sigma_1\ \forall\ i > 1, \exists\ c_i \in E$ s.t., $\sigma_i(c_i) \neq \sigma_1(c_i)$.

Now $\beta_i(\sigma_i(c_i) - \sigma_1(c_i) = 0 \quad \forall\ i = 2, 3, ...,$

$\Rightarrow\ \beta_i = 0 \quad \forall\ i = 2, 3, ..., r.$

So, $\sigma_1(a) = 0 \quad \forall\ a \in E$, by (i)

$\Rightarrow\ \sigma_1(1) = 0$

$\Rightarrow 1 = 0$, which is not true.

Thus $\{\sigma_i\}_i$ is a linearly independent set over E'.

Theorem 39: *Let E, E′ be extensions of K. Let* $[E : K] = n$. *Then, there are at most n K-homomorphisms from E into E′.*

Proof: Let $\{u_1, u_2, ..., u_n\}$ be a basis of E/K. Let $\sigma_0, \sigma_1, ..., \sigma_n$ be $n + 1$ distinct K-homomorphisms from E into E'.

Consider the system of equations $\sum_{i=0}^{n} \sigma_i(u_j)x_i = 0, \quad j = 1, 2, ..., n.$

Then, we have n equation in $n + 1$ unknowns $x_i s \in E'$. Since the number of equations is less than number of unknowns, the above system of equations has a non zero solution, say $c_0, c_1, ..., c_n \in E'$ where some $c_i \neq 0$.

Let $a \in E$. Since $\{u_1, u_2, ..., u_n\}$ spans E/K, $a = \alpha_1 u_1 + ... + \alpha_n u_n$, $\alpha_i \in K$

$$\text{Thus } \sum_{i=0}^{n} \sigma_i(a)\, c_i = \sum_i \sigma_i \left(\sum_j \alpha_j u_j \right) c_i$$

$$= \sum_i \sum_j (\sigma_i(\alpha_j)\, \sigma_i(u_j)) c_i$$

$$= \sum_i \sum_j (\alpha_j \sigma_i(u_j)) c_i$$

$$= \sum_j \alpha_j \left(\sum_i \sigma_i(u_j)) c_i \right)$$

$$= 0 \quad \text{as } \sum_i \sigma_i(u_j)\, c_i = 0$$

$$\Rightarrow \quad \sum_{i=0}^{n} c_i \sigma_i(a) = 0 \quad \forall\ a \in E$$

$$\Rightarrow \quad \sum_{i=0}^{n} c_i \sigma_i = 0 \Rightarrow c_i = 0 \quad \forall\ i \text{ by above theorem.}$$

But some $c_i \neq 0$. So, we get a contradiction. Thus, there are at most n K-homomorphisms from E into E'.

Cor.: There are at most n K-automorphisms of E, where $n = [E : K]$.

Proof: Take $E' = E$ in above theorem. By automorphism of E, we mean isomorphism of E into E. Now any K-homomorphism from E into E is a linear transformation from E into E as vector space over K. Also, any homomorphism from E into E is 1-1 and so onto as $[E : K]$ = finite. By above theorem, there are at most n K-automorphisms of E where $n = [E : K]$.

Example 11: Define $\theta : \mathbf{C} \to \mathbf{C}$ s.t.,

$$\theta(z) = \bar{z}\text{, where } \bar{z} = \text{conjugate of } z$$

Then θ is **R**-homomorphism and $\theta \neq I$. So, θ, I are two distinct **R**-homomorphisms of **C** into **C**. But $[\mathbf{C} : \mathbf{R}] = 2 \Rightarrow$ there are at most two **R**-automorphismss of **C**. Also, any **R**-homomorphism of **C** into **C** is an **R**-automorphism of **C**. So, θ, I are only **R**-automorphisms of **C**. Note, **C**/**R** is normal as $[\mathbf{C} : \mathbf{R}] = 2$ and **C**/**R** is separable as char $\mathbf{R} = 0 \Rightarrow$ **R** is perfect $\Rightarrow$ every algebraic extension of **R** is separable.

Example 12: Let α be the real cube root of $f(x) = x^3 - 2$. Let $F = \mathbf{Q}(\alpha) \subseteq \mathbf{R}$. Let θ be a **Q**-automorphism of F.

Since α is a root of $f(x)$ in **R**, $\theta(\alpha)$ is a root of $\theta(f(x)) = f(x)$ in **R**.

So, $\theta(\alpha) = \alpha$. But $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg Irr(\mathbf{Q}, \alpha) = \deg f(x) = 3$ and $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

$\Rightarrow \mathbf{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbf{Q}\}$.

Since $\theta(a_i) = a_i$ and $\theta(\alpha) = \alpha$, θ fixes every element of $\mathbf{Q}(\alpha)$.

So, $\theta = I \Rightarrow$ Identity map is the only **Q**-automorphism of $F = \mathbf{Q}(\alpha)$.

Note $\mathbf{Q}(\alpha)/\mathbf{Q}$ is separable as char $\mathbf{Q} = 0 \Rightarrow$ **Q** is perfect $\Rightarrow$ every algebraic extension of **Q** is separable.

As seen before $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Thus, we notice that if E/K is separable but not normal, then one may not get the *full quota* (*i.e.*, $[E : K]$) of K-automorphisms of E.

Example 13: Let char $K = p$ and $F = K(t)$. Then $x^p - t$ is irreducible over F.

Let α be a root of $f(x)$ in some extension of F.

Now $f(x) = x^p - t$ is irreducible over $F \Rightarrow [F(\alpha) : F] = p$.

$\Rightarrow \{1, \alpha, ..., \alpha^{p-1}\}$ is a basis of $F(\alpha)/F$.

So, $$F(\alpha) = \{\sum_{i=0}^{p-1} a_i\alpha^i \mid a_i \in F\}.$$

If θ is F-automorphism of $F(\alpha)$, then $\theta(\alpha)$ is a root of $f(x) = \theta(f(x))$ in $F(\alpha)$.

But α is the only root of $f(x)$ in any extension of F.

$\Rightarrow \theta(\alpha) = \alpha \Rightarrow \theta$ fixes every element of $F(\alpha)$.

$\Rightarrow \theta$ is the identity map.

Thus, identity map is the only F-automorphism of $F(\alpha)$.

Since α is not a simple root of $f(x)$, α is not separable over F.

Therefore, if E/K is not sparable then one may not get $[E : K]$, K-automorphisms of E.

The above two examples clearly demonstrate that in order that an extension E/K has $[E : K]$, K-automomorphisms of E, E/K should be both normal and separable. In the first example, we saw that we do get $[E : K]$, K-automorphisms of E when E/K is both normal and separable. We would like to prove this in general.

Theorem 40: *Let $K \subseteq L \subseteq F \subseteq E$ be a tower of fields. Suppose E/K is finite normal. If r is the number of K-homorphisms from L into E and s the number of L-homomorphisms from F into E, then the number of K-homomorphisms from F into E is rs.*

Proof: Let $\sigma_1, \ldots, \sigma_r$ be the K-homomorphisms of L into E and $\tau_1, \tau_2, \ldots, \tau_s$ be the L-homomorphisms from F into E. Since E/K is finite normal, each σ_i can be extended to K-automorphisms $\bar{\sigma}_i$ of E.

We show that $\{\bar{\sigma}_i\tau_j \mid 1 \le i \le r, 1 \le j \le s\}$ is the set of distinct K-homomorphisms from F into E.

Suppose $\bar{\sigma}_i\ \tau_j = \bar{\sigma}_p\,\tau_q$. Then $\bar{\sigma}_i\tau_j(a) = \bar{\sigma}_p\ \tau_q(a), \quad \forall\ a \in F$

$\Rightarrow\ \bar{\sigma}_i\tau_i(l) = \bar{\sigma}_p\,\tau_q(l) \quad \forall\ l \in L$

$\Rightarrow\ \bar{\sigma}_i(l) = \bar{\sigma}_p\,(l) \quad \forall\ l \in L$

$\Rightarrow\ \sigma_i = \sigma_p \Rightarrow i = p \Rightarrow \tau_j = \tau_q \Rightarrow j = q.$

Let σ be any K-homomorphisms from F into E. Then $\sigma \mid L$ is a K-homomorphisms from L into E.

$\Rightarrow\ \sigma \mid L\ = \sigma_i$ for some i.

Then $\bar{\sigma}_i^{-1}\sigma$ is K-homomorphisms from F into E.

So, $\bar{\sigma}_i^{-1}\sigma(l) = \bar{\sigma}_i^{-1}\sigma_i(l) = \bar{\sigma}_i^{-1}\ \bar{\sigma}_i(l) = l \quad \forall\ l \in L$

$\Rightarrow\ \bar{\sigma}_i^{-1}\sigma$ is L-homomorphism from F into E

$\Rightarrow\ \sigma_i^{-1}\sigma = \tau_j$ for some $j \Rightarrow \sigma = \bar{\sigma}_i\tau_j$

Thus, $\bar{\sigma}_i\,\tau_j$ are the only K-homomorphisms from F into E and so, there are exactly rs K-homomorphisms from F into E.

Theorem 41: *Let $K \subseteq E \subseteq E'$ be a tower of fields. Suppose E'/K is finite normal. Then E/K is separable if and only if the number of K-homomorphisms from E into E′ is $[E : K]$.*

Proof: Suppose E/K is separable. We prove the result by induction on $n = [E : K]$.

If $n = 1$, then $E = K$ and $I : E \to E'$ s.t., $I(a) = a$ is K-homomorphisms from E into E'.

So, the result is true for $n = 1$.

Let $n > 1$. Assume that the result is true for all integers $< n$.

Let $a \in E$, $a \notin K$.

Now $K \subseteq K(a) \subseteq E \subseteq E'$ and E'/K is finite normal $\Rightarrow E'/K(a)$ is finite normal.

Also, $[E : K] = [E : K(a)]\ [K(a) : K]$ and $[K(a) : K] > 1$

$\Rightarrow [E : K(a)] < [E : K] = n$.

Since E/K is separable $E/K(a)$ is also separable.

By induction hypothesis (applied to tower of fields $K(a) \subseteq E \subseteq E'$), the number of $K(a)$-homomorphisms from E into E' is $[E : K(a)]$.

Let $p(x) = Irr(K, a)$. Since $a \in E$, a is separable over K. So, all roots of $p(x)$ are simple.

Let deg $p(x) = r$. Since E'/K is normal, $p(x)$ splits in E' as $a \in E \subseteq E'$.

Let $a = a_1, a_2, ..., a_r$ be distinct roots of $p(x)$ in E'. Then $\exists$ K-isomorphisms

$\sigma_i : K(a) \to K(a_i)$ s.t., $\sigma_i(a) = a_i \quad \forall\ i = 1, 2, ..., r$. $\sigma_i's$, $a_i's$ being distinct.

Since $a_i \in E'$, $\sigma_i's$ are r K-homomorphisms from $K(a)$ into E'.

Also as $[K(a) : K] = \deg Irr\,(K, a) = \deg p(x) = r$, these $\sigma_i's$ are only K-homomorphisms from $E(a)$ into E'.

By previous theorem these are excatly $[E : K(a)]\ [K(a) : K] = [E : K]$, K-homomorphisms from E into E'.

So, the result is true in this case. By induction the result is true for all $n \geq 1$.

Conversely, let there be $n = [E : K]$ K-homomorphisms from E into E'. Let $a \in E$.

Now, the number m of K-homomorphisms from $K(a)$ into E' is at most $r = [K(a) : K]$.

Let $m < r$. Let s be the number of $K(a)$-homomorphisms from E into E'. Then

$$s \leq [E : K(a)] = \frac{[E:K]}{[K(a):K]} = \frac{n}{r}.$$

By above theorem, the number of K-automorphisms from E into E' is $ms < r\frac{n}{r} = n$, a contradiction. So, $m = r$. That is, the number of K-homomorphisms from $K(a)$ into E' is $[K(a) : K] = \deg Irr\ (K, a)$.

Let $p(x) = Irr\ (K, a)$, deg $p(x) = r$.

Since E'/K is normal, $p(x)$ splits in E' as $a \in E \subseteq E'$.

Let $a = a_1, a_2, ..., a_t$ be distinct roots or $p(x)$ in E'.

Then, for each i $\exists$ K-isomorphisms $\theta_i : K(a) \to K(a_i)$ s.t., $\theta_i(a) = a_i$.

Since $a_i \in E'$, $K(a_i) \subseteq E'$. So, $\theta_i : K(a) \to E'$ is K-homomorphism.

Again as a_is are distinct, θ is are also distinct K-homomorphisms from $K(a)$ into E'.

If θ is a K-homomorphisms from $K(a)$ into E', then a is a root of $p(x)$ in E

$\Rightarrow \theta(a)$ is a root of $\theta(p(x)) = p(x)$ in E'

$\Rightarrow \theta(a) = a_i$ for some $i \Rightarrow \theta(a) = \theta_i(a)$ for some $i \Rightarrow \theta = \theta_i$ for some i.

So, $\theta_1, \theta_2, ..., \theta_t$ are the only K-homomorphisms from $K(a)$ into E

$\Rightarrow t = [K(a) : K] = \deg p(x) = r$.

$\Rightarrow$ all roots of $p(x)$ are distinct and so simple.

$\Rightarrow a$ is separable over K. Thus, E/K is separable.

Cor. 1: Let E/K be finite normal. Then E/K is separable if and only if the number of K-automorphisms of E is $[E : K] = n$.

Proof: Since E/K is finite, a K-homomorphism of E is K-automorphism of E and conversely. The result then follows by above theorem.

Cor. 2: Let $K \subseteq E \subseteq E'$ be a tower of fields s.t., E/K and E'/E are finite separable. Then E'/K is also finite separable.

Proof: Let $[E : K] = r$, $[E' : E] = s$. Since E/K, E'/E are finite so is E'/K.

Thus $\exists$ an extension F of K s.t., F/K is finite normal and $K \subseteq E \subseteq E' \subseteq F$.

By above theorem since E/K is separable, there are r K-homomorphisms from E into F.

Now F/K is normal $\Rightarrow$ F/E is also normal.

As E'/E is separable, there are s E-homomorphisms from E' into F.

Therefore, there are rs K-homomorphisms from E' into F. But $rs = [E' : K]$.

By above theorem then E'/K is finite seperable.

Cor.3: Let E be an extension of K. Let $a_1, a_2, ..., a_n \in E$ be separable over K. Then $K(a_1, a_2, ..., a_n)/K$ is separable.

Proof: We prove the result by induction on n. Since $a_1, a_2, ..., a_n$ are separable over K, $a_1, a_2, ..., a_n$ are algebraic over K. So, $K(a_1, a_2, ..., a_n)/K$ is finite. Let E'/K be finite normal extension s.t., $K \subseteq K(a_1, ..., a_n) \subseteq E'$. Let $n = 1$. Let $p(x) = Irr\ (K, a_1)$, deg $p(x) = r$. Then $\exists$ r K-homomorphisms from $K(a_1)$ into E' as seen in above theorem. But $r = [K(a_1) : K]$. By above theorem, $K(a_1)/K$ is separable. So, the result is true for $n = 1$. Let $n > 1$. Assume that the result is true for all integers $< n$. By induction hypothesis, $K(a_1, ..., a_n)/K$ is finite separable. Also, a_n is separable over K and $K \subseteq K(a_1, \ldots, a_{n-1}) \subseteq K(a_1, \ldots, a_n) \Rightarrow a_n$ is separable over $K(a_1, \ldots, a_{n-1}) \Rightarrow K(a_1, ..., a_n) \mid K(a_1, ..., a_n)$ is finite separable.. By above corollary, $K(a_1, ..., a_n)/K$ is separable. By induction the result is true $\forall\ n \geq 1$.

Cor. 4: Let $F \subseteq K \subseteq E$ be a tower of fields s.t., E/K and K/F are separable. Then E/F is also separable.

Proof: Let $a \in E$.

Let $p(x) = Irr\ (K, a)$

$= b_0 + b_1x + ... + b_rx^r, \quad b_i \in K$

Let $K' = F(b_0, b_1, ..., b_r) \subseteq K$

$b_i \in K \Rightarrow b_i$ is separable over F

$\Rightarrow K'/F$ is separable by above Cor.

Since $p(x)$ is irreducible over K, it is also irreducible over K'.

So, $p(x) = Irr\ (K', a)$

Now $K' \subseteq K \subseteq E$ and $a \in E$ is separable over $K \Rightarrow p'(a) \neq 0 \Rightarrow a$ is separable over $K' \Rightarrow K'(a)/K'$ is separable and finite. Also, K'/F is finite separable.

So, $K'(a)/F$ is finite separable.

$\Rightarrow$ a is separable over F.

Thus, E/F is separable.

Theorem 42: *Let $K \subseteq E \subseteq E'$ be a tower of fields s.t., E'/K is finite normal. Then following are equivalent:*

(*a*) *There are exactly $n = [E : K]$ K-homomorphisms from E into E'.*

(*b*) *E/K is separable.*

(*c*) *E/K is generated by separable elements.*

Proof: (*a*) $\Leftrightarrow$ (*b*) follows from previous theorem

(*b*) $\Rightarrow$ (*c*) $[E : K] = n \Rightarrow E = K(a_1, ..., a_n)$. Since $a_i \in E$, a_i is separable over K. So, E is generated by separable elements over K.

(*c*) $\Rightarrow$ (*b*). Let $E = K(S)$, where $S \subseteq E$ is a set of separable elements over K. Let $a \in E$, then $a = \dfrac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)}$, $f, g \in K[x_1, ..., x_n]$, $u_i \in S$. So, $a \in K(u_1, u_2, ..., u_n)$. Since $u_1, u_2, ..., u_n$ are separable over K, $K(u_1, u_2, ..., u_n)/K$ is separable. Therefore, a is separable over K. Thus, E/K is separable. This proves (*b*).

Theorem 43 (Artin's): *Let E be a field, G the group of automorphisms of E and suppose K is the set of elements of E fixed by G. Then K is a subfield of E, called the fixed field of G. E/K is finite if and only if G is finite. In that case, $[E : K] = o(G)$.*

Proof: $K = \{a \in E \mid \sigma(a) = a \quad \forall\ \sigma \in G\}$

$0, 1 \in K \Rightarrow K \neq \varphi$.

Let $a, b \in K$. Then $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b \Rightarrow a \pm b \in K$. Also $\sigma(ab) = \sigma(a)\ \sigma(b) = ab \Rightarrow ab \in K$. If $b \neq 0$, then $\sigma(ab^{-1}) = \sigma(a)\ \sigma(b)^{-1} = ab^{-1} \Rightarrow ab^{-1} \in K$. So, K is a subfield of E.

Clearly, G is a group of K-automorphism of E. If E/K is finite, then the number of K-automorphisms of E is at most $[E : K]$. So, G is finite. Suppose $o(G) = r$. Let $u_0, u_1, ..., u_r \in E$ be linearly independent over K. Consider the r equations (in $r + 1$ unknowns x_js in E)

$$\sum_{j=0}^{r} \sigma(u_j)x_j = 0 \quad \text{for all } \sigma \in G$$

Since the number of equations is less than the number of unknowns, the system of equations has a non-zero solution.

Let $(a_0, a_1, ..., a_s, 0, 0, ..., 0)$ be a non zero solution of least length $s + 1$

$(a_i \neq 0\ \forall\ i = 0, 1, ..., s)$

Then $\sigma(u_0)a_0 = -\sigma(u_1)a_1 + ... + -\sigma(u_s)a_s$

$\Rightarrow$ $\sigma(u_0) = \sigma(u_1)b_1 + ... + \sigma(u_s)b_s$ for all $\sigma \in G$ ...(*i*)

Take $\sigma = I$. Then $u_0 = u_1b_1 + ... + u_sb_s$

If $b_i \in K$ for all i, then

$(-1)u_0 + b_1u_1 + ... + b_su_s = 0$, contradicting that $u_0, u_1, ..., u_s$ linearly independent over K.

So, some $b_i \notin K$. Let $b_1 \notin K$.

Then $\exists\ \tau \in G$ s.t., $\tau(b_1) \neq b_1$.

Replace σ by $\tau^{-1}\sigma$ in (*i*) to get

$$\tau^{-1}\sigma(u_0) = \sum_{j=1}^{r} \tau^{-1}\sigma(u_j)b_j \quad \text{for all } \sigma \in G$$

$$\Rightarrow \quad \tau(\tau^{-1}\sigma(u_0)) = \sigma(u_0) = \sum_{j=1}^{r} \sigma(u_j)\,\tau(b_j) \quad \text{for all } \sigma \in G \qquad ...(ii)$$

Then $(ii) - (i)$ gives

$$\sum_{j=1}^{r} \sigma(u_j)\,(\tau(b_j - b_j) = 0, \quad \text{for all } \sigma \in G$$

$$\Rightarrow \quad \sum_{j=1}^{r} \sigma(u_j)\,c_j = 0, \quad \text{for all } \sigma \in G, \text{ where } c_j = \tau(b_j) - b_j$$

Since $c_1 = \tau(b_1) - b_1 \neq 0$.

We have a non zero solution $(0, c_1, ..., c_s, 0, ..., 0)$ of length less than $s + 1$, a contradiction.

Therefore, $r + 1$ elements in E are not linearly independenent over K

$\Rightarrow [E : K] \leq r \Rightarrow E/K$ is finite.

So, $[E : K] \leq o(G)$. But $o(G) \leq [E : K] \Rightarrow o(G) = [E : K]$.

Problem 5: *Let E be a field with n distinct automorphisms and suppose K is the fixed field of the set of automorphisms. Show that* $[E : K] \geq n$.

Solution: Let $\sigma_1, \sigma_2, ..., \sigma_n$ be distinct automorphisms of E. Let G be the group generated by $\sigma_1, \sigma_2, ..., \sigma_n$. Then $o(G) \geq n$. If F is the fixed field of G,

then $K \subseteq F \subseteq E$. By Artin's theorem, $[E : F] = o(G) \geq n$.

So, $[E : K] \geq [E : F] \geq n$.

Problem 6: *Find the fixed field F of* $K(x)$ *under the automorphisms* $x \to 1 - x$, $x \to \frac{1}{x}$. *Show that the degree is* 6. *Verify that* $\frac{(x^2 - x + 1)^3}{(x^2 - x)^2}$ *lies in F and use this to find an equation for x over F.*

Solution: Let $\sigma(x) = 1 - x$, $\eta(x) = \frac{1}{x}$. Then $\sigma, \eta, \sigma\eta, \eta\sigma, \sigma\eta\sigma, I$ are six distinct automorphisms of $E = K(x)$. Let F' be the fixed field of these 6 automorphisms of E. So, $F \subseteq F' \subseteq E$. By previous problem, $[E : F'] \geq 6 \Rightarrow [E : F] \geq 6$.

Let $g(x) = \frac{(x^2 - x + 1)^3}{(x^2 - x)^2}$

Then $\eta(g(x)) = g(x)$, $\sigma(g(x)) = g(x)$

$\Rightarrow \quad g(x) \in F$

Let $L = K(g(x)) \subseteq F \subseteq E$

Then $[E : L] = [E : F]\,[F : L] \geq 6$.

Now $L(x) = K(x) = E$.

Also, $(x^2 - x + 1)^3 - g(x)\, x^2(x-1)^2 = 0$

$\Rightarrow x$ is a root of a polynomial of degree 6 with coefficients in L

$\Rightarrow [L(x) : L] \leq 6$

$\Rightarrow [E : L] \leq 6 \Rightarrow [E : L] = 6$

So, $[E : F]\ [F : L] = 6 \leq [E : F]$

$\Rightarrow [F : L] \leq 1$

$\Rightarrow F = L = K(g(x))$

$\Rightarrow (x^2 - x + 1)^3 - g(x)x^2(x-1)^2 = 0$ is an equation for x over F.

Problem 7: *If φ is an automorphisms of the field of real numbers* **R**, *show that φ leaves every element of* **R** *fixed.*

Solution: Since $\varphi(1) = 1$, $\varphi(n) = n$ for any positive integer n.

Also, $\varphi(0) = 0$, $\varphi(-n) = -\varphi(n) = -n$ and $\varphi(m^{-1}) = \varphi(m)^{-1} = m^{-1}$ for all non zero integers m.

Thus, $\varphi(nm^{-1}) = \varphi(n)\ \varphi(m)^{-1} = nm^{-1}$.

Let $r \in \mathbf{R}$ and $r > 0$. Then $r = s^2$, $s \in \mathbf{R}$.

So, $\varphi(r) = \varphi(s)^2 > 0$.

Also, $r > t \Rightarrow r - t > 0 \Rightarrow \varphi(r - t) > 0 \Rightarrow \varphi(r) > \varphi(t)$.

Let $r \in \mathbf{R}$ and let $p < r < q$, where $p, q \in \mathbf{Q}$.

Then $\varphi(p) = p < \varphi(r) < \varphi(q) = q$.

Thus, given any rational numbers p, q such that $p < r < q$, both r and $\varphi(r)$ are in the interval between p and q.

So, $\varphi(r) = r$ for all $r \in \mathbf{R}$. Hence, identity is the only automorphism of **R**.

Theorem 44: *Let K/F be a finite separable extension. Then $K = F(a)$ for some $a \in K$.*

Proof: Since K/F is finite, $K = F(a_1, ..., a_n)$ for some $a_1, ..., a_n \in K$. It is enough to prove the theorem for $n = 2$.

Let $K = F(\alpha, \beta)$. Then α, β are separable over F.

Case 1: Let F be an infinite field.

Let $p(x) = Irr(F, \alpha)$

$q(x) = Irr(F, \beta)$

Let $\alpha = \alpha_1, ..., \alpha_n$, $\beta = \beta_1, ..., \beta_m$ be the roots of $p(x)$, $q(x)$ respectively in a splitting fields of $p(x)$ and $q(x)$. Since K is finite, there exists $a \in K$ such that $a \neq 0$ and $a \neq \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$ for $1 \leq i \leq n$, $2 \leq j \leq m$.

Since α, β are separable over F, $\alpha_i s$ and $\beta_j s$ are distinct roots of $p(x)$, $q(x)$ respectively.

Let $\theta = a\beta + \alpha$. We show that $F(\theta) = F(\alpha, \beta)$. Clearly $F(\theta) \subseteq F(\alpha, \beta)$.

Define $g(x) = p(\theta - ax)$.

Then $g(\beta) = p(\theta - a\beta) = p(\alpha) = 0$.

Also, $g(\beta_j) = p(\theta - a\beta_j) \neq 0$ for all $j = 2, ..., m$.

(For, $p(\theta - a\beta_j) = 0 \Rightarrow \theta - a\beta_j - \alpha_i = 0$ for some i

$\Rightarrow a\beta + \alpha - a\beta_j - \alpha_i = 0$

$\Rightarrow a = \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$, a contradiction

Now β is a root of $g(x)$ and $q(x)$ and no β_j ($j \neq 1$) is a root of $g(x) \Rightarrow \beta$ is the only common root of $g(x)$ and $q(x)$. Let $f(x) = Irr\,(F(\theta), \beta)$.

Since $g(x) \in F(\theta)[x]$ and $g(\beta) = 0$, $f(x)$ divides $g(x)$. Similarly $f(x)$ divides $q(x)$

So, $f(x)$ divides g.c.d. of $g(x)$ and $q(x)$.

$\Rightarrow f(x)$ divides $x - \beta \Rightarrow f(x) = x - \beta$

Since $f(x) \in F(\theta)[x]$, $\beta \in F(\theta)$

Also, $\alpha = \theta - a\beta \in F(\theta)$

$\Rightarrow F(\alpha, \beta) \subseteq F(\theta)$.

Thus, $F(\theta) = F(\alpha, \beta)$.

Case 2: K is finite. We shall prove later that $K^* = K - \{0\}$ is a cyclic group. If $K^* = \langle a \rangle$, then $K = F(a)$.

Note: An extension K/F a called a *simple extension* if $K = F(a)$ for some $a \in K$. In the above theorem, we have shown that a finite separable extension is a simple extension. a is called a *primitive element* of K over F if $K = F(a)$.

Problem 8: *Find a primitive element for* $\mathbf{Q}(i, 2^{1/2})$ *over* $\mathbf{Q}$.

Solution: Since char $\mathbf{Q} = 0$, $\mathbf{Q}$ is perferct. So, $\mathbf{Q}(i, 2^{1/2})/\mathbf{Q}$ is separable. Therefore, primitive element of $\mathbf{Q}(i, 2^{1/2})$ over $\mathbf{Q}$ exists.

Let $p(x) = Irr\,(\mathbf{Q}, 2^{1/2}) = x^2 - 2 = (x - 2^{1/2})\,(x + 2^{1/2})$

$q(x) = Irr\,(\mathbf{Q}, i) = x^2 + 1 = (x - i)\,(x + i)$.

Consider $\dfrac{-2^{\frac{1}{2}} - 2^{\frac{1}{2}}}{i - (-i)} = \dfrac{-2^{\frac{1}{2}}}{i} = -2^{1/2}i$.

Take $a = 1$.

Then $\theta = a\beta + \alpha = i + 2^{1/2}$.

By above theorem $\mathbf{Q}(i, 2^{1/2}) = \mathbf{Q}(\theta) = \mathbf{Q}(i + 2^{1/2})$.

Problem 9: *Find a primitive element for* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *over* $\mathbf{Q}$.

Solution: Here $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$

$p(x) = Irr\,(\mathbf{Q}, \sqrt{2}) = x^2 - 2 = (x - \sqrt{2})\,(x + \sqrt{2})$

$q(x) = Irr\,(\mathbf{Q}, \sqrt{3}) = x^2 - 3 = (x - \sqrt{3})\,(x + \sqrt{3})$

Consider $\dfrac{-\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = \dfrac{-\sqrt{2}}{\sqrt{3}}$.

Take $a = 1$.

Then $\theta = a\beta + \alpha = \sqrt{3} + \sqrt{2}$.

So, $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\theta) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Problem 10: *Let E/K be normal. Show that an element of E, of degree r over K has at most r congugates over K with equality iff it is separable.*

Solution: Let $p(x) = Irr\ (K, \alpha)$. Then deg $p(x) = r$.

Now $K \subseteq K(\alpha) \subseteq E$. Suppose $\alpha, \alpha_1, \alpha_2, ..., \alpha_r$ are distinct conjugates of α, over K.

Then $\exists$ r K-automorphisms $\sigma_1, \sigma_2, ..., \sigma_r$ of E s.t., $\sigma_i(\alpha) = \alpha_i\ \forall\ i$.

Each σ_i is a K-homomorphism from $K(\alpha)$ into E.

But $[K(\alpha) : K] = \deg p(x) = r \Rightarrow$ there are at most r K-homomorphisms from $K(\alpha)$ into E.

But we have $r + 1$ K-homomorphisms, $I, \sigma_1, ..., \sigma_r$ from $K(\alpha)$ into E, which is a contradiction.

Thus, there are at most r conjugates of α over K.

Suppose $\alpha \in E$ is separable over K.

Then α is a simple root of $p(x)$.

$\Rightarrow$ each root of $p(x)$ is simple.

Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_r$ be distinct roots of $p(x)$.

Then $\exists$ K-isomorphisms $\sigma_i : K(\alpha) \to K(\alpha_i)$ s.t., $\sigma_i(\alpha) = \alpha_i \quad \forall\ i = 1, 2, ..., r$.

$\sigma_1, \sigma_2, ..., \sigma_r$ are distinct maps.

Since $[K(\alpha) : K] = \deg p(x) = r$, σ_is are only K-homomorphisms from $K(\alpha)$ into E.

If η is a K-automorphism of E s.t., $\eta(\alpha) = \alpha_i$, then η is also a K-homomorphism of $K(\alpha)$ into E.

$\therefore\ \eta = \sigma_i$ on $K(\alpha)$. So, there are only r K-automorphisms of E transforming α into α_i.

Thus, there are exactly r conjugates of α over K.

Conversely, let $\alpha = \alpha_1, \alpha_2, ..., \alpha_r$ be r conjugates of α over K. Then, there are exactly r K-automorphisms of E transforming α into α_i. These are also K-homomorphisms from $K(\alpha)$ into E. So, there are only r K-homomorphisms of $K(\alpha)$ into E.

Thus, $K(\alpha)/K$ is separable $\Rightarrow$ α is separable over K.

Galois Extensions

Definition: An extension E of F is called a *Galois extension* if (*i*) E/F is finite (*ii*) F is the fixed field of a group of automorphisms of E.

We first find a necessary and sufficient condition for a finite extension to be Galois.

Theorem 45: *Let E/F be a finite extension. Then E/F is a Galois extension if and only if it is both normal and seperable.*

Proof: Let E/F be a Galois extension.Then F is the fixed field of a group G of automorphisms of E. By Artin's theorem, since E/F is finite, G is also finite.

Let $G = \{\sigma_1 = I, \sigma_2, ..., \sigma_n\}$.

Let $a \in E$. Let $\sigma_i(a) = a_i$, $i = 1, 2, ..., n$.

Suppose $a_1 = a, a_2, ..., a_r$ are distinct elements of $\{a_1, a_2, ..., a_n\}$.

Let $S = \{a_1, a_2, ..., a_r\}$. Then $S \subseteq E$.

Now $\sigma_j(a_i) = \sigma_j \sigma_i(a) = \sigma_k(a) = a_k \in S$.

So, $\sigma_j : S \to S$ for all $j = 1, 2, ..., n$. Since $\sigma_j : E \to E$ is 1-1, so is $\sigma_j : S \to S$. Also, S is finite $\Rightarrow \sigma_j : S \to S$ is onto. Therefore, σ_j is a permutation of S for all j.

Let $f(x) = (x - a_1) ... (x - a_r)$

$= x^r + \alpha_1 x^{r-1} + ... + \alpha_r x^r$

Now $\sigma_t(f(x)) = (x - \sigma_t(a_1)) ... (x - \sigma_t(a_r))$

$= (x - a_1) ... (x - a_r) = f(x)$ for all t.

So, $x^r + \sigma_t(\alpha_1)x^{r-1} + ... + \sigma_t(\alpha_r) = x^r + \alpha_1 x^{r-1} + ... + \alpha_r$

$\Rightarrow \sigma_t(\alpha_i) = \alpha_i$ for all t and i

$\Rightarrow \alpha_i$ belongs to the fixed field of G

$\Rightarrow \alpha_i \in F$, for all i

$\Rightarrow f(x) \in F[x]$.

Let $g(x)$ be a monic irreducible factor of $f(x)$ in $F[x]$.

Let a_i be a zero of $g(x)$ in E. Now $a_j = \sigma_j(a) = \sigma_j \sigma_i^{-1}(a_i) = \sigma_t(a_i)$. So, a_i is a zero of $g(x)$ in E.

$\Rightarrow \sigma_t(a_i)$ is a zero of $\sigma_t(g(x)) = g(x)$ in E

$\Rightarrow a_j$ is a zero of $g(x)$ in E for all j

$\Rightarrow g(x) = f(x)$

$\Rightarrow f(x) = Irr\ (F, a)$.

Since a is a simple zero of $f(x)$, a is separable over F. So, E/F is separable. Also, $f(x)$ splits in $E[x]$.

$\Rightarrow E/F$ is normal.

Conversely, let G be the group of all F-automorphisms of E. Let F' be the fixed field of G.

Then $F \subseteq F' \subseteq E$ and $o(G) = [E : F]$.

Since E/F is finite, So is E/F'.

Also, E/F is seperable normal $\Rightarrow E/F'$ is separable, normal.

Therefore, there are exactly $n = [E : F]$ F-automorphisms of E.

$\Rightarrow o(G) = n \Rightarrow [E : F'] = n \Rightarrow [F' : F] = 1 \Rightarrow F' = F$.

$\Rightarrow F$ is the fixed field of $G \Rightarrow E/F$ is Galois.

Cor. 1: Let E/F be finite extension. Then E/F is Galois if and only if F is the fixed field of the group of all F-automorphisms of E.

Proof: Let E/F be Galois. Then from above E/F is finite, normal, separable. Again by converse part of the above result, F is the fixed field of the group of all F-automorphisms of E. Converse, follows by definition.

Cor. 2: Let char $k = 0$. Then k is contained in some Galois extension of k.

Proof: Let $f(x)$ be a non constant polynomial in $k[x]$. Let E be a minimal splitting field of $f(x)$ over k. Then E/K is finite normal. Since char $k = 0$, k is perfect $\Rightarrow$ E/K is separable. So, E/K is Galois.

Note: When E/F is Galois, the group of all F-automorphisms of E is denoted by $Gal(E/F)$ or $G(E/F)$ called the *Galois group* of E/F.

Theorem 46: *Let E/F be a finite extension. Then E/F is contained in a Galois extension if and only if it is separable.*

Proof: Let E/F be a contained in a Galois extension E'/F. Then $F \subseteq E \subseteq E'$.

Now E'/F is Galois $\Rightarrow$ E'/F is separable $\Rightarrow$ E/F' is separable.

Conversely, let E/F be separable. Since E/F is finite, $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$.

Let $p_i = Irr(F, \alpha_i), \quad \alpha_i \in E$

$\alpha_i \in E \Rightarrow \alpha_i$ is separable over F

$\Rightarrow \alpha_i$ is a simple zero of p_i, for all i

$\Rightarrow$ each zero of p_i in a splitting field is simple

Let $f = \prod_{i=1}^{n} p_i$. Then $f \in k[x] \subseteq E[x]$, and f splits in some extension of E.

Let L be a minimal splitting field of $f(x)$ over F.

Then $L = F$ (zeros of f in an extension of E)

$= F(\alpha_1, \alpha_2, ..., \alpha_n,$ zeros of f other than $\alpha_i s$ in an extension of $E)$

$= E$ (zeros of f other than $\alpha_i s$ in an extension of E)

$\Rightarrow$ $F \subseteq E \subseteq L$

Also, L is generated by separable elements over F (as each zero of f in an extension of E is simple and is a zero of an irreducible polynomial of $p_i \in F[x]$) $\Rightarrow$ L/F is separable $\Rightarrow$ E/F is contained in a separable extension L/F.

Theorem 47: *Let E/k be Galois and F be any extension of k. Then EF/F is Galois and G(EF/F) is isomorphic to a subgroup of G(E/k).*

Proof: Since E/k is Galois, E/k is finite normal. So, E is a minimal splitting field of some polynomial $f(x) \in k[x]$.

Let $f(x) = \alpha(x - \alpha_1)(x - \alpha_2) ... (x - \alpha_n), \alpha_i \in E, \alpha \in k.$

Then $E = k(\alpha_1, \alpha_2, ..., \alpha_n)$.

Also, E/k is separable $\Rightarrow$ each α_i is separable over k. Now $k \subseteq F \subseteq EF$ and α_i is separable over $k \Rightarrow \alpha_i$ is separable over F.

Again, $E = k(\alpha_1, \alpha_2, ..., \alpha_n)$.

$\Rightarrow$ $EF = FE = Fk(\alpha_1, \alpha_2, ..., \alpha_n) = F(\alpha_1, \alpha_2, ..., \alpha_n)$ as $k \subseteq F$

$\Rightarrow$ EF is a minimal splitting field of $f(x)$ over F

$\Rightarrow$ EF/F is finite normal

Also, EF is generated by separable elements over $F \Rightarrow EF/F$ is separable.

So, EF/F is Galois.

Let $\sigma \in G(EF/F)$.

Let $f = \alpha f_1 f_2 \ldots f_r$ where each f_i is monic irreducible polynomial in $k[x]$.

So, each α_i is a zero of some $f_j \in k[x]$.

Since α_i is separable over k, α_i is a simple zero.

Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Then α_i is a zero of f in $E \subseteq EF$

$\Rightarrow$ $\sigma(\alpha_i)$ is a zero of $\sigma(f) = f$ in $EF \Rightarrow \sigma(\alpha_i) \in S$.

So, $\{\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

$\Rightarrow$ $\sigma(E) = k(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) = k(\alpha_1, \alpha_2, \ldots, \alpha_n) = E$

$\Rightarrow$ σ restricted to E belongs to $G(E/k)$

Define $\theta : G(EF \mid F) \to G(E/k)$ s.t.,

$\theta(\sigma) = \sigma \mid E$

Then θ is a homomorphism.

Also θ is 1-1 as $\sigma \mid E = I \Rightarrow \sigma(\alpha_i) = \alpha_i$ for all i $\Rightarrow \sigma(a) = a$ for all $a \in EF$ as $EF = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and σ fixes each element of $F \Rightarrow \sigma = I$ on EF.

So, $G(EF/F) \cong \theta(G(EF/F)) \leq G(E/F)$.

Cor.: If E/k is Galois and F, an extension of k, then $[EF : F]$ divides $[E : k]$.

Proof: By above theorem, EF/F is Galois

$\Rightarrow$ $[EF : F] = o(G(EF/F))$

Also, $[E : k] = o(G(E/k))$

But $\theta(G(EF/F)) \leq G(E/F)$

$\Rightarrow$ $o(\theta(G(EF/F))$ divides $o(G(E/F))$

$\Rightarrow$ $o(G(EF/F))$ divides $o(G(E/F))$

$\Rightarrow$ $[EF : F]$ divides $[E : k]$.

Remark: The above corollary need not be true if E/k is not Galois. For example, let $k = \mathbf{Q}$, let α be the real cube root of 2. Then α, αw, αw^2 are roots of $f(x) = x^3 - 2$ in $\mathbf{C}$.

Let $E = \mathbf{Q}(\alpha w)$, $F = \mathbf{Q}(\alpha)$.

Then $EF = \mathbf{Q}(\alpha w)\ \mathbf{Q}(\alpha) = \mathbf{Q}(\alpha, \alpha w) = \mathbf{Q}(\alpha, \sqrt{3}i)$

$= F(\sqrt{3}i)$

So, $[EF : F] = [F(\sqrt{3}i) : F] = 2$

while $[E : k] = [\mathbf{Q}(\alpha w) : \mathbf{Q}] = \deg Irr\ (\mathbf{Q}, \alpha w)$

$= \deg f(x) = 3$.

Theorem 48: (**The fundamental theorem of Galois Theory**). *Let E/k be Galois. Let* $G = G(E/k)$ *be the group of all k-automorphisms of E. Then*

(*i*) *There is one-one correspondence between the sets* $\mathscr{A} = \{F \mid F = \text{field}, k \subseteq F \subseteq E\}$ *and* $\mathscr{B} = \{H \mid H \leq G\}$ *which is an order inverting bijection.*

(*ii*) *$F \in \mathscr{A}$ is the fixed field of the subgroup $H \in \mathscr{B}$ corresponding to F and $H \in \mathscr{B}$ is the group of H^*-automorphisms of E, where H^* is the fixed field of H.*

(*iii*) *If H is the subgroup of $\mathscr{B}$ corresponding to the field F in $\mathscr{A}$, then $o(H) = [E : F]$ and $[G : H] = [F : k]$.*

(*iv*) *If $H_1, H_2 \in \mathscr{B}$ corresponding to $F_1, F_2 \in \mathscr{A}$ respectively, then F_1, F_2 are conjugate under an automorphism $\sigma \in G$ if and only if $\sigma^{-1} H_1 \sigma = H_2$.*

(*v*) *If $H \in \mathscr{B}$ corresponds to $F \in \mathscr{A}$, then F/k is normal if and only if H is normal subgroup of G and in that case, $G(F/k) \cong \dfrac{G}{H}$.*

Proof: Define $\theta : \mathscr{A} \to \mathscr{B}$ s.t.,

$$\theta(F) = F^*$$

where $F^* = \{\sigma \in G \mid \sigma(x) = x \text{ for all } x \in F\}$. Then $F^* \in \mathscr{B}$.

Similarly, define $\theta : \mathscr{B} \to \mathscr{A}$ s.t.,

$$\theta(H) = H^*$$

where $H^* = \{x \in E \mid \sigma(x) = x \text{ for all } \sigma \in H\}$

Then $H^* \in \mathscr{A}$ is the fixed field of H.

Let $F_1, F_2 \in \mathscr{A}$ such that $F_1 \subseteq F_2$.

Let $\sigma \in F_2^*$. Then $\sigma(x) = x$ for all $x \in F_2$

$\Rightarrow \sigma(x) = x$ for all $x \in F_1$ as $F_1 \subseteq F_2$

$\Rightarrow \sigma \in F_1^* \Rightarrow F_2^* \subseteq F_1^* \Rightarrow \theta(F_2) \subseteq \theta(F_1) \Rightarrow \theta$ is an order inverting map.

Similarly, φ is an order inverting map.

Let $H \in \mathscr{B}$. Then $\sigma \in H \Rightarrow \sigma(x) = x$ for all $x \in H^* \Rightarrow \sigma \in H^{**} \Rightarrow H \subseteq H^{**}$.

Also $x \in F (F \in \mathscr{A}) \Rightarrow \sigma(x) = x$ for all $\sigma \in F^*$

$\Rightarrow x$ belongs to the fixed field of F^*

$\Rightarrow x \in F^{**} \Rightarrow F \subseteq F^{**}$ for all $F \in \mathscr{A}$.

Let $F \in \mathscr{A}$ and $F^* = H$. Then $H^{**} = F^{***}$.

Now $H \subseteq H^{**} \Rightarrow F^* \subseteq F^{***}$ for all $F \in \mathscr{A}$.

Also, $F \subseteq F^{**} \Rightarrow \theta(F^{**}) \subseteq \theta(F) \Rightarrow F^{***} \subseteq F^*$ for all $F \in \mathscr{A}$. So, $F^* = F^{***}$. Similarly, $H^* = H^{***}$ for all $H \in \mathscr{B}$.

Now θ is 1-1 onto if and only if $\theta\varphi$ = Identity and $\varphi\theta$ = Identity if and only if $H = H^{**}$ for all $H \in \mathscr{B}$ and $F = F^{**}$ for all $F \in \mathscr{A}$.

Let $H \in \mathscr{B}$. Then $H^* = F$ is the fixed field of H.

By Artin's theorem $o(H) = [E : F]$.

Also, $o(H^{**}) = [E : H^{***}] = [E : H^*] = [E : F]$.

So, $o(H) = o(H^{**})$. But $H \subseteq H^{**}$. Therefore, $H = H^{**}$.

Let $F \in \mathscr{A}$. Then $k \subseteq F \subseteq E$.

Now E/k is Galois $\Rightarrow E/F$ is Galois $\Rightarrow F$ is the fixed field of the group H of all F-automorphisms of E.

$\Rightarrow H \leq G \Rightarrow H \in \mathscr{B}$.

Now H^* = fixed field of $H = F \Rightarrow H^{***} = F^{**} \Rightarrow H^* = F^{**} \Rightarrow F = F^{**}$ for all $F \in \mathscr{A}$.

Thus, θ is 1-1 onto.

This proves (*i*).

(*ii*) Let $F \in \mathscr{A}$. Let $\theta(F) = H$. Then $F^* = H \Rightarrow F^{**} = H^* \Rightarrow F = H^* \Rightarrow F$ is the fixed field of H.

Let $H \in \mathscr{B}$. Then there exists $F \in \mathscr{A}$ such that $\theta(F) = H \Rightarrow H = F^*$.

Let $\sigma \in H$. Then $\sigma \in F^* \Rightarrow \sigma(x) = x$ for all $x \in F \Rightarrow \sigma$ is an F-automorphism of E.

Conversely, let σ be an F-automorphism of E.

Then $\sigma(x) = x$ for all $x \in F \Rightarrow \sigma \in F^* = H$.

So, H is the group of all $F = H^*$-automorphisms of E.

(*iii*) By Artin's theorem

$$o(H) = [E : H^*] = [E : F]$$

$$[G : H] = \frac{o(G)}{o(H)} = \frac{[E : k]}{[E : F]} = [F : k].$$

(*iv*) Suppose $F_1, F_2 \in \mathscr{A}$ are conjugate under $\sigma \in G$. Then $\sigma(F_1) = F_2$.

Let $y \in F_2$. Then $y = \sigma(z)$, $z \in F_1$. Therefore, $\sigma^{-1}(y) = z$.

$\Rightarrow \tau\sigma^{-1}(y) = \tau(z)$, for all $\tau \in H_1$

$\Rightarrow \sigma\tau\sigma^{-1}(y) = \sigma\tau(z) = \sigma(z)$, for all $\tau \in H_1$

$\Rightarrow \sigma\tau\sigma^{-1}(y) = y$, for all $\tau \in H_1, y \in F_2$

$\Rightarrow \sigma\tau\sigma^{-1} \in H_2$, for all $\tau \in H_1$

$\Rightarrow \sigma H_1\sigma^{-1} \subseteq H_2$

Let $a \in F_1$. Then $\sigma(a) = b \in F_2$

$\Rightarrow \eta\sigma(a) = \eta(b)$, for all $\eta \in H_2$

$\Rightarrow \eta\sigma(a) = b$, for all $\eta \in H_2$

$\Rightarrow \sigma^{-1}\eta\sigma(a) = \sigma^{-1}(b) = a$, for all $\eta \in H_2, a \in F_1$

$\Rightarrow \sigma^{-1}\eta\sigma \in H_1$, for all $\eta \in H_2$

$\Rightarrow \sigma^{-1}H_2\,\sigma \subseteq H_1$

$\Rightarrow H_2 \subseteq \sigma H_1\sigma^{-1}$

So, $H_2 = \sigma H_1\sigma^{-1}$.

Conversely, let $H_2 = \sigma H_1\sigma^{-1}$ for $\sigma \in G$.

Let $y \in F_2$. Now $\sigma\tau\sigma^{-1} \in H_2$, for all $\tau \in H_2$

$\Rightarrow \sigma\tau\sigma^{-1}(y) = y$

$\Rightarrow \tau\sigma^{-1}(y) = \sigma^{-1}(y) = z$

$\Rightarrow \tau(z) = z$, for all $\tau \in H_1$

$\Rightarrow z \in F_1$

$\Rightarrow y = \sigma(z) \in \sigma(F_1)$

$\Rightarrow F_2 \subseteq \sigma(F_1)$

Let $x \in F_1$. Now $\sigma^{-1}\eta\sigma \in H_1$, for all $\eta \in H_2$

$\Rightarrow \sigma^{-1}\eta\sigma(x) = x$

$\Rightarrow \eta\sigma(x) = \sigma(x) = x'$

$\Rightarrow \eta(x') = x'$, for all $\eta \in H_2$

$\Rightarrow x' \in F_2$

$\Rightarrow \sigma(x) \in F_2$

$\Rightarrow \sigma(F_1) \subseteq F_2$.

So, $\sigma(F_1) = F_2 \Rightarrow F_2$ are conjugate under σ.

(*v*) Suppose F/k is normal. Since E/k is finite, so is F/k. Therefore, F/k is finite normal $\Rightarrow F$ is a minimal splitting field of some $f \in k[x]$.

Let $f = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in E$, $\alpha \in k$.

Then $F = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Let $\sigma \in G$. Then σ is a k-autmorphism of $E \Rightarrow \sigma(f) = f$.

$\Rightarrow f = \alpha(x - \sigma(\alpha_1)) \ldots (x - \sigma(\alpha_n))$

$\Rightarrow \sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are zeros of f in E

$\Rightarrow \{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$.

So, $\sigma(F) = k(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$

$= k(\alpha_1, \ldots, \alpha_n) = F$ for all $\sigma \in G$.

By (*iv*), $\sigma^{-1}H\sigma = H$ for all $\sigma \in G$

$\Rightarrow H$ is a normal subgroup of G.

Conversely, let $H = F^*$ be normal subgroup of G. Then $\sigma^{-1} H\sigma = \sigma$ for all $\sigma \in G$.

$\Rightarrow \sigma(F) = F$ by (*iv*) for all $\sigma \in G$

Let $\alpha \in F$, $p(x) = Irr\ (k, \alpha)$.

Since E/k is normal and $\alpha \in E$, we find $p(x)$ splits in E.

Let β be a zero of $p(x)$ in E.

Then α, β are zeros of $p(x)$ in E.

$\Rightarrow$ there is an isomorphism $\theta : k(\alpha) \to k(\beta)$ s.t.,

$\theta(\alpha) = \beta$, $\theta(a) = a$ for all $a \in k$.

Since $\beta \in E$, $k(\beta) \subseteq E$. So θ is a k-homomorphisms from $k(\alpha)$ to E.

Since E/K is finite normal, θ can be extended to k-automorphism σ of E. So, $\sigma \in G$.

Now $\sigma(\alpha) = \theta(\alpha) = \beta$ and $\sigma(\alpha) \in \sigma(F) = F \Rightarrow \beta \in F$.

Thus, $p(x)$ splits in $F \Rightarrow F/K$ is normal.

Let H be a normal subgroup of G. Then the corresponding field F is normal over k from above. Since E/k is Galois, so is F/k. Let $N = \text{Gal}(F/k)$

Define $\psi : G \to N$ s.t.,

$\psi(\sigma) = \bar{\sigma}$, where $\bar{\sigma}$ is the restriction of σ on F.

(Since $H \leq G$, $\sigma^{-1}H\sigma = H \Rightarrow \sigma(F) = F$)

Let $\sigma, \eta \in G$.

Then $\overline{\sigma\eta}(\alpha) = (\sigma\eta)(\alpha), \quad \alpha \in F$

$= \sigma(\eta(\alpha)), \quad \eta(\alpha) \in F$

$= \bar{\sigma}(\eta(\alpha))$

$= \bar{\sigma}(\bar{\eta}(\alpha))$

$= (\bar{\sigma}\,\bar{\eta})(\alpha)$, for all $\alpha \in F$

$\Rightarrow \overline{\sigma\eta} = \bar{\sigma}\,\bar{\eta}$

$\Rightarrow \psi(\sigma\eta) = \psi(\sigma)\psi(\eta)$

$\Rightarrow \psi$ is a homomorphism

Let $\theta \in N$. Then θ can be extended to k-automorphism σ of $E \Rightarrow \sigma \in G \Rightarrow \psi(\sigma) = \bar{\sigma} = \theta$. So, ψ is onto. Now $\sigma \in \text{Ker } \psi \Leftrightarrow \psi(\sigma) =$ Identity of $N \Leftrightarrow \bar{\sigma} =$ Identity on $F \Leftrightarrow \bar{\sigma}(\alpha) = \alpha$, for all $\alpha \in F$.

The result now follows by using fundamental theorem of homomorphism.

Example 14: (*i*) Let E be a minimal splitting field of $f(x) = x^3 - 2$ over $\mathbf{Q}$. Let α be the real cube root of 2.

Then $E = \mathbf{Q}(\alpha, \alpha w, \alpha w^2) = \mathbf{Q}(\alpha, \sqrt{3}\ i) = \mathbf{Q}(\alpha, \alpha w) = \mathbf{Q}(\alpha, w)$

Also, $[E : \mathbf{Q}] = 6$. Since char $\mathbf{Q} = 0$, $E/\mathbf{Q}$ is separable (as $\mathbf{Q}$ is perfect $\Rightarrow$ every algebraic extension of $\mathbf{Q}$ is separable.)

Also, E is a minimal splitting field of $f(x)$ over $\mathbf{Q} \Rightarrow E/\mathbf{Q}$ is finite normal.

So, $E/\mathbf{Q}$ is Galois.

Let $G = G(E/\mathbf{Q})$ be the group of all $\mathbf{Q}$-automorphisms of E.

Then $\mathbf{Q}$ is the fixed field of G. By Artin's theorem $o(G) = [E : \mathbf{Q}] = 6$.

Since α, αw are roots of $f(x)$, there exists $\mathbf{Q}$-isomorphism

$$\sigma_0 : \mathbf{Q}(\alpha) \to \mathbf{Q}(\alpha w) \text{ s.t.,}$$
$$\sigma_0(\alpha) = \alpha w$$

Let $g(x) = x^2 + x + 1$, then $g(x)$ is irreducible over $\mathbf{Q}(\alpha) \subseteq \mathbf{R}$ and $\sigma_0(g(x)) = g(x)$ is irreducible over $\mathbf{Q}(\alpha w)$

Since w, w are roots of $g(x)$, there exists an isomorphism

$$\sigma : \mathbf{Q}(\alpha, w) = E \to \mathbf{Q}(\alpha w, w) = E \text{ s.t.,}$$
$$\sigma(w) = w$$
$$\sigma(\alpha) = \sigma_0(\alpha) = \alpha w$$
$$\sigma(a) = \sigma_0(a) = a \quad \forall\ a \in \mathbf{Q}$$

Thus σ is $\mathbf{Q}$-automorphism of E, $\sigma \neq I$.

Also w, w^2 are roots of $g(x)$ which is irreducible over $\mathbf{Q}(\alpha)$ and $\exists$ $\mathbf{Q}(\alpha)$ isomorphism

$$\tau : \mathbf{Q}(\alpha, w) = E \to \mathbf{Q}(\alpha, w^2) = E \text{ s.t.,}$$
$$\tau(w) = w^2,\ \tau(\alpha) = \alpha$$

and so τ is $\mathbf{Q}$-automorphism of E, $\tau \neq \sigma$, $\tau \neq I$

Now $\sigma^2(\alpha) = \alpha w^2$, $\sigma^2(w) = w$

$(\sigma\ \tau)\ (\alpha) = \alpha w$, $(\sigma\tau)\ (w^2) = w^2$

$(\sigma^2\tau)\ (\alpha) = \alpha w^2$, $(\sigma^2\tau)\ (w^2) = w^2$.

Since $o(G) = 6$, $G = \{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$

Also $(\tau\sigma)\ (\alpha) = \tau(\alpha w) = \alpha w^2$, $\tau\sigma \neq \sigma\tau$

So G is a non abelian group of order 6 and so $G \cong S_3$.

Denote αw by 1, αw^2 by 2 and αw^3 by 3 and we get

$\tau = (12)$, $\sigma T = (13)$, $\sigma^2 T = (23)$, $\sigma = (123)$, $\sigma^2 = (132)$

Write $\tau = \sigma_2$, $\sigma = \sigma_3$, $\sigma T = \sigma_4$, $\sigma^2 = \sigma_5$ and $\sigma^2\ T = \sigma_6$

Then $G = \{I, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

Subgroups of G are:

$H_1 = \{I, \sigma_2\}$, $H_2 = \{I, \sigma_4\}$, $H_3 = \{I, \sigma_6\}$, $H_4 = \{I, \sigma_3, \sigma_5\}$, $H_5 = G$, $H_6 = \{I\}$.

Let $F_1 = H_1^*$, the fixed field of H_1.

Now H_1 fixes $\alpha \Rightarrow \mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq F_1 \subseteq E$.

But $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$, $[E : F_1] = [E : H_1^*] = o(H_1) = 2$ and $[E : \mathbf{Q}] = 6 \Rightarrow F_1 = \mathbf{Q}(\alpha)$.

Let $F_2 = H_2^*$, the fixed field of H_2.

Then $F_2 = \mathbf{Q}(\alpha w^2)$ and F_3, the fixed field of H_3 is $\mathbf{Q}(\alpha\omega)$

Let $F_4 = H_4^*$, the fixed field of H_4. Now H_4 fixes $\sqrt{3i} \Rightarrow \mathbf{Q} \subseteq \mathbf{Q}(\sqrt{3i}) \subseteq F_4 \subseteq E$. Since $[E : F_4] = 3$. $[\mathbf{Q}(\sqrt{3}\, i) : \mathbf{Q}] = 2$, $[E : \mathbf{Q}] = 6$, $F_4 = \mathbf{Q}(\sqrt{3}\, i)$.

Clearly, F_5 = fixed field of $G = \mathbf{Q}$ and F_6 = fixed field of $H_6 = E$.

So, we have 6 intermediate fields between $\mathbf{Q}$ and E corresponding to 6 subgroups of G.

Since H_1, H_2, H_3 are not normal, $F_1/\mathbf{Q}$, $F_2/\mathbf{Q}$, $F_3/\mathbf{Q}$ are also nor normal. Also H_4, H_5, H_6 are normal subgroup of G, and thus $F_4/\mathbf{Q}$, $F_5/\mathbf{Q}$, $F_6/\mathbf{Q}$ are normal subgroups of G.

(*ii*) Let E be a minimal splitting field of $f(x) = x^4 + 1$ over $\mathbf{Q}$.

Then α, α^3, α^5, α^7 are roots of $f(x)$, where $\alpha = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$

and $E = \mathbf{Q}(\alpha) = \mathbf{Q}(\alpha^3) = \mathbf{Q}(\alpha^5) = \mathbf{Q}(\alpha^7)$

Then $[E : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg\ Irr\ (\mathbf{Q}, \alpha) = \deg f(x) = 4$.

Char $\mathbf{Q} = 0 \Rightarrow E/\mathbf{Q}$ is separable.

Also E is a minimal splitting field of $f(x)$ over $\mathbf{Q}$ implies $E/\mathbf{Q}$ is normal.

Hence $E/\mathbf{Q}$ is Galois.

Let $G = G(E/\mathbf{Q})$ be the Galois group of $E/\mathbf{Q}$.

By Artin's theorem, $o(G) = [E : \mathbf{Q}] = 4$

Since α and α^3 are roots of an irreducible polynomial $f(x)$ over $\mathbf{Q}$, there exists $\mathbf{Q}$-automorphism

$\sigma_3 : \mathbf{Q}(\alpha) = E \to \mathbf{Q}(\alpha^3) = E$, s.t.,

$\sigma_3(\alpha) = \alpha^3$

Similarly, there exists **Q**-automorphisms

$$\sigma_5 : \mathbf{Q}(\alpha) = E \to \mathbf{Q}(\alpha^5) = E \quad \text{s.t.,}$$
$$\sigma_5(\alpha) = \alpha^5$$
$$\sigma_7 : \mathbf{Q}(\alpha) = E \to \mathbf{Q}(\alpha^7) = E \quad \text{s.t,}$$
$$\sigma_7(\alpha) = \alpha^7$$

So $G = \{I, \sigma_3, \sigma_5, \sigma_7\}$

Also $\sigma_3^2 = \sigma_5^2 = \sigma_7^2 = I$

Thus G is an abelian non cyclic group of order 4 and so it is the Klein's four group.

Subgroups of G are $H_1 = \{I, \sigma_3\}$, $H_2 = \{I, \sigma_5\}$, $H_3 = \{I, \sigma_7\}$, $H_4 = G$, $H_5 = \{I\}$.

Now $\sigma \in G \Rightarrow \sigma(\sqrt{2})^2 = \sigma(2) = 2 \Rightarrow (\sigma(\sqrt{2}))^2 = 2 = 0 \Rightarrow \sigma(\sqrt{2})$ is a zero of $x^2 + 2$ in $E \subseteq \mathbf{C} \Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$. Similarly $\sigma(i) = \pm i$.

So, $\sigma_3(\alpha) = \alpha^3 \Rightarrow \sigma_3\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

$$\Rightarrow \sigma_3(\sqrt{2}) = -\sqrt{2},\ \sigma_3(i) = -i$$
$$\Rightarrow \sigma_3(\sqrt{2}\, i) = \sqrt{2}\, i$$
$$\Rightarrow H_1 \text{ fixes } \sqrt{2}\, i$$

Let $F_1 = H_1^*$, the fixed field of H_1

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}\, i) \subseteq F_1 \subseteq E$

But $[\mathbf{Q}(\sqrt{2}\, i) : \mathbf{Q}] = 2,\ [E : F_1] = 2,\ [E : \mathbf{Q}] = 4$

So, $F_1 = \mathbf{Q}(\sqrt{2}\, i)$

Also, $\sigma_5(\alpha) = \sigma^5 \Rightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = -\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$.

$\sigma_5(\sqrt{2}) = -\sqrt{2}$ and $\sigma_5(i) = i \Rightarrow H_2$ fixes i.

Let $F_2 = H_2^*$, the fixed field of H_2.

Then $\mathbf{Q} \subseteq \mathbf{Q}(i) \subseteq F_2 \subseteq E$ and $[E : F_2] = 2,\ [\mathbf{Q}(i) : \mathbf{Q}] = 2,\ [E : \mathbf{Q}] = 4 \Rightarrow F_2 = \mathbf{Q}(i)$.

Now $\sigma_7(\alpha) = \sigma^7 \Rightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} \Rightarrow \sigma_5(\sqrt{2}) = \sqrt{2} \Rightarrow H_3$ fixes $\sqrt{2}$. Let $F_3 = H_3^*$, the fixed field of H_3.

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq F_3 \subseteq E$ and $[E : F_3] = 2,\ [\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2,\ [E : \mathbf{Q}] = 4 \Rightarrow F_3 = \mathbf{Q}(\sqrt{2})$.

Clearly F_4 = fixed field of H_4 $(= G)$ is $\mathbf{Q}$ and F_5 = fixed field of $H_5 = E$.

So, F_1, F_2, F_3, F_4, F_5 are intermediate fields lying between $\mathbf{Q}$ and E.

Since F_1, F_2, F_3 are quadratic extensions of $\mathbf{Q}$, $F_1/\mathbf{Q}$, $F_2/\mathbf{Q}$, $F_3/\mathbf{Q}$ are normal. Also $F_4/\mathbf{Q}$, $F_5/\mathbf{Q}$ are normal. But G being abelian, all subgroup of G are normal subgroups of G.

Roots of Unity

Definition: Let E be a minimal splitting field of $f(x) = x^n - 1$ over k. Then the roots of $f(x)$ in E are called *nth roots of unity*. E is called the *associated cyclotomic field*.

Theorem 49: *The nth roots of unity form a cyclic group under multiplication, whose order is a divisor of n.*

Proof: Let $G = \{\alpha \in E \mid \alpha^n = 1\} \subseteq E^* = E - (0)$. Then $1 \in G \Rightarrow G \neq \varphi$.

Let $\alpha, \beta \in G$. Then $\alpha^n = 1 = \beta^n$. Now E^* is abelian group under multiplication.

So, $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = \alpha\beta^{-1} \Rightarrow \alpha\beta^{-1} \in G \Rightarrow G$ is a subgroup of E^*.

So, G is a finite abelian group.

Let $\alpha \in G$ be an element of maximum order m in G.

So, $o(\beta)$ divides m for all $\beta \in G \Rightarrow \beta^m = 1$ for all $\beta \in G$.

Let $n = mq + r$, $0 \leq r < m$. Let $r \neq 0$.

Now $1 = \alpha^n = \alpha^{mq}\alpha^r = \alpha^r \Rightarrow \alpha^r = 1$, $r < m$, $r > 0$, contradicting $o(\alpha) = m$.

So, $r = 0$. Thus, m divides n.

Now $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ are distinct elements of $G \Rightarrow o(G) \geq m$.

Since E has at most n roots of $g(x) = x^m - 1$ over k, $o(G) \leq m$.

So, $o(G) = m$ and $G = \{1, \alpha, \ldots, \alpha^{m-1}\}$.

$\Rightarrow G$ is a cyclic group generated by α such that $o(G) = o(\alpha) = m$ divides n.

Note: Let k be a field and n, a positive integer. Suppose char $k = 0$ or char $k = p$ such that $(p, n) = 1$. Then all nth roots of unity over k are simple and so distinct.

Proof: Let $f(x) = x^n - 1 \in k[x]$

Then $f'(x) = nx^{n-1}$

Let α be a zero of $f(x)$ in a splitting field of f over k.

If $f'(\alpha) = 0$, then $n\alpha^{n-1} = 0$. If char $k = 0$, then $n = 0$ or $\alpha = 0$, none of which is true. If char $k = p$, $(p, n) = 1$, then $\alpha = 0$ or p divides n, none of which is true. So, $f'(\alpha) \neq 0 \Rightarrow$ roots of f are simple.

Throughout this section, we assume that char $k = 0$ or char $k = p$, $(p, n) = 1$. Then, $o(G) = n$, where $G = \{\alpha \in E \mid \alpha^n = 1\}$, E a minimal splitting field of f over k. Also G is cyclic. *A* generator of G is called *primitive nth root of unity*. Since the number of generators of G is $\phi(n)$, the number of primitive nth roots of unity is $\phi(n)$. Since G is cyclic, let $G = \langle\alpha\rangle$. Then $\alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n = 1$ are distinct roots of $f(x)$ in E. So, $E = k(\alpha, \alpha^2, \ldots, \alpha^{n-1}) = k(\alpha)$, the cyclotomic field over k.

The polynomial $\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ 0(\alpha^i) = n}} (x - \alpha^i) = \prod_{\substack{1 \leq i \leq n \\ (i,n)=1}} (x - \alpha^i)$ is called *nth cyclotomic polynomial over k* Then $\Phi_d(x) = \prod_{\substack{0(\alpha^i) = d \\ 1 \leq i \leq n}} (x - \alpha^i) = \prod_{\substack{1 \leq i \leq n \\ (i,d)=1}} (x - \alpha^i)$ is dth cyclotomic polynomial over k.

Theorem 50: $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$

Proof: $x^n - 1 = \prod_{1 \le i \le n} (x - \alpha^i)$, where $G = <\alpha>$.

Now $d \mid n \Leftrightarrow n = kd \Leftrightarrow o(\alpha^k) = d$.

So, $x^n - 1 = \prod_{d \mid n} \prod_{o(\alpha^k) = d} (x - \alpha^k)$

$$= \prod_{d \mid n} \Phi_d(x).$$

Now $\Phi_1(x) = x - 1$ by taking $n = 1$.

Let n = prime p. Then $x^p - 1 = \Phi_1(x)\Phi_p(x)$ as p, 1 are only divisors of p.

So, $\Phi_p(x) = \dfrac{x^p - 1}{\Phi_1(x)} = \dfrac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}$

Therefore, $\Phi_{p^2}(x) = \dfrac{x^{p^2} - 1}{\Phi_1(x)\Phi_p(x)}$

$$= \frac{x^{p^2} - 1}{x^p - 1} = 1 + x^p + \ldots + x^{p(p-1)}$$

Thus, $\Phi_2(x) = 1 + x$, $\Phi_3(x) = 1 + x + x^2$

$\Phi_4(x) = 1 + x^2$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}$$

$$= \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)}$$

$$= x^2 - x + 1.$$

Theorem 51: *For any prime p and a positive integer m,*

$$\Phi_{p^m}(x) = 1 + x^{p^{m-1}} + \ldots + x^{(p-1)p^{m-1}}$$

Proof:

Now $\Phi_{p^m}(x) = \dfrac{x^{p^m} - 1}{\Phi_1(x)\,\Phi_p(x) \ldots \Phi_{p^{m-1}}(x)}$

$$= \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = 1 + x^{p^{m-1}} + \ldots + x^{(p-1)p^{m-1}}.$$

Möbius function: The map $\mu : \mathbf{N} \to \{0, 1, -1\}$ such that $\mu(1) = 1$, $\mu(n) = 0$ if p^2 divides n for some prime p and $\mu(p_1 p_2 \ldots p_r) = (-1)^r$, where $p_1, p_2, \ldots, p_r$ are distinct primes is called the Möbius function. Clearly, $\mu(12) = 0$, $\mu(15) = 1$, $\mu(3) = -1$.

The following result is known as *Möbius inversion formula.*

If $f, g : \mathbf{N} \to \mathbf{R}$ (where **N** denotes the set of natural numbers and **R**, the set of real numbers), then

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu(\tfrac{n}{d}).$$

Theorem 52: $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$.

Proof: Now $x^n - 1 = \prod_{d|n} \Phi_d(x)$

$\Rightarrow \log (x^n - 1) = \sum_{d|n} \log \Phi_d(x)$

Let $f(x) = \log x^n - 1$

$g(d) = \log \Phi_d(x)$.

Then $f(x) = \sum_{d|n} g(d)$.

By Möbius inversion formula

$$\log \Phi_n(x) = \sum_{d|n} \log(x^d - 1)\, \mu\left(\frac{n}{d}\right).$$

$$= \sum_{d|n} \log(x^d - 1)^{\mu(\frac{n}{d})}$$

$$= \log \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

$\Rightarrow$ $$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

Theorem 53: $\sum_{d|n} u(d) = 0$, for $n > 1$.

Proof: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ where $p_i s$ are distinct primes.

Thus, $$\sum_{d|n} u(d) = \mu(1) + \mu(p_1) + \ldots + \mu(p_r) + \mu(p_1 p_2) + \ldots + \mu(p_{r-1} p_r) + \ldots + \mu(p_1 p_2 \ldots p_r)$$
$$= 1 + r_{c_1}(-1)^2 + \ldots + r_{c_r}(-1)^r$$
$$= (1 + (-1))^r = 0.$$

Problem 11: *Show that* $\prod_{d|n} (x-1)^{\mu(\frac{n}{d})} = 1$, $n > 1$.

Solution: Let P denote L.H.S.

Then $\log P = \sum_{d|n} \log (x-1)^{\mu(\frac{n}{d})}$

$$= \sum_{d|n} (\log(x-1))\mu(\tfrac{n}{d})$$

$$= \log(x-1) \sum_{d|n} \mu(\tfrac{n}{d})$$

$$= \log(x-1) \sum_{d|n} \mu(d)$$

$$= 0 \Rightarrow P = 1.$$

Problem 12: *Prove that* $\Phi_n(1) = \prod_{d|n} d^{\mu(\frac{n}{d})}$, $n > 1$. *Deduce that* $\Phi_n(1) = 0$, p *or* 1 *according as* n *is* 1, p^α (*p, a prime*) *or divisible by at least two primes.*

Solution: $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$

$$= \prod_{d|n} (x-1)^{\mu(\frac{n}{d})} \prod_{d|n} (x^{d-1} + \ldots + x + 1)^{\mu(\frac{n}{d})}$$

$$= \prod_{d|n} (x^{d-1} + \ldots + x + 1)^{\mu(\frac{n}{d})} \text{ by above problem}$$

So, $\Phi_n(1) = \prod_{d|n} d^{\mu(\frac{n}{d})}$, when $n > 1$.

(Note $\Phi_n(1) = \prod_{d|n} (\frac{n}{d})^{\mu(d)}$ as $d \mid n \Rightarrow \frac{n}{d} \mid n$)

when $n = 1$, $\Phi_n(1) = 0$.

when $n = p^\alpha$, $\Phi_n(1) = (p^\alpha)^{\mu(1)} (p^{\alpha-1})^{\mu(p)}$

$$= \frac{p^\alpha}{p^{\alpha-1}} = p$$

when $n = p_1^{\alpha_1} p_2^{\alpha_2}$

Then $\Phi_n(1) = (p_1^{\alpha_1 - 1} p_2^{\alpha_2})^{-1} (p_1^{\alpha_1} p_2^{\alpha_2 - 1})^{-1}$

$$\times (p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1})^1 \times (p_1^{\alpha_1} p_2^{\alpha_2})^1$$

$$= 1$$

Let $n = p^k p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ where p, p_is are distinct primes and $r \geq 2$.Then $n = p^k m$, where $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$.

So, $$\Phi_{mp^k}(1) = \prod_{d|mp^k} \left(\frac{mp^k}{d} \right)^{\mu(d)}$$

$$= \prod_{d|mp} \left(\frac{mp^k}{d} \right)^{\mu(d)}$$

$$= \prod_{d|m}\left(\frac{mp^k}{d}\right)^{\mu(d)} \prod_{d|m}\left(\frac{mp^{k-1}}{d}\right)^{-\mu(d)} \quad \text{as } \mu(p) = -1$$

$$= \prod_{d|m} p^{\mu(d)} = 1$$

(as $P = \prod_{d|m} p^{\mu(d)} \Rightarrow \log P = \sum_{d|m} (\log p)^{\mu(d)} = \log p \sum_{d|m} \mu(d) = 0$)

(**Note:** We have used the fact that $\mu(mn) = \mu(m)\,\mu(n)$ whenever $(m, n) = 1$).

Theorem 54: *$a \in F_p$ is primitive nth root of unity if and only if $p \equiv 1 (mod\ n)$.*

Proof: Suppose $a \in F_p$ is a primitive nth root of unity. Now $0 \neq a \in F_p \Rightarrow a^{p-1} = 1 \Rightarrow o(a) \mid p - 1 \Rightarrow n \mid p - 1 \Rightarrow p \equiv 1 \pmod{n}$

Conversely, let $p \equiv 1 \pmod{n}$. Let $F_p^* = <\alpha>$. Then $o(\alpha) = p - 1 = nm$

$$\Rightarrow o(\alpha^m) = \frac{o(\alpha)}{(o(\alpha), m)} = \frac{nm}{(nm, m)} = \frac{nm}{m} = n$$

$\Rightarrow \alpha^m$ is a primitive nth root in F_p.

Problem 13: *Let p, q be distinct primes. Show that x^{q-1} splits into linear factors over F_p if and only if $p \equiv 1 (mod\ q)$.*

Solution: Suppose $x^q - 1$ splits into linear factors over F_p.

Let $1 \neq \alpha$ be a zero of x^{q-1} in F_p.

Then $\alpha^q = 1 \Rightarrow o(\alpha)$ divides $q \Rightarrow o(\alpha) = q$ as $\alpha \neq 1 \Rightarrow \alpha$ is a primitive qth root of unity in $F_p \Rightarrow p \equiv 1 (\text{mod } q)$.

Conversely, let $p \equiv 1 \pmod{q}$. Then F_p contains a primitive qth root α of unity. $\alpha \in F_p$ and $o(\alpha) = q$. Since q is prime, $\alpha, \alpha^2, \ldots \alpha^{q-1}$ each have order q and are in F_p.

Let $f(x) = x^q - 1$

Then $f(x) = (x - 1)(x - \alpha) \ldots (x - \alpha^{q-1})$ splits into linear factors in F_p.

Theorem 55: *The coefficients of $\Phi_n(x)$ over $\mathbf{Q}$ are integers for all $n \geq 1$.*

Proof: We prove the result by induction on n. Let $n = 1$.

Then $\Phi_n(x) = \Phi_1(x) = x - 1 \in \mathbf{Z}[x]$. Assume that the result is true for all positive integers $m < n$.

Then $\Phi_d(x) \in \mathbf{Z}[x]$, for all $d \mid n$.

Let $$f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \in \mathbf{Z}[x]$$

Then $x^n - 1 = \Phi_n(x)\, f(x)$.

Since $f(x)$ is monic, by division algorithm, $x^n - 1 = h(x)f(x) + r(x)$, $h(x), r(x) \in \mathbf{Z}[x]$ and $r(x) = 0$ or deg $r(x) <$ deg $f(x)$, $h(x), r(x)$ are uniquely determined.

But $x^n - 1 = \Phi_n(x) f(x)$, $\Phi_n(x) \in \mathbf{Q}[x]$ and $h(x), r(x) \in \mathbf{Z}[x] \subseteq \mathbf{Q}[x]$ are uniquely determined $\Rightarrow \Phi_n(x) = h(x) \in \mathbf{Z}[x]$, $r(x) = 0$.

So, the result is true for n also.

By induction the result is true for all integers $n \geq 1$.

Theorem 56: *Let* $\Phi_n(x)$ *be nth cyclotomic polynomial over* **Q**. *Then* $\Phi_n(x)$ *is irreducible over* **Q**.

Proof: Since **Z** is a UFD and $\Phi_n(x) \in \mathbf{Z}[x]$ is monic, $\Phi_n(x)$ is primitive.

$\Phi_n(x)$ is irreducible over **Z** if and only if $\Phi_n(x)$ is irreducible over **Q**, the quotient field of **Z**.

We show that $\Phi_n(x) \in \mathbf{Z}[x]$ is irreducible over **Z**.

Let h be an irreducible factor of $\Phi_n(x)$ in $\mathbf{Z}[x]$.

Let $\Phi_n(x) = f(x)\ h(x)$, $f, h \in \mathbf{Z}[x]$, deg $h \geq 1$.

Since $\Phi_n(x)$ is monic, so are f, h.

Let α be a root of h in **C** and let p be a prime such that $(p, n) = 1$.

We show that α^p is also a root of h in **C**.

Since $h(\alpha) = 0$, $\Phi_n(\alpha) = 0$. So, α is a primitive nth root of unity.

$\Rightarrow o(\alpha) = n \Rightarrow o(\alpha^p) = \dfrac{o(\alpha)}{(p, n)} = n \Rightarrow \alpha^p$ is also a primitive nth root of unity

$\Rightarrow \Phi_n(\alpha^p) = 0 \Rightarrow f(\alpha^p) = 0$ or $h(\alpha^p) = 0$. Suppose $h(\alpha^p) \neq 0$. Then $f(\alpha^p) = 0 \Rightarrow \alpha$ is a root of $f(x^p)$.

Now h is irreducible over $\mathbf{Z} \Rightarrow h$ is irreducible over **Q** as h is primitive.

Also $h(\alpha) = 0$. So, $h = Irr\ (\mathbf{Q}, \alpha)$. Since α is also a root of $f(x^p)$ over **Q**, $h(x)$ divides $f(x^p)$ in **Q**.

Let $f(x^p) = h(x)\ k(x)$, $k(x) \in \mathbf{Q}[x]$. By division algorithm

$f(x^p) = h(x)\ k_1(x) + r_1(x)$, where $r_1(x) = 0$ or deg $r_1(x) <$ deg $h(x)$, $k_1, r_1 \in \mathbf{Z}[x]$. So, $h, r_1 \in \mathbf{Q}[x]$. But in $\mathbf{Q}[x]$, the quotient and remainder obtained by dividing $f(x^p)$ with $h(x)$ are uniquely determined. So, $k(x) = k_1(x) \in \mathbf{Z}[x]$.

Now $\theta : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$ s.t.,

$\theta(\Sigma a_i x^i) = \Sigma \bar{a}_i\ x^i$, where $a_i = pq_i + \bar{a}_i$, $\bar{a}_i \in \mathbf{Z}$, $0 \leq a_i < p$

(*i.e.*, $\theta(g(x)) = \bar{g}(x)$)

is a ring homorphism.

So, $\theta(f(x^p)) = \theta(h(x))\ \theta(k(x))$

$\Rightarrow \bar{f}(x^p) = \bar{h}(x)\ \bar{k}(x)$

Since char $\mathbf{Z}_p = p$, $\bar{f}(x^p) = (\bar{f}(x))^p$

$\Rightarrow \bar{h}(x)$ divides $(\bar{f}(x))^p$

$\Rightarrow$ some irreducible factor $\bar{h}_1$ of $\bar{h}$ divides $(\bar{f}(x))^p$

$\Rightarrow \bar{h}_1$ divides $\bar{f}(x)$ in $\mathbf{Z}_p[x]$

$\Rightarrow \bar{f}, \bar{h}$ have common factor $\bar{h}_1$ in $\mathbf{Z}_p[x]$

Now $x^n - 1 = \Phi_n(x)\ r(x)$, $r(x) \in \mathbf{Z}[x]$

$= f(x)\ h(x)\ r(x)$

$\Rightarrow x^n - \bar{1} = \bar{f}(x)\ \bar{h}(x)\ \bar{r}(x)$

$\Rightarrow x^n - \bar{1}$ has a multiple root as $\bar{f}$, $\bar{h}$ have $\bar{h}_1$ as common factor.

Since char $\mathbf{Z}_p = p$ and $(p, n) = 1$, $x^n - \bar{1}$ has distinct roots.

So, we get a contradiction.

So, $h(\alpha^p) = 0$. Thus, whenver $h(\alpha) = 0$ and $(p, n) = 1$, p a prime, then $h(\alpha^p) = 0$.

Now $\Phi_n(x) = \prod_{\substack{(r,n)=1 \\ 1 \le r \le n}} (x - \alpha^r)$, $o(\alpha) = n$.

Let $(r, n) = 1$, $r > 1$, $r = p_1^{k1}\ p_2^{k2}\ \ldots\ p_s^{ks}$, where $p_i s$ are distinct primes. Since $(r, n) = 1$, $(p_i, n) = 1$ for all i.

Therefore, α^{p_i} is a root of h for all i.

$\Rightarrow \alpha^{p_i^{k_i}}$ is a root of h for all i.

$\Rightarrow \alpha^r$ is a root of h.

Therefore, $\Phi_n(x)$ divides $h(x)$.

But $h(x)$ already divides $\Phi_n(x)$.

Thus, $\Phi_n(x) = h(x)$ is irreducible over $\mathbf{Q}$.

Theorem 57: $\mathbf{Q}(\alpha)/\mathbf{Q}$ *is Galois, where* α *is a primitive nth root of unity over* $\mathbf{Q}$.

Proof: Now $\mathbf{Q}(\alpha)$ is a minimal splitting field of $f(x) = x^n - 1$ over $\mathbf{Q}$

$\Rightarrow \mathbf{Q}(\alpha)/\mathbf{Q}$ is finite normal.

Also, char $\mathbf{Q} = 0 \Rightarrow \mathbf{Q}$ is perfect $\Rightarrow \mathbf{Q}(\alpha)/\mathbf{Q}$ is separable.

So, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois.

Theorem 58: *Let* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *be n distinct roots of unity over* $\mathbf{Q}$ *in* $\mathbf{C}$. *Then* $\Phi_n(x) = (x - \alpha_1)\ (x - \alpha_2)\ \ldots\ (x - \alpha_n) \in \mathbf{Q}[x]$.

Proof: Let α be a primitive nth root of unity over $\mathbf{Q}$. By above theorem, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois $\Rightarrow$ $\mathbf{Q}$ is the fixed field of G, the group of all $\mathbf{Q}$-automorphisms of $\mathbf{Q}(\alpha)$. Let $\sigma \in G$. Then $o(\sigma(\alpha)) = o(\alpha) \Rightarrow \sigma(\alpha)$ is also a primitive nth root of unity in $\mathbf{C}$.

So, $\sigma(\Phi_n(x)) = (x - \sigma(\alpha_1))\ \ldots\ (x - \sigma(\alpha_n))$. But $\mathbf{C}$ already has n roots of $f(x) = x^n - 1 \in \mathbf{Q}[x]$.

$\Rightarrow \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

$\Rightarrow \sigma(\Phi_n(x)) = (x - \alpha_1)\ \ldots\ (x - \alpha_n) = \Phi_n(x)$

Let $\Phi_n(x) = x^n + a_1\ x^{n-1} + \ldots + a_n, \quad a_i \in \mathbf{C}$

Then $\Phi_n(x) = \sigma(\Phi_n(x))$

$= x^n + \sigma(a_1)\ x^{n-1} + \ldots + \sigma(a_n)$

$\Rightarrow \sigma(a_i) = a_i$ for all i, $\sigma \in G$

$\Rightarrow a_i$ belongs to the fixed field of G

$\Rightarrow a_i \in \mathbf{Q}$, for all i

$\Rightarrow \Phi_n(x) \in \mathbf{Q}[x]$.

Theorem 59: Let $U_n = \{a \in \mathbf{Z} \mid 1 \le a \le n, (a, n) = 1\}$. *Then* U_n *is a group under multiplication modulo n. If G is the Galois group of* $\mathbf{Q}(\alpha)/\mathbf{Q}$, *then* $G \cong U_n$.

Proof: By Artin's theorem,

$$o(G) = [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg Irr\ (\mathbf{Q}, \alpha)$$
$$= \deg \Phi_n(x)$$
$$= \varphi(n)$$

Let $\sigma \in G$. Then $\sigma(\alpha)$ is a primitive nth root of unity in $\mathbf{C} \Rightarrow \sigma(\alpha) = \alpha^i$, for some i, $(i, n) = 1$

Define $\theta : G \to U_n$ s.t.,
$\theta(\sigma) = i$.

Let $\sigma, \eta \in G$. Let $\theta(\sigma) = i$, $\theta(\eta) = j$

Then $(\sigma\eta)(\alpha) = \sigma(\eta(\alpha)) = \sigma(\alpha^j) = (\sigma(\alpha))^j = \alpha^{ioj}$

So, $\theta(\sigma\eta) = ioj = \theta(\sigma) o\ \theta(\eta)$.

Thus, θ is a homomorphism.

Let $\theta(\sigma) =$ Identity $= 1$.

Then $\sigma(\alpha) = \alpha \Rightarrow \sigma = I \Rightarrow \theta$ is 1-1.

So, $G \cong \theta(G) \le U_n$.

But $o(G) = \varphi(n) \Rightarrow 0(\theta(G)) = \varphi(n) = o(U_n)$.

$\Rightarrow$ $(o(\theta(G)) = o(U_n) \Rightarrow \theta(G) = U_n \Rightarrow G \cong U_n$.

Note: If V_n denotes the units of $\dfrac{\mathbf{Z}}{< n >}$, then V_n forms a group under multiplication and $V_n \cong U_n$.

Proof: $\dfrac{\mathbf{Z}}{< n >} = \{< n > + 1, < n > + 2, ..., < n > + n\}$.

Let $< n > + a$ be a unit in $\dfrac{\mathbf{Z}}{< n >}$.

Then $(< n > + a)(< n > + b) = < n > + 1,\ 1 \le b \le n$

$\Rightarrow < n > + ab = < n > + 1$

$\Rightarrow 1 - ab \in < n > \Rightarrow 1 - ab = nm$

Let $(a, n) = d > 1$. Let p be a prime dividing d. Then $p \mid d \mid a \Rightarrow p \mid a \Rightarrow p \mid ab$. Also $p \mid n \Rightarrow p \mid nm \Rightarrow p \mid ab + nm = 1$, not ture.

$\Rightarrow (a, n) = 1 \Rightarrow a \in U_n$.

Define $f : V_n \to U_n$ s.t.,
$f(< n > + a) = a$

Then f is 1-1 homomorphism.

Also, $a \in U_n \Rightarrow (a, n) = 1$

$\Rightarrow ar + ns = 1$ for some integers r, s

$\Rightarrow (< n > + a)(< n > + r) = < n > + 1$

Let $r = nq + t,\ 0 \le t < n$

So, $< n > + r = < n > + t$.

If $t = 0$, then $< n > + t = < n > + n$.

So, $< n > + r \in \dfrac{\mathbf{Z}}{< n >}$. Therefore, $< n > + a$ is a unit in $\dfrac{\mathbf{Z}}{< n >}$.

$\Rightarrow < n > + a \in V_n$ and $\theta(< n > + a) = a \Rightarrow \theta$ is onto.

So, $V_n \cong U_n$.

Problem 14: *If α is a primitive nth root of unity over k, then $k(\alpha)/k$ is Galois.*

Solution: Let $f(x) = x^n - 1 \in k[x]$. Let $g(x) = Irr\,(k, \alpha)$.

Now $f(x)$ splits in $k(\alpha)$ and $f(\alpha) = 0 \Rightarrow g(x) \mid f(x)$ in $k[\alpha]$.

But zeros of $f(x)$ are simple in $k[\alpha]$.

$\Rightarrow \alpha$ is a simple zero.

$\Rightarrow \alpha$ is separable over k.

$\Rightarrow k(\alpha)/k$ is separable

Also $k(\alpha)/k$ is a minimal splitting field of $f(x)$ over k, $k(\alpha)/k$ is finite normal

$\Rightarrow k(\alpha)/k$ is Galois.

Problem 15: *Let $\Phi_n(x) = (x - \alpha_1)\,(x - \alpha_2)\,\ldots\,(x - \alpha_n)$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are nth roots of unity over k. Show that $\Phi_n(x) \in P[x]$, where P is the prime subfield of k.*

Solution: We prove the result by induction on n. Let $n = 1$.

Then $\Phi_n(x) = \Phi_1(x) = x - 1 \in P[x]$ as $1 \in P$.

Assume that the result is true for all integers $m < n$.

Then $\Phi_d(x) \in P[x]$ for $d < n$. Let $f(x) = \prod_{d \mid n} \Phi_d(x) \in P[x]$.

Then $x^n - 1 = \Phi_n(x)\, f(x)$

Since $x^n - 1, f(x) \in P[x]$, by division algorithm

$$x^n - 1 = h(x)\, f(x) + r(x), \quad h(x), r(x) \in P[x]$$

and are uniquely determined such that $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

Now $x^n - 1 = \Phi_n(x)\, f(x)$, where $\Phi_n(x) \in k(\alpha)[x]$ and $x^n - 1 \in P[x] \subseteq k(\alpha)[x]$

(Here α is a primitive nth root of unity over k), $f(x) \in P[x] \subseteq k(\alpha)[x]$.

So, $h(x) = \Phi_n(x) \in P[x] \Rightarrow$ the result is true for n also. By induction the result is true for all integers $n \geq 1$.

Problem 16: *Determine the Galois group of Cyclotomic extension $\mathbf{Q}(\alpha)/\mathbf{Q}$, where α is a primitive 12th root of unity over $\mathbf{Q}$. Also, find the intermediate fields between $\mathbf{Q}$ and $\mathbf{Q}(\alpha)$.*

Solution: Let G denote the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

Since α is a primitive 12th root of unity, $o(\alpha) = 12$.

Also, $o(G) = \varphi(12) = 4$ and $G = \{\sigma_1 = I, \sigma_5, \sigma_7, \sigma_{11}\}$, where $\sigma_5(\alpha) = \alpha^5$, $\sigma_7(\alpha) = (\alpha)^7$, $\alpha_{11}(\alpha) = \alpha^{11}$. (As in Example 14(*ii*))

Also, $\sigma_5^2(\alpha) = \sigma_5\sigma_5(\alpha) = \alpha^{25} = \alpha \Rightarrow \sigma_5^2 = I$.

Similarly, $\sigma_7^2 = I = \sigma_{11}^2$.

$\Rightarrow G$ is non cyclic group of order 4 *i.e.*, G is Klein's 4-group.

Let $H_1 = \{I, \sigma_5\}$, $H_2 = \{I, \sigma_7\}$, $H_3 = \{I, \sigma_{11}\}$, $H_4 = \{I\}$, $H_5 = G$.

Then these are the only subgroups of G.

Now $\sigma_5(\alpha^3) = (\sigma_5(\alpha))^3 = \alpha^{15} = \alpha^3$

$\Rightarrow \sigma_5$ fixes α^3

$\Rightarrow H_1$ fixes α^3

If F_1 is the fixed field of H_1, then

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha^3) \subseteq F_1 \subseteq \mathbf{Q}(\alpha)$$

But $[\mathbf{Q}(\alpha^3) : \mathbf{Q}] = [\mathbf{Q}(i) : \mathbf{Q}]$, $\alpha = e^{\frac{2\pi i}{12}}$

$= \deg Irr\ (\mathbf{Q}, i)$

$= \deg\ (x^2 + 1) = 2$

Also, by Artin's theorem

$2 = o(H_1) = [\mathbf{Q}(\alpha) : F_1]$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = o(G) = 4 \Rightarrow F_1 = \mathbf{Q}(\alpha^3)$

If F_2 is the fixed field of H_2, then $\sigma_7(\alpha^4) = \alpha^{28} = \alpha^4 \Rightarrow \alpha^4 \in F_2$.

But $\alpha^4 = e^{\frac{2\pi i}{3}} = \dfrac{-1}{2} + \dfrac{\sqrt{3}\,i}{2}$

$$\Rightarrow \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i)$$

So, $$\mathbf{Q} \subseteq \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i) \subseteq F_2 \subseteq \mathbf{Q}(\alpha)$$

and $[\mathbf{Q}(\sqrt{3}i) : \mathbf{Q}] = \deg Irr\ (\mathbf{Q}, \sqrt{3}i)$

$= \deg\ (x^2 + 3) = 2$

Also $[\mathbf{Q}(\alpha) : F_2] = 2$ by Artin's theorem

$$\Rightarrow F_2 = \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i)$$

Now $\sigma_{11}(\alpha) = \alpha^{11} \Rightarrow \sigma_{11}\left(\cos\dfrac{\pi}{6} + i\sin\dfrac{\pi}{6}\right) = \cos\dfrac{11\pi}{6} + i\sin\dfrac{11\pi}{6}$

$$\Rightarrow \sigma_{11}\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

But $\sigma_{11}(i) = \sigma_{11}(\alpha^3) = \alpha^{33} = \alpha^9 = -i$

So, $$\frac{1}{2}\sigma_{11}(\sqrt{3}) - \frac{1}{2}i = 8\,\frac{\sqrt{3}}{2} - \frac{1}{2}i$$

$$\Rightarrow \sigma_{11}\,(\sqrt{3}) = \sqrt{3} \Rightarrow H_3 \text{ fixes } \sqrt{3}$$

Thus, if F_3 is the fixed field of H_3, then $F_3 = \mathbf{Q}(\sqrt{3})$

Also, $F_4 = \mathbf{Q}(\alpha)$ = the fixed field of H_4.

$F_5 = \mathbf{Q}$ = the fixed field of H_5.

Finite Fields

A field having finite number of elements is called a finite field or a Galois field.

Theorem 60: *If F is a finite field, then $o(F) = p^n$ for some prime p and an integer $n \geq 1$.*

Proof: Let P be the prime subfield of F.

Since F is finite, so is P. Therefore, $P \cong \dfrac{\mathbf{Z}}{< p >}$ for some prime p.

But $\dfrac{\mathbf{Z}}{< p >} \cong \{0, 1, 2, ..., p - 1\} \bmod p = F_p \Rightarrow P \cong F_p$.

Since $P \subseteq F$, we can regard $F_p \subseteq F$. Now F is a vector space over F_p. Since F is finite, $[F : F_p] = n$ = finite.

Let $\{u_1, ..., u_n\}$ be a basis of F/F_p.

Then $F = \{\alpha_1 u_1 + ... + \alpha_n u_n \mid \alpha_i \in F_p\}$.

Now each α_i can be chosen in p ways and $\Sigma\alpha_i u_i = \Sigma\beta_i u_i \Rightarrow \alpha_i = \beta_i$, therefore $o(F) = p^n$.

Remark: We had proved this result earlier under rings also (see page 331).

Theorem 61: *Let p be a prime and $n \geq 1$ be an integer. Then there exists a field with p^n elements.*

Proof: Let $f(x) = x^q - x \in F_p[x]$, $q = p^n$. Let F be a minimal splitting field of $f(x)$ over F_p.

Then $F = F_p$ (zeros of f in F).

Let $S = \{\text{zeros of } f \text{ in } F\}$.

Now $f' = qx^{q-1} - 1 = -1$ as char $F = p \Rightarrow q - 1 = p^n - 1 = -1$.

Therefore, $(f, f') = 1$

$\Rightarrow$ all zeros of f in F are simple and so distinct.

So, $o(S) = q$.

Now $0 \in S \Rightarrow S \neq \varphi$.

Also $a, b \in F_q \Rightarrow a^q = a$, $b^q = b \Rightarrow (a \pm b)^q = a^q \pm b^q = a \pm b$,

$(ab)^q = a^q b^q = ab$, $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$

$\Rightarrow a \pm b, ab, ab^{-1}$ (if $b \neq 0$) $\in S$.

Thus, S is a subfield of F.

Let $a \in F_p$. Then $a^{p-1} = 1 \Rightarrow a^p = a \Rightarrow a^{p^n} = a \Rightarrow a^q = a$.

$\Rightarrow a$ is a zero of f in $F \Rightarrow a \in S \Rightarrow F_p \subseteq S$.

So S is a field containing F_p and S.

But F is the smallest field containing F_p and S.

$\Rightarrow F \subseteq S$. Also $S \subseteq F$. So, $S = F \Rightarrow o(F) = o(S) = q$.

We now prove the following results from group theory.

Lemma 1: *Let G be an abelian group under multiplication. Let $a, b \in G$ be such that $o(a) = m$, $o(b) = n$ and $(m, n) = 1$. Then $o(ab) = mn$*

Proof: See Problem 36 on page 94.

Lemma 2: *Let G be an abelian group under multiplication. Let $a, b \in G$ be such that $o(a) = m$, $o(b) = n$. Then there exists $c \in G$ such $o(c)$ = l.c.m. of m and n.*

Proof: Let $(m, n) > 1$.

Let $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$

$n = p_1^{\beta_1} \ldots p_r^{\beta_r}$

where $p_1, \ldots, p_r$ are distinct primes and α_i, β_i are non negative integers.

Let $l = p_1^{\alpha_1} \ldots p_s^{\alpha_s} \; p_{s+1}^{\beta_{s+1}} \ldots p_r^{\beta_r}$

where $\alpha_i \geq \beta_i$ for $i = 1, \ldots, s$ and $\beta_j \geq \alpha_j$ for $j = s + 1, \ldots, r$.

Then l is the l.c.m of m and n.

Let $x = a^{p_{s+1}^{\alpha_{s+1}}} \ldots p_r^{\alpha_r}$, $y = b^{p_1^{\beta_1}} \ldots p_s^{\beta_s}$

Then $o(x) = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$

$o(y) = p_{s+1}^{\beta_{s+1}} \ldots p_r^{\beta_r}$

and $(o(x)), o(y)) = 1$.

By Lemma 1,

$o(xy)$ = l.c.m. of m and n

$= p_1^{\alpha_1} \ldots p_s^{\alpha_s} \; p_{s+1}^{\beta_{s+1}} \ldots p_r^{\beta_r}$.

Lemma 3: *With the hypothesis of lemma 2, if $n \nmid m$, then the l.c.m. l of m and n is greater than m.*

Proof: Now $m \mid l \Rightarrow m \leq l$. If $m = l$, then $n \mid l \Rightarrow n \mid m$, a contradiction. So $l > m$.

Lemma 4: *Let G be a finite abelian group under multiplication. Let $\alpha \in G$ be of maximum order. Then $o(\beta) \mid o(\alpha)$ for all $\beta \in G$.*

Proof: Let $o(\alpha) = m$, $o(\beta) = n$.

Suppose $n \nmid m$. By lemma 3, l = l.c.m. of m, $n > m$. By lemma 2, there is $\gamma \in G$ such that $o(\gamma) = l > m$ contradicting $\alpha \in G$ is of maximum order. So, $n \mid m \Rightarrow o(\beta) \mid o(\alpha)$ for all $\beta \in G$.

Theorem 62: *Let F be a finite field. Then F^*, the set of non zero elements of F forms a cyclic group under multiplication in F.*

Proof: Now F^* is an abelian group under multiplication.

Let $\alpha \in F^*$ be an element of maximum order m.

Then by lemma 4, $o(\beta) \mid m$ for all $\beta \in F^*$.

So, $m = o(\beta)r \Rightarrow \beta^m = \beta^{o(\beta)r} = 1$ for all $\beta \in F^*$.

$\Rightarrow \beta$ satisfies $x^m - 1$ over F.

Since F can't have more than m zeros of $x^m - 1$, $o(F^*) \leq m$.

But $\alpha \in F^*$ and $o(\alpha) = m \Rightarrow 1, \alpha, \alpha^2, ..., \alpha^{m-1}$ are distinct elements of F^*

$\Rightarrow \quad o(F^*) \geq m \Rightarrow o(F^*) = m = o(\alpha) \Rightarrow F^* = <\alpha>$.

The generators of F^* are called *primitive elements* of F.

Theorem 63: *Let F be a finite field of order p^n. Then F is a minimal splitting field of $x^{p^n} - x$ over F_p.*

Proof: We can regard F as an extension of F_p. Let $q = p^n$.

Now $F^* = <\alpha>$, $o(\alpha) = o(F^*) = q - 1$. Also $\alpha^{q-1} = 1. \Rightarrow \alpha^q = \alpha$.

$\Rightarrow$ elements of F are zeros of $f(x) = x^q - x$ over F_p.

So, $f(x)$ splits in F.

Therefore, $f(x) = x(x - \alpha) ... (x - \alpha^{q-1})$

$\Rightarrow$ Minimal splitting field of f over F_p is $F_p(\alpha, \alpha^2, ..., \alpha^{m-1}, 1, 0) = F_p(F) = F$.

Theorem 64: *Any two finite fields with the same number of elements p^n are F_p-isomorphic.*

Proof: Let F_1, F_2 be finite fields such that $o(F_1) = p^n = o(F_2)$. Then, by above theorem F_1, F_2 are minimal splitting fields of $f(x) = x^{p^n} - x$ over $F_p \Rightarrow F_1$, F_2 are F_p-isomorphic.

The above theorem shows that there is unique field of order $q = p^n$ upto an isomorphism. It is denoted by $GF(p^n)$ or $GF(q)$ or Fq.

Problem 17: *Show that $x^m - 1$ divides $x^n - 1$ over a field F if and only if m divides n.*

Solution: Let $n = km + r$, $0 \leq r < m$.

The $x^n - 1 = x^r \left(\sum_{i=0}^{k-1} x^{im} \right) (x^m - 1) + (x^r - 1)$.

Therefore, $x^m - 1$ divides $x^n - 1$ if and only if $x^r - 1 = 0$.

Also $x^r - 1 = 0$ if and only if $r = 0$.

So $x^m - 1$ divides $x^n - 1$ if and only if m divides n.

Problem 18: *Show that $x^{p^m} - x$ divides $x^{p^n} - x$ if m divides n.*

Solution: Let $n = mu$.

Then
$$\begin{aligned} p^n - 1 &= p^{mu} - 1 \\ &= (p^m)^u - 1 \\ &= (p^m - 1) \text{ (integer)} \end{aligned}$$

$\Rightarrow p^m - 1$ divides $p^n - 1$

By above problem

$x^{p^m - 1} - 1$ divides $x^{p^n - 1} - 1$

$\Rightarrow x^{p^m} - x$ divides $x^{p^m} - x$.

Theorem 65: *Let F be a field with p^n elements. Then F has a subfield k with p^m elements if and only if m divides n.*

Proof: Suppose k is a subfield of F. Then k can be regarded as an extension of F_p such that $[k : F_p] = m$. Similarly, F can be regarded as an extension of F_p such that $[F : F_p] = n$. Now $[F : F_p] = [F : k]\ [k : F_p] \Rightarrow m$ divides n.

Conversely, let F be a field such that $o(F) = p^n$. Suppose m divides n. Now F is a minimal splitting field of $x^{p^n} - x$ over F_p.

Let $f(x) = x^{p^n} - x$ and $g(x) = x^{p^m} - x$.

Since m divides n, by above problem $g(x)$ divides $f(x)$.

Consider $F' = \{\text{zeros of } g(x) \text{ in } F\}$.

Then F' is a subfield of F.

Since $g(x)$ has p^m distinct zeros, F' is a subfield of F with p^m elements.

If k is another subfield of F such that $o(k) = p^m$, then $o(k) = o(F') = p^m$.

$\Rightarrow k, F'$ are F_p-isomorphic.

Thus, there is exactly one subfield of F (up to isomorphism) with p^m elements.

Problem 19: *Determine the algebraic closure of* F_p.

Solution: We know $m!$ divides $n!$ for all positive integers $m < n$. By above theorem $F_p m!$ is a subfield of $F_p n!$. Thus, there is an ascending chain of subfields

$$F_p \subseteq F_{p^{2!}} \subseteq F_{p^{3!}} \subseteq \ldots$$

and

$F_{p^\infty} = \bigcup_n F_{p^{n!}}$ is a field such that $F_{p^n} \subseteq F_{p^{n!}} \subseteq F_{p^\infty}$ for any positive integer n.

Let S be the set of all polynomials over F_p. Let $f \in S$.

Then the minimal splitting field of f over F_p is a finite field F_{p^n}.

So, each $f \in S$ splits in F_{p^∞}.

Thus, the minimal splitting field of S over F_p is

F_p (zeros of $f \in S$ in F_{p^∞}) $\subseteq F_{p^\infty}$.

Also, $a \in F_{p^\infty} \Rightarrow a \in F_{p^n}$ for some $n \Rightarrow a$ is zero of $x^{p^n} - x$ over F_p.

Now $f = x^{p^n} - x \in S \Rightarrow a$ is zero of $f \in S$ in F_{p^∞}

$\Rightarrow F_{p^\infty} \subseteq F_p$ (zeros of $f \in S$ in F_{p^∞})

$\Rightarrow$ Minimal splitting field of S over F_p is F_{p^∞}

$\Rightarrow F_{p^\infty}$ is the algebraic closure of F_p.

Theorem 66: *Every finite extension of a finite field is Galois.*

Proof: Let K be a finite extension of a finite field k. Then K is also a finite field. So, char k = char $K = p$, for some prime p. Let $o(k) = p^m$, $o(K) = p^n$.

Now K is a minimal splitting field of $x^{p^n} - x$ over $F_p \Rightarrow K/F_p$ is finite normal.

Also F_p is finite $\Rightarrow F_p$ is perfect $\Rightarrow$ every algebraic extension of F_p is separable $\Rightarrow K/F_p$ is separable $\Rightarrow K/F_p$ is Galois. Now, $F_p \subseteq k \subseteq K$ and K/F_p is Galois $\Rightarrow K/k$ is Galois.

Cor.: F_q/F_p is Galois, $q = p^n$.

Theorem 67: *Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over k.*

Proof: Let $o(F) = p^m$, p being a prime.

Let $q = p^{nm}$ and let $f(x) = x^q - x$

Then F_q is the minimal splitting field of $f(x)$ over F_p.

Since m/nm, $F_{p^m} = F$ can be imbedded in F_q.

Now $F_p \subseteq F = F_{p^m} \subseteq F_{p^{mn}} = E$.

Then $[E : F] = n$.

Let E^* be the multiplicative group of non zero elements of E and let $E^* = <\alpha>$

Then $E = F(\alpha)$ as $F \subseteq E$, $\alpha \in E$

So, $n = [E : F] = [F(\alpha) : F] = \deg Irr(F, \alpha)$

$\Rightarrow Irr(F, \alpha)$ is an irreducible polynomial of degree n over F.

Theorem 68: *Let G be the group of F_p-automorphisms of F_q. Then G is a cyclic group generated by Frobenius map of order n, where $q = p^n$.*

Proof: Let $\theta : F_q \to F_q$ s.t.,

$$\theta(b) = b^p.$$

Then θ is called Frobenius map.

Since char F_p = char $F_q = p$, θ is a homomorphism.

Also θ is 1-1.

Since F_q is finite, θ is onto.

If $b \in F_p$, then $b^p = b \Rightarrow \theta(b) = b$ for all $b \in F_p$.

So, θ is an F_p-automorphism of $F_q \Rightarrow \theta \in G$.

By Artin's theorem, $o(G) = [F_q : F_p]$ as F_p is the fixed field of G.

$\Rightarrow o(G) = n$. We show that $o(\theta) = n$.

Let $\theta^r = I$, let $F_q^* = <a>$.

Then $a^{q-1} = 1 \Rightarrow a^q = a \Rightarrow a^{p^n} = a$.

Now $\theta^r = I \Rightarrow \theta^r(a) = a \Rightarrow a^{p^r} = a \Rightarrow a^{p^r - 1} = 1$.

$\Rightarrow o(a) \mid p^r - 1 \Rightarrow q - 1 \mid r - 1 \Rightarrow p^n - 1 \mid p^r - 1 \Rightarrow p^n - 1 \leq p^r - 1 \Rightarrow n \leq r$.

Also $\theta^n(b) = b^{p^n} = b$ for all $b \in F_q \Rightarrow \theta^n = I$.

So, $o(\theta) = n \Rightarrow G = <\theta>$.

Problem 20: *Prove that every element in a finite field can be written as the sum of two squares.*

Solution: Let F be a finite field such that $o(F) = p^n$.

Case 1: $p = 2$. Define $\theta : F \to F$ s.t.,

$$\theta(b) = b^2$$

Then
$$\theta(b_1 + b_2) = (b_1 + b_2)^2 = b_1^2 + b_2^2 = \theta(b_1) + \theta(b_2)$$
$$\theta(b_1 b_2) = (b_1 b_2)^2 = b_1^2 b_2^2 = \theta(b_1)\theta(b_2)$$

$\Rightarrow \theta$ is a homomorphisms.

Also, θ is 1-1. Since F is finite, θ is onto.

Let $a \in F$. Then there is $b \in F$ such that $\theta(b) = a \Rightarrow a = b^2 = b^2 + 0^2$ = sum of two squares in F.

Case 2: $p \neq 2$. Let $a \in F$. Let $X = \{a - x^2 \mid x \in F\}$.

Then $a - x_1^2 = a - x_2^2$, $x_1, x_2 \in F \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = -x_2$ if $x_1 \neq x_2$

$$\Rightarrow \qquad o(X) = \frac{p^n - 1}{2} + 1 = \frac{p^n + 1}{2}.$$

Let $Y = \{y^2 \mid y \in F\}$. Then $o(Y) = \dfrac{p^n + 1}{2}$.

Since $X, Y \subseteq F$ and $o(F) = p^n$, $X \cap Y \neq \varphi$.

So, $a - x^2 = y^2$ for some $x, y \in F \Rightarrow a = x^2 + y^2$ = sum of two squares in F.

Problem 21: *Show that for any integer a and prime p, $a^p \equiv a$ (mod p).*

Solution: Let $a = pq + r, \quad 0 \leq r \leq p.$

Then $a \equiv r \pmod{p}$

Now $0 \leq r < p \Rightarrow r \in F_p$

$$\Rightarrow r_o \underbrace{r_o \ldots o}_{p \text{ times}} r = r$$

$$\Rightarrow r^p - pu = r$$

$$\Rightarrow r^p \equiv r \pmod{p}$$

$$\Rightarrow r^p \equiv a \pmod{p}$$

So, $a \equiv r \pmod{p}$

$$\Rightarrow a^p \equiv r^p \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

(The above result is known as Fermat's theorem)

Problem 22: *Show that every irreducible polynomial $f(x) \in F_p[x]$ is a divisor of $x^{p^n} - x$ for some n.*

Solution: Let deg $f(x) = d$ and α be a zero of $f(x)$ in an extension of F_p. Then, $[F_p(\alpha) : F_p]$ = deg $Irr\,(F_p, \alpha)$ = deg $f(x) = d$.

So, $o(F_p(\alpha)) = p^d$. Then $\alpha \in F_p(\alpha) \Rightarrow \alpha^{p^d} = \alpha \Rightarrow \alpha$ is zero of $x^{p^d} - x \in F_p[x] \Rightarrow f(x)$ divides $x^{p^d} - x$.

Problem 23: *Show that $x^{p^n} - x$ is the product of monic irreducible polynomials in $F_p[x]$ of degree d, d dividing n.*

Solution: Let $f(x) = x^q - x$, $q = p^n$. Let $p(x)$ be a monic irreducible factor of $f(x)$ over F_p. Let α be a zero of $p(x)$ in F, where F is a minimal splitting field of $f(x)$ over F_p. Then $F = F_q$ and $p(x) = Irr\,(F_p, \alpha)$

Now $F_p \subseteq F_p(\alpha) \subseteq F_q$

and $n = [F_q : F_p] = [F_q : F_p(\alpha)]\ [F_p(\alpha) : F_p]$
$= [F_q : F_p(\alpha)]$ deg $Irr\ (F_p, \alpha)$
$= [F_q : F_p(\alpha)]$ deg $p(x)$

$\Rightarrow$ deg $p(x)$ divides n.

$\Rightarrow$ any monic irreducible polynomial dividing $x^{p^n} - x$ is of degree dividing n.

Problem 24: *Show that* $x^p - x - a$ $(a \neq 0)$ *is irreducible over* F_p.

Solution: Let $f(x) = x^p - x - a$

Let α be a zero of $f(x)$ in some extension of F_p. Then $f(\alpha) = 0$

Consider $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a$
$= a^p - \alpha - a = f(\alpha) = 0$
$f(\alpha + 2) = (\alpha + 2)^p - (\alpha + 2) - a$
$= (\alpha + 1)^p - (\alpha + 1) - a$
$= f(\alpha + 1) = 0$

In this way, α, $\alpha + 1$, $\alpha + 2$, ..., $\alpha + (p - 1)$ are all zeros of $f(x)$.

Also $f'(x) = px^{p-1} - 1 = -1 \neq 0 \Rightarrow f'(\beta) = -1 \neq 0$ for $\beta = \alpha, \alpha + 1, ..., \alpha + (p - 1)$

$\Rightarrow \alpha, \alpha + 1, ..., \alpha + (p - 1)$ are distinct zeros of $f(x)$

Now $F_p(\alpha)$ is a minimal splitting field of $f(x)$ over F_p.

Also $[F_p(\alpha) : F_p] = \deg Irr(F_p, \alpha) \leq p$ as α satisfies $f(x)$ of degree p.

Since F_p is finite, so is $F_p(\alpha)$.

Also char $F_p(\alpha) = p \Rightarrow o(F_p(\alpha)) = p^m \Rightarrow [F_p(\alpha) : F_p] = m = \deg Irr\ (F_p, \alpha) = \deg g(x) \leq p$.

Now $\alpha^{p^m} = \alpha$. But $\alpha^p = \alpha + a \Rightarrow \alpha^{p^2} = (\alpha + a)^p = \alpha^p + a^p = \alpha + 2a$ as $a \in F_p \Rightarrow a^p = a$.

In this way, $\alpha^{pm} = \alpha + ma \Rightarrow \alpha = \alpha + ma \Rightarrow ma = 0 \Rightarrow p$ divides m as $a \neq 0 \Rightarrow p \leq m$.

So, $p = m \Rightarrow$ deg $g(x) = p$. Also $g(x)$ divides $f(x)$ and deg $g(x) = \deg f(x)$.

$\Rightarrow g(x) = f(x) \Rightarrow f(x)$ is irreducible over F_p.

Problem 25: *Contruct a field of order* 9.

Solution: Let F_9 be the field of order 9. Let $F_3 = \{0, 1, 2\}$ mod 3. Then $[F_9 : F_3] = 2$. Let $f(x) = x^9 - x$. Then F_9 is a minimal splitting field of $f(x)$ over F_3. Let $p(x)$ be an irreducible factor of $f(x)$ over F_3. Let α be a zero of $p(x)$ in F_9. Then α is a zero of $f(x)$. If $\alpha \in F_3$, then $p(x) = x - \alpha \Rightarrow$ deg $p(x) = 1$. If $\alpha \notin F_3$, then $F_3 \subseteq F_3(\alpha) \subseteq F_9 \Rightarrow [F_9 : F_3] = 2 = [F_9 : F_3(\alpha)]\ [F_3(\alpha) : F_3]$.

Since $\alpha \notin F_3$, $[F_3(\alpha) : F_3] \neq 1$
$\Rightarrow [F_3(\alpha) : F_3] = 2$
But $[F_3(\alpha) : F_3] = \deg Irr\ (F_3, \alpha)$
$= \deg p(x)$

Thus deg $p(x) = 2$.

Hence any irreducible factor of $f(x)$ over F_3 has degree 1 or 2.

Now $x^9 - x = x(x^8 - 1)$

$= x(x^4 - 1)\ (x^4 + 1)$

$= x(x - 1)\ (x + 1)\ (x^2 + 1)\ (x^2 - x - 1)\ (x^2 + x - 1)$

Note, $x^2 + 1$, $x^2 - x - 1$, $x^2 + x - 1$ are irreducible over F_3 as none of 0, 1, 2 are zeros of these factors.

Let $p(x) = x^2 + 1$. Let α be a zero of $p(x)$.

Then $\{1, \alpha\}$ is a basis of $F_9 = F_3(\alpha)$ over F_3.

So, $F_9 = \{a + b\alpha \mid a, b \in F_3\}$

$= \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

Let $u = \alpha + 1$. Then $u^2 = 2\alpha$, $u^4 = -1$, $u^8 = 1$. So, $o(u) = 8 \Rightarrow F_9^* = < u >$.

Therefore, $F_9 = \{0, 1 = u^8, 2 = u^4, \alpha = u^6, \alpha + 1 = u, \alpha + 2 = u^7, 2\alpha = u^2, 2\alpha + 1 = u^3, 2\alpha + 2 = u^5\}$

Now multiplication is defined by element u^i in F_9. We wish to define addition in F_9 with the help of u^i.

If $u^n + 1 \neq 0$, let $u^n + 1 = u^{z(n)}$.

Define $u^a + u^b = u^{z(a-b)+b}$ if $u^{a-b} + 1 \neq 0$ where $a \geq b$

$= 0$ if $u^{a-b} + 1 = 0$

Let's find

$u^7 + u^1$

Now $u^6 + 1 = \alpha + 1 = u^1 \neq 0$. So, $\mathbf{z}(6) = 1$. Therefore, $u^7 + u^1 = u^{\mathbf{Z}(6)+1} = u^2$

Also, $u^6 + u^2 = 0$ as $u^4 + 1 = -1 + 1 = 0$. In this way addition is defined in terms of u^i.

Let $a = u^i$. Then write $\log a = i$. If $b = u^j$, then $ab = u^{i \oplus j}$, where $\oplus$ denotes the addition modulo 9.

So, $\log ab = i \oplus j = \log a \oplus \log b$.

Such a logarithm is known as *Zech logarithm.*

Ruler and Compass Constructions

The word "ruler" means straight edge. Greeks used only two instruments, the ruler and the compass. They could perform many geometrical constructions with these. However, some of the constructions which they thought were constructible but could not perform were : Duplication of the cube, Trisection of the angle, Squaring the circle. They found these constructions very difficult. Indeed, we shall prove in this section that these constructions are impossible.

Let P_0 be a subset of $\mathbf{R}^2$ having at least two points with integer co-ordinates. We say a point in $\mathbf{R}^2$ is *constructible at one step from* P_0 if (*i*) it is the intersection of two lines of P_0 (By a line of P_0 we mean the line joining two points of P_0).

or (*ii*) it is the intersection of two circles of P_0 (By a circle of P_0 we mean a circle with centre from P_0 and passing through a point of P_0)

or (*iii*) it is the intersection of a line and a circle of P_0.

A point $r \in \mathbf{R}^2$ is said to be constructible from P_0 if $\exists$ a finite sequence of points $r_1, r_2, ..., r_n = r$ s.t., each r_i is constructible at one step from $P_0 \cup \{r_1, ..., r_{i-1}\}$. In fact, *this is called ruler and compass construction*. For example, let $P_0 = \{p_1, p_2\}$ be a set of two points in $\mathbf{R}^2$. Let l be the line joining two points p_1 and p_2. Let c_1 be the circle with centre p_1 and passing through p_2 and c_2 be the circle with centre p_2 and passing through p_1. Then l is a line of P_0 and c_1, c_2 are circles of P_0. Let r_1 and r_2 be the points of intersection of c_1 and c_2 and c_3 be the intersection of l and line r_1r_2. Then r_3, the middle point of line joining p_1, p_2 is constructible from P_0.

Remark: Since P_0 has at least 2 points with integer co-ordinates, (0, 0) and (1, 0) can be taken as two points in P_0. From now onward instead of writing constructible from P_0 we shall write it as constructible. Similarly line or circle of P_0, we shall write as constructible line or circle.

Problem 26: *Show that* (a, b) *is constructible for all integers a and b.*

Solution: Since (0, 0) and (1, 0) are constructible, line x-axis is also constructible. Also circle with centre (1, 0) and passing through (0, 0) is constructible and meets x-axis at (2, 0). So (2, 0) is constructible. In this way $(a, 0)$ is constructible for all integers a. Circles $(x - 1)^2 + y^2 = 4$ and $(x + 1)^2 + y^2 = 4$ are constructible as these have centres (1, 0), (–1, 0) and pass through (–1, 0) (1, 0) respectively. $\therefore$ Their intersection $(0, \sqrt{3})$ is also constructible and so line y-axis is constructible. So, circle $x^2 + y^2 = 1$ meets y-axis at (0, 1). Thus (0, 1) is constructible. In this way $(0, b)$ is constructible for all integers b. Line $y = x$ is constructible being the intersection of circles $(x - 1)^2 + y^2 = 1$ and $x^2 + (y - 1)^2 = 1$. Also (a, a) is constructible being the intersection of line $y = x$ and circle $(x - a)^2 + y^2 = a^2$ for all integers a.

Thus line $x = a$ joining $(a, 0)$ and (a, a) is constructible. Also $y = b$ joining $(0, b)$ and (b, b) is constructible.

$\therefore$ (a, b) = Intersection of lines $x = a$ and $y = b$ is constructible for all integers a and b.

Definition: *A* real number c is said to be constructible if the point $(c, 0)$ is constructible.

Problem 27: *If real number a is constructible, show that* $(a, 0)$, (a, a) *and* $(0, a)$ *are also constructible.*

Solution: $(a, 0)$ is constructible follows from the definition. Consider the circle $C : (x - a)^2 + y^2 = a^2$. It is constructible as its centre is $(a, 0)$ and passes through (0, 0) which are constructible points. Also line L $y = x$ joining (0, 0) and (1, 1) is constructible.

$\therefore$ $(a, a) = L \cap C$ is constructible.

Line $y = –x$ passing through (0, 0), (1, –1) and circle $x^2 + y^2 = 2a^2$ with centre (0, 0) and passing through (a, a) are constructible.

$\therefore$ $(–a, a)$, their point of intersection is constructible. So, line $y = a$ joining (a, a) and $(–a, a)$ is constructible. $\therefore$ $(a, 0) = (y = a) \cap (x = 0)$ is constructible.

Problem 28: *If real numbers a and b are constructible, show that* (a, b) *is constructible.*

Solution: By above theorem $(a, 0)$ and (a, a) are constructible $\Rightarrow$ line $x = a$ joining them is constructible. Also $(0, b)$ and (b, b) are constructible. Thus line $y = b$ joining them is constructible.

So, $(a, b) = (x = a) \cap (y = b)$ is constructible.

Problem 29: *If a, b are constructible numbers, show that* $a \pm b$, ab, ab^{-1} $(b \neq 0)$ *are constructible.*

Solution: Circle $(x - a)^2 + y^2 = b^2$ with centre $(a, 0)$ are passing through (a, b) is constructible. Also $y = 0$ is constructible $\Rightarrow (a \pm b, 0)$, the intersection of above line and circle are constructible.

$\Rightarrow a \pm b$ are constructible numbers.

Since b, 1 are constructible numbers, so is $b - 1$. Thus $(a, b - 1)$ and $(0, b)$ are constructible points (Problem 22). So, the line $ay = -x + ab$ joining them is constructible.

$\therefore$ $(ab, 0) = (y = 0) \cap (ay = -x + ab)$ is constructible.

$\therefore$ ab is constructible number. Also line joining $(0, a)$ and $(a, a(1 - b))$, $bx = a - y$ is constructible.

$\therefore$ $(a/b, 0) = (y = 0) \cap (bx = a - y)$ is constructible.

$\therefore$ a/b is constructible number.

It follows from above problem that the set of rational numbers forms a set of constructible numbers. Also, the set of constructible numbers forms a subfield of real numbers that contains the rationals.

Remark: Since rational numbers are constructible numbers, (a, b) is constructible point for all rationals a and b. So, we can take

P_0 $\{(a, b) | a = \text{rational}, b = \text{rational}\}$.

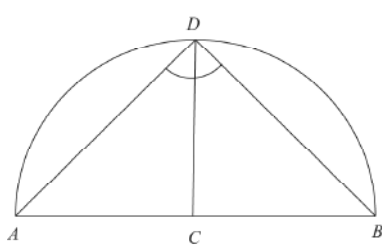
Problem 30: *If* $a > 0$ *is constructible, show that* $\sqrt{a}$ *is constructible.*

Solution: Since a is constructible, so is $\dfrac{1+a}{2}$.

$\therefore$ $\left(\dfrac{1+a}{2}, 0\right)$ is a constructible point. Then the circle $\left(x - \dfrac{1+a}{2}\right)^2 + y^2 = \left(\dfrac{1+a}{2}\right)^2$ passes through $(0, 0)$ and has centre $\left(\dfrac{1+a}{2}, 0\right)$.

$\therefore$ It is constructible circle.

Consider its intersection with the constructible line $x = 1$. The intersection point is $(1, \sqrt{a})$. So $(1, \sqrt{a})$ is constructible. Consider the circle $(x - 1)^2 + (y - \sqrt{a})^2 = a + 1$ with constructible centre $(1, \sqrt{a})$ and passing through $(0, 0)$. So, it is constructible. Its intersection with $x = 0$, gives $(0, 2\sqrt{a})$ as a constructible point. Then the circle with centre $(0, 0)$ and passing through $(0, 2\sqrt{a})$ will meet x-axis at $(2\sqrt{a}, 0)$. So $(2\sqrt{a}, 0)$ is a constructible point, *i.e.*, $2\sqrt{a}$ is a constructible number. Hence $\sqrt{a}$ is a constructible number.



Aliter: Consider a semicircle with diameter $AB = a + 1$. Let C be a point on AB s.t., $AC = a$. Draw a perpendicular from C and let it meet the semicircle at D. Join A and D., and B and D. The triangles ADC and DBC are similar. The

angle ADB is right angle.

So. $$\frac{DC}{AC} = \frac{AB}{DC} \Rightarrow (DC)^2 = (AC)(CB)$$

Since $$AC = a,\ CB = 1,\ (DC)^2 = a$$

Hence $\sqrt{a} = DC$ is constructible .

Problem 31: *If P is a constructible point, not on a constructible line l, then show that line through P perpendicular to l is constructible.*

Solution: Let Q be a constructible point on l. Let C be the constructible circle with centre P and passing through Q. If C meets l at Q only, then l is tangent at Q to C and so $PQ \perp l$, is constructible. If C meets l at Q and R, then circles with centres Q and R and passing through R and Q respectively, are constructible. The line of intersection of these circles is also constructible. But this line passes through P and perpendicular to l.

Theorem 69: *The real number c is constructible if and only if* $\exists$ *real numbers* $v_1, ..., v_n$ s.t., $\mathbf{Q} = F_0 \subseteq F_1 = \mathbf{Q}(v_1) \subseteq F_2 = F_1(v_2) \subseteq ... \subseteq F_n = F_{n-1}(v_n) = \mathbf{Q}(v_1, ..., v_n)$, $v_1^2 \in \mathbf{Q}$, $v_i^2 \in \mathbf{Q}(v_1, ..., v_{i-1})$ *for all i and* $c \in F_n$.

Proof: Suppose c is constructible number then $(c, 0)$ is a constructible point. Also $\exists$ a finite sequence of points $r_1, ..., r_n = (c, 0)$ s.t., each r_i is constructible at one step from $P_0 \cup \{r_1, ..., r_{i-1}\}$. Consider r_1. Then r_1 is constructible at one step from P_0. r_1 is the intersection of two lines or two circles or a line and a circle constructible from P_0. Suppose r_1 is the intersection of line L given by $dx + ey + f = 0$ where $d, e, f \in \mathbf{Q}$ and circle given by $x^2 + y^2 + ax + by + c = 0$ where $a, b, c \in \mathbf{Q}$. It can be proved that $r_1 = (x_1, y_1)$ where $x_1, y_1 \in \mathbf{Q}(v_1)$ where $v_1 \in \mathbf{Q}$, $u_1 \geq 0$. Let $u_1 = v_1^2$. Then $v_1^2 \in \mathbf{Q}$ and $x_1, y_1 \in \mathbf{Q}(v_1)$. In this way, we shall get

$$\mathbf{Q} \subset \mathbf{Q}(v_1) \subset \mathbf{Q}(v_1, v_2) \subset ... \subset \mathbf{Q}(v_1, ..., v_n)$$

s.t. $$v_i^2 \in \mathbf{Q}(v_1, ..., v_{i-1}) \text{ for all } i$$

and $r_n = (c, 0)$ where $c \in \mathbf{Q}(v_1, ..., v_n)$

Conversely, let L be the field of all constructible numbers. We saw just before the theorem that $\mathbf{Q} \subseteq L$. We show that $F_i \subseteq L$ for all i. It is true for $i = 0$ as $F_0 = \mathbf{Q}$. Suppose $F_r \subseteq L$. We show $F_{r+1} \subseteq L$. Now $F_{r+1} = F_r(v_{r+1})$. If $F_{r+1} = F_r$, then $F_{r+1} \subseteq L$.

Let $F_{r+1} \neq F_r$. Since $v_{r+1}^2 \in \mathbf{Q}(v_1, ..., v_r) = F_r \subseteq L$. v_{r+1}^2 is constructible. Thus by above problem $\sqrt{v_{r+1}^2} = v_{r+1}$ is constructible and so $v_{r+1} \in L$.

$\therefore\ F_r(v_{r+1}) = F_{r+1} \subseteq L$.

So our assertion is true for $r + 1$. By induction $F_i \subseteq L$ for all $i \geq 0$. In particular $F_n \subseteq L$ $\Rightarrow c \in L \Rightarrow c$ is constructible.

Cor. 1: If c is a constructible number, then c lies in some extension of the rationals of degree a power of 2.

Proof: Since $v_i^2 \in \mathbf{Q}(v_1, ..., v_{i-1}) = F_{i-1}$ by above theorem

v_i satisfies $x^2 - v_i^2 \in F_{i-1}[x]$ for all i

Thus $[F_i : F_{i-1}] = [F_{i-1}(v_i) : F_{i-1}]$

$= \deg Irr\ (F_{i-1}, v_i) \leq 2$

$\therefore$ $[F_n : \mathbf{Q}] = [F_n : F_{n-1}] ... [F_i : F_{i-1}] ... [F_1 : \mathbf{Q}]$

$= 2^r,\ r \leq n.$

Cor. 2: If the real number c satisfies an irreducible polynomial over $\mathbf{Q}$ of degree k and k is not a power of 2, then c is not constructible.

Proof: We are given $[\mathbf{Q}(c) : \mathbf{Q}] = k$. Let c be constructible. Now $\mathbf{Q} \subseteq \mathbf{Q}(c) \subseteq F_n$

and $[F_n : \mathbf{Q}] = [F_n : \mathbf{Q}(c)][\mathbf{Q}(c) : \mathbf{Q}]$

By Cor. 1, $[F_n : \mathbf{Q}] = 2^r$

$\therefore$ $[\mathbf{Q}(c) : \mathbf{Q}]$ = power of 2

$\therefore$ k = power of 2, a contradiction.

$\therefore$ c is not constructible.

By above results we notice that if c is a constructible number then $F = \mathbf{Q}(c)$ is an extension of $\mathbf{Q}$ such that $[F:\mathbf{Q}]$ is a power of 2. Since c is constructible, $F = \mathbf{Q}(c)$ is a subfield of all constructible numbers.

However, the converse of above result need not be true. For example, there is a real root c of the irreducible polynomial $x^4 - 4x + 2$ which is not constructible but $[\mathbf{Q}(c) : \mathbf{Q}] = 2^2$.

Again, a partial converse to the above result can be proved as

Theorem 70: *Let E be a subfield of the real numbers containing a field F of constructible numbers such that E/F is normal and $[E:F] = 2^n$. Then every element in E is constructible.*

Proof: We prove the result by induction on n. Let $n = 1$. Then $[E : F] = 2$. Let $c \in E$ such that $c \notin F$. Then $F \subseteq F(c) \subseteq E$. Since $c \notin F$ and $[E : F] = 2$, $E = F(c)$.

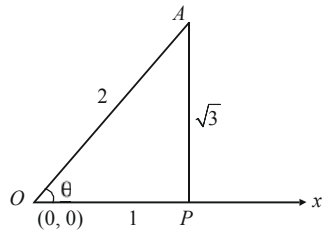
Therefore, $[F(c) : F] = [E : F] = 2 = \deg \text{Irr}(F, c)$. Let $p(x) = \text{Irr}(F, c)$. Then, $p(x) \in F[x]$ and $p(x) = x^2 - (c + d)x + cd$. So, $c + d \in F$, $cd \in F$ implies $c(c + d) \in F$. So, $c^2 + cd \in F$ and $cd \in F$ implies $c^2 \in F$. We can take $c > 0$. Since c^2 is constructible, so, is $c = \sqrt{c^2}$. Therefore, $E = F(c)$ is constructible. The result is true for $n = 1$. Assume that the result is true for all positive integers less than $n (n > 1)$. Let G be the group of F-automorphisms of E. Then, $o(G) = [E : F] = 2^n$. Let H be a subgroup of G such that $o(H) = 2^{n-1}$. Let H^* denote the fixed field of H, i.e., $H^* = \{x \in E \mid \sigma(x)\} = x \ \forall\ \sigma \in H\}$. Then by fundamental theorem of Galois theory (Theorem 48 on page 735), $[G : H] = [H^*: F] = 2$. So, H^* is a normal extension of F. By above, every element in H^* is constructible. Since E/F is normal and $F \subseteq H^* \subseteq E$, E/H^* is normal and $[E : H^*] = o(H) = 2^{n-1}$. So, by induction hypothesis every element in E is constructible. By induction, the result then follows:

Definition: An angle is said to be constructible if its vertex and arms are constructible.

Problem 32: *Show that* 60° *is constructible.*

Solution: Take the vertex at $O(0, 0)$ and take one arm as the x-axis.

Since 3 is constructible, $\sqrt{3}$ will be constructible and, therefore, $A(1, \sqrt{3})$ is constructible. Join O and A and we get line OA as constructible line. Then $\theta = \angle XOA = 60^\circ$ as



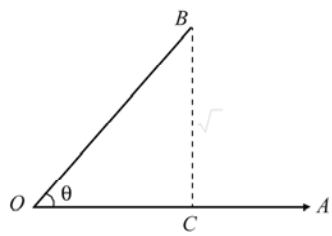
A is constructible, x-axis is constructible, therefore, line AP, (through A and $\perp$ to x-axis) is constructible.

Now $OP = 1,\ PA = \sqrt{3},\ OA = \sqrt{3+1} = 2$

$\therefore$ $\cos\theta = \frac{1}{2}$ or that $\theta = 60^\circ$ is constructible.

Problem 33: *Show that an angle θ is constructible if and only if sin θ is constructible.*

Solution: Let angle θ be constructible. Then OA and OB are constructible. Draw perpendicular from B on OA. Let it meet OA in C. Then OC is constructible. Also BC and OB are constructible imply $\frac{BC}{OB} = \sin\theta$ is constructible.



Conversly, let $\sin\theta = \frac{BC}{OB}$ be constructible. Then OC and OB are constructible imply angle θ is constructible.
(Similarly, θ is constructible if and only if cos θ is constructible).

Problem 34: *Let angles θ and ϕ be constructible. Show that $m\theta + n\phi$ is also constructible for all integers m and n.*

Solution: Since the set of constructible numbers form a subfield of real numbers. $m\theta$ and $n\phi$ are constructible numbers. So, $m\theta + n\phi$ is also constructible.

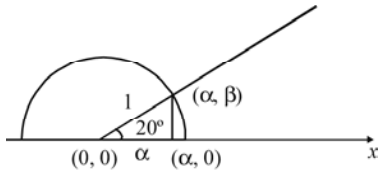
Problem 35: *Let $\theta = \frac{2\pi}{m}$ and $\phi = \frac{2\pi}{n}$ be constructible numbers where m and n are coprime. Show that $\alpha = \frac{2\pi}{nx}$ is also constructible .*

Solution: Since m and n are coprime integers, there exist integers x and y such that $mx + ny = 1$. So, $\alpha = m\alpha x + n\alpha y = \frac{2\pi}{n}x + \frac{2\pi}{m}y = \theta x + \theta y$.

By above problem, α is also constructible.

Problem 36: *Show that it is impossible to trisect* 60° *by ruler and compass.*

Solution: Suppose angle 60° can be trisected by ruler and compass. Then (α, β) is constructible where (α, β) is the point of intersection of constructible circle with centre (0, 0) and passing through (1, 0) and arm of angle 20° which is constructible. So $(\alpha, 0)$ the point of intersection of x-axis and perpendicular from (α, β) is also constructible. So, $\alpha = \cos 20^\circ$ is constructible.



Now $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

Put $\theta = 20°$, to get

$$\frac{1}{2} = 4\cos^3 20° - 3\cos 20° = 4\alpha^3 - 3\alpha$$

$\therefore$ α satisfies $f(x) = 8x^3 - 6x - 1 \in \mathbf{Q}[x]$.

By Eisenstein criterion $f(x + 2)$ is irreducible over $\mathbf{Q}$ (by taking $p = 3$) and so, $f(x)$ is irreducible over $\mathbf{Q}$.

$\therefore$ α satisfies an irreducible polynomial over $\mathbf{Q}$ of degree 3 which is not a power of 2. By Cor. 2 above, α is not constructible, a contradiction.

Hence, it is impossible to trisect 60° by ruler and compass.

Problem 37: *Show that it is impossible to duplicate the cube by ruler and compass.*

Solution: Suppose cube is of unit length. Volume of this cube is 1. If we could construct a cube of volume 2, then we could construct a point $(\alpha, 0)$, a vertex of cube s.t., $\alpha^3 = 2$, where one side of the cube is the join of points (0, 0) and $(\alpha, 0)$. But $\alpha^3 = 2 \Rightarrow \alpha$ satisfies $x^3 - 2 \in \mathbf{Q}[x]$.

Let $f(x) = x^3 - 2$. We have seen before that $f(x)$ is irreducible over $\mathbf{Q}$. Since degree of $f(x)$ is not a power of 2, α is not constructible. So, it is impossible to duplicate cube by ruler and compass.

Problem 38: *Show that regular pentagon is constructible.*

Solution: It would be possible to construct a pentagon if we can construct $\alpha = 2\cos\frac{2\pi}{5} = 2\cos 72° = 2\sin 18°$.

Since $\sin 18° = \frac{-1+\sqrt{5}}{4}$ which is constructible, (See Problem 29) we find it is possible to construct a regular pentagon.

Construction of the regular *n*-gon

In the following few results, we discuss the construction of the regular n-sided polygon, $n \geq 3$ (also called the regular n-gon)

Problem 39: *Use the fact that* $8\cos^3\frac{2\pi}{7} + 4\cos^2\frac{2\pi}{7} - 4\cos\frac{2\pi}{7} - 1 = 0$ *to show that a regular seven sided polygon is not constructible.*

Solution: We first show that $8\cos^3\frac{2\pi}{7} + 4\cos^2\frac{2\pi}{7} - 4\cos\frac{2\pi}{7} - 1 = 0$

Let $\theta = \frac{2\pi}{7}$

Now $2\cos\theta = \cos i\theta + e^{-i\theta}$

Also the roots of $y^7 = 1$ are given by $e^{ri\theta}$, $0 \le r \le 6$.

For $r = 1$, $e^{i\theta}$ is a root of $y^6 + y^5 + y^4 + y^3 + y^2 + y + 1 = 0$

Therefore, $(\cos 6\theta + i \sin 6\theta) + (\cos 5\theta + i \sin 5\theta) + (\cos 4\theta + i \sin 4\theta) +$
$(\cos 3\theta + i \sin 3\theta) + (\cos 2\theta + i \sin 2\theta) + (\cos\theta + i \sin\theta) + 1 = 0.$

Now $\cos 6\theta = \cos\frac{12\pi}{7} = \cos\left(2\pi - \frac{2\pi}{7}\right) = \cos\frac{2\pi}{7} = \cos\theta$

$\cos 5\theta = \cos\frac{10\pi}{7} = \cos\left(2\pi - \frac{4\pi}{7}\right) = \cos\frac{4\pi}{7} = \cos 2\theta$

$\cos 4\theta = \cos\frac{8\pi}{7} = \cos\left(2\pi - \frac{6\pi}{7}\right) = \cos\frac{6\pi}{7} = \cos 3\theta$

Similarly, $\sin 6\theta = -\sin\theta$, $\sin 5\theta = -\sin 2\theta$, $\sin 4\theta = -\sin 3\theta$

So, $2\cos 3\theta + 2\cos 2\theta + \cos\theta + 1 = 0$

or $2(4\cos^3\theta - 3\cos\theta) + 2(2\cos^2\theta - 1) + 2\cos\theta + 1 = 0$

or $3\cos^3\theta + 4\cos^2\theta - 4\cos\theta - 1 = 0$

Therefore, $2\cos\theta$ satisfies $f(x) = x^3 + x^2 - 2x - 1$ over $\mathbf{Q}$ which is irreducible over $\mathbf{Q}$.

So, $[\mathbf{Q}(2\cos\theta) : \mathbf{Q}] = \deg f(x) = 3 \neq 2^k$.

Therefore, $2\cos\theta$ is not constructible

or $\cos\theta$ is not constructible

or $\theta = \frac{2\pi}{7}$ is not constructible.

Hence, regular seven sided polygon (septagon) is not constructible.

Problem 40: *Suppose that a regular p-gon is constructible, where p is a prime. Show that p is a Fermat prime (A prime number of the form* $2^{2^n} + 1$ *is called a Fermat prime).*

Solution: Let $\alpha = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ be a p-th root of unity. Suppose a regular p-gon is constructible. Then $\frac{2\pi}{p}$ is constructible and so $\cos\frac{2\pi}{p}$ and $\sin\frac{2\pi}{p}$ are constructible numbers.

So, $\left[\mathbf{Q}\left(2\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p}\right) : \mathbf{Q}\right] = 2^r$ for some integer $s \ge 0$.

Therefore, $\left[\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p},\ i\right):\mathbf{Q}\right]=2^{s+1}$

as $\left[\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p},\ i\right):\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p}\right)\right]=2=\deg(x^2+1)$

Let $F=\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p}\right).$

Then $[F(i):F]\ =\deg Irr\ (F,i)$

$=\deg x^2+1=2 \quad F\subseteq\mathbf{R}$

Also, $\mathbf{Q}(\alpha)\subseteq\ \mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p},i\right)$

So, $\mathbf{Q}\subseteq\mathbf{Q}(\alpha)\subseteq\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p},\ i\right)$ implies $[\mathbf{Q}(\alpha):\mathbf{Q}]=2^r$,

for some integer $r\le s+1$.

Since α is a root of $x^{p-1}+x^{p-2}+\ldots+x+1$, which is irreducible over $\mathbf{Q}$, $[\mathbf{Q}(\alpha):\mathbf{Q}]=p-1$.

So, $p-1=2^r$ implies $p=2^r+1$.

By Exercise 10 on page 43, r is a power of 2. This proves the result.

(**Note:** By above problem, regular 7-gon is not constructible.)

Problem 41: *If the regular n-gon is constructible and n = qr, show that the regular q-gon is also constructible.*

Solution: Since the regular n-gon is constructible, $\frac{2\pi}{n}$ is constructible.

So, $\frac{2\pi}{qr}$ is constructible.

Therefore, $r\frac{2\pi}{qr}=\frac{2\pi}{q}$ is constructible, (as product of two constructible numbers is constructible).

Hence, the regular q-gon is constructible.

Problem 42: *If the regular n-gon is constructible, show that* $n=2^k p_1p_2\ldots p_r$, *where* p_i*'s are distinct Fermat's prime.*

Solution: Let $n=2^k.m$, m is an odd integer.

If $m=1$, then we have nothing to prove.

Let $m>1$ be an odd integer.

Suppose p^2 divides m for some odd prime p.

Then p^2 divides m. By Problem 41, since regular n-gon is constructible, the regular p^2-gon is also constructible. So, $\frac{2\pi}{p^2}$ is constructible.

Therefore, $\cos\frac{2\pi}{p^2}$ and $\sin\frac{2\pi}{p^2}$ are constructible numbers.

Let $\alpha = \cos\frac{2\pi}{p^2} + i\sin\frac{2\pi}{p^2}$

Then $\left[\mathbf{Q}\left(\cos\frac{2\pi}{p^2}, \sin\frac{2\pi}{p^2}\right) : \mathbf{Q}\right] = 2^s$ for some integer $s \geq 0$

So, $\left[\mathbf{Q}\left(\cos\frac{2\pi}{p^2}, \sin\frac{2\pi}{p^2}, i\right) : \mathbf{Q}\right] = 2^{s+1}$ (See Problem 40)

Also $\mathbf{Q}(\alpha) \subseteq \mathbf{Q}\left(\cos\frac{2\pi}{p^2}, \sin\frac{2\pi}{p^2}, i\right)$ implies $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^r$ for some integer $r \geq 0$.

But $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg \text{Irr}(\mathbf{Q}, \alpha) = \deg f(x) = p(p-1)$ by exercises 5 and 10.

So, $p(p-1) = 2^r$, a contradiction as p is an odd prime.

Therefore, $n = 2^k p_1 p_2 \ldots p_r$ where p_i's are distinct primes. By Problem 41, the regular p_i-gon is constructible for all i. By Problem 40, p_i's are Fermat primes. This proves the result.

(**Note**: By above problem the regular 14-gon is not constructible as 7 is not a Fermat prime.)

(The converse of the above problem is also true. See problem 43).

Theorem 71: *Let* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, *where* p_i*'s are distinct primes and* α_i*'s are positive integers. Show that the regular n-gon is constructible if and only if the regular* $p_i^{\alpha_i}$ *-gon is constructible for all i.*

Proof: Suppose the regular n-gon is constructible.

Then $\frac{2\pi}{n}$ is constructible.

So, $\frac{n}{p_i^{\alpha_i}}\frac{2\pi}{n}$ is also constructible.

This means that $\frac{2\pi}{p_i^{\alpha_i}}$ is constructible for all i. So, the regular $p_i^{\alpha_i}$ -gon is constructible for all i.

Conversely, let $p_i^{\alpha_i}$ -gon be constructible for all i. Then the angle $\frac{2\pi}{p_i^{\alpha_i}}$ is constructible for all i.

(By problem 35 on page 764) the angle $\frac{2\pi}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}} = \frac{2\pi}{n}$ is constructible as p_i's are distinct primes. So, the regular n-gon is constructible.

Theorem 72: *Show that the regular n-gon is constructible if and only if* $\phi(n) = 2^k$ *for some integer* $k \geq 0$.

Proof: Let $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Then α is a primitive nth root of unity (i.e., $\alpha^n = 1$ and $\alpha^m = 1$ for some positive integer m implies $m \geq n$).

Suppose the regular n-gon is constructible.

Then $\frac{2\pi}{n}$ is constructible. so, $\beta = \cos\frac{2\pi}{n}$ is constructible.

Now $\alpha + \alpha^{-1} = \alpha + \bar{\alpha} = 2\cos\frac{2\pi}{n} \in \mathbf{Q}(\alpha)$

Clearly, $\mathbf{Q} \subseteq \mathbf{Q}(\beta) \subseteq \mathbf{Q}(\alpha)$.

Also $\left(\alpha - \cos\frac{2\pi}{n}\right)^2 = \alpha^2 + \cos^2\frac{2\pi}{n} - 2\cos\frac{2\pi}{n}\alpha.$

$$= -\sin^2\frac{2\pi}{n}$$

So, $\alpha^2 - 2\cos\frac{2\pi}{n}\alpha + 1 = 0$ implies α satisfies

$$f(x) = x^2 - \left(2\cos\frac{2\pi}{n}\right)x + 1 \in \mathbf{Q}(\beta)[x]$$

i.e., $f(\alpha) = 0$

Therefore, $[\mathbf{Q}(\alpha) : \mathbf{Q}(\beta)] = [F(\alpha) : F] = \deg \operatorname{lrr}(F, \alpha) \leq 2$

where $F = \mathbf{Q}(\beta)$ and $F(\alpha) = \mathbf{Q}(\alpha)$

Let $\Phi_n(x)$ be the nth cyclotomic polynomial.

Then $\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ (i,n)=1}} (x - \alpha^i)$

So, $\deg \Phi_n(x) = \phi(n)$

Also $\Phi_n(x)$ is irreducible over $\mathbf{Q}$ (See Theorem 56, page 747).

Therefore $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg \operatorname{Irr}(\mathbf{Q}, \alpha)$

$= \deg \Phi_n(x)$

$= \phi(n)$

Since β is constructible, $[\mathbf{Q}(\beta) : \mathbf{Q}] = 2^k$.

So, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^r$ implies $\phi(n) = 2^r$.

Conversely, let $\phi(n) = 2^k$.

Then $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \phi(n) = 2^k$.

So, $[\mathbf{Q}(\beta) : \mathbf{Q}] = 2^r \quad r \leq k$

Now $\mathbf{Q}(\alpha)/\mathbf{Q}$ is a Galois extension of degree 2^k and $\mathbf{Q}(\alpha)/\mathbf{Q}$ is a minimial splitting field of $f(x) = x^n - 1$ over $\mathbf{Q}$. The roots of $f(x)$ are distinct as $f'(x) = nx^{n-1} \neq 0$. If σ is a $\mathbf{Q}$-automorphism of $\mathbf{Q}(\alpha)$, then σ is completely known by its effect on α. If $\sigma(\alpha) = \sigma^j$, $i \leq j \leq n$, denote σ by σ_y. If $G = G(\mathbf{Q}(\alpha)/\mathbf{Q})$ is the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}$ then G is abelian as $\sigma_i\sigma_j(\alpha) = \sigma_i(\alpha^j) = \alpha^{ij} = \sigma_j\sigma_i(\alpha)$.

Since, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois, so is $\mathbf{Q}(\alpha)/\mathbf{Q}(\beta)$. Let H be the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}(\beta)$ i.e., H is the group of $\mathbf{Q}(\beta)$-automorphisms of $\mathbf{Q}(\alpha)$. So, H is a subgroup of G. Since G is abelian H is normal in G. Therefore, the fixed field $\mathbf{Q}(\beta)$ of H is normal extension of $\mathbf{Q}$ by the fundamental theorem of Galois theory. Since $\mathbf{Q}(\beta) \subseteq \mathbf{R}$ and $\mathbf{Q}(\beta)/\mathbf{Q}$ is normal such that $[\mathbf{Q}(\beta) : \mathbf{Q}] = 2^r$, β is constructible. So, $\frac{2\pi}{n}$ is constructible implies $\frac{2\pi}{n}$ is constructible. Therefore, the regular n-gon is constructible.

Problem 43: *Let $n = 2^k p_1 p_2 \ldots p_r$ where p_i's are distinct Fermat's primes and $k \geq 0$ is an integer. Show that regular n-gon is constructible.* [*This is the converse of problem 42*]

Solution: Let $n = 2^k p_1 p_2 \ldots p_r$ where $p_i = 2^{2^{n_i}} + 1$ is a prime.

Then
$$\begin{aligned}\phi(n) &= 2^{k-1}\,\phi(p_1)\phi(p_2)\ldots\phi(p_r) \quad \text{if } k > 0\\ &= 2^{k-1}(p_1 - 1)(p_2 - 1)\ldots(p_r - 1)\\ &= 2^{k-1}\,2^{2^{n_1}}\,2^{2^{n_2}}\ldots 2^{2^{n_r}} = 2^m\end{aligned}$$

Also,
$$\begin{aligned}\phi(n) &= \phi(p_1)\phi(p_2)\ldots\phi(p_r) \quad \text{if } k = 0\\ &= (p_1 - 1)(p_2 - 1)\ldots(p_r - 1)\\ &= 2^{2^{n_1}}\,2^{2^{n_2}}\ldots 2^{2^{n_r}} = 2^u\end{aligned}$$

By above Theorem, the regular n-gon is constructible.

Exercises

1. Show that it is not possible to construct a square with area equal to the area of a circle of radius 1.
2. Prove that it is possible to trisect 72°.
3. Prove that the regular hexagon is constructible.
4. Prove that the regular 9-gon is not constructible.
5. Show that $\alpha = \cos\left(\frac{2\pi}{p^2}\right) + i\sin\left(\frac{2\pi}{p^2}\right)$ is a root of $f(x) = 1 + x^p + x^{2p} + \ldots + x^{(p-1)p}$
6. Prove that the regular 15-gon is constructible.
7. Prove that $\cos 2\theta$ is constructible if and only if $\cos\theta$ is constructible.

8. Prove that sin θ is constructible if and only if cos θ is constructible.

9. Use the fact that $4\cos^2\frac{2\pi}{5}+2\cos\frac{2\pi}{5}-1=0$ to show that a regular pentagon is constructible. (Hint: cos4θ = cosθ, cos 3θ = cos2θ).

10. Show that $f(x) = 1 + x^p + x^{2p} + \ldots + x^{(p-1)p}$ is irreducible over **Q**. (Take $x^p = y$).

11. Show that 17-gon is constructible.

12. Can the cube be quadrupled?

A Quick Look at what's been done

- The intersection P of all subfields of a field F is the smallest subfield of F and is called the **prime subfield** of F and either $P \cong \mathbf{Q}$or $P \cong \mathbf{Z}/(p)$ for some prime p.
- A polynomial $f(x)$is said to be **separable** if all its roots are simple. Equivalently, a polynomial $f(x)$ is separable iff f and f' are relatively prime.
- If *char* $K = p$, then every algebraic extension of K is separable iff $K = K^p$.
- A field K is called **perfect field** if every algebraic extension of K is separable. A field of characteristic zero is perfect, so **Q**, **R**, **C** are perfect.
- An extension E of K is called **normal extension** of K if E/K is algebraic and $a \in E \Rightarrow p(x) = Irr(K, \alpha)$ splits in $E[x]$ or E. A quadratic extension is normal.
- A finite normal extension is a minimal splitting field of some polynomial and conversely.
- A field k is called **algebraically closed** if every polynomial f over k splits in k.
- If k is a field, then the following are equivalent :(i) k is algebraically closed,. (ii) Every irreducible polynomial over k has degree one,. (iii) Every algebraic extension over k is k itself.
- A minimal splitting field of a set of polynomials over k is an algebraic closure of k.
- Artin's theorem: Let G be the group of automorphisms of a field E and suppose K is the set of elements of E fixed by G. Then K is a subfield of E (called the fixed field of G) and E/K is finite iff G is finite and $[E:K] = o(G)$.
- An extension E of F is called a **Galois extension** if E/F is finite and F is the fixed field of a group of automorphisms of E.
- Let E/F be a finite extension, then E/F is a Galois extension iff it is both normal and separable.
- **The fundamental theorem of Galois theory** is stated and proved. It gives us the number of fields between F and E where E/F is Galois and also tells us which of these intermediate fields are normal extensions.
- Let E be a minimal splitting field of $f(x) = x^n - 1$ over k. The roots of $f(x)$ in E are called n^{th} roots of unity, and E is called associated *cyclotomic* field.
- $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois where α is a primitive n^{th} root of unity.
- A field of order p^m is a subfield of a field of order p^n iff m divides n.
- The last portion of the chapter discusses the construction by ruler and compass.

Index