BACHELOR OF COMPUTER APPLICATIONS (BCA)

CSB-1113 (Mathematics - I)

Block 1: Introduction to Sets Functions and Numbers

Unit 1: Sets, Relation and Function

Structure

1.1 INTRODUCTION

In this unit, we will delve into fundamental concepts related to sets and functions, which serve as the cornerstone of mathematics, particularly in the field of algebra. These concepts are the building blocks of mathematical reasoning and are pivotal in understanding more advanced mathematical ideas. We will also explore essential elements of number theory, with the primary goal of laying the groundwork for the subsequent sections of this course. Our aim is not only to equip you with the necessary knowledge but also to provide you with a glimpse of the inherent elegance and sophistication of number theory, a field where seemingly simple ideas can lead to profound and beautiful insights. With that in mind, let's embark on a step-by-step exploration of these foundational concepts.

1.2 OBJECTIVES

After the completion of this unit, a solid grasp of essential concepts in set theory and number theory will be achieved. Proficiency in explaining set operations like union, intersection, and complement, as well as the effective use of Cartesian products to represent connections between sets will be developed. Additionally, an understanding of the significance of equivalence classes in the context of equivalence relations and set partitions will be gained. Furthermore, differentiation between various types of functions, including injective, surjective, and bijective functions, and comprehension of their unique roles and characteristics will be accomplished. Lastly, a comprehensive understanding of the application of the well-ordering principle and division algorithm in integer division in number theory will be achieved. This unit will provide a solid foundation in these mathematical principles and their practical applicability in various mathematical and real-world contexts.

1.3 SETS

In the realm of abstract algebra, sets serve as the building blocks of mathematical structures. A set is a collection of objects, often denoted by curly braces { }. These objects can be anything: numbers, letters, or even other sets. Understanding sets and the operations performed on them is crucial to grasp the core concepts of abstract algebra.

For instance, the set of natural numbers, N, which is well defined and can be considered a set. On the other hand, when we think about the set of all rich people, it's not a set because there's no clear way to determine whether someone is rich or not.

Elements are the individual items within a set. For example, in the set$A = \{1, 2, 3\}$, the elements are $1, 2,$ and 3. We represent this using the symbol " $a \in S$ " which is read as "a is in S " or " $a$belongs to$S$". If something is not part of the set, we express it as " $a \notin S$ ". For instance, we say "$3 \in R$" when talking about the set of real numbers. However, we say "$-1 \notin R$" to indicate that it is not a part of the set of real numbers.

Cardinality of a Set: The cardinality of a set is the number of elements it contains. For example, the cardinality of set $A = \{1, 2, 3\}$ is 3.

A set that doesn't contain any elements in it is known as the empty set, and we represent it with the Greek letter φ (phi). For instance, the set of all natural numbers less than 1 is an empty set, represented as φ.

There are usually two ways of describing a non-empty set:

(1) Roster method, and (2) Set builder method.

(1) Roster Method: In this method, all the elements of a set are listed within curly braces. For instance, the set of positive divisors of 48 includes the numbers $1, 2, 3, 4, 6, 8, 12, 16, 24,$ and 48. So, this set can be written as $\{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$.This method follows two conventions:

Convention 1: The order in which elements are listed doesn't matter.

Convention 2: Each element is written only once; there should be no repetition of elements. For example, the set$S$ containing integers between 11 and 41 would be written as$S = \{11, 12, 13, \ldots, 41\}$. It's important not to write$S = \{11, 12, 13, \ldots, 41, 12\}$, as this violates Convention 2.

The roster method is also used when listing elements of larger sets. In such cases, we may not list all elements but just enough to provide a sense of what the set contains. For example, the set of integers between 0 and 100 can be expressed as $\{0, 1, 2, \ldots, 100\}$, and the set of all integers, Z, can be written as $\{0, +1, -2, \ldots\}$.

(2) Set Builder Method: In Set Builder Method, we begin by identifying a defining property, denoted as P that characterizes the elements of the set. This property should be unique to the elements of the set and not shared by any other objects. We then represent the set as:

$\{x \mid x \text{ has property} P\}$ or $\{x : x \text{ has property} P\}$

This can be read as 'the set of all x such that x has property P'. For example, we can express the set of all integers as:$Z = \{x \mid x \text{ is an integer}\}$.

Similarly, the set of rational numbers, Q, can be described as$Q = \{a/b \mid a, b \in \mathrm{Z}, b \neq 0\}$, the set of real numbers, R, can be represented as $R = \{x \mid x \in \mathbb{R}\}$ and for the set of complex numbers, C, we can write $C = \{a+ib \mid a, b \in \mathbb{R}\}$ (where $i = \sqrt{(-1)}$).

Subsets: Take the sets $A = \{1, 3, 4\}$ and $B = \{1, 4\}$ as an example. In this case, every element of set B is also an element of set A. When this happens, meaning that every element of set B belongs to set A, we call B a subset of A. This is written as $B \subseteq A$.It's evident that for any set A, A is certainly a subset of itself, as every element of A is also in A. So, for any set A, $A \subseteq A$. Additionally, for any set A, the empty set φ is also a subset of A, denoted as $\varphi \subseteq A$.

It's important to realize that if B is not a subset of A, it implies that there must be at least one element in B that is not part of A. In mathematical terms, we can express this as 'there exists an x in B such that x is not in A'.

We can now assert that sets, A and B, are considered equal, meaning they have exactly the same elements, if and only if A is a subset of B ($A \subseteq B$) and B is a subset of A ($B \subseteq A$).

1.3.1 Operations on Sets

Sets can be manipulated through various operations. These operations are essential for understanding abstract algebra, as they provide the foundation for more complex algebraic structures.

(i) Union: The union of A and B consists of all elements in S that belong to either A or B. We denote this union as $A \cup B$. In mathematical terms, $A \cup B$ is defined as follows:

$$A \cup B = \{x \in \mathrm{S} \mid (x \in A) \text{ or } (x \in B)\}$$

For example, if $A = \{1, 2\}$ and $B = \{4, 6, 7\}$, then their union, $A \cup B$, is $\{1, 2, 4, 6, 7\}$.

Moreover, if $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8\}$, then their union, $A \cup B$, becomes $\{1, 2, 3, 4, 6, 8\}$.

(ii) Intersection: The intersection of two sets, denoted as "$A \cap B$," results in a new set containing elements that are shared by both set A and set B. To formally define this intersection, we say that $A \cap B$ is the set of elements x in S where x belongs to A and x also belongs to B.

For example, if we have set $P = \{1, 2, 3, 4\}$ and set $Q = \{2, 4, 6, 8\}$, their intersection, $P \cap Q, is$ $\{2, 4\}$. Moreover, for any set A, the intersection of A with itself, $A \cap A$, is simply A.Now, let's imagine we have set $A = \{1, 2\}$ and set $B = \{4, 6, 7\}$. In this scenario, A and B share no common elements, so their intersection, $A \cap B$, is an empty set, denoted as φ. When two sets have an empty intersection, we say that they are disjoint, or mutually disjoint. For example, the sets $\{1, 4\}$ and $\{0, 5, 7, 14\}$ are disjoint because they do not share any common elements.

(iii) Complement: The complement of a set A, represented as A' or $\bar{A}$ or A^c, encompasses all the elements that do not belong to set A but are part of the universal set U. Mathematically, the complement A' or $\bar{A}$ or A^c can be defined as$A' = \{x \in X \mid x \notin A\}$.

For example, if we have a universal set U, which contains all the integers from 1 to 10, and we define set A as $\{2, 4, 6, 8\}$, then the complement of set A will include all the integers from 1 to 10 that are not in set A. So, A' will be $\{1, 3, 5, 7, 9, 10\}$, containing all the elements that are in U but not in A.

(iv) Difference: The difference of sets A and B, denoted as $A - B$, creates a new set comprising all the elements that are in A but not in B.

Let us consider sets $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ as an example. The set of all elements in A that are absent in B is $\{1\}$, and we refer to this set as the difference $A - B$. Similarly, the difference $B - A$ comprises the elements in B that are not part of A, which in this case is $\{4\}$.Hence, for any two subsets A and B of a set S, the difference $A - B$ can be defined as the set of elements x in S where x belongs to A but is not part of B:

$$A - B = \{ x \in S \mid x \in A \text{ and } x \notin B \}$$

1.3.2 Cartesian Product of Sets

A fascinating set that arises from combining two given sets is their Cartesian product, named after the French philosopher and mathematician René Descartes (1596 - 1650), who is also credited with inventing the Cartesian coordinate system.

In this context, let us consider two sets, A and B. Each ordered pair, denoted as (a, b), consists of the first element from set A and the second element from set B. The order in which the elements are listed in an ordered pair matter; therefore, (a, b) and (b, a) are distinct ordered pairs. Two ordered pairs, (a, b) and (c, d), are considered equal if and only if a is equal to c and b is equal to d.

The Cartesian product, written as $A \times B$, is the set of all possible ordered pairs (a, b), where a belongs to A and b belongs to B. For instance, if $A = \{1, 2, 3\}$ and $B = \{4, 6\}$, then $A \times B$ includes the pairs $\{(1, 4), (1, 6), (2, 4), (2, 6), (3, 4), and\ (3, 6)\}$.

It is to be noted that $B \times A$ is different from $A \times B$, emphasizing that the order of elements matters in ordered pairs.

Here are some key remarks about the Cartesian product:

(i) The Cartesian product $A \times B$ results in an empty set ($A \times B = \emptyset$) if and only if either A or B is an empty set.

(ii) If set A contains m elements and set B contains n elements, the Cartesian product $A \times B$ contains mn elements. The same applies to $B \times A$. However, the elements in $B \times A$ may not be the same as those in $A \times B$.

1.4 RELATIONS

In the realm of mathematics, a relation R defined on a set S represents a connection or association between the elements within S. When element 'a' in set S is related to element 'b' within the same set through this relation, we denote it as '$a\ R\ b$' or as '$(a, b) \in R$'.A relation R on a set S is essentially a subset of the Cartesian product of S with itself, denoted as $S \times S$.

For instance, if N stands for the set of natural numbers and we consider R as the relation 'is a multiple of,' then $15\ R\ 5$ holds true, but the reverse, $5\ R\ 15$, is not valid. This means that $(15, 5)$ belongs to R, while $(5, 15)$ does not. In this case, R is a subset of $N \times N$. Similarly, if we consider Q as the set of rational numbers and R as the relation 'is greater than' then,$3\ R\ 2$ because 3 is greater than 2.

Definition: A relation R defined on a set S is termed as

(i) *Reflexive* if, for every element 'a' in S, it satisfies the condition $a\ R\ a$.

(ii) *Symmetric* if, whenever $a\ R\ b$ is true, it implies that $b\ R\ a$ is also true, for all a and b in S.

(iii) *Transitive* if $a\ R\ b$ and $b\ R\ c$ together imply $a\ R\ c$, for all a, b, and c in S.

For instance, if we consider the relation R on the set of integers (Z) as $a\ R\ b$ if and only if 'a' is greater than 'b', we can analyze its properties. We find that R is not reflexive because '$a > a$' is not true for all 'a'. However, it is symmetric because if $'a > b$,' it certainly implies that '$b < a$,' making it symmetric. Furthermore, R is transitive because if '$a > b$' and '$b > c$,' it definitely implies that '$a > c$'.

Consider another example: Let S be a non-empty set. We use $P(S)$ to represent the set of all subsets of S, denoted as $P(S) = \{A \mid A \text{ is a subset of } S\}$. This set is commonly referred to as the power set of S.

Now, we define a relation R on $P(S)$ as follows:

$R = \{(A, B) \mid A, B \in P(S) \text{ and } A \text{ is a subset of } B\}$.

Let us check whether R is reflexive, symmetric, or transitive.

Reflexivity: Since A is a subset of itself $(A \subseteq A)$, it follows that R is reflexive.

Symmetry: However, it's important to note that if A is a subset of B, it does not necessarily imply that B is a subset of A. In fact, $A \subseteq B$ and $B \subseteq A$ together imply that A and B are the same set $(A = B)$. As this isn't always the case, R is not symmetric.

Transitivity: Now, if A is a subset of B and B is a subset of C, it implies that A is also a subset of C $(A \subseteq C)$, while ensuring that A, B, and C are elements of $\wp(S)$. Therefore, R is transitive.

Hence, the relation R is reflexive and transitive but not symmetric.

1.4.1 Equivalence Relation

An equivalence relation on a set A has three key properties: reflexivity, symmetry, and transitivity.An essential property of an equivalence relation on a set S is that it effectively divides S into several mutually disjoint subsets, that is, it partitions$S$ which areknown as equivalence classes. Elements within the same class are considered equivalent under the relation.

Let us say R is an equivalence relation on the set S. If 'a' is an element of S, then the set $\{b \in S \mid a\ R\ b\}$ is known as the equivalence class of 'a' in S. This set consists of elements in S that are related to 'a' and is denoted by $[a]$.

For example, let [1] represent the equivalence class of 1 in N, the set of natural numbers. It can be expressed as $[1] = \{n \mid 1\ R\ n;\ n \in N\}$. This set is effectively all those natural numbers 'n' for which '1' is related (in this case, '5 divides $1 - n$'). It turns out that $[1] = \{1, 6, 11, 16, 21, \ldots\}$. Similarly, we can define $[2], [3], [4]$, and [5] as the equivalence classes for other elements in N, and they follow a similar pattern. It is to be noted that, [1] and [6] are not separate; they are, in fact, the same set, which also applies to [2] and [7], and so on. Moreover, the entire set N can be expressed as the union of these equivalence classes, which are mutually exclusive, further illustrating the concept of partitioning the set.

1.5 FUNCTIONS

Functions are mathematical tools that describe the relationship between elements of two sets. Given two non-empty sets, A and B, a function f from A to B is essentially a rule that assigns precisely one element from B to each element of A. In this context, when we say $f(a) = b$, it signifies that 'b' is the unique element in B that the function f associates with the element 'a' in A. We formally represent this as $f: A \rightarrow B$. Functions are sometimes referred to as mappings or transformations.

In the context of a function from A to B, we designate A as the domain of the function, representing the set from which input elements are drawn. B is identified as the co-domain of the function, signifying the encompassing set to which the output elements belong. When we state that $f(a) = b$, we essentially express that 'b' is the image of 'a,' and 'a' is considered a pre-image of 'b'. The range, or image, of the function comprises all the images of elements from the domain A. Also, it's appropriate to say that the function f maps elements from A to B.

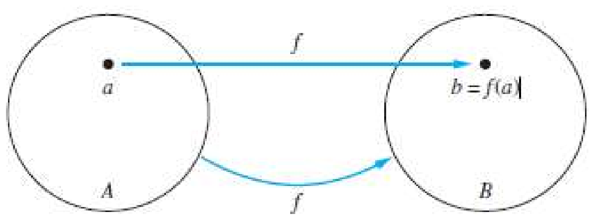

Figure 1.1: Function f from A to B

Example: We have a function $f: Z \rightarrow Z$ that assigns the square of an integer to the integer itself. In other words, for any integer x, $f(x) = x^2$. Here, the domain of f encompasses all integers, the co-domain of f includes all integers, and the range of f specifically comprises integers that are perfect squares, which are $\{0, 1, 4, 9, \ldots\}$.

It is to be noted that if we have two functions, $f1$ and $f2$, both mapping elements from set A to the real numbers R, we can define the functions $f1 + f2$ and $f1f2$ as follows for all x in A:

$$(f1 + f2)(x) = f1(x) + f2(x)$$

$$(f1f2)(x) = f1(x) * f2(x)$$

1.5.1 Image of a Subset

If we have a function f from A to B and a subset S of A, the image of S under the function f is the subset of B that comprises the images of the elements within S. We denote this image as $f(S)$, expressed as $f(S) = \{t \mid s \in S, t = f(s)\}$. Alternatively, we can use the shorthand $\{f(s) \mid s \in S\}$ to represent this set.

Please remember that the notation $f(S)$ for the image of the set S under the function f denotes a set and not the value of the function f for the set S.

For instance, consider sets $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$, along with the function $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$, and $f(e) = 1$. If we take the subset $S = \{b, c, d\}$, the image of this subset is represented as $f(S) = \{1, 4\}$.

Let us explore the concepts of one-to-one and onto functions:

(i) One-to-One Function (Injective Function): A function f is termed one-to-one, or injective, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. This means that for each pair of distinct elements a and b in the domain, the function assigns them distinct values. Mathematically, a function is considered one-to-one if, for all elements a and b in the domain, $f(a) = f(b)$ implies $a = b$.

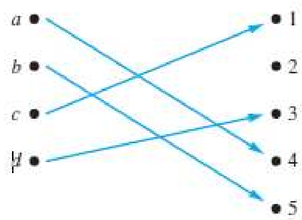

Figure 1.2: One-to-One function

Examples:

1. Consider the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$. The function f is one-to-one because it assigns different values to each element in its domain.

2. Consider the function $f(x) = x^2$ from the set of integers to the set of integers is not one-to-one because, for instance, $f(1) = f(-1) = 1$, but $1 \neq -1$.

(ii) Onto Function (Surjective Function): A function f from A to B is said to be as onto, or surjective, if and only if for every element b in the co-domain B, there exists an element a in the domain A such that $f(a) = b$. In simpler terms, onto function ensures that every element in the co-domain is mapped to by at least one element from the domain. Mathematically, a function is surjective if $\forall y \, \exists x \, (f(x) = y)$, where x ranges over the domain of the function and y over the co-domain.

Examples:

1. Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ with $f(a) = 3, f(b) = 2, f(c) = 1$, and $f(d) = 3$. In this case, f is onto because every element in the co-domain $\{1, 2, 3\}$ has at least one element in the domain $\{a, b, c, d\}$ that maps to it.

2. The function $f(x) = x^2$ from the set of integers to the set of integers is not onto since there is no integer x such that $x^2 = -1$, and hence, not all elements in the co-domain are reached.

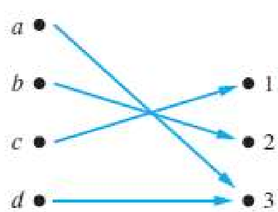

Figure 1.3: Onto function

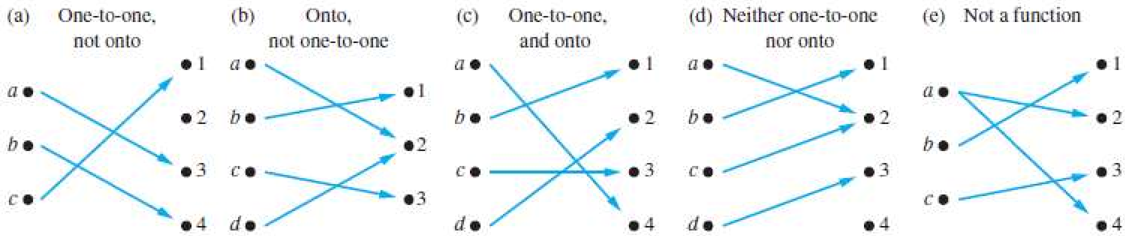

Figure 1.4: Different types of correspondences

(iii) One-to-One Onto Function (Bijective Function): A function f is referred to as a one-to-one onto correspondence, or a bijection, if it possesses both one-to-one and onto properties. We can also say that such a function is bijective.

Example: Consider the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ with $f(a) = 4, f(b) = 2, f(c) = 1$, and $f(d) = 3$. Is f a bijection? Yes, this function is a bijection because it is both one-to-one (no two-domain values map to the same co-domain value) and onto (covers all co-domain elements).

When dealing with functions whose domain and co-domain are subsets of the real numbers, we can classify them as either **increasing or decreasing function**.

(a) Increasing Function: A function f is considered increasing if, for all x and y in its domain, where $x < y$, it holds that $f(x) \leq f(y)$. In simple terms, as the input increases, the function value does not decrease.

(b) Strictly Increasing Function: A function is strictly increasing if, for all x and y in its domain, where $x < y$, it holds that $f(x) < f(y)$. Here, the function values strictly increase as the input increases.

(c) Decreasing Function: A function f is termed decreasing if, for all x and y in its domain, where $x < y$, it holds that $f(x) \geq f(y)$. In this case, as the input increases, the function value does not increase.

(d) Strictly Decreasing Function: A function is strictly decreasing if, for all x and y in its domain, where $x < y$, it holds that $f(x) > f(y)$. In this situation, the function values strictly decrease as the input increases.

The universe of discourse in these statements is the domain of the function.

1.5.2 Inverse Functions and Compositions of Functions

(i) Inverse Function: When we have a one-to-one correspondence (bijective function) from set A to set B, the inverse function of this correspondence assigns to an element b in B the unique element a in A such that $f(a) = b$. This inverse function is denoted by f^{-1}. Thus, $f^{-1}(b) = a$ when $f(a) = b$.

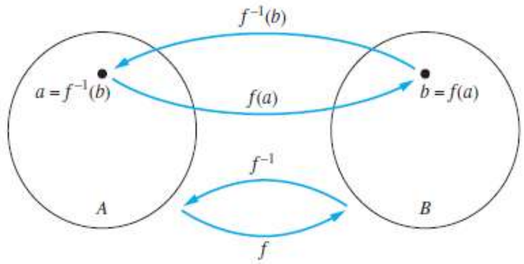

Figure 1.5: Inverse of function $f(x)$

Examples:

1. Consider the function f from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, and $f(c) = 1$. Is f invertible, and if it is, what is its inverse?

   Solution: The function f is invertible because it's a one-to-one correspondence. The inverse function f^{-1} reverses the correspondence, so $f^{-1}(1) = c$, $f^{-1}(2) = a$, and $f^{-1}(3) = b$.

2. Let $f: Z \to Z$ be such that $f(x) = x + 1$. Is f invertible, and if it is, what is its inverse?

   Solution: The function f has an inverse because it's a one-to-one correspondence. To reverse the correspondence, suppose y is the image of x, so $y = x + 1$. Then $x = y - 1$. This means that $f^{-1}(y) = y - 1$.

(ii) Composition of Functions: If you have a function g from set A to set B and a function f from set B to set C, the composition of the functions f and g, denoted as $f \circ g$, is defined for all a in set A by $(f \circ g)(a) = f(g(a))$. It's essentially applying the function g first and then the function f.

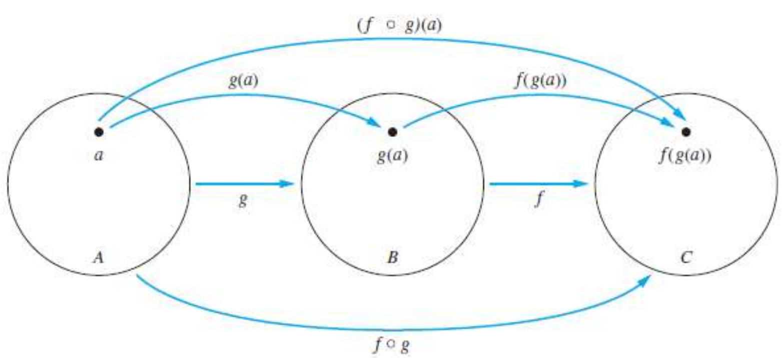

Figure 1.6: Composition of functions $f(x)$ and $g(x)$

Examples:

1. Let g be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b$, $g(b) = c$, and $g(c) = a$. Let f be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3$, $f(b) = 2$, and $f(c) = 1$. What is the composition of f and g, and what is the composition of g and f?

Solution: The composition $f \circ g$ is defined as $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$. Note that $g \circ f$ is not defined because the range of f is not a subset of the domain of g.

2. Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g? What is the composition of g and f?

Solution: Both compositions, $f \circ g$ and $g \circ f$, are defined. Moreover, $(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$ and $(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$.

1.6 WELL-ORDERING PRINCIPLE

Much of abstract algebra relies on the properties of integers, particularly the well-ordering principle. Let us start with a definition.

Definition: Let S be a non-empty subset of the set of integers,Z. An element $a \in S$ is termed as the least element (or a minimum element) of S if it satisfies the condition $a \leq b \; \forall \; b \in S$.

For instance, the set of natural numbers, N possesses a least element, which is 1. But the set of all integers does not have a least element. In fact, several subsets of integers, like $2Z$ or the set of negative integers, do not exhibit a least element.

The well-ordering principle, as an axiom, provides insights into sets that do indeed have a least element.

Well-ordering Principle: Every non-empty set of positive integers contains a smallest member.

1.7 DIVISIBILITY IN Z AND THE DIVISION ALGORITHM

Divisibility of integers is one of the fundamental ideas of number theory.

Definition: Let $a, b \; \forall \; a \neq 0$, then an integer '$a$' is said to divide another integer 'b' if there exists an integer 'c' such that $b = ac$. This relationship is represented as '$a \mid b$,' indicating that 'a' is a divisor or factor of 'b,' or that 'b' is divisible by 'a,' or that 'b' is a multiple of 'a'.

If a does not divide b we write $a \times b$.

Theorem 1.1 (Division Algorithm): Let $a, b \in Z$ with $b > 0$, then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$.

Proof: Let's start with the existence part. Consider the set $S = \{a - bk \mid k$ is an integer and $a - bk \geq 0\}$. If 0 is an element of S, then b divides a, and we can get the desired result with $q = a/b$ and $r = 0$. Now, assume 0 is an element of S. Since S is nonempty (if $a > 0, a - b \,.\, 0 \in S$; if $a < 0, a - b(2a) = a(1 - 2b) \in S$; and $a \neq 0$ since $0 \notin S$), we can apply the Well-Ordering Principle, and S has a smallest member, denoted as $r = a - bq$. Then $a = bq + r$, and $r \geq 0$. To complete the proof, we need to show that $r < b$.

If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, meaning $a - b(q + 1) \in S$. However, $a - b(q + 1) < a - bq$, and $a - bq$ is the smallest member of S. So, $r < b$.

Uniqueness of q and r: Let us suppose there are integers q, q', r, and r' such that $a = bq + r, 0 \leq r < b$, and $a = bq' + r', 0 \leq r' < b$. For convenience, let us assume that $r' \geq r$. Then, $bq + r = bq' + r'$ and $b(q - q') = r' - r$. As b divides $r' - r$ and $0 \leq r' - r \leq r' < b$, it follows that $r' - r = 0$, and hence $q = q'$.

The integer q in the Division Algorithm is called the quotient when 'a' is divided by 'b,' and the integer r is called the remainder when 'a' is divided by 'b.'

For instance, when $a = 17$ and $b = 5$, the division algorithm gives $17 = 5.3 + 2$. Similarly, when $a = -23$ and $b = 6$, the division algorithm yields $-23 = 6.(-4) + 1$.

Definition (Greatest Common Divisor, Relatively Prime Integers): The greatest common divisor of two nonzero integers a and b is thelargest of all common divisors of a and b. We denote this integer by$gcd(a, b)$. When $gcd(a, b) = 1$, we say a and b are relatively prime.

Theorem 1.2 (GCD Is a Linear Combination): For any nonzero integers a and b, there exist integers s and t such that $gcd(a, b) = as + bt$. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Corollary 1.1: If a and b are relatively prime, than there exist integers s and t suchthat $as + bt = 1$.

Example: $gcd(4, 15) = 1$; $gcd(4, 10) = 2$; $gcd(2^2 . 3^2 . 5, 2 . 3^3 . 7^2) = 2 . 3^2$. Note that 4 and 15 are relatively prime, whereas 4 and 10 are not.

Euclid's Lemma:$p \mid ab$ implies $p \mid a$ or $p \mid b$

If p is a prime that divides ab, then p divides a or p divides b.

Theorem 1.3 (Fundamental Theorem of Arithmetic): Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 \ldots p_r$ and $n = q_1 q_2 \ldots q_s$, where the $p's$ and $q's$ are primes, then $r = s$ and, after renumbering the $q's$, we have $p_i = q_i$ for all i.

Definition (Least Common Multiple): The least common multiple of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b. We will denote this integer by $lcm(a, b)$.

Example: $lcm(4, 6) = 12$; $lcm(4, 8) = 8$; $lcm(10, 12) = 60$; $lcm(6, 5) = 30$;
$lcm(2^2 . 3^2 . 5, 2 . 3^3 . 7^2) = 2^2 . 3^3 . 5 . 7^2$.

1.7.1 Modular Arithmetic

Another application of the division algorithm that will be important to us is modular arithmetic.

For example, if it is now September, what month will it be 25 months from now?

Of course, the answer is October, but the interesting fact is that you didn't arrive at the answer by starting with September and counting off 25 months.

Instead, without even thinking about it, you simply observed that $25 = 2.12 + 1$

When $a = qn + r$, where q is the quotient and r is the remainder upon dividing a by n, we write $a \, mod \, n = r$. Thus,

$3 \, mod \, 2 = 1$ since $3 = 1.2 + 1$,

$6 \, mod \, 2 = 0$ since $6 = 3.2 + 0$,

$11 \, mod \, 3 = 2$ since $11 = 3.3 + 2$,

$-2 \, mod \, 15 = 13$ since $-2 = (-1)15 + 13$.

In this unit, we have covered a range of foundational concepts in abstract algebra, starting with sets and their operations. We explored the power of Cartesian products, which are crucial for defining functions and relations. Equivalence classes were introduced as a key concept, leading to the creation of quotient sets. Functions were discussed in detail, categorizing them as one-to-one, onto, and bijective, and highlighting their relevance in abstract algebra. Lastly, we delved into the well-ordering principle and division algorithm, both of which have significant applications in algebraic structures.

1.8 LET US SUM UP

In this unit we have covered the following points:

- Some properties of sets and subsets.
- The union, intersection, difference and complements of sets.
- The Cartesian product of Sets.
- Relations in general, and equivalence relations in particular.
- The definition of a function, a 1-1 function, an unto function and a bijective function.
- The composition of functions.
- The well-ordering principle, which states that every subset of N has a least element.
- Properties of divisibility in Z, like the division algorithm and unique prime factorization.

1.9 UNIT END EXERCISE

1. Let $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$. Find the union $(A \cup B)$ and the intersection $(A \cap B)$.
2. Given $A = \{2, 4, 6\}$ and $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, find the complement of A, (A') and the difference of B and A, $(B - A)$.
3. Find the Cartesian product of sets $X = \{a, b\}$ and $Y = \{1, 2, 3\}$.
4. Define the equivalence relation $\sim$ on the set of integers Z as $a \sim b$ if and only if $(a - b)$ is a multiple of 5. Show that this is an equivalence relation and find the equivalence class of 7.
5. Define a function $f: R \to R$ by $f(x) = 2x + 1$. Determine if f is one-to-one, onto, or bijective.
6. Find the least elements for following sets by using the well-ordering principle.

   (i) Set of real numbers, $S = \{1, 2, 3, 4, 5, \ldots\}$

   (ii) Set of non-negative even integers, $S = \{0, 2, 4, 6, 8, \ldots\}$

   (iii) Set of rational numbers, $S = \{1/2, 3/4, 2/5, 5/7, 4/9, 6/11\}$

   (iv) Set $S = \{3, 7, 11, 15, 20, 27\}$

   (v) Set $S = \{5, 3, 8, 12, 9, 15\}$
7. Using the Division Algorithm, divide 53 by 6.

ANSWERS

1. $A \cup B = \{1,2,3,4,5,6\}$; $A \cap B = \{3,4\}$
2. $A' = \{1,3,5,7,8\}$; $B - A = \{1,3,5,7,8\}$
3. $X \times Y = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}$
4. $[7] = \{7,12,17,22,\ldots\}$
5. f is both one-to-one and onto, so it is bijective
6. (i) 1; (ii) 0; (iii) $1/2$; (iv) 3; (v) 3
7. $53 = 6 * 8 + 5$

1.10 REFERENCES AND SUGGESTED READINGS

1. Herstein I. N.; Topics in Algebra, Wiley Eastern.
2. Dummit D. S. and Foote R. M.; Abstract Algebra, John Wiley & Sons.
3. Bhattacharya P. B., Jain S. K. and Nagpal S. R.; Basic Abstract Algebra, Cambridge University Press.
4. Gallian J. A.; Contemporary Abstract Algebra, Thomson Press.

***