GROUPS

L. MARIZZA A BAILEY

1. Groups

We will now study the objects called Groups. Given that so little is required to have a group, they have quite an amazing structure. Theorems flow merely from the definition of group and subgroup. We will study many examples of groups and subgroups.

Definition 1. A *group* is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying:

- **(G1)** $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$ (associativity);
- **(G2)** there exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (existence of an identity);
- **(G3)** for every $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$ (existence of inverses).

A group is a set that has an associative binary operation with an identity, and in which every element has an inverse in the set.

Note that a set can be many different groups depending on the choice of binary operation. Identify for which of the following binary operations, the sets below are groups?
If the set is not a group under a binary operation, find the largest group in that set under that operation.

(a) $\mathbb{Z}$ with multiplication? addition? concatenation?

(b) $\mathbb{R}$ with multiplication? addition?

Date: October 17, 2014.

(c) $\mathbb{Q}$ with multiplication? addition?

(d) $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$ under function addition? function multiplication? composition?

(e) $\mathrm{Sym}(X)$ under composition? addition? multiplication?

(f) The set of all strings in $\{0, 1\}$ under concatenation? multiplication? addition?

(g) $\mathbb{Z}_n$ under addition? multiplication?

There are two important theorems we need to get through. The first is that, in a group,G, every element has a unique inverse. This allows the function $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ to be well defined. The second is that their is only one identity. This allows the function which sends everything to the identity to be well-defined.

Lemma 1 (Uniqueness of inverse)**.** *Let G be a group, and $g \in G$.*
Let $h \in G$ such that $h * g = e$, and $g^{-1} \in G$ such that $g * g^{-1} = e$. Then $h * g * g^{-1} = h * (g * g^{-1}) = h * e = h$.
Also $h * g * g^{-1} = (h * g) * g^{-1} = e * g^{-1} = g^{-1}$.
Therefore, $h = g^{-1}$.

Lemma 2 (Uniqueness of identity)**.** *Let G be a group, with identity e. Suppose there exists $e' \in G$ such that $e' * g = g$ for all $g \in G$. Then $e * e' = e$ by definition of e' identity,*
and $e * e' = e'$ by definition of e identity.

Definition 2 (Abelian)**.** A group is called *abelian* if its operation is commutative.

$$g * h = h * g$$

for all $g, h \in G$.

Example 1. The following are abelian groups:

- $(\mathbb{Z}, +, 0)$, the integers under addition;
- $(\mathbb{Q}, +, 0)$, the rational numbers under addition;
- $(\mathbb{R}, +, 0)$, the real numbers under addition;
- $(\mathbb{C}, +, 0)$, the complex numbers under addition;
- $(\mathbb{Q}^*, \cdot, 1)$, the nonzero rational numbers under multiplication;
- $(\mathbb{R}^*, \cdot, 1)$, the nonzero real numbers under multiplication;
- $(\mathbb{C}^*, \cdot, 1)$, the nonzero complex numbers under multiplication.

1.1. **Standard Notation.** Usually the operation of abelian groups is denoted by $+$, and the identity is denoted as 0.
If the group is not abelian then the operation of the group is denoted as $\cdot$, and the identity is denoted as 1 or e.

Example 2. Let X be a set and let $\mathcal{P}(X) = \{A \subset X\}$. Define the *symmetric difference* of $A, B \in \mathcal{P}(X)$ by

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Then $(\mathcal{P}(X), \triangle, \varnothing)$ is a group under symmetric difference.
What is the identity?
What is the inverse of each element?

Example 3. Let $M_{m \times n}(\mathbb{R})$ be the set of $m \times n$ matrices over the real numbers. Then $M_{m \times n}(\mathbb{R})$ is a group under matrix addition.
What is the identity? What is the inverse of each element?

Example 4. Let $\mathbf{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices over the real numbers. Then $\mathbf{GL}_n(\mathbb{R})$ is a group under matrix multiplication. For those who do not know GL_n, a matrix is invertible if and only if it's determinant is nonzero. Finding the inverse of an arbitrary matrix can be time consuming, unless you write a program that can do it for you. Let us examine GL_2R to identify the identity and inverse of a matrix. We will then venture on to $GL_3(R)$.

Example 5. Let X be a set and let $\mathrm{Sym}(X) = \{\sigma : X \to X \mid \sigma \text{ is bijective}\}$. Then $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ is a group under composition of functions. This is called the permutation group of X. A permutation is defined to be a bijective function from X to X.

Example 6. Let $C_n = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$ be a set of symbols, and define a multiplication on C_n by $g^k g^l = g^{k+l \pmod n}$. This is called a *cyclic group of order n* . The identity is g^0, and we write $1 = g^0$ and $g = g^1$.

- C_n is abelian;
- $|C_n| = n$;

Example 7. Let S_n be the set of permutations of the set $\{1, \ldots, n\}$. The group operation is composition of functions, and the identity is the identity function.

- S_n is nonabelian for $n \geq 3$;
- $|S_n| = n!$.

Proof 1 (Non-abelian)**.** *We know that $f \circ g$ does not always equal $g \circ f$. In order to prove that S_n is not abelian for $n \geq 3$, we are going to have to find two permutation of 3 things which do not commute.*
Let (123) *be the permutation which sends* $1 \to 2$, $2 \to 3$ *and* $3 \to 1$.
and (12) *be the permutation which sends* $1 \to 2$ *and* $2 \to 1$.
Then $(123)(12) = (13)$ *because* $1 \to 2 \to 3$ *and* $2 \to 1 \to 2$ *and* $3 \to 3 \to 1$.
However $(12)(123) = (23)$.
Since every permutation group of n things where $n \geq 3$ *must also permute* 3 *things, then these elements are contained in all larger permutation groups.*

Example 8. Let A_n be the set of even permutations of the set $\{1, \ldots, n\}$; that is, A_n is the set of permutations whose decomposition into transpositions always yields an even number of transposition.

- A_n is nonabelian for $n \geq 4$;
- $|A_n| = n!/2$.
- $A_n \leq S_n$;

Example 9. Let D_n be the set of symmetries of a regular n-gon ($n \geq 3$); that is, D_n is the set of rigid motions of a regular polygon with n-vertices which send vertices to vertices. Then D_n is generated by a rotation and a reflection. For example, consider an equilateral triangle. We may rotate it by 120 degrees, 240 degrees, or 360 degrees; the latter represents the identity map. We may also reflect it through a line which intersects a vertex and bisects the opposite side. (Bailey, Paul, Notes on Group Theory)

2. Order

Definition 3. The *order* of a group, G, is denoted $|G|$ and is defined to be the cardinality of the set G.

Example 10. The order of $\mathbb{Z}_n$ is n
The order of S_n is $n!$
The order of the dihedral group of a regular polygon with n sides is $2n$.
The order of the set of invertible functions from $\mathbb{R}$ to $\mathbb{R}$ is very large.
Why?

Definition 4. Let G be a group, and $g \in G$. The *order* of an element is denoted $\text{ord}(g)$ and is the smallest positive integer $n \in \mathbb{N}$ such that $g^n = e$.
If this never happens, then we say g has infinite order.

Example 11. Let $(\mathbb{Z}_8, +)$ be the group of equivalence classes of remainders when you divide an integer by 8.
Then $g^n = ng$ because adding g to itself n times is called multiplication.

- $\text{ord}(0) = 1$
- $\text{ord}(1) = 8$
- $\text{ord}(2) = 4$ because $2 + 2 + 2 + 2 = 8 \equiv 0 \mod (8)$ or $4(2) = 8$
- $\text{ord}(3) = 8$ because 3 and 8 are relatively prime.
- $\text{ord}(4) = 2$
- $\text{ord}(5) = 8$
- $\text{ord}(6) = 4$
- $\text{ord}(7) = 8$

Note that the orders of all the elements constitute the set of factors of 8.

Example 12. Each element of S_n can be written as a product of it's disjoint cycles. For example

$$2 \to 3$$
$$3 \to 5$$
$$4 \to 6$$
$$5 \to 1$$
$$6 \to 4$$

can be more easily written as (1235)(46).This is called the disjoint cycle decomposition. Note that (1235) has order 4, and (46) has order 2. Do you think this holds true for any cycle of length n.

3. Exercises

Exercise 1. Let S_4 be the group of permutations of 4 elements.

- **(a)** Classify all the elements by their *shape*.
  The *shape* of a permutation is the number of disjoint cycles and the number of elements in each cycle.
  For example: (12)(34) has shape $2-2$
  and (123) has shape $3-1$.
- **(b)** Find the order of each element. Is it determined by their shape? You don't have to list all twenty-four, just a representative of each shape class
- **(c)** Let A_4 be the subset of permutations with an even number of disjoint cycles. Is this a group? What is the order of A_4?
- **(d)** Let D_4 be the group of permutations which model the rigid motions of a square. What is the order or D_4? List the elements.
- **(e)** Let $K_4 = A_4 \cap D_4$. What is the order of K_4? Find the order of each element in K_4. This is called the Klein-4 group.

Exercise 2. Write the multiplication table for Z_6. List the elements which are multiplicatively invertible.

Exercise 3. Let G be a group such that $g^2 = e$ for all $g \in G$. Show that G is abelian, or $gh = hg$ for all $g \in G$.

Exercise 4 (# 26)**.** Let G be a group, and $a, b \in G$.
Show that if $(ab)^2 = a^2b^2$ then $ab = ba$

Department of Mathematics, BASIS Scottsdale
E-mail address: marizza.bailey@basisscottsdale.org