Introduction

1.1 What is a group?

Definition 1.1: If G is a nonempty set, a *binary operation* μ on G is a function $\mu : G \times G \to G$.

For example $+$ is a binary operation defined on the integers $\mathbb{Z}$. Instead of writing $+(3, 5) = 8$ we instead write $3 + 5 = 8$. Indeed the binary operation μ is usually thought of as *multiplication* and instead of $\mu(a, b)$ we use notation such as ab, $a + b$, $a \circ b$ and $a * b$. If the set G is a finite set of n elements we can present the binary operation, say $*$, by an n by n array called the *multiplication table*. If $a, b \in G$, then the (a, b)–entry of this table is $a * b$.

Here is an example of a multiplication table for a binary operation $*$ on the set $G = \{a, b, c, d\}$.

$*$	a	b	c	d
a	a	b	c	a
b	a	c	d	d
c	a	b	d	c
d	d	a	c	b

Note that $(a * b) * c = b * c = d$ but $a * (b * c) = a * d = a$.

Definition 1.2: A *binary operation* $*$ on set G is *associative* if

$$(a * b) * c = a * (b * c)$$

for all $a, b, c \in G$.

Subtraction $-$ on $\mathbb{Z}$ is not an associative binary operation, but addition $+$ is. Other examples of associative binary operations are matrix multiplication and function composition.

A set G with a associative binary operation $*$ is called a *semigroup*. The most important semigroups are groups.

Definition 1.3: A *group* $(G, *)$ is a set G with a special element e on which an associative binary operation $*$ is defined that satisfies:

1. $e * a = a$ for all $a \in G$;
2. for every $a \in G$, there is an element $b \in G$ such that $b * a = e$.

Example 1.1: *Some examples of groups.*

1. The integers $\mathbb{Z}$ under addition $+$.
2. The set $GL_2(\mathbb{R})$ of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation. This is the *general linear group* of 2 by 2 matrices over the reals $\mathbb{R}$.
3. The set of matrices

$$G = \left\{ e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

   under matrix multiplication. The multiplication table for this group is:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

4. The non-zero complex numbers $\mathbb{C}$ is a group under multiplication.

5. The set of complex numbers $G = \{1, i, -1, -i\}$ under multiplication. The multiplication table for this group is:

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

6. The set $\mathsf{Sym}\,(X)$ of one to one and onto functions on the n-element set X, with multiplication defined to be composition of functions. (The elements of $\mathsf{Sym}\,(X)$ are called *permutations* and $\mathsf{Sym}\,(X)$ is called the *symmetric group* on X. This group will be discussed in more detail later. If $\alpha \in \mathsf{Sym}\,(X)$, then we define the image of x under α to be x^α. If $\alpha, \beta \in \mathsf{Sym}\,(X)$, then the image of x under the composition $\alpha\beta$ is $x^\alpha\beta = (x^\alpha)^\beta$.)

1.1.1 Exercises

1. For each fixed integer $n > 0$, prove that $\mathbb{Z}_n$, the set of integers modulo n is a group under $+$, where one defines $\overline{a} + \overline{b} = \overline{a+b}$. (The elements of $\mathbb{Z}_n$ are the congruence classes $\overline{a}$, $a \in \mathbb{Z}$.. The congruence class $\bar{a}$ is

$$\{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{a + kn : k \in \mathbb{Z}\}.$$

   Be sure to show that this addition is well defined. Conclude that for every integer $n > 0$ there is a group with n elements.

2. Given integer $n > 0$ let G be the subset of complex numbers of the form $e^{\frac{2k\pi}{n}i}$, $k \in \mathbb{Z}$. Show that G is a group under multiplication. How many elements does G have?

Some properties are unique.

Lemma 1.2.1. *If $(G, *)$ is a group and $a \in G$, then $a*a = a$ implies $a = e$.*

Proof. Suppose $a \in G$ satisfies $a*a = a$ and let $b \in G$ be such that $b*a = e$. Then $b * (a * a) = b * a$ and thus

$$a = e * a = (b * a) * a = b * (a * a) = b * a = e$$

□

Lemma 1.2.2. *In a group $(G, *)$*

(i) *if $b * a = e$, then $a * b = e$ and*

(ii) *$a * e = a$ for all $a \in G$*

Furthermore, there is only one element $e \in G$ satisfying (ii) *and for all $a \in G$, there is only one $b \in G$ satisfying $b * a = e$.*

Proof. Suppose $b * a = e$, then

$$(a * b) * (a * b) = a * (b * a) * b = a * e * b = a * b.$$

Therefore by Lemma 1.2.1 $a * b = e$.

Suppose $a \in G$ and let $b \in G$ be such that $b * a = e$. Then by (i)

$$a * e = a * (b * a) = (a * b) * a = e * a = a$$

Now we show uniqueness. Suppose that $a * e = a$ and $a * f = a$ for all $a \in G$. Then

$$(e * f) * (e * f) = e * (f * e) * f = e * f * e = e * f$$

Therefore by Lemma 1.2.1 $e * f = e$. Consequently

$$f * f = (f * e) * (f * e) = f * (e * f) * e = f * e * e = f * e = f$$

and therefore by Lemma 1.2.1 $f = e$. Finally suppose $b_1 * a = e$ and $b_2 * a = e$. Then by (i) and (ii)

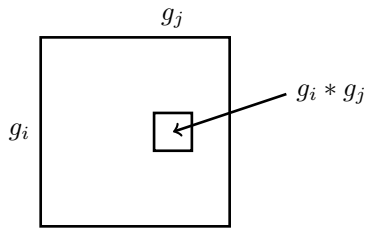
$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

□

Definition 1.4: Let $(G, *)$ be a group. The unique element $e \in G$ satisfying $e * a = a$ for all $a \in G$ is called the *identity* for the group $(G, *)$. If $a \in G$, the unique element $b \in G$ such that $b * a = e$ is called the *inverse* of a and we denote it by $b = a^{-1}$.

If $n > 0$ is an integer, we abbreviate $\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$ by a^n. Thus $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}}$

Let $(G, *)$ be a group where $G = \{g_1, g_2, \ldots, g_n\}$. Consider the multiplication table of $(G, *)$.



Let $[x_1\ x_2\ x_3\ \cdots\ x_n]$ be the row labeled by g_i in the multiplication table. I.e. $x_j = g_i * g_j$. If $x_{j_1} = x_{j_2}$, then $g_i * g_{j_1} = g_i * g_{j_2}$. Now multiplying by g_i^{-1} on the left we see that $g_{j_1} = g_{j_2}$. Consequently $j_1 = j_2$. Therefore

> *every row of the multiplication table contains every element of G exactly once*

a similar argument shows that

> *every column of the multiplication table contains every element of G exactly once*

A table satisfying these two properties is called a Latin Square.

Definition 1.5: A *latin square* of side n is an n by n array in which each cell contains a single element form an n-element set $S = \{s_1, s_2, \ldots, s_n\}$, such that each element occurs in each row exactly once. It is in *standard form* with respect to the sequence $s_1, s_2, \ldots, s_n$ if the elements in the first row and first column are occur in the order of this sequence.

The multiplication table of a group $(G, *)$, where $G = \{e, g_1, g_2, \ldots, g_{n-1}\}$ is a latin square of side n in standard form with respect to the sequence

$$e, g_1, g_2, \ldots, g_{n-1}.$$

The converse is not true. That is not every latin square in standard form is the multiplication table of a group. This is because the multiplication represented by a latin square need not be associative.

Example 1.2: A latin square of side 6 in standard form with respect to the sequence $e, g_1, g_2, g_3, g_4, g_5$.

e	g_1	g_2	g_3	g_4	g_5
g_1	e	g_3	g_4	g_5	g_2
g_2	g_3	e	g_5	g_1	g_4
g_3	g_4	g_5	e	g_2	g_1
g_4	g_5	g_1	g_2	e	g_3
g_5	g_2	g_4	g_1	g_3	e

The above latin square is not the multiplication table of a group, because for this square:

$$(g_1 * g_2) * g_3 = g_3 * g_3 = e$$

but

$$g_1 * (g_2 * g_3) = g_1 * g_5 = g_2$$

1.2.1 Exercises

1. Find all Latin squares of side 4 in standard form with respect to the sequence $1, 2, 3, 4$. For each square found determine whether or not it is the multiplication table of a group.
2. If $(G, *)$ is a finite group, prove that, given $x \in G$, that there is a positive integer n such that $x^n = e$. The smallest such integer is called the *order* of x and we write $|x| = n$.
3. Let G be a *finite* set and let $*$ be an associative binary operation on G satisfying for all $a, b, c \in G$
   (i) if $a * b = a * c$, then $b = c$; and
   (ii) if $b * a = c * a$, then $b = c$.

Then $(G, *)$ must be a group. Also provide a counter example that shows that this is false if G is infinite.

4. Show that the Latin Square

e	g_1	g_2	g_3	g_4	g_5	g_6
g_1	e	g_3	g_5	g_6	g_2	g_4
g_2	g_3	e	g_4	g_1	g_6	g_5
g_3	g_2	g_1	g_6	g_5	g_4	e
g_4	g_5	g_6	g_2	e	g_3	g_1
g_5	g_6	g_4	e	g_2	g_1	g_3
g_6	g_4	g_5	g_1	g_3	e	g_2

is not the multiplication table of a group.

5. **Definition 1.6:** A group $(G, *)$ is *abelian* if $a * b = b * a$ for all elements $a, b \in G$.

   (a) Let $(G, *)$ be a group in which the square of every element is the identity. Show that G is abelian.

   (b) Prove that a group $(G, *)$ is abelian if and only if $f : G \to G$ defined by $f(x) = x^{-1}$ is a homomorphism.

Subgroup

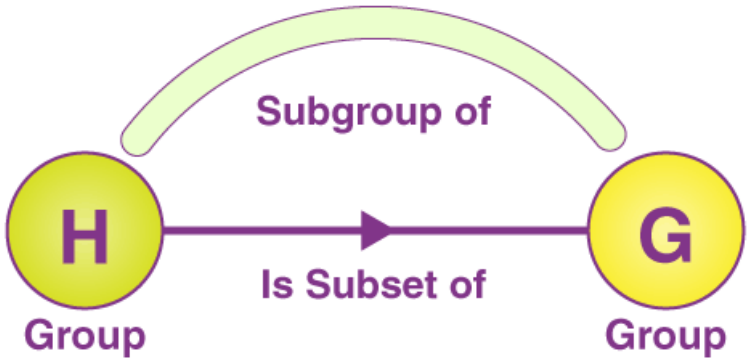
In mathematics, group theory is one of the most important branches, where we learn about different algebra concepts, such as groups, subgroups, cyclic groups, and so on. As we know, a group is a combination of a set and a binary operation that satisfies a set of axioms, such as closure, associative, identity and inverse of elements. A subgroup is defined as a subset of a group that follows all necessary conditions to be a group. Let's understand the mathematical definition of a subgroup here.

Definition

Let (G, ⋆) be a group and H be a non-empty subset of G, such that (H, ⋆) is a group then, "H" is called a subgroup of G.

That means H also forms a group under a binary operation, i.e., (H, ⋆) is a group.

Also, any subset of a group G is called a complex of G.



Below are some important points about subgroups.

- A subset H of a group G is a subgroup of G, if H itself is a group under the operation in G.
- A subgroup of a group consisting of only the identity element, i.e., {e} is called the trivial subgroup.
- A subgroup H of a group G, a proper subset of G, i.e., $H \neq G$ is called the proper subgroup and is represented by $H < G$. This can be read as "H is a proper subgroup of G".
- If H is a subgroup of G, then G may be called an over group of H in some cases.

Theorems on Subgroups

Theorem 1:

H is a subgroup of G. Prove that the identity element of H is equal to the identity element in G.

Proof:

Given that H is a subgroup of G.

Let us assume that e and e’ be the two identity elements in H and G, respectively.

Let $a \in H \Rightarrow a \in G$ [since H is a subset of G]

Identity element in group H = e

Thus, $a \star e = e \star a = a$…..(1)

Identity element in group G = e

Therefore, $a \star e' = e' \star a = a$…..(2)

From (1) and (2),

$a \star e = a \star e'$

$\Rightarrow e = e'$

That means, the identity element in H is equal to the identity element in G.

Hence proved.

Theorem 2:

H is a subgroup of G. The inverse of any element in H is equal to the inverse of the same element in G.

Proof:

Given that H is a subgroup of G.

Consider $a \in H \Rightarrow a \in G$

Let us assume that b and c are two inverse elements of a in H and G respectively.

Let b be the inverse element of a in H.

Then, $a \star b = b \star a = e$….(1)

Let c be the inverse element of a in G.

Then, $a \star c = c \star a = e$….(2)

From (1) and (2),

$a \star b = a \star c$

$\Rightarrow b = c$

That means the inverse element of a in H is equal to the inverse element of a in G.

Hence proved.

Difference between Groups and Subgroups

The below table illustrates a few differences between groups and subgroups.

Group	**Subgroup**
A group is a set combined with a binary operation, such that it connects any two elements of a set to produce a third element, provided certain axioms are followed.	A subgroup is a subset of a group. H is a subgroup of a group G if it is a subset of G, and follows all axioms that are required to form a group.
Groups satisfy the following laws: • Closure • Associative • Identity element • Inverse law	Subgroups also satisfy the following laws: • Closure • Associative • Identity element • Inverse law
The number of elements of a finite group is called the order of a group.	A subgroup is also a group, and the order of a subgroup is less than the order of a group.

Properties of Subgroups

We can also prove the following statements using the properties of groups and subgroups.

1. Let H be any subgroup of G, such that $H^{-1} = H$ and $HH = H$.
2. H is a non-empty complex of a group G. The necessary and sufficient condition for H to be a subgroup of G is: $a, b \in H \Rightarrow ab^{-1} \in H$, where b^{-1} is the inverse of b in G.
3. H is a subgroup of G if and only if $HH^{-1} = H$.
4. If H and K are two subgroups of a group G, then HK is a subgroup of G if and only if HK = KH.
5. If H and K are two subgroups of a group G, then $H \cap K$ is a subgroup of G.
6. The union of two subgroups of a group is a subgroup, if and only if one is contained in the other. (or) If H and G are two subgroups of G, then $H \cup K$ is a subgroup of G, if and only if $H \subseteq K$ or $K \subseteq H$.

What makes a subset a subgroup?

A subset of a group is said to be a subgroup if it holds all group axioms, i.e. associativity, closure, inverse, and identity law under the binary operation of the group.

How many subgroups can a group have?

The number of subgroups of a group can be determined based on the order of a group.

Subgroups

Definition: A subset H of a group G is a subgroup of G if H is itself a group under the operation in G.

Note: Every group G has at least two subgroups: G itself and the subgroup $\{e\}$, containing only the identity element. All other subgroups are said to be proper subgroups.

Examples

1. GL(n,R), the set of invertible $n \times n$ matrices with real entries is a group under matrix multiplication. We denote by SL(n,R) the set of $n \times n$ matrices with real entries whose determinant is equal to 1. SL(n,R) is a proper subgroup of GL(n,R) . (GL(n,R), is called the general linear group and SL(n,R) the special linear group.)

2. In the group D_4, the group of symmetries of the square, the subset $\{e, r, r^2, r^3\}$ forms a proper subgroup, where r is the transformation defined by rotating $\frac{\pi}{2}$ units about the z-axis.

3. In Z_9 under the operation +, the subset {0, 3, 6} forms a proper subgroup.

Problem 1: Find two different proper subgroups of S_3.

We will prove the following two theorems in class:

Theorem: Let H be a nonempty subset of a group G. H is a subgroup of G iff

(i) H is closed under the operation in G and

(ii) every element in H has an inverse in H.

For finite subsets, the situation is even simpler:

Theorem: Let H be a nonempty *finite* subset of a group G. H is a subgroup of G iff H is closed under the operation in G .

Problem 2: Let H and K be subgroups of a group G.

(a) Prove that $H \cap K$ is a subgroup of G.

(b) Show that $H \cup K$ need not be a subgroup

Example: Let $\mathbb{Z}$ be the group of integers under addition. Define H to be the set of all multiples of n. It is easy to check that H_n is a subgroup of Z. Can you identify the subgroup $H_n \cap H_m$? Try it for $H_6 \cap H_9$.

Note that the proof of part (a) of Problem 2 can be extended to prove that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup.

Cyclic Groups and Subgroups

We can always construct a subset of a group G as follows:
Choose any element a in G. Define $\langle a \rangle = \{a^n \mid n \in Z\}$, i.e. $\langle a \rangle$ is the set consisting of all powers of a.

Problem 3: Prove that $\langle a \rangle$ is a subgroup of G.

Definition: $\langle a \rangle$ is called the cyclic subgroup generated by a. If $\langle a \rangle = G$, then we say that G is a cyclic group. It is clear that cyclic groups are abelian.

For the next result, we need to recall that two integers a and n are relatively prime if and only if gcd(a, n)=1. We have proved that if gcd(a, n)=1, then there are integers x and y such that $ax + by = 1$. The converse of this statement is also true:

Theorem: Let a and n be integers. Then gcd(a, n)=1 if and only if there are integers x and y such that $ax + by = 1$.

Problem 4: (a) Let $U_n = \{a \in Z_n \mid \gcd(a,n)=1\}$. Prove that U_n is a group under multiplication modulo n. (U_n is called the group of units in Z_n.)
(b) Determine whether or not U_n is cyclic for n= 7, 8, 9, 15.

We will prove the following in class.
Theorem: Let G be a group and $a \in G$.

(1) If a has infinite order, then $\langle a \rangle$ is an infinite subgroup consisting of the distinct elements a^k with $k \in Z$.

(2) If a has finite order n, then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \{e = a^0, a^1, a^2, \ldots a^{n-1}\}$.

Theorem: Every subgroup of a cyclic group is cyclic.