Lecture Notes
in
MAT-205, Group Theory

Dr. Bhavin Patel

Government Science College, Gandhinagar
Gujarat University

May 19, 2013

"For example," is not proof.

The way to learn mathematics
is
to do mathematics.

Contents

Chapter 1

Binary Operations

1.1. Definitions and Examples

We are familiar with two fundamental operations: addition and multiplication in $\mathbb{Z}$. We may look upon " $+$ " and " $\cdot$ " as are machines such that when we feed integers m and n into this machine, the output is the integers $m+n$ and mn. In other words addition and multiplication can be consider as mappings from $\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$. More precisely, $+:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ is a mapping defined by $+(m,n)=m+n$, and $\cdot:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ is a mapping defined by $\cdot(m,n)=m\cdot n=mn$. Such mappings are called binary operations. Let us give the exact definition of binary operation.

1.1. Definition.

For a nonempty set A, a mapping from $A\times A$ to A is called a ***binary operation*** on A.

Thus binary operation is a rule which assigns to each element $(a,b)\in A\times A$, a unique element $c\in A$. We will use notations such as $\circ,*,\triangle,\nabla,+,\cdot,\oplus,\star,\bullet$, etc for binary operations. If $*$ is a binary operation on A, then we will denote by $a*b$, the value of $*$ at $(a,b)\in A\times A$ and call it the *product* of a and b. If we denote a binary operation in a set A by $*$ (respectively $\circ,\triangle,\nabla,+,\cdot,\oplus,\star,\bullet$) and $a,b\in A$, then the product of a and b under this binary operation is denoted by $a*b$ (respectively $a\circ b, a\triangle b, a\nabla b, a+b, a\cdot b, a\oplus b, a\star b, a\bullet b$).

1.2. Example. The binary operation $*$ on $\mathbb{Z}$ is defined as follows:

$$m * n = m - n \ \ (m, n \in \mathbb{Z}).$$

1.3. Example. The binary operation $+$ on $\mathbb{N}$ is defined as follows:

$$m + n = m^n \ \ (m, n \in \mathbb{N}).$$

Here, $2 + 3 = 2^3 = 8$, while $3 + 2 = 3^2 = 9$.

Remark: In Example 1.3, $2+3 = 8$, but in usual we have $2+3 = 5$. What is reason behind it? The reason is simple, here the definition of $+$ is different. So let us be clear from the beginning that the notations $+$ and $\cdot$ which we use for binary operations are not necessarily addition and multiplication notations, respectively, in our usual sense.

1.4. Example. The binary operation $\bullet$ on $\mathbb{N}$ is defined as follows:

$$m \bullet n = \min\{m, n\} \ \ (m, n \in \mathbb{N}).$$

Here, $2 \bullet 7 = \min\{2, 7\} = 2$ and $7 \bullet 2 = \min\{7, 2\} = 2$.

1.5. Example. The binary operation $\star$ on $\mathbb{N}$ is defined as follows:

$$m \star n = \max\{m, n\} \ \ (m, n \in \mathbb{N}).$$

Here, $2 \star 7 = \max\{2, 7\} = 7$ and $7 \star 2 = \max\{7, 2\} = 7$.

1.6. Example. The binary operation $\triangle$ on $\mathbb{Z}$ is defined as follows:

$$m \triangle n = m + n - mn \ \ (m, n \in \mathbb{Z}).$$

Thus, $2 \triangle 3 = 2 + 3 - (2 \cdot 3) = -1$

1.7. Example. The operation $\triangle$ on $\mathbb{N}$ is defined as follows:

$$m \triangle n = m + n - mn \ \ (m, n \in \mathbb{N})$$

is not binary operation on $\mathbb{N}$. Because, $2, 3 \in \mathbb{N}$, but $2 \triangle 3 = 2 + 3 - (2 \cdot 3) = -1 \notin \mathbb{N}$.

1.8. Example. Usual subtraction is not binary operation on $\mathbb{N}$. Because, $2, 3 \in \mathbb{N}$, but $2 - 3 = -1 \notin \mathbb{N}$.

1.9. Example. The operation $\circ$ on $\mathbb{Z}$ is defined as follows:

$$m \circ n = m \triangle n + 2 \ \ (m, n \in \mathbb{N}),$$

where $\triangle$ is a binary operation defined on $\mathbb{Z}$ in Example 1.6. Then,

$$2 \circ 3 = 2 \triangle 3 + 2 = (2 + 3 - 6) + 2 = 1.$$

1.10. Example. Let $M_n(\mathbb{R})$ be the set of all real matrices of order n. Binary operations $\oplus$ and $\bullet$ are defined in $M_n(\mathbb{R})$ as follows: For $P, Q \in M_n(\mathbb{R})$,

$$P \oplus Q = P + Q \quad \text{and} \quad P \bullet Q = PQ.$$

Here $P + Q$ and PQ are, respectively, addition and multiplication of matrices P and Q.

1.11. Example. For universal set U, three binary operations $*, \bullet$ and $\oplus$ are defined as follows: For $A, B \in P(U)$,

$$A * B = A \cup B, \;\; A \bullet B = A \cap B \;\; A \oplus B = A \triangle B.$$

Here, $A \triangle B$ is the symmetric difference of sets A and B.

Composition Tables

If A be a finite set, consisting of n elements say, then a composition $*$ in A can be described by means of a table consisting of n rows and n columns in which the entry at the intersection of a row headed by an element $a \in A$ and the column headed by an element $b \in A$ is $a*b$. Such tables are called composition tables. For example, Let $A = \{a, b, c\}$, then composition table of A is given by

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

From this table we find that,

$$a * a = a \;\; a * b = b \;\; a * c = a$$
$$b * a = b \;\; b * b = b \;\; b * c = c$$
$$c * a = a \;\; c * b = c \;\; c * c = c$$

In Example 1.11, take $U = \{a, b\}$. Then $P(U) = \{\phi, \{a\}, \{b\}, U\}$. Note that, $*$ on $P(U)$ is defined as $A*B = A \cup B$. Thus the composition table with respect to operation $*$ is give by

$*$	ϕ	$\{a\}$	$\{b\}$	U
ϕ	ϕ	$\{a\}$	$\{b\}$	U
$\{a\}$	$\{a\}$	$\{a\}$	U	U
$\{b\}$	$\{b\}$	U	$\{b\}$	U
U	U	U	U	U

1.2. Properties of Binary Operations

In Example 1.10, for any two real matrices P and Q of order n, $P \oplus Q = P + Q = Q + P = Q \oplus P$. While in Example 1.2,

$3 * 2 = 3 - 2 = 1$, and $2 * 3 = 2 - 3 = -1$. i.e. $2 * 3 \neq 3 * 2$. Thus for binary operation $*$ defined on the set A, the value $(a, b) \in A \times A$ may be independent of the order of a and b. This property of binary operation is called commutativity of binary operation. Let us define commutativity and other properties of binary operations exactly.

2.1. Definition.

A binary operation $*$ defined on a set A is said to be ***associative***, if

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in A.$$

Addition and multiplication are associative binary operations in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ but subtraction is not associative in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$.

2.2. Definition.

A binary operation $*$ defined on a set A is said to be ***commutative***, if

$$a * b = b * a \text{ for all } a, b \in A.$$

Any two elements in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are commutative under the binary operations addition and multiplication.

2.3. Definition.

Let $*$ be the binary operation in A. An element $e \in A$ is said to be an ***identity element*** (or a ***neutral element*** or a ***unit element***) for the binary operation $*$, if

$$a * e = e * a = a \text{ for all } a \in A.$$

We know that e is 0 for addition and e is 1 for multiplication in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. This shows that an identity element depends completely on the binary operation defined on a set.

2.4. Definition.

Let e be the identity element for the binary operation $*$ on A. If for a given element $a \in A$, there exists an element $b \in B$ such that

$$a * b = b * a = e,$$

then a is called a ***non-singular*** (***invertible***) element of A and b is said to be an ***inverse*** of a.

2.5. Remarks.

- ✓ According to the above definition, if b is an inverse of a then a will be also an inverse of b. Thus inverse of a non-singular element is always non-singular. Clearly, the identity element is always non-singular with itself as its inverse.
- ✓ If inverse of a does not exist, then a is said to be singular (or not invertible).
- ✓ From the definitions 2.3 and 2.4 we can see that, without existence of an identity element for $*$, we can not talk about an inverse of an element of A.

2.6. Definition.

Let $*_1$ and $*_2$ be two binary operations in A. The binary operation $*_2$ is said to be distributive over $*_1$, if

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c) \text{ for all } a, b, c \in A.$$

1.3. Solved Examples

3.1. Example. Define the binary operation $*$ on $\mathbb{Z}$ as follows $m * n = m - n$ $(m, n \in \mathbb{Z})$. Examine the binary operation $*$ for associativity, commutativity, identity element, and inverse.

SOLUTION. $(2 * 3) * 4 = (2 - 3) * 4 = (-1) * 4 = (-1) - 4 = -5$, and $2*(3*4) = 2*(3-4) = 2*(-1) = 2-(-1) = 3$ i.e. $(2*3)*4 \neq 2*(3*4)$. Thus $*$ is not associative.

$2 * 3 = 2 - 3 = -1$, and $3 * 2 = 3 - 2 = 1$ i.e. $2 * 3 \neq 3 * 2$. Thus $*$ is not commutative.

Let $e \in \mathbb{Z}$ be an identity element for $*$, then for any $m \in \mathbb{Z}$, we have

$m*e = m \Rightarrow m-e = m \Rightarrow e = 0$; also $e*m = m \Rightarrow e-m = m \Rightarrow e = 2m$.

Thus $2m = 0 \Rightarrow m = 0$, which is a contradiction. Hence, $*$ has no identity element.

Since $*$ has no identity element, we can not talk about inverse of an element. □

3.2. Example. Define the binary operation $+$ on $\mathbb{N}$ as follows $m+n = m^n \quad (m, n \in \mathbb{N})$. Examine the binary operation $+$ for associativity, commutativity, identity element, and inverse.

SOLUTION. $(2+3)+4 = (2^3)+4 = 8+4 = 8^4$, and $2+(3+4) = 2+(3^4) = 2+81 = 2^{81}$ i.e. $(2+3)+4 \neq 2+(3+4)$. Thus $+$ is not associative.

$2+3 = 2^3 = 8$, and $3+2 = 3^2 = 9$ i.e. $2+3 \neq 3+2$. Thus $+$ is not commutative.

Let $e \in \mathbb{N}$ be an identity element for $+$, then for any $m \in \mathbb{N}$, we have

$$m+e = m \;\Rightarrow\; m^e = m \;\Rightarrow\; e = 1;$$

also,

$$e+m = m \;\Rightarrow\; e^m = m \;\Rightarrow\; 1^m = m \;\Rightarrow\; m = 1.$$

Which is a contradiction. Hence, $+$ has no identity element.

Since $+$ has no identity element, we can not talk about inverse of an element. □

3.3. Example. Define the binary operation $\bullet$ on $\mathbb{N}$ as $m \bullet n = \min\{m, n\} \quad (m, n \in \mathbb{N})$. Examine the binary operation $\bullet$ for associativity, commutativity, identity element, and inverse.

SOLUTION. For $l, m, n \in \mathbb{N}$,

$$(l \bullet m) \bullet n = \min\{l, m\} \bullet n = \min\{l, m, n\} = l \bullet \min\{m, n\} = l \bullet (m \bullet n)$$

Thus $\bullet$ is associative.

Since $l \bullet m = \min\{l, m\} = \min\{m, l\} = m \bullet l$, $\bullet$ is not commutative.

Suppose $e \in \mathbb{N}$ be an identity element for $\bullet$. Choose $l \in \mathbb{N}$ such that $l > e$. Then

$$l = l \bullet e = \min\{l, e\} = e < l.$$

Which is a contradiction. Hence, $\bullet$ has no identity element.

Since $\bullet$ has no identity element, we can not talk about inverse of an element. □

3.4. Example. Define the binary operation $\star$ on $\mathbb{N}$ as $m \star n = \max\{m, n\}$ $(m, n \in \mathbb{N})$. Examine the binary operation $\star$ for associativity, commutativity, identity element, and inverse.

SOLUTION. Mimic the Example 3.3. □

3.5. Example. Define the binary operation $\triangle$ on $\mathbb{Z}$ as

$$m \triangle n = m + n - mn \ \ (m, n \in \mathbb{Z}).$$

Examine the binary operation $\triangle$ for associativity, commutativity, identity element, and inverse.

SOLUTION. For $l, m, n \in \mathbb{Z}$,

$$\begin{aligned}(l \triangle m) \triangle n &= (l + m - lm) \triangle n \\ &= l + m - lm + n - (l + m - lm)n \\ &= l + m - lm + n - ln - mn + lmn;\end{aligned}$$

on the other hand,

$$\begin{aligned}l \triangle (m \triangle n) &= l \triangle (m + n - mn) \\ &= l + m + n - mn - l(m + n - mn) \\ &= l + m + n - mn - lm - ln + lmn \\ &= l + m - lm + n - ln - mn + lmn.\end{aligned}$$

i.e. $(l \triangle m) \triangle n = l \triangle (m \triangle n)$. Thus $\triangle$ is associative.

Since $m \triangle n = m + n - mn = n + m - nm = n \triangle m$ for all $m, n \in \mathbb{Z}$, $\triangle$ is commutative.

Clearly, $0 \in \mathbb{Z}$ be an identity element for $\triangle$. Because for any $m \in \mathbb{Z}$,

$$m \triangle 0 = m + 0 - 0 = m \quad \text{and} \quad 0 \triangle m = 0 + m - 0 = m.$$

Let $m \in \mathbb{Z}$, and let $n \in \mathbb{Z}$ be an inverse of m, then

$$m \triangle n = 0 \ \Rightarrow \ m + n - mn = 0 \ \Rightarrow \ m + n = mn.$$

Which is true only, if $m = n = 0$ or 2. Thus 0 and 2 are the only invertible elements of $\mathbb{Z}$ w.r.t. $\triangle$. Note that, $0^{-1} = 0$ and $2^{-1} = 2$. □

3.6. Example. Define the binary operation $\oplus$ on $M_2(\mathbb{R})$ as

$$P \oplus Q = P + Q \ \ (P, Q \in M_2(\mathbb{R})).$$

Examine the binary operation $\oplus$ for associativity, commutativity, identity element, and inverse.

SOLUTION. We know that if $P, Q, R \in M_n(\mathbb{R})$, then

$$(P \oplus Q) \oplus R = (P + Q) \oplus R = (P + Q) + R = P + (Q + R) = P \oplus (Q + R) = P \oplus (Q \oplus R);$$

and

$$P \oplus Q = P + Q = Q + P = Q \oplus P.$$

Thus $\oplus$ is associative and commutative.

Let $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$. Consider $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then $O \in M_n(\mathbb{R})$, and

$$P \oplus O = P + O = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = P.$$

Similarly, $O \oplus P = P$. Thus O is an identity element for $\oplus$.

Let $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$. Consider $-P = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, then $-P \in M_n(\mathbb{R})$, and

$$P \oplus (-P) = P + (-P) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O.$$

Similarly, $(-P) \oplus P = O$. Thus $-P$ is inverse of P for $\oplus$. □

3.7. Example. Define the binary operation $\bullet$ on $M_2(\mathbb{R})$ as $P \bullet Q = PQ$ $(P, Q \in M_2(\mathbb{R}))$. Examine the binary operation $\bullet$ for associativity, commutativity, identity element, and inverse.

SOLUTION. We know that if $P, Q, R \in M_n(\mathbb{R})$, then

$$(P \bullet Q) \bullet R = (PQ) \bullet R = (PQ)R = P(QR) = P \bullet (QR) = P \bullet (Q \bullet R).$$

Thus $\bullet$ is associative.

Let $P = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}$ and $Q = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$. Then

$$P \bullet Q = PQ = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix};$$

and

$$Q \bullet P = QP = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}.$$

i.e. $P \bullet Q \neq Q \bullet P$. Thus $\bullet$ is not commutative.

Let $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$. Consider $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $I_2 \in M_n(\mathbb{R})$, and

$$P \bullet I_2 = PI_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = P.$$

Similarly, $I_2 \bullet P = P$. Thus I_2 is an identity element for $\bullet$.

Let $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$. If $|P| \neq 0$, then consider P^{-1}. Clearly $P^{-1} \in M_n(\mathbb{R})$, and

$$P \bullet P^{-1} == PP^{-1} = I_2 \quad \text{and} \quad P^{-1} \bullet P == P^{-1}P = I_2.$$

Thus P^{-1} is inverse of P for $\bullet$. If $|P| = 0$, then the inverse of P does not exist, i.e. P is singular if $|P| = 0$. □

3.8. Definition. Addition Modulo n

Let n be a fixed positive integer, and let $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$. Let $\oplus_n$ be the operation *addition modulo n* defined on $\mathbb{Z}_n$ as: for $[a], [b] \in \mathbb{Z}_n$

$$[a] \oplus_n [b] = [a + b] = \text{remainder when } a + b \text{ is divided by } n.$$

3.9. Definition. Multiplication Modulo n

Let n be a fixed positive integer, and let $\mathbb{Z}_n = \{\{[0], [1], [2], \ldots, [n-1]\}$. Let $\odot_n$ be the operation *multiplication modulo n* defined on $\mathbb{Z}_n$ as: for $[a], [b] \in \mathbb{Z}_n$

$$[a] \odot_n [b] = [ab] = \text{remainder when } ab \text{ is divided by } n.$$

3.10. Example. Show that $\oplus_n$ and $\odot_n$ defined on $\mathbb{Z}_n$ are a binary operations.

Solution. When a non-negative integer is divided by n, the remainder is one of the n numbers, $0, 1, 2, \ldots, n-1$. Therefore, for each pair $[a], [b] \in \mathbb{Z}_n$, $[a] \oplus_n [b]$ and $[a] \odot_n [b]$ are both elements of $\mathbb{Z}_n$. i.e. each of these is a binary operation on $\mathbb{Z}_n$. □

3.11. Example. Show that there are exactly n^{n^2} binary operations on a set containing n elements.

Solution. If the set A contains n elements then the set $A \times A$ contains n^2 elements. Now total number of elements from $A \times A$ to A is n^{n^2}, i.e. the number of binary operations on A is n^{n^2}. □

3.12. Theorem. *Uniqueness of Identity*

There can be at most one identity element for a binary operation $*$ on A.

PROOF. If possible, suppose e and e' are two identity elements for binary operation $*$ on A. Now e being an identity element, we have

$$e * e' = e'.$$

Similarly, e' being an identity element, we have

$$e * e' = e.$$

Thus $e = e * e' = e'$. i.e. $e = e'$. □

3.13. Theorem. *Uniqueness of Inverse*

If the binary operation $*$ on A with identity e is associative, then a given element $a \in A$ can have at most one inverse.

PROOF. If b and c are inverses of a in A, then we have,

$$b * a = a * b = e \text{ and } c * a = a * c = e.$$

Now,

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

This completes the proof. □

3.14. Theorem. $(a^{-1})^{-1} = a$

Let $*$ be an associative binary operation on A. If $a \in A$ is non-singular, then its inverse a^{-1} is also non-singular and $(a^{-1})^{-1} = a$.

PROOF. Here a being non-singular,

$$a * a^{-1} = e = a^{-1} * a.$$

This shows that a^{-1} is also non-singular and $(a^{-1})^{-1} = a$. □

3.15. Theorem. *Socks-Shoes Property*

Let $*$ be an associative binary operation on A. If $a, b \in A$ are non-singular, then $a * b$ is also non-singular and $(a * b)^{-1} = b^{-1} * a^{-1}$.

PROOF. Here a and b being non-singular, a^{-1} and b^{-1} exist. Using associativity of $*$,

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1}) &= a*[b*(b^{-1}*a^{-1})]\\ &= a*[(b*b^{-1})*a^{-1}]\\ &= a*[e*a^{-1}]\\ &= a*a^{-1}\\ &= e.\end{aligned}$$

Similarly, we have $(b^{-1}*a^{-1})*(a*b) = e$. Hence by definition $(a*b)^{-1} = b^{-1}*a^{-1}$. □

1.4. Cancelation Law

For $m, n, p \in \mathbb{Z}$, $m + n = m + p \quad \Rightarrow \quad n = p$. Moreover if $m \neq 0$, then $mn = mp \quad \Rightarrow \quad n = p$. It is easy to show that a similar result does not hold for binary operation of Examples 1.4 and 1.5. This observation leads us to the following definition:

4.1. Definition.

Suppose $*$ is a binary operation on A and $a \in A$. If for every $b, c \in A$, $b*a = c*a$ and $a*b = a*c$ together imply $b = c$, then a is called a ***cancelable element*** for $*$ in A.

4.2. Definition.

A binary operation $*$ on A is said to satisfy the ***cancelation law*** if each element $a \in A$ is cancelable for $*$ in A.

4.3. Definition.

If for every $a, b, c \in A$

$$a*b = a*c \quad \Rightarrow \quad b = c$$

is satisfied then we say that $*$ satisfies ***left cancelation*** law in A.

4.4. Definition.

If for every $a, b, c \in A$

$$b*b = c*a \quad \Rightarrow \quad b = c$$

is satisfied then we say that $*$ satisfies ***right cancelation*** law in A.

4.5. Example. Suppose $*$ is a binary operation on A and $a \in A$. Define mappings $L_a : A \to A$ and $R_a : A \to A$ as follows:

$$L_a(x) = a * x \quad \text{and} \quad R_a(x) = x * a \ \ (x \in A)$$

(1) Show that the mappings L_a and R_a are both one-one iff a is cancelable for $*$.
(2) If $*$ is associative and a is non-singular, then show that
  (a) a is cancelable for $*$ in A
  (b) mappings L_a and R_a are one-one correspondence.

SOLUTION. (1) Suppose a is cancelation for $*$. Let $b, c \in A$ such that

$$L_a(b) = L_a(c) \ \Rightarrow \ a * b = a * c \ \Rightarrow \ b = c \ \ (\because \ a \text{ is cancelable for } *).$$

i.e. L_a is one-one. Similarly we can prove that R_a is one-one.
Conversely, suppose L_a and R_a are one-one mappings. Let $a, b, c \in A$ such that

$$\begin{aligned} & a * b = a * c \text{ and } b * a = c * a \\ \Rightarrow \ & L_a(b) = L_a(c) \text{ and } R_a(b) = R_a(c) \\ \Rightarrow \ & b = c \quad (\because \ L_a \text{ and } R_a \text{ are one-one}). \end{aligned}$$

i.e. a is cancelable for $*$.
(2) Suppose $*$ is associative, and a is non-singular.
(a) For $a, b, c \in A$, we have

$$\begin{aligned} a * b = a * c \ & \Rightarrow \ a^{-1} * (a * b) = a^{-1} * (a * c) \\ & \Rightarrow \ (a^{-1} * a) * b = (a^{-1} * a) * c \quad (\because * \text{ is associative}) \\ & \Rightarrow \ b = c; \end{aligned}$$

and,

$$\begin{aligned} b * a = c * a \ & \Rightarrow \ (b * a) * a^{-1} = (c * a) * a^{-1} \\ & \Rightarrow \ b * (a * a^{-1}) = c(*a * a^{-1}) \quad (\because * \text{ is associative}) \\ & \Rightarrow \ b = c. \end{aligned}$$

i.e. a is cancelable for $*$ in A.
(b) Since $*$ is associative, and a is non-singular by $(2(a))$, a is cancelable for $*$ in A, and hence by (1), L_a is one-one. Now we show that, L_a is onto. For that, let $b \in A$, then $a^{-1} * b \in A$ and

$$L_a(a^{-1} * b) = a * (a^{-1} * b) = (a * a^{-1}) * b = b.$$

i.e. L_a is one-one correspondence. Similarly, R_a is one-one correspondence. □

1.5. Exercise

(1) For each binary operation $*$ defined below, determine wether it is commutative and wether it is associative:

(a) on $\mathbb{Z}$, $a * b = a - b$
(b) on $\mathbb{Q}$, $a * b = ab + 2$
(c) on $\mathbb{Q}$, $a * b = ab/3$
(d) on $\mathbb{Q}$, $a * b = a$
(e) on $\mathbb{R}$, $a * b = a + b + ab$
(f) on $\mathbb{N}$, $a * b = a^2 + b^2$
(g) on $\mathbb{Q}$, $a * b = 1 + ab$
(h) on $\mathbb{N}$, $a * b = a^b$
(i) on $\mathbb{N}$, $a * b = 2^{ab}$

(2) On $\mathbb{Z} \times \mathbb{Z}$, define the binary operation $*$ by

$$(a, b) * (c, d) = (ac, bc + d).$$

Examine $*$ for commutativity, associativity, and identity element.

(3) For each of the following binary operations on $\mathbb{R}$, examine wether or not it is commutative, associative, and wether or not it has an identity element. For $x, y \in \mathbb{R}$,

(a) $x * y = x + y - 3$
(b) $x * y = 2x + 2y$
(c) $x * y = \dfrac{x + y}{2}$
(d) $x * y = \min\{x, 2\}$
(e) $x * y = 7xy$
(f) $x * y = xy + 1$
(g) $x * y = 10$

(4) Prove that: there can be at most one identity element for a binary operation $*$ on A.
(5) If the binary operation $*$ on A with identity e is associative, then show that for a given element $a \in A$ can have at most one inverse.
(6) Suppose $\triangle$ is an associative binary operation on A and $b \in A$. If a binary operation $*$ is defined on A as $x * y = x \triangle b \triangle y$ $(x, y \in A)$, then show that $*$ is also associative in A.
(7) Let $S = \{a, b, c, d\}$ and $*$ be a commutative binary operation on S. Complete the missing entries in the following table.

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

Chapter 2

Groups

2.1. Definition and Examples of Group

1.1. Definition. Group

A non-empty set G with a binary operation $*$ is said to be a ***group*** with respect to $*$ if the following conditions hold good:

G1. *Associativity.* For all $a, b, c \in G$,

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

G2. *Identity.* There exist an element $e \in G$, called the ***identity*** (or **the neutral element**), such that

$$a * e = e * a = a \quad \text{for all } a \in G.$$

G3. *Inverse.* For each $a \in G$, there exists $b \in G$, called the ***inverse*** of a, such that

$$a * b = b * a = e.$$

1.2. Remarks.

- ✓ In words, then, a group is a set together with an associative operation such that there is an identity, every element has an inverse, and any pair of elements can be combined without going outside the set. Notice that if a is the inverse of b, then b is the inverse of a.
- ✓ Now onwards, when we say that G is a group, we will take it for granted that there is a binary operation $*$ on G satisfying conditions $G1, G2$ and $G3$. In fact, the condition of a group G

depends on both (1) the non empty set G and (2) the binary operation on G satisfying $G1, G2$, and $G3$ and hence the notation of the form $(G, *)$ will be more appropriate for it. But if there is no ambiguity about the binary operation, we will denote the group simply by G.

✓ Now onwards, we will denote binary operation by $\cdot$ instead of $*$.

Now we take some examples of Group.

1.3. Example. The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, and the set of real numbers $\mathbb{R}$ are all groups under ordinary addition. In each case, the identity is 0 and the inverse of a is $-a$.

1.4. Example. The set of integers $\mathbb{Z}$ under ordinary multiplication is not a group. Since the number 1 is the identity, property 3 fails. For example, there is no integer b such that $5b = 1$.

1.5. Example. The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication. Note that 1 is the identity, and -1 is its own inverse, whereas the inverse of i is $-i$, and vice versa.

1.6. Example. The set $\mathbb{Q}^+$ of positive rationals is a group under ordinary multiplication. The identity is 1 and inverse of any a is $1/a = a^{-1}$.

1.7. Example. The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} \cdot \sqrt{2} = 2 \notin S$, so S is not closed under multiplication.

1.8. Example. A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is called a 2×2 matrix. The set of all 2×2 matrices with real entries is a group under componentwise addition. That is,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

1.9. Example. The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in $\mathbb{Z}_n$, the inverse of j is $n - j$. This group is usually referred to as the group of integers modulo n.

As we have seen, the real numbers, the 2×2 matrices with real entries, and the integers modulo n are all groups under the appropriate addition. But what about multiplication? In each case, the existence of some elements that do not have inverses prevents the set from being a group under the usual multiplication. However, we can form a group in each case by simply throwing out the rascals. Examples 8, 9, and 11 illustrate this.

1.10. Example. The set $\mathbb{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

Notation: Let $M_n(\mathbb{R})$ be the collection of all $n \times n$ real matrices and for $A \in M_n(\mathbb{R})$, $|A|$ denote the determinant of A.

1.11. Example. Show that: the set $GL(2,\mathbb{R}) := \{A \in M_2(\mathbb{R}) : |A| \neq 0\}$ is a group under matrix multiplication.

SOLUTION. Let $A, B \in GL(2,\mathbb{R})$ with $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$. Then

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

and $|AB| = |A||B| \neq 0$. Thus $AB \in GL(2,\mathbb{R})$. i.e. $GL(2,\mathbb{R})$ is closed under matrix multiplication.
Since matrix multiplication is associative, for $A, B, C \in GL(2,\mathbb{R})$, we have $A(BC) = (AB)C$. Hence $G2$ is satisfy.
Clearly, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ is identity; and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$ is

$$\begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}.$$

Thus $G2$ and $G3$ are satisfy. i.e. $GL(2,\mathbb{R})$ is a group under matrix multiplication. This very important group is called the ***general linear group*** of 2×2 matrices over $\mathbb{R}$. □

1.12. Example.

(1) Show that: the set $GL(2,\mathbb{Q}) := \{A \in M_2(\mathbb{Q}) : |A| \neq 0\}$ is a group under matrix multiplication.

(2) Show that: the set $GL(2,\mathbb{C}) := \{A \in M_2(\mathbb{C}) : |A| \neq 0\}$ is a group under matrix multiplication.

SOLUTION. Mimic the Example 1.11. □

1.13. Example. $M_2(\mathbb{R})$ is not a group under the matrix multiplication. Inverses do not exist when the determinant is 0.

1.14. Example. Show that: the set $SL(2,\mathbb{R}) := \{A \in M_2(\mathbb{R}) : |A| = 1\}$ is a group under matrix multiplication. The set of all 2×2 matrices with determinant 1 with entries from $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), or $\mathbb{C}$ (complex numbers), group under matrix multiplication. This group is called the special linear group of 2×2 matrices over $bq, \mathbb{R}$ or $\mathbb{C}$, respectively.

SOLUTION. Let $A, B \in SL(2,\mathbb{R})$ with $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$. Then

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

and $|AB| = |A||B| = 1 \cdot 1 = 1$. Thus $AB \in SL(2,\mathbb{R})$. i.e. $SL(2,\mathbb{R})$ is closed under matrix multiplication.
Since matrix multiplication is associative, for $A, B, C \in SL(2,\mathbb{R})$, we have $A(BC) = (AB)C$. Hence $G2$ is satisfy.
Clearly, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2,\mathbb{R})$ is identity; and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{R})$ is

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad (\because ad - bc = 1).$$

Thus $G2$ and $G3$ are satisfy. i.e. $SL(2,\mathbb{R})$ is a group under matrix multiplication. This very important group is called the ***special linear group*** of 2×2 matrices over $\mathbb{R}$. □

1.15. Example.

(1) Show that: the set $SL(2,\mathbb{Q}) := \{A \in M_2(\mathbb{Q}) : |A| = 1\}$ is a group under matrix multiplication.
(2) Show that: the set $SL(2,\mathbb{C}) := \{A \in M_2(\mathbb{C}) : |A| = 1\}$ is a group under matrix multiplication.

SOLUTION. Mimic the Example 1.14. □

1.16. Example. The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not.

1.17. Example. The set of integers under subtraction is not a group, since the operation is not associative.

1.18. Example. Show that for a fixed given positive integer n, the set of n^{th} root of unity forms a group under multiplication.

SOLUTION. Let $n \in \mathbb{N}$ be given. Let R_n denote the set of n^{th} root of unity. Then $R_n = \{z \in \mathbb{C} : z^n = 1\}$.

$$\begin{aligned} z^n = 1 &\Rightarrow z^n = \cos 0 + i \sin 0 \\ &\Rightarrow z = (\cos 0 + i \sin 0)^n \\ &\Rightarrow z = (\cos(0 + 2k\pi) + i \sin(0 + 2k\pi))^n \ \ (k = 0, 1, 2, \ldots, n-1) \\ &\Rightarrow z_k = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) = e^{i(2k\pi/n)} = (e^{i(2\pi/n)})^k \end{aligned}$$

We write $z_1 = e^{i(2\pi/n)} = \rho$. Then, the set of n^{th} roots of unity is

$$R_n = \{1 = \rho^0, \rho^1, \rho^2, \ldots, \rho^{n-1}\}.$$

Now we will show that $(R_n, \cdot)$ is a group.

Let $a, b \in R_n$. If $a = \rho^i$ and $b = \rho^j$ for some $0 \leq i, j \leq n-1$, then $ab = \rho^i \rho^j = \rho^{i+j}$.

case 1: If $i + j \leq n$, then $ab = \rho^{i+j} \in R_n$.

case 2: If $i + j > n$, then $i + j = nq + r, 0 \leq r < n$. Thus

$$ab = \rho^{i+j} = \rho^{nq+r} = (\rho^n)^q \rho^r = 1^q \rho^r = \rho^r \in R_n.$$

i.e. R_n is closed under multiplication.

G1. R_n being a subset of $\mathbb{C}$, multiplication is associative.

G2. $1 \in R_n$ becomes an identity element for multiplication.

G3. Let $a \in R_n$, if $a = \rho^j \in R_n, 0 \leq i < n$, then $b = \rho^{n-j} \in R_n$. Also,

$$ab = \rho^j \rho^{n-j} = \rho^{j+n-j} = \rho^n = 1,$$

similarly, $ba = 1$. i.e. b is an inverse of a. □

1.19. Remarks.

- ✓ For $n = 2$, $R_2 = \{1, -1\}$.
- ✓ For $n = 3$, $R_3 = \{1, \omega, \omega^2\}$ where $\omega = \dfrac{-1 + i\sqrt{3}}{2}$.
- ✓ For $n = 4$, $R_4 = \{1, -1, i, -i\}$.

1.20. Example. Let $\mathbb{R}^n := \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{R}, 1 \leq i \leq n\}$. Define $+$ on $\mathbb{R}^n$ as $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$. Show that $(\mathbb{R}^n, +)$ is a group.

SOLUTION. Given that $\mathbb{R}^n := \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{R}, 1 \leq i \leq n\}$. Let $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n), c = (c_1, c_2, \ldots, c_n) \in \mathbb{R}^n$. Then

$$a+b = (a_1, a_2, \ldots, a_n)+(b_1, b_2, \ldots, b_n) = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n) \in \mathbb{R}^n,$$

as $a_i + b_i \in \mathbb{R}, 1 \leq i \leq n$. i.e. $\mathbb{R}^n$ is closed under $+$.

$$\begin{aligned}
[a + b] + c &= [(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)] + (c_1, c_2, \ldots, c_n) \\
&= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) + (c_1, c_2, \ldots, c_n) && \text{(by definition of } +) \\
&= \Big((a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \ldots, (a_n + b_n) + c_n\Big) && \text{(by definition of } +) \\
&= \Big(a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \ldots, a_n + (b_n + c_n)\Big) && (+\text{is associative in } \mathbb{R}) \\
&= (a_1, a_2, \ldots, a_n) + \Big((b_1 + c_1), (b_2 + c_2), \ldots, (b_n + c_n)\Big) && \text{(by definition of } +) \\
&= (a_1, a_2, \ldots, a_n) + [(b_1, b_2, \ldots, b_n) + (c_1, c_2, \ldots, c_n)] && \text{(by definition of } +) \\
&= a + [b + c]
\end{aligned}$$

i.e. G1 is satisfied. Consider $o = \underbrace{(0, 0, \ldots, 0)}_{n \text{ times}}$. Then

$$a + o = (a_1, a_2, \ldots, a_n) + (0, 0, \ldots, 0) = (a_1, a_2, \ldots, a_n).$$

i.e. $0 = (0, 0, \ldots, 0)$ is an identity for $+$. i.e. G2 is satisfied.
Inverse of $a = (a_1, a_2, \ldots, a_n)$ is $-a = (-a_1, -a_2, \ldots, -a_n) \in \mathbb{R}^n$. i.e. G3 is satisfied. □

1.21. Example. Let $n \in \mathbb{N}$. Show that $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, the set of integers mod n, is a group under the binary operation $\oplus_n$.

SOLUTION. When a non-negative integer is divided by n, the remainder is one of the n numbers, $0, 1, 2, \ldots, n-1$. Therefore, for each pair $[a], [b] \in \mathbb{Z}_n$, $[a] \oplus_n [b]$ is an element of $\mathbb{Z}_n$. i.e. $\oplus_n$ is a binary operation on $\mathbb{Z}_n$.
G1. *Associativity.* Let $[a], [b], [c] \in \mathbb{Z}_n$. we have to show that

$$([a] \oplus_n [b]) \oplus_n [c] = [a] \oplus_n ([b] \oplus_n [c]).$$

By division algorithm,

$$a + b = d_1 n + r_1, \quad \text{where } 0 \leq r_1 < n.$$

This means

$$[a] \oplus_n [b] = [a + b] = [r_1].$$

Again, by division algorithm,

$$r_1 + c = d_2 n + r_2, \quad \text{where } 0 \leq r_2 < n,$$

and this means

$$[r_1] \oplus_n [c] = [r_1 + c] = r_2.$$

Hence

$$([a] \oplus_n [b]) \oplus_n [c] = [r_1] \oplus_n [c] = r_2. \tag{1.21.1}$$

Similarly, suppose

$$\begin{aligned} b + c &= d_3 n + r_3, \quad \text{where } 0 \leq r_3 < n, \\ a + r_3 &= d_4 n + r_4, \quad \text{where } 0 \leq r_4 < n. \end{aligned}$$

Then

$$[a] \oplus_n ([b] \oplus_n [c]) = [a] \oplus_n [b+c] = [a] \oplus_n [r_3] = [a+r_3] = [r_4]. \tag{1.21.2}$$

It follows from (1.21.1) and (1.21.2) that in order to prove the associativity of $\oplus_n$ we have to show that $r_2 = r_4$. Now,

$$r_2 = r_1 + c - d_2 n = (a + b - d_1 n) + c - d_2 n = (a + b + c) - (d_1 + d_2)n,$$

which shows that r_2 is the reminder when $a + b + c$ is divided by n. Also,

$$r_4 = a + r_3 - d_4 n = a + (b + c - d_3 n) - d_4 n = (a + b + c) - (d_3 + d_4)n,$$

which shows that r_4 is the reminder when $a + b + c$ is divided by n. Thus $r_2 = r_4$. i.e. G1 is satisfy.

G2. *Identity.* If $[a] \in \mathbb{Z}_n$, then $0 \leq a < n$. Hence when a is divided by n, the remainder is a itself. Thus we can write

$$[a] \oplus_n [0] = [a + 0] = [a] \ \ ([a] \in \mathbb{Z}_n).$$

This shows that 0 is an identity for $\oplus_n$. i.e. G2 is satisfy.

G3. *Inverse.* Let $[a] \in \mathbb{Z}_n, a \neq 0$.

$$\begin{aligned} [a] \in \mathbb{Z}_n \setminus \{[0]\} &\Rightarrow 0 < a < n \\ &\Rightarrow 0 > -a > -n \\ &\Rightarrow n > n - a > 0 \\ &\Rightarrow [n - a] \in \mathbb{Z}_n. \end{aligned}$$

Also,

$$[a] \oplus_n [n-a] = \text{the remainder when } a+n-a(=n) \text{ is divided by } n = 0.$$

i.e. the inverse of $[a]$ is $[n-a]$. Note that the inverse of $[0]$ is $[0]$.
Thus G1, G2, G3 are satisfy. i.e. $(\mathbb{Z}_n, \oplus_n)$ is a group. □

1.22. Example. Let $p \in \mathbb{N}$ be a prime number. Then $\mathbb{Z}_p = \{[1], [2], \ldots, [n-1]\}$, the set of integers mod n, is a group under the binary operation $\odot_n$.

1.23. Theorem.

An element $[m] \in \mathbb{Z}_n$ has a multiplicative inverse iff $(m, n) = 1$.

1.24. Definition. Commutative or Abelian

Let $(G, *)$ be a group. G is said to be a ***commutative group*** or ***Abelian group*** if

$$a * b = b * a \ \ (a, b \in G).$$

Summary of Group Examples (F can be any of $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$)

Group	Operation	Form of Element	Identity	Inverse	Abelian
$\mathbb{Z}$	Addition	a	0	$-a$	Yes
$\mathbb{Q}$	Addition	$\frac{a}{b}$	0	$-\frac{a}{b}$	Yes
$\mathbb{R}$	Addition	a	0	$-a$	Yes
$\mathbb{Q}^+$	Multiplication	$\frac{a}{b}$	1	$\frac{b}{a}$	Yes
$\mathbb{R}^*$	Multiplication	x	1	$\frac{1}{x}$	Yes
$M_2(F)$	Matrix Addition	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$	Yes
$GL(2,F)$	Matrix Multiplication	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $ad-bc \neq 0$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$	No
$SL(2,F)$	Matrix Multiplication	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $ad-bc=1$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
$\mathbb{R}^n$	Componentwise Addition	$(a_1,\ldots,a_n)$	$(0,\ldots,0)$	$(-a_1,\ldots,-a_n)$	Yes
$\mathbb{Z}_n$	Addition modulo n	$[a]$	$[0]$	$[n-a]$	Yes
R_n	Multiplication	$\rho^k(\rho = e^{i(2\pi/n)}$ $\rho^n = 1)$	1	ρ^{n-k}	Yes

2.2. Elementary Properties of Group

2.1. Definition. Finite Group and its Order

A group G is said to be a ***finite group*** if the number of elements in G is finite. In this case, the number of elements in G is called the ***order*** of of G.

2.2. Definition. Infinite Group

A group G is said to be a ***infinite group*** if the number of elements in G is infinite.

2.3. Example. $(\mathbb{Z}_n, \oplus_n), (R_n, \cdot)$ and $(\{1,-1,i,-i\},\cdot)$ are examples of finite group. While $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(M_2(\mathbb{R}),+),GL(2,\mathbb{R}),SL(2,\mathbb{R})$ are examples of infinite group.

2.4. Theorem. *Uniqueness of the Identity*

In a group G, there is only one identity element.

PROOF. If possible, suppose e and e' are two identity elements in G. Now e being an identity element, we have

$$e * e' = e'.$$

Similarly, e' being an identity element, we have

$$e * e' = e.$$

Thus $e = e * e' = e'$. i.e. $e = e'$. □

2.5. Theorem. ***Cancellation***

In a group G, the right and left cancellation laws hold; that is, for $a, b, c \in G$

$$b * a = c * a \;\Rightarrow\; b = c, \text{ and } a * b = a * c \;\Rightarrow\; b = c.$$

PROOF. Suppose $b * a = c * a$. Let a^{-1} be an inverse of a. Then

$$\begin{aligned} b * a = c * a &\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1} \\ &\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1}) \quad (*\text{is associative }) \\ &\Rightarrow b * e = c * e \\ &\Rightarrow b = c. \end{aligned}$$

Similarly, we can show that $a * b = a * c \;\Rightarrow\; b = c$. □

2.6. Theorem. ***Uniqueness of the Inverse***

For each element a in a group G, there is a unique element b in G such that

$$a * b = b * a = e.$$

PROOF. Let $a \in G$. Suppose b and c are inverses of a in G, then we have,

$$b * a = a * b = e \text{ and } c * a = a * c = e.$$

Now,

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

This completes the proof. □

2.7. Theorem. ***Socks-Shoes Property***

Let G be a group . For $a, b \in G$,

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

PROOF. Let a^{-1} and b^{-1} be the inverses of a and b respectively. Using associativity of $*$, we have

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1}) &= a*[b*(b^{-1}*a^{-1})]\\ &= a*[(b*b^{-1})*a^{-1}]\\ &= a*[e*a^{-1}]\\ &= a*a^{-1}\\ &= e.\end{aligned}$$

Similarly, we have $(b^{-1}*a^{-1})*(a*b) = e$. Hence by definition $(a*b)^{-1} = b^{-1}*a^{-1}$. □

2.8. Theorem. ***Uniqueness of Solution***

Let G be a group, and $a, b \in G$. The equations $a*x = b$ and $y*a = b$ have unique solutions.

PROOF.

$$\begin{aligned}a*(a^{-1}*b) &= (a*a^{-1})*b && (*\text{is associative })\\ &= e*b && (\text{definition of } a^{-1})\\ &= b && (\text{property of } e)\end{aligned}$$

Thus $a^{-1}*b$ is a solution of $a*x = b$.
Uniqueness: Suppose $a*x = b$ have two solutions say x_1 and x_2. Then,

$$a*x_1 = b \text{ and } a*x_2 = b.$$

It follows that

$$a*x_1 = a*x_2 \;\Rightarrow\; x_1 = x_2 \text{ (cancellation law holds in } G).$$

Similarly, we can show that the equation $y*a = b$ have unique solution in G. □

2.3. Solved Examples

3.1. Example. Suppose $a, b \in G$. If $ab = ba$, then for each $n \in \mathbb{N}$

(1) $ab^n = b^n a$
(2) $(ab)^n = a^n b^n$

SOLUTION. We prove this theorem with the help of PMI (Principal of Mathematical Induction).
(1) Let $P(n) : ab^n = b^n a \ \ (n \in \mathbb{N})$. By assumption $ab = ba$, thus $P(1)$ is true. Assume that $P(k)$ is true. i.e.

$$ab^k = b^k a.$$

Now we prove that $P(k+1)$ is true.

$$\begin{aligned} ab^{k+1} &= a(b^k b) && (\text{ by definition of power}) \\ &= (ab^k)b && (\text{ associative law}) \\ &= (b^k a)b && (P(k) \text{ is true}) \\ &= b^k(ab) && (\text{ associative law}) \\ &= b^k(ba) && (\text{ by assumption}) \\ &= (b^k b)a && (\text{ associative law}) \\ &= b^{k+1}a && (\text{ by definition of power}) \end{aligned}$$

i.e. $P(k+1)$ is true. Since $P(1)$ is true, and $P(k)$ is true implies $P(k+1)$ is true. Thus by PMI, $P(n)$ is true for $n \in \mathbb{N}$.

(2) Let $P(n) : (ab)^n = a^n b^n \ \ (n \in \mathbb{N})$. Clearly $ab = ab$, thus $P(1)$ is true. Assume that $P(k)$ is true. i.e.

$$(ab)^k = a^k b^k.$$

Now we prove that $P(k+1)$ is true.

$$\begin{aligned} (ab)^{k+1} &= (ab)^k(ab) && (? \quad) \\ &= a^k b^k(ab) && (? \quad) \\ &= a^k(b^k a)b && (? \quad) \\ &= a^k(ab^k)b && (? \quad) \\ &= (a^k a)(b^k b) && (? \quad) \\ &= a^{k+1}b^{k+1} && (? \quad) \end{aligned}$$

i.e. $P(k+1)$ is true. Since $P(1)$ is true, and $P(k)$ is true implies $P(k+1)$ is true. Thus by PMI, $P(n)$ is true for $n \in \mathbb{N}$. □

3.2. Example. Suppose $a \in G$ and $m \in \mathbb{N}$. For each $n \in \mathbb{Z}$,
(1) $a^m a^n = a^{m+n}$
(2) $(a^m)^n = a^{mn}$

SOLUTION. Please Try your self.

□

3.3. Theorem.

Suppose G is a finite group of order n. For $a \in G$, there exists a positive integer $r \leq n$ such that $a^r = e$.

PROOF. Since $a^0, a^1, a^2, \ldots, a^n \in G$ and G has n elements, these $(n+1)$ elements can not be distinct, i.e. at least two of them must be equal. i.e.

$$a^i = a^j \text{ for some } i \text{ and } j \text{ with } 0 \leq i < j \leq n.$$

Hence

$$e = a^0 = a^i a^{-i} = a^j a^{-i} = a^{i-j}.$$

If $i - j = r$, then $1 \leq r \leq n$ and $a^r = e$. □

This result leads us the following definition.

3.4. Definition. Order of the Element

The order of an element a in a group G is the smallest positive integer n such that $a^n = e$. (In additive notation, this would be $na = e$.) If no such integer exists, we say that a has infinite order. The order of an element a is denoted by $O(a)$ or $|a|$.

So, to find the order of a group element g, you need only compute the sequence of products $a, a^2, a^3, \ldots$ until you reach the identity for the first time. The exponent of this product (or coefficient if the operation is addition) is the order of a. If the identity never appears in the sequence, then a has infinite order.

3.5. Remark.

✓ By definition, if $a^n = e$ for some positive integer n, then $O(a) \leq n$.

3.6. Theorem.

In a finite group, each element is of finite order.

PROOF. Suppose $O(G) = n$. For $a \in G$, by Theorem 3.3, there exists a positive integer $r \leq n$ such that $a^r = e$, i.e. $O(a) \leq r$. □

3.7. Example. Find the order of $[2], [5], [6]$, and $[7]$ in $\mathbb{Z}_{10}$.

SOLUTION.

$$1([2]) = [2]$$
$$2([2]) = [2] \oplus_{10} [2] = [4]$$
$$3([2]) = [2] \oplus_{10} [2] \oplus_{10} [2] = [4] \oplus_{10} [2] = [6]$$
$$4([2]) = [2] \oplus_{10} [2] \oplus_{10} [2] \oplus_{10} [2] = [6] \oplus_{10} [2] = [8]$$
$$5([2]) = [2] \oplus_{10} [2] \oplus_{10} [2] \oplus_{10} [2] \oplus_{10} [2] = [8] \oplus_{10} [2] = 0.$$

Thus the smallest positive integer such that $n[2](= [2]^n) = [0]$ is $n = 5$. Hence $O([2]) = 5$.

$$1([5]) = [5]$$
$$2([5]) = [5] \oplus_{10} [5] = [0].$$

Thus the smallest positive integer such that $n[5] = [0]$ is $n = 2$. Hence $O([5]) = 2$. Similarly, we can conclude that $O([6]) = 5$ and $O([7]) = 10$. □

3.8. Example. Consider $\mathbb{Z}$ under ordinary addition. Here every nonzero element has infinite order, since the sequence $a, 2a, 3a, \ldots$ never includes 0 when $a \neq 0$. Thus every nonzero element in $\mathbb{Z}$ is of infinite order, while order of 0 is 1.

3.9. Example. In any group, the order of the identity element is 1 (in fact, the converse is also true).

3.10. Example. Consider $R_4 = \{1, -1, i, -i\}$ with multiplication. Find order of each element of R_4.

SOLUTION. Since 1 is identity element $O(1) = 1$.

$(-1)^1 = -1,\ \ (-1)^2 = (-1) \cdot (-1) = 1 \quad \Rightarrow \quad O(-1) = 2.$

$(i)^1 = i,\ \ (i)^2 = -1,\ \ (i)^3 == -i,\ \ (i)^4 = 1 \quad \Rightarrow \quad O(i) = 4.$

$(-i)^1 = -i,\ \ (-i)^2 = -1,\ \ (-i)^3 == i,\ \ (-i)^4 = 1 \quad \Rightarrow \quad O(-i) = 4.$

□

3.11. Example. Let $\mathbb{Q}_0 = \mathbb{Q} \setminus \{0\}$. Define $a * b = \dfrac{ab}{2} \quad (a, b \in \mathbb{Q}_0)$. Then show that $(\mathbb{Q}_0, *)$ is a commutative group.

SOLUTION. Let $a, b \in \mathbb{Q}_0$. Since a, b are non zero rational number, $a * b = \dfrac{ab}{2}$ also becomes a non-zero rational number. i.e. $\mathbb{Q}_0$ is closed under $*$.

G1. For $a, b, c \in \mathbb{Q}_0$,

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4} = \frac{a(\frac{bc}{2})}{2} = a * (\frac{bc}{2}) = a * (b * c).$$

i.e. $*$ is associative.

G2. For identity element e,

$$a * e = a \quad \Rightarrow \quad \frac{ae}{2} = a \quad \Rightarrow \quad e = 2 \ \ (a \neq 0).$$

Also, for $a \in \mathbb{Q}_0$

$$a * 2 = \frac{2a}{2} = a \quad \text{and} \quad 2 * a = \frac{2a}{2} = a.$$

i.e. $e = 2$ is the identity for $\mathbb{Q}_0$.

G3. If c is an inverse of a, then

$$a * c = 2 \quad \Rightarrow \quad \frac{ac}{2} = 2 \quad \Rightarrow \quad c = \frac{4}{a}.$$

Also

$$a * \frac{4}{a} = \frac{4a}{2a} = 2 \quad \text{and} \quad \frac{4}{a} * a = \frac{4a}{2a} = 2.$$

i.e. each element $a \in \mathbb{Q}_0$ has inverse. Finally,

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a.$$

Thus, $(\mathbb{Q}_0, *)$ is a commutative group. □

3.12. Example. Show that $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$ is a commutative group under usual multiplication of two real numbers.

SOLUTION. Let $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in G$. Then $a, b, c, d \in \mathbb{Q}$ with $a^2 + b^2 \neq 0$ and $c^2 + d^2 \neq 0$. Also

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

clearly, $(ac + 2bd), (ad + bc) \in \mathbb{Q}$ as $a, b, c, d \in \mathbb{Q}$. Since $x \neq 0$ and $y \neq 0$, $xy \neq 0$. Thus

$$\begin{aligned} xy \neq 0 \quad &\Rightarrow \quad (ac + 2bd) + (ad + bc)\sqrt{2} \neq 0 \\ &\Rightarrow \quad (ac + 2bd) \neq 0 \quad \text{or} \quad (ad + bc)\sqrt{2} \neq 0 \\ &\Rightarrow \quad (ac + 2bd) \neq 0 \quad \text{or} \quad (ad + bc) \neq 0 \\ &\Rightarrow \quad (ac + 2bd)^2 \neq 0 \quad \text{or} \quad (ad + bc)^2 \neq 0 \\ &\Rightarrow \quad (ac + 2bd)^2 + (ad + bc)^2 \neq 0 \end{aligned}$$

i.e. $xy \in G$. Thus G is closed under multiplication.

G1. Since G is a subset of $\mathbb{R}$, multiplication is associative in G.
G2. For $e = 1 + 0\sqrt{2}$, $e \in G$ and

$$x * e = (a + b\sqrt{2})(1 + 0\sqrt{2}) = a + b\sqrt{2} = x$$
$$e * x = (1 + 0\sqrt{2})(a + b\sqrt{2}) = a + b\sqrt{2} = x.$$

i.e. $e = 1 + 0\sqrt{2}$ is the identity for G.

G3. If $x = a+b\sqrt{2} \in G$, then $a^2-2b^2 \neq 0$, and hence $z = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2} \in G$. And

$$xz = (a + b\sqrt{2})\Big(\frac{a - b\sqrt{2}}{a^2 - 2b^2}\Big) = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1 = 1 + 0\sqrt{2} = e.$$

Similarly, $zx = e$. i.e. each element $x \in G$ has inverse. Finally, since G is a subset of $\mathbb{R}$, multiplication is commutative in G. Thus G is a commutative group. □

3.13. Example. Show that the set G of mappings where

$$G = \{f_{ab} : \text{ for given } a, b \in \mathbb{R}, a \neq 0, f_{ab} : \mathbb{R} \to \mathbb{R} \text{ with } f_{ab}(x) = ax+b, x \in \mathbb{R}\}$$

is a group under composition of mappings.

Solution. If $f_{ab}, f_{cd} \in G$, then $f_{ab} : \mathbb{R} \to \mathbb{R}$ and $f_{cd} : \mathbb{R} \to \mathbb{R}$ with $a, c \neq 0$ and

$$f_{ab}(x) = ax + b \quad \text{and} \quad f_{cd}(x) = cx + d \quad x \in \mathbb{R}.$$

Now,

$$\begin{aligned}(f_{ab} \circ f_{cd})(x) &= f_{ab}(f_{cd}(x)) = f_{ab}(cx + d)\\ &= a(cx + d) + b = acx + ad + b\\ &= (ac)x + (ad + b) = px + q\end{aligned}$$

where $p = ac$ and $q = ad + b$, i.e. $f_{ab} \circ f_{cd} = f_{pq}$. Also, $a, c \neq 0$ implies $p = ac \neq 0$. Thus G is composition of mappings is a binary operation in G. The element of G being mappings on $\mathbb{R}$, the associative property holds in G. The mapping f_{10} acts as an identity element while the mapping $f_{(1/a)(-b/a)}$ is an inverse of f_{ab}. Thus G is a group under composition of mappings. □

3.14. Example. Show that $G = \{[1], [2], [3], [4]\}$ under multiplication modulo 5 is a group

Solution. The composition table under $\odot_5$ is

$\odot_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

From the composition table it is clear that G is closed under $\odot_5$.
G1. Each element appears only once in each row and each column, thus $\odot_5$ is associative.
G2. 1 is the identity element for $\odot_5$.
G3. $1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$. Thus $(G, \odot_5)$ is a group. □

3.15. Example. Show that for a given natural number n, the set

$$G = \{[a] \in \mathbb{Z}_n | (a, n) = 1\}$$

is a group under multiplication modulo n.

SOLUTION. Since $(1, n) = 1, [1] \in G$ i.e. G is non-empty subset of $\mathbb{Z}_n$. For

$$[a], [b] \in G \;\Rightarrow\; (a, n) = (b, n) = 1 \;\Rightarrow\; (ab, n) = 1.$$

If $ab < n$, then $[a] \odot_n [b] = [ab] \in G$. If $ab > n$, then by Euclid's algorithm,

$$ab = qn + r,\ 0 \leq r < n.$$

Thus

$$[a] \odot_n [b] = [ab] = [r] \in G.$$

i.e. G is closed under $\odot_n$. $G \subset \mathbb{Z}_n$ gives associative property of $\odot_n$. For, $[a] \in G$

$$[1] \odot_n [a] = [a] \odot_n [1] = [a].$$

i.e. $[1]$ is the identity in G. For $[a] \in G, (a, n) = 1$ and hence by Theorem 1.23, $[a]$ has multiplicative inverse in G. Thus G is a group. □

3.16. Example. Let G be a group. For any two elements $a, b \in G$, and $n \in \mathbb{Z}$. Prove that: $(aba^{-1})^n = ab^n a^{-1}$.

SOLUTION. First we prove this result for $n \in \mathbb{N}$. For that we will use PMI.
Let $P(n) : (aba^{-1})^n = ab^n a^{-1}$ $n \in \mathbb{N}$.

Clearly $aba^{-1} = aba^{-1}$, thus $P(1)$ is true. Assuume that $P(k)$ is true. i.e.

$$(aba^{-1})^k = ab^k a^{-1}$$

is true. Now we prove that $P(k+1)$ is true.

$$\begin{aligned}
(aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) && (? \quad) \\
&= (ab^k a^{-1})(aba^{-1}) && (? \quad) \\
&= (ab^k)(a^{-1}a)(ba^{-1}) && (? \quad) \\
&= (ab^k)e(ba^{-1}) && (? \quad) \\
&= (ab^k)(ba^{-1}) && (? \quad) \\
&= a(b^k b)a^{-1} && (? \quad) \\
&= ab^{k+1}a^{-1} && (? \quad)
\end{aligned}$$

i.e. $P(k+1)$ is true. Since $P(1)$ is true, and $P(k)$ is true implies $P(k+1)$ is true. Thus by PMI, $P(n)$ is true for $n \in \mathbb{N}$. Now if n be a negative integer, then $n = -m$, where $m \in \mathbb{N}$. Thus

$$\begin{aligned}
(aba^{-1})^n &= (aba^{-1})^{-m} && (n = -m) \\
&= ((aba^{-1})^m)^{-1} && \text{(by definition of power)} \\
&= (ab^m a^{-1})^{-1} && (m \in \mathbb{N}) \\
&= (a^{-1})^{-1}(b^m)^{-1}a^{-1} && ((ab)^{-1} = b^{-1}a^{-1}) \\
&= ab^{-m}a^{-1} \\
&= ab^n a^{-1} && (-m = n)
\end{aligned}$$

i.e. $(aba^{-1})^n = ab^n a^{-1} \quad n \in \mathbb{Z}$. □

3.17. Example. Let G be a group, and $a \in G$ such that $O(a) = n$. Then show that

(1) $O(a^p) \leq O(a), p \in \mathbb{Z}$
(2) $O(a^{-1}) = O(a)$
(3) if for a positive integer q, $(q, n) = 1$ then $O(a^q) = O(a)$
(4) $O(a) = O(bab^{-1})$ for $b \in G$.

Solution. (1) $e = e^p = (a^n)^p = a^{np} = (a^p)^n$, i.e. $O(a^p) \leq n = O(a)$.
(2) Give that $O(a) = n$, thus $a^n = e$. Now,

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$$

Suppose $m \in \mathbb{N}$, such that $m < n$ and $(a^{-1})^m = e$. Then,

$$(a^{-1})^m = e \;\Rightarrow\; (a^m)^{-1} = e \;\Rightarrow\; a^m = e^{-1} = e.$$

Which is a contradiction as $O(a) = n$ and $m < n$. This shows that n is the least positive integer such that $(a^{-1})^n = e$. Hence $O(a^{-1}) = n$. i.e. $O(a) = O(a^{-1})$.
(3) Since $(q, n) = 1$, there exists integers s, t such that $sq + tn = 1$. Now,

$$a = a^1 = a^{sq+tn} = a^{sq}a^{tn} = (a^q)^s(a^n)^t = (a^q)^s e^t = (a^q)^s.$$

Since $O(a^p) \leq O(a), p \in \mathbb{Z}$,

$$O(a) = O((a^q)^s) \leq O(a^q) \leq O(a).$$

i.e. $O(a) = O(a^q)$.
(4) We know that in a group, $(bab^{-1})^n = ba^nb^{-1}$. Now,

$$(bab^{-1})^n = e \;\Leftrightarrow\; ba^nb^{-1} = e \;\Leftrightarrow\; a^n = b^{-1}eb \;\Leftrightarrow\; a^n = e.$$

Hence $O(a) = O(bab^{-1})$. □

3.18. Example. Let G be a group, and $a, b \in G$. Show that $O(ab) = O(ba)$.

Solution. We know that for $x, y \in G$, $O(x) = O(yxy^{-1})$. Taking $x = ab$ and $y = b$, we have

$$O(ab) = O(b(ab)b^{-1}) = O(ba(bb^{-1})) = O(ba).$$

□

3.19. Example. If $a \in G$ is of order n, then $a^m = e$ for some integer m iff $n|m$.

Solution. Given that $O(a) = n$. Suppose $a^m = e$ for some integer n. By division algorithm

$$m = qn + r, \;\; 0 \leq r < n.$$

Hence

$$e = a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r.$$

If $r \neq 0$, then this implies that $n = O(a) \leq r$, a contradiction. Hence $r = 0$. i.e.

$$m = qn \;\Rightarrow\; n|m.$$

Conversely suppose $n|m$, then $m = kn$ for some integer k. Now

$$a^m = a^{kn} = (a^n)^k = e^k = e.$$

□

3.20. Example. If $a \in G$ is of order $n(> 1)$ and it is the only element of order n, then $n = 2$.

SOLUTION. Given that $O(a) = n$. We know that for $a \in G$, $O(a) = O(a^{-1})$. Thus we have $O(a) = O(a^{-1}) = n$. i.e. a and a^{-1} are two elements of the same order n. Hence by assumption, $a = a^{-1}$ or $a^2 = e$. Thus $O(a) \leq 2$. As $a \neq e$, $O(a) = 2$. □

3.21. Example. Let G be an abelian group, and $a, b \in G$ with $O(a) = m$ and $O(b) = n$. If $(m, n) = 1$, then $O(ab) = mn$.

SOLUTION. Suppose $O(ab) = t$. Then $a^m = b^n = (ab)^t = e$. Now,

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = ee = e.$$

Thus $t|mn$. Also,

$$\begin{aligned} a^t b^t = (ab)^t = e &\Rightarrow a^t = b^{-t} \\ &\Rightarrow a^{tm} = b^{-tm} \\ &\Rightarrow (a^m)^t = b^{-tm} \\ &\Rightarrow (e)^t = b^{-tm} \\ &\Rightarrow e = b^{-tm} \\ &\Rightarrow e = b^{tm} \end{aligned}$$

Thus $n|tm$. As $(m, n) = 1$, this gives $n|t$. Similarly $m|t$. As $(m, n) = 1$, we have

$$mn|t.$$

Thus $t = mn$. □

3.22. Example. Show that: A group G is abelian iff $(ab)^2 = a^2b^2$, $(a, b \in G)$.

SOLUTION. Let $a, b \in G$. Suppose G is abelian. Then

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2.$$

Conversely, suppose $(ab)^2 = a^2b^2$. Then

$$(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2$$

$$\begin{aligned} &\Rightarrow \quad a^{-1}(abab)b^{-1} = a^{-1}(a^2b^2)b^{-1} \\ &\Rightarrow \quad ba = ab. \end{aligned}$$

i.e. G is abelian. □

3.23. Example. If G is a group such that $(ab)^n = a^nb^n$, for three consecutive integer n for all $a, b \in G$, then show that G is abelian.

SOLUTION. We are given that for all $a, b \in G$,

$$(ab)^n = a^nb^n \tag{3.23.1}$$
$$(ab)^{n+1} = a^{n+1}b^{n+1} \tag{3.23.2}$$
$$(ab)^{n+2} = a^{n+2}b^{n+2} \tag{3.23.3}$$

From (3.23.1) and (3.23.2), we have

$$\begin{aligned} a^{n+1}b^{n+1} = (ab)^{n+1} &= (ab)^n(ab) \\ &= a^nb^n(ab) \\ a^n(ab^n)b &= a^n(b^na)b, \end{aligned}$$

using the cancelation laws,

$$ab^n = b^na. \tag{3.23.4}$$

Similarly from (3.23.2) and (3.23.2), we have

$$ab^{n+1} = b^{n+1}a. \tag{3.23.5}$$

From (3.23.4) and (3.23.4), we have

$$\begin{aligned} b^{n+1}a &= ab^{n+1} \\ b^n(ba) &= (ab^n)b \\ &= (b^na)b \\ &= b^n(ab) \\ ba &= ab. \end{aligned}$$

i.e. G is abelian. □

3.24. Example. If $a^2 = e$ for all $a \in G$, then G is abelian.

SOLUTION. Given that

$$a^2 = e \text{ for all } a \in G \quad \Rightarrow \quad a = a^{-1} \text{ for all } a \in G.$$

Now for $a, b \in G$,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Thus G is abelian. □

3.25. Example. If G is a finite group of even order then there exists at least one element $a \neq e$ in G such that $a = a^{-1}$.

SOLUTION. Suppose $O(G) = 2n$ and $G = \{e, a_1, a_2, \ldots, a_{2n-1}\}$. For each element $a_i \neq e$, we have its inverse a_i^{-1} in G. Consider the subset

$$A = \{a_i, a_i^{-1} : a_i \neq a_i^{-1}\}$$

of G. Then the number of elements in A is even and since $e \notin A$, the maximum number of elements in A can be 2n-2. Thus there must be at least one element $a \neq e$ such that $a \notin A$, i.e. $a = a^{-1}$. □

3.26. Example. Let G be a group, and $e \neq a \in G$ such that $O(a) = p$, where p is a prime number. Prove that $O(a^i) = p$ for each $a \leq i < p$.

SOLUTION. Let $1 \leq i < p$. Since $O(a) = p$,

$$(a^i)^p = (a^p)^i = e^i = e.$$

Hence we may assume $O(a^i) = m \leq p$. Suppose $m < p$. Thus

$$e = (a^i)^m = a^{im} \quad \Rightarrow \quad p|im.$$

$$\begin{aligned} e = (a^i)^m = a^{im} &\Rightarrow p|im \qquad (O(a) = p) \\ &\Rightarrow p|i \quad \text{or} \quad p|m \end{aligned}$$

which is not possible as $i < p$ and $m < p$. Thus $p = m$. i.e. $O(a^i) = m = p$. □

3.27. Example. Let G be a finite group. Prove that number of elements x of G such that $x^7 = e$ is odd.

SOLUTION. Let $e \neq x \in G$ such that $x^7 = e$. Since 7 is a prime number and $x \neq e$, $O(x) = 7$. Now by Example 3.26, $O(x^i) = p$ for each $1 \leq i \leq 6$. Thus, number of non identity elements x of G such that $x^7 = e$ is $6n$ for some positive integer n. Also $e^7 = e$, number of elements x of G such that $x^7 = e$ is $6n+1$ which is an odd number. □

2.4. Exercise

(1) Give two reasons why the set of odd integers under addition is not a group.

(2) Show that $\{[1],[2],[3]\}$ under multiplication modulo 4 is not a group but that $\{[1],[2],[3],[4],[5],[6]\}$ under multiplication modulo 7 is a group.

(3) Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2,\mathbb{Z}_{11})$.

(4) Show that the set $\{[5],[15],[25],[35]\}$ is a group under multiplication modulo 40. What is the identity element of this group?

(5) Let G be a group with the following property: Whenever $a,b,c \in G$ and $ab = ca \quad \Rightarrow \quad b = c$. Prove that G is Abelian. (Cross cancellation implies commutativity.)

(6) Suppose that G is a group with the property that for $a,b,c,d,x \in G$,

$$axb = cxd \quad \Rightarrow \quad ab = cd.$$

Prove that G is abelian. (Middle cancellation implies commutativity.)

(7) Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a,b \in G$.

(8) For any elements a and b from a group and any integer n, prove that $(aba^{-1})^n = ab^n a^{-1}$.

(9) Prove that the set $G = \{3^m 6^n : m,n \in \mathbb{Z}\}$ is a group under multiplication.

(10) Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

(11) Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian.

(12) Show that a group of order 5 is always commutative.

(13) Prove that the set of all 3×3 matrices with real entries of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ is a group under matrix multiplication. This group, sometimes called the *Heisenberg group* (after the Nobel Prizewinning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of quantum physics.)

(14) In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4.

(15) Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinant.

(16) If $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$, show that G is a commutative group under matrix addition.

(17) If $G_1 = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \quad \text{and} \quad a^2 + b^2 \neq 0 \right\}$ and $G_2 = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$ then show that both are is a commutative groups under matrix multiplication.

Chapter 3

Subgroups

3.1. Definition and Examples

1.1. Definition. Subgroup

If a subset H of a group G is itself a group under the operation of G, we say that H is a ***subgroup*** of G.

For any group G, $H_1 = \{e\}$ and $H_2 = G$ are always subgroup of G. Clearly, the study of these two subgroups will not be interesting. Both these two subgroups are called *improper* subgroups of a group G. A subgroup different from these two are called *proper* subgroup.

We use the notation $H \leq G$ to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. The subgroup $\{e\}$ is called the trivial subgroup of G.

1.2. Remark.
✓ It follows from the definition that if H is a subgroup of a group K and K is a subgroup of a group G, then H is also a subgroup of G. (Here it is assumed that K and G are groups under the same binary operations.) conversely if H and K are subgroups of G with $H \subset K$ then H becomes a subgroup of K too.

Now we take some examples of subgroups.

1.3. Example. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$. Similarly $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$ and $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$.

1.4. Example. $(\mathbb{Q}^+, \cdot)$ is a subgroup of $(\mathbb{R}^+, \cdot)$.

1.5. Example. Notice that $\mathbb{Z}_n$ under addition modulo n is not a subgroup of $\mathbb{Z}$ under addition, since addition modulo n is not the operation of $\mathbb{Z}$.

When determining whether or not a subset H of a group G is a subgroup of G, one need not directly verify the group axioms. The next three results provide simple tests that suffice to show that a subset of a group is a subgroup.

1.6. Theorem. ***One-Step Subgroup Test***

Let G be a group and H a nonempty subset of G. If
$$ab^{-1} \in H \text{ whenever } a, b \in H,$$
then H is a subgroup of G.
(In additive notation, if $a - b \in H$ whenever $a, b \in H$, then H is a subgroup of G.)

Proof. Given that H is a non empty subset of G and $ab^{-1} \in H$ whenever $a, b \in H$.
Claim: H is a subgroup of G.
We will show that H is closed under the binary operation which is on G, and satisfies all the three postulates $G1, G2$ and $G3$.
$G1$. If $a, b, c \in H$, then $a, b, c \in G$. i.e. $(ab)c = a(bc)$.
$G2$. By assumption if $a, b \in H$, then $ab^{-1} \in H$. In particular take $b = a$, then
$$ab^{-1} \in H \;\Rightarrow\; aa^{-1} \in H \;\Rightarrow\; e \in H.$$
i.e. H contains the identity element.
$G3$. Let $b \in H$. Since $a = e \in H$, by assumption
$$ab^{-1} \in H \;\Rightarrow\; eb^{-1} \in H \;\Rightarrow\; b^{-1} \in H.$$
i.e. H contains the inverse of each of its elements.
Finally, let $a, b \in H$. As proved above $b^{-1} \in H$, and hence by assumption
$$ab = a(b^{-1})^{-1} \in H.$$
i.e. H is closed under the binary operation which is defined on G. □

1.7. Example. Let G be an abelian group. If $H = \{x \in G : x^2 = e\}$ where e is the identity of G, then show that H is a subgroup of G.

SOLUTION. Since $e^2 = e$, $e \in H$. Thus H is non-empty. Let $x, y \in G$, then $x^2 = e$ and $y^2 = e$. Now, since G is abelian

$$(xy^{-1})^2 = x^2(y^{-1})^2 = x^2(y^2)^{-1} = ee^{-1} = e.$$

Thus $xy^{-1} \in G$. i.e. H is a subgroup of G. □

1.8. Example. Let G be an abelian group with identity e. If $H = \{x^2 : x \in G\}$, then show that H is a subgroup of G.

SOLUTION. Since $e \in G$, $e = e^2 \in H$. Thus H is non-empty. Let $a, b \in H$, then $a = x^2$ and $b = y^2$ for some $x, y \in G$. Now, as G is abelian

$$ab^{-1} = x^2(y^2)^{-1} = x^2(y^{-1})^2 = (xy^{-1})^2,$$

since G is a group and $x, y \in G$, we have $xy^{-1} \in G$. Thus $ab^{-1} \in H$. i.e. H is a subgroup of G. □

1.9. Theorem. ***Two-Step Subgroup Test***

Let G be a group and H a nonempty subset of G. Then H is a subgroup of G if
(1) $ab \in H$ whenever $a, b \in H$ (H is closed under the operation)
(2) $a^{-1} \in H$ whenever $a \in H$ (H is closed under taking inverses).

PROOF. By Theorem 1.6, it suffices to show that $a, b \in H$ implies ab^{-1}. So, we suppose that $a, b \in H$. By assumption, we also have $b^{-1} \in H$ as $b \in H$. Again by assumption, $ab^{-1} \in H$ as $a, b^{-1} \in H$. □

How do you prove that a subset of a group is not a subgroup? Here are three possible ways, any one of which guarantees that the subset is not a subgroup:

(1) Show that the identity is not in the set.
(2) Exhibit an element of the set whose inverse is not in the set.
(3) Exhibit two elements of the set whose product is not in the set.

1.10. Example. Let G be the group of nonzero real numbers under multiplication, $H = \{x \in G : x = 1 \text{ or } x \text{ is irrational }\}$ and $K = \{x \in G : x \geq 1\}$. Then H is not a subgroup of G, since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Also, K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$.

When dealing with finite groups, it is easier to use the following subgroup test.

1.11. Theorem. ***Finite Subgroup Test***

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

PROOF. In view of Theorem 1.9, we need only prove that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, then by assumption $a^2 = aa \in H$, $a^3 = a^2a \in H, \ldots, a^n \in H$ etc. i.e. $a, a^2, a^3, \ldots \in H$. Since H is finite,

$$a^r = a^s \text{ for some } r > s > 0 \quad \Rightarrow \quad a^{r-s} = e.$$

Now, $r - s > 0$ is a positive integer and $r - s - 1 \geq 0$. Hence both $a^{r-s} = e$ and a^{r-s-1} are elements of H. □

1.12. Theorem.

For any element a of a group G, the set $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

PROOF. Since $a = a^1 \in H$, H is non-empty. Let $a^m, a^n \in H$. Then $a^n(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in H$ as $n - m \in \mathbb{Z}$. Thus by one-step subgroup test H is a subgroup of G. □

For $a \in G$, the subgroup $H = \{a^n : n \in \mathbb{Z}\}$ of G is called the *cyclic subgroup* of G generated by a. In this case H is denoted by $H =< a >$. In the case that $G =< a >$, we say that G is cyclic and a is a generator of G.

1.13. Remark.
✓ If we have a group G and one member of G, then immediately by Theorem 1.12 we can generate a subgroup of G using the member of G.

1.14. Example. In $\mathbb{Z}_{10}$, $< [2] >= \{[2], [4], [6], [8], [0]\}$. Remember, a^n means na when the operation is addition.

1.15. Example. In $\mathbb{Z}$, $< -1 >= \mathbb{Z}$. Here each entry in the list

$$\ldots, -2(-1), -1(-1), 0(-1), 1(-1), 2(-1), \ldots$$

represents a distinct group element. Also note that $< 1 >= \mathbb{Z}$ as

$$\ldots, -2(1), -1(1), 0(1), 1(1), 2(1), \ldots$$

i.e. $\mathbb{Z} =< 1 >=< -1 >$.

1.16. Definition. Center of a Group

The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G : ax = xa \text{ for all } x \text{ in } G\}.$$

1.17. Theorem. *Center Is a Subgroup*

The center of a group G is a subgroup of G.

PROOF. Clearly, for any $x \in G$, $xe = x = ex$. i.e. $e \in Z(G)$. Thus $Z(G)$ is non-empty. To prove $Z(G)$ is a subgroup of G, we will use two-step test. Let $a, b \in Z(G)$. Then for any $x \in G$,

$$ax = xa \quad \text{and} \quad bx = xb.$$

Now,

$$\begin{aligned}
(ab)x &= a(bx) && \text{(associativity)} \\
&= a(xb) && (bx = xb) \\
&= (ax)b && \text{(associativity)} \\
&= (xa)b && (ax = xa) \\
&= x(ab) && \text{(associativity)}
\end{aligned}$$

i.e. $ab \in Z(G)$. Let $a \in Z(G)$. Then we have $ax = xa$.

$$\begin{aligned}
ax = xa &\Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} && \text{(multiplying both sides by} a^{-1}) \\
&\Rightarrow (a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1}) && \text{(associativity)} \\
&\Rightarrow exa^{-1} = a^{-1}xe \\
&\Rightarrow xa^{-1} = a^{-1}x.
\end{aligned}$$

i.e. $a^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup of G. □

1.18. Definition. Normalizer of a in G

Let a be a fixed element of a group G. The ***normalizer*** of a in G, $N(a)$, is the set of all elements in G that commute with a. In symbols,

$$N(a) = \{x \in G : xa = ax\}.$$

1.19. Theorem. $N(a)$ *Is a Subgroup*

For each a in a group G, the normalizer of a is a subgroup of G.

PROOF. Clearly, $ae = a = ea$. i.e. $e \in N(a)$. Thus $N(a)$ is non-empty. To prove $N(a)$ is a subgroup of G, we will use two-step test. Let $x, y \in N(a)$. Then, $ax = xa$ and $ay = ya$. Now,

$$\begin{aligned}(xy)a &= x(ya) && \text{(associativity)}\\ &= x(ay) && (ay = ya)\\ &= (xa)y && \text{(associativity)}\\ &= (ax)y && (ax = xa)\\ &= a(xy) && \text{(associativity)}\end{aligned}$$

i.e. $xy \in N(a)$. Let $x \in N(a)$. Then we have $ax = xa$.

$$\begin{aligned}ax = xa &\Rightarrow x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} && \text{(multiplying both sides by} x^{-1})\\ &\Rightarrow x^{-1}a(xx^{-1}) = (x^{-1}x)ax^{-1} && \text{(associativity)}\\ &\Rightarrow x^{-1}ae = eax^{-1}\\ &\Rightarrow x^{-1}a = ax^{-1}.\end{aligned}$$

i.e. $x^{-1} \in N(a)$. Thus $N(a)$ is a subgroup of G. □

1.20. Example. For a group G,

(1) $Z(G) = G$ iff G is abelian
(2) For an element $a \in G$, $a \in Z(G)$ iff $N(a) = G$.

SOLUTION. Please try your self. □

1.21. Theorem.

The intersection of two subgroups of a group is also a subgroup.

PROOF. Let H_1 and H_2 be the subgroups of a group G.
Claim: $H_1 \cap H_2$ is a subgroup of G.
Since H_1 and H_2 are subgroups of G, $e \in H_1$ and $e \in H_2$. Hence $e \in H_1 \cap H_2$. Thus $H_1 \cap H_2$ is non-empty. Let $a, b \in H_1 \cap H_2$.

$$\begin{aligned}a, b \in H_1 \cap H_2 &\Rightarrow a, b \in H_1 \text{ and } a, b \in H_2\\ &\Rightarrow ab^{-1} \in H_1 \text{ and } ab^{-1} \in H_2 && (H_1 \text{ and } H_2 \text{ are subgroups of } G)\\ &\Rightarrow ab^{-1} \in H_1 \cap H_2.\end{aligned}$$

Thus by one-step test, $H_1 \cap H_2$ is a subgroup of G. □

1.22. Theorem.

The intersection of an arbitrary family of subgroups of a group is also a subgroup.

PROOF. Let $C = \{H_\alpha : H_\alpha \text{ is a subgroup of } G, \alpha \in \Lambda\}$ be an arbitrary family of subgroups of G.
Claim: $\bigcap_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G.
Since for each $\alpha \in \Lambda$, H_α is a subgroup of G, $e \in H_\alpha$ for each $\alpha \in \Lambda$. Thus $e \in \bigcap_{\alpha\in\Lambda} H_\alpha$. i.e. $\bigcap_{\alpha\in\Lambda} H_\alpha$ is non-empty. Let $a, b \in \bigcap_{\alpha\in\Lambda} H_\alpha$.

$$\begin{aligned} a, b \in \bigcap_{\alpha\in\Lambda} H_\alpha &\Rightarrow a, b \in H_\alpha \text{ for each } \alpha \in \Lambda \\ &\Rightarrow ab^{-1} \in H_\alpha \text{ for each } \alpha \in \Lambda \quad (H_\alpha \text{ is a subgroups of } G) \\ &\Rightarrow ab^{-1} \in \bigcap_{\alpha\in\Lambda} H_\alpha. \end{aligned}$$

Thus by one-step test, $\bigcap_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G. □

1.23. Question. Prove or disprove:

(1) The union of two subgroups of a group is also a subgroup.
(2) The union of an arbitrary family of subgroups of a group is also a subgroup.
(3) If (1) and (2) are false, then can we have any condition(s) so that (1) and (2) becomes true.

3.2. Cosets and It's Properties

Our main aim is to prove the single most important theorem in finite group theory - Lagrange's Theorem. But first, we introduce a new and powerful tool for analyzing a group - the notion of a coset. This notion was invented by Galois in 1830, although the term was coined by G. A. Miller in 1910.

2.1. Definition. Congruent

Let H be a subgroup of a group G and let $a, b \in H$. We will say that a is ***congruent*** to b mod H and will write as

$$a \equiv b(\text{mod } H) \text{ if } ab^{-1} \in H.$$

The above relation defined in G is known as the ***congruent modulo*** H relation.

2.2. Example. Let $G = (\mathbb{Z}, +)$ and $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. For $a = 5$ and $b = 2$, $ab^{-1} = a - b = 5 - 2 = 3 \in 3\mathbb{Z}$, i.e. $5 \equiv 2(\text{mod } 3\mathbb{Z})$.

But For $a = 11$ and $b = -18$, $ab^{-1} = a - b = 11 - (-18) = 29 \in 3\mathbb{Z}$, i.e. $11 \not\equiv (-18) (\text{mod } 3\mathbb{Z})$.

2.3. Theorem. *Equivalence Relation*

The relation $a \equiv b (\text{mod } H)$ is equivalence relation in G.

PROOF. We will show that this relation is reflexive, symmetric and transitive.
reflexive: For $a \in G$, $aa^{-1} = e \in H$, i.e. $a \equiv a (\text{mod } H)$.
symmetric: For $a, b \in H$, if

$$\begin{aligned} a \equiv b (\text{mod } H) &\Rightarrow ab^{-1} \in H \\ &\Rightarrow (ab^{-1})^{-1} \in H \quad (H \text{ is a subgroup of } G) \\ &\Rightarrow ba^{-1} \in H \\ &\Rightarrow b \equiv a (\text{mod } H) \end{aligned}$$

transitive: For $a, b, c \in H$, if

$$\begin{aligned} a \equiv b (\text{mod } H) \text{ and } b \equiv c (\text{mod } H) &\Rightarrow ab^{-1} \in H \text{ and } bc^{-1} \in H \\ &\Rightarrow (ab^{-1})(bc^{-1}) \in H \qquad (H \text{ is a subgroup of } G) \\ &\Rightarrow a(b^{-1}b)c^{-1} \in H \qquad (\text{ associativity }) \\ &\Rightarrow ac^{-1} \in H \\ &\Rightarrow a \equiv c (\text{mod } H) \end{aligned}$$

□

2.4. Definition. Left and Right Cosets

If H is a subgroup of a group G, and if $a \in G$, then

$$aH = \{ah : h \in H\} \text{ and } Ha = \{ha : h \in H\}$$

respectively are said to be the ***left*** and ***right cosets*** of H ***with respect to*** a in the group G.

2.5. Remark.
✓ For group $(G, +)$, we will denote right coset Ha and left coset aH in G by $H + a$ and $a + H$ respectively.

2.6. Example. Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$ under addition. In the case that the group operation is addition, we use the notation $a + H$ instead

of aH. Then the cosets of H in $\mathbb{Z}_9$ are

$$\begin{aligned} 0+H &= \{0,3,6\} = 3+H = 6+H \\ 1+H &= \{1,4,7\} = 4+H = 7+H \\ 2+H &= \{2,5,8\} = 5+H = 8+H \end{aligned}$$

The observations raise many questions. When does $aH = bH$? Do aH and bH have any elements in common? When does $aH = Ha$? Which cosets are subgroups? Why are cosets important? The next lemma and theorem answer these questions. (Analogous results hold for right cosets.)

2.7. Theorem.

For each $a \in G$, $cl(a) = \{b \in G : b \equiv a(mod\ H)\} = Ha$.

Proof.

$$\begin{aligned} b \in cl(a) &\Rightarrow b \equiv a(mod\ H) \\ &\Rightarrow ba^{-1} \in H \\ &\Rightarrow ba^{-1} = h \text{ for some } h \in H \\ &\Rightarrow b = ha \in Ha \\ &\Rightarrow cl(a) \subset Ha. \end{aligned}$$

$$\begin{aligned} b \in Ha &\Rightarrow b = ha \text{ for some } h \in H \\ &\Rightarrow ba^{-1} = h \in H \\ &\Rightarrow b \equiv a(mod\ H) \\ &\Rightarrow b \in c(a) \\ &\Rightarrow Ha \subset cl(a). \end{aligned}$$

i.e. $cl(a) = Ha$. □

2.8. Theorem. ***Properties of Cosets***

Let H be a subgroup of G, and let a and b belong to G. Then,
(1) $eH = H$
(2) $a \in aH$
(3) $aH = H$ iff $a \in H$
(4) $aH = bH$ iff $a \in bH$
(5) $aH = bH$ or $aH \cap bH = \phi$
(6) $aH = bH$ iff $a^{-1}b \in H$
(7) $O(aH) = O(bH)$
(8) $aH = Ha$ iff $H = aHa^{-1}$
(9) aH is a subgroup of G iff $a \in H$

PROOF. (1) If $h \in H$, then $h = eh \in eH$. Thus $H \subset eH$. If $a \in eH$, then $a = eh$ for some $h \in H$. But $a = eh = h \in H$, i.e. $H \subset eH$. Thus $eH = H$.
(2) Since a can be written as $a = ae$, $a = ae \in aH$.
(3) We first suppose that $aH = H$. Then $a = ae \in aH = H$. i.e. $a \in H$. Next, we assume that $a \in H$. To prove that $aH = H$, we have to show that $aH \subset H$ and $H \subset aH$.

$$\begin{aligned} b \in aH &\Rightarrow b = ah \quad (\text{for some } h \in H) \\ &\Rightarrow b \in H \quad (a, h \in H \text{and H is a subgroup }) \\ &\Rightarrow aH \subset H \end{aligned}$$

Now, since $a \in H$, $a^{-1} \in H$ as H is a subgroup. Thus

$$\begin{aligned} h \in H &\Rightarrow a^{-1}h \in H \quad (a^{-1}, h \in H \text{and H is a subgroup }) \\ &\Rightarrow a(a^{-1}h) \in aH \\ &\Rightarrow (aa^{-1})h \in aH \\ &\Rightarrow h = eh \in aH \\ &\Rightarrow H \subset aH. \end{aligned}$$

i.e. $aH = H$.
(4) If $aH = bH$, then $a = ae \in aH = bH$. Conversely, if $a \in bH$ we have $a = bh$ where $h \in H$, and therefore $aH = (bh)H = b(hH) = bH$.

(5) Suppose $aH \cap bH \neq \phi$, then there exists $c \in aH \cap bH$. Then

$$\begin{aligned} c \in aH \cap bH &\Rightarrow c \in aH \text{ and } c \in bH \\ &\Rightarrow cH = aH \text{ and } cH = bH \quad (\text{By property 4}) \end{aligned}$$

$$\Rightarrow \quad aH = bH$$

(6) If $aH = bH$, then

$$\begin{aligned} b = be \in bH = aH \quad &\Rightarrow \quad b = ah \text{ for some } h \in H \\ &\Rightarrow \quad a^{-1}b = h \in H. \end{aligned}$$

Conversely, suppose $a^{-1}b \in H$, then $a^{-1}b = h_1$ for some $h_1 \in H$. Now,

$$\begin{aligned} c \in bH \quad &\Rightarrow \quad c = bh_2 \text{ for some } h_2 \in H \\ &\Rightarrow \quad c = ah_1h_2 \qquad\qquad (a^{-1}b = h_1 \Rightarrow b = ah_1) \\ &\Rightarrow \quad c = ah_1h_2 \in aH \\ &\Rightarrow \quad bH \subset aH. \end{aligned}$$

Next,

$$\begin{aligned} c \in aH \quad &\Rightarrow \quad c = ah_3 \text{ for some } h_3 \in H \\ &\Rightarrow \quad c = bh_1^{-1}h_3 \qquad\qquad (a^{-1}b = h_1 \Rightarrow a^{-1} = h_1b^{-1} \Rightarrow a = bh_1^{-1}) \\ &\Rightarrow \quad c = bh_1^{-1}h_3 \in bH \\ &\Rightarrow \quad aH \subset bH. \end{aligned}$$

Thus $aH = bH$.

(7) To prove that $O(aH) = O(bH)$, it suffices to define a one-to-one mapping from aH onto bH. Define $f : aH \to bH$ by $f(ah) = bh$.

f is one-to-one: suppose

$$\begin{aligned} f(ah_1) = f(ah_2) \quad &\Rightarrow \quad bh_1 = bh_2 \\ &\Rightarrow \quad h_1 = h_2 \quad (\text{ cancellation property}) \\ &\Rightarrow \quad ah_1 = ah_2. \end{aligned}$$

i.e. f is one-to-one.

f is onto: Let $bh_0 \in bH$. Since $h_0 \in H$, $ah_0 \in aH$. Then $f(ah_0) = bh_0$. Thus f is onto.

(8)

$$\begin{aligned} aH = Ha \quad &\Rightarrow \quad (aH)a^{-1} = (Ha)a^{-1} \\ &\Rightarrow \quad aHa^{-1} = H(aa^{-1}) \\ &\Rightarrow \quad aHa^{-1} = He \\ &\Rightarrow \quad aHa^{-1} = H. \end{aligned}$$

(9) If aH is a subgroup, then $e \in aH$. Clearly $e \in eH$, hence $aH \cap eH \neq \phi$. Thus by property 5, we have $aH = eH = H$. Thus from property

3, $a \in H$. Conversely, if $a \in H$, then again by property 3, we have $aH = H$. Since H is a subgroup, aH is also subgroup. □

Although most mathematical theorems are written in symbolic form, one should also know what they say in words. In the preceding lemma,

- ✓ property 2 says simply that the left coset of H containing a does contain a.
- ✓ Property 3 says that the H **absorbs** an element if and only if the element belongs to H.
- ✓ Property 4 shows that a left coset of H is uniquely determined by any one of its elements. In particular, any element of a left coset can be used to represent the coset.
- ✓ Property 5 says-and this is very important-that two left cosets of H are either identical or disjoint.
- ✓ Property 6 shows how we may transfer a question about equality of left cosets of H to a question about H itself and vice versa.
- ✓ Property 7 says that all left cosets of H have the same size.
- ✓ Property 8 is analogous to property 6 in that it shows how a question about the equality of the left and right cosets of H containing a is equivalent to a question about the equality of two subgroups of G.
- ✓ The last property of the lemma says that H itself is the only coset of H that is a subgroup of G.
- ✓ Note that properties 2, 5, and 7 of the lemma guarantee that the left cosets of a subgroup H of G partition G into blocks of equal size. Indeed, we may view the cosets of H as a partitioning of G into equivalence classes under the equivalence relation defined by $a \sim b$ if $aH = bH$.

The following theorem is analogue form of Theorem 2.8.

2.9. Theorem. ***Properties of Cosets (For Right Cosets)***

Let H be a subgroup of G, and let a and b belong to G. Then,
(1) $He = H$
(2) $a \in Ha$
(3) $Ha = H$ iff $a \in H$
(4) $Ha = Hb$ iff $a \in Hb$
(5) $Ha = Hb$ or $Ha \cap Hb = \phi$
(6) $Ha = Hb$ iff $ab^{-1} \in H$
(7) $O(Ha) = O(Hb)$
(8) $Ha = aH$ iff $H = aHa^{-1}$
(9) Ha is a subgroup of G iff $a \in H$

PROOF. See the proof of Theorem 2.8. □

3.3. Lagrange's Theoerm and Consequences

We are now ready to prove a theorem that has been around for more than 200 yearslonger than group theory itself! (This theorem was not originally stated in group theoretic terms.)

3.1. Theorem. *Lagranges Theorem:* $O(H)$ *Divides* $O(G)$

If G is a finite group and H is a subgroup of G, then $O(H)$ divides $O(G)$. Moreover, the number of distinct left (right) cosets of H in G is $\frac{O(G)}{O(H)}$.

PROOF. Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G. Then we have following:
(1) For each $a \in G$, we have $aH = a_iH$ for some i.
(2) By property of cosets $a \in aH$.
(3) Each member of G belongs to one of the cosets a_iH.

In symbols,

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH$$

Since two left cosets are either identical or disjoint, this union is disjoint, so that

$$\begin{aligned} O(G) &= O(a_1H) \cup O(a_2H) \cup \ldots \cup O(a_rH) \\ &= O(H) \cup O(H) \cup \ldots \cup O(H) \qquad (O(a_iH) = O(H)) \\ &= r\ O(H). \end{aligned}$$

i.e. $O(H)$ divides $O(G)$. Moreover,

$$\text{No of distinct left cosets of } H \text{ in } G = r = \frac{O(G)}{O(H)}.$$

□

We pause to emphasize that Lagrange's Theorem is a subgroup candidate criterion; that is, it provides a list of candidates for the orders of the subgroups of a group. Thus, a group of order 12 may have subgroups of order 12, 6, 4, 3, 2, 1, but no others. *Warning*! The converse of Lagranges Theorem is false. For example, a group of order 12 need not have a subgroup of order 6. We prove this later on.

A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group.

3.2. Definition. Index of a subgroup

The ***index*** of a subgroup H in G is the number of distinct left(right) cosets of H in G. This number is denoted by $i_G(H)$.

As an immediate consequence of the proof of Lagrange's Theorem, we have the following useful formula for index of a subgroup H in G.

3.3. Corollary. $i_G(H) = \frac{O(G)}{O(H)}$

If G is a finite group and H is a subgroup of G, then $i_G(H) = \frac{O(G)}{O(H)}$.

3.4. Corollary. $O(a)$ *Divides* $O(G)$

In a finite group, the order of each element of the group divides the order of the group.

PROOF. Let $a \in G$. If $O(a) = n$, then $H =< a >= \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$ is a subgroup of G and $O(H) = n$. Thus by Lagrange's Theorem

$$O(H)/O(G) \;\Rightarrow\; n/O(G) \;\Rightarrow\; O(a)/O(G).$$

□

3.5. Corollary. *Groups of Prime Order Are Cyclic*

A group of prime order is cyclic.

PROOF. Suppose that G is a group of prime order say p. Let $a \in G$ and $a \neq e$. Then $H =< a >$ is a cyclic subgroup of G. By Lagrange's Theorem,

$$O(H)/O(G) \;\Rightarrow\; O(H)/p \;\Rightarrow\; O(H) = 1 \text{ or } p.$$

If $O(H) = 1$, then $H = \{e\}$, a contradiction as $a \neq e$. Hence $O(H) = p = O(G)$. As $H \subset G$ and H and G have same number of finite elements, we have $G = H =< a >$. Thus a is cyclic group. □

3.6. Corollary. $a^{O(G)} = e$

Let G be a finite group, and let $a \in G$. Then, $a^{O(G)} = e$.

PROOF. Let $a \in G$. Then by Corollary, 3.4 $O(a)$ divides $O(G)$, i.e.

$$O(a)|O(G) \;\Rightarrow\; O(G) = kO(a) \;\; (\text{ for some } k \in \mathbb{N}).$$

Thus

$$a^{O(G)} = a^{kO(a)} = (a^{O(a)})^k = e^k = e.$$

□

3.7. Definition. Euler's Phi Function

The mapping $\phi : \mathbb{N} \to \mathbb{N}$ defined by

$$\phi(n) = \begin{cases} 1 & (\text{ if } n = 1) \\ \text{the number of positive integers less than } n & (\text{ if } n \geq 2) \\ \text{ and relatively prime to } n & \end{cases}$$

is known as ***Euler's Phi function***.

3.8. Proposition. ***Properties of Euler's Phi Function***

(1) If p is prime, then $\phi(p) = p^{n-1}(p-1)$
(2) If $m, n \in \mathbb{N}$ and $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$
(3) If $a \in \mathbb{N}$ with $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where $p_1, p_2, \dots p_k$ are distinct primes, then

$$\phi(a) = a\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \dots \Big(1 - \frac{1}{p_k}\Big)$$

3.9. Corollary. ***Euler's Theorem***

If $(n, a) = 1$ for $n, a \in \mathbb{N}$, then $a^{\phi(n)} \equiv 1 (mod\ n)$, where ϕ is the Euler's phi-function defined on $\mathbb{N}$.

PROOF. The set $G = \{[b] \mid 1 \leq b < n \text{ and } (b, n) = 1\}$ is a group under multiplication mod n with $O(G) = \phi(n)$, where ϕ is Euler's phi function. As [1] is the identity element of G, by Corollary 3.6,

$$[b]^{\phi(n)} = [1] \;\Rightarrow\; [b^{\phi(n)}] = [1] \;\; ([b] \in G).$$

Equivalently, $b^{\phi(n)} \equiv 1(mod\ n)$.

Now we have $(a, n) = 1$. If $a = qn + r, 0 < r < n$ then $(a, n) = (r, n) = 1$. Also

$$a \equiv r(mod\ n) \;\Rightarrow\; a^{\phi(n)} \equiv r^{\phi(n)}(mod\ n)$$

Since $1 \leq r < n$ and $(r, n) = 1$, $[r] \in G$. Thus $r^{\phi(n)} \equiv 1(mod\ n)$. Using the transitivity of the relation 'Congruence modulo n', we get $a^{\phi(n)} \equiv 1(mod\ n)$. □

3.10. Corollary. ***Fermat's Little Theorem***

For every integer a and every prime p, $a^p \equiv a(mod\ p)$.

PROOF. Since p is prime, $\phi(p) = n - 1$. Thus by Euler's Theorem

$$\begin{aligned} a^{\phi(p)} \equiv 1(mod\ p) &\Rightarrow a^{p-1} \equiv 1(mod\ p) \\ &\Rightarrow a^{p-1} \cdot a \equiv a(mod\ p) \\ &\Rightarrow a^p \equiv a(mod\ p). \end{aligned}$$

□

3.4. Solved Examples

4.1. Example. If H is a subgroup of G, then show that $x^{-1}Hx = \{x^{-1}hx : h \in H\}$ is also a subgroup of G for $x \in G$.

SOLUTION. Since $e \in H$, $x^{-1}ex = x^{-1}x = e \in x^{-1}Hx$. Thus $x^{-1}Hx \neq \phi$. If $a, b \in x^{-1}Hx$, then $a = x^{-1}h_1x$ and $b = x^{-1}h_2x$, for some $h_1, h_2 \in H$. Thus

$$\begin{aligned} ab^{-1} &= (x^{-1}h_1x)(x^{-1}h_2x)^{-1} \\ &= (x^{-1}h_1x)(x^{-1}h_2^{-1}x) \\ &= x^{-1}h_1(x(x^{-1})h_2^{-1}x \\ &= x^{-1}h_1h_2^{-1}x \\ &= x^{-1}h_3x \qquad (\text{ as } H \text{ is a subgroup } h_1h_2^{-1} = h_3 \in H) \end{aligned}$$

i.e. $ab^{-1} \in x^{-1}Hx$. Thus by one step test $x^{-1}Hx$ is a subgroup of G for $x \in G$. □

4.2. Example. Show that: For a commutative group G, $H = \{a \in G : O(a) \text{ is finite}\}$ is a subgroup of G.

SOLUTION. As $O(e) = 1$, which is finite $e \in H$. If $a, b \in H$, then $O(a)$ and $O(b)$ are finite. Let $O(a) = m$ and $O(b) = n$.

$$\begin{aligned}(ab^{-1})^{mn} &= (b^{-1})^{mn}a^{mn} \\ &= (b^n)^{-m}(a^m)^n \\ &= e\ e \qquad\qquad (O(a) = m \text{ and } O(b) = n) \\ &= e\end{aligned}$$

i.e. $O(ab^{-1})$ is finite. Hence $ab^{-1} \in H$. Thus by one step test H is a subgroup of G. □

4.3. Example. Show that: A group can not be a union of its two proper subgroups.

SOLUTION. If possible, suppose $G = H_1 \cup H_2$, where H_1 and H_2 are proper subgroups of G. As H_1 is a proper subgroup of G, there exists an element $a \in G$ such that $a \notin H_1$, i.e. $a \in H_2$. Similarly, we have an element $b \in G$ such that $b \notin H_2$, i.e. $b \in H_1$. Consider the element $ab \in G = H_1 \cup H_2$.

$$\text{If } ab \in H_1 \ \Rightarrow\ a = a(bb^{-1}) = (ab)b^{-1} \in H_1,$$

a contradiction. Similarly, if $ab \in H_2$ also gives a contradiction. Hence the result. □

4.4. Example. Show that: If the index of a subgroup H of a group G is 2, then $aH = Ha$ for each $a \in G$.

SOLUTION. If $a \in H$, then $aH = Ha = H$. If $a \notin H$, then right coset $He = H$ and Ha are disjoint and since index of H in G by 2, $G = H \cup Ha$. Similarly, $G = H \cup aH$. Now,

$$H \cup Ha = H \cup aH \text{ with } H \cap Ha = \phi = H \cap aH$$

gives us $Ha = aH$. □

4.5. Example. Let H and K be finite subgroups of a given group G. If $O(H)$ and $O(K)$ are relatively prime, then $H \cap K = \{e\}$.

SOLUTION. Since $H \cap K$ is a sub group of a finite group H, we have $O(H \cap K)|O(H)$ by Lagrange's Theorem, Similarly, we get $O(H \cap K)|O(K)$. As $O(H)$ and $O(K)$ are relatively prime, this is possible only when $O(H \cap K) = 1$. i.e. $H \cap K = \{e\}$. □

4.6. Example. If $G = (\mathbb{Z}, +)$ and $H = n\mathbb{Z}$, then obtain all right cosets of H in G and find the index of H in G.

SOLUTION. By definition $H = n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots, \}$. By division algorithm

$$m = qn + r, \quad 0 \leq r \leq n-1 \quad (m \in \mathbb{Z}).$$

Hence

$$\begin{aligned} H + m = H + (qn + r) &\Rightarrow H + m = (H + qn) + r \\ &\Rightarrow H + m = H + r \qquad (qn \in H) \end{aligned}$$

Thus we can have at the most n right cosets of H in G, namely

$$H, H+1, H+2, \ldots, H+(n-1).$$

These n right cosets are distinct. If possible, suppose for some $0 \leq i < j \leq n-1$

$$\begin{aligned} H + i = H + j &\Rightarrow j - i \in H \\ &\Rightarrow j - i = kn \text{ for some integer } k \\ &\Rightarrow n|(j-i) \qquad \text{and } 0 < (j-i) < n. \end{aligned}$$

Which is a contradiction. Thus H has n distinct right cosets $H, H+1, H+2, \ldots, H+(n-1)$. Thus $i_G(H) = n$.

□

4.7. Example. Find the remainder obtained on dividing 3^{256} by 14.

SOLUTION. Here $\phi(14) = \phi(2 \cdot 7) = \phi(2)\phi(7) = 1 \cdot 6 = 6$. Also $(3, 14) = 1$. Hence by Euler's Theorem

$$3^{\phi(14)} \equiv 1 (mod\ 14) \Rightarrow 3^6 \equiv 1 (mod\ 14).$$

Now $256 = 42 \times 6 + 4$. Thus $3^{256} = 3^{42 \times 6 + 4} = (3^6)^{42} \cdot 3^4$. Since

$$\begin{aligned} 3^6 \equiv 1 (mod\ 14) &\Rightarrow (3^6)^{42} \equiv 1^{42} (mod\ 14) \\ &\Rightarrow (3^6)^{42} \equiv 1 (mod\ 14) \end{aligned}$$

$$\begin{aligned} &\Rightarrow \quad (3^6)^{42} \cdot 3^4 \equiv 1 \cdot 3^4 (mod\ 14) \\ &\Rightarrow \quad 3^{256} \equiv 81 (mod\ 14) \\ &\Rightarrow \quad 3^{256} \equiv 11 (mod\ 14) \qquad\qquad (81 = 14 \times 5 + 11) \end{aligned}$$

Thus remainder will be 11. □

4.8. Example. Using the Fermat's Theorem, show that if p is an odd prime then

(1) $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv (-1)(mod\ p)$
(2) $1^p + 2^p + \ldots + (p-1)^p \equiv 0(mod\ p)$

SOLUTION. (1) For any $k, 1 \leq k \leq p-1$, we have $(k, p) = 1$. Hence by Fermat's Theorem

$$k^p \equiv k(mod\ p) \quad \Rightarrow \quad k^{p-1} \equiv 1(mod\ p) \ \ (1 \leq k < p-1). \qquad (4.8.1)$$

Taking $k = 1, 2, \ldots, (p-1)$ in 4.8.1, we get

$$\begin{aligned} k = 1 \quad &\Rightarrow \quad 1^{p-1} \equiv 1(mod\ p) \\ k = 2 \quad &\Rightarrow \quad 2^{p-1} \equiv 1(mod\ p) \\ k = 3 \quad &\Rightarrow \quad 3^{p-1} \equiv 1(mod\ p) \\ \cdots \quad &\cdots \quad \cdots \quad \cdots \\ k = p-1 \quad &\Rightarrow \quad k^{p-1} \equiv 1(mod\ p) \end{aligned}$$

Adding the corresponding sides of congruency we obtain

$$\begin{aligned} 1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + k^{p-1} &\equiv \underbrace{(1 + 1 + 1 + \ldots + 1)}_{p-1 \text{ times}} (mod\ p) \\ &\equiv (p-1)(mod\ p) \\ &\equiv (-1)(mod\ p) \end{aligned}$$

(2) By 4.8.1, $k^p \equiv k(mod\ p)$. Taking $k = 1, 2, \ldots, (p-1)$, we have

$$\begin{aligned} k = 1 \quad &\Rightarrow \quad 1^p \equiv 1(mod\ p) \\ k = 2 \quad &\Rightarrow \quad 2^p \equiv 2(mod\ p) \\ k = 3 \quad &\Rightarrow \quad 3^p \equiv 3(mod\ p) \\ \cdots \quad &\cdots \quad \cdots \quad \cdots \\ k = p-1 \quad &\Rightarrow \quad k^p \equiv (p-1)(mod\ p) \end{aligned}$$

Adding the corresponding sides of congruency we obtain

$$1^p + 2^p + 3^p + \ldots + k^p \equiv 1 + 2 + 3 + \ldots + (p-1)(mod\ p)$$

$$\equiv \frac{(p-1)p}{2}(mod\ p)$$

As p is odd prime $2|(p-1)$ and hence

$$p \left| \frac{p(p-1)}{2} \right. \Rightarrow \frac{p(p-1)}{2} \equiv 0(mod\ p).$$

Thus $1^p + 2^p + 3^p + \ldots + k^p \equiv 0(mod\ p)$. □

3.5. Exercise

(1) Verify that the following subsets of the group $GL(2;\mathbb{R})$ under matrix multiplication are its subgroups.

$$S_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} : a \in \mathbb{R}, a \neq 0 \right\} \quad S_2 = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{R}, a \neq 0 \right\}.$$

Examine commutativity of each subgroup S_1 and S_2.

(2) Suppose $G = \{(a,b) : a, b \in \mathbb{R} \text{ and } a \neq 0\}$. The binary operations $\oplus$ is defined on G as follows:

$$(a,b) \oplus (c,d) = (ac, bc+d)$$

(a) Show that $(G, \oplus)$ is a non-commutative group
(b) The subset $H = \{(1,b) : b \in \mathbb{R}\}$ is a subgroup of G.

(3) Obtain the normaliser $N(a)$, where $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $G = GL(2;\mathbb{R})$.

(4) Obtain center Z of the group $GL(2;\mathbb{R})$ under matrix multiplication.

(5) Show that: If H is a subgroup of a group G and $i_G(H) = 2$, then H is commutative.

(6) Prove that a group having only a finite number of subgroups must be a finite group.

(7) For subgroups H and K of a group G, the product HK is defined as $HK = \{hk \mid h \in H \text{ and } k \in K\}$, then show that
(a) HK is a subgroup of G iff $HK = KH$.
(b) HK is always a subgroup of G if G is a commutative group.

(8) Let H be a subgroup of a group G and $a, b \in G$. Show that
(a) the set $K = \{x^{-1} \mid x \in Ha\}$ is a left coset of H in G and $K = a^{-1}H$.
(b) $Ha = Hb$ iff $a^{-1}H = b^{-1}H$.

(9) For a subgroup H of a group G, established the existence of a one-one correspondence between the set of all right cosets and the set of all left cosets of H in G.

(10) For a subgroups H and K of a group G and $a \in G$, show that $(H \cap K)a = Ha \cap Ka$.
(11) Show that a non-cyclic group has always a proper subgroup.
(12) Using Fermat's Theorem, show that $5^{38} \equiv 4(mod\ 11)$.
(13) Using Euler's Theorem, find the remainder obtained on dividing 7^{1000} by 24.

Chapter 4

Permutations

4.1. Definitions and Examples

1.1. Definition. Let S be a non empty set. Then we define $A(S)$ is the set of all one-one and onto functions (one-one correspondence) defined from S to S. i.e.

$$A(S) = \{f : S \longrightarrow S : f \text{ is one-one and onto } \}$$

1.2. Example. $A(S)$ is a group under composition of functions.

1.3. Definition. If S is a finite set and consist of n elements, then the group $A(S)$ is denoted by a S_n and called the symmetric group of degree n (or the permutation group of order n). The elements of S_n are called permutations.

1.4. Example. For $n > 2$, $(S_n, \circ)$ is a non-commutative group.

Let $S = \{1, 2, 3, 4, 5\}$. Then S_5 is the set of all one-one and onto functions defined from S to S. Let $f \in S_5$ with

$$f(1) = 3,\ f(2) = 1,\ f(3) = 4,\ f(4) = 5,\ f(5) = 2$$

We may write f in different way as follows: