



Abstract Algebra I

Prepared by

Dr. Amr M. Elrawy

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, SOUTH
VALLEY UNIVERSITY

PREPARING BY DR. AMR M. ELRAWY

First release, 2021



Contents

1	Fundamental Concepts	7
1.1	Binary Relation	7
1.2	Equivalence Relation	8
1.3	Mapping or Functions	10
1.4	Binary Operation	12
2	Groups	13
2.1	Definitions and Examples	15
2.2	Properties	18
2.3	Relation between semi group and group	24
2.4	Exercise	26

3	Subgroups	29
3.1	Subgroup Tests	30
3.2	Exercise	37
4	Cyclic Groups	39
4.1	Definitions and Examples	39
4.2	Classification of Cyclic Groups	41
4.3	Classification of Subgroups of Cyclic Groups	46
4.4	Euler Phi	48
4.5	Exercise	50
5	Permutation Groups	51
5.1	Properties of Permutations	56
5.2	Exercises	62
6	Lagrange's Theorem	63
6.1	Lagrange's Theorem.	67
6.2	Exercises	72
7	Normal Subgroups	73
7.1	Quotient Group	76
7.2	Exercise	81

8	Homomorphis- Isomorphism	83
8.1	Properties of Subgroups Under Homomorphisms	85
8.2	The isomorphism theorems	91
8.3	Exercises	95
9	Direct product, direct sum	97
10	Ring	99
10.0.1	Subring	105
10.1	Characteristic of a Ring	106
10.2	Exercises	112
11	Ring Homomorphisms	113
12	Ideals and Factor Rings	115
12.1	Factor Ring	117
12.2	Maximal ideals	120
12.3	Prime Ideal	120

1. Fundamental Concepts

In this chapter, we will review some concepts without elaborating on the proofs.

1.1 Binary Relation

Definition 1.1.1 A **Cartesian product** of two sets A and B is the set of all possible ordered pairs (a, b) , where $a \in A$ and $b \in B$ such that

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Definition 1.1.2 If $R \subseteq A \times B$ and $A = B$, the binary relation R is called a **homogeneous binary relation** defined on the set A .

Let $R \subseteq A \times B$ be a binary relation defined on a pair of sets A and B . The set of all $a \in A$ such that aRb for at least one $b \in B$ is called the domain of the binary relation R . The set of all $b \in B$ such that aRb for at least one $a \in A$ is called the codomain (also referred to as image or range) of the binary relation R .

■ **Example 1.1** The relation "greater than", denoted by $>$, on the set $A = \{1, 2, 3\}$. The Cartesian square of the set A is given by

$$A^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

We find all pairs (a, b) where $a > b$. This yields:

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

■

1.2 Equivalence Relation

Definition 1.2.1 A relation R on a set A is called **reflexive** if aRa for every $a \in A$.

Definition 1.2.2 A relation R on a set A is called **Symmetric** if whenever aRb , then every bRa .

Definition 1.2.3 A relation R on a set A is called **Transitive** if whenever aRb , and bRc , then every aRc .

Definition 1.2.4 A relation R on a set A is called an equivalence relation on A when R is

- (1) Reflexive,
- (2) Symmetric,
- (3) Transitive.

■ **Example 1.2** The relation $=$ on the set \mathbb{R} is undoubtedly the most familiar equivalence relation for.

(i) R is reflexive, i.e.,

$$\forall a \in \mathbb{R} \Rightarrow a = a \Rightarrow aRa.$$

(ii) R is Symmetric, i.e.,

$$\forall aRb \Rightarrow a = b \Rightarrow b = a \Rightarrow bRa.$$

(iii) R is Transitive, i.e.,

$$\forall aRb \text{ and } bRc \Rightarrow a = b \wedge b = c \Rightarrow b = c \Rightarrow bRc.$$

Definition 1.2.5 Let A be a set and R be an equivalence relation on A . If $a \in A$, the elements $b \in A$ satisfying bRa constitute a subset, $cl[a]$, of A , called an equivalence set or equivalence class. i.e.,

$$cl[a] = \{b : b \in A, aRb\}.$$

■ **Example 1.3** Let $R = \{(a, a), (b, b), (c, c)\}$ be equivalence relation on $A = \{a, b, c\}$, then

$$cl[a] = \{a\},$$

$$cl[b] = \{b\}$$

and

$$cl[c] = \{c\}.$$

■ **Example 1.4** Consider the relation of congruence "mod n " on \mathbb{Z} , and let $a \in \mathbb{Z}$. The **congruence class** of a is defined by

$$\{x \in \mathbb{Z} : x = a + kn, k \in \mathbb{Z}\}.$$

On the other hand, the equivalence class of a is, by definition,

$$\{x \in \mathbb{Z} : x \equiv a, \text{ mod } n\}.$$

Since $x \equiv a, \text{ mod } n$ if and only if $x = a + kn$ for some $k \in \mathbb{Z}$, these two subsets coincide; that is, the equivalence class $cl[a]$ is the congruence class. ■

Proposition 1.2.1 If $R = \equiv$ is an equivalence relation on a set A , then $x \equiv y$ if and only if $cl[x] = cl[y]$.

Proof. Assume that $x \equiv y$. If $z \in cl[x]$, then $z \equiv x$, and so transitivity gives $z \equiv y$; hence $cl[x] \subset cl[y]$. By symmetry, $y \equiv x$, and this gives the reverse inclusion $cl[y] \subset cl[x]$. Thus, $cl[x] = cl[y]$.

Conversely, if $cl[x] = cl[y]$, then $x \in cl[x]$, by reflexivity, and so $x \in cl[y]$. Therefore, $x \equiv y$. ■

Proposition 1.2.2 Suppose that $R = \equiv$ is an equivalence relation on a set A and if $cl[x] \cap cl[y] = \phi$, then $cl[x] = cl[y]$.

Theorem 1.2.3 An equivalence relation R on a set A effects a partition of A , and conversely, a partition of A defines an equivalence relation on A .

1.3 Mapping or Functions

Definition 1.3.1 Let X and Y be (not necessarily distinct) sets. A **function** (mapping) f from X to Y , denoted by

$$f : X \rightarrow Y,$$

is a subset $f \subset X \times Y$ such that, for each $a \in X$, there is a unique $b \in Y$ with $(a, b) \in f$.

For each $a \in X$, the unique element $b \in Y$ for which $(a, b) \in f$ is called the value of f at a , and b is denoted by $f(a)$. Thus, f consists of all those points in $X \times Y$ of the form $(a, f(a))$. If $f : X \rightarrow Y$, call X the **domain** of f , call Y the **target** (or **codomain**) of f , and define

the **image** (or **range**) of f , denoted by $im f$, to be the subset of Y consisting of all the values of f .

Definition 1.3.2 Functions $f : X \rightarrow Y$ and $g : A \rightarrow B$ are equal if $X = A$, $Y = B$, and the subsets $f \subset X \times Y$ and $g \subset A \times B$ are equal.

Definition 1.3.3 If $f : X \rightarrow Y$ is a function, and if $A \subset X$, then the **restriction** of f to A is the function $f|_A : X \rightarrow Y$ defined by $(f|_A)(a) = f(a)$ for all $a \in A$.

Proposition 1.3.1 Let $f : X \rightarrow Y$ and $g : A \rightarrow B$ be functions, then $f = g$ if and only if $X = A$, $Y = B$, and $f(a) = g(b)$ for all $a \in A$.

Definition 1.3.4 A function $f : X \rightarrow Y$ is **injective** (or one-to-one) if, whenever

$$\forall x, y \in X, f(x) = f(y) \Rightarrow x = y.$$

or

$$\forall x, y \in X, x \neq y \Rightarrow f(x) \neq f(y).$$

Definition 1.3.5 A function $f : X \rightarrow Y$ is **surjective** (or **onto**) if

$$im f = Y.$$

Thus, f is surjective if, for each $y \in Y$, there is some $x \in X$ (probably depending on y) with $y = f(x)$.

Definition 1.3.6 If $f : A \rightarrow B$ and $g : B \rightarrow C$ are mappings (the target of f is the domain of g), then their **composite**, denoted by $g \circ f$, is the function $A \rightarrow C$ given by $g \circ f : x \rightarrow g(f(x))$; that is, first evaluate f on x and then evaluate g on $f(x)$.

Proposition 1.3.2 Composition of mappings is associative: if

$$f : X \rightarrow Y, g : Y \rightarrow Z \text{ and } h : Z \rightarrow W,$$

are mappings, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Definition 1.3.7 A mapping $f : X \rightarrow Y$ is **bijective** (or is a one-one correspondence) if it is both injective and surjective.

Definition 1.3.8 A map $f : X \rightarrow Y$ has an inverse if there exists a map $g : Y \rightarrow X$ with both composites $g \circ f$ and $f \circ g$ being identity maps.

Proposition 1.3.3 If $f : X \rightarrow Y$ and $g : Y \rightarrow X$ are maps such that $(g \circ f)(x) = e(x) = x$, then f is injective and g is surjective.

Proposition 1.3.4 A function $f : X \rightarrow Y$ has an inverse $g : Y \rightarrow X$ if and only if it is a bijection.

Proposition 1.3.5 Let X and Y be sets, and let $f : X \rightarrow Y$ be a mapping.

- (i) If $A \subset B$ are subsets of X , then $f(A) \subset f(B)$, and if $C \subset D$ are subsets of Y , then $f^{-1}(C) \subset f^{-1}(D)$.
- (ii) If $C \subset Y$, then $ff^{-1}(C) \subset C$; if f is a surjection, then $ff^{-1}(C) = C$.
- (iii) If $A \subset X$, then $A \subset f^{-1}f(A)$.

1.4 Binary Operation

Definition 1.4.1 A *binary operation* $*$ on a set G is a function mapping $G \times G$ into G . For each $(a, b) \in G \times G$, we will denote the element $*((a, b))$ of G by $a * b$ i.e.,

$$* : G \times G \rightarrow G,$$

$$(a, b) \rightarrow a * b.$$



2. Groups

Group theory is a branch of mathematics and abstract algebra that analyses the algebraic structures known as groups. Other well-known algebraic structures, such as rings, fields, and vector spaces, can also be regarded as groups with additional operations and axioms. Groups appear frequently in mathematics, and group theory's approaches have affected many aspects of algebra. Linear algebraic groups and Lie groups are two aspects of group theory that have advanced to the point where they have become separate subject areas.

The history of group theory, which is a branch of mathematics that studies groups in all of their forms, has unfolded in several parallel strands. The theory of algebraic equations, number theory, and geometry are the three historical roots of group theory. Early researchers in the field of group theory included Joseph Louis Lagrange (1736 – 1813), Niels Henrik Abel (1802 – 1829), and Évariste Galois (1811 – 1832).



Niels Henrik Abel



Joseph-Louis Lagrange



Évariste Galois

Why is group theory important?

Group theory is the study of symmetry in general. When working with an ostensibly symmetric object, group theory can aid in the analysis. Anything that remains invariant under some modifications is referred to as symmetric. This can be applied to geometric figures (a circle is highly symmetric and invariant under any rotation), but it can also be applied to more abstract objects such as functions: $x^2 + y^2 + z^2$ is invariant under any rearrangement of x, y , and z , and the trigonometric functions $\sin(t)$ and $\cos(t)$ are invariant when t is replaced with $t + 2$.

Without group theory, modern particle physics would not exist; in fact, group theory predicted the existence of many elementary particles long before they were discovered experimentally.

Molecules and crystals have diverse symmetries that influence their structure and behavior. As a result, group theory is an important tool in various branches of chemistry.

With group theory, traditional algebraic problems have been solved. Mathematicians discovered analogues of the quadratic formula for roots of generic polynomials of degree 3 and 4 throughout the Renaissance. The cubic and quartic formulas, like the quadratic formula, express the roots of all polynomials of degree 3 and 4 in terms of polynomial coefficients and root extractions (square roots, cube roots,

and fourth roots). The search for a quadratic formula equivalent for the roots of all polynomials of degree 5 or above proved fruitless. The failure to establish such broad formulas was explained in the 19th century by Evariste Galois' discovery of subtle algebraic symmetry in the roots of a polynomial.

The mathematics of public-key cryptography uses a lot of group theory. Different cryptosystems use different groups, such as the group of units in modular arithmetic and the group of rational points on elliptic curves over a finite field.

2.1 Definitions and Examples

Definition 2.1.1 Let G be a non empty set, together with a binary operation \star , then the couple (G, \star) is said to be a *semi-group* if

$$(i) \quad a \star (b \star c) = (a \star b) \star c \text{ for all } a, b, c \in G.$$

Semi-group = binary operation + associative law.

■ **Example 2.1** Each of the following sets with the usual definition of addition and multiplication of numbers are a semi-group:

1. \mathbb{N} the set of all natural numbers.
2. \mathbb{Z} the set of all integer numbers.
3. \mathbb{Q} the set of all rational numbers.
4. \mathbb{R} the set of all real numbers.
5. \mathbb{C} the set of all complex numbers.

Definition 2.1.2 Let G be a non empty set, together with a binary operation \star , then the couple (G, \star) is said to be a *monoid* if it satisfies the following axioms

$$(i) \quad a \star (b \star c) = (a \star b) \star c \text{ for all } a, b, c \in G.$$

$$(ii) \quad \exists e \in G \text{ such that } a \star e = e \star a = a \text{ for all } a \in G.$$

A monoid is a semigroup with an identity.

■ **Example 2.2** Each of the following sets with the usual definition of addition and multiplication of numbers are a semi-group:

1. \mathbb{Z} the set of all integer numbers.
2. \mathbb{Q} the set of all rational numbers.
3. \mathbb{R} the set of all real numbers.
4. \mathbb{C} the set of all complex numbers.

Definition 2.1.3 Let G be a non empty set, together with a binary operation \star , then the couple (G, \star) is said to be a **group** if it satisfies the following axioms

- (i) $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$.
- (ii) $\exists e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.
- (iii) $\forall a \in G \exists a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$ for all $e \in G$.

A group is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$.

If we define a binary algebraic structure as a set with a binary operation on it, then we have the following schematic:

Binary algebraic structure \supseteq Semi group \supseteq Monoid \supseteq Group

Definition 2.1.4 A group (G, \star) is called a **commutative** or **abelian** group if

- (i) $a \star b = b \star a$ for all $a, b, c \in G$.

■ **Example 2.3** Each of the following sets with the usual definition of addition and multiplication of numbers are a semi-group:

1. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.
2. $\mathbb{R}^* = \mathbb{R} - \{0\}$.
3. $\mathbb{C}^* = \mathbb{C} - \{0\}$.

■ **Example 2.4** Show that (\mathbb{Z}_5, \oplus_5) is abelian group?

Solution:

We represent (\mathbb{Z}_5, \oplus_5) by the following table:

\oplus_5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 2.1: (\mathbb{Z}_5, \oplus_5)

From the above table, we find:

- (i) \oplus_5 is a binary operation on \mathbb{Z}_5 .
- (ii) Associative law holds in general for the two operations \oplus_n and \otimes_n on \mathbb{Z}_5 . So \oplus_5 is associative on \mathbb{Z}_5 .
- (iii) 0 is the identity.
- (iv)

The element	0	1	2	3	4
The inverse	4	3	2	1	0

- (v) \oplus_5 is commutative.

Thus, (\mathbb{Z}_5, \oplus_5) is abelian group ■

■ **Example 2.5** (\mathbb{Z}_n, \oplus_n) is abelian group where $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. ■

■ **Example 2.6** Show that (G, \times) is abelian group where $G = \{3^n : n \in \mathbb{Z}\}$ and \times the usual multiplication?

Solution:

- (i) Let $3^n, 3^m \in G$, then $3^n \times 3^m = 3^{n+m} \in G \forall m, n \in \mathbb{Z}$.
(ii) Let $3^n, 3^m, 3^u \in G$, then

$$\begin{aligned} 3^n \times (3^m \times 3^u) &= 3^n \times 3^{m+u} \\ &= 3^{n+m+u} \\ &= 3^{n+m} \times 3^u \\ &= (3^n \times 3^m) \times 3^u, \end{aligned}$$

where $n, m, u \in \mathbb{Z}$.

- (iii) The identity is $3^0 = 1$.
(iv) $\forall 3^n \in G \exists 3^{-n} \in G$ such that $3^n \times 3^{-n} = 3^{-n} \times 3^n = 3^0$.
(v) Let $3^n, 3^m \in G$, then

$$\begin{aligned} 3^n \times 3^m &= 3^{n+m} \\ &= 3^{m+n} \\ &= 3^m \times 3^n. \end{aligned}$$

■
Example 2.7 Show that $(F(A), \circ)$ is not abelian group where $F(A)$ is the set of all 1-1 corresponding mappings from A to A and \circ the composition of mappings?

Solution: It easy to show that. ■

2.2 Properties

Let (G, \star) be a group, then the following properties are satisfied

(1) The identity element e is unique.

proof:

Let e_1, e_2 be two identities in G , then

$$e_1 \star e_2 = e_1 = e_2.$$

(2) The inverse element a^{-1} is unique.

proof:

Let b, c be two inverses of a in G , then

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c.$$

(3) $(a^{-1})^{-1} = a$.

proof:

For $a^{-1} \star a = a \star a^{-1} = e$.

(4) $a^n = a \star a \star \dots \star a$.

(5) $a^{-n} = a^{-1} \star a^{-1} \star \dots \star a^{-1}$.

Theorem 2.2.1 Let (G, \star) be a group, then the cancellation law hold i.e.;

$$a \star x = a \star y \Rightarrow x = y.$$

$$x \star a = y \star a \Rightarrow x = y.$$

Proof. Let $a, x, y \in G$, then

$$\begin{aligned}
a \star x = a \star y &\Rightarrow a^{-1} \star (a \star x) = a^{-1} \star (a \star y) \\
&\Rightarrow (a^{-1} \star a) \star x = (a^{-1} \star a) \star y \\
&\Rightarrow e \star x = e \star y \\
&\Rightarrow x = y.
\end{aligned}$$

Similarly, for $x \star a = y \star a \Rightarrow x = y$. ■

(6) The equations

$$a \star x = b,$$

$$y \star a = b,$$

have unique solutions

$$x = a^{-1} \star b,$$

$$y = b \star a^{-1},$$

respectively.

proof:

For the equation $a \star x = b$.

$$L.H.S = a \star x = a \star (a^{-1} \star b) = (a \star a^{-1}) \star b = e \star b = b,$$

so $x = a^{-1} \star b$ is a solution.

Now, we prove the uniqueness. Let x_1, x_2 be two solutions of the equation $a \star x = b$, then

$$a \star x_1 = b, a \star x_2 = b,$$

this lead to

$$a \star x_1 = a \star x_2,$$

so, $x_1 = x_2$ by cancellation law.

Similarly, for the equation $y \star a = b$ has solution $y = b \star a^{-1}$.

■ **Example 2.8** Find a solution of the equation $2x = 3$ in a group (\mathbb{Z}_5, \oplus_5) .

Solution

Since

$$\begin{aligned} 2 \oplus_5 x = 3 &\Rightarrow x = 2^{-1} \oplus_5 3 \\ &= 3 \oplus_5 3 \\ &= 1. \end{aligned}$$

■

■ **Example 2.9** Find a solution of the equation $5x = -2$ in a group (\mathbb{Z}, \star) , where $a \star b = a + b - 3 \forall a, b \in \mathbb{Z}$.

Solution

Since

$$\begin{aligned} 5 \star x = -2 &\Rightarrow x = 5^{-1} \star (-2) \\ &= (6 - 5) \star (-2) \\ &= 1 \star (-2) \\ &= 1 + (-2) - 3 \\ &= -4. \end{aligned}$$

■

$$(7) (a \star b)^{-1} = b^{-1} \star a^{-1} \forall a, b \in G.$$

proof:

Let $a, b \in G$, then

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

Thus, $(a \star b)^{-1} = b^{-1} \star a^{-1} \forall a, b \in G$.

■ **Example 2.10 The Klein 4-group is an Abelian group.**

Let $G = \{e, i, j, k\}$, then (G, \star) is a group where $i \star j = k = j \star i$ and $i \star i = e = j \star j = k \star k$.

■ **Example 2.11 The Quaternion Group.**

Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, ij = -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \end{aligned}$$

then G forms a group, but G is not abelian as $ij \neq ji$.

■ **Example 2.12 The General Linear Group.**

The set of all matrices of order $n \times n$ over real number with non-zero determinant forms a non abelian group under matrix multiplication. This group called general linear group of $n \times n$, i.e.,


$$GL(n, \mathbb{R}) = \{A : A \in M_{n \times n}, \det(A) \neq 0\}.$$

■ **Example 2.13 The Special Linear Group.**

The set of all matrices of order $n \times n$ over real number with determinant 1 forms a group under matrix multiplication. This group called special linear group of $n \times n$, i.e.,

$$SL(n, \mathbb{R}) = \{A : A \in M_{n \times n}, \det(A) = 1\}.$$

Definition 2.2.1 Let (G, \star) be a group, then the order of a group means the number of its distinct elements, and denoted $|G|$ or $o(G)$.

 We say that G is a finite group if its order is finite; otherwise, it is an infinite group.

■ **Example 2.14** If $G = Z_6$, then $|G| = 6$, and therefore G is a finite group. On the other hand, \mathbb{Q} is an infinite group. ■

Definition 2.2.2 The order of an element g in a group G is the smallest positive integer n such that

$$g^n = e \text{ or } ng = e.$$

If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

■ **Example 2.15** Consider Z_{10} under addition modulo 10. Find $|0|$, $|2|$, $|5|$, $|6|$ and $|7|$?

Solution:

Since

$$0 \oplus_{10} 0 = 0,$$

so $|0| = 1$.

Since

$$2 \cdot 2 = 2 \oplus_{10} 2 = 4,$$

$$3 \cdot 2 = 2 \oplus_{10} 2 \oplus_{10} 2 = 6,$$

$$4 \cdot 2 = 2 \oplus_{10} 2 \oplus_{10} 2 \oplus_{10} 2 = 8,$$

$$5 \cdot 2 = 2 \oplus_{10} 2 \oplus_{10} 2 \oplus_{10} 2 \oplus_{10} 2 = 0,$$

so $|2| = 5$.

Similar computations show that $|5| = 2$, $|6| = 5$ and $|7| = 10$. ■

2.3 Relation between semi group and group

Theorem 2.3.1 A semi group G is a group iff the equations

$$a \star x = b,$$

$$y \star a = b,$$

have a solution for all $a, b \in G$.

Proof. The first direction. Let G be a group, the the equations $a \star x = b, y \star a = b$, have a solution (by property (6)).

The other direction. Let G be a semi group and the equations

$$a \star x = b,$$

$$y \star a = b,$$

have a solution. (ii) Since $a \star x = b$ has solutions in G , then $a \star x = a$ has solutions in G this means there exists an identity element $e \in G$ such that $a \star e = e \star a = a$.

(iii) $a \star x = b$ has solutions in G , then $a \star x = e$ has solutions in G this means there exists an inverse element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$. Thus, G is a group. ■

Theorem 2.3.2 A finite semi group G is a group iff the cancelation laws hold.

Proof. The first direction. If G is a group, then the cancelation law hold.

The other direction. Let $G = \{a_1, a_2, \dots, a_n\}$ be a finite semi group in which cancellation laws hold. Let $a \in G$ be any element, then by closure property aa_1, aa_2, \dots, aa_n are all in G . Suppose any two of these elements are equal say, $aa_i = aa_j$ for some $i \neq j$ then $a_i = a_j$ by cancellation. But $a_i \neq a_j$ as $i \neq j$. Hence no two of aa_1, aa_2, \dots, aa_n can be equal. These being n in number, will be distinct members of

G (Note $o(G) = n$). Thus if $b \in G$ be any element then $b = aa_i$ for some i i.e., for $a, b \in G$ the equation $ax = b$ has a solution ($x = a_i$) in G . Similarly, the equation $ya = b$ will have a solution in G . G being a semi-group, associativity holds in G . Hence G is a group. ■

2.4 Exercise

- Exercise 2.1**
- If G is a group in which $(ab)^n = a^n b^n$ for three consecutive integers n and any a, b in G , then show that G is abelian.
 - Suppose $(ab)^n = a^n b^n$ for all $a, b \in G$ where $n > 1$ is a fixed integer. Show that
 - $(ab)^{n-1} = b^{n-1} a^{n-1}$.
 - $a^n b^{n-1} = b^{n-1} a^n$.
 - $(aba^{-1} \cdot b^{-1})^{n(n-1)} = e$ for all $a, b \in G$
 - Which of the following is group? Give reasons for your assertion.
 - $G = \{\pm 1, \pm i\}$, where $i = \sqrt{-1}$ under multiplication.
 - $G =$ set of rational numbers under composition $*$ defined by $a * b = \frac{ab}{2}, a, b \in G$.
 - $G = \{1, w, w^2\}$ where w is cube root of unity under multiplication.
 - Set of all matrices of the form $\begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}, \theta \in \mathbf{R}$, under matrix multiplication.
 - Set of all 2×2 matrices over integers under matrix multiplication.
 - $G = \{2, 4, 6, 8\}$ under multiplication modulo 10.
 - $G = \{(a, b) \mid a, b \in \mathbf{Z}\}$ under $*$ defined by $(a, b) * (c, d) = (ac + bd, ad + bc)$.
 - Suppose the table below is a group table. Fill in the blank

entries.

	e	a	b	c	d
e	e	$-$	$-$	$-$	$-$
a	$-$	b	$-$	$-$	e
b	$-$	c	d	e	$-$
c	$-$	d	$-$	a	b
d	$-$	$-$	$-$	$-$	$-$

5. Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.
6. Prove that in a group, $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$.
7. In the group Z_{12} , find $|a|$, $|b|$, and $|a + b|$ for each case.
 - (i) $a = 6, b = 2$.
 - (ii) $a = 3, b = 8$.
 - (iii) $a = 5, b = 4$.





3. Subgroups

Definition 3.0.1 A non-empty subset H of a group G is said to be a *subgroup* of G , if H itself is a group w.r.t. the same binary operation in G and we denoted by $H \leq G$.

Ⓡ If $H \leq G$ and $K \leq H$, then $K \leq G$.

If G is a group with identity element e then the subsets $\{e\}$ and G are trivially subgroups of G and we call them the trivial subgroups (or improper subgroups). All other subgroups will be called non-trivial (or proper subgroups).

■ **Example 3.1** The set \mathbb{Z}_E of all even integers forms a subgroup w.r.t. addition in the additive group of all integers. ■

■ **Example 3.2** Let $(G = \{\pm 1, \pm i\}, \times)$ be a group and let $(H = \{\pm 1\}, \times)$, $(K = \{\pm i\}, \times)$, then $H \leq G$ but $K \not\leq G$. ■

3.1 Subgroup Tests

It is not necessary to directly check the group axioms when deciding whether or not a subset H of a group G is a subgroup of G . The following three theorems show that a subset of a group is a subgroup using basic tests.

Theorem 3.1.1 A non empty subset H of a group G is a subgroup of G if and only if

(i) $a, b \in H \Rightarrow ab \in H$.

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof. The first direction. Let H be a subgroup of G then by definition it follows that (i) and (ii) hold.

The other direction. Suppose that the given conditions hold in H , then

- Closure holds in H by (i).
- Let $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a(bc) = (ab)c$ Hence associativity holds in H .
- For any $a \in H, a^{-1} \in H$ and so by (i)

$$aa^{-1} \in H \Rightarrow e \in H$$

thus H has identity.

- Inverse of each element of H is in H by (ii).

Hence H satisfies all conditions in the definition of a group and thus it forms a group and therefore a subgroup of G . ■

■ **Example 3.3** Let G be an abelian group with identity e and $H, K \leq G$. Show that $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G

Solution:

To prove $HK \leq G$ we apply Theorem 3.1.1.

Since $e = ee \in HK$. So HK is non empty subset.

Assume that $a, b \in HK$ such that $a = h_1k_1$ and $a = h_2k_2$. Now, we must show that $ab \in HK$.

$$\begin{aligned} ab &= h_1k_1h_2k_2 \\ &= (h_1h_2)(k_1k_2) \in HK. \end{aligned}$$

Also, we show that $a^{-1} \in HK$

$$\begin{aligned} a^{-1} &= (h_1k_1)^{-1} \\ &= k_1^{-1}h_1^{-1} \\ &= h_1^{-1}k_1^{-1} \in HK, \end{aligned}$$

Therefore, by Theorem 3.1.1, $HK \leq G$. ■

Theorem 3.1.2 A non empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof. The first direction. Suppose that H is a subgroup of G then, $a, b \in H \Rightarrow ab^{-1} \in H$

The other direction. Assume that the given condition hold in H .

- Associativity holds in H follows as in previous theorem.
- Let $a \in H$ be any element ($H \neq \varnothing$) then

$$a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H.$$

So H has identity.

- For any $a \in H$, as $e \in H$

$$ea^{-1} \in H \Rightarrow a^{-1} \in H$$

i.e., H has inverse of each element.

- For any

$$\begin{aligned} a, b \in H, a, b^{-1} \in H &\Rightarrow a(b^{-1})^{-1} \in H \\ &\Rightarrow ab \in H \end{aligned}$$

i.e., H is closed under multiplication.

Hence, H is a group w.r.t. multiplication in G . ■

■ **Example 3.4** Let G be an abelian group with identity e . Show that $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G

Solution:

To prove $H \leq G$ we apply Theorem 3.1.2.

Since every element in H has the property $x^2 = e$. So, $e^2 = e$ i.e., H is non empty subset.

Now, we assume that $a, b \in H \Rightarrow a^2 = e, b^2 = e$, and we must show that $(ab^{-1})^2 = e$.

$$\begin{aligned} (ab^{-1})^2 &= ab^{-1}ab^{-1} \\ &= a^2(b^{-1})^2 \\ &= a^2(b^2)^{-1} \\ &= ee^{-1} = e. \end{aligned}$$

Therefore, $ab^{-1} \in H$, by Theorem 3.1.2, $H \leq G$. ■

■ **Example 3.5** Let G be the group of nonzero real numbers under multiplication, is the following subgroup of G

(i) $H = \{x \in G \mid x = 1 \text{ or } x \text{ is irrational}\}$

(ii) $K = \{x \in G \mid x \geq 1\}$.

Solution:

(i) H is not a subgroup of G , since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$.

(ii) K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$. ■

Theorem 3.1.3 A non empty finite subset H of a group G is a subgroup of G if and only if H is closed under multiplication.

Proof. The first direction. Let H be a subgroup of G then it is closed under multiplication by definition, so there is nothing to prove.

The other direction. Suppose that H be a finite subset s.t.,

$$a, b \in H \Rightarrow ab \in H$$

Now,

$$\begin{aligned} a, b, c \in H &\Rightarrow a, b, c \in G \\ &\Rightarrow a(bc) = (ab)c \end{aligned}$$

So, associativity holds in H , and therefore H is a semi-group. Again, trivially the cancellation laws hold in H (as they hold in G) and thus H is a finite semi-group in which cancellation laws hold. Hence H forms a group. ■

Definition 3.1.1 Let G be a group, then

$$Z(G) = \{x : x \in G, gx = xg \forall g \in G\}$$

is called **center** of G .

Theorem 3.1.4 $Z(G) \leq G$.

Proof. Suppose that $Z(G)$ be the centre of the group G . Then $Z(G) \neq \emptyset$ as $e \in Z(G)$.

Let $x, y \in Z(G) \Rightarrow xg = gx, yg = gy \forall g \in G$, then

$$g^{-1}x^{-1} = x^{-1}g^{-1}, g^{-1}y^{-1} = y^{-1}g^{-1}$$

Now, we show $xy^{-1} \in Z(G)$.

Since

$$\begin{aligned}
 g(xy^{-1}) &= (gx)y^{-1} \\
 &= (xg)y^{-1} \\
 &= (xg)y^{-1}(g^{-1}g) \\
 &= xg(y^{-1}g^{-1})g \\
 &= xg(g^{-1}y^{-1})g \\
 &= x(gg^{-1})y^{-1}g \\
 &= (xy^{-1})g \quad \text{for all } g \in G \\
 &\Rightarrow xy^{-1} \in Z(G)
 \end{aligned}$$

Hence $Z(G)$ is a subgroup. ■

R G is abelian iff $Z(G) = G$.

Definition 3.1.2 Let G be a group and for any element $a \in G$. The subset

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

is called normalize or centralizer of a in G .

It is easy to see that normalize is a subgroup of G .

■ **Example 3.6** Let G be the group of all 2×2 non singular matrices over the reals. Find center of G ?

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(G)$, then it should commute with all elements of G . In particular, we should have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

this lead to $b = c, a = d$.

Also

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

gives

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

this leads to $a+b = a, b = c = 0$

Hence any element $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $Z(G)$ we writ it in this form

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

In other words, elements of the centre $Z(G)$ are the 2×2 scalar matrices of G

Theorem 3.1.5 Let $H \leq G$ and $K \leq G$. Then $H \cap K \leq G$, but $H \cup K$ is not necessary to be subgroup of G .

Proof. We prove the first part of this theorem and the next example shows the last part.

Now, we show $H \cap K \leq G$

$$\begin{aligned} \text{Let } a, b \in H \cap K &\Rightarrow a, b \in H \wedge a, b \in K \\ &\Rightarrow ab^{-1} \in H \wedge ab^{-1} \in K \\ &\Rightarrow ab^{-1} \in H \cap K \\ &\Rightarrow H \cap K \leq G. \end{aligned}$$

■

■ **Example 3.7** Prove that union of two subgroups may not be a subgroup.

Solution:

Suppose that $(\mathbf{Z}, +)$ is the group of integers and let $H = \{2n \mid n \in \mathbf{Z}\}$, $K = \{3n \mid n \in \mathbf{Z}\}$, then it is easy to show H and K subgroups of \mathbf{Z} . Indeed

$$2n - 2m = 2(n - m) \in H$$

Now $H \cup K$ is not a subgroup as $2, 3 \in H \cup K$ but $2 - 3 = -1 \notin H \cup K$.

■

The next theorem obvious the union of two subgroups may be a subgroup.

Theorem 3.1.6 Union of two subgroups is a subgroup iff one of them is contained in the other.

Proof. The first direction. Let H, K be two subgroups of a group G and suppose $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G .

The other direction. Let H, K be two subgroups of G such that $H \cup K$ is also a subgroup of G . We show one of them must be contained in the other. Suppose it is not true, i.e.,

$$H \not\subseteq K \Rightarrow \exists x \in H \text{ and } x \notin K,$$

$$K \not\subseteq H \Rightarrow \exists y \in K \text{ and } y \notin H,$$

then $x, y \in H \cup K$ and since $H \cup K$ is a subgroup,

$$xy \in H \cup K \Rightarrow xy \in H \text{ or } xy \in K$$

If $xy \in H$, then as $x \in H$, $x^{-1}(xy) \in H \Rightarrow y \in H$, which is not true.

Also, if $xy \in K$, then as $y \in K$, $(xy)y^{-1} \in K \Rightarrow x \in K$ which is not true. i.e., either way we land up with a contradiction. Hence our supposition that $H \not\subseteq K$ and $K \not\subseteq H$ is wrong.

Thus, one of the two is contained in the other. ■

3.2 Exercise

- Exercise 3.1**
1. Show that $A = \{0, 2, 4\} \leq Z_6$ under addition modulo 6.
 2. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.
 3. Complete the statement “A group element x is its own inverse if and only if $|x| = \dots$ ”
 4. Let G be a group, and let $a \in G$. Prove that $N(a) = N(a^{-1})$. ■

4. Cyclic Groups

Cyclic groups are the most fundamental type of group; we've already seen instances like Z_n . Cyclic groups are useful because their entire structure can be defined easily.

In this chapter, we define and classify all cyclic groups and to understand their subgroup structure.

4.1 Definitions and Examples

Definition 4.1.1 Let G be a group and $a \in G$, then the **cyclic subgroup** generated by a is the set of all powers of a in G , and we write

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

The group G is **cyclic** iff there exists an $a \in G$ such that $G = \langle a \rangle$.

- **Example 4.1** The set $Z_n = \{0, 1, \dots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n . Again, 1 and $-1 = n-1$ are generators. ■
- **Example 4.2** Show that $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

Solution:

We note that

$$\begin{aligned}\langle 3 \rangle &= \{3, 3+3, 3+3+3, 3+3+3+3, \dots\} \\ &= \{3, 6, 9, 12, 15, 18, \dots\}.\end{aligned}$$

Thus, $Z_8 = \langle 3 \rangle$. Similarly, we find $Z_8 = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle$. ■

Theorem 4.1.1 Let G be a group and $a \in G$, then $\langle a \rangle \leq G$.

Proof. Since $e = a^0 \in \langle a \rangle$. Let $a^m, a^n \in \langle a \rangle$, then

$$a^m a^n = a^{m+n} \in \langle a \rangle.$$

Finally, if $a^m \in \langle a \rangle$, then $(a^m)^{-1} = a^{-m} \in \langle a \rangle$. Therefore, $\langle a \rangle \leq G$. ■

Theorem 4.1.2 Every subgroup of a cyclic group is cyclic.

Proof. Suppose that $G = \langle a \rangle$, and $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$, and we are done.

Now, we assume that H is not the trivial subgroup, then H contains a^m , for some $m \in \mathbb{Z}^+$. If $m < 0$, then H also contains $(a^m)^{-1} = a^{-m}$, so H contains a positive power of a . Let n be the smallest positive integer such that $a^n \in H$. We claim that $H = \langle a^n \rangle$. Surely H contains every power of a^n , so $\langle a^n \rangle \leq H$. But suppose $a^k \in H$. Then write $k = nq + r$, with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Now, H contains a^k and $(a^n)^{-q}$, and therefore $a^k (a^n)^{-q} = a^{k-nq} = a^r$. But n is the smallest positive integer such that $a^n \in H$. As $r < n$, we can only have $r = 0$. Thus, $a^k = (a^n)^q \in \langle a^n \rangle$. That is, $H \leq \langle a^n \rangle$, proving the claim. ■

■ **Example 4.3** The integers \mathbb{Z} form a cyclic group under addition, where $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. The subgroup generated by 2 is the group of even numbers under addition:

$$\langle 2 \rangle = \{2m : m \in \mathbb{Z}\} = 2\mathbb{Z} \subseteq \mathbb{Z}.$$

R The generator of a cyclic group is not unique. ■

4.2 Classification of Cyclic Groups

Theorem 4.2.1 A cyclic group is abelian group.

Proof. Let $G = \langle a \rangle$ and $x, y \in G$, then $x = a^n, y = a^m \forall n, m \in \mathbb{Z}^+$.
Now,

$$\begin{aligned} xy &= a^n a^m \\ &= a^{n+m} \\ &= a^{m+n} \\ &= a^m a^n \\ &= yx. \end{aligned}$$

■

R The converse is false for example the Klein 4-group is abelian but not cyclic.

Theorem 4.2.2 Let G be a group, and let $a \in G$, then

- (i) If $|a| = \infty$, then $a^i = a^j$ iff $i = j$.
- (ii) If $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ iff $n \mid i - j$.

Proof. (i) If $|a| = \infty$, then there no nonzero n such that $a^n = e$. Since

$$\begin{aligned} a^i = a^j &\Leftrightarrow a^{i-j} = e \\ &\Leftrightarrow a^{i-j} = a^0 \\ &\Leftrightarrow i - j = 0 \\ &\Leftrightarrow i = j. \end{aligned}$$

(ii) Suppose that $|a| = n$ and we prove that $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$. Suppose that $a^k \in \langle a \rangle$, by the division algorithm,

$$k = qn + r \quad \text{with } 0 \leq r < n,$$

then

$$\begin{aligned} a^k &= a^{qn+r} \\ &= a^{qn} a^r \\ &= (a^n)^q a^r \\ &= (e)^q a^r \\ &= ea^r \\ &= a^r, \end{aligned}$$

so $a^k \in \{e, a, a^2, \dots, a^{n-1}\}$. This proves that $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$. Next, Let $a^i = a^j$ and prove that $n \mid i - j$.

Now, since $a^i = a^j \Rightarrow a^{i-j} = e$. Again, by the division algorithm,

$$i - j = qn + r \quad \text{with } 0 \leq r < n,$$

then

$$\begin{aligned} a^{i-j} &= a^{qn+r} \\ e &= a^{qn} a^r \\ &= (a^n)^q a^r \\ &= (e)^q a^r \\ &= ea^r \\ &= a^r, \end{aligned}$$

since $|a| = n$ such that a^n is the identity, we must have $r = 0$, thus $n \mid i - j$.

Conversely, if $i - j = nq$, then

$$\begin{aligned} a^{i-j} &= a^{qn} \\ &= (a^n)^q \\ &= (e)^q \\ &= e, \end{aligned}$$

thus $a^i = a^j$. ■

Corollary 4.2.3 Let G be a group and $a \in G$, then $|a| = |\langle a \rangle|$

Corollary 4.2.4 Let G be a group and $a \in G$ with $|a| = n$. If $a^k = e$, then $n \mid k$.

Proof. Suppose that

$$a^k = e = a^0,$$

then this lead to $n \mid k$ by Theorem 4.2.2. ■

Corollary 4.2.5 Let G be a finite group. If $a, b \in G$ with $ab = ba$, then $|ab|$ divides $|a| |b|$.

Proof. Suppose that $|a| = m$ and $|b| = n$, then

$$\begin{aligned} (ab)^{mn} &= (a^m)^n (b^n)^m \\ &= (e)^n (e)^m \\ &= e, \end{aligned}$$

So by Corollary 4.2.4 and Theorem 4.2.2, we have the required. ■

Theorem 4.2.6 Let G be a group and $a \in G$ with $|a| = n$, $k \in \mathbb{Z}^+$, then

$$(i) \quad \langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle,$$

$$(ii) \quad |a^k| = \frac{n}{\gcd(n,k)}.$$

Proof. (i) Suppose that $d = \gcd(n, k)$ and let $k = dr$. Since $a^k = (a^d)^r$, this lead to $\langle a^k \rangle \subseteq \langle a^{\gcd(n,k)} \rangle$.

By the gcd theorem, we have $d = ns + kt$. So

$$\begin{aligned} a^d &= a^{ns+kt} \\ &= a^{ns} a^{kt} \\ &= (a^n)^s (a^k)^t \\ &= (e)^s (a^k)^t \\ &= (e)(a^k)^t \\ &= (a^k)^t \in \langle a^k \rangle. \end{aligned}$$

This lead to $\langle a^{\gcd(n,k)} \rangle \subseteq \langle a^k \rangle$.

Therefore, $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

(ii) First, we prove that

$$|a^d| = \frac{n}{d},$$

for any $d \mid n$.

Since $(a^d)^{\frac{n}{d}} = a^n = e$, this lead to $|a^d| \leq \frac{n}{d}$.

On the other hand, let $i \in \mathbb{Z}^+$ and $i < \frac{n}{d}$, then $(a^d)^i \neq e$. Thus,

$$|a^d| = \frac{n}{d}.$$

Now, suppose that $d = \gcd(n, k)$ to obtain

$$\begin{aligned} |a^k| &= |\langle a^k \rangle| \\ &= |\langle a^{\gcd(n,k)} \rangle| \\ &= |a^{\gcd(n,k)}| \\ &= \frac{n}{\gcd(n,k)}, \end{aligned}$$

which is a required. ■

■ **Example 4.4** Let G be a group and $a \in G$. For $|a| = 30$, find the following

1. $\langle a^{26} \rangle$, $|a^{26}|$.
2. $\langle a^{18} \rangle$, $|a^{18}|$.
3. $\langle a^{17} \rangle$ and $|a^{17}|$.

Solution:

1. Since $\gcd(30, 26) = 2$, we have

$$\begin{aligned}\langle a^{26} \rangle &= \langle a^2 \rangle \\ &= \{e, a^2, a^4, a^6, \dots, a^{28}\}.\end{aligned}$$

$$\text{Also, } |a^{26}| = |a^2| = \frac{30}{2} = 15.$$

2. Since $\gcd(30, 18) = 6$, we have

$$\begin{aligned}\langle a^{18} \rangle &= \langle a^6 \rangle \\ &= \{e, a^6, a^{12}, a^{18}, a^{24}\}.\end{aligned}$$

$$\text{Also, } |a^{18}| = |a^6| = \frac{30}{6} = 5.$$

3. Since $\gcd(30, 17) = 1$, we have

$$\begin{aligned}\langle a^{17} \rangle &= \langle a^1 \rangle \\ &= \{e, a^1, a^2, \dots, a^{29}\}.\end{aligned}$$

$$\text{Also, } |a^{17}| = |a^1| = \frac{30}{1} = 30. \quad \blacksquare$$

Corollary 4.2.7 Let G be a finite cyclic group and $a \in G$, then

$$|a| \mid |G|.$$

Corollary 4.2.8 Let $|a| = n$, then

- (i) $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n, i) = \gcd(n, j)$.
- (ii) $|a^i| = |a^j|$ iff $\gcd(n, i) = \gcd(n, j)$.

Corollary 4.2.9 Let $|a| = n$, then

- (i) $\langle a \rangle = \langle a^j \rangle$ iff $1 = \gcd(n, j)$.
- (ii) $|a| = |a^j|$ iff $1 = \gcd(n, j)$.

Corollary 4.2.10 Let $k \in \mathbb{Z}_n$, then $\langle k \rangle = \mathbb{Z}_n$ iff $\gcd(n, k) = 1$.

4.3 Classification of Subgroups of Cyclic Groups

In this section, we show how many subgroups of a finite cyclic group and how to find them.

Theorem 4.3.1 Let $|\langle a \rangle| = n$, $|H| = m$ where $H \leq \langle a \rangle$, then $m \mid n$; and, for each $k \mid n$, the group $\langle a \rangle$ has exactly one subgroup of order k —namely, $\langle a^{\frac{n}{k}} \rangle$.

Proof. Assume that $|\langle a \rangle| = n$ and H is any subgroup of $\langle a \rangle$. So, we write $H = \langle a^m \rangle$, where m is the least positive integer such that $a^m \in H$. Since $e = a^n$, we have $n = mq$ these lead to $m \mid n$.

Finally, let $k \in \mathbb{Z}^+$ with $k \mid n$. Since $|\langle a^{\frac{n}{k}} \rangle| = \frac{n}{\gcd(n, \frac{n}{k})} = k$. Now,

let $H = \langle a^m \rangle \leq \langle a \rangle$ and $|H| = k$, then $m = \gcd(n, m)$ and

$$\begin{aligned} k &= |\langle a^m \rangle| \\ &= |\langle a^{\gcd(n, m)} \rangle| \\ &= \frac{n}{\gcd(n, m)} \\ &= \frac{n}{m}, \end{aligned}$$

thus, $m = \frac{n}{k}$ and $H = \langle a^{\frac{n}{k}} \rangle$. ■

■ **Example 4.5** Find all subgroup of a cyclic group $\langle a \rangle$ where a has order 30?

Solution: We assume that $\langle a^m \rangle \leq \langle a \rangle$ where $m \mid 30$. By the Theorem 4.3.1 we find if $k \mid 30$, the subgroup of k is $\langle a^{\frac{30}{k}} \rangle$. So the list of subgroup of $\langle a \rangle$ is

$$\begin{aligned} \langle a \rangle &= \{e, a, a^2, \dots, a^{29}\}, & |\langle a \rangle| &= 30, \\ \langle a^2 \rangle &= \{e, a^2, a^4, \dots, a^{28}\}, & |\langle a^2 \rangle| &= 15, \\ \langle a^3 \rangle &= \{e, a^3, a^6, \dots, a^{27}\}, & |\langle a^3 \rangle| &= 10, \\ \langle a^5 \rangle &= \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}, & |\langle a^5 \rangle| &= 6, \\ \langle a^6 \rangle &= \{e, a^6, a^{12}, a^{18}, a^{24}\}, & |\langle a^6 \rangle| &= 5, \\ \langle a^{10} \rangle &= \{e, a^{10}, a^{20}\}, & |\langle a^{10} \rangle| &= 3, \\ \langle a^{15} \rangle &= \{e, a^{15}\}, & |\langle a^{15} \rangle| &= 2, \\ \langle a^{30} \rangle &= \{e\}, & |\langle a^{30} \rangle| &= 1. \end{aligned}$$

■

Corollary 4.3.2 For $k \in \mathbb{Z}^+$ and $k \mid n$, the set $\langle \frac{n}{k} \rangle$ is the unique and only subgroup of Z_n of order k .

■ **Example 4.6** Find the generator of subgroup of order 9 in Z_{36} ?

Solution:

Since $\frac{36}{9} = 4$ is one generator.

Now, we find the other. The Corollary 4.2.9 show that the all element of Z_{36} can written in the form $4i$ where $\gcd(9, i) = 1$ i.e., $i = \{1, 2, 4, 5, 7, 8\}$. The list of subgroup of order 9 is

$$\langle (a^4)^1 \rangle = \langle (a^4)^2 \rangle = \langle (a^4)^5 \rangle = \langle (a^4)^7 \rangle = \langle (a^4)^8 \rangle .$$

■

4.4 Euler Phi

Leonhard Euler introduced the function in 1763 which called Euler Phi. In number theory, Euler phi $\phi(n)$ counts the positive integers up to a given integer n that are relatively prime to n .

$\phi(n)$ = the number of k such that $\gcd(n, k) = 1$, where $1 \leq k \leq n$.



Leonhard Euler

1707 –1783

■ **Example 4.7** $\phi(1) = 1$. ■

■ **Example 4.8** $\phi(6) = 2$.

For $1, 5 < 6$ and $\gcd(1, 6) = \gcd(5, 6) = 1$. ■

■ **Example 4.9** $\phi(10) = 4$.

For $1, 3, 7, 9 < 10$ and $\gcd(1, 10) = \gcd(3, 10) = \gcd(7, 10) = \gcd(9, 10) = 1$ ■

- Ⓡ (i) $\phi(p) = p - 1$ if p is a prime.
 (ii) $\phi(mn) = \phi(m)\phi(n)$ if m, n relative prime.

Theorem 4.4.1 Let $d \in \mathbb{Z}^+$ and $d \mid n$. The number of elements of order d in a cyclic group of order n is $\phi(d)$.

Proof. Since the group has exactly one subgroup of order d — call it $\langle a \rangle$. Then every element of order d also generates the subgroup $\langle a \rangle$ and an element a^k generates $\langle a \rangle$ if and only if $\gcd(k, d) = 1$. The number of such elements is precisely $\phi(d)$. ■

- Ⓡ Notice that for a finite cyclic group of order n , the number of elements of order d for any divisor d of n depends only on d .

■ **Example 4.10** Let $d = 8$. Find the number of elements of order 8?

Solution:

Since $\phi(8) = 4$, for $(1, 3, 5, 7 < 8)$. Thus, the number of elements of order 8 is 4. ■

Corollary 4.4.2 In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

4.5 Exercise

- Exercise 4.1**
1. Find the generators of the cyclic group $G = \langle a \rangle$ of orders 7, 10 and 21.
 2. Let $G = \langle a \rangle$ be cyclic group. Then prove that $G = \langle a^{-1} \rangle$.
 3. Every element of a cyclic group generates the group. Prove that.
 4. Prove Corollary 4.4.2.
 5. Complete the statement: $|a| = |a^2|$ if and only if $|a| \dots$
 6. Complete the statement: $|a^2| = |a^{12}|$ if and only if \dots
 7. Let a be a group element and $|a| = \infty$. Complete the following statement: $|a^i| = |a^j|$ if and only if \dots



5. Permutation Groups

The permutation group, often known as the symmetric group, is made up of all possible permutations of n objects. An invertible function from a set to itself is called a permutation. S_n is the most common abbreviation for the group. It is a central object of study in group theory since it is a group of order $n!$.

Definition 5.0.1 Let $S = \{1, 2, \dots, n\}$ be a finite group. A 1 – 1 corresponding from S to S is said to be permutation of degree n . If $\alpha \in S_n$, then we can write it in this form

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$$

(S_n, \circ) is called **symmetric group of order n** and this group non abelian when $n \geq 3$.

Definition 5.0.2 Composition of permutations expressed in array notation is carried out from right to left by going from top to bottom,

then again from top to bottom.

■ **Example 5.1** Let S_3 be the set of all one-to-one functions from $\{1, 2, 3\}$ to itself. Then S_3 , under function composition, is a group with six elements. The six elements are

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Note that $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha^2\beta \neq \alpha\beta$, so that S_3 is non-Abelian.

■

Cycle Notion

There is another notation commonly used to specify permutations. It's known as cycle notation, and it was originally used in 1815 by the brilliant French mathematician Cauchy. When cycle notation is employed, certain important aspects of the permutation may be easily computed, which has theoretical advantages.

Augustin-Louis Cauchy

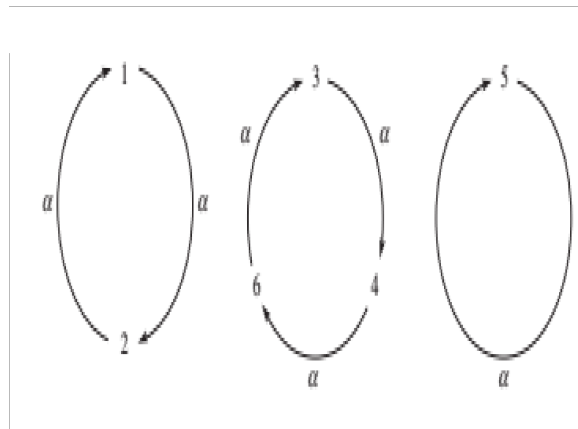


Cauchy around 1840. Lithography by Zéphirin Belliard after a painting by Jean Roller.

As an example of cycle notation. Let α be a permutations in a set S_6 where

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

This assignment of values could be presented schematically as follows.



Although mathematically satisfactory, such diagrams are cumbersome. Instead, we leave out the arrows and simply write

$$\alpha = (1 \ 2)(3 \ 4 \ 6)(5) = (1 \ 2)(3 \ 4 \ 6).$$

In general, $(a_1 \ a_2 \ \dots \ a_n)$ is a cycle of length n or an n -cycle.

■ **Example 5.2** Let α, β, γ be a permutations of a set S_4 , where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

then

1. Write α, β, γ in a cycle notation?
2. Find $\alpha \circ \beta$?
3. Find α^{-1} ?

Solution:

1.

$$\begin{aligned}
 \alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\
 &= \begin{pmatrix} 2 & 3 & 4 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
 &= \begin{pmatrix} 3 & 4 & 1 & 2 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\
 &= \begin{pmatrix} 4 & 1 & 2 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
 &= (13)(2)(4) \\
 &= (13),
 \end{aligned}$$

$$\begin{aligned}
 \beta &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\
 &= (1\ 4\ 3\ 2), \\
 \gamma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\
 &= (1\ 3)(24).
 \end{aligned}$$

2. The composition of the two permutations α, β is defined as follow:

$$\begin{aligned}
 \alpha \circ \beta &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
 &= (1\ 4)(2\ 3)
 \end{aligned}$$

3. The inverse of a permutation β is defined as follow:

$$\beta^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1 \ 2 \ 3 \ 4)$$

and the permutation $I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is the identity. ■

Definition 5.0.3 We say that there is an inversion in a permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix},$$

if for $i < j$ we have: $\frac{\alpha(i) - \alpha(j)}{i - j} < 0$ or, in other words, when a bigger number precedes a smaller number in α , and the total number of inversions in α is denoted by V_α

Definition 5.0.4 A permutation is called even (odd) permutation if the number of its inversions is even (odd).

R The group of even permutations of n symbols is denoted by A_n and is called the **alternating group** of degree n .

■ **Example 5.3** Find the number of inversions in a permutation define as follows:

1. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

2. $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

3. $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

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

Solution:

1. $V_\alpha = 2 + 1 + 0 + 0 = 3$ (odd), so it is odd.
2. $V_\beta = 3 + 0 + 0 + 0 = 3$ (odd), so it is odd.
3. $V_\gamma = 2 + 2 + 0 + 0 = 4$ (even), so it is even.
4. $V_\rho = 3 + 3 + 1 + 4 + 1 + 1 + 0 + 0 = 13$ (odd).

■

R

1. The identity permutation is an even permutation.
2. The composition of two even (odd) permutations is even permutation, while the composition of two permutations one of them even and the other odd is odd permutation
3. A group S_n has an equal number of even and odd permutations.

5.1 Properties of Permutations

In this section, we will study the properties of permutations.

Theorem 5.1.1 Every permutation of a finite set can be written as a cycle or a product of disjoint cycles.

Proof. Suppose that $\alpha \in S_n$, and for any $a_1 \in S$. Let

$$a_2 = \alpha(a_1),$$

$$a_3 = \alpha(a_2) = \alpha^2(a_1),$$

:

etc, until

$$a_1 = \alpha^m(a_1),$$

for some $m \leq n$. Thus, $(a_1 a_2 \dots a_m)$ is a cycle of α .

If $m < n$, then we choose any element $b_1 \in S$ such that b_1 is not in the first cycle, and let

$$\begin{aligned} b_2 &= \alpha(b_1), \\ b_3 &= \alpha(b_2) = \alpha^2(b_1), \\ &\vdots \end{aligned}$$

etc, until

$$b_1 = \alpha^k(b_1),$$

for some $k \leq n$. Now, we have a second cycle $(b_1 b_2 \dots b_k)$ is a cycle of α .

If $\alpha^i(a_1) = \alpha^j(b_1)$ for some i, j , then $\alpha^{i-j}(a_1) = b_1$ and this lead to $b_1 \in (a_1 a_2 \dots a_m)$ which gives contradiction.

If $m+k < n$, then we continue as above until there are no elements left. Thus

$$\alpha = (a_1 a_2 \dots a_m)(b_1 b_2 \dots b_k)\dots(c_1 c_2 \dots c_s).$$

■

Theorem 5.1.2 If the pair of cycles $\alpha = (a_1 a_2 \dots a_m)$ and $\beta = (b_1 b_2 \dots b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof. Assume that α and β are permutations of S where

$$S = \{a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n, c_1, c_2, \dots, c_k\}.$$

Now, we show that $\alpha\beta(x) = \beta\alpha(x) \forall x \in S$.

If $x = a_i$ for some i , since β fixes all a elements,

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

with $a_{m+1} = a_1$ and

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1},$$

therefore $\alpha\beta = \beta\alpha$ on the a elements. A similar argument shows $\alpha\beta = \beta\alpha$ on the b elements. Since α and β both fix the c elements,

$$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i,$$

and

$$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i.$$

Thus $\alpha\beta(x) = \beta\alpha(x) \forall x \in S$. ■

■ **Example 5.4** In S_6 ,

$$\beta = (1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

and

$$\gamma = (2\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{pmatrix}$$

then we find

$$\alpha = \beta\gamma = \gamma\beta = (1\ 3)(2\ 5\ 6) = (2\ 5\ 6)(13)$$

since the cycles are disjoint. ■

■ **Example 5.5** In S_8 , let $\alpha = (1382)(47)(56)$ and $\beta = (283)(476)$.

Then

$$\beta\alpha = (283)(476)(1382)(47)(56) \neq (12)(465).$$

This means $\alpha\beta \neq \beta\alpha$ ■

■ **Example 5.6** In S_8 , let $\alpha = (14)(263)(587)$ and $\beta = (18)(26)(35)(47)$.

Then

$$\alpha\beta = (1\ 7)(2\ 3\ 8\ 4\ 5)$$

and

$$\beta\alpha = (1\ 7\ 3\ 5)(48).$$

■

■ **Example 5.7** Find $Z(S_3)$?

Solution:

Since

$$S_3 = \{I, (12), (13), (23), (123), (132)\},$$

and

$$Z(S_3) = \{\alpha \in S_3 : \alpha\beta = \beta\alpha \forall \beta \in S_3\},$$

Then

$$Z(S_3) = \{I\}.$$

■

The next theorem is an powerful tool for calculating the orders of permutations and the number of permutations of a particular order.

Theorem 5.1.3 The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

■ **Example 5.8** Find the order of:

(i) $(1\ 3\ 2)(4\ 5)$.

(ii) $(1\ 4\ 3\ 2)(5\ 6)$.

(iii) $(1\ 2\ 3)(4\ 5\ 6)(7\ 8)$.

(iv) $(1\ 2\ 3)(1\ 4\ 5)$.

Solution:

(i) Since $l.c.m(3, 2) = 6$, then $|(1\ 3\ 2)(4\ 5)| = 6$.

(ii) Since $l.c.m(4, 2) = 4$, then $|(1\ 4\ 3\ 2)(5\ 6)| = 4$.

(iii) Since $l.c.m(3, 3, 2) = 6$, then $|(1\ 2\ 3)(4\ 5\ 6)(7\ 8)| = 6$.

(iv) Since $(1\ 2\ 3)(1\ 4\ 5) = (1\ 4\ 5\ 3\ 2)$, then $|(1\ 4\ 5\ 3\ 2)| = 5$. ■

■ **Example 5.9** In S_7 , find the list of disjoint and distinct cycles?

Solution:

Since $|S_7| = 7! = 5040$. Now we need only consider the possible

disjoint cycle structures of the elements of S_7 . For convenience, we denote an n -cycle by (n) . Then, arranging all possible disjoint cycle structures of elements of S_7 according to longest cycle lengths left to right, we have

cycle	order
(7)	7
$(6)(1)$	6
$(5)(2)$	10
$(5)(1)(1)$	5
$(4)(3)$	12
$(4)(2)(1)$	8
$(4)(1)(1)(1)$	4
$(3)(3)(1)$	3
$(3)(2)(2)$	6
$(3)(2)(1)(1)$	6
$(3)(1)(1)(1)(1)$	3
$(2)(2)(2)(1)$	2
$(2)(2)(1)(1)(1)$	2
$(2)(1)(1)(1)(1)(1)$	2
$(1)(1)(1)(1)(1)(1)(1)$	1

Theorem 5.1.4 Every permutation in S_n , $n > 1$, is a product of **2-cycles** or **transpositions**.

Proof. Since

$$(1) = (12)(21),$$

thus (1) is a product of 2 -cycles. By Theorem 5.1.1, for any $\alpha \in S_n$

we can write

$$\alpha = (a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_t) \cdots (c_1 c_2 \cdots c_s)$$

Then

$$\alpha = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(b_1 b_t)(b_1 b_{t-1}) \cdots (b_1 b_2) \cdots \\ (c_1 c_s)(c_1 c_{s-1}) \cdots (c_1 c_2)$$

■

■ **Example 5.10** $(12345) = (54)(53)(52)(51)$.

$(12345) = (54)(52)(21)(25)(23)(13)$. ■

Lemma 5.1 If $I = \beta_1 \beta_2 \cdots \beta_r$ where the β s are 2-cycles, then r is even.

Theorem 5.1.5 If $\alpha \in S_n$ and $\alpha = \beta_1 \beta_2 \cdots \beta_r = \gamma_1 \gamma_2 \cdots \gamma_s$ where the β 's and γ 's are 2-cycles, then r and s are both even or both odd.

Theorem 5.1.6 The set of even permutations in S_n forms a subgroup of S_n .

Proof. Suppose that $\alpha, \beta \in S_n$ are both even, then $\alpha\beta$ is also even since it is an even number of 2-cycles followed by an even number of 2-cycles. Since multiplication is closed for even permutations, we have a subgroup by the previous theorem. ■

5.2 Exercises

Exercise 5.1 1. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}$$

Compute each of the following.

a. α^{-1}

b. $\beta\alpha$

c. $\alpha\beta$

2. Let

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

and

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

. Write α , β , and $\alpha\beta$ as

a. products of disjoint cycles;

b. products of 2-cycles.

3. Write each of the following permutations as a product of disjoint, cycles.

a. $(1235)(413)$

b. $(13256)(23)(46512)$

c. $(12)(13)(23)(142)$

4. Find the order of each of the following permutations.

a. (14)

b. (147)

c. (14762)

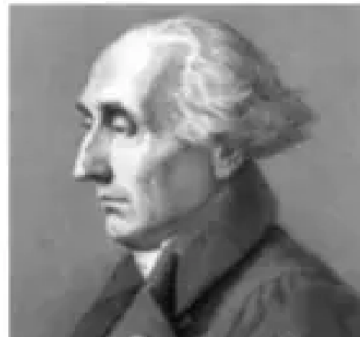
d. $(a_1 a_2 \cdots a_k)$

■

LAGRANGE'S THEOREM

Lagrange theorem exists in many fields, respectively

- Lagrange theorem in fluid mechanics
- Lagrange theorem in calculus
- Lagrange theorem in number theory
- Lagrange's theorem in group theory



6. Lagrange's Theorem

The order of a subgroup must divide the order of the group, according to Lagrange's Theorem, one of the most significant results in finite group theory. This theorem is a useful tool for analyzing finite groups since it tells us what kind of subgroups we should expect a finite group to have. The concept of a coset is important to understand Lagrange's Theorem.

Definition 6.0.1 Let $H \leq G$ and $a, b \in G$, we say a is congruent to $b \pmod{H}$ if $ab^{-1} \in H$, and we write $a \equiv b \pmod{H}$.

It is easy to prove that this relation is an equivalence relation. For any $a \in G$, the equivalence class of a , we define as follow

$$cl(a) = \{x \in G \mid x \equiv a \pmod{H}\}.$$

Definition 6.0.2 Let H be a subgroup of G and let $a \in G$ be any element. Then $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G .

■ **Example 6.1** Let $H = \{0, 3, 6\} \leq \mathbb{Z}_9$ under addition. Then the cosets

of H in Z_9 are

$$0 + H = \{0, 3, 6\} = 3 + H = 6 + H,$$

$$1 + H = \{1, 4, 7\} = 4 + H = 7 + H,$$

$$2 + H = \{2, 5, 8\} = 5 + H = 8 + H.$$

■

■ **Example 6.2** Let $H \leq S_3$, where $H = \{(1), (123), (132)\}$. Then the left cosets of H are

$$(1)H = (123)H = (132)H = \{(1), (123), (132)\}$$

$$(12)H = (13)H = (23)H = \{(12), (13), (23)\}$$

Also, the right cosets of H are exactly the same as the left cosets:

$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$

$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}$$

■

Ⓡ It is not always the case that a left coset is the same as a right coset.

Next example explain the above remark.

■ **Example 6.3** Let $K \leq S_3$, where $K = \{(1), (12)\}$. Then the left cosets of K are

$$(1)K = (12)K = \{(1), (12)\}$$

$$(13)K = (123)K = \{(13), (123)\}$$

$$(23)K = (132)K = \{(23), (132)\}$$

however, the right cosets of K are

$$K(1) = K(12) = \{(1), (12)\}$$

$$K(13) = K(132) = \{(13), (132)\}$$

$$K(23) = K(123) = \{(23), (123)\}$$

■

Now, the next theorem show that any right coset of H in G is an equivalence class.

Theorem 6.0.1 $Ha = \{x \in G \mid x \equiv a \pmod{H}\} = cl(a)$ for any $a \in G$.

Proof. Let $x \in Ha$, then $x = ha$ for some $h \in H$ this lead to

$$\begin{aligned} \Rightarrow xa^{-1} &= h \\ \Rightarrow xa^{-1} &\in H \\ \Rightarrow x &\equiv a \pmod{H} \\ \Rightarrow x &\in cl(a), \end{aligned}$$

thus, $Ha \subseteq cl(a)$.

Also, let $x \in cl(a)$, then

$$\begin{aligned} x \equiv a \pmod{H} &\Rightarrow xa^{-1} \in H \\ &\Rightarrow xa^{-1} = h \quad \text{for some } h \in H \\ &\Rightarrow x = ha \in Ha \end{aligned}$$

thus, $cl(a) \subseteq Ha$, therefore, $Ha = cl(a)$ ■

Now, we show the properties of cosets

Lemma 6.1 Let $H \leq G$ and $a, b \in G$. Then the following are satisfied.

1. $a \in aH$.
2. $aH = H$ iff $a \in H$.
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4. $aH = bH$ iff $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \emptyset$.
6. $aH = bH$ iff $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ iff $H = aHa^{-1}$.
9. $aH \leq G$ iff $a \in H$.

Proof. 1. Since $a = ae$ this lead to $a \in aH$.

2. (\Rightarrow) Suppose that $aH = H$. Then

$$a = ae \in aH = H.$$

(\Leftarrow) Assume that $a \in H$ then

$$aH \subseteq H \quad \rightarrow (1)$$

Since $a \in H$ and $h \in H$, we know that

$$a^{-1}h \in H.$$

Thus,

$$\begin{aligned} h &= eh \\ &= (aa^{-1})h \\ &= a(a^{-1}h) \in aH. \end{aligned}$$

So

$$H \subseteq aH \quad \rightarrow (2)$$

From (1) and (2), we have $H = aH$.

3. This follows directly from

$$(ab)h = a(bh),$$

and

$$h(ab) = (ha)b.$$

4. (\Rightarrow) Suppose that $aH = bH$, then

$$a = ae \in aH = bH.$$

(\Leftarrow) If $a \in bH$ we have $a = bh$ where $h \in H$, and therefore

$$\begin{aligned} aH &= (bh)H \\ &= b(hH) \\ &= bH. \end{aligned}$$

5. Property 5 follows directly from property 4, for if there is an element c in $aH \cap bH$, then $cH = aH$ and $cH = bH$.

6. Since $aH = bH$ if and only if $H = a^{-1}bH$.

7. Exercises.

8. Note that $aH = Ha$ if and only if

$$\begin{aligned} (aH)a^{-1} &= (Ha)a^{-1} \\ &= H(aa^{-1}) \\ &= H, \end{aligned}$$

that is, if and only if $aHa^{-1} = H$.

9. (\Rightarrow) If aH is a subgroup, then it contains the identity e . Thus,

$$aH \cap eH \neq \emptyset,$$

and, by property 5, we have $aH = eH = H$. Thus, from property 2, we have $a \in H$.

(\Leftarrow) If $a \in H$, then, again by property 2, $aH = H$. ■

6.1 Lagrange's Theorem.

In this section, we show the Lagrange's Theorem.

Theorem 6.1.1 If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Proof. Let $|G| = n$. For any element in G , we can define a right coset of H in G , the number of distinct right cosets of H in G is less than or equal to n . Using the properties of equivalence classes we know

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r,$$

and this lead to

$$|G| = |Ha_1| + |Ha_2| + \dots + |Ha_r|$$

Finally, since $|Ha_i| = |H|$ for each i , we have $|G| = r|H|$. ■

Definition 6.1.1 Let G be a group and $H \leq G$, then the **index** of H in G is the number of distinct right (left) cosets of H in G and denoted by $[G : H]$.

Ⓡ By Lagrang's theorem we find

$$[G : H] = \frac{|G|}{|H|}$$

Corollary 6.1.2 Let G be a finite group, for each element $a \in G$, then

$$|a| \mid |G|.$$

Corollary 6.1.3 A group of prime order is cyclic.

Proof. Assume that G has prime order and let $e \neq a \in G$, then

$$|\langle a \rangle| \mid |G|$$

with $|\langle a \rangle| \neq 1$. Thus, $|\langle a \rangle| = |G|$ and the corollary follows. ■

Corollary 6.1.4 Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

Proof. By Corollary 6.1.2 we find

$$|G| = m |a| \quad \forall m \in \mathbb{Z}^+$$

then

$$a^{|G|} = a^{m|a|} = e^m = e.$$

■

Now, we show the Fermat's Theorem.

Theorem 6.1.5 For any integer a and prime p .

$$a^p \equiv a \pmod{p}$$

Proof. If $(a, p) = 1$, then by Euler's theorem

$$\begin{aligned} a^{\phi(p)} &\equiv 1 \pmod{p} \\ \Rightarrow a^{p-1} &\equiv 1 \pmod{p} \quad \text{as } \phi(p) = p-1 \\ \Rightarrow a^p &\equiv a \pmod{p} \end{aligned}$$

If $(a, p) = p$, then $p|a \Rightarrow p|a^p$

$$\begin{aligned} \therefore p &| a^p - a \\ \Rightarrow a^p &\equiv a \pmod{p} \end{aligned}$$

(Note $(a, p) = 1$ or p as 1 and p are only divisors of p)

■

Definition 6.1.2 Let $H, K \leq G$, then we define

$$Hk = \{hk : h \in H \wedge k \in K\}$$

Theorem 6.1.6 $HK \leq G$ iff $HK = KH$.

Theorem 6.1.7 If H and K are finite subgroups of a group G , then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof. Let $D = H \cap K$ then D is a subgroup of K and as in the proof of Lagrange's theorem, \exists a decomposition of K into disjoint right cosets of D in K and

$$K = Dk_1 \cup Dk_2 \cup \dots \cup Dk_t$$

so $t = \frac{|K|}{|D|}$

Again, $HK = H \left(\bigcup_{i=1}^t Dk_i \right)$ and since $D \subseteq H, HD = H$.

Thus

$$HK = \bigcup_{i=1}^t Hk_i = Hk_1 \cup Hk_2 \cup \dots \cup Hk_t.$$

Now no two of Hk_1, Hk_2, \dots, Hk_t can be equal as if $Hk_i = Hk_j$ for some i, j then

$$\begin{aligned} k_i k_j^{-1} \in H &\Rightarrow k_i k_j^{-1} \in H \cap K \\ &\Rightarrow k_i k_j^{-1} \in D \\ &\Rightarrow Dk_i = Dk_j, \end{aligned}$$

which is not true.

$$\begin{aligned} |HK| &= |Hk_1| + |Hk_2| + \dots + |Hk_p| \\ &= |H| + |H| + \dots + |H| \\ &= t |H| \\ &= \frac{|H| \cdot |K|}{|H \cap K|}, \end{aligned}$$

which proves the result. ■

Lemma 6.2 If H and K are subgroups of a finite group G such that

$$|H| > \sqrt{|G|},$$

$$|K| > \sqrt{|G|},$$

then

$$|H \cap K| > 1.$$

Proof. We have

$$\begin{aligned} |G| &\geq |HK| \\ &= \frac{|H||K|}{|H \cap K|} \\ &> \frac{\sqrt{|G|} \cdot \sqrt{|G|}}{|H \cap K|} \\ &= \frac{|G|}{|H \cap K|} \\ &\Rightarrow |H \cap K| > 1 \end{aligned}$$

■

■ **Example 6.4** Let $G = S_3$, and suppose $H = \{I, (12)\}$, $K = \{I, (13)\}$, then $|H| = |K| = 2$ and

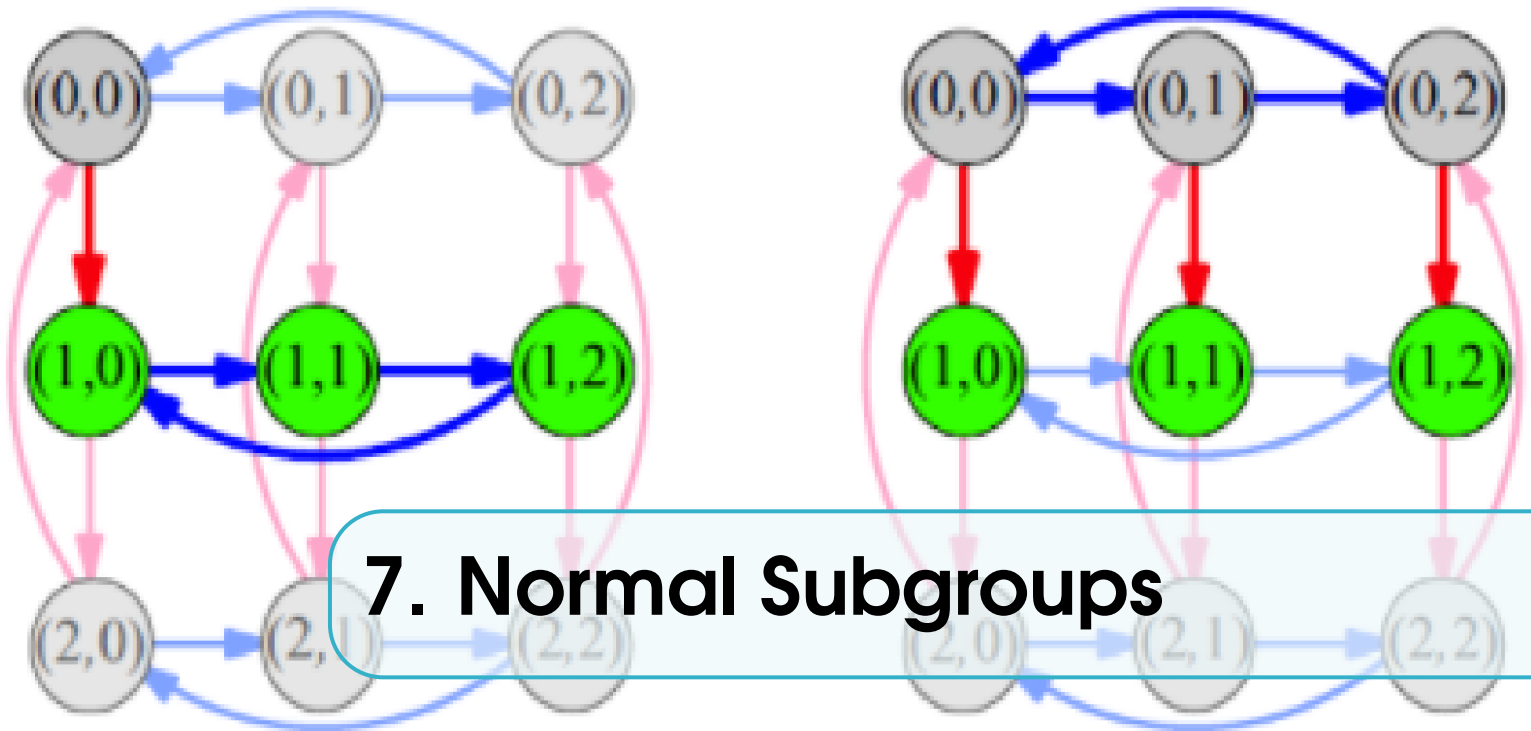
$$|HK| = \frac{2 \times 2}{1} = 4$$

Since $4 \nmid 6 = |G|$, HK is not a subgroup of G . ■

6.2 Exercises

- Exercise 6.1**
1. Find all cosets of the subgroup $4\mathbb{Z}$ of \mathbb{Z} .
 2. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.
 3. Find all cosets of the subgroup $\langle 2 \rangle$ of \mathbb{Z}_{12} .
 4. Find all cosets of the subgroup $\langle 4 \rangle$ of \mathbb{Z}_{12} .
 5. Find all cosets of the subgroup $\{18\}$ of \mathbb{Z}_{36} .
 6. Mark each of the following true or false.
 - a. Every subgroup of every group has left cosets (.....).
 - b. The number of left cosets of a subgroup of a finite group divides the order of the group (.....).
 - c. Every group of prime order is abelian (.....).
 - d. One cannot have left cosets of a finite subgroup of an infinite group (.....).
 - e. A subgroup of a group is a left coset of itself (.....).
 - f. Only subgroups of finite groups can have left cosets (.....).
 - g. A_n is of index 2 in S_n for $n > 1$ (.....).
 - h. The theorem of Lagrange is a nice result (.....).
 - i. Every finite group contains an element of every order that divides the order of the group (.....).
 - j. Every finite cyclic group contains an element of every order that divides the order of the group (.....).

■



7. Normal Subgroups

A normal subgroup is one that is invariant under conjugation by members of the group it belongs to. Normal subgroups are useful because they may be used to create quotient groups for a given group. Furthermore, the kernels of group homomorphisms with domain G are the normal subgroups of G .

Definition 7.0.1 A subgroup N of a group G is called a **normal subgroup** (invariant or self conjugate subgroup) of G if

$$Na = aN, \quad \forall a \in G$$

We use the notation $H \trianglelefteq G$ to convey that H is normal in G .

- Ⓡ G and $\{e\}$ are clearly normal subgroups of G , and they are known as the trivial normal subgroups.
- Ⓡ Subgroups of abelian groups are always normal.

Definition 7.0.2 A group $G \neq \{e\}$ is called a **simple group** if the only normal subgroups of G are $\{e\}$ and G .

- R Any group of prime order is simple. Also, this group has no subgroups except $\{e\}$ and G .

- R If H is a normal subgroup of G and K is a subgroup of G s.t., $H \subseteq K \subseteq G$ then H is normal in K .

- R If G is abelian, all its subgroups will be normal.

■ **Example 7.1** Show that $H = \{1, -1\}$ is a normal subgroup of the Quaternion group G ?

Solution:

Since $Ha = \{a, -a\} = aH$ for any $a \in G$, then $H \trianglelefteq G$. ■

■ **Example 7.2** The center $Z(G)$ of a group is always normal. ■

The two theorems that follow provide comparable criteria for a subgroup of a group to be normal. As a result, any of these might be used to define a normal subgroup.

Theorem 7.0.1 A subgroup $H \leq G$ of a group G is normal in G iff $g^{-1}Hg = H$ for all $g \in G$.

Proof. Suppose that H is a normal in G then

$$\begin{aligned} Hg = gH &\Rightarrow g^{-1}Hg = g^{-1}(gH) \\ &= (g^{-1}g)H = H. \text{ for all } g \in G. \end{aligned}$$

Conversely, let $g^{-1}Hg = H$ for all $g \in G$. Then

$$\begin{aligned} g(g^{-1}Hg) &= gH \Rightarrow (gg^{-1})Hg = gH \\ &\Rightarrow Hg = gH \end{aligned}$$

Hence H is normal. ■

Theorem 7.0.2 A subgroup H of a group G is normal in G iff $g^{-1}hg \in H$ for all $h \in H, g \in G$

Proof. Suppose that H is a normal in G , then

$$Hg = gH \text{ for all } g \in G$$

Let $h \in H, g \in G$ be any elements, then

$$\begin{aligned} hg &\in Hg = gH \\ \Rightarrow hg &= gh \text{ for some } h \in H \\ \Rightarrow g^{-1}hg &= h \in H. \end{aligned}$$

This establishes the claim.

Conversely, let $g \in G$ be any element, then

$$\begin{aligned} g^{-1}hg &\in H \text{ for all } h \in H \\ \Rightarrow g(g^{-1}hg) &\in gH \text{ for all } h \in H \\ \Rightarrow hg &\in gH \\ \Rightarrow Hg &\subset gH. \end{aligned}$$

Taking $b = g^{-1}$, we note, as $b \in G$

$$\begin{aligned} b^{-1}hb &\in H, \quad h \in H \\ \Rightarrow ghg^{-1} &\in H \\ \Rightarrow (ghg^{-1})g &\in Hg \\ \Rightarrow gh &\in Hg \\ \Rightarrow gH &\subseteq Hg \end{aligned}$$

Hence $Hg = gH$, showing H is normal. ■

■ **Example 7.3** The group $SL(2, \mathbb{R})$ of 2×2 is a normal subgroup of $GL(2, \mathbb{R})$. Verify that?

Solution:

Let $x \in GL(2, \mathbb{R}) = G$, $h \in SL(2, \mathbb{R}) = H$, and note that

$$\begin{aligned} \det(x^{-1}hx) &= (\det x)^{-1}(\det h)(\det x) \\ &= (\det x)^{-1}(\det x) \\ &= 1. \end{aligned}$$

So, $x^{-1}hx \in H$. ■

7.1 Quotient Group

Let $N \trianglelefteq G$, then the cosets of N in G form a group G/N under the operation $(aN)(bN) = abN$. This group is called the quotient or factor group of G and N .

Theorem 7.1.1 Let $N \trianglelefteq G$, then the cosets of N in G form a group G/N of order $[G : N]$

Proof. Let $Na, Nb \in G/N$, then

$$NaNb = Nab \in G/N.$$

Let $Na, Nb, Nc \in G/N$, then

$$\begin{aligned} Na(NbNc) &= Na(Nbc) \\ &= Na(bc) \\ &= N(ab)c \\ &= NabNc \\ &= (NaNb)Nc. \end{aligned}$$

There exists $Ne \in G/N$ will act as identity of G/N .

For any $Na \in G/N$ there exists Na^{-1} will be the inverse of Na .

Thus G/N forms a group. The order of G/N is, of course, the number of cosets of N in G . ■

R It is easy to see that if G is abelian then so would be any of its quotient groups as

$$\begin{aligned} NaNb &= Nab \\ &= Nba \\ &= NbNa. \end{aligned}$$

R The elements in a factor group are sets of elements in the original group.

■ **Example 7.4** Let $4Z = \{0, \pm 4, \pm 8, \dots\}$. Find $Z/4Z$.

Solution:

Firstly, we must determine the left cosets of $4Z$ in Z . If $k \in Z$, then

$$k = 4q + r,$$

where $0 \leq r < 4$; and, therefore,

$$\begin{aligned} k + 4Z &= r + 4q + 4Z \\ &= r + 4Z. \end{aligned}$$

Thus, the following four cosets:

$$\begin{aligned} 0 + 4Z &= 4Z = \{0, \pm 4, \pm 8, \dots\} \\ 1 + 4Z &= \{1, 5, 9, \dots, -3, -7, -11, \dots\} \\ 2 + 4Z &= \{2, 6, 10, \dots, -2, -6, -10, \dots\} \\ 3 + 4Z &= \{3, 7, 11, \dots, -1, -5, -9, \dots\}, \end{aligned}$$

and there are no others. Its Cayley table is

	$0 + 4Z$	$1 + 4Z$	$2 + 4Z$	$3 + 4Z$
$0 + 4Z$	$0 + 4Z$	$1 + 4Z$	$2 + 4Z$	$3 + 4Z$
$1 + 4Z$	$1 + 4Z$	$2 + 4Z$	$3 + 4Z$	$0 + 4Z$
$2 + 4Z$	$2 + 4Z$	$3 + 4Z$	$0 + 4Z$	$1 + 4Z$
$3 + 4Z$	$3 + 4Z$	$0 + 4Z$	$1 + 4Z$	$2 + 4Z$

■ **Example 7.5** Let $G = Z_{18}$ and let $H = \langle 6 \rangle = \{0, 6, 12\}$. Find G/H .

Solution:

$$G/H = \{0 + H, 1 + H, 2 + H, 3 + H, 4 + H, 5 + H\}. \quad \blacksquare$$

Theorem 7.1.2 Let G is a finite group and $N \trianglelefteq G$, then

$$|G/N| = \frac{|G|}{|N|}$$

Proof. Since G is finite, using Lagrange's theorem

$$\begin{aligned} \frac{|G|}{|N|} &= \text{number of distinct right cosets of } N \text{ in } G \\ &= |G/N|. \end{aligned}$$

■

Theorem 7.1.3 Every quotient group of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ be a cyclic group. Then G is abelian, so every subgroup of G is normal. Suppose that $H \leq G$. Now we show G/H is a cyclic. In fact we claim G/H is generated by Ha . Let $Hx \in G/H$ be any element. Then $x \in G = \langle a \rangle$, i.e., x will be some power of a . Let

$$x = a^m.$$

Then

$$\begin{aligned} Hx &= Ha^m = Haa \dots a \quad (m \text{ times}) \\ &= HaHa \dots Ha \quad (m \text{ times}) \\ &= (Ha)^m, \end{aligned}$$

so any element Hx of G/H is a power of $Ha \Rightarrow Ha$ generates G/H or that G/H is cyclic. ■

Theorem 7.1.4 Let G be a group such that $G/Z(G)$ is cyclic, then G is abelian.

Proof. Assume that $Z(G) = N$. Then G/N is cyclic. Suppose it is generated by Ng . Let $a, b \in G$ and $Na, Nb \in G/N$ such that $Na = (Ng)^n, Nb = (Ng)^m$ for some n, m . Then

$$\begin{aligned} Na = Ng^n &\Rightarrow ag^{-n} \in N. \\ Nb = Ng^m &\Rightarrow bg^{-m} \in N. \end{aligned}$$

We put

$$\begin{aligned} ag^{-n} = x &\Rightarrow a = xg^n, \\ bg^{-m} = y &\Rightarrow b = yg^m, \end{aligned}$$

for some $x, y \in N$. Now,

$$\begin{aligned} ab &= (xg^n)(yg^m) = x(g^ny)g^m \\ &= x(yg^n)g^m \text{ as } y \in N = Z(G) \\ &= xyg^{n+m} \\ &= xyg^{n+m}. \end{aligned}$$

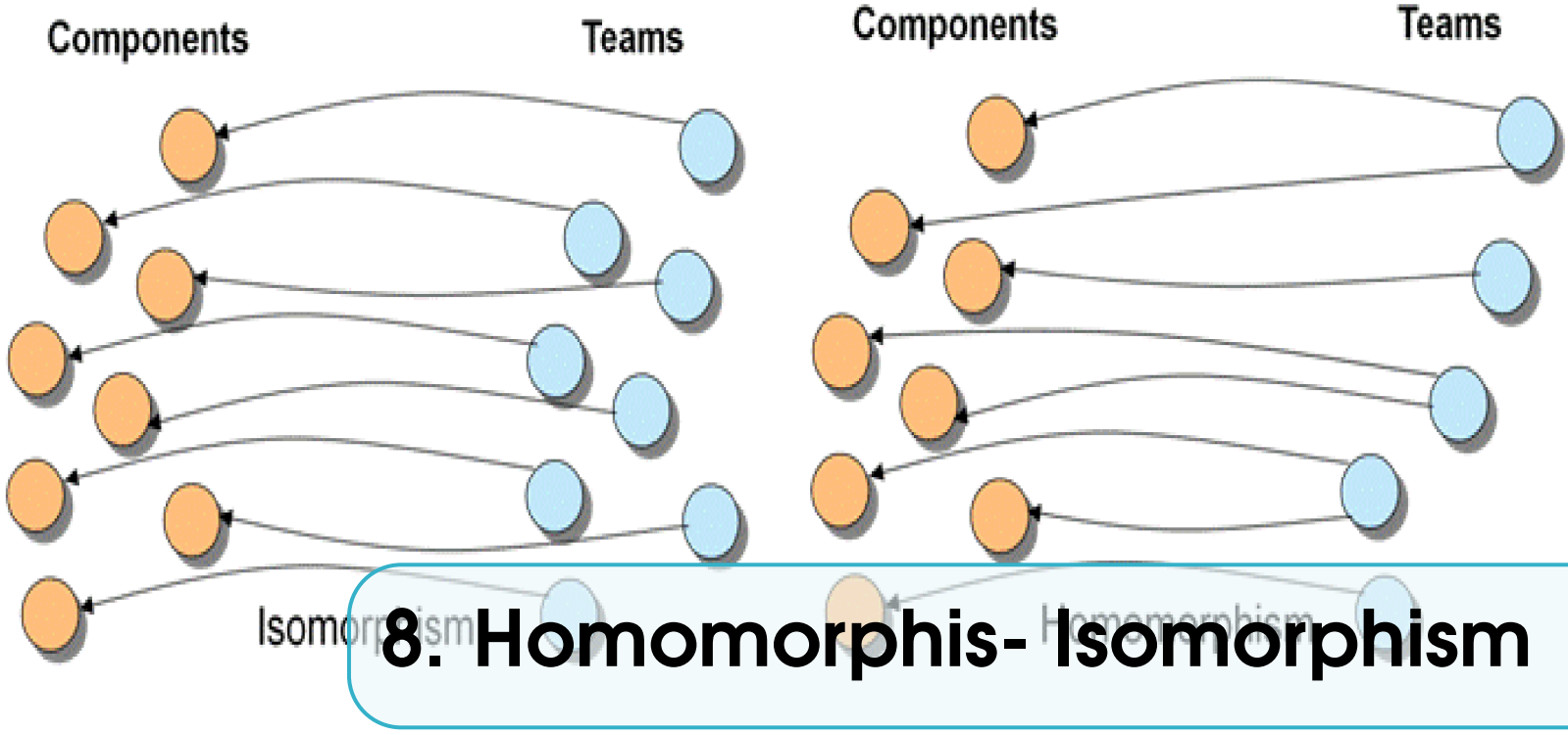
Similarly,

$$\begin{aligned} ba &= (yg^m)(xg^n) = y(g^mx)g^n = y(xg^m)g^n \\ &= (yx)g^{m+n}. \end{aligned}$$

i.e., $ab = ba$ as $xy = yx \forall x, y \in Z(G)$. Thus, G is abelian. ■

7.2 Exercise

- Exercise 7.1**
1. Show that every subgroup of a cyclic group is normal.
 2. Show that intersection of two normal subgroups is a normal subgroup.
 4. If H and N are two subgroups of G such that N is normal in G then show that $H \cap N$ is a normal subgroup of H . Show by an example that $H \cap N$ may not be normal in G .
 5. Every subgroup of an abelian group is normal. Prove that converse is not true. (Consider Quaternion group).
 6. Prove that center of a group is a normal subgroup. ■



8. Homomorphisms - Isomorphism

A structure-preserving map between two algebraic structures of the same type is called a homomorphism. The concept "homomorphism" first appears in 1892, given by (attributed to) the German mathematician Felix Klein (1849–1925).

Definition 8.0.1 Let (G, \star) and (Q, \circ) be two groups. A mapping f is called **Homomorphism** if

$$f(a \star b) = f(a) \circ f(b) \quad \forall a, b \in G$$

■ **Example 8.1** Let G be a group and $g \in G$. Show that a map $\phi : \mathbb{Z} \rightarrow G$ by $\phi(n) = gn$ is a group homomorphism?

Solution:

Let $m, n \in \mathbb{Z}$, then ϕ

$$\begin{aligned} \phi(m+n) &= g(m+n) \\ &= gm + gn \\ &= \phi(m) + \phi(n) \end{aligned}$$

Therefore, ϕ is a group homomorphism. ■

- Definition 8.0.2**
- (i) An onto homomorphism is called epimorphism.
 - (ii) A one-one homomorphism is called monomorphism.
 - (iii) A homomorphism from a group G to itself is called an endomorphism of G .
 - (iv) A one-one and onto homomorphism is called isomorphism.
 - (v) An isomorphism from a group G to itself is called automorphism of G .

■ **Example 8.2** Let $(\mathbf{Z}, +)$ and $(\mathbf{E}, +)$ be the groups of integers and even integers. Define a map $f : \mathbf{Z} \rightarrow \mathbf{E}$, s.t.,

$$f(x) = 2x \text{ for all } x \in \mathbf{Z}$$

then f is well defined as

$$\begin{aligned} x = y &\Rightarrow 2x = 2y \\ &\Rightarrow f(x) = f(y) \end{aligned}$$

that f is 1 – 1 is clear by taking the steps backwards.

f is a homomorphism for

$$\begin{aligned} f(x + y) &= 2(x + y) \\ &= 2x + 2y \\ &= f(x) + f(y). \end{aligned}$$

Also f is onto as any even integer $2x$ would have x as its pre-image. Hence f is an isomorphism. ■

■ **Example 8.3** Let G be a group and $N \trianglelefteq G$. Define a map

$$\begin{aligned} f : G &\rightarrow G/N \text{ s.t.} \\ f(x) &= Nx, \quad x \in G \end{aligned}$$

then f is clearly well defined. Again

$$\begin{aligned} f(xy) &= Nxy \\ &= NxNy \\ &= f(x)f(y) \end{aligned}$$

shows f is a homomorphism. It is sometimes called the natural (or canonical) homomorphism. ■

8.1 Properties of Subgroups Under Homomorphisms

Theorem 8.1.1 Let $f : G \rightarrow G'$ be a homomorphism, then

(i) $f(e) = e'$.

(ii) $f(x^{-1}) = (f(x))^{-1}$.

(iii) $f(x^n) = [f(x)]^n$, n an integer,

where e, e' are identity elements of G and G' respectively.

Proof. (i) Since

$$\begin{aligned} e \cdot e &= e \Rightarrow f(e \cdot e) = f(e) \\ &\Rightarrow f(e) \cdot f(e) = f(e) \\ &\Rightarrow f(e) \cdot f(e) = f(e) \cdot e' \\ &\Rightarrow f(e) = e' \text{ (cancellation)} \end{aligned}$$

(ii) Also, since

$$\begin{aligned} xx^{-1} = e = x^{-1}x &\Rightarrow f(xx^{-1}) = f(e) = f(x^{-1}x) \\ &\Rightarrow f(x)f(x^{-1}) = e' = f(x^{-1})f(x) \\ &\Rightarrow (f(x))^{-1} = f(x^{-1}). \end{aligned}$$

(iii) Let n be an integer number, then

$$\begin{aligned} f(x^n) &= f(\underbrace{xx \dots x}_{(n \text{ times})}) \\ &= f(x)f(x) \dots f(x) \quad (n \text{ times}) \\ &= (f(x))^n. \end{aligned}$$

■

Definition 8.1.1 Let $f : G \rightarrow G'$ be a homomorphism. The Kernel of f , (denoted by $\text{Ker } f$) is defined by

$$\text{Ker } f = \{x \in G \mid f(x) = e'\},$$

where e' is identity of G'

Theorem 8.1.2 Let $f : G \rightarrow G'$ be a homomorphism, then $\text{Ker } f \trianglelefteq G$.

Proof. Since $f(e) = e', e \in \text{Ker } f$, thus $\text{Ker } f \neq \emptyset$. Let

$$x, y \in \text{Ker } f \Rightarrow f(x) = e', f(y) = e'$$

Now

$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1}) \\ &= f(x)(f(y))^{-1} \\ &= e' \cdot e'^{-1} \\ &= e' \\ &\Rightarrow xy^{-1} \in \text{Ker } f. \end{aligned}$$

Hence $\text{Ker } f \leq G$.

Again, for any $g \in G, x \in \text{Ker } f$

$$\begin{aligned} f(g^{-1}xg) &= f(g^{-1})f(x)f(g) \\ &= (f(g))^{-1}f(x)f(g) \\ &= (f(g))^{-1}e'f(g) \\ &= (f(g))^{-1}f(g) = e' \\ &\Rightarrow g^{-1}xg \in \text{Ker } f. \end{aligned}$$

So $\text{Ker } f \trianglelefteq G$. ■

Theorem 8.1.3 A homomorphism $f : G \rightarrow G'$ is 1-1 iff $\text{Ker } f = \{e\}$.

Theorem 8.1.4 Let f be a homomorphism from a group G to a group \bar{G} and let g be an element of G . Then

1. If $|g|$ is finite, then $|f(g)|$ divides $|g|$.
2. $\text{Ker } f \leq G$.
3. $f(a) = f(b)$ if and only if $a\text{Ker } f = b\text{Ker } f$.
4. If $f(g) = \bar{g}$, then $f(g) = \{x \in G : f(x) = \bar{g}\} = g\text{Ker } f$.

Proof. 1. Let $|g| = n$, then $g^n = e$.

Now

$$\begin{aligned} e &= f(e) \\ &= f(g^n) \\ &= (f(g))^n. \end{aligned}$$

Thus, $|f(g)|$ divides $|g|$.

2. Exercise.
3. First assume that $f(a) = f(b)$. Then

$$\begin{aligned} e &= (f(b))^{-1}f(a) \\ &= f(b^{-1})f(a) \\ &= f(b^{-1}a), \end{aligned}$$

thus $b^{-1}a \in \text{Ker } f$ and since $\text{ker } f \trianglelefteq G$, this argument completes the proof.

4. Exercise. ■

Theorem 8.1.5 Let f be a homomorphism from a group G to a group \bar{G} and let $H \leq G$. Then

1. $f(H) = \{f(h) \mid h \in H\} \leq \bar{G}$.
2. If H is cyclic, then $f(H)$ is cyclic.
3. If H is Abelian, then $f(H)$ is Abelian.
4. If H is normal in G , then $f(H)$ is normal in $f(G)$.
5. If $|\text{Ker } f| = n$, then f is an n -to-1 mapping from G onto $f(G)$.
6. If $|H| = n$, then $|f(H)|$ divides n .
7. If \bar{K} is a subgroup of \bar{G} , then $f^{-1}(\bar{K}) = \{k \in G \mid f(k) \in \bar{K}\}$ is a subgroup of G .
8. If \bar{K} is a normal subgroup of \bar{G} , then $f^{-1}(\bar{K}) = \{k \in G \mid f(k) \in \bar{K}\}$ is a normal subgroup of G .
9. If f is onto and $\text{Ker } f = \{e\}$, then f is an isomorphism from G to \bar{G} .

Proof. 1. Since $e \in H$, then we have $f(e) \in f(H)$, so that $f(H)$ is not empty..

Let $x, y \in f(H)$, then $x = f(h_1)$ and $y = f(h_2)$ and this lead to

$$\begin{aligned} xy^{-1} &= f(h_1)(f(h_2))^{-1} \\ &= f(h_1)f(h_2)^{-1} \\ &= f(h_1h_2^{-1}) \in f(H). \end{aligned}$$

So, $f(H) \leq \bar{G}$.

2. Exercises.
3. Exercises.

4. Assume $f(h) \in f(H)$ and $f(g) \in f(G)$. Then

$$f(g)f(h)f(g)^{-1} = f\left(ghg^{-1}\right) \in f(H),$$

since H is normal in G .

5. Exercises.

6. Exercises.

7. Clearly, $e \in f^{-1}(\bar{K})$, so that $f^{-1}(\bar{K})$ is not empty.

Suppose that $k_1, k_2 \in f^{-1}(\bar{K})$. Then, by the definition of $f^{-1}(\bar{K})$, we know that $f(k_1), f(k_2) \in \bar{K}$. Thus,

$$f(k_2)^{-1} \in \bar{K}$$

and

$$f\left(k_1k_2^{-1}\right) = f(k_1)f(k_2)^{-1} \in \bar{K}.$$

So, by the definition of $f^{-1}(\bar{K})$, we have

$$k_1k_2^{-1} \in f^{-1}(\bar{K}).$$

8. Exercises.

9. Exercises.

■

■ **Example 8.4** Define $f : Z_{12} \rightarrow Z_{12}$ by $f(x) = 3x$. Verify that f is a homomorphism and Find $\text{Ker } f$?

Solution:

Since

$$\begin{aligned} f(x \oplus_{12} y) &= 3((x \oplus_{12} y)) \\ &= 3x \oplus_{12} 3y \\ &= f(x) \oplus_{12} f(y). \end{aligned}$$

So f is homomorphism.

Since the solution of

$$f(x) = 0,$$

in Z_{12} is $\text{Ker } f$ i.e., $\text{Ker } f = \{0, 4, 8\}$.

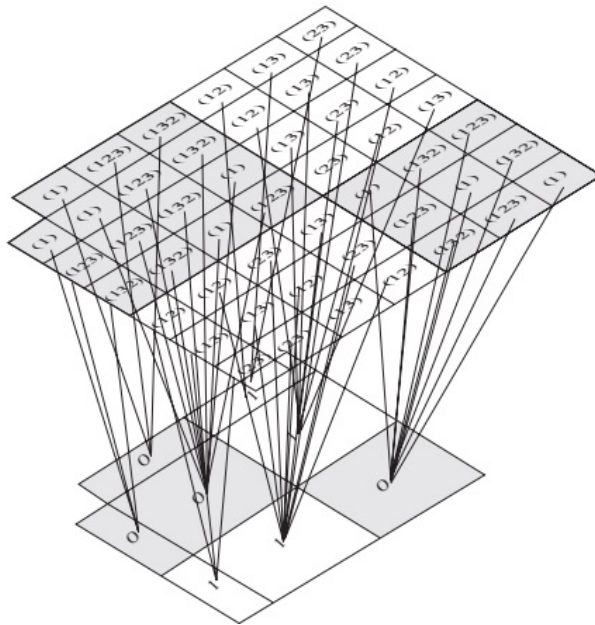
We apply some properties of the previous theorems:

By property 5 of Theorem 8.1.5 that f is a 3-to-1 mapping. Since $f(2) = 6$, we have by property 4 of Theorem 8.1.4 that $f^{-1}(6) = 2 \oplus_{12} \text{Ker } f = \{2, 6, 10\}$. Also that $\langle 2 \rangle$ is cyclic and $f(\langle 2 \rangle) = \{0, 6\}$ is cyclic. Moreover, $|2| = 6$ and $|f(2)| = |6| = 2$, so $|f(2)|$ divides $|2|$ in agreement with property 1 of Theorem 8.1.4. Letting $\bar{K} = \{0, 6\}$, we see that the subgroup $f^{-1}(\bar{K}) = \{0, 2, 4, 6, 8, 10\}$. This verifies property 7 of Theorem 8.1.5 in this particular case. ■

■ **Example 8.5** The mapping $f : S_3 \rightarrow Z_2$ define by

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is odd} \\ 0 & \text{if } \alpha \text{ is even} \end{cases}$$

is homomorphism. Verify that? ■



8.2 The isomorphism theorems

Now, we show the fundamental theorem of group homomorphism.

Theorem 8.2.1 If $f : G \rightarrow G'$ be an onto homomorphism with $K = \text{Ker } f$, then

$$G/K \cong G'.$$

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G .

Proof. Firstly, we define a map $\varphi : G/K \rightarrow G'$, s.t.

$$\varphi(Ka) = f(a), \quad a \in G$$

Now, we show φ is an isomorphism.

Since φ is well defined as follows

$$\begin{aligned} Ka = Kb &\Rightarrow ab^{-1} \in K = \text{Ker } f \\ &\Rightarrow f(ab^{-1}) = e' \\ &\Rightarrow f(a)(f(b))^{-1} = e' \\ &\Rightarrow f(a) = f(b) \\ &\Rightarrow \varphi(Ka) = \varphi(Kb) \end{aligned}$$

The next step, we will prove that φ is 1-1?

Since

$$\begin{aligned} \varphi(KaKb) &= \varphi(Kab) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \varphi(Ka)\varphi(Kb). \end{aligned}$$

So φ is a homomorphism. To check that φ is onto, let $g' \in G'$ be any element. Since $f : G \rightarrow G'$ is onto, $\exists g \in G$, s.t.

$$\begin{aligned} f(g) &= g' \\ \varphi(Kg) &= f(g) = g' \end{aligned}$$

Showing there by that Kg is the required pre-image of g' under φ . Hence φ is an isomorphism. ■

The second theorem of isomorphism shown in the following.

Theorem 8.2.2 Let $H, K \leq G$, where $H \trianglelefteq G$, then

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Proof. Since $H \cap K \trianglelefteq K$ and as $H \subseteq HK \subseteq G$, H will be normal in HK . Firstly, we define a map

$$f : K \rightarrow \frac{HK}{H} \text{ s.t. } f(k) = Hk$$

this map well define for

$$\begin{aligned} k_1 = k_2 &\Rightarrow Hk_1 = Hk_2 \\ &\Rightarrow f(k_1) = f(k_2). \end{aligned}$$

Also, this mapping is homomorphism

$$\begin{aligned} f(k_1k_2) &= Hk_1k_2 \\ &= Hk_1Hk_2 \\ &= f(k_1)f(k_2). \end{aligned}$$

That f is onto by using Fundamental theorem, we find

$$\frac{HK}{H} \cong \frac{K}{\text{Ker } f}$$

Since

$$\begin{aligned} k \in \text{Ker } f &\Leftrightarrow f(k) = H \\ &\Leftrightarrow Hk = H \\ &\Leftrightarrow k \in H \\ &\Leftrightarrow k \in H \cap K \quad (k \in K \text{ as } \text{Ker } f \subseteq K) \end{aligned}$$

We find $\text{Ker } f = H \cap K$ and our theorem is proved. ■

Now, we show the third theorem of isomorphism.

Theorem 8.2.3 If $H, K \trianglelefteq G$ such that $H \subseteq K$, then

$$\frac{G}{K} \cong \frac{G/H}{K/H}$$

Proof. Obvious $\frac{K}{H} \trianglelefteq \frac{G}{H}$ and, therefore, we can talk of $\frac{G/H}{K/H}$. ■

Firstly, we define a map

$$f: \frac{G}{H} \rightarrow \frac{G}{K} \text{ s.t., } f(Ha) = Ka, \quad a \in G$$

Now, we prove f is well defined as

$$\begin{aligned} Ha = Hb &\Rightarrow ab^{-1} \in H \subset K \\ &\Rightarrow Ka = Kb \\ &\Rightarrow f(Ha) = f(Hb). \end{aligned}$$

Also, f is a homomorphism as

$$\begin{aligned} f(HaHb) &= f(Hab) \\ &= Kab \\ &= KaKb \\ &= f(Ha)f(Hb). \end{aligned}$$

The mapping f is onto by Using Fundamental theorem of group homomorphism as follow

$$\frac{G}{K} \cong \frac{G/H}{\text{Ker } f}$$

We claim $\text{Ker } f = \frac{K}{H}$. The element of $\text{Ker } f$ will be some element of $\frac{G}{H}$.

Now

$$\begin{aligned} Ha \in \text{Ker } f &\Leftrightarrow f(Ha) = K \quad (\text{identity of } G/K) \\ &\Leftrightarrow Ka = K \\ &\Leftrightarrow a \in K \\ &\Leftrightarrow Ha \in \frac{K}{H} \end{aligned}$$

Hence we find

$$\frac{G}{K} \cong \frac{G/H}{K/H}$$

which proves our result.

8.3 Exercises

Exercise 8.1 1- A homomorphism $f : G \rightarrow G'$ is 1-1 iff $\text{Ker } f = \{e\}$. Prove that.

2- Let f be a homomorphism from a group G to a group \bar{G} and let g be an element of G . Then

(i) $f(a) = f(b)$ if and only if $a\text{Ker } f = b\text{Ker } f$.

(ii) If $f(g) = \bar{g}$, then $f(g) = \{x \in G : f(x) = \bar{g}\} = g\text{Ker } f$. 3- Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

(a) $\phi : \mathbb{R}^* \rightarrow GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : \mathbb{R} \rightarrow GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \rightarrow \mathbb{R}$ defined by

$$\phi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \rightarrow \mathbb{R}^*$ defined by

$$\phi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \rightarrow \mathbb{R}$ defined by

$$\phi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = b$$

where $\mathbb{M}_2(\mathbb{R})$ is the additive group of 2×2 matrices with entries in \mathbb{R} . ■



9. Direct product, direct sum

Definition 9.0.1 Let G_1 and G_2 be two groups, then $G_1 \times G_2$ denote the set of all ordered pairs with first component coming from the group G_1 and second component coming from the group G_2 :

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}.$$

Define componentwise multiplication on $G_1 \times G_2$ by

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2).$$

Theorem 9.0.1 $G_1 \times G_2$ is a group under componentwise multiplication.

Proof. We need to check the three group axioms.

(G1) The proof of associativity of componentwise multiplication.

(G2) We claim that (e_1, e_2) is an identity element, where e_i is the identity element of $G_i (i = 1, 2)$. For $(x_1, x_2) \in G_1 \times G_2$, we have

$$(e_1, e_2)(x_1, x_2) = (e_1x_1, e_2x_2) = (x_1, x_2)$$

and similarly $(x_1, x_2)(e_1, e_2) = (x_1, x_2)$. Therefore, (e_1, e_2) is an identity element.

(G3) Let $(x_1, x_2) \in G_1 \times G_2$. We claim that (x_1^{-1}, x_2^{-1}) is an inverse of (x_1, x_2) . We have

$$(x_1^{-1}, x_2^{-1})(x_1, x_2) = (x_1^{-1}x_1, x_2^{-1}x_2) = (e_1, e_2)$$

and similarly

$$(x_1, x_2)(x_1^{-1}, x_2^{-1}) = (e_1, e_2).$$

Therefore, (x_1^{-1}, x_2^{-1}) is an inverse of (x_1, x_2) . ■



- $G_1 \times G_2$ is the **direct product** of the groups G_1 and G_2 .
- If the groups G_1 and G_2 are additive groups, then the direct product is called the **direct sum** and it is denoted $G_1 \oplus G_2$. In this case, the operation is denoted $+$ and it is called componentwise addition:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$



10. Ring

Definition 10.0.1 A ring is a set R with two binary operations, usually denoted $+$ and \cdot , such that

1. $(R, +)$ is an abelian group.
2. (R, \cdot) is a semi-group.
3. For any a, b, c in R , $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definition 10.0.2 A ring R is called a **ring with unity** (or sometimes a unital ring) if there exists an element, denoted 1 , which has the property that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Definition 10.0.3 A ring R is called a **commutative ring**, if

$$a \cdot b = b \cdot a,$$

for all $a, b \in R$.

Definition 10.0.4 A ring R with identity $1 \neq 0$, is called a **division ring** (or **skew field**) if every nonzero element $a \in R$ has a multiplica-

tive inverse, i.e.,

$$\exists b \in R \text{ such that } ab = ba = 1.$$

A commutative division ring is called a field.

- **Example 10.1** 1. The ring of integers \mathbb{Z} , under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1).
- 2. Similarly, the rational numbers \mathbb{Q} , the real numbers \mathbb{R} , and the complex numbers \mathbb{C} , are commutative rings with identity (in fact they are fields).
- 3. The quotient group Z/nZ is a commutative ring with identity (the element 1) under the operations of addition and multiplication of residue classes.
- 4. The set of all $n \times n$ matrices over real numbers is non commutative rings with identity I .
- 5. The set

$$M_{2 \times 2} = \left\{ \begin{pmatrix} 2a & 2b \\ 2c & 3d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

is non commutative rings without identity I .

■

Proposition 10.0.1 Let R be a ring. Then

- (1) $0a = a0 = 0$ for all $a \in R$.
- (2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
- (3) $(-a)(-b) = ab$ for all $a, b \in R$.
- (4) If R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof. (1) Since $0a = (0 + 0)a = 0a + 0a$. The equality $(-a)b = -(ab)$ in (2) follows from $ab + (-a)b = (a + (-a))b = 0b = 0$. The rest follow similarly. ■

Definition 10.0.5 Let R be a ring.

(1) A nonzero element a of R is called a **zero divisor** if there is a nonzero element $b \in R$ such that either

$$ab = 0 \quad \text{or} \quad ba = 0.$$

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a **unit** in R if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted R^\times .

R The units in a ring R form a group under multiplication so R^\times will be referred to as the group of units of R .

Definition 10.0.6 A **field** is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.

R A zero divisor can never be a unit.

■ **Example 10.2** The ring \mathbb{Z} of integers has no zero divisors and its only units are ± 1 , i.e., $\mathbb{Z}^\times = \{\pm 1\}$ ■

Definition 10.0.7 A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

■ **Example 10.3** The ring of integers is an integral domain. ■

■ **Example 10.4** The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain. ■

■ **Example 10.5** The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain. ■

■ **Example 10.6** The ring \mathbb{Z}_p of integers modulo a prime p is an integral domain, also, is field. ■

■ **Example 10.7** The ring $M_2(\mathbb{Z})$ of 2×2 matrices over the integers is not an integral domain. ■

Theorem 10.0.2 Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In particular, if a, b , and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof. If $ab = ac$ then $a(b - c) = 0$ so either $a = 0$ or $b - c = 0$. The second, from $ab = ac$, we have $a(b - c) = 0$. Since $a \neq 0$, we must have $b - c = 0$ ■

Theorem 10.0.3 A finite integral domain is a field.

Theorem 10.0.4 For every prime p , \mathbb{Z}_p , the ring of integers modulo p is a field.

Proof. By using Theorem 10.0.3, we need only prove that \mathbb{Z}_p has no zero divisors. So, suppose that $a, b \in \mathbb{Z}_p$ and $ab = 0$. Then $ab = pk$ for some integer k . Since p is prime this lead to, $p \mid a$ or $p \mid b$. Thus, in \mathbb{Z}_p , $a = 0$ or $b = 0$. ■

■ **Example 10.8** The ring of Gaussian integers modulo 3 define as follows

$$\begin{aligned} \mathbb{Z}_3[i] &= \{a + bi \mid a, b \in \mathbb{Z}_3\} \\ &= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}. \end{aligned}$$

Also, the table below is the multiplication table for the nonzero elements of $\mathbb{Z}_3[i]$. ■

	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$2+i$	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$2i$	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$2+2i$	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

■ **Example 10.9** Let $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$. It is easy to see that $Q[\sqrt{2}]$ is a ring. Viewed as an element of \mathbf{R} , the multiplicative inverse of any nonzero element of the form $a + b\sqrt{2}$ is simply $1/(a + b\sqrt{2})$. To verify that $Q[\sqrt{2}]$ is a field, we must show that $1/(a + b\sqrt{2})$ can be written in the form $c + d\sqrt{2}$. In high school algebra, this process is called "rationalizing the denominator." Specifically,

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2}$$

(Note that $a + b\sqrt{2} \neq 0$ guarantees that $a - b\sqrt{2} \neq 0$) ■

■ **Definition 10.0.8** A ring element a is called an **idempotent** if $a^2 = a$.

(a) If $a \neq 1$ is an idempotent element of R , then a is a zero divisor.

By definition of an idempotent element, we have $a^2 = a$.

It yields that

$$a(a - 1) = a^2 - a = 0.$$

Since $a \neq 1$, the element $a - 1$ is a nonzero element in the ring R . Thus a is a zero divisor.

(b) Suppose that \bar{R} is an integral domain. Determine all the idempotent elements of \bar{R} .

Suppose that a is an idempotent element in the integral domain \bar{R} . Thus, we have $a^2 = a$.

It follows that we have

$$a(a - 1) = a^2 - a = 0.$$

Since \bar{R} is an integral domain, there is no nonzero zero divisor. Hence from the above equation yields that $a = 0$ or $a - 1 = 0$.

Clearly, the elements 0 and 1 are idempotent. Thus, the idempotent elements in the integral domain \bar{R} must be 0 and 1.

■ **Example 10.10** Find all idempotent elements in Z_{10} ?

Solution:

Since $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then the idempotent elements are 0, 1, 5 and 6. ■

■ **Example 10.11** Find all idempotent elements in Z_5 ?

Solution:

Since $Z_5 = \{0, 1, 2, 3, 4\}$, then the idempotent elements are 0, and 1. ■

Definition 10.0.9 Let a belong to a ring R with unity, then a is called **nilpotent** when $a^n = 0$ for some positive integer n .

■ **Example 10.12** Find all nilpotent elements in Z_4 ?

Solution:

Since $Z_4 = \{0, 1, 2, 3\}$, then the nilpotent element is 2, for

$$2^2 = 0.$$

Now, we show some properties of nilpotent element. ■

Theorem 10.0.5 Let $(R, +, \cdot)$ be a commutative ring and let $a, b \in R$ be nilpotent. Then $a + b$ is nilpotent.

Theorem 10.0.6 Let $(R, +, \cdot)$ be a commutative ring and let $a \in R$ be nilpotent. Then for all $r \in R$, $r.a$ and $a.r$ are nilpotent.

Proof. Let $a \in R$ be nilpotent. Then there exists a positive integer $n \in \mathbb{N}$ such that $a^n = 0$. Let $r \in R$. Then since R is a commutative ring:

$$\begin{aligned}(r.a)^n &= r^n . a^n \\ &= r^n . 0 \\ &= 0,\end{aligned}$$

and

$$\begin{aligned}(a.r)^n &= a^n . r^n \\ &= 0 . r^n \\ &= 0.\end{aligned}$$

So $r.a$ and $a.r$ are nilpotent. ■

Theorem 10.0.7 Let $(R, +, \cdot)$ be a commutative ring and let $u, a \in R$. If u is a unit and a is nilpotent, then $u - a$ is a unit.

10.0.1 Subring

Definition 10.0.10 A subset S of a ring R is a **subring** of R if S is itself a ring with the operations of R .

■ **Example 10.13** For $n \in \mathbb{Z}^+$, the set

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

is a subring of the integers \mathbb{Z} . ■

Theorem 10.0.8 A nonempty subset S of a ring R is a subring if

$$(1) a - b \in S \quad \forall \quad a, b \in S.$$

$$(2) ab \in S \quad \forall \quad a, b \in S.$$

In the following example it is easy to apply the above theorem to prove it.

■ **Example 10.14** The set of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is a subring of the complex numbers \mathbb{C} . ■

■ **Example 10.15** The set

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

of diagonal matrices is a subring of the ring of all 2×2 matrices over \mathbb{Z} . ■

10.1 Characteristic of a Ring

Definition 10.1.1 The **characteristic of a ring** R is the least positive integer n such that

$$nx = 0 \quad \forall \quad x \in R.$$

If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\text{char } R$.

■ **Example 10.16** (1) $\text{char } (\mathbb{C}) = 0$, $\text{char } (\mathbb{R}) = 0$, $\text{char } (\mathbb{Q}) = 0$ and $\text{char } (\mathbb{Z}) = 0$.

(2) $\text{char } (\mathbb{Z}_n) = n$ since for all x in \mathbb{Z}_n we have $nx = 0$. ■

■ **Example 10.17** Prove that $R = \{0, 2, 4, 6, 8\}$ is a subring of $\langle \mathbb{Z}_{10}, \oplus_{10}, \otimes_{10} \rangle$. Find the characteristic of R .

Solution: Firstly, we will be shown that R is a subring of $\langle \mathbb{Z}_{10}, \oplus_{10}, \otimes_{10} \rangle$.
 Given $R = \{0, 2, 4, 6, 8\}$ and $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ We find that: (1) R is a nonempty subset of \mathbb{Z}_{10} .

(2) R is closed under inverse of addition and multiplication modulo 10.

Thus, R is subring of \mathbb{Z}_{10} .

Finally, we compute the characteristic of R .

Choose the positive integer $n = 1$. Take any $x \in R$, we got that $1x \neq 0$.

Choose the positive integer $n = 2$. Take any x in R , we got that $2x \neq 0$.

Choose the positive integer $n = 3$. Take any $x \in R$, we got that $3x \neq 0$.

Choose the positive integer $n = 4$. Take any $x \in R$, we got that $4x \neq 0$.

Choose the positive integer $n = 5$. Take any $x \in R$, we got that $5x = 0$.

So, the least positive integer $n = 5$ such that $nx = 0$ for all $x \in R$.

Then we conclude that $\text{char } R = 5$. ■

■ **Example 10.18** $M_2(\mathbb{Z})$ is the set of 2×2 matrices with integer entries under matrix addition and multiplication. Find the characteristic of ring $M_2(\mathbb{Z})$?

Solution:

The elements of

$$M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$$

Since there is no positive integer n such that $nx = 0$ for all $x \in M_2(\mathbb{Z})$, so the characteristic of ring $M_2(\mathbb{Z})$ is 0. ■

Next, we show the characteristic of a ring with unity.

Theorem 10.1.1 Let R be a ring with unity 1.

(i) If 1 has infinite order under addition, then the characteristic of R is 0.

(ii) If 1 has order n under addition, then the characteristic of R is n .

Proof. If 1 has infinite order, then there is no positive integer n such that $n \cdot 1 = 0$, so R has characteristic 0. Now suppose that 1 has additive order n . Then $n \cdot 1 = 0$, and n is the least positive integer with this property. So, for any x in R , we have

$$\begin{aligned} n \cdot x &= x + x + \cdots + x(n \text{ summands}) \\ &= 1x + 1x + \cdots + 1x(n \text{ summands}) \\ &= (1 + 1 + \cdots + 1)x(n \text{ summands}) \\ &= (n \cdot 1)x = 0x = 0 \end{aligned}$$

Thus, R has characteristic n . ■

■ **Example 10.19** Let ring \mathbb{Z} is the set of integer number under ordinary additon and multiplication. Find the characteristic of ring \mathbb{Z} .

Solution:

The elements of $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$. Since 1 is an identity, and then we need to find the order of element 1 in ring \mathbb{Z} . Here, the unity element 1, has infinite order. So, by using the Theorem 10.1.1 (i), we find that $\text{char}(\mathbb{Z}) = 0$. ■

■ **Example 10.20** Let set $Z_3[i] = \{a + bi | a, b \in Z_3\}$ is a ring under addition and multiplication modulo 3. Prove that $Z_3[i]$ has a unity and find the characteristic of $Z_3[i]$.

Solution:

Since $Z_3[i] = \{a + bi | a, b \in Z_3\}$ is a ring under addition and multiplication modulo 3 and

$$Z_3[i] = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$$

To prove that $Z_3[i]$ has a unity, we check from the multiplication modulo 3 table for $Z_3[i]$ (**Verify that**).

\otimes_3	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2
i
$1+i$
$2+i$
$2i$
$1+2i$
$2+2i$

We find the unity is 1. Now, we need to find the order of element 1 in ring $Z_3[i]$. Since

$$1 \cdot 1 = 1,$$

$$2 \cdot 1 = 2,$$

$$3 \cdot 1 = 0,$$

we know that $|1| = 3$. By using the Theorem 10.1.1 3, we find that $\text{char } Z_3[i] = 3$. ■

Next, we show the characteristic of an integral domain.

Theorem 10.1.2 The characteristic of an integral domain is 0 or prime.

Proof. By Theorem 10.1.1, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that $n = st$, where $1 \leq s, t \leq n$. Then

$$\begin{aligned} 0 &= n \cdot 1 \\ &= (st) \cdot 1 \\ &= (s \cdot 1)(t \cdot 1). \end{aligned}$$

So, $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since n is the least positive integer with the property that $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus, n is prime. ■

■ **Example 10.21** The ring Z_7 of integer modulo a prime 7. Show that Z_7 is an integral domain, then find the characteristic of Z_7 .

Solution:

First, we check that Z_7 is a commutative ring with unity from the multiplication table of Z_7 .

\otimes_7	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Since the multiplication modulo Z_7 in the above table is symmetrical to main diagonal, so the commutative property is satisfied. Also, the unity is 1. Furthermore, we find that Z_7 has no zero divisor, then Z_7 is an integral domain.

Now, we find the order of element 1 in ring Z_7 . Since

$$1 \otimes_7 1 = 1,$$

$$2 \otimes_7 1 = 2,$$

$$3 \otimes_7 1 = 3,$$

$$4 \otimes_7 1 = 4,$$

$$5 \otimes_7 1 = 5,$$

$$6 \otimes_7 1 = 6,$$

$$7 \otimes_7 1 = 0,$$

we know that $|1| = 7$. By using the Theorem 10.1.2, we find that $\text{char } Z_7 = 7$ is a prime number. ■

10.2 Exercises

- Exercise 10.1** (1) Find a zero divisor in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.
- (2) Find an idempotent in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.
- (3) Find all units, zero divisors, idempotent s , and nilpotent elements in Z_9 .
- (4) List all zero divisors in Z_{20} . Can you see a relationship between the zero divisors of Z_{20} and the units of Z_{20} ?
- (5) Show that every nonzero element of Z_n is a unit or a zero divisor.
- (6) Let $(R, +, \cdot)$ be a commutative ring and let $a, b \in R$ be nilpotent. Then $a + b$ is nilpotent. Prove that. ■



11. Ring Homomorphisms

Definition 11.0.1 Let R and S be rings, then a **ring homomorphism** is a map $\phi : R \rightarrow S$ satisfying

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b)\end{aligned}$$

for all $a, b \in R$.

If $\phi : R \rightarrow S$ is a one-to-one and onto homomorphism, then ϕ is called an **isomorphism of rings**.

Definition 11.0.2 Let $\phi : R \rightarrow S$ be a ring homomorphism maps, then we define the kernel of a ring homomorphism to be the set

$$\ker \phi = \{r \in R : \phi(r) = 0\}$$

- **Example 11.1** For any integer n we can define a ring homomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $a \mapsto a \pmod{n}$. This is indeed a ring homomorphism,

since

$$\begin{aligned}\phi(a+b) &= (a+b) \pmod{n} \\ &= a \pmod{n} + b \pmod{n} \\ &= \phi(a) + \phi(b)\end{aligned}$$

and

$$\begin{aligned}\phi(ab) &= ab \pmod{n} \\ &= a \pmod{n} \cdot b \pmod{n} \\ &= \phi(a)\phi(b)\end{aligned}$$

The kernel of the homomorphism ϕ is $n\mathbb{Z}$. ■

■ **Example 11.2** Let $C[a, b]$ be the ring of continuous real-valued functions on an interval $[a, b]$. For a fixed $\alpha \in [a, b]$, we can define a ring homomorphism $\phi_\alpha : C[a, b] \rightarrow \mathbb{R}$ by $\phi_\alpha(f) = f(\alpha)$. This is a ring homomorphism since

$$\begin{aligned}\phi_\alpha(f+g) &= (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g) \\ \phi_\alpha(fg) &= (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g)\end{aligned}$$

Ring homomorphisms of the type ϕ_α are called evaluation homomorphisms. ■

In the next proposition we will examine some fundamental properties of ring homomorphisms. The proof of the proposition is left as an exercise.

Proposition 11.0.1 Let $\phi : R \rightarrow S$ be a ring homomorphism.

1. If R is a commutative ring, then $\phi(R)$ is a commutative ring.
2. $\phi(0) = 0$.
3. Let 1_R and 1_S be the identities for R and S , respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.
4. If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.



12. Ideals and Factor Rings

Normal subgroups are important in group theory because they allow us to create factor groups. The comparable ideas for rings—ideals and factor rings—are introduced in this chapter.

Definition 12.0.1 A subring I of a ring R is called a (two-sided) ideal of R ($I \trianglelefteq R$) if for every $r \in R$ and every $a \in I$ both ra and ar are in I .

So, a subring I of a ring R is an ideal of R if

$$rI = \{ra \mid a \in I\} \subseteq I,$$

and

$$Ir = \{ar \mid a \in I\} \subseteq I,$$

for all $r \in R$.

R An ideal I of R is called a proper ideal of R if I is a proper subset of R .

Theorem 12.0.1 A nonempty subset I of a ring R is an ideal of R if

1. $a - b \in I$ for all $a, b \in I$.
2. $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.

■ **Example 12.1** For any positive integer n , the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is an ideal of \mathbb{Z} . ■

■ **Example 12.2** For any ring R both $\{0\}$ and R are ideals of R . ■

Definition 12.0.2 Let R be a commutative ring with unity and let $a \in R$. The set

$$\langle a \rangle = \{ra : r \in R\}$$

is an ideal of R called the **principal ideal** generated by a .

■ **Example 12.3** Let

$$R[x] = \{c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 : c_n, c_{n-1}, \dots, c_1, c_0 \in \mathbb{R}\}$$

be the set of all polynomials with real coefficients and let

$$A[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x : a_n, a_{n-1}, \dots, a_1 \in \mathbb{R}\} \subseteq R[x].$$

Then $A[x]$ is an ideal of $R[x]$ and $A = \langle x \rangle$. ■

■ **Example 12.4** Let R be a commutative ring with unity and let a_1, a_2, \dots, a_n belong to R . Then

$$I = \langle a_1, a_2, \dots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_i \in R\}$$

is an ideal of R called the ideal generated by a_1, a_2, \dots, a_n . ■

■ **Example 12.5** Let $Z[x]$ denote the ring of all polynomials with integer coefficients and let I be the subset of $Z[x]$ of all polynomials with even constant terms. Then I is an ideal of $Z[x]$ and $I = \langle x, 2 \rangle$ ■

12.1 Factor Ring

Theorem 12.1.1 Let R be a ring and let A be a subring of R . The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations

$$(s + A) + (t + A) = s + t + A,$$

and

$$(s + A)(t + A) = st + A,$$

if and only if $A \trianglelefteq R$.

Proof. Since the set of cosets forms a group under addition, Also, it is trivial to check that the multiplication is associative and that multiplication is distributive over addition. Thus, the proof boils down to showing that multiplication is well-defined if and only if $A \trianglelefteq R$. To do this, suppose that A is an ideal and let $s + A = s' + A$ and $t + A = t' + A$. Then we must show that $st + A = s't' + A$. Well, by definition, $s = s' + a$ and $t = t' + b$, where $a, b \in A$. Then

$$st = (s' + a)(t' + b) = s't' + at' + s'b + ab,$$

and so

$$st + A = s't' + at' + s'b + ab + A = s't' + A$$

Thus, multiplication is well-defined when A is an ideal.

On the other hand, suppose that A is a subring of R that is not an ideal of R . Then there exist elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. For convenience, say $ar \notin A$. Consider the elements $a + A = 0 + A$ and $r + A$. Clearly,

$$(a + A)(r + A) = ar + A,$$

but

$$(0 + A) \cdot (r + A) = 0 \cdot r + A = A.$$

Since $ar + A \neq A$, the multiplication is not well defined and the set of cosets is not a ring. ■

Definition 12.1.1 If R is a ring and I is a two-sided ideal, the quotient ring of $R \bmod I$ is the group of cosets R/I with the operations of coset addition and coset multiplication.

Proposition 12.1.2 Let R be a ring, and let I be an ideal

- (a) If R is a commutative ring, so is R/I .
 (b) If R has a multiplicative identity 1 , then $1 + I$ is a multiplicative identity for R/I . In this case, if $r \in R$ is a unit, then so is $r + I$, and $(r + I)^{-1} = r^{-1} + I$.

Proof. (a) Let $r + I, s + I \in R/I$. Since R is commutative,

$$(r + I)(s + I) = rs + I = sr + I = (s + I)(r + I)$$

Therefore, R/I is commutative.

(b) Suppose R has a multiplicative identity 1 . Let $r \in R$. Then

$$(r + I)(1 + I) = r \cdot 1 + I = r + I,$$

and

$$(1 + I)(r + I) = 1 \cdot r + I = r + I.$$

Therefore, $1 + I$ is the identity of R/I . If $r \in R$ is a unit, then

$$(r^{-1} + I)(r + I) = r^{-1}r + I = 1 + I,$$

and

$$(r + I)(r^{-1} + I) = rr^{-1} + I = 1 + I.$$

Therefore, $(r + I)^{-1} = r^{-1} + I$. ■

■ **Example 12.6** The set of even integers $\langle 2 \rangle = 2\mathbb{Z}$ is an ideal in \mathbb{Z} . Form the quotient ring $\mathbb{Z}/2\mathbb{Z}$.

Now, we show the element of $\mathbb{Z}/2\mathbb{Z}$.

The two cosets $a + 2\mathbb{Z}$ and $b + 2\mathbb{Z}$ are the same exactly when a and b differ by an even integer. Every even integer differs from 0 by an even integer. Every odd integer differs from 1 by an even integer. So there are really only two cosets

$$0 + 2\mathbb{Z} = 2\mathbb{Z}, \quad 1 + 2\mathbb{Z}$$

. Here are the addition and multiplication tables:

+	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$1 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$

\times	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$
$1 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$

It is easy to see that $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to Z_2 . ■

R In general, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to Z_n , with addition and multiplication mod n .

This remark gives a formal construction of Z_n as the quotient ring $\mathbb{Z}/n\mathbb{Z}$.

■ **Example 12.7** $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$. ■

■ **Example 12.8** $\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$. ■

12.2 Maximal ideals

Definition 12.2.1 Let R be a ring and M be an proper ideal of R . Then M is said to be a maximal ideal of R , if there is no other ideal N between M and R . That means if,

$$\text{for ideal } N, \quad M \subseteq N \implies (N = M \quad \text{or} \quad N = R)$$

■ **Example 12.9** Let p be a (positive) prime integer. Then, $p\mathbb{Z}$ is maximal ideal of \mathbb{Z} .

Proof. Suppose N is an ideal of \mathbb{Z} and $p\mathbb{Z} \subseteq N$. Since N is a subgroup of \mathbb{Z} , there is a positive integer n such that $N = n\mathbb{Z}$. Since $p\mathbb{Z} \subseteq N = n\mathbb{Z}$, we have $p = nk$. So, $n = 1$ or $k = 1$. So, $N = n\mathbb{Z} = \mathbb{Z}$ or $N = p\mathbb{Z}$. ■

Theorem 12.2.1 Let R be a commutative ring (with unity, as always) and M be an ideal. Then M is maximal iff R/M is a field.

Corollary 12.2.2 A commutative ring R is a field if and only if it has no nontrivial ideals.

12.3 Prime Ideal

Definition 12.3.1 Let R be a commutative ring and $P \neq R$ be an ideal R . Then, P is called a prime ideal

$$\forall a, b \in R, \quad (ab \in P \implies a \in P \vee b \in P)$$

■ **Example 12.10** Let n be an integer greater than 1. Then, in the ring of integers, the ideal $n\mathbb{Z}$ is prime if and only if n is prime ■

■ **Example 12.11** In $\mathbb{Z} \times \mathbb{Z}$ the ideal $\mathbb{Z} \times \{0\}$ and $\{0\} \times \mathbb{Z}$ are prime ideals. More generally, let R be an integral domain. In $R \times R$ the ideal $R \times \{0\}$ and $\{0\} \times R$ are prime ideals.

Proof. We give a proof of the later statement and prove $\mathbb{R} \times \{0\}$ is a prime ideal. First, it is easy to see $\mathbb{R} \times \{0\}$ an ideal and $\mathbb{R} \times \{0\} \neq \times \mathbb{R}$.

Now suppose $(a,b)(x,y) \in \mathbb{R} \times \{0\}$. So, $by = 0$. Since R is an integral domain, $b = 0$ or $y = 0$. So, $(a,b) \in \mathbb{R} \times \{0\}$ or $(x,y) \in \mathbb{R} \times \{0\}$. The proof is complete. ■

Lemma 12.1 Let R be a commutative ring. Then, R is an integral domain $\Leftrightarrow \{0\}$ is a prime ideal.

Theorem 12.3.1 Let R be a commutative ring and $P \neq R$ is an ideal of R . Then,

$$P \text{ is a prime ideal} \Leftrightarrow R/P \text{ is an integral domain}$$

Corollary 12.3.2 Let R be a commutative ring. Then, any maximal ideal is a prime ideal.

Proof. Let M be a maximal ideal. Then, R/M is a field. So, R/M is an integral domain. So, M is a prime ideal ■

Wish you all the best, Dr. Amr M. Elrawy