ALGEBRA-I

[MTH1C01]

STUDY MATERIAL

I SEMESTER
CORE COURSE

M.Sc. Mathematics

(2019 Admission onwards)

UNIVERSITY OF CALICUT

SCHOOL OF DISTANCE EDUCATION
CALICUT UNIVERSITY- P.O
MALAPPURAM- 673635, KERALA

190551

SCHOOL OF DISTANCE EDUCATION

UNIVERSITY OF CALICUT

STUDY MATERIAL
FIRST SEMESTER

M.Sc. Mathematics (2019 ADMISSION ONWARDS)

CORE COURSE:

MTH1C01-ALGEBRA-I

Prepared by:

Dr. Sini P
Assistant Professor
Department of Mathematics
University of Calicut

Scrutinized By:

Dr. Preethi Kuttipulackal
Associate Professor & Head
Department of Mathematics
University of Calicut

Contents

Introduction

The term group was used by Galois around 1830 to describe sets of one to one functions on finite sets that could be grouped together to form a set closed under composition. The modern definition of a group that follows is the result of long evolutionary process. The modern definition of a group was given by both Heinrich Weber and Walther von Dyck in 1982.

0.1 Groups

In order to define a group, first we define a binary operation

Definition 0.1. *Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.*

Let G be a finite set of cardinality n, then the number of binary operation on G is n^{n^2}.

Definition 0.2. *Let G be a set together with a binary operation $*$ that assigns to each ordered pair (a, b) of elements of G, an element in G denoted by $a*b$. We say that G is a group under this binary operation if the following axioms are satisfied*

1. *For all a, b, $c \in G$, we have*

$$a * (b * c) = (a * b) * c, \quad \textit{associativity of } * .$$

2. *There is an element e (identity element) in G such that $a*e = a = e*a$ for all $a \in G$*

3. *For each element $a \in G$, there is an element a' (inverse of a) in G such that $a * a' = e = a' * a$.*

In other words, a group is a set together with an associative operation such that there is an identity, every element has an inverse and any pair of elements can be combined without going outside the set.

A group G is abelian if its binary operation is commutative. In a group G, there is only one identity element. For each element a in a group G, there is a unique element b in G such that $ab = e = ba$. For group elements a, $b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Examples 0.3. 1. *The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are all groups under ordinary addition.*

2. *The set $\mathbb{Q}^+$ of positive rationals is a group under multiplication.*

3. *The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ for $n \geq 1$ is a group under addition modulo n.*

4. *The set $\{1, 2, 3, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is a prime.*

5. *The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication.*

Note that the set of integers under ordinary multiplication is not a group.

If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G. We use the notation $H \leq G$ to mean that H is a subgroup of G. If H is a subgroup of G, but $H \neq G$ itself, we write $H < G$. Such a subgroup is called proper subgroup. The subgroup $\{e\}$ is called the trivial subgroup of G.

The number of elements of a group G is called its order. The order of an element g in G is the smallest positive integer n such that $g^n = e$. If no such integer exists, we say that g has infinite order. The identity elements is always of order one and it is the only element with order one. The order of an an element and its inverse is always same.

Cyclic Group

Let G be a group and $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G, which is called the cyclic subgroup $\langle a \rangle$ of G generated by a. Note that $\langle a \rangle$ is the smallest subgroup of G containing a. If $G = \{a^n : n \in \mathbb{Z}\}$, then a is a generator of G and G is cyclic. Every cyclic group is abelian and a subgroup of a cyclic group is cyclic. A finite group is cyclic if and only if it has an element, which has the same order as that of the group itself.
We know that $\mathbb{Z}$ is a cyclic group with generator 1 or -1 and the subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.

Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.
Let G be a cyclic group of order n with generator a. Then

1. a^k is a generator of G if and only if $g.c.d(k, n) = 1$.

2. The number of generators of G is $\phi(n)$ where ϕ is the Euler ϕ-function. Since $\phi(n)$ is even for $n > 2$, the number of generators of a cyclic group is always even.

3. If d is a positive divisor of n, the number of elements of order d is $\phi(d)$ where ϕ is the Euler ϕ-function.

4. The number of subgroups of a cyclic group of order n is the number of positive divisors of n.

5. For each positive divisor d of n, G has a subgroup of order d, namely $\langle a^{n/d} \rangle$ (the cyclic group generated by $a^{n/d}$).

Symmetric Group

A permutation of a set A is a function from A to A that is both one one and onto. Let A be a non empty set and S_A be the collection of all permutations on A. Then S_A is a group under permutation multiplication (composition). Let A be a finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the symmetric group on n letters, and is denoted by S_n. Note that S_n has $n!$ elements.

Example 0.4. We know that S_3 denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself (symmetric group) and $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ where

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The multiplication table for S_3 is given the following table.

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Clearly S_3 is non abelian. Note that the symmetric group defined on a set with at least three elements is always non-abelian.

Let A be a set and $\sigma \in S_A$. We define a relation on A as follows.

$$\text{For } a,\, b \in A,\; a \sim b \Leftrightarrow b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}.$$

We can easily show that $\sim$ is an equivalence relation. The equivalence class determined by this relation is are called the orbits of σ.

A permutation $\sigma \in S_n$ is a cycle if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit. Every permutation is a product of disjoint cycles. A cycle of length 2 is a transposition. Any permutation of a finite set of at least two elements is a product of transpositions. No permutation in S_n can be expressed both as a product of even number of transpositions and as a product of odd number of transpositions. A permutation is even or odd according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions, respectively. If $n \geq 2$, the collection of even permutations of S_n forms a subgroup of order $n!/2$ and it is called the alternating group A_n on n letters.

0.2 Rings

First we recall the definition of a ring.

Definition 0.5. *A ring R is set with two binary operations, addition(+) and multiplication (.) such that for all a, b, c in R:*

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. *There is an additive identity* 0. *That is, there is an element* 0 *in* R *such that* $a + 0 = a$ *for all* $a \in R$.
4. *There is an element* $-a$ *in* R *such that* $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$.

So a ring is a abelian group under addition, also having an associative multiplication that is left and right distributive over addition.

A ring in which the multiplication is commutative is a commutative ring. A ring with a multiplicative identity element is a ring with unity. The multiplicative identity element 1 is called unity.

Let R be a ring with unity $1 \neq 0$. An element u in R is a unit of R if it has a multiplicative inverse in R. If every non zero element of R is a unit, then R is a division ring(skew field).

A zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

An integral domain is a commutative ring with unity no zero divisors.

A field F is a commutative ring with unity in which every non zero element is a unit. That is a field is a commutative division ring. A non commutative division ring is called a strictly skew field.

Module 1

Here we study direct product of groups, factor groups and group actions.

1.1 Direct Products and Finitely Generated Abelian Groups

You are familiar with various groups, finite or infinite and their subgroups. Here we will pay special attention to finitely generated abelian groups and discuss their structures. To describe the structure of these groups we need some knowledge of direct product of groups.

Definition 1.1. *Let $S_1, S_2, \ldots S_n$ be non-empty set. Then the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in S_i$ for $i = 1, 2, \ldots n$ is called the cartesian product of sets $S_1, S_2, \ldots S_n$, which is denoted by either $S_1 \times S_2 \times \ldots \times S_n$ or by $\prod_{i=1}^{n} S_i$.*
That is

$$\prod_{i=1}^{n} S_i = \{(a_1, a_2, \ldots, a_n) : a_i \in S_i, i = 1, 2, \ldots n\}.$$

Let $G_1, G_2, \ldots G_n$ be groups. We use multiplicative notation for the group operation on G_i for $i = 1, 2, \ldots, n$. Now consider $\prod_{i=1}^{n} G_i$.
Can we define a binary operation on $\prod_{i=1}^{n} G_i$ using the operations on G_i's?

Let us try the obvious method of component wise multiplication. That is, we define the operation on $\prod_{i=1}^{n} G_i$ as

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

where $a_i, b_i \in G_i$ for $i = 1, 2, \ldots, n$.

For example, if $G_1 = (\mathbb{Z}, +)$, $G_2 = (\mathbb{R}^*, \times)$ (the group of non zero real numbers under multiplication) and $G_3 = (\mathbb{Z}_6, +_6)$ (addition modulo 6), then for $(a_1, a_2, a_3),\ (b_1, b_2, b_3) \in G_1 \times G_2 \times G_3$, we have

$$(a_1, a_2, a_3)(b_1, b_2, b_3) = (a_1 + b_1, a_2 \times b_2, a_3 +_6 b_3).$$

In particular,

$$(3, 4, 5)(3, 5, 4) = (6, 20, 3).$$

Here we show that we can make $\prod_{i=1}^{n} G_i$ into a group by means of the above binary operation of component wise multiplication.

Theorem 1.2. *Let $G_1, G_2, \ldots G_n$ be groups. For $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ in $\prod_{i=1}^{n} G_i$, define*

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

Then $\prod_{i=1}^{n} G_i$ is a group under this binary operation.

Proof. Here each product a_ib_i is performed with the operation of G_i, $a_ib_i \in G_i$. So $\prod_{i=1}^{n} G_i$ is closed under the binary operation.

Let $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n)$ and $(c_1, c_2, \ldots, c_n)$ are in $\prod_{i=1}^{n} G_i$. Then

$(a_1, a_2, \ldots, a_n)[(b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)]$

$$= (a_1, a_2, \ldots, a_n)(b_1c_1, b_2c_2, \ldots, b_nc_n)$$

$$= (a_1(b_1c_1),\, a_2(b_2c_2),\, \ldots, a_n(b_nc_n))$$
$$= ((a_1b_1)c_1,\, (a_2b_2)c_2,\, \ldots, (a_nb_n)c_n)$$
$$= (a_1b_1,\, a_2b_2,\, \ldots,\, a_nb_n)(c_1,\, c_2,\, \ldots,\, c_n)$$
$$= [(a_1,\, a_2,\, \ldots, a_n)(b_1,\, b_2,\, \ldots, b_n)](c_1,\, c_2,\, \ldots, c_n).$$

Hence the above binary operation is associative in G.

Let e_i be the identity element in G_i for $i = 1,\, 2,\, \ldots, n$. Clearly $(e_1,\, e_2,\, \ldots e_n)$ is the identity element in $\prod_{i=1}^{n} G_i$.

Now the inverse of $(a_1,\, a_2,\, ..., a_n,)$ is $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$. For,

$$(a_1,\, a_2,\, ..., a_n,)(a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) = (a_1a_1^{-1}, a_2a_2^{-1}, \ldots, a_na_n^{-1}) = (e_1,\, e_2,\, \ldots e_n).$$

Note that $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) \in \prod_{i=1}^{n} G_i$. Hence G is a group. □

Note that:

1. $\prod_{i=1}^{n} G_i$ is called the direct product of the groups G_i under the above binary operation.

2. If the operation of each G_i is commutative, we use additive notation $\bigoplus_{i=1}^{n} G_i$ for $\prod_{i=1}^{n} G_i$ and is called direct sum of the groups G_i.

3. If the sets S_i has r_i elements for $i = 1,\, 2,\, \ldots, n$. Then $\prod_{i=1}^{n} S_i$ has $r_1r_2 \ldots r_n$ elements.

Let us look at some examples.

Examples 1.3. 1. Let $G_1 = (\mathbb{Z}_2, +_2)$ and $G_2 = (\mathbb{Z}_3, +_3)$. Then $G_1 \times G_2 = \mathbb{Z}_2 \times \mathbb{Z}_3$. We have

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Let (a, b), $(c, d) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. Then $(a, b) + (c, d) = (a +_2 c, b +_3 d)$. We claim that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. Here

$$\begin{aligned}
(1,1) &= (1,1) \\
2(1,1) &= (1,1) + (1,1) = (0,2) \\
3(1,1) &= (1,1) + (1,1) + (1,1) = (1,0) \\
4(1,1) &= (1,1) + (1,1) + (1,1) + (1,1) = (0,1) \\
5(1,1) &= (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (1,2) \\
6(1,1) &= (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (0,0)
\end{aligned}$$

Hence $(1, 1)$ generates the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. Hence $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group.

2. Consider $\mathbb{Z}_2 \times \mathbb{Z}_4$.

$$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}.$$

Here we claim that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cylclic. Since in $\mathbb{Z}_2$, 1 added to itself gives the identity and in $\mathbb{Z}_4$, every element added to itself four times gives the identity. Hence for any $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$,

$$(a,b) + (a,b) + (a,b) + (a,b) = (0,0).$$

That is, every element in $\mathbb{Z}_2 \times \mathbb{Z}_4$ has order less than or equal to 4. In particular there can be no element of order 8. So $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

Theorem 1.4. *The group $Z_m \times Z_n$ is isomorphic to Z_{mn} if and only if m and n are relatively prime.*

Proof. Since $Z_m \times Z_n$ and Z_{mn} had same number of elements and since Z_{mn} is cyclic, it is enough to show that $Z_m \times Z_n$ is cyclic in order to prove $Z_m \times Z_n$ is isomorphic to Z_{mn}.

Consider the cyclic subgroup of $Z_m \times Z_n$ generated by (1, 1). Then the order of this cyclic subgroup is the smallest power of (1, 1) that gives the identity (0, 0). That is, the smallest number of times adding $(1, 1)$ to itself repeatedly to give the element $(0, 0)$. The first component $1 \in \mathbb{Z}_m$ gives 0 only after m summands, $2m$ summands and so on and the second component $1 \in \mathbb{Z}_n$ gives 0 only after n summands, $2n$ summands and so on. So for $(1, 1)$ to give $(0, 0)$, the number of summands must be a multiple of both m and n. The smallest number that is a multiple of both m and n is mn if m and n are relatively prime. In this case $(1, 1)$ generates a cyclic group of order mn, which is the order of the whole group. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn and is isomorphic to $\mathbb{Z}_{mn}$ if m and n are relatively prime.

Conversely suppose that the gcd of m and n is $d > 1$. Note that $\frac{mn}{d}$ is divisible by both m and n. Let $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Then

$$\underbrace{(r,s) + (r,s) + \ldots + (r,s)}_{mn/d \text{ summands}} = (0,0).$$

Since (r, s) is arbitrary, no element (r, s) in $\mathbb{Z}_m \times \mathbb{Z}_n$ can generate the entire group. So $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic and therefore not isomorphic to $\mathbb{Z}_{mn}$. □

This theorem can be extended to a product of more than two factors by similar arguments.

Corollary 1.5. *The group $\Pi_{i=1}^{n}\mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \ldots m_n}$ if and only if the numbers m_i for $i = 1, 2, \ldots, n$ are such that gcd of any two of them is* 1.

Remark 1.6. If $n = (p_1)^{n_1}(p_2)^{n_2}\dots(p_r)^{n_r}$, product of powers of distinct primes, then $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \dots \mathbb{Z}_{(p_r)^{n_r}}$.

Example 1.7. Consider $\mathbb{Z}_7 \times \mathbb{Z}_6$. Since $gcd(6,\ 7) = 1$, $\mathbb{Z}_7 \times \mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_{42}$. Hence $\mathbb{Z}_7 \times \mathbb{Z}_6$ is a cyclic group.

Let $r, s \in \mathbb{Z}$. Then the subset of $\mathbb{Z}$ consisting of all multiples of both r and s is a subgroup of $\mathbb{Z}$ and hence it is a cyclic group. Similarly the set of all common multiples of n positive integers $r_1, r_2, \dots, r_n$ is a subgroup of $\mathbb{Z}$ and hence is cyclic.

Definition 1.8. *Let $r_1,\ r_2,\ \dots, r_n$ be positive integers. Their least common multiple(l.c.m.) is the positive generator of the cyclic group of all common multiples of the r_i, that is the cyclic group of all integers divisible by each r_i for $i = 1,\ 2,\ \dots n$.*

Consider 3, 4 and 6. The common multiples of these three numbers are $0,\ \pm 12,\ \pm 24,\ \dots$. Now consider the set $\{\dots, -24, -12, 0, 12, 24, \dots\}$, which is a cyclic subgroup of $\mathbb{Z}$ generated by 12. So $l.c.m.(3, 4, 6) = 12$.

Theorem 1.9. *Let $(a_1,\ a_2,\ \dots,\ a_n) \in \prod_{i=1}^{n} G_i$. If a_i is of order r_i in G_i, then the order of $(a_1,\ a_2,\ \dots,\ a_n)$ in $\prod_{i=1}^{n} G_i$ is the least common multiple of all the r_i.*

We need the following Theorem which you have already studied.

Theorem 1.10. *Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^m$. Then b generates a cyclic subgroup H of G containing n/d elements, where $d = gcd(m, n)$.*

So if G is a cyclic group with n elements and generated by a and $b \in G$, then $b = a^m$ for some m, $1 \leq m \leq n$ and order of $b = n/gcd(n.m)$.

Example 1.11. Find the order of (3, 10, 9) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.

$$o(3) \text{ in } \mathbb{Z}_4 = \frac{4}{gcd(3,4)} = 4$$
$$o(10) \text{ in } \mathbb{Z}_{12} = \frac{12}{gcd(12,10)} = 6$$
$$\text{and } o(9) \text{ in } \mathbb{Z}_{15} = \frac{15}{gcd(15,9)} = 5.$$

Hence the order of (3, 10, 9) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is $l.c.m.(o(3), o(10), o(9)) = l.c.m.(4, 6, 5) = 60$.

The Structure of Finitely Generated Abelian Groups

There is no formula which gives the number of groups of order n for any $n > 0$. But it is possible to classify the finite abelian groups of order n. This classification follows from the following Theorem.

Theorem 1.12. ***Fundamental Theorem for Finitely Generated Abelian Groups***

Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$$

*where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors: that is the number(***Betti number** *of G) of factors of $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.*

Proof. The proof is omitted. □

Theorem 1.12 gives us complete structural information about all finite abelian groups.

Example 1.13. Find all abelian groups up to isomorphism, of order (i) 1089 (ii) 32.

(i) We have $1089 = 3^2 11^2$. Now using Theorem 1.12, we get the following possibilities.

1. $\mathbb{Z}_9 \times \mathbb{Z}_{121}$
2. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{121}$
3. $\mathbb{Z}_9 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$
4. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

(ii) Since $32 = 2^5$ we get the following possibilities.

1. $\mathbb{Z}_{32}$
2. $\mathbb{Z}_2 \times \mathbb{Z}_{16}$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8$
4. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
6. $\mathbb{Z}_4 \times \mathbb{Z}_8$
7. $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$

Definition 1.14. *A group G is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.*

Now we give a characterisation of finite indecomposible abelian groups.

Theorem 1.15. *The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime*

Proof. Let G be a finite indecomposable abelian group. Then by Theorem 1.12, G is isomorphic to the direct product of cyclic groups of prime power order. Since G is indecomposable, this direct product must consist of just one cyclic group of prime power order.

Conversely, let p be a prime and G be a finite abelian group of order a power of p. Then

$$G \cong \mathbb{Z}_{p^r}.$$

If $\mathbb{Z}_{p^r}$ is isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, where $i+j=r$, then order of every element is atmost $p^{max\{i,j\}} < p^r$. Hence $\mathbb{Z}_{p^r}$ is indecomposable. □

Theorem 1.16. *If m divides the order of a finite abelian group G, then G has a subgroup of order m.*

Proof. Since G is a finite abelian group, by Theorem 1.12, G is isomorphic to $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}}$ where p_i are primes not necessarily distinct. So the order of the group G,

$$o(G) = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}.$$

Since m divides $o(G)$, $m = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$ where $0 \leq s_i \leq r_i$.
Note that $(p_i)^{r_i - s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ and order of this group is

$$\frac{(p_i)^{r_i}}{gcd((p_i)^{r_i}, (p_i)^{r_i - s_i})} = \frac{(p_i)^{r_i}}{(p_i)^{r_i - s_i}} = (p_i)^{s_i}.$$

Recall that $< a >$ denotes the cyclic group generated by a. Consider the subgroup $< (p_1)^{r_1 - s_1} > \times < (p_2)^{r_2 - s_2} > \times \ldots \times < (p_n)^{r_n - s_n} >$ of G. The

order the above subgroup is $p_1^{s_1}p_2^{s_2}\dots p_n^{s_n} = m$. Hence G has a subgroup of order m. □

Theorem 1.17. *If m is a square free integer(m is not divisible by square of any prime), then every abelian group of order m is cyclic.*

Proof. Let G be an abelian group of square free order m. Then by Theorem 1.12, we have

$$G \cong \mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}}$$

where $m = p_1^{r_1}p_2^{r_2}\dots p_n^{r_n}$.
Since m is square free integer, we must have $r_i = 1$ for all $i = 1, 2, \ldots, n$ and p_i are distinct primes. Then G is isomorphic to $\mathbb{Z}_{p_1p_2\dots p_n}$ and hence cyclic. □

Question 1.18. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.

Solution. Suppose that G is a finite abelian group that is not cyclic. Then by Fundamental theorem of finitely generated abelian group, G contains a subgroup isomorphic to $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ for some prime p. Otherwise G must be cyclic.

If $r = s = 1$, there is nothing to prove. If $r, s > 1$, consider the subgroup $\langle p^{r-1}\rangle \times \langle p^{s-1}\rangle$ of $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$.

$$\begin{aligned}\text{The order of } (p^{r-1}, p^{s-1}) \text{ in } \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s} &= l.c.m.(o(p^{r-1}) \text{ in } \mathbb{Z}_{p^r}, o(p^{s-1}) \text{ in } \mathbb{Z}_{p^s}) \\ &= l.c.m.(\frac{p^r}{gcd(p^r, p^{r-1})}, \frac{p^s}{gcd(p^s, p^{s-1})}) \\ &= p.\end{aligned}$$

So $\langle p^{r-1}\rangle \times \langle p^{s-1}\rangle$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Thus G contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.

Next consider the case $r = 1$ and $s > 1$. Here we consider the subgroup $\mathbb{Z}_p \times \langle p^{s-1} \rangle$ of $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$. Clearly this subgroup is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Similarly if $r > 1$ and $s = 1$, then G has a subgroup isomorphic to $\langle p^{r-1} \rangle \times \mathbb{Z}_p$, which is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Conversely assume that G contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p. Recall that every subgroup of a cylic group is cyclic and $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic. So G cannot be cyclic. ■

EXERCISES

1. Find the order of the given element of the direct product.

   a. $(2, 5)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{10}$

   b. $(3, 10, 9)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$

2. Find all abelian groups, up to isomorphism, of the given order.

   a. Order 8

   b. Order 720

   c. Order 100

3. For any two groups G_1 and G_2, show that $G_1 \times G_2 \cong G_2 \times G_1$.

4. If r is a divisor of m and s is a divisor of n, find a subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ that is isomorphic to $\mathbb{Z}_r \times \mathbb{Z}_s$.

5. Find a subgroup of $\mathbb{Z}_{800} \times \mathbb{Z}_{200}$ that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

1.2 Plane Isometries

The study of symmetry provides one of the applications of group theory. Here we study the symmetry of figures in plane in terms of the group of isometries of the plane.

Consider the Euclidean plane $\mathbb{R}^2$. An isometry of $\mathbb{R}^2$ is a permutation $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ that preserve distance, that is, for any two points P and Q in $\mathbb{R}^2$, the distance between P and Q is equal to the distance between $\phi(P)$ and $\phi(Q)$.

We can easily prove that the composition of two isometries is again an isometry. For, let ϕ and ψ be two isometries of $\mathbb{R}^2$ and $P, Q \in \mathbb{R}^2$. Then $\phi \circ \psi$ is a bijection and the distance between $(\phi \circ \psi)(P)$ and $(\phi \circ \psi)(Q)$ is same as the distance between $\psi(P)$ and $\psi(Q)$ which is equal to the distance between P and Q.

Clearly the identity map is an isometry and the inverse of an isometry is an isometry.

So the collection of all isometries of $\mathbb{R}^2$ forms a group under function composition.

Let S be a subset of $\mathbb{R}$. The isometries that carry S onto itself form a subgroup of the group of isometries and this subgroup is called the group of symmetries of of S in $\mathbb{R}^2$.
What is the group symmetries of an equilateral triangle.
The set of all isometries on $\mathbb{R}^2$ which maps the triangle to itself. That is, the ways in which two copies of an equilateral triangle with vertices 1, 2 and 3 can be placed, one covering the other. So the symmetry can interchange some of the sides and vertices.

Here we show that there is a natural correspondence between elements of the symmetric group S_3 and the group of symmetries of an equilateral triangle. Recall that S_3 denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself(symmetric group) and $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ where

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

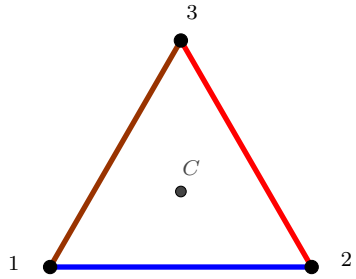
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

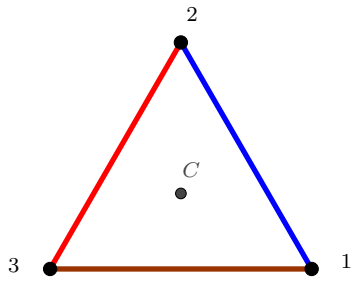
The multiplication table for S_3 is given the following table.

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Consider the following triangle.

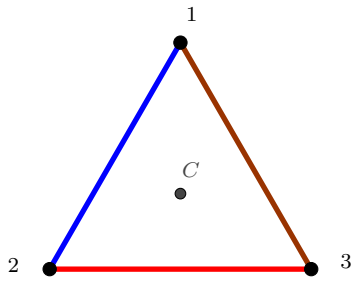


Rotate counter clockwise 120° about the centre C of this equilateral triangle, then we get the following figure.



We can think this rotation as a map on vertices. That is, $1 \to 2$, $2 \to 3$ and $3 \to 1$. Here we get the map $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

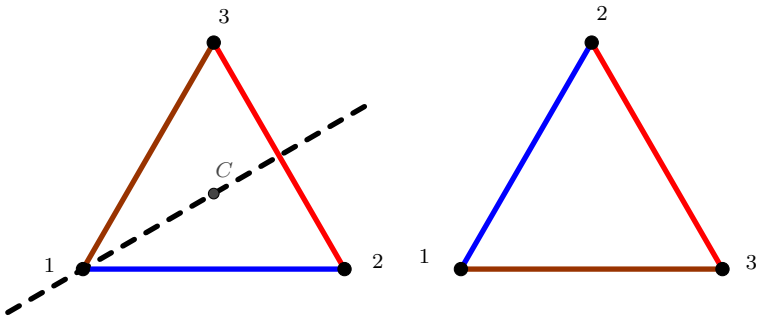
Now we rotate the original triangle 240° counter clockwise about the centre C, we get the following figure.



We can think this rotation as a map on vertices. That is $1 \to 3$, $2 \to 1$ and $3 \to 2$. We get $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

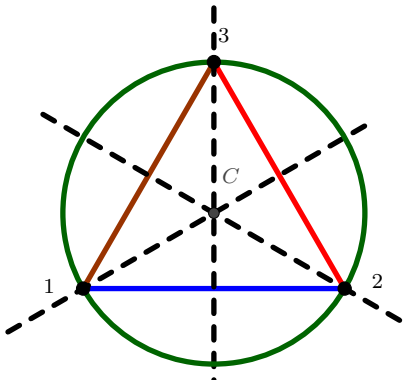
The identity map of the plane takes every point to itself. So we can think this function as rotation through 0° and denote this isometry as ρ_0. That is, $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

Now we reflect about perpendicular bisector of the side 23. Then the map is shown in the following figure.



We can think of this as a function μ_1 on the vertices as $\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Simillarly if we reflect about perpendicular bisectors of the sides 31 and 12,

we get two functions μ_2 and μ_3 respectively. Here $\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.



Thus we have 6 symmetries of an equilqteral triangle, three rotations ρ_0, ρ_1, ρ_2 and three reflections (mirror images in bisectors of angles) μ_1, μ_2, μ_3.

The isometries of the plane are translations, rotations, reflections and glide reflections.

transalation τ: Slide every point the same distance in the same direction. That is, parallel motion of the plane by a vector.(Example: $\tau(x, y) = (x, y) + (-1, 3)$.)

rotation ρ: Rotate the plane about a point P through an angle θ.(Example: $\rho(x, y) = (-y, x)$ is a rotation through 90° counter clockwise about the origin.)

reflection μ: Map each point into its mirror image across a line L, each point of L is left fixed by μ. The line L is the axis of reflection. (Example: $\mu(x, y) = (y, x)$ is a reflection across the line $y = x$.)

glide reflection γ: Obtained by reflecting about a line L and then translating by a non-zero vector a parallel to L.(Example: $\gamma(x, y) = (x+3, -y)$ is a glide reflection along the x-axis.)

Note that translation and rotation are orientation preserving motions and reflection and glide reflection are the orientation reversing motions.

Now we investigate the possible finite groups of symmetries of subsets of $\mathbb{R}^2$ or finite subgroups of the full isometry group.

Theorem 1.19. *Every finite group G of isometries of the plane is isomorphic to either $\mathbb{Z}_n$ or to a dihedral group D_n for some positive integer n.*

Proof. Let

$$G = \{\phi_1, \phi_2, \ldots, \phi_m\}.$$

First we prove that there is a point P in the plane that is left fixed by every isometry in G.

Let $(x_i, y_i) = \phi_i(0, 0)$ and $P = (\overline{x}, \overline{y})$ where

$$\overline{x} = \frac{x_1 + x_2 + \ldots + x_m}{m}$$

and

$$\overline{y} = \frac{y_1 + y_2 + \ldots + y_m}{m}.$$

That is, P is the centroid of the set $S = \{(x_i, y_i) : i = 1, 2, \ldots, m\}$.

Let $\phi_i\phi_j = \phi_k$. Then

$$\phi_i(x_j, y_j) = \phi_i(\phi_j(0, 0)) = \phi_k(0, 0) = (x_k, y_k).$$

So each isometry in G just permutes the elements of S and hence it must leave the centroid $(\overline{x}, \overline{y})$ fixed. Thus G consists of the identity, rotations about P and reflections across a line through P. Note that G can not contain a

translation or a glide-reflection because in either case G would be infinite. Thus we proved that all elements in G have a common fixed point.

The orientation-preserving isometries in G form a subgroup H of G which is either all of G or of order $\frac{m}{2}$.

Because G is finite the orientation preserving isometries in G consist of the rotations in G and the identity map. Because the product of two orientation preserving isometries is orientation preserving, we see that the set H of all orientation preserving isometries in G is closed under function composition. Because the inverse of a rotation is also a rotation, we see that H contains the inverse of each element, and is thus a subgroup of G. If $H \neq G$, let μ be an element of G that is not in H. If σ is another element of G not in H, then $\mu^{-1}\sigma \in H$, because the product of two orientation reversing isometries is order preserving. Thus $\sigma \in \mu H$.

This shows that the coset μH contains all elements of G that are not in H. Because $|\mu H| = |H|$, we see that in this case $|G| = 2|H|$. Note that H consists of the identity and the rotations in G. We can consider all the rotations in G to be clockwise. Let ρ be the rotation in G which rotates the plane clockwise through the smallest positive angle. Such a rotation exists because G is a finite group. We claim that G is cyclic, generated by ρ. Let α be the angle of rotation for ρ. Let σ be another rotation in G with angle of rotation β. Write $\beta = q\alpha + \theta$, according to the division algorithm. Then $\theta = \beta - q\alpha$, and the isometry $\rho^{-q}\sigma$ rotates the plane through the angle θ. By the division algorithm, either $\theta = 0$ or $0 < \theta < \alpha$. Because $0 < \theta < \alpha$ is impossible by our choice of α as the smallest non zero angle of rotation, we see that $\theta = 0$. Hence $\beta = q\alpha$, so $\sigma = \rho^q$, showing that G is cyclic and generated by ρ. This shows that if $G = H$, then G is cyclic of order m and isomorphic to $\mathbb{Z}_m$.

Suppose $H \neq G$. So that G contains some reflections. Let

$$H = \{i, \rho_1, \ldots, \rho_{n-1}\}$$

with $n = m/2$. If μ is a reflection in G, then the coset $H\mu$ consists of all n of the reflections in G.

Consider a regular n-gon in the plane having P as its center with a vertex lying on the line through P left fixed by μ. The elements of H rotate this n-gon through all positions and the elements of $H\mu$ first reflect an axis through a vertex turning the n-gon over then rotate through all positions. That is the action of G on n-gon is the action of D_n and hence G is isomorphic to D_n. □

Now we consider infinite groups of plane isometries. There are two types of infinite symmetric groups that arise from periodic designs in the plane. The discrete frieze groups are the plane symmetry groups of patterns whose subgroups of translations are isomorphic to $\mathbb{Z}$. These kinds of designs are used for decorative strips and for patterns of jewellery. Consider integral signs spaced equal distances apart and continuing infinitely to the left and right is a simple example of discrete frieze.

$$\cdots \int \int \int \int \int \int \int \int \int \int \int \int \int \cdots$$

The symmetric group of this frieze is generated by a transalation τ sliding the place one unit to right and by a rotation ρ of 180° about a point in the centre of some integral sign. Note there are no vertical, horizontal or glide reflections. The frieze group is a non abelian group generated by τ and ρ and it is denoted by D_∞.

Question 1.20. 1. Describe all symmetries of a point in the real line $\mathbb{R}$.

2. Describe all symmetries of a line segment in $\mathbb{R}$.

3. Describe all symmetries of a line segment in $\mathbb{R}^2$.

Solution. 1. Let a be the point in the real line. We have to find all symmetries of the point a, which is the isometries of $\mathbb{R}$ that leaves a fixed. Clearly identity map is an isometry that leaves a fixed. Obviously translation is not symmetry of the point a. Now consider the reflection μ through the point a. That is, μ carries $a + x$ to $a - x$ for all $x \in \mathbb{R}$. Them μ is a symmetry of the point a. So the only isometries on $\mathbb{R}$ leaving the point a fixed are reflection through a that carries $a + x$ to $a - x$ for all $x \in \mathbb{R}$ and the identity map.

2. Clearly the isometries of $\mathbb{R}$ that carry a line segment to itself are the identity map and the reflection through the midpoint of the line segment.

3. The isometries of $\mathbb{R}^2$ that carry a line segment into itself include rotations of 180° about the midpoint of the line segment, a reflection in the axis containing the line segment, a reflection in the axis perpendicular the line segment at its midpoint, and the identity map.

■

EXERCISES

1. Determine the group of symmetries of a square in $\mathbb{R}^2$.

1.3 Factor Groups

First we recall some preliminary concepts which are needed in the following sections.

Let H be a subgroup of G. The subset $aH = \{ah : h \in H\}$ of G is the left coset of H containing a and $Ha = \{ha : h \in H\}$ is the right coset of H containing a. Every coset (left or right) of a subgroup H of a group G has the same number of elements as H. Let H be a subgroup of G. The number of left cosets of H in G is the index $(G : H)$ of H in G. Two cosets aH and bH are equal if and only if $a^{-1}b \in H$.

Let G and G' be two groups and $\phi : G \to G'$ be a map. Then ϕ is called a homomorphism if

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$.

Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.

2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.

3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.

4. If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

The subgroup $\phi^{-1}[\{e'\}] = \{x \in G : \phi(x) = e'\}$ is called the kernel of ϕ and is denoted by $Ker(\phi)$. Also ϕ is a one-to-one map if and only if $Ker(\phi) = \{e\}$.

Theorem 1.21. *Let $\phi : G \to G'$ be a homomorphism and let $H = Ker(\phi)$ and $a \in G$. Then the set*

$$\phi^{-1}[\phi(a)] = \{x \in G : \phi(x) = \phi(a)\}$$

is the left coset aH of H and is also the right coset Ha of H in G.

Recall that for a subgroup H of G, the right coset Ha and the left coset aH need not be the same. A subgroup H is normal if its left and right cosets coincide, that is if $gH = Hg$ for all $g \in G$. Note that all subgroups of abelian

groups are normal and the kernel of a group homomorphism $\phi : G \to G'$ is a normal subgroup of G.

In this section first we show that if H is the kernel of the homomorphism $\phi : G \to G'$, then the cosets of H are indeed elements of a group whose binary operation is derived from the group operation of G.

Theorem 1.22. *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the left cosets of H form a factor group, G/H, where*

$$(aH)(bH) = (ab)H.$$

Also the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both the coset multiplication and μ are well-defined, independent of the choices a and b from the cosets.

Proof. We have $(aH)(bH) = (ab)H$ in G/H. This product is computed by choosing an element from each of the cosets aH and bH and find the coset containing their product.

Claim: G/H is a group.

First we show that the binary operation is well defined. Let $ah_1 \in aH$ and $bh_2 \in bH$ are two representatives. Here we show that $(ab)H = (ah_1bh_2)H$. That is, ab and ah_1bh_2 lie in the same coset of G/H.

Since H is the kernel of the homomorphism $\phi : G \to G'$, by Theorem 1.21, we have

$$\phi^{-1}[\phi(a)] = aH = Ha \text{ for } a \in G.$$

Hence $(ab)H = \phi^{-1}[\phi(ab)]$ and $(ah_1bh_1)H = \phi^{-1}[\phi(ah_1bh_2)]$. So in order to prove $(ab)H = (ah_1bh_2)H$, it is enough to show that $\phi(ab) = \phi(ah_1bh_2)$. Now

$$\phi(ah_1bh_2) = \phi(a)\phi(h_1)\phi(b)\phi(h_2) = \phi(a)\phi(b) = \phi(ab).$$

This implies that $ah_1bh_2 \in \phi^{-1}(\phi(ab)) = abH$. Hence the binary operation is well defined.

Let aH, bH, $cH \in G/H$. Then

$$\begin{aligned}(aH)((bH)(cH)) &= (aH)(bcH) = [a(bc)]H \\ &= [(ab)c]H = (abH)(cH) \\ &= ((aH)(bH))(cH).\end{aligned}$$

Hence the binary operation is associative. We have $eH = H \in G/H$ and

$$(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH).$$

So $H = eH$ acts as identity coset in G/H.

We have

$$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H = (aa^{-1})H = (aH)(a^{-1}H).$$

So $a^{-1}H$ is the inverse of aH in G/H. Thus G/H is a group.

Next we show that $\mu : G/H \to \phi[G]$ is an isomorphism. Since μ is defined by choosing elements from coset and computing ϕ of these elements, first we show that μ is well defined (independent of the choices of elements from the cosets). Let $x \in aH$, then $x = ah$ for some $h \in H$. Now

$$\phi(x) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a).$$

Thus the computation of the element of $\phi[G]$ corresponding to the coset $aH = xH$ is the same whether we compute it as $\phi(a)$ or $\phi(x)$.

Suppose that $\mu(aH) = \mu(bH)$. Then $\phi(a) = \phi(b)$ and hence $\phi^{-1}[\phi(a)] =$

$\phi^{-1}[\phi(b)]$. This implies that $aH = bH$, by Theorem 1.21. That is, μ is one to one.

Let $y \in \phi[G]$. Then $y = \phi(x)$ for some $x \in G$. Now $\mu(xH) = \phi(x) = y$. So μ is onto.

Now

$$\mu(aH)(bH) = \mu((ab)H) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bH).$$

Hence μ is an isomorphism.

□

Example 1.23. Consider the map $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ where $\gamma(m)$ is the reminder when m is divided by n with the division algorithm. Then γ is a homomorphism with $ker(\gamma) = n\mathbb{Z}$. Then by Theorem 1.22, the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. For example, taking $n = 3$,we get

$$\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

where

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -5, -2, 1, 4, \ldots\} \\ \text{and } 2 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, \ldots\}. \end{aligned}$$

Note that the isomorphism $\mu : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}_3$ assigns to each coset of $3\mathbb{Z}$ its smallest non negative element.

That is,

$$\begin{aligned} \mu(3\mathbb{Z}) &= 0 \\ \mu(1+3\mathbb{Z}) &= 1 \\ \text{and } \mu(2+3\mathbb{Z}) &= 2. \end{aligned}$$

Factor Groups from Normal Subgroups

We have obtained factor groups from homomorphisms. Let H be a subgroup of G. Then H has both left cosets and right cosets. A left coset aH need not equal to Ha. Consider the collection of all left cosets of H in G, define a binary operation on this collection as in the statement of Theorem 1.22. The following Theorem shows that the binary operation is well defined if and only if the right and left cosets aH and bH coincide for all $a \in G$. That is, H is normal in G.

Theorem 1.24. *Let H be a subgroup of a group G. Then the coset multiplication is well defined by the equation*

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Proof. Suppose that the coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H.$$

Let $a \in G$. We want show that aH and Ha are the same set. Let $x \in aH$. Choosing representatives $x \in aH$ and $a^{-1} \in a^{-1}H$, we have $(xH)(a^{-1}H) = (xa^{-1})H$.

On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = eH = H$. Since the coset multiplication is well defined by the equation $(aH)(bH) = (ab)H$, we must have $xa^{-1} = h \in H$.Then $x = ha \in Ha$. Hence $aH \subseteq Ha$. Similarly we can show that $Ha \subseteq aH$.

Conversely assume that H is a normal subgroup of G. Since H is normal in G, the right and left cosets coincide. We compute $(aH)(bH)$. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$.
Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$, we obtain the coset ah_1bh_2H. We claim that these two cosets are same. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus

$$(ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2)$$

and $(ab)(h_3h_2) \in (ab)H$. Therefore $ah_1bh_2 \in (ab)H$. That is, the coset multiplication is well defined by the equation $(aH)(bH) = (ab)H$ □

So if H is a normal subgroup of a group G, then we have a well defined binary operation on cosets. We can easily show that under this binary operation, the cosets form a group.

Corollary 1.25. *Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$.*

Proof. The associativity in G/H follows from associativity in G. Let aH, bH and cH in G/H. Then

$$\begin{aligned}(aH)[(bH)(cH)] &= (aH)[(bc)H] = a(bc)H \\ &= (ab)cH = [(ab)H](cH) = [(aH)(bH)](cH)\end{aligned}$$

We have

$$(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH).$$

So $eH = H$ is the identity element in G/H. Also we have

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H = (a^{-1}a)H = (a^{-1}H)(aH).$$

So $(aH)^{-1} = a^{-1}H$. Hence G/H is a group. □

Definition 1.26. *The group G/H in the preceding corollary is the factor group (quotient group) of G by H.*

The Fundamental Homomorphism Theorem

We proved that every homomorphism $\phi : G \to G'$ gives a factor group $G/ker(\phi)$. Here we show that each factor group G/H gives a natural homomorphism having H as kernel.

Theorem 1.27. *Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.*

Proof. Let x, $y \in G$. Then

$$\begin{aligned}\gamma(xy) &= (xy)H = (xH)(yH)\\ &= \gamma(x)\gamma(y).\end{aligned}$$

So γ is a homomorphism. Since $xH = H$ if and only if $x \in H$. So the kernel of γ is H. □

The factor group construction is related to general homomorphism $\phi : G \to G'$ of groups as follows.

Theorem 1.28. ***(The Fundamental Homomorphism Theorem)*** *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.*

Proof. By Theorem 1.22, if $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. Theorem 1.27 shows that $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H. Let $g \in G$. Then

$$\mu \circ \gamma(g) = \mu(\gamma(g)) = \mu(gH) = \phi(g).$$

□

The isomorphism μ in the above Theorem is referred to as a natural or canonical isomorphism.

Thus we showed that every homomorphism with domain G gives rise to a factor group G/H and every factor group G/H gives a homomorphism mapping G into G/H.

Example 1.29. Consider the projection map $\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ defined by $\pi_1(x, y) = x$, which is a homomorphism of $\mathbb{Z}_4 \times \mathbb{Z}_2$ onto $\mathbb{Z}_4$.

$$\begin{aligned} \text{Kernel of } \pi_1 &= \{(x, y) \in \mathbb{Z}_4 \times \mathbb{Z}_2 : \pi_1(x, y) = 0\} \\ &= \{(x, y) \in \mathbb{Z}_4 \times \mathbb{Z}_2 : x = 0\} \\ &= \{0\} \times \mathbb{Z}_2. \end{aligned}$$

Then by Theorem 1.28,

$$(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) \cong \mathbb{Z}_4.$$

Next we give various characterisations of normal subgroups, which provide us an easier way to check normality than finding both the right and left coset decomposition.

Theorem 1.30. *The following are three equivalent conditions for a subgroup H of a group G to be a normal subgroup of G.*

1. *$ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

2. *$gHg^{-1} = H$ for all $g \in G$.*

3. *$gH = Hg$ for all $g \in G$.*

Proof. (1) $\Rightarrow$ (2)**:** Assume that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
Therefore,

$$gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H. \tag{1.1}$$

Let $h \in H$. Then $ghg^{-1} \in H$ for all $g \in G$. So $g^{-1}hg \in H$. This implies that $g^{-1}hg = h_1$ and hence $h = gh_1g^{-1} \in gHg^{-1}$. Hence

$$H \subseteq gHg^{-1}. \tag{1.2}$$

From 1.1 and1.2, we get

$$H = gHg^{-1}.$$

(2) $\Rightarrow$ (3): Assume that $gHg^{-1} = H$ for all $g \in G$. Then $ghg^{-1} = h_1$. So $gh = h_1g \in Hg$ and this implies that

$$gH \subseteq Hg.$$

Similarly we get $Hg \subseteq gH$. Thus $gH = Hg$ for all $g \in G$.
(3) $\Rightarrow$ (1): Suppose that $gH = Hg$ for all $g \in G$. Then $gh = h_1g$ for all

$g \in G$.
This implies $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. This means that $gHg^{-1} = H$ for all $g \in G$ □

Let G be an abelian group and H be a subgroup of G. Since G is abelian, $gh = hg$ for all $g \in G$ and $h \in H$, every subgroup of an abelian group is normal.

Let G be a group and $i_G : G \to G$ defined by $i_g(x) = gxg^{-1}$ for all $x \in G$. Then

$$\begin{aligned} i_g(xy) &= gxyg^{-1} = gx(g^{-1}g)yg^{-1} \\ &= (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y) \end{aligned}$$

for all x, y in G. So i_g is a homomorphism of G. Now

$$i_g(x) = i_g(y) \implies gxg^{-1} = gyg^{-1}$$

if and only if $x = y$. So i_g is one to one.

Let $y \in G$. Then $g^{-1}yg \in G$ and $g(g^{-1}yg)g^{-1} = y$. That is i_g is onto G. Hence i_g is an isomorphism on G.

Definition 1.31. *An isomorphism $\phi : G \to G$ of a group G with itself is an automorphism of G. The automorphism $i_g : G \to G$ where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the inner automorphism of G by g. Performing i_g on x is called conjugation of x by g.*

Using Theorem 1.30, can we see that the normal subgroups of a group G are precisely those that are invariant under all inner automorphisms.

EXERCISES

1. Find the order of the given factor group.

(a) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,1)\rangle$

(b) $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4,3)\rangle$

(c) $(\mathbb{Z}_6 \times \mathbb{Z}_4)/\langle(2,1)\rangle$

(d) $(\mathbb{Z}_9 \times \mathbb{Z}_6)/\langle(3,2)\rangle$

2. Give the order of the element in the factor group.

   (a) $5 + \langle 4\rangle \in \mathbb{Z}_{12}/\langle 4\rangle$

   (b) $(3,3) + \langle(1,2)\rangle \in \mathbb{Z}_4 \times \mathbb{Z}_8/\langle(1,2)\rangle$.

3. Show that A_n is a normal subgroup of S_n and compute S_n/A_n.

4. Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.

1.4 Factor-group Computations and Simple Groups

Let N be a normal subgroup of G. In the factor group G/N, the subgroup N act as identity element. We may regard N as being collapsed to a single element either to 0 in additive notation and e in multiplicative notation. The collapsing of N with the algebraic structure of G require that the other cosets of N also collapse into a single elements on the factor group. It is very important to remember that the multiplication of cosets of G/N can be computed by multipling in G using any representative elements of the cosets. Hence two elements of G will collapse into the same element of G/N if they differ by an element of N, that is, $a - b$ is in N, in additively and if ab^{-1} is in N in multiplicative notation.

Example 1.32. The trivial subgroup $N = \{0\}$ of $\mathbb{Z}$ is a normal subgroup. Since N has only one element, every coset of N has only one element. That

is the cosets are of the form $\{m\}$ for $m \in \mathbb{Z}$. There is no collapsing at all, and consequently, $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$. Each $m \in \mathbb{Z}$ is simply renamed $\{m\}$ in $\mathbb{Z}/\{0\}$.

Example 1.33. Let n be a positive integer. The set $n\mathbb{R} = \{nr : r \in \mathbb{R}\}$ is a subgroup of $\mathbb{R}$ under addition and it is normal since $\mathbb{R}$ is abelian. Each $x \in \mathbb{R}$ is of the form $n(\frac{x}{n})$ and $\frac{x}{n} \in \mathbb{R}$. Thus $n\mathbb{R} = \mathbb{R}$. So $\mathbb{R}/n\mathbb{R}$ has only one element, the subgroup $n\mathbb{R}$. That is, every element in $\mathbb{R}$ collapse into a single coset $\mathbb{R}$. The factor group $\mathbb{R}/n\mathbb{R}$ is a trivial group consisting only of the identity.

Remark 1.34. For any group G, we have $G/\{e\} \simeq G$ and $G/G \simeq \{e\}$.

Consider the factor group G/N. If $N = \{e\}$, then the factor group G/N has the same structure as G and if $N = G$, then the factor group has no significant structure. If G is a finite group and $N \neq G$ be a normal subgroup of G, then order of G/N is smaller than order of G and hence its structure is less complicated than that of G.

Question 1.35. Show that if a finite group G contains a nontrivial subgroup N of index 2 in G, then N is normal.

Solution. Since the index of N in G is 2, the number of left(right) cosets of N in G is two. Let $a \in G$. If $a \in N$, we have $aN = N = Na$. If $a \notin N$, then N and aN are the two distinct left cosets and N and Na are the two distinct right cosets. It follows that $N \cup aN = G = N \cup Na$. This implies that $aN = G \setminus N = Na$. So the right and left cosets of N coincide and hence N is normal in G. ■

Falsity of the Converse of the Theorem of Lagrange

Here we illustrate one application of factor group. We can often deduce properties of a group G by examining the less complicated group, factor group.

Recall that the Theorem of Lagrange states that if H is a subgroup of a finite group G, then the order of H divides the order of G. But the converse is false.

Here we show that it is false that if d divides the order of G, then there exists a subgroup of H of G having order d.

For example, consider the group A_4,of even permutations on the set $\{1, 2, 3, 4\}$ which has order 12. We show that A_4 contains no subgroup of order 6. Suppose that A_4 does have a subgroup H of order 6. Since $|A_4| = 2|H|$, H must be normal in G. So the factor group A_4/H exists and has order 2. Since the order of an element divides order of a group, we have for all $\sigma \in A_4$ that $\sigma^2 H = (\sigma H)^2 = H$. Thus $\sigma^2 \in H$ for all $\sigma \in A_4$. That is square of every element in A_4 must be in H.

But in A_4, we have $(1, 2, 3)^2 = (1, 3, 2)$ and $(1, 3, 2)^2 = (1, 2, 3)$. So $(1, 2, 3)$ and $(1, 3, 2)$ are in H. Similarly we can show that
$(1, 2, 4)$, $(1, 4, 2)$, $(1, 3, 4)$, $(1, 4, 3)$, $(2, 3, 4)$ and $(2, 4, 3)$ are all in H. This shows that there must be at least 8 elements in H, contradicting the fact that H was supposed to have order 6. So A_4 has no subgroup of order 6.

Example 1.36. Compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 1)\rangle$.
Let

$$H = \langle(0, 1)\rangle = \{(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (0, 5)\}.$$

Since $\mathbb{Z}_4 \times \mathbb{Z}_6$ has 24 elements and H has 6 elements, all cosets of H must have 6 elements and $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle(0, 1)\rangle$ must have order 4. The cosets of H are

$$H = (0, 0) + H,\ (1, 0) + H,\ (2, 0) + H,\ (3, 0) + H.$$

Since we can compute by choosing the representatives, $(0, 0), (1, 0), (2, 0)$ and $(3, 0)$, it is clear that $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 1)\rangle$ is isomorphic to $\mathbb{Z}_4$.

Theorem 1.37. *Let $G = H \times K$ be the direct product of groups H and K. Then $\bar{H}$= $\{(h, e) : h \in H\}$ is a normal subgroup of G. Also $G/\bar{H}$ is*

isomorphic to K in a natural way. Similarly $G/\bar{K} \simeq H$ in a natural way.

Proof. Consider the map $\pi_2 : H \times K \to K$, where

$$\pi_2(h, k) = k.$$

Let (h_1, k_1), $(h_2, k_2) \in H \times K$. Then

$$\pi_2((h_1, k_1)(h_2, k_2)) = \pi_2(h_1h_2, k_1k_2) = k_1k_2 = \pi_2(h_1, k_1)\pi_2(h_2, k_2).$$

Hence $\pi_2 : H \times K \to K$ is a homomorphism. We have

$$Ker(\pi_2) = \{(h, k) : k = e\} = \overline{H},$$

we see that $\bar{\mathrm{H}}$ is a normal subgroup of $H \times K$. Since π_2 is onto K, we have $(H \times K)/\bar{\mathrm{H}} \simeq K$ by fundamental homomorphism theorem. □

Theorem 1.38. *A factor group of a cyclic group is cyclic.*

Proof. Let G be a cyclic group with generator a and N be a normal subgroup of G.
We show that aN generates G/N.

Consider the all powers of aN. Recall that the computation of the product of cosets is accomplished by choosing representatives from cosets, multiplying them and finding the coset in which the resulting product lies. So here all powers of the representative a and all these powers give all elements in G. Hence the powers of aN certainly give all cosets of N and G/N is cyclic. □

Example 1.39. Compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 2)\rangle$.

Let $H = \{(0, 0), (0, 2), (0, 4)\}$, be the subgroup generated by $\langle(0, 2)\rangle$. Here $|H| = 3$. Here the first factor $\mathbb{Z}_4$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is left as it is. On the other

hand, the second factor $\mathbb{Z}_6$ is collapsed by a subgroup of order 3, giving a factor group, which is isomorphic to $\mathbb{Z}_2$. Thus

$$(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2.$$

Example 1.40. Compute the factor group $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$.

We may visualise $\mathbb{Z} \times \mathbb{Z}$ as the points in the plane with both coordinates integers. The elements of the subgroup $\langle(1,1)\rangle$ are those points that lie on the 45° line through the origin. The coset $(1,0) + \langle(1,1)\rangle$ consists of those dots on the 45° line through the point $(1,0)$. Continuing we see that each coset consists of those dots lying on one of the 45° lines through the point $(a,0)$ where a is an integer. We may choose the representatives

$$\ldots, (-3,0), (-2,0), (-1,0), (0,0), (1,0), (2,0), \ldots$$

of these cosets to compute in the factor group. Note that these representatives correspond precisely to the points of $\mathbb{Z}$ on the x-axis. So

$$(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle \simeq \mathbb{Z}.$$

Simple Groups

We already mentioned that factor groups of a group G give important information about the structure of the group G. But for some groups may not have proper non trivial normal subgroups. For example, consider the group $\mathbb{Z}_p$, p is a prime number. Then by Lagrange's theorem $\mathbb{Z}_p$ has no proper non trivial subgroups and hence no non trivial normal subgroups.

Definition 1.41. *A group G is simple if it is non trivial and has no proper nontrivial normal subgroups.*

Theorem 1.42. *The alternating group A_n is simple for $n \geq 5$.*

Proof. The proof is omitted. □

Here we characterise those normal subgroups N of a group G for which G/N is a simple group. In order to prove this characterisation, we need the following Theorem.

Theorem 1.43. *Let $\phi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G.*

Proof. Assume that N is a normal subgroup of G. Then $\phi[N]$ is a subgroup of $\phi[G]$.
Claim: $\phi[N]$ is normal in $\phi[G]$. Let $g \in G$, $x \in N$. Since N is normal in G, $gxg^{-1} \in N$. We have

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(x)\phi(g)^{-1}.$$

This implies that

$$\phi(g)\phi(x)\phi(g)^{-1} = \phi(gxg^{-1}) \in \phi[N].$$

So $\phi[N]$ is normal in $\phi[G]$. Similarly we can show that if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G. □

That is, a homomorphism $\phi : G \to G'$ preserves normal subgroups between G and $\phi[G]$. Note that $\phi[N]$ may not be normal in G' even though N is normal in G.
For example, $\phi : \mathbb{Z}_2 \to S_3$, where $\phi(0) = \rho_0$ and $\phi(1) = \mu_1$ is a homomorphism and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\rho_0, \mu_1\}$ is not a normal subgroup of S_3.

Definition 1.44. *A maximal normal subgroup of a group G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M.*

Theorem 1.45. *M is a maximal subgroup of G if and only if G/M is simple.*

Proof. Let M be a maximal normal subgroup of G. Consider the canonical homomorphism $\gamma : G \to G/M$ defined by $\gamma(g) = gM$. If K is a non trivial proper normal subgroup of G/M, then by Theorem 1.43, $\gamma^{-1}[K]$ is a proper normal subgroup of G properly containing M. But M is maximal, so this can not happen. So G/M has no proper non trivial normal subgroups. Thus G/M is simple.

Conversely assume that G/M is simple. Let N be a normal subgroup of G properly containing M. Then $\gamma[N]$ is normal in G/M. If $N \neq G$, then $\gamma[N] \neq G/M$. Since N contains M properly, $\gamma[N] \neq \{M\}$. It follows that $\gamma[N]$ is a proper non trivial normal subgroup of G/M. Since G/M is simple, no such $\gamma[N]$ exists and hence no such N can exist. Thus M is maximal. □

The Center and Commutator Subgroups

Here we define two important subgroups of a group G, the center $Z(G)$ and the commutator subgroup C, which are normal in G.

Definition 1.46. *The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. That is, $Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}$*

Theorem 1.47. *$Z(G)$ is an abelian subgroup of G.*

Proof. Clearly $e \in Z(G)$. So $Z(G)$ is nonempty. Suppose a, $b \in G$. Then

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Therefore $ab \in Z(G)$. Let $a \in Z(G)$. Then $ax = xa$ for all $x \in G$. We get $axa^{-1} = x$ and hence $xa^{-1} = a^{-1}x$ for all $x \in G$. This implies that $a^{-1} \in Z(G)$. Clearly $Z(G)$ is abelian. □

Let $g \in G$ and $a \in Z(G)$. We have $gag^{-1} = agg^{-1} = a$. This is true for all $g \in G$ and $a \in Z(G)$. Hence $Z(G)$ is a normal subgroup of G.

The center of a group G always contains the identity element e. If $Z(G) = \{e\}$, we say that the center of G is trivial. If G is abelian, then $Z(G) = G$.

Question 1.48. Show that if G is nonabelian, then the factor group $G/Z(G)$ is not cyclic.

Solution. Suppose that factor group $G/Z(G)$ is cyclic with generator $aZ(G)$. Let $x, y \in G$. Then x is a member of a coset $a^mZ(G)$ and y is a member of a coset $a^nZ(G)$ for some $m, n \in \mathbb{Z}$. So $x = a^mz_1$ and $y = a^nz_2$ where $z_1, z_2 \in Z(G)$. Since z_1 and z_2 commute with every element of G,

$$\begin{aligned} xy &= a^mz_1a^nz_2 \\ &= a^ma^nz_1z_2 \\ &= a^{m+n}z_1z_2 \\ &= a^{n+m}z_2z_1 \\ &= a^na^mz_2z_1 = \\ &= a^nz_2a^mz_1 \\ &= yx. \end{aligned}$$

Hence G is abelian. Therefore if G is nonabelian, then the factor group $G/Z(G)$ is not cyclic. ■

An element $aba^{-1}b^{-1}$ in a group is a commutator of the group G. We need the following Theorem in order to prove our next Theorem on commutators.

Theorem 1.49. *If G is a group and $a_i \in G$ for $i \in I$, then the subgroup H of G generated by $\{a_i : i \in I\}$ has as elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.*

Theorem 1.50. *Let G be a group. The set of all commutators $aba^{-1}b^{-1}$ for $a, b \in G$ generates a normal subgroup C of G and G/C is abelian. Furthermore, if N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.*

Proof. Note that the commutators generate a subgroup C. Note that the inverse $(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$ of a commutator is again a commutator. Also $e = eee^{-1}e^{-1}$ is a commutator. Then by Theorem 1.49, C consists precisely of all finite products of commutators. Let $x \in C$. We show that $g^{-1}xg \in C$ for all $g \in G$. Since $x \in C$, either $x = cdc^{-1}d^{-1}$ or x is a product of commutators. By inserting $e = gg^{-1}$ between each product of commutators occuring in x, we see that it is enough to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C. Now

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}(cdc^{-1})(e)(d^{-1})g) \\ &= (g^{-1}(cdc^{-1})(gd^{-1}dg^{-1})(d^{-1})g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1})d^{-1}][dg^{-1}d^{-1})g], \end{aligned}$$

which belongs to C. Thus C is normal in G.

Now we show that G/C is abelian. Let aC, $bC \in G/C$. Then

$$\begin{aligned} (aC)(bC) = abC &= ab(b^{-1}a^{-1}ba)C \\ &= (abb^{-1}a^{-1})baC \end{aligned}$$

$$= baC = (bC)(aC).$$

Furthermore, assume that N is a normal subgroup of G and G/N is abelian. Then $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$ iff $aba^{-1}b^{-1}N = N$. So $aba^{-1}b^{-1} \in N$ and hence C is a subgroup of N. Conversely assume that C is a subgroup of N. Then $(aN)(bN) = (ab)N = ab(b^{-1}a^{-1}ba)N = (abb^{-1}a^{-1})baN = baN = (bN)(aN)$. This implies that G/N is abelian. Hence the proof. □

Definition 1.51. *The subgroup C in Theorem 1.50 is called the commutator subgroup of G.*

EXCERCISES

1. Classify the given group according to the fundaamental theorem of finitely generated abelian groups.

   (a) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,1)\rangle$

   (b) $(\mathbb{Z} \times \mathbb{Z})/\langle(1,2)\rangle$

   (c) $(\mathbb{Z}_8 \times \mathbb{Z}_4)/\langle(2,1)\rangle$

   (d) $(\mathbb{Z} \times \mathbb{Z})/\langle(1,0)\rangle$

2. Find the center and commutator subgroup of S_3.

1.5 Group Action on a Set

Here we discuss an action of a group on a set.

Suppose we are given a group G and a set X. An action of G on X is a rule $*$ for combining elements $g \in G$ and $x \in X$ to get an element $*(g, x)$ of X and this rule is required to satisfy two axioms. We shall write $*(g, x)$ as $g * x$ or gx.

Definition 1.52. *Let X be a set and G a group. An action of G on X is a map $* : G \times X \to X$ such that*

1. *$ex = x$ (That is, $*(e, x) = x$) for all $x \in X$.*
2. *$(g_1g_2)(x) = g_1(g_2x)$ (That is, $*(g_1g_2, x) = *(g_1, *(g_2, x)))$ for all $x \in X$ and all g_1, $g_2 \in G$*

Under these conditions, X is a G-set.

Examples 1.53. 1. Consider the binary operation $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Let a, $b \in \mathbb{R}$. Then $+(a, b) = a + b$. Note that $+(0, a) = 0 + a = a$ for all $a \in \mathbb{R}$ and $+(a, +(b, c)) = +(a, b + c) = a + (b + c) = (a + b) + c = +(+(a, b), c)$ for all a, b, $c \in \mathbb{R}$. So according to the definition, $\mathbb{R}$ acts on $\mathbb{R}$ through addition.

In general a group can act on itself via the binary operation that makes it a group. This action is called the regular action of G.

2. Let X be any set and let H be a subgroup of the group S_X of all permutations of X. Define the action of $\sigma \in H$ on X is its action as an element of S_X. Thus $*(\sigma, x) = \sigma x = \sigma(x)$ for all $x \in X$. Then clearly X is an H-set.

3. Let G be a group. Define an action of G on itself as follows. The action on $g_2 \in G$ by $g_1 \in G$ is given by left multiplication. That is $*(g_1, g_2) = g_1g_2$. Similarly if H is a subgroup of G, we can regard G as an H-set where $*(h, g) = hg$.

Theorem 1.54. *Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.*

Proof. First we have to show that σ_g is a permutation of X. That is σ_g is a one-to-one map of X onto itself.
Suppose that $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$. Then

$$\begin{aligned} gx_1 &= gx_2. \\ g^{-1}(gx_1) &= g^{-1}(gx_2). \\ (g^{-1}g)x_1 &= (g^{-1}g)x_2, \text{ by condition 2 in Definition 1.52.} \\ ex_1 &= ex_2. \\ x_1 &= x_2, \text{ by condition 1 in Definition 1.52.} \end{aligned}$$

So σ_g is one-one.

Now for $x \in X$ we have

$$\sigma_g(g^{-1}x) = g(g^{-1})x = (gg^{-1})x = ex = x.$$

That is, for any x in X, there exists $g^{-1}x$ such that $\sigma_g(g^{-1}x) = x$. So σ_g is onto. Thus σ_g is a permutation of X.

Next we claim that $\phi : G \to S_X$ is a homomorphism. Here we show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. It is enough to show that $\phi(g_1g_2)(x) = \phi(g_1)\phi(g_2)(x)$ for all $x \in X$. Now using the definition of group action and the rule for function composition, we have

$$\begin{aligned} \phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) &= (g_1g_2)x = g_1(g_2x) = g_1\sigma_{g_2}(x) \\ &= \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) \\ &= \phi(g_1)\phi(g_2)(x) \end{aligned}$$

Hence ϕ is a homomorphism. Now $\phi(g)(x) = \sigma_g(x) = gx$. Hence the proof.

□

Remark 1.55. Consider the above homomorphism $\phi : G \to S_X$. Here the kernel of this homomorphism is

$$ker(\phi) = \{g \in G : \phi(g) \text{ is the identity permutation in } S_X\}.$$

That is, kernel of ϕ is the subset of G leaving every element of X fixed and which is a normal subgroup of G. (Kernel of a homomorphism is a normal subgroup of G.) If $Ker(\phi) = \{e\}$, then the identity element of G is the only element that leaves every $x \in X$ fixed. In this case, we say that G acts faithfully on X.

Definition 1.56. *Let X be a G-set. If for each $x_1, x_2 \in X$, there exists $g \in G$ such that $gx_1 = x_2$ then we say that G is transitive on X. Notice that G is transitive on X if and only if the subgroup $\phi[G]$ of S_X is transitive on X.*

Now we define two sets that comes when a group act on a set.
Let X be a G-set, $x \in X$ and $g \in G$. Consider two sets

$$X_g = \{x \in X : gx = x\}$$

and

$$G_x = \{g \in G : gx = x\}.$$

Note that X_g is the set of all elements in X that are fixed by $g \in G$ and G_x is the set of all elements in G that fix x.

Theorem 1.57. *Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.*

Proof. Let $x \in X$ and $g_1,\ g_2 \in G_x$. Then $g_1x = x$ and $g_2x = x$. Now

$$(g_1g_2)x = g_1(g_2x) = g_1x = x.$$

So $g_1g_2 \in G_x$. Thus G_x is closed under the induced operation of G. We have $ex = x$. So $e \in G$. If $g \in G_x$, then $gx = x$, so $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$. That is, if $g \in G_x$ then $g^{-1} \in G_x$. Thus G_x is a subgroup of G. □

The subgroup G_x of G is called the isotropy subgroup of x.

Here we define another important subset of X related to the group action on X.

Theorem 1.58. *Let X be a G-set. For $x_1,\ x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation.*

Proof. For each x in X, we have $ex = x$ and hence $x \sim x$ and the relation $\sim$ is reflexive.

Let $x_1 \sim x_2$. Then $gx_1 = x_2$ for some $g \in G$. Now $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = x_1$, so $x_2 \sim x_1$ and $\sim$ is symmetric.

Let $x_1 \sim x_2$ and $x_2 \sim x_3$. Then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1,\ g_2 \in G$. Since $g_1,\ g_2 \in G$, $g_2g_1 \in G$ and $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$. Hence $x_1 \sim x_3$ and $\sim$ is transitive. □

Definition 1.59. *Let X be a G-set. Each cell in the partition of the equivalence relation in Theorem 1.58 is an orbit in X under G. Let $x \in X$. The cell containing x is the orbit of x, which is denoted by Gx.*

Note that for $x \in X$, the orbit containing x is $Gx = \{gx : g \in G\}$. So $X = \cup_{x \in X} Gx$.

Next theorem gives the relationship between the orbits in X and the group structure of G. For $x \in X$, here we show that the cardinality of an orbit containing x is the index of the isotropy subgroup of x in G.

Theorem 1.60. *Let X be a G-set and $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.*

Proof. We define a one-to-one map ψ from Gx onto the collection of left cosets of G_x in G. Let $x_1 \in Gx$. Then there exists $g_1 \in G$ such that $g_1 x = x_1$.

We define $\psi(x_1)$ to be the left coset $g_1 G_x$ of G_x. Suppose there exists g_1' such that $g_1' x = x_1$. Then $g_1 x = g_1' x$. So $x = (g_1^{-1} g_1')x$. Therefore $g_1^{-1} g_1' \in G_x$. Hence $g_1 G_x = g_1' G_x$. This implies that the map ψ is well defined.

Now we claim that the map ψ is one to one. Suppose x_1, $x_2 \in Gx$ and $\psi(x_1) = \psi(x_2)$. Then there exist g_1, $g_2 \in G$ such that $x_1 = g_1 x$, $x_2 = g_2 x$. Since $\psi(x_1) = \psi(x_2)$, we have $g_1 G_x = g_2 G_x$. So $g_2 \in g_1 G_x$ and hence $g_2 = g_1 g$ for some $g \in G_x$. So $x_2 = g_2 x = (g_1 g)x = g_1(gx) = g_1 x = x_1$.

Next we prove ψ is onto. Let $g_1 G_x$ be a left coset. Then if $g_1 x = x_1$, then we have $g_1 G_x = \psi(x_1)$. Hence ψ is onto. Thus there exists a bijection from Gx onto $\{gG_x : g \in G\}$ and hence $|Gx| = (G : G_x)$.

If $|G|$ is finite, then $|Gx| = \frac{|G|}{|G_x|}$. and hence $|Gx|$ is a divisor of $|G|$. □

1.6 Applications of G-set to Counting

In this section we discuss an application of group action for counting.

The following theorem which is known as Burnside's formula, gives a tool for determining the number of orbits in a G-set X under a finite group G.

Theorem 1.61. *Let G be a finite group and X a finite set. If r is the number of orbits in X under G, then*

$$r.|G| = \sum_{g \in G} |X_g|.$$

Proof. Let N denote the number of pairs (g, x) with $g \in G$, $x \in X$ and $gx = x$. First, for each $g \in G$, there are $|X_g|$ pairs having g as first member where $X_g = \{x \in X : gx = x\}$. So

$$N = \sum_{g \in G} |X_g|. \tag{1.3}$$

Second, for each particular $x \in X$, there are $|G_x|$ pairs having x as second member. Then $N = \sum\limits_{x \in X} |G_x|$. By Theorem 1.60, we have

$$|Gx| = (G : G_x) = \frac{|G|}{|G_x|}.$$

Then

$$N = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|}. \tag{1.4}$$

Note that $1/|Gx|$ has the same value for all x in the same orbit. Let $\mathcal{O}$ be any orbit, then

$$\sum_{x \in \mathcal{O}} \frac{1}{|Gx|} = \sum_{x \in O} \frac{1}{|\mathcal{O}|} = 1 \tag{1.5}$$

Substituting 1.5 in 1.4, we obtain

$$N = |G|(\text{number of orbits in } X \text{ under } G) = |G|.r \tag{1.6}$$

From 1.3 and 1.6, we get $r.|G| = \sum_{g\in G} |X_g|$. Hence the proof. □

Corollary 1.62. *If G is a finite group and X is a finite G-set, then number of orbits in X under G=$\frac{1}{|G|}.\sum_{g\in G} |X_g|$*

Proof. The proof follows immediately follows from the above theorem. □

Question 1.63. Find the number of orbits in $\{1, 2, 3, 4, 5, 6, 7\}$ under the cyclic subgroup $\langle(1, 3, 5, 6)\rangle$ of S_7.

Solution. Let

$$G = \langle(1, 3, 5, 6)\rangle = \{I, (1, 3, 5, 6), (1, 5)(3, 6), (1, 6, 5, 3)\}$$

and $X = \{1, 2, 3, 4, 5, 6, 7\}$. Note that

$$|X_I| = 7,\ |X_{(1,3,5,6)}| = |\{2, 4, 7\}| = 3,\ |X_{(1,5)(3,6)}| = |\{2, 4, 7\}| = 3$$

and

$$|X_{(1,6,5,3)}| = |\{2, 4, 7\}| = 3.$$

We have $\sum_{g\in G} |X_g| = 7 + 3 + 3 + 3 = 16$. Hence the number of orbits under $G = \frac{1}{|G|}\sum_{g\in G} |X_g| = \frac{16}{4} = 4$. ■

Consider the problem of marking one to six dots on a cube to make a die. The standard die is marked so that when placed on a table with the one on the bottom and the 2 toward the front, the 6 is on top, the 3 on the left, the 4 on the right and 5 on the back. There are $6! = 720$ ways the cube faces can be marked in all. Note that one marking can be carried into another by a rotation of the marked cube. For example, if the standard die rotated 90° counter clockwise, then 3 will be on the front face rather than 2, but it is the same die. So some markings give the same die as others.

Let 1 be placed down. Then there are four rotations giving four positions, which gives the same die. Since there are six faces, we get $6 \times 4 = 24$ possible positions, which can be achieved from any other by a rotation of the die. These rotations form a group G.

Let X be the 720 possible ways of marking the cube. Consider the action of G on X by the rotation of the cube. Two markings give the same die if one can be carried in to the other under action by an element of G (rotating the cube). That is, each orbit in X under G correspond to a single die and different orbits to give different dice. So the number of distinguishable dice is actually the number of orbits under G in X.

Here $|X| = 720$ and $|G| = 24$. We have $X_g = \{x \in X : gx = x\}$ for all $g \in G$. Note that any rotation other than the identity element changes any one of the 720 markings in to a different one. So $|X_g| = 0$ for $g \neq e$ and $|X_e = 720$. Hence

$$(\text{number of orbits}) = \frac{1}{24}.720 = 30.$$

Example 1.64. How many distinguishable ways can seven people be seated at a round table, where there is no distinguishable "head"to the table?
Note that there are 7! ways to assign people to the different chairs. Let X to be the 7! possible arrangements. Consider the rotation ρ of people achieved by asking each person to move one place to the right results in the same arrangement. Clearly ρ generates a cyclic group G of order 7. Then G acts on X in the obvious way. We have

$$(\text{number of orbits in } X \text{ under } G) = \frac{1}{|G|}.\sum_{g \in G}|X_g|.$$

and $X_g = \{x \in X : gx = x\} = \{x \in X : g(x) = x\}$. Here the identity

element in G is the identity permutation I and

$$X_I = \{x \in X : I(x) = x\} = X.$$

Note that the only identity leaves any arrangement fixed and it leaves all 7! arrangements fixed. So by Corollary 1.62, the number of orbits=$\frac{1}{7}.7!$

Question 1.65. How many distinguishable necklaces with no clasp can be made using seven different colored beads of the same size?

Solution. Here the beads can be arranged in 7! ways and the necklace can be turned over as well as rotated. So instead of the cyclic group generated by the rotation, here the group is the dihedral group D_7 of order 14 as acting on the set X of 7! possibilities. Hence the number of distinguishable necklace is the number of orbits= $\frac{7!}{14} = 360$ ■

Question 1.66. Find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paint are available, assuming one colour is used on each edge, and the same colour may be used on different edges.

Solution. There are $4^3 = 64$ ways of painting the edges in all, since each of the three edges may be any one of four colours. Let X be the set of these 64 possible painted triangles. The group G acting on X is the group of symmetries of the triangle, which is isomorphic to S_3. We have $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$. Now $|X_{\rho_0}| = 64$, $|X_{\rho_1}| = |\{x \in X : \rho_1(x) = x\}| = 4$ (Since all edge must be the same colour and there are four possible colours). $|X_{\rho_2}| = 4$ $|X_{\mu_1}| = 16$(Since the edges that are interchanged must be the same colour or four possibilities and the other edge may also be any of the colours with four possibilities.) $|X_{\mu_2}| = 16 = |X_{\mu_3}|$(same reason as for μ_1).

Then

$$\sum_{g \in S_3} |X_g| = 64 + 4 + 4 + 16 + 16 + 16 = 120.$$

Thus the number of orbits=$\frac{1}{6}.120 = 20$. Hence there are 20 distinguishable painted triangles. ■

Question 1.67. Find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paints are available, assuming that a different color is used on each edge.

Solution. The number of possible ways of painting the edges is $4.3.2.1 = 24$.

Let X be the set of 24 possible painted triangles. The group acting on X can be considered to be S_3. Since all edges are a different color, we get $|X_{\rho_0}| = 24$ and $|X_g| = 0$ for all $g \in S_3 \setminus \{\rho_0\}$.
Thus the number of orbits=$\frac{1}{6}.24 = 4$. ■

EXERCISES

1. Find the number of orbits in $\{1, 2, \ldots, 8\}$ under the cyclic subgroup $\langle(1, 3, 5, 6, 7)\rangle$ of S_8.

2. Find the number of orbits in $\{1, 2, \ldots, 8\}$ under the subgroup of S_8 generated by $(1, 3)$ and $(2, 4, 7)$.

3. Wooden cubes of the same size are to be painted a different color on each face to make children's block. How many distinguishable blocks can be made if eight colors of paints are available?

4. Find the number of distinguishable ways the edges of a square of cardboard can be painted if six colours of paint are available and

   (a) no colour is used more than once.

   (b) the same colour can be used on any number of edges.

Module 2

In first module we studied direct products of groups, factor groups and group actions. This module also continues the study of group theory. Here we discuss isomorphism theorems, series of groups, Sylow Theorems and free groups.

2.1 Isomorphism Theorems

In this section we study some theorems about the relationship between factor groups and homomorphism. First we recall the fundamental homomorphism Theorem studied in the section entitled Factor Groups. This Theorem is also called First isomorphism Theorem.

Theorem 2.1. *(**First Isomorphism Theorem**) Let $\phi : G \to G'$ be a homomorphism with kernel K and let $\gamma_K : G \to G/K$ be the canonical homomorphism. There is a unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_K(x))$ for each $x \in G$.*

The above theorem tells us precisely what groups can be expected to arise as homomorphic images of a given group. We can express those in the form G/K where K is normal in G.

Let N be a normal subgroup of G. Here we show that there is a bijection between the set of all normal subgroups of G containing N and the set of all

normal subgroups of G/N.

Lemma 2.2. *Let N be a normal subgroup of a group G and let $\gamma : G \to G/N$ be the canonical homomorphism. Then the map ϕ from the set of normal subgroups of G containing N to the set of normal subgroups of G/N given by $\phi(L) = \gamma[L]$ is one to one and onto.*

Proof. Let L be a normal subgroup of G containing N. Since γ is a homomorphism, $\gamma(L)$ is a normal subgroup of $\gamma(G) = G/N$. Since $N \leq L$, for each $x \in L$ the coset xN in G is a subset of L. So $\gamma^{-1}[\phi(L)] = L$. Thus if L and M are normal subgroups of G containing N and if $\phi(L) = \phi(M) = H$, then $L = \gamma^{-1}[H] = M$. This implies that ϕ is one to one. Hence ϕ is a bijection.

If H is a normal subgroup of G/N, then $\gamma^{-1}[H]$ is a normal subgroup of G. Since $N \in H$ and $\gamma^{-1}[N] = N$. Thus we get $N \subseteq \gamma^{-1}[H]$. Hence $\phi(\gamma^{-1}[H]) = \gamma[\gamma^{-1}[H]] = H$. That is the map ϕ is onto. □

Let H and N be subgroups of a group G. Define

$$HN = \{hn : h \in H, n \in N\}$$

and $H \vee N$ is the intersection of all subgroups of G containing HN. Note that the join $H \vee N$ is the smallest subgroup of G containing HN. In general HN need not be a subgroup of G. If H or N is a normal subgroup of G, then we can show that HN is a subgroup of G and hence $HN = H \vee N$. This is our next theorem.

Theorem 2.3. *If N is a normal subgroup of G and if H is any subgroup of G, then $H \vee N = HN = NH$. Furthermore, if H is also normal in G, then HN is normal in G.*

Proof. First we show that HN is a subgroup of G. Let h_1, $h_2 \in H$ and n_1, $n_2 \in N$. Since N is a normal subgroup of G, we have $n_1h_2 = h_2n_3$ for some $n_3 \in N$. Then

$$\begin{aligned}(h_1n_1)(h_2n_2) &= h_1(n_1h_2)n_2 \\ &= h_1(h_2n_3)n_2 \\ &= (h_1h_2)(n_3n_2) \in HN.\end{aligned}$$

Hence HN is closed under the induced operation in G.

Obviously $e = ee$ is in HN. Let $h \in H$ and $n \in N$. Since N is a normal subgroup of G, $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}n_4$ for some $n_4 \in N$. Thus we get $(hn)^{-1} \in HN$. So HN is a subgroup of G.

Similarly we can show that NH is a subgroup of G. Hence $HN = NH$. Since $H \vee N$ is the smallest subgroup of G containing HN and HN itself a group, we have $HN = H \vee N = NH$.

Assume that H is also normal in G. Let $g \in G$, $h \in H$ and $n \in N$. Then

$$ghng^{-1} = (ghg^{-1})(gng^{-1}) \in HN.$$

Since g, h, n are arbitrary, we have HN is a normal subgroup of G. □

Next we prove the second isomorphism theorem using the fundamental homomorphism theorem.

Theorem 2.4. *(**Second Isomorphism Theorem**) Let H be a subgroup of G and let N be a normal subgroup of G. Then $(HN)/N \simeq H/(H \cap N)$.*

Proof. Let $\gamma : G \to G/N$ be the canonical homomorphism and $H \leq G$. Then $\gamma[H]$ is a subgroup of $\gamma[G]$. Since γ is onto, $\gamma[H]$ is a subgroup of G/N. Now

consider the restriction of γ to H, $\gamma_{|H}$, which is a homomorphism mapping H onto $\gamma[H]$.

Now the kernel of this homomorphism is

$$\begin{aligned} Ker(\gamma_{|H}) &= \{x \in H : \gamma(x) = N\} \\ &= \{x \in H : x + N = N\} \\ &= \{x \in H : x \in N\} \\ &= H \cap N. \end{aligned}$$

Then by Theorem 2.1, there is an isomorphism μ_1 from $H/H \cap N$ to $\gamma[H]$.

Since H is a subgroup of G and N is a normal subgroup of G, HN is a subgroup of G. Then γ restricted to HN provides a homomorphism mapping HN onto $\gamma[H]$. Now kernel of γ restricted to HN,

$$ker(\gamma_{|HN}) = \{g \in G : g \in HN \text{ and } \gamma(g) = N\} = N.$$

Then by Theorem 2.1, there is an isomorphism μ_2 from HN/N to $\gamma[H]$.

Define $\phi : (HN)/N \to H/(H \cap N)$ where $\phi = \mu_1^{-1}\mu_2$. Then

$$\begin{aligned} \phi((hn)N) &= \mu_1^{-1}(\mu_2((hn)N)) \\ &= \mu_1^{-1}((hn)N) \\ &= \mu_1^{-1}(hN) \\ &= h(H \cap N). \end{aligned}$$

Since the inverse of an isomorphism is an isomorphism and the composition of two isomorphisms is again an isomorphism, ϕ is an isomorphism. Hence the theorem. □

Example 2.5. Let $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, $H = \mathbb{Z} \times \mathbb{Z} \times \{0\}$ and $N = \{0\} \times \mathbb{Z} \times \mathbb{Z}$. Then

$$HN = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

and

$$H \cap N = \{0\} \times \mathbb{Z} \times \{0\}.$$

We have $HN/N \simeq \mathbb{Z}$ and $H/H \cap N \simeq \mathbb{Z}$.

Question 2.6. *Let H and K are two normal subgroups of G and $K \leq H$. Then prove that H/K is a normal subgroup of G/K.*

Solution. Let $hK \in H/K$ and $gK \in G/K$. Since H is normal in G,

$$(gK)^{-1}(hK)(gK) = (g^{-1}K)(hK)(gK) = (g^{-1}hg)K = h_1K \in H/K.$$

Hence H/K is a normal subgroup of G/K. ■

Here we prove the Third isomorphism Theorem.

Theorem 2.7. *Let H and K be normal subgroups of a group G with $K \leq H$. Then $G/H \simeq (G/K)/(H/K)$.*

Proof. Let $\phi : G \to (G/K)/(H/K)$ defined by $\phi(g) = gK(H/K)$ for $g \in G$. Let g_1, $g_2 \in G$. Then

$$\begin{aligned}
\phi(g_1g_2) &= [(g_1g_2)K](H/K) \\
&= [(g_1K)(g_2K)](H/K) \\
&= [(g_1K)(H/K)][(g_2K)(H/K)] \\
&= \phi(g_1)\phi(g_2).
\end{aligned}$$

So ϕ is a homomorphism. Now

$$\begin{aligned}\ker(\phi) &= \{x \in G : \phi(x) = H/K\} \\ &= \{x \in G : \ (xK)(H/K) = H/K\} \\ &= \{x \in G : \ xK \in H/K\} \\ &= \{x \in G : \ x \in H\} = H.\end{aligned}$$

So $\phi : G \to (G/K)/(H/K)$ defined by $\phi(g) = gK(H/K)$ is a homomorphism. Clearly ϕ is onto. Hence $G/H \simeq (G/K)/(H/K)$. □

Example 2.8. Let $K = 6\mathbb{Z}$, $H = 2\mathbb{Z}$ and $G = \mathbb{Z}$. Then $G/H = \mathbb{Z}/2\mathbb{Z}$ which is isomorphic to $\mathbb{Z}_2$.
Here $G/K = \mathbb{Z}/6\mathbb{Z}$ and $H/K = 2\mathbb{Z}/6\mathbb{Z}$. Now

$$G/K = \{6\mathbb{Z},\ 1 + 6\mathbb{Z},\ 2 + 6\mathbb{Z},\ 3 + 6\mathbb{Z},\ 4 + 6\mathbb{Z},\ 5 + 6\mathbb{Z}\}$$

and

$$H/K = \{6\mathbb{Z}, 2 + 6\mathbb{Z},\ 4 + 6\mathbb{Z}\}.$$

Hence$(G/K)/(H/K)$ has two elements and is isomorphic to $\mathbb{Z}_2$. Thus

$$\mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z}).$$

Question 2.9. *Let $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{12}$ be the homomorphism where $\phi(1) = 10$.*

1. *Find the kernel K of ϕ.*

2. *List the cosets in $\mathbb{Z}_{18}/K$, showing the elements in each coset.*

3. *Find the group $\phi[\mathbb{Z}_{18}]$.*

4. *Give the correspondence between $\mathbb{Z}_{18}/K$ and $\phi[\mathbb{Z}_{18}]$ as in First isomorphism theorem.*

Solution. Given that $\phi(1) = 10$. Now
$\phi(2) = \phi(1) +_{12} \phi(1) = 10 +_{12} 10 = 8$.
$\phi(3) = 8 +_{12} 10 = 6$.
$\phi(4) = 6 +_{12} 10 = 4$
$\phi(5) = 4 +_{12} 10 = 2$.
$\phi(6) = 0$. So $\phi(1) = \phi(7) = \phi(13) = 10$, $\phi(2) = \phi(8) = \phi(14) = 8$, $\phi(3) = \phi(9) = \phi(131) = 6$,$\phi(4) = \phi(10) = \phi(16) = 4$, $\phi(5) = \phi(11) = \phi(17) = 2$ and $\phi(0) = \phi(6) = \phi(12) = 0$.

1. $K = Ker(\phi) = \{x \in \mathbb{Z}_{18} : \phi(x) = 0\} = \{0, 6, 12\}$.

2. The cosets are $0+K = \{0, 6, 12\}$, $1+K = \{1, 7, 13\}$, $2+K = \{2, 8, 14\}$, $3 + K = \{3, 9, 15\}$, $4 + K = \{4, 10, 16\}$ and $5 + K = \{5, 11, 17\}$.

3. The group $\phi[\mathbb{Z}_{18}]$ is the subgroup $\{0, 2, 4, 6, 8, 10\}$ of $\mathbb{Z}_{12}$.

4. $\mu(0+K) = 0$, $\mu(1+K) = 10$, $\mu(2+K) = 8$, $\mu(3+K) = 6$, $\mu(4+K) = 4$ and $\mu(5 + K) = 2$.

■

Question 2.10. *In the group $\mathbb{Z}_{36}$, let $H = \langle 6 \rangle$ and $N = \langle 9 \rangle$.*

1. *List the elements in HN and in $H \cap N$.*

2. *List the cosets in HN/N.*

3. *List the cosets in $H/(H \cap N)$.*

4. *Give the isomorphism ϕ between HN/N and $H/(H \cap N)$.*

Solution. We have $H = \{0, 6, 12, 18, 24, 30\}$ and $N = \{0, 9, 18, 27\}$.

1. $HN = H + N = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$.
2. $HN/N = \{N, 3 + N, 6 + N\}$.
3. $H/(H \cap N) = \{H \cap N, 6 + H \cap N, 12 + H \cap N\}$.
4. $\phi(0+N) = H \cap N$, $\phi(3+N) = 12+H \cap N$ and $\phi(6+N) = 6+H \cap N$.

■

2.2 Series of Groups

Here we introduce the notion of series of a group G which is used to study the structure of G. Here we study the properties of various series of groups obtained from a given group G namely subnormal series, normal series and composition series.

Definition 2.11. *A subnormal(or subinvariant) series of a group G is a finite sequence $H_0, H_1, \ldots, H_n$ of subgroups of G such that $H_i < H_{i+1}$ and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = G$. A normal (or invariant) series of G is a finite sequence $H_0, H_1, \ldots, H_n$ of normal subgroups of G such that $H_i < H_{i+1}$ with $H_0 = \{e\}$ and $H_n = G$.*

A normal series is always subnormal. But the converse is not true.

Example 2.12. *Two examples of normal series of $\mathbb{Z}$ under addition are*

$$\{0\} < 16\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

and

$$\{0\} < 9\mathbb{Z} < \mathbb{Z}.$$

Consider the group D_4 of symmetries of the square. The series

$$\{\rho_0\} < \{\rho_0, \mu_1\} < \{\rho_0, \rho_2, \mu_1, \mu_2\} < D_4$$

is a subnormal series but it is not a normal series. Since $\{\rho_0, \mu_1\}$ is not normal in D_4.

Definition 2.13. *A subnormal(normal) series $\{K_j\}$ is a refinement of a subnormal (normal) series $\{H_i\}$ of a group G if $\{H_i\} \subseteq \{K_j\}$, that is if each H_i is one of the K_j.*

Example 2.14. *The series*

$$\{0\} < 144\mathbb{Z} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

is a refinement of the series $\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}$.

Definition 2.15. *Two subnormal(normal) series $\{H_i\}$ and $\{K_j\}$ of the same group G are isomorphic if there is a one-to-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that corresponding factor groups are isomorphic.*

Clearly two isomorphic subnormal (normal) series must have the same number of groups.

Example 2.16. Consider the group $\mathbb{Z}_{35}$ and two series $\{0\} < \langle 7\rangle < \mathbb{Z}_{35}$ and $\{0\} < \langle 5\rangle < \mathbb{Z}_{35}$. Note that the order of 7 in $\mathbb{Z}_{35}$ is $\frac{35}{gcd(7,35)} = 5$ and the order of 5 in $\mathbb{Z}_{35}$ is $\frac{35}{gcd(5,35)} = 7$. Hence

$$\mathbb{Z}_{35}/\langle 7\rangle \simeq \mathbb{Z}_7$$

and

$$\mathbb{Z}_{35}/\langle 5\rangle \simeq \mathbb{Z}_5.$$

So these two series are isomorphic.

Theorem 2.17. *Schreier Theorem*
Two subnormal(normal) of a group G have isomorphic refinements.

Definition 2.18. *A subnormal series $\{H_i\}$ of a group G is a composition series if all the factor groups H_{i+1}/H_i are simple. A normal series $\{H_i\}$ of G is principal or chief series if all the factor groups H_{i+1}/H_i are simple.*

Note that, for any group G, every principal series is a composition series and for abelian groups the concepts of composition and principal series coincide.

Question 2.19. *Prove that $\mathbb{Z}$ has no composition series.*

Solution. Suppose that $\{0\} = H_0 < H_1 < \ldots < H_{n-1} < H_n = \mathbb{Z}$ is a subnormal series. Then H_1 must be of the form $r\mathbb{Z}$ for some $r \in \mathbb{Z}^+$. Then H_1/H_0 is isomorphic to $r\mathbb{Z}$. We know that $r\mathbb{Z}$ is an infinite cyclic group with many proper non trivial normal subgroups (for example $2r\mathbb{Z}$ or $3r\mathbb{Z}$ etc.). So H_1/H_0 is not simple. Thus $\mathbb{Z}$ has no composition series. ■

Question 2.20. *Prove that, for $n \geq 5$, the series $\{e\} < A_n < S_n$ is a composition series of S_n.*

Solution. Consider the factor groups $A_n/\{e\}$ and S_n/A_n. We have $A_n/\{e\}$ is isomorphic to A_n, which is simple for $n \geq 5$. Also S_n/A_n is isomorphic to $\mathbb{Z}_2$ which is simple. ■

Remark 2.21. By Theorem 1.45, H_{i+1}/H_i is simple if and only if H_i is a maximal normal subgroup of H_{i+1}. So in a composition series, each H_i must be a maximal normal subgroup of H_{i+1}. To form a composition series of a group G, we first find a maximal normal subgroup H_{n-1} of G, then a

maximal normal subgroup H_{n-2} of H_{n-1} and so on. If this process terminates in a finite number of steps, then we have a composition series. Again by Theorem 1.45, a composition series cannot have any further refinement. To form a principal series, we find a maximal normal subgroup H_{n-1} of G, then a maximal normal subgroup H_{n-2} of H_{n-1} that is also normal in G and so on.

Theorem 2.22. ***Jordan-Holder Theorem***
Any two composition (principal) series of a group G are isomorphic.

Proof. Let $\{H_i\}$ and $\{K_i\}$ be two composition(principal) series of G. Then by Schreier Theorem, these two series have isomorphic refinements. But since all the factor groups are already simple, Theorem 1.45 shows that neither series has any refinement. Thus $\{H_i\}$ and $\{K_i\}$ must already be isomorphic. □

Theorem 2.23. *If G has a composition (principal) series and if N is a proper normal subgroup of G, then there exists a composition (principal) series containing N.*

Proof. Consider the series $\{e\} < N < G$, which is both a subnormal and normal series. Given that G has a composition series $\{H_i\}$. Then by Theorem 2.22, there is a refinement of $\{e\} < N < G$ to a subnormal series isomorphic to a refinement of $\{H_i\}$. Since $\{H_i\}$ is a composition series, it can have no further refinement. So $\{e\} < N < G$ can be refined to a subnormal series all of whose factor groups are simple. That is there exists a composition series containing N. Similarly we can easily show that there exists a principal series containing N if we start with a principal series $\{K_j\}$ of G. □

Definition 2.24. *A group G is solvable if it has a composition series $\{H_i\}$ such that all factor groups H_{i+1}/H_i are abelian.*

The group S_3 is solvable. The series $\{e\} < A_3 < S_3$ is a composition series and has factor groups isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_2$, which are abelian.

The Ascending Central Series

We already defined the center

$$Z(G) = \{z \in G : \ zg = gz \text{ for all } g \in G\}$$

of a group G and proved that it is a normal subgroup of G. So we can form the factor group $G/Z(G)$ and find the $Z(G/Z(G))$.
Note that $Z(G/Z(G))$ is normal in $G/Z(G)$.

Consider the cannonical homomorphism $\gamma : G \to G/Z(G)$. Then $\gamma^{-1}(Z(G/Z(G)))$ is a normal subgroup of G. Let it be $Z_1(G)$. Now form the group $G/Z_1(G)$ and find its center $Z(G/Z_1(G))$. Again consider the cannonical homomorphism $\gamma_1 : G \to G/Z_1(G)$. Take $Z_2(G) = \gamma_1^{-1}(Z(G/Z_1(G)))$ and so on.

Definition 2.25. *The series $\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \ldots$ described above is called the ascending central series of the group G.*

For example, the center of S_3 is $\{\rho_0\}$. So the ascending central series of of S_3 is $\{\rho_0\} \leq \{\rho_0\} \leq \{\rho_0\} \leq \{\rho_0\} \leq \ldots$.
The center of the group D_4 of symmetries of the square is $\{\rho_0, \rho_2\}$. Now $|D_4/\{\rho_0, \rho_2\}| = 4$ and hence abelian. So its center is $D_4/\{\rho_0, \rho_2\}$. So the ascending central series is $\{\rho_0\} \leq \{\rho_0, \rho_2\} \leq D_4 \leq D_4 \leq D_4 \leq D_4 \leq \ldots$.

Question 2.26. *Show that an infinite abelian group can have no composition series.*

2.3 Sylow Theorems

In finite group theory, the Sylow theorems are a collection of theorems named after the Norwegian mathematician Peter Ludwig Sylow (1872) that give

detailed information about the number of subgroups of fixed order that a given finite group contains. The Sylow theorems form a fundamental part of finite group theory and have very important applications in the classification of finite simple groups.

Let X be a finite G-set. Recall that for $x \in X$, the orbit of x in X under G is $Gx = \{gx : g \in G\}$. Assume that there are r orbits in X under G. Now every element of X is precisely in one orbit, so

$$|X| = \sum_{i=1}^{r} |Gx_i|.$$

Let $X_G = \{x \in X : gx = x \text{ for all } g \in G\}$. Then X_G is the union of one element orbits in X. Take $|X_G| = s$ where $1 \leq s \leq r$. Then

$$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i| \tag{2.1}$$

Using this equation here we prove an important theorem which have many application.

Theorem 2.27. *Let G be a group of order p^n and let X be a finite G-set. Then $|X| \equiv |X_G| (mod\, p)$.*

Proof. We have $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$. Since G is a finite group, $|Gx_i|$ divides $|G|$. Consequently p divides $|Gx_i|$ for $s+1 \leq i \leq r$. Hence $|X| - |X_G|$ is divisible by p. So $|X| \equiv |X_G| (mod\, p)$. □

Definition 2.28. *Let p be a prime. A group G is a p-group if every element in G has order a power of the prime p. A subgroup of a group G is a p-subgroup of G if the subgroup is itself a p-group.*

Theorem 2.29. *Cauchy's Theorem*

Let p be a prime. Let G be a finite group and p divides $|G|$. Then G has an element of order p and consequently, a subgroup of order p.

Proof. Let

$$X = \{(g_1, g_2, \ldots, g_p) : g_i \in G \text{ and } g_1 g_2 \ldots g_n = e\}.$$

Since $(e, e, e, \ldots, e) \in X$, X is non empty. Let $g_1, g_2, \ldots g_{p-1}$ be any $p-1$ elements of G and g_p is uniquely determined by $(g_1 g_2 \ldots g_{p-1})^{-1}$. So

$$|X| = |G|^{p-1}.$$

Since p divides $|G|$, p divides $|X|$ also. Let σ be the cycle $(1, 2, 3, \ldots, p)$ in S_P. Let σ act on X by

$$\sigma(g_1, g_2, \ldots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_P, g_1).$$

Let $(g_1, g_2, \ldots, g_p) \in X$. Then $e = g_1 g_2 \ldots g_p = g_1(g_2 g_3 \ldots g_p)$. Thus $g_1^{-1} = (g_2 g_3 \ldots g_p)$. Now

$$g_2 g_3 \ldots g_P g_1 = (g_2 g_3 \ldots g_P).g_1 = g_1^{-1} g_1 = e.$$

So $(g_2, g_3, \ldots, g_P, g_1) \in X$. Thus σ acts on X.

Consider the group $\langle\sigma\rangle$ generated by σ. It is of order p and it acts on X. So X is a finite $\langle\sigma\rangle$-set. Then we have

$$|X| \equiv |X_{\langle\sigma\rangle}| (mod\, p).$$

Hence $p||X| - |X_{\langle\sigma\rangle}|$. Also we have $p||X|$. This implies that $p||X_{\langle\sigma\rangle}|$. Now

$$X_{\langle\sigma\rangle} = \{(g_1, g_2, \ldots, g_p) : \sigma(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)\}.$$

Since $\langle\sigma\rangle$ is generated by σ, it is enough to check $\sigma(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)$ instead of checking with all elements from $\langle\sigma\rangle$. Now

$$\begin{aligned}\sigma(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)\} \\ &\Leftrightarrow (g_2, g_3, \ldots, g_p, g_1) = (g_1, g_2, \ldots, g_p)\} \\ &\Leftrightarrow g_1 = g_2 = \ldots = g_p.\end{aligned}$$

Since $(e, e, \ldots, e) \in X_{\langle\sigma\rangle}$ and $p||X_{\langle\sigma\rangle}|$, there must at least p elements in $X_{\langle\sigma\rangle}$. Hence there exists some element $a \in G$, $a \neq e$ such that $(a, a, \ldots, a) \in X_{\langle\sigma\rangle}$ and hence $a^p = e$. So a has order p and $\langle a\rangle$ is a subgroup of G of order p. Hence the proof. □

Let G be a group of order 6. Then by Cauchy's theorem, G must contain an element of order 2 and an element of order 3.

Corollary 2.30. *Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.*

Proof. Let G be a p-group. Then every element in G has order a power of the prime p. If a prime $q \neq p$ divides $|G|$, then G has an element of order q by Cauchy's Theorem. This is a contradiction since G is a p-group. So the order of G must be a power of p.

Conversely suppose that $|G|$ is a power of p. Let $a \in G$. Since the order of a divides order of G, order of a is a power of p. Since a is arbitrary, the order of every element in G is a power of p. Thus G is a p-group. □

The Sylow Theorems

Let G be a group and $\mathscr{S}$ be the collection of all subgroups of G. Now we define an action of G on $\mathscr{S}$ as follows.
For, $g \in G$ and $H \in \mathscr{S}$, $g * H = gHg^{-1}$. Now

$$G_H = \{g \in G : gHg^{-1} = H\}$$

is a subgroup of G and H is a normal subgroup of G_H. Since G_H consists of all $g \in G$ with $gHg^{-1} = H$, G_H is the largest subgroup of G in which H is normal. The subgroup G_H is called the normalizer of H in G and is denoted by $N[H]$.

Lemma 2.31. *Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \equiv (G : H) \, (mod\, p)$.*

Proof. Let $\mathscr{L}$ be the set of all left cosets of H in G, and H acts on $\mathscr{L}$ by left translation, so that $h(xH) = (hx)H$. Then $\mathscr{L}$ becomes an H-set. Note that $\mathscr{L} = (G : H)$. We have

$$\mathscr{L}_H = \{xH \in \mathscr{L} : h(xH) = xH \text{ for all } h \in H\}.$$

That is, $\mathscr{L}_H$ is the set of all left cosets that are fixed under action by all elements of H. Note that

$$\begin{aligned} xH = h(xH) &\Leftrightarrow H = x^{-1}hxH \\ &\Leftrightarrow x^{-1}hx \in H \\ &\Leftrightarrow x^{-1}h(x^{-1})^{-1} \in H \, \forall \, h \in H \\ &\Leftrightarrow x \in N[H]. \end{aligned}$$

Thus

$$xH = h(xH) \text{ for all } h \in H \Leftrightarrow x^{-1}h(x^{-1})^{-1} \in H \Leftrightarrow x \in N[H].$$

Hence $|\mathscr{L}_H| = (N[H] : H)$.

Given that H is a p subgroup of G, the order of H is a power of p by Corollary 2.30. Then by Theorem 2.27, we get $|\mathscr{L}| \equiv |\mathscr{L}_H| (mod\, p)$. Note that $|\mathscr{L}| = (G : H)$. Hence $(N[H] : H) \equiv (G : H) \, (mod\, p)$. □

Corollary 2.32. *Let H be a p-subgroup of a finite group G. If p divides $(G : H)$, then $N[H] \neq H$.*

Proof. Given that p divides $(G : H)$. By the above theorem, we have $(N[H] : H) \equiv (G : H) \, (mod\, p)$. That is p divides $(N[H] : H) - (G : H)$. So p must divide $(N$[H]: H). Hence $N[H] \neq H$. □

Now we state the first Sylow theorem.

Theorem 2.33. ***(First Sylow Theorem)*** *Let G be a finite group and $|G| = p^n m$ where $n \geq 1$ and p does not divide m. Then*

1. *G contains a subgroup of order p^i for each i where $1 \leq i \leq n$.*
2. *Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i \leq n$.*

Proof. 1. By Cauchy's theorem, G contains a subgroup of order p. We use mathematical induction to prove the existence of a subgroup of order p^i for $i < n$ implies the existence of a subgroup of order p^{i+1}. Let H be a subgroup of order p^i. Since $i < n$, p divides $(G : H)$. By Lemma 2.31, we have p divides $(N[H] : H)$. Since H is a normal subgroup of $N[H]$, we can find $N[H]/H$. Clearly p divides $|N[H]/H|$. Since

p divides $|N[H]/H|$, the factor group $|N[H]/H|$ has a subgroup K of order p. Let $\gamma : N[H] \to N[H]/H$ be the Canonical homomorphism, then $\gamma^{-1}[K] = \{x \in N[H] : \gamma(x) \in K\}$ is a subgroup of $N[H]$ and hence a subgroup of G. This subgroup contains H and is of order p^{i+1}.

2. From the first part, we have $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[K]| = p^{i+1}$. Since H is normal in $N[H]$, H is normal in $\gamma^{-1}[K]$.

□

Definition 2.34. *A Sylow p-subgroup P of a group G is a maximal p-subgroup of G.*
That is, Sylow p-subgroup P of a group G is a p-subgroup not contained in a larger p-subgroup.

That is a Sylow p-subgroup is a subgroup whose order is a power of p and whose index is relatively prime to p.

The First Sylow theorem guarantees the existence of a Sylow p-subgroup of G for any prime p dividing the order of G.

The second Sylow theorem states that all the Sylow subgroups of a given order are conjugate.

Theorem 2.35. ***(Second Sylow Theorem)*** *Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.*

Proof. Let $\mathscr{L}$ be the collection of left cosets of P_1. We define an action of P_2 on $\mathscr{L}$ as follows.
$*(y, xP_1) = (yx)P_1$ where $y \in P_2$ and $xP_1 \in \mathscr{L}$.
Then $\mathscr{L}$ is a P_2-set. Then by Theorem 2.27, $|\mathscr{L}_{P_2}| \equiv |\mathscr{L}|(modp)$. Here $|\mathscr{L}| = (G : P_1)$. Since P_1 is a Sylow subgroup, $|\mathscr{L}|$ is not divisible by p. So $|\mathscr{L}_{P_2}| \neq 0$. Recall that $\mathscr{L}_{P_2} = \{xP_1 : y(xP_1) = xP_1 \text{for all } y \in P_2\}$.

Let $xP_1 \in \mathscr{L}_{P_2}$. Then $y(xP_1) = xP_1$ for all $y \in P_2$. This implies that $(x^{-1}yx)P_1 = P_1$ for all $y \in P_2$. That is $x^{-1}yx \in P_1$ for all $y \in P_2$ and hence $x^{-1}P_2x$ is contained in P_1. Since $|P_1| = |P_2|$, $x^{-1}P_2x = P_1$. Thus we get P_1 and P_2 are conjugate subgroups of G. □

The third Sylow theorem gives information about the number of Sylow p-subgroups.

Theorem 2.36. ***(Third Sylow Theorem)***
Let G be a finite group and p divides $|G|$. Then the number of Sylow p-groups is congruent to 1 modulo p and divides $|G|$.

Proof. Let P be a Sylow p-subgroup of G. Let $\mathscr{S}$ be the set of all Sylow p-subgroups. Define an action of P on $\mathscr{S}$ by $(x, T) \to xTx^{-1}$ for $x \in P$ and $T \in \mathscr{S}$. Then

$$|\mathscr{S}| \equiv |\mathscr{S}_P| (mod\, p).$$

We have

$$\mathscr{S}_P = \{T \in \mathscr{S} : xTx^{-1} = T \text{ for all } x \in P\}.$$

If $T \in \mathscr{S}_P$, then $P \leq N[T]$. Clearly $T \leq N[T]$. Since P and T are Sylow p-subgroups of G, they are also Sylow p-subgroups of $N[T]$. Then by the Second Sylow Theorem, T and P are conjugate in $N[T]$. Since T is a normal subgroup of $N[T]$, the conjugate of T in $N[T]$ is T itself. Hence $T = P$. So $\mathscr{S}_P = \{P\}$. Thus we get $|\mathscr{S}| \equiv 1 (mod\, p)$. That is the number of Sylow p-groups is congruent to 1 modulo p.

Next we define an action of G on $\mathscr{S}$ by conjugation. Since all sylow p-subgroups are conjugates, there is only one orbit in $\mathscr{S}$ under G. If $P \in \mathscr{S}$, then

$$|\mathscr{S}| = |\text{orbit of } P| = (G : G_P).$$

But $(G : G_p)$ is a divisor of $|G|$. So the number of Sylow p-subgroups divides $|G|$. □

Example 2.37. Let G be a group of order 15. Using Sylow Theorem we can easily show that G has a normal subgroup of order 5 and hence G is not simple.

By First Sylow Theorem G has at least one subgroup of order 5 and by third Sylow theorem, the number n of such subgroups is congruent to 1 modulo 5 and divides 15. The numbers congruent 1 modulo 5 is 1, 6, 11, ... and this number must divides 15. This implies that there is only one subgroup P of order 5.

For each $g \in G$, consider the inner automorphism $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$ for all $x \in G$. Since an automorphism maps subgroups to subgroups, $i_g(P)$ must be subgroup of G of order 5. But there is only one subgroup P of order 5. Hence $i_g(P) = gPg^{-1} = P$ for all $g \in G$. This implies that P is normal in G.

Question 2.38. *Let G be a finite group and p divides order of G. Show that if G has only one proper Sylow p-subgroup, it is simple*

2.4 Applications of the Sylow Theory

Here we discuss several applications of Sylow theorems. Using Sylow's theorems, we prove the existence of subgroups of a specified order, and analyse the structure of some finite groups.

Applications to p-Groups and the Class Equation

Theorem 2.39. *Every group of prime-power order (that is, every finite p-group) is solvable.*

Proof. Let G be a group with order p^r. Then by First Sylow theorem, G has a subgroup of H_i of order p^i and H_i is normal in H_{i+1} for $1 \leq i < r$. Then

$$\{e\} = H_0 < H_1 < H_2 < \ldots < H_r = G$$

is a composition series. Note that the order of the factor group H_{i+1}/H_i is p. Since every group of order p is cyclic and hence abelian, each factor group H_{i+1}/H_i is abelian. So G is solvable. □

Let X be a finite G-set where G is a finite group. In Section 2.3, we derived the following equation (2.1)

$$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$$

where $X_G = \{x \in X : gx = x \text{ for all } g \in G\}$ and $Gx_i = \{gx : g \in G\}, x_i$ is the element in the ith orbit in X.

Now we consider the conjugation action of G on G itself. That is, $g \in G$ carries $x \in G$ into gxg^{-1}. Then

$$\begin{aligned} X_G &= \{x \in G : gxg^{-1} = x \text{ for all } g \in G\} \\ &= \{x \in X : gx = xg \text{ for all } g \in G\} \\ &= Z(G). \end{aligned}$$

Recall that $Z(G)$ is the center of G. So we have

$$|G| = |Z(G)| + \sum_{i=s+1}^{r} |Gx_i|$$

Take $c = |Z(G)|$ and $n_i = |Gx_i|$. Then we obtain

$$|G| = c + n_{c+1} + \ldots + n_r. \tag{2.2}$$

where n_i is the number of elements in the ith orbit of G under conjugation by itself. We have $|Gx| = (G : G_x)$ and hence $|G_x| = |G|/|Gx|$. So n_i divides $|G|$ for $c + 1 \leq i \leq r$.

Definition 2.40. *The equation 2.2 is the class equation of G. Each orbit in G under conjugation by G is a conjugate class in G.*

If G is abelian, then the class equation is $|G| = |Z(G)|$.

Question 2.41. *Find the class equation of S_3.*

Solution. In Module I, section 1.2, the group table for S_3 is given. From the table, we can easily calculate the conjugate classes. They are $\{\rho_0\}$, $\{\rho_1, \rho_2\}$ and $\{\mu_1, \mu_2, \mu_3\}$. So the class equation is

$$6 = 1 + 2 + 3.$$

■

We can easily deduce the following theorem from the class equation.

Theorem 2.42. *The center of a finite non trivial p-group G is nontrivial.*

Proof. We have the class equation $|G| = c + n_{c+1} + \ldots + n_r$. Here each n_i divides $|G|$ for $c+1 \leq i \leq r$ and the order of G is a power of p. This implies that p divides n_i and p divides $|G|$. Hence p divides $|G| - c + n_{c+1} + \ldots + n_r$. That is, p divides c. Since $e \in Z(G)$, $c \geq 1$. So $c \geq p$. So there exists some $a \in Z(G)$ where $a \neq e$. □

Next we prove that every group of order p^2 is abelian. In order to prove this result we need the following lemma on direct product of groups.

Lemma 2.43. *Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.*

Proof. Recall that $H \vee K$ is the intersection of all groups containing HK. By lemma 2.3, we have $H \vee K = HK$. First we show that $hk = kh$ for all $h \in H$ and $k \in K$.

Consider the commutator $hkh^{-1}k^{-1}$. Since H and K are normal subgroups of G, we have

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1`} = k_1k^{-1}$$

for some $k_1 \in K$ and

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = h_1h^{-1}$$

for some $h_1 \in H$. Hence $hkh^{-1}k^{-1} \in H \cap K = \{e\}$. Thus $hkh^{-1}k^{-1} = e$ and hence $hk = kh$.

Let $\phi : H \times K \to G$ be defined by $\phi(h, k) = hk$. First we verify that ϕ is a homomorphism. Let (h, k), $(h', k') \in H \times K$. Then

$$\begin{aligned}\phi((h, k), (h', k')) &= \phi(hh', kk') \\ &= hh'kk' \\ &= hkh'k' \\ &= \phi(h, k)\phi(h', k')\end{aligned}$$

So ϕ is a homomorphism. Now the kernel of $\phi = \{(h, k) \in H \times K : \phi(h, k) =$

$e\} = \{(h,k) \in H \times K : hk = e\} = \{(h,k) \in H \times K : h = k^{-1}\}$. That is, both h and k are in $H \cap K$. Since $H \cap K = \emptyset$, $h = k = e$. So $Ker(\phi) = \{(e,e)\}$ and ϕ is one to one. By lemma 2.3, we know that $HK = H \vee K$. By our assumption $H \vee K = G$. Thus ϕ is onto G, and $H \times K \simeq G$. □

Theorem 2.44. *For a prime p, every group G of order p^2 is abelian.*

Proof. If G is cyclic, there is nothing to prove.

Suppose that G is not cyclic. Since the order of an element in a finite group divides the order of G, order of every element other than e is p. Let $a \in G \setminus \{e\}$. Consider the cyclic group $\langle a \rangle$ generated by a, which is of order p. So we can choose $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$. Otherwise a non identity element $c \in \langle a \rangle \cap \langle b \rangle$ would generate both $\langle a \rangle$ and $\langle b \rangle$. This implies that $\langle a \rangle = \langle b \rangle$, which is a contradiction. Since the order of a and b is p, $\langle a \rangle$ and $\langle b \rangle$ are normal in G, by First Sylow theorem. Now $\langle a \rangle \vee \langle b \rangle$ is a subgroup of G properly containing a and of order dividing p^2. Hence $\langle a \rangle \vee \langle b \rangle = G$. Then by Lemma 2.43, $G \simeq \langle a \rangle \vee \langle b \rangle$ and hence G is abelian. □

Further Applications

Theorem 2.45. *If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.*

Proof. Let G be a group of order pq. Then by First Sylow theorem, G has a Sylow q-subgroup. The number of Sylow q-subgroups is congruent to 1 modulo q and this number divides the order of $G\,(pq)$ by Third Sylow theorem. This imples that number of Sylow q-subgroups is congruent to 1

modulo q and divides p. So the only possibility is one. Thus there is only one Sylow q-subgroup Q of G. Consider the inner automorphism $i_g : G \to G$ defined by$i_g(x) = gxg^{-1}$ for all $x \in G$. Then $i_g[Q]$ is a subgroup of G of order q. Since G has only one subgroup of order q, $i_g[Q] = Q$. This is true for all $g \in G$. That is $gQg^{-1} = Q$ for all $g \in G$. So Q is normal in G and hence G is not simple.

Again using First Sylow theorem and Third Sylow theorem, G has a Sylow p-subgroup P and the number of Sylow p-subgroup is congruent to 1 modulo p and this number divides pq. Hence the number must be either 1 or q. If q is not congruent to 1 modulo p, then the number must be 1 and P is normal in G.

Suppose hat $q \not\equiv 1(mod)p$. Since every element in $Q \setminus \{e\}$ is of order q and every element in $P \setminus \{e\}$ is of order p, we have $Q \cap P = \{e\}$. Also $Q \vee P$ must be a subgroup of G properly containing Q and order dividig pq. This implies that is $G = Q \vee P$. Then by Lemma 2.43, $G \simeq Q \times P \simeq \mathbb{Z}_q \times \mathbb{Z}_p$. Thus G is abelian and cyclic. □

Example 2.46. We have $15 = 3 \times 5$ and 5 is not congruent 1 mod 3. So every group of order 15 is cyclic.

Every group of order 159 is cyclic. Since $159 = 53 \times 3$ and 53 is not congruent to 1 mod 3.

Lemma 2.47. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}.$$

Proof. Let $|H| = r$, $|K| = s$ and $|H \cap K| = t$. Recall that $HK = \{hk : h \in H, k \in K\}$. Here $|HK| \leq rs$. We have to show that $|HK| = \frac{rs}{t}$. That is,

it is enough to show that each element $hk \in HK$ can be represented in the form h_ik_i, $h_i \in H$ and $k_i \in K$, as many times as there are elements of $H \cap K$, that is, t times.

For every $x \in H \cap K$, $hk = (hx)(x^{-1}k)$. So each element in HK is represented by at least $|H \cap K|$ elements in HK.

Now $hk = h_1k_1$ implies that $x = hh_1^{-1} = k_1k^{-1} \in H \cap K$. So $h_1 = x^{-1}h$ and $k_1 = xk$. Thus each element in HK is represented by $|H \cap K|$ products. Hence $|HK| = \dfrac{(|H|)(|K|)}{|H \cap K|}$. □

Example 2.48. Let p be a prime. No group of order p^r for $r > 1$ is simple. Let G be a group of order p^r. Then by First Sylow theorem, G contains a subgroup of order p^{r-1} normal in G.

A group of order $16 = 2^4$ is not simple. Since it has a normal subgroup of order $2^3 = 8$.

Remark 2.49. Let G be a finite group. If we show that there is only one Sylow p subgroup for some prime p dividing the order of G, then all conjucate of it must be itself and hence it is normal in G. So G is not$G$ has only one simple. Hence in order to prove a group is not simple, it is enough to show that one Sylow p subgroup for some prime p dividing the order of G.

Example 2.50. No group G of order 20 is simple. This is because G contains Sylow 5-subgroup and the number of Sylow 5-subgroup is congruent to 1 modulo 5 and a divisor of 20. So there is only one Sylow 5-subgroup. Then all conjugates of it must be itself and hence normal in G.

Example 2.51. No group G of order 30 is simple. Here the possible number of Sylow 5-subgroups are 1 or 6 and the possible number of Sylow 3-subgroups are 1 or 10. If the number of Sylow 5-subgroup or Sylow 5-subgroup is

one, there is nothing to prove. If G has six Sylow 5-subgroups, then the intersection of any two is a subgroup of each of order dividing 5. Hence the intersection must be the trivial group. Thus each contains four elements of order 5. Thus there are 24 elements of order 5.Similarly if G has 10 Sylow 3-subgroups, it has atleast 20 elements of order three. Since the order of G is 30, this is not possible. So there is a normal subgroup either of order 3 or 5.

Question 2.52. *Prove that no group G of order* 96 *is simple.*

Solution. Since $96 = 2^5 \times 3$, G has a Sylow 2-subgroup of order 32. The number of Sylow 2-subgroup is congruent to 1 modulo 2 and a divisor of 96. Hence G has 1 or 3 subgroups of order 32. If there is only one Sylow 2-subgroup, then it is normal in G. If not, let H and K be two distinct subgroups of order 32. We have $|HK| = \dfrac{(|H|)(|K|)}{|H \cap K|}$. So $H \cap K$ must have order 16. Since $(H : H \cap K) = 2$, $H \cap K$ is normal in H. Similarly $H \cap K$ is normal in K also. So the normalizer of $H \cap K$, $N[H \cap K]$ has order a multiple greater than 1 of 32 and a divisor of 96. So the order must be 96. That is $H \cap K$ is normal in G. ■

EXERCISES

1. Show that every group of order 255 is abelian.

2.5 Free Groups

In some groups such as the symmetric group S_3, the dihedral group D_n and the group M of rigid motions of the plane, one can compute easily using a list of generators and a list of relations for manipulating them. Here we consider groups which have a set of generators satisfying no relations other

than the relationship between an element and its inverse required as one of the defining properties of a groups

Words and Reduced Words

Let A be any set of elements a_i for $i \in I$. We think A as an alphabet and a_i as letters in the alphabet. Symbol of the form a_i^n with $n \in \mathbb{Z}$ is a syllable and a finite string w of syllables written in juxtaposition is a word. We also permit the word with no syllables which is called the empty word.

Example 2.53. *Let $A = \{a, b, c\}$. Then $ab^{-2}c^2b$, $b^3b^{-1}ca^2a^{-7}$ and c^2 are all words.*

There are two types elementary contractions(modifications of certain words). The first type consists of replacing an occurrence of $a_i^n a_i^m$ in a word by a_i^{n+m} and the second type consists of replacing an occurrence of a_i^0 in a word by 1, which is dropped out from the word. Note that every word can be changed to a reduced word by means of a finite number of elementary contractions. In a reduced word no elementary contraction is possible. Note that there is often more than one way to proceed the elementary contraction, but there is only one reduced word for a given word. .

Example 2.54. *The reduced form of the word $b^3b^{-1}ca^2a^{-7}$ is b^2ca^{-5}.*

Free Groups

Let A be an alphabet and $F[A]$ denotes the set of all reduced words formed from the alphabet A. Two words can be composed by juxtaposition. That is, for w_1, $w_2 \in F[A]$, $w_1.w_2$ to be the reduced form of the word obtained by juxtaposition w_1w_2 of the two words.

Example 2.55. *Let $w_1 = b^3a^{-5}c^2$ and $w_2 = c^{-2}a^2cb^{-2}$. Then $w_1.w_2 = b^3a^{-5}c^2.c^{-2}a^2cb^{-2} = b^3a^{-3}cb^{-2}$*

The operation of multiplication(the reduced form of the word obtained by juxtaposition) on $F[A]$ is well defined and associative. The empty word 1 acts as an identity element. Given a reduced word $w \in F[A]$, if we form the word obtained by first writing the syllables of w in the opposite order and second by replacing each a_i^n by a_i^{-n}, then the resulting word w^{-1} is a reduced word and $w.w^{-1} = w^{-1}.w = 1$. Thus we get $F[A]$ forms a group and which is called the free group generated by A.

Definition 2.56. *If G is a group with a set $A = \{a_i\}$ of generators, and if G is isomorphic to $F[A]$ under a map $\phi : G \to F[A]$ such that $\phi(a_i) = a_i$, then G is free on A and the a_i are free generators of G. A group is free if it is free on some nonempty set A.*

The free group on the set $A = \{a\}$ consisting of one element is the same as the set of all powers of a. That is $F[A] = \{a^n : n \in \mathbb{Z}\}$. So it is an infinite cyclic group $(\mathbb{Z})$.

Remark 2.57. *Every free group is infinite.*

Definition 2.58. *If G is free on A, the number of elements in A is the rank of the free group G.*

Two free groups are isomorphic if and only if they have the same rank. A non trivial proper subgroup of a free group is free.

Example 2.59. *Let $F[\{x, y\}]$ be the free group on $\{x, y\}$. Let $y_k = x^k y x^{-k}$ for $k \geq 0$. The y_k for $k \geq 0$ are free generators for the subgroup of $F[\{x, y\}]$ that they generate.*

The above example shows that subgroup of a free group is free and the rank of the subgroup may be much greater than the rank of the whole group.

Homomorphisms of Free Groups

Here we show that a homomorphism of a group is completely determined if we know its values on each element of a generating set.

Theorem 2.60. *Let G be generated by $A = \{a_i : i \in I\}$ and let G' be any group. If a'_i for $i \in I$ are any elements in G', not necessarily distinct, then there is at most one homomorphism $\phi : G \to G'$ such that $\phi(a_i) = a'_i$. If G is free on A, then there is exactly one such homomorphism.*

Proof. Let ϕ be a homomorphism from G into G' such that $\phi(a_i) = a'_i$. For any $x \in G$, we have $x = \prod_j a_{i_j}^{n_j}$ for some finite product of the generators a_i where the a_{i_j} appearing in the product need not be distinct. We have

$$\phi(x) = \prod_j \phi(a_{i_j}^{n_j}) = \prod_j (a'_{i_j})^{n_j}.$$

This implies that a homomorphism is completely determined by by its values on elements of a generating set. Hence there is at most one homomorphism such that $\phi(a_i) = a'_i$.

Suppose that $G = F[A]$. That is, G is free on A. Then define $\psi : G \to G'$ as $\psi(x) = \prod_j (a'_{i_j})^{n_j}$ for $x = \prod_j a_{i_j}^{n_j} \in F[A]$. Since $F[A]$ consists precisely of reduced words; no two different formal products in $F[A]$ are equal, the map ψ is well defined. It is easy to show that $\psi(xy) = \psi(x)\psi(y)$ for x, $y \in G$. So ψ is a homomorphism. □

A homomorphism of a cyclic group is completely determined if we know its value on any single generator of the group.

Theorem 2.61. *Every group G' is a homomorphic image of a free group G.*

Proof. Let $G' = \{a'_i : i \in I\}$ and let $A = \{a_i : i \in I\}$ be set with same number of elements as G'. Let $G = F[A]$. Then by Theorem 2.60, there

exists a homomorphism ψ mapping G into G' such that $\psi(a_i) = a_i'$. Then clearly the image of G under ψ is all of G'. □

Question 2.62. *Find the reduced form and the inverse of the reduced form of the word* $a^2b^{-1}b^3a^3c^{-1}c^4b^{-2}$.

Solution. The reduced form is $a^2b^2a^3c^3b^{-2}$ and the inverse is $b^2c^{-3}a^{-3}b^{-2}a^{-2}$.

■

Question 2.63. *How many different homomorphism are there of a free group of rank* 2 *into*
1). $\mathbb{Z}_4$, 2). $\mathbb{Z}_6$ *and* 3). S_3?

Solution. Let G be a free group of rank 2. Then G is generated by $\{a_1, a_2\}$ say. For any two element x, y in G', not necessarily distinct, there is exactly one homomorphism $\phi : G \to G'$ such that $\phi(a_1) = x$ and $\phi(a_2) = y$.

1. Since $\mathbb{Z}_4$ has four elements, there are $4 \times 4 = 16$ homomorphisms.
2. There are $6 \times 6 = 36$ homomorphisms.
3. There are $6 \times 6 = 36$ homomorphisms.

■

Question 2.64. *How many different homomorphism are there of a free group of rank* 2 *onto 1)* $\mathbb{Z}_4$*? 2)*

Solution. In the previous problem, we determined the number of homomorphisms. Here we have to find the number of onto homomorphisms.

Here we have to find the number of homomorphisms from G onto $\mathbb{Z}_4$. The homomorphism will be onto if and only if not both a_1 and a_2 are mapped into the subgroup $\{0, 2\}$. So there are $16 - 4 = 12$ homomorphisms onto $\mathbb{Z}_4$.

■

Module 3

In this Module, we discuss rings of polynomials, factorization of polynomials over a field, homomorphisms and factor rings. the group presentation is also studied.

3.1 Rings of Polynomials

We already studied polynomials with integer coefficients, rational coefficients, real coefficients and complex coefficients. Note that all of these sets of polynomials are rings and in each case the set of coefficients is also a ring. In this section, we study rings of polynomials over arbitrary rings.

Definition 3.1. *Let R be a ring and x be an indeterminate. A polynomial $f(x)$ with coefficients in R is an infinite formal sum*

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values i. The a_i are coefficients of $f(x)$. If for some $i \geq 0$, $a_i \neq 0$, the largest such value of i is the degree of $f(x)$. If all $a_i = 0$, then the degree of $f(x)$ is undefined.

Let $f(x) = a_n x^n + \ldots a_1 x + a_0$ where $a_n \neq 0$. The term a_n is called the

leading coefficient of $f(x)$. If the leading coefficient of $f(x)$ is the multiplicative identity of R, we say that $f(x)$ is a monic polynomial.

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n + \ldots$ be two polynomials. Then

$$f(x) + g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n + \ldots$$

where $c_n = a_n + b_n$ and

$$f(x)g(x) = d_0 + d_1x + d_2x^2 + \ldots + d_nx^n + \ldots$$

where $d_n = \sum_{i=0}^{n} a_ib_{n-i} = a_0b_n + a_1b_{n-1} + \ldots + a_nb_0$. Note that c_i and d_i are 0 for all but a finite number of values of i. Hence $f(x) + g(x)$ and $f(x)g(x)$ are polynomials.

Theorem 3.2. *The set $R[x]$ of all polynomials in an indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication. If R is commutative, then so is $R[x]$ and if R has unity $1 \neq 0$, then 1 is also unity for $R[x]$.*

Proof. Our definitions for addition and multiplication of polynomials were formulated so that they commutative and associative and so that multiplication is distributive over addition. We leave the verification that $R[x]$ is a ring as an exercise. □

Examples 3.3.

1. $\mathbb{Z}[x]$ is the ring of polynomials in the indeterminate x with integral coefficients.

2. $\mathbb{Q}[x]$ is the ring of polynomials in the indeterminate x with rational coefficients.

3. $\mathbb{Z}_2[x]$ is the ring of polynomials in the indeterminate x with coefficients in $\mathbb{Z}_2$. We have

$$(x+1)^2 = (x+1)(x+1) = x^2 + (1+1)x + 1 = x^2 + 1.$$

and

$$(x+1) + (x+1) = (1+1)x + (1+1) = 0.$$

.

Note 3.4. Let R be a ring and x and y are two indeterminates, then $R[x]$ is a ring. Now we can form the ring $(R[x])[y]$. That is the ring of polynomials in y with coefficients that are polynomials in x. Since every polynomial in y with coefficients that are polynomials in x can be rewritten as a polynomial in x with coefficients that are polynomials in y. So $(R[x])[y]$ is isomorphic to $(R[y])[x]$. These rings are isomorphic to $R[x, y]$, the ring of polynomials in two indeterminates x and y with coefficients in R. Similarly we can define the ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in the n indeterminates x_i with coefficients in R.

Question 3.5. *If D is an integral domain, then prove that $D[x]$ is an integral domain.*

Solution. Let D be an integral domain. Then D is a commutative ring with unity and hence $D[x]$ is a commutative ring with unity. We need to show that $D[x]$ has no zero divisors. Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ be two polynomials in $D[x]$ where $a_n \neq o$ and $b_m \neq 0$. Then the leading coefficients $f(x)g(x)$ is a_nb_m . Since D is an integral domain, we have $a_nb_m \neq 0$. So $f(x)g(x) \neq 0$. Thus $D[x]$ has no zero divisors and hence $D[x]$ is an integral domain. ■

Remark 3.6. If F is a field, then $F[x]$ is an integral domain. Here $F[x]$ is not a field for x is not a unit in $F[x]$. But we can construct the field of quotients $F(x)$ of $F[x]$. Any element in $F(x)$ can be represented as a quotient $f(x)/g(x)$ of two polynomials in $F[x]$ with $g(x) \neq 0$.

The Evaluation Homomorphisms

Here we show how homomorphism can be used to solve a polynomial equation.

Theorem 3.7. *Let F be a subfield of a field E, x be an indeterminate and α be any element of E. The map $\phi_\alpha : F[x] \to E$ defined by*

$$\phi_\alpha(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

for $a_0 + a_1x + \ldots + a_nx^n \in F[x]$ is a homomorphism from $F[x]$ into E. Also $\phi_\alpha(x) = \alpha$, and ϕ_α maps F isomorphically by the identity map; that is $\phi_\alpha(a) = a$ for $a \in F$. The homomorphism ϕ_α is evaluation at α.

Proof. The map ϕ_α is well defined. That is, ϕ_α is independent of our representation of $f(x)$ as finite sum. Let

$$f(x) = a_0 + a_1x + \ldots + a_nx^n,\ g(x) = b_0 + b_1x + \ldots + b_mx^m,$$

$h(x) = f(x)+g(x) = c_0+c_1x+\ldots+c_rx^r$ and $d(x) = f(x)g(x) = d_0+d_1x+\ldots+d_sx^s$.

Then by the definition of polynomial addition and multiplication, we have $c_i = a_i + b_i$ and $d_j = \sum_{i=0}^{j} a_ib_{j-i}$. Now

$$\begin{aligned}\phi_\alpha(f(x) + g(x)) &= \phi_\alpha(h(x)) \\ &= c_0 + c_1\alpha + \ldots c_r\alpha^r\end{aligned}$$

$$\begin{aligned}
&= (a_0 + b_0) + (a_1 + b_1)\alpha + \dots \\
&= (a_0 + a_1\alpha + \dots + a_n\alpha^n) + (b_0 + b_1\alpha + \dots + b_m\alpha^m) \\
&= \phi_\alpha(f(x)) + \phi_\alpha(g(x)).
\end{aligned}$$

and

$$\begin{aligned}
\phi_\alpha(f(x)g(x)) &= \phi_\alpha(d(x)) \\
&= d_0 + d_1\alpha + \dots d_s\alpha^s \\
&= (a_0b_0) + (a_1b_1)\alpha + \dots \\
&= (a_0 + a_1\alpha + \dots + a_n\alpha^n)(b_0 + b_1\alpha + \dots + b_m\alpha^m) \\
&= \phi_\alpha(f(x))\phi_\alpha(g(x)).
\end{aligned}$$

Thus ϕ_α is a homomorphism.
Let $a \in F$. Then $\phi_\alpha(a) = a$ and hence ϕ_α maps F isomorphically by the identity map. Also we have $\phi_\alpha(x) = \alpha$. □

Example 3.8. Consider the field $\mathbb{Q}$. Then $\mathbb{R}$ is an extension field of $\mathbb{Q}$. Consider the evaluation homomorphism $\phi_2 : \mathbb{Q}[x] \to \mathbb{R}$. Then

$$\phi_2(a_0 + a_1x + \dots + a_nx^n) = a_0 + a_12 + \dots + a_n2^n.$$

Note that $\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0$. That is, $x^2 + x - 6 \in Ker(\phi_2)$.

Consider the evaluation homomorphism $\phi_0 : \mathbb{Q}[x] \to \mathbb{R}$. Then

$$\phi_0(a_0 + a_1x + \dots + a_nx^n) = a_0 + a_10 + \dots + a_n0^n = a_0.$$

Here every polynomial is mapped onto its constant term.

Now consider the evaluation homomorphism $\phi_\pi : \mathbb{Q}[x] \to \mathbb{R}$. Here

$$\phi_\pi(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1\pi + \ldots + a_n\pi^n.$$

Now $a_0 + a_1\pi + \ldots + a_n\pi^n = 0$ if and only if $a_i = 0$ for $i = 0, 1, \ldots, n$. Thus the kernel of ϕ_π is $\{0\}$ and hence ϕ_π is one-to-one. Hence all formal polynomials in π with rational coefficients form a ring isomorphic to $\mathbb{Q}[x]$.

Definition 3.9. *Let F be a subfield of a field E and let α be an element of E. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be in $F[x]$ and $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism. Let $f(\alpha) = \phi_\alpha(f(x)) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$. If $f(\alpha) = 0$, then α is a zero of $f(x)$.*

EXERCISES

1. Find all zeros in the given field of the given polynomial with coefficients in that field.

   (a) $x^2 + x + 1 \in \mathbb{Z}_3[x]$.

   (b) $x^3 + x^2 + 3 \in \mathbb{Z}_5[x]$.

2. Find a polynomial of degree greater than 0 in $\mathbb{Z}_4[x]$ that is a unit.

3. Find the units in $\mathbb{Z}[x]$.

4. Find the units in $\mathbb{Z}_5[x]$.

5. Show that the polynomial $x^2 - 2$ has no zeros in rational numbers.

6. Find a polynomial of degree greater than zero in $\mathbb{Z}_4[x]$ that is a unit.

3.2 Factorization of Polynomials over a Field

In high school, we gave considerable emphasis to find the factors of polynomials with real coefficients and finding their zeros. Here we consider the same work for polynomials with coefficients from any field.

Let E and F are fields with $F \leq E$ and $f(x) \in F[x]$. Suppose that $f(x)$ factors in $F[x]$. Let $f(x) = g(x)h(x)$ for $g(x)$, $h(x) \in F[x]$ and $\alpha \in E$. We have

$$f(\alpha) = \phi_\alpha = \phi_\alpha(f(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

This implies that $f(\alpha) = 0$ if and only if either $g(\alpha) = 0$ or $h(\alpha) = 0$. So the problem of finding a zero of $f(x)$ can be reduced to the problem of finding a zero of a factor of $f(x)$. So it is very useful to study factorisation of polynomials.

Division Algorithm in $F[x]$

We had already studied the division algorithm for integers: If a and b are integers and $b \neq 0$, then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < |b|$. The following Theorem is the analogous statement for polynomials over a field.

Theorem 3.10. *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

and

$$g(x) = b_m + b_{m-1}x^{m-1} + \ldots + b_0$$

be two elements in $F[x]$, with a_n and b_m both non zero elements of F and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

where either $r(x) = 0$ *or the degree of* $r(x)$ *is less than the degree* m *of* $g(x)$.

Proof. Let

$$S = \{f(x) - g(x)s(x) : \ s(x) \in F[x]\}.$$

Case(i): $0 \in S$

If $0 \in S$, then there exists an $s(x)$ such that $f(x) - g(x)s(x) = 0$. That is, $f(x) = g(x)s(x)$. Take $q(x) = s(x)$ and $r(x) = 0$.

Case (ii): $0 \notin S$.

Let $r(x)$ be an element of minimal degree in S. Then $f(x) = g(x)q(x) + r(x)$ for some $q(x) \in F[x]$. Now we claim that the degree of $r(x)$ is less than m. Suppose that

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \ldots + c_0, \ c_j \in F \text{ and } c_t \neq 0.$$

If $t \geq m$, then

$$\begin{aligned} f(x) - g(x)[q(x) - (c_t/b_m)x^{t-m}] &= f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) \\ &= r(x) - (c_t/b_m)x^{t-m}g(x) \\ &= r(x) - (c_t x^t + \text{ terms of lower degree }). \end{aligned}$$

This implies that

$$f(x) - g(x)[q(x) - (c_t/b_m)x^{t-m}] \in S,$$

which is a polynomial of degree lower than t (degree of $r(x)$). This is a contradiction to the fact that $r(x)$ was selected to have minimal degree in S. Thus $t < m$. That is, the degree of $r(x)$ is less than the degree m of $g(x)$.

Uniqueness

Suppose that there exist $q_1(x)$, $q_2(x)$ and $r_1(x)$, $r_2(x)$ such that

$$f(x) = q_1(x)g(x) + r_1(x)$$

and

$$f(x) = q_2(x)g(x) + r_2(x).$$

This implies that

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x).$$

That is,

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Since either $r_2(x) - r_1(x) = 0$ or the degree of $r_1(x) - r_1(x)$ is less than the degree of $g(x)$, $q_1(x) - q_2(x) = 0$. Hence $q_1(x) = q_2(x)$. Then we must have $r_2(x) - r_1(x) = 0$ and hence $r_1(x) = r_2(x)$. □

Example 3.11. Let

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

and

$$g(x) = x^2 - 2x + 3$$

be two polynomials in $\mathbb{Z}_5[x]$.

Here we can easily find $q(x)$ and $r(x)$ using long division.The only point to remember that is the coefficients of the polynomials are belongs to $\mathbb{Z}_5$.

$$
\begin{array}{r|l}
 & +x^2 \quad -x \quad -3 \\
\hline
x^2-2x+3 & x^4 \quad -3x^3 \quad +2x^2 \quad +4x \quad -1 \\
\cline{2-2}
 & x^4 \quad -2x^3 \quad +3x^2 \\
\cline{2-4}
 & \quad -x^3 \quad -x^2 \quad +4x \\
 & \quad -x^3 \quad +2x^2 \quad -3x \\
\cline{2-4}
 & \quad\quad -3x^2 \quad +2x \quad -1 \\
 & \quad\quad -3x^2 \quad +x \quad -4 \\
\cline{2-5}
 & \quad\quad\quad\quad x \quad +3
\end{array}
$$

Thus we get

$$q(x) = x^2 - x - 3 \text{ and } r(x) = x + 3$$

We may now give several important corollaries of the division algorithm. We had studied these for the special case where F is the field of real numbers.

Corollary 3.12. *An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.*

Proof. Assume that a is a zero of $f(x)$. Then $f(a) = 0$. Since $f(x), (x - a) \in F[X]$, by division algorithm, there exist $q(x)$, $r(x) \in F[x]$ such that $f(x) = (x - a)q(x) + r(x)$ where either $r(x) = 0$ or the degree of $r(x) < 1$. Thus we must have $r(x) = c$ for $c \in F$. So $f(x) = (x - a)q(x) + c$. Since $f(a) = 0$, we get $0 = f(a) = 0q(a) + c$. this implies that $c = 0$. Then $f(x) = (x - a)q(x)$. So $(x - a)$ is a factor of $f(x)$.

Conversely, if $(x - a)$ is a factor of $f(x)$ in $F[X]$ where $a \in F$, then $f(x) = (x - a)q(x)$. So $f(a) = 0$ □

Example 3.13. Let us consider a polynomial $f(x) = x^4 + 3x^3 + 2x + 4$ in

$\mathbb{Z}_5[x]$. Here $f(1) = 1 + 3 + 2 + 4 = 0$. So $(x - 1)$ is a factor of $f(x)$.

$$
\begin{array}{r|llll}
 & x^3 & +4x^2 & +4x & +1 \\
\hline
x-1 & x^4 & +3x^3 & +4x & +4 \\
\cline{2-5}
 & x^4 & -x^3 & & \\
\cline{2-3}
 & & 4x^3 & & \\
 & & 4x^3 & -4x^2 & \\
\cline{3-4}
 & & & 4x^2 & +2x \\
 & & & 4x^2 & -4x \\
\cline{4-5}
 & & & & x \quad +4 \\
 & & & & x \quad -1 \\
\cline{5-5}
 & & & & 0
\end{array}
$$

Hence $f(x) = (x - 1)(x^3 + 4x^2 + 4x + 1)$ in $\mathbb{Z}_5[x]$. Again 1 is a zero of $x^3 + 4x^2 + 4x + 1$ and hence we can divide this polynomial by $(x - 1)$. We get

$$
\begin{array}{r|llll}
 & x^2 & +4 & & \\
\hline
x-1 & x^3 & +4x^2 & +4x & +1 \\
\cline{2-5}
 & x^3 & -x^2 & & \\
\cline{2-3}
 & & 0x^2 & +4x & +1 \\
 & & & 4x & -4 \\
\cline{4-5}
 & & & & 0
\end{array}
$$

Since 1 is a zero of x^2+4 in $\mathbb{Z}_5[x]$, we can again divide by $x-1$ and get

$$\begin{array}{r|l} & x \quad +1 \\ \hline x-1 & x^2 \quad +0x \quad +4 \\ \hline & x^2 \quad -x \\ \hline & \qquad x \quad +4 \\ & \qquad x \quad -1 \\ \hline & \qquad\qquad 0 \end{array}$$

Thus we get $f(x) = (x-1)^3(x+1)$ in $\mathbb{Z}_5[x]$.

Corollary 3.14. *A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.*

Proof. Let a_1 be a zero of $f(x)$. Then $f(x) = (x-a_1)q_1(x)$, where degree of $q_1(x)$ is $n-1$. Let a_2 be a zero of $q_1(x)$. Then $f(x) = (x-a_1)(x-a_2)q_2(x)$. Continuing this process, we get

$$f(x) = (x-a_1)(x-a_2)\dots(x-a_r)q_r(x)$$

where $q_r(x)$ has no further zeros in F. Since the degree of $f(x)$ is n, at most n factors $(x-a_i)$ can appear on the right hand side of the above equation. So $r \leq n$. Also if $b \neq a_i$, for $i = 1, 2, \dots r$ and $b \in F$,

$$f(b) = (b-a_1)(b-a_2)\dots(b-a_r)q_r(b) \neq 0.$$

Hence $a_1, a_2, \dots a_n$ are all zeros in F of $f(x)$. □

The above corollary is not true for arbitrary polynomial rings. Consider the polynomial x^2+3x+2 in $\mathbb{Z}_6[x]$. It has four zeros 1,2,4 and 5 in $\mathbb{Z}_6$.

Our next corollary is concerned with the structure of the multiplicative group F^* of non zero elements of a field F.

Corollary 3.15. *If G is a finite subgroup of the multiplicative group $\langle F^*, . \rangle$ of a field F, then G is cyclic. In particular multiplicative group of all nonzero elements of a finite field is cyclic.*

Proof. Given that G is a finite subgroup of the multiplicative group $\langle F^*, . \rangle$. So G is a finite abelian group. Then by fundamental theorem for finitely generated abelian groups, $G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_r}$ where each d_i is a power of prime. Let m be the least common multiple of all the d_i for $i = 1, 2, \ldots r$. Then $m \leq d_1 d_2 \ldots d_r$.Take $\mathbb{Z}_{d_i}$ as cyclic group of order d_i in the multiplicative notation. If $a_i \in \mathbb{Z}_{d_i}$, then $a_i^{d_i} = 1$ and hence $a_i^m = 1$. Thus for all $\alpha \in G$, $\alpha^m = 1$. So every element in G is a zero of the polynomial $x^m - 1$. But G has $d_1 d_2 \ldots d_r$ elements. So $m \geq d_1 d_2 \ldots d_r$. Hence $m = d_1 d_2 \ldots d_r$. This implies that the primes involved in the prime powers $d_1, d_2, \ldots, d_r$ are distinct and the group $G \simeq \mathbb{Z}_m$. Thus G is cyclic. □

Irreducible Polynomials

Definition 3.16. *A non constant polynomial $f(x) \in F[x]$ is irreducible over F or is an irreducible polynomial in $F[x]$ if $f(x)$ can not be expressed as a product $f_1(x)f_2(x)$ of two polynomials $f_1(x)$ and $f_2(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$.*

For example, the polynomial $f(x) = 2x^2 + 4$ irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$. A polynomial may be irreducible over F, but may not be irreducible over a larger field E containing F.
For example the polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$. But $x^2 + 1 = (x + i)(x - i_)$ in $\mathbb{C}[x]$. So $x^2 + 1$ is reducible over $\mathbb{C}$.

Remark 3.17. Recall that the units in $F[x]$ are precisely the nonzero elements of F. So an irreducible polynomial $f(x) \in F[x]$ is a non constant polynomial such that in any factorisation $f(x) = f_1(x)f_2(x)$ in $F[x]$, either $f_1(x)$ is a unit or $f_1(x)$ is a unit.

It is difficult to decide whether or not a polynomial is reducible over $\mathbb{F}$. But there are some special cases.

The following Theorem shows that the question of irreducibility of a polynomial of degree 2 or 3 to one of finding a zero.

Theorem 3.18. *Let $f(x) \in F[x]$ and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.*

Proof. Assume that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ where the degree of $g(x)$ and the degree $h(x)$ are both less than the degree of $f(x)$. Since $f(x)$ is either quadratic or cubic, either $g(x)$ or $h(x)$ is of degree 1. If $g(x)$ is of degree 1, then except for a possible factor in F, $g(x)$ is of the form $(x - a)$. Then $g(a) = 0$ and hence $f(a) = 0$. So $f(x)$ has a zero in F.

Suppose $f(x)$ has a zero a in F. So $f(a) = 0$. Then $x - a$ is a factor of $f(x)$. So $f(x)$ is reducible. □

Example 3.19. Let $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$. Suppose that $f(x)$ is reducible. Since the degree of $f(x) = 3$, $f(x)$ has a linear factor $(x - a)$. Then $f(a) = 0$. Here $f(0) = 2$, $f(1) = 1$, $f(2) = 1$, $f(3) = f(-2) = -2$ and $f(4) = f(-1) = -2$. So $f(x)$ has no zeros in $\mathbb{Z}_5$. Thus $f(x)$ is irreducible over $\mathbb{Z}_5$.

Now we consider irreducibility of polynomials with integer coefficients.

Theorem 3.20. *If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorisation with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.*

Proof. The proof is omitted here. □

Corollary 3.21. *If $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$ and if $f(x)$ has in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and m must divide a_0.*

Proof. If $f(x)$ has a zero a in $\mathbb{Q}$, then $f(x)$ has a linear factor $x - a$ in $\mathbb{Q}[x]$ by factor Theorem. Then by Theorem 3.20, $f(x)$ has a factorisation with a linear factor in $\mathbb{Z}[x]$. So for some $m \in \mathbb{Z}$, we must have $f(x) = (x - m)(x^{n-1} + \ldots - a_0/m)$. Thus a_0/m is in $\mathbb{Z}$, so m divides a_0. □

Example 3.22. Consider the polynomial $x^2 - 2 \in \mathbb{Q}[x]$. Then $x^2 - 2$ factors in $\mathbb{Q}[x]$ if and only if it has a zero in $\mathbb{Q}$. But it has a zero in $\mathbb{Q}$ if and only if it has a zero m in $\mathbb{Z}$. Then m divides 2. So the only possibilities are ± 1 and ± 2 of 2. But none of these are zeros of $x^2 - 2$. So $x^2 - 2$ is irreducible.

Here we prove an important irreducibility test for polynomials in $\mathbb{Z}[x]$.

Theorem 3.23. ***Eisenstein Criterion***
Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i \equiv 0 \pmod{p}$ for $i < n$. with $a_0 \not\equiv 0 \pmod{p}^2$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. We have to show that $f(x)$ is irreducible over $\mathbb{Q}$. Now by Theorem 3.20, we need only show that $f(x)$ is irreducible over $\mathbb{Z}$. Suppose not,

$$f(x) = (b_r x_r + \ldots + b_0)(c_s x^s + \ldots + c_0)$$

is a factorization of $f(x)$ in $\mathbb{Z}[x]$, with $r, s < n$, $b_r \neq 0$ and $c_s \neq 0$. Given that $a_0 \not\equiv 0 \pmod{p}^2$. So b_0 and c_0 are not both congruent to 0 modulo p. Suppose that $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \equiv 0 \pmod{p}$. Now $a_n \not\equiv 0 \pmod{p}$ and

$a_n = b_r c_s$ implies that $b_r, c_s \not\equiv 0 \pmod{p}$. Let m be the smallest value of k such that $c_k \not\equiv 0 \pmod{p}$. Then

$$a_m = b_0 c_m + b_1 c_{m-1} + \ldots + \begin{cases} b_m c_0 & \text{if } r \geq m \\ b_r c_{m-r} & \text{if } r < m \end{cases}$$

Then $a_m \not\equiv 0 \pmod{p}$. For, $b_0 \not\equiv 0 \pmod{p}$ and $c_m \not\equiv 0 \pmod{p}$ while $c_{m-1}, \ldots, c_0$ are all congruent to 0 modulo p. So $m = n$. It follows that $s = n$. This is a contradiction. Hence the theorem. □

Example 3.24. The polynomial $4x^5 + 15x^4 + 20x^3 + 10x + 30$ is irreducible over $\mathbb{Q}$ because 5 does not divides 4 and 25 not divides 20 but 5 does divide 15, 20, 10 and 30.

Corollary 3.25. *The polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$.

Proof. Here $\Phi_p(x) \in \mathbb{Z}[x]$. So need only consider factorizations in $\mathbb{Z}[x]$. Let

$$g(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \ldots + px}{x}$$

Then

$$g(x) = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + p$$

Then $g(x)$ satisfies the Eisenstein condition for the prime p and is thus irreducible over $\mathbb{Q}$. Suppose $\Phi_p(x)$ is not irreducible, then $\Phi_p(x)$ has a non-trivial factorisation of $\Phi_p(x) = h(x)i(x)$ in $\mathbb{Z}[x]$. So $\Phi_p(x+1) = g(x) =$

$h(x+1)i(x+1)$ is a nontrivial of $g(x)$ in $\mathbb{Z}[x]$. This is not possible. Hence $\Phi_p(x)$ must be irreducible. □

Uniqueness of Factorization in $F[x]$

Polynomials in $F[x]$ can be factored into a product of irreducible polynomials in $F[x]$. For $f(x)$, $g(x) \in F(x)$, we say that $g(x)$ divides $f(x)$ in $F[x]$ if there exists $q(x) \in F[x]$ such that $f(x) = g(x)q(x)$.

Theorem 3.26. *Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x)$, $s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.*

Proof. Proof is omitted. □

Corollary 3.27. *Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides the product $r_1(x)r_2(x)\dots r_n(x)$ for $r_i(x) \in F[x]$, then $p(x)$ divides $r_i(x)$ for at least one i.*

Proof. Using Theorem 3.26 and mathematical induction, one can easily prove the result. □

Theorem 3.28. *If F is a field, then every non constant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit factors in F.*

Proof. Let $f(x)$ be a nonconstant polynomial. Let $f(x)$ be reducible. Then $f(x) = g(x)h(x)$ where the degree of $g(x) <$ degree of $f(x)$ and degree of $h(x) <$ degree of $f(x)$. If $g(x)$ and $h(x)$ are both irreducible, then there is nothing to prove. If not, at least one of them factors into polynomials

of lower degree. Continuing this process, we get a factorisation $f(x) = p_1(x)p_2(x)\dots p_r(x)$ where $p_i(x)$ is irreducible for $i = 1, 2, \dots, r$.

Next we prove the uniqueness of factorisation. Suppose that

$$f(x) = p_1(x)p_2(x)\dots p_r(x) = q_1(x)q_2(x)\dots q_s(x)$$

are two factorizations of $f(x)$ into irreducible polynomials. Then by Corollary 3.27, $p_1(x)$ divides some $q_j(x)$. Let $p_1(x)$ divides $q_1(x)$. Since $q_1(x)$ is irreducible, $q_1(x) = u_1p_1(x)$ where u_1 is a non zero unit in F. Then by substituting $q_1(x) = u_1p_1(x)$, we get

$$p_2(x)\dots p_r(x) = u_1q_2(x)\dots q_s(x).$$

By similar arguments, we have $p_2(x) = u_2q_2(x)$ and hence

$$p_3(x)p_4(x)\dots p_r(x) = u_1u_2q_3(x)q_4(x)\dots q_s(x).$$

Continuing like this, we get

$$1 = u_1u_1\dots q_{r+1}(x)\dots q_s(x).$$

This implies that $s = r$ and $1 = u_1u_2\dots u_r$. Hence the irreducible factors $p_i(x)$ and $q_j(x)$ were the same except possibly for order and unit factors. □

Question 3.29. *Let p be a prime. Show that the polynomial $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.*

Solution. First consider the case $p = 2$. We have $x^2 = xx$ and $x^2 + 1 = (x + 1)(x + 1)$ are reducible in $\mathbb{Z}p$.

Let $p \neq 2$ and $a \in \mathbb{Z}_p$. We have $(-a)^p + a = -a + a = 0$. That is, $-a$ is

a zero of $x^p + a$. Hence the polynomial $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$. ■

EXERCISES

1. Show that the polynomial $x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.
2. Factorise the polynomial $x^4 + 4$ in $\mathbb{Z}_5[x]$.
3. Determine whether the following polynomials are irreducible.
   (a) $x^2 - 12$
   (b) $8x^3 + 6x^2 - 9x + 24$
   (c) $4x^9 - 9x^3 + 24x - 18$
4. Find all irreducible polynomials of degree 2 in $\mathbb{Z}_2[x]$.

3.3 Noncommutative Examples

A noncommutative ring is a ring R whose multiplication is not commutative; that is, there exists a and b in R with $ab \neq ba$.

Let $M_n(F)$ be the set of all $n \times n$ matrices with entries in a field F. We can easily verify that $M_n(F)$ is a non commutative ring.

Rings of Endomorphisms

Let A be an abelian group. A homomorphism of A into itself is an endomorphism of A.

Let the set of all endomorphisms of A be $End(A)$. Now we define two operations addition and multiplication on $End(A)$ as follows and prove that $End(A)$ is a ring under these operations.

Let ϕ and ψ be two elements in $End(A)$. Then define $\phi + \psi : R \to R$ and $\phi\psi : R \to R$ as $(\phi + \psi)(a) = \phi(a) + \psi(a)$ and $\phi\psi(a) = \phi(\psi(a))$. Then

$$\begin{aligned}(\phi + \psi)(a + b) &= \phi(a + b) + \psi(a + b) \\ &= [\phi(a) + \phi(b)] + [\psi(a) + \psi(b)] \\ &= [\phi(a) + \psi(a)] + [\phi(b) + \psi(b)] \\ &= (\phi + \psi)(a) + (\phi + \psi)(b).\end{aligned}$$

So $\phi + \psi$ is a homomorphism and hence belongs to $End(A)$.

Since A is abelian, we have

$$(\phi + \psi)(a) = \phi(a) + \psi(a) = \psi(a) + \phi(a) = (\psi + \phi)(a)$$

for all $a \in A$. Thus $\phi + \psi = \psi + \phi$. That is, addition in $End(A)$ is commutative.

Next we prove the associativity property of addition.

$$\begin{aligned}[\phi + (\psi + \theta)](a) =& \phi(a) + [(\psi + \theta)(a)] \\ =& \phi(a) + [\psi(a) + \theta(a)] \\ =& [\phi(a) + \psi(a)] + \theta(a) \\ =& (\phi + \psi)(a) + \theta(a) \\ =& [(\phi + \psi) + \theta](a)\end{aligned}$$

Let e be the additive identity of A and $0 : R \to R$ be the homomorphism defined by $0(a) = e$ for $a \in A$. Then $(\phi + 0)(a) = \phi(a) + e = e + \phi(a) = (0+\phi)(a)$ for all $a \in A$. That is, the homomorphism 0 is the additive identity in $End(A)$. For $\phi \in End(A)$, $-\phi$ defined by $(-\phi)(a) = -\phi(a)$ is in $End(A)$. For,

$$(-\phi)(a + b) = -\phi(a + b)$$

$$\begin{aligned}
&= -[\phi(a) + \phi(b)] \\
&= -\phi(a) - \phi(b) \\
&= (-\phi(a)) + (-\phi(b)) \\
&= (-\phi)(a) + (-\phi)(b)
\end{aligned}$$

Also note that $(\phi+(-\phi))(a) = \phi(a)+(-\phi)(a) = e = 0(a) = (-\phi)(a)+\phi(a) = ((-\phi) + \phi)(a)$ for all $a \in A$. So $\phi + (-\phi) = 0$. Hence $\langle End(A), + \rangle$ is an abelian group.

Note that function composition is an associative operation.

Let ϕ, ψ and θ be in $End(A)$ and $a \in A$. Then

$$\begin{aligned}
(\theta(\phi + \psi))(a) &= \theta((\phi + \psi)(a)) \\
&= \theta(\phi(a) + \psi(a)) \\
&= \theta(\phi(a)) + \theta(\psi(a)) \quad \text{Since } \theta \in End(A) \\
&= (\theta\phi)(a) + (\theta\psi)(a) \\
&= (\theta\phi + \theta\psi)(a)
\end{aligned}$$

Thus we have $\theta(\phi + \psi) = \theta\phi + \theta\psi$. Now

$$\begin{aligned}
((\phi + \psi)\theta)(a) &= (\phi + \psi)(\theta(a)) \\
&= \phi(\theta(a)) + \psi(\theta(a)) \\
&= (\phi\theta)(a) + (\psi\theta)(a) \\
&= (\phi\theta + \psi\theta)(a).
\end{aligned}$$

Hence the left distributive and right distributive laws hold. Thus we have proved the following Theorem.

Theorem 3.30. *The set $End(A)$of all endomorphisms of an abelian group A forms a ring under homomorphism addition and homomorphism multiplication(function composition).*

Remark 3.31. The set A^A of all functions from A into A is an abelian group under the same addition and multiplication(function composition) defined above. Moreover $\langle A^A, +, . \rangle$ satisfies all the axioms of a ring except the left distributive law.

Note that in general the function composition need not be commutative and hence the ring of endomorphisms need not be commutative. See the following example.

Example 3.32. Consider the abelian group $\langle \mathbb{Z} \times \mathbb{Z}, + \rangle$ which we have discussed earlier. Define ϕ, $\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by

$$\phi((m,n)) = (m+n, 0) \quad \text{and} \quad \psi((m,n)) = (0,n).$$

First we show that ϕ and ψ are elements in $End(\langle \mathbb{Z} \times \mathbb{Z}, + \rangle)$.

Let (m_1, n_1), $(m_2, n_2) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$\begin{aligned} \phi((m_1,n_1) + (m_2,n_2)) &= \phi((m_1+m_2, n_1+n_2)) \\ &= (m_1+m_2+n_1+n_2, 0) \\ &= (m_1+n_1, 0) + (m_2+n_2, 0) \\ &= \phi((m_1,n_1)) + \phi((m_2,n_2)) \end{aligned}$$

Thus ϕ is a homomorphism on $\mathbb{Z} \times \mathbb{Z}$. Simillarly we can easily verify that ψ is also a homomorphism on $\mathbb{Z} \times \mathbb{Z}$. Here

$$(\psi\phi)(m,n) = \psi(m+n, 0) = (0,0)$$

and

$$(\phi\psi)(m,n) = \phi(0,n) = (n,0).$$

So $\phi\psi \neq \psi\phi$. It follows that $End(\langle \mathbb{Z} \times \mathbb{Z}, + \rangle)$ is not a commutative ring.

Group Rings and Group Algebras

Here we discuss another example for a non commutative ring.

Let $G = \{g_i : i \in I\}$ be any group written multiplicatively and R be any commutative ring with non zero unity. Let

$$RG = \{\sum_{i \in I} a_i g_i : g_i \in G \text{ and } a_i \in R, \text{ all but a finite number of the } a_i \text{ are } 0\}.$$

Here we show that $\langle RG, +, . \rangle$ is a ring. This is our next Theorem.

Theorem 3.33. *If G is any group written multiplicatively and R is a commutative ring with nonzero unity, then $\langle RG, +, . \rangle$ is a ring.*

Proof. Using the addition in R, we define addition in RG and under this addition, RG is a group. Define the sum of two elements of RG by

$$\Big(\sum_{i \in I} a_i g_i\Big) + \Big(\sum_{i \in I} b_i g_i\Big) = \sum_{i \in I} (a_i + b_i) g_i.$$

Since a_i and b_i are zero except for finite number of indices i, $(a_i + b_i) = 0$ except for a finite number of indices i and hence $\sum_{i \in I} (a_i + b_i) g_i \in RG$. So RG is closed under addition. It is easy to show that $\langle RG, + \rangle$ is an abelian group with additive identity

$$\sum_{i \in I} 0 g_i$$

.

Define the product of two elements of RG by

$$\Big(\sum_{i \in I} a_i g_i\Big)\Big(\sum_{i \in I} b_i g_i\Big) = \sum_{i \in I} \Big(\sum_{g_i g_k = g_i} a_j b_k\Big) g_i.$$

Since G is a group under multiplication and a_i and b_i are 0 for all but a finite number of i, the sum $\sum_{g_ig_k=g_i} a_jb_k$ contains only a finite number of non zero summands $a_jb_k \in R$ and hence an element of R. Again, at most a finite number of such sums $\sum_{g_ig_k=g_i} a_jb_k$ are nonzero. It follows that RG is closed under multiplication.

Next we prove the associativity of multiplication in RG.

$$\begin{aligned}\Big(\sum_{i\in I} a_ig_i\Big)\Big[\Big(\sum_{i\in I} b_ig_i\Big)\Big(\sum_{i\in I} c_ig_i\Big)\Big] &= \Big(\sum_{i\in I} a_ig_i\Big)\Big[\sum_{i\in I}\Big(\sum_{g_jg_k=g_i} b_jc_k\Big)g_i\Big] \\ &= \sum_{i\in I}\Big(\sum_{g_hg_jg_k=g_i} a_hb_jc_k\Big)g_i \\ &= \Big[\sum_{i\in I}\Big(\sum_{g_hg_j=g_i} a_hb_j\Big)g_i\Big]\Big(\sum_{i\in I} c_ig_i\Big) \\ &= \Big[\Big(\sum_{i\in I} a_ig_i\Big)\Big(\sum_{i\in I} b_ig_i\Big)\Big]\Big(\sum_{i\in I} c_ig_i\Big)\end{aligned}$$

It is easy to prove the distributive laws from the definition of addition and the formal way we used distributivity to define multiplication. □

Remark 3.34. Let $g \in G$. Then $1g \in RG$. We can identify $1g$ with g and hence RG can be considered to contain G. So if G is non abelian, RG is not a commutative ring.

Definition 3.35. *The ring RG is called the group ring of G over R. If F is a field, then FG is the group algebra of G over F.*

Example 3.36. Let $R = \mathbb{Z}_2$ and $G = \{e, a\}$ be the cyclic group of order 2. Then

$$\mathbb{Z}_2G = \{0e + 0a,\ 0e + 1a,\ 1e + 0a,\ 1e + 1a\} = \{0,\ a,\ e,\ e + a\}.$$

The addition and multiplication tables for $\mathbb{Z}_2G$ is as follows.

$+$	0	a	e	$e+a$
0	0	a	e	$e+a$
a	a	0	$e+a$	e
e	e	$e+a$	0	a
$e+a$	$e+a$	e	a	0

	0	a	e	$e+a$
0	0	0	0	0
a	0	e	a	$e+a$
e	0	a	e	$e+a$
$e+a$	0	$e+a$	$e+a$	0

Note that group algebra may have 0 divisors. For,

$$(e+a)(e+a) = (1e+1a)(1e+1a) = (1+1)e + (1+1)a = 0e + 0a$$

The Quaternions

Recall that a non commutative division ring is called a strictly skew field. Here we give an example of a strictly skew field.

Let $\mathbb{H}$ be $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. We know that $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ is a group under addition by components. This gives the operation of addition on $\mathbb{H}$.

Theorem 3.37. *The quaterions $\mathbb{H}$ form a strictly skew field under addition and multiplication.*

Proof. The addition in $\mathbb{H}$ is the component wise addition.

Let $1 = (1,0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$ and $k = (0,0,0,1)$. Then 1, i, j and k be elements of $\mathbb{H}$.

Let $a_1 = (a_1,0,0,0)$, $a_2 i = (0,a_2,0,0)$, $a_3 j = (0,0,a_3,0)$ and $a_4 k = (0,0,0,a_4)$. Then $(a_1,a_2,a_3,a_4) = a_1 + a_2 i + a_3 j + a_4 k$.
Thus $(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$.

In order to define multiplication on $\mathbb{H}$, we start by defining

$$1a = a1 = a \text{ for } a \in \mathbb{H}, \quad i^2 = j^2 = k^2 = -1,$$

and

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad \text{and } ik = -j.$$

Now

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k)&(b_1 + b_2 i + b_3 j + b_4 k)\\ &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)i\\ &\quad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)j + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)k.\end{aligned}$$

Note that we defined multiplication in such a manner the distributive laws hold. Here the multiplication is not commutative (for example, $ij = k$ and $ji = -k$). So $\mathbb{H}$ is not a field.

Next we show that every non zero element has a multiplicative inverse. Let $a = a_1 e + a_2 i + a_3 j + a_4 k$ with not all $a_{=}0$. We have

$$(a_1 + a_2 i + a_3 j + a_4 k)(a_1 - a_2 i - a_3 j - a_4 k) = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Let $|a|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $\overline{a} = a_1 - a_2 i - a_3 j - a_4 k$. Now

$$a(\frac{\overline{a}}{|a|^2}) = (a_1 + a_2 i + a_3 j + a_4 k)(\frac{a_1}{|a|^2} - \frac{a_2}{|a|^2} j - \frac{a_3}{|a|^2} j - \frac{a_4}{|a|^2} k) = 1.$$

Hence $\frac{a_1}{|a|^2} - \frac{a_2}{|a|^2} j - \frac{a_3}{|a|^2} j - \frac{a_4}{|a|^2} k$ is the multiplicative inverse of a. Since a is arbitrary, every non zero element in $\mathbb{H}$ has a multiplicative inverse. So the quaterions $\mathbb{H}$ form a strictly skew field □

Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Then G is a group of order 8 under quaternion multiplication. Clearly G is generated by i and j where

$$i^4 = 1, \qquad j^2 = i^2 \qquad \text{and} \qquad ji = i^3 j.$$

Theorem 3.38. *Every finite division ring is a field.*

Proof. Proof is omitted. □

Hence there are no finite strictly skew fields.

3.4 Homomorphisms and Factor Rings

We know that the group homomorphism preserves the group operation. Similarly a ring homomorphism preserves the ring operations. That means a homomorphism for rings must relate both their additive structure and their multiplicative structure.

Definition 3.39. *A ring homomorphism ϕ from a ring R to a ring R' is a mapping from R to R' that preserves the two ring operations. That is, for all $a, b \in R$,*

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

The roles of isomorphisms and homomorphisms are entirely distinct. An isomorphism is used to show that two rings are algebraically identical, but a homomorphism is used to simplify a ring while retaining certain of its features.

Examples 3.40.

- For any positive integer n, the mapping ϕ which maps $m \to m \pmod{n}$ is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$. That is, $\phi(m)$ is the reminder of m when divided by n.

- The mapping $a + ib \to a - ib$ is a ring isomorphism from the complex numbers onto itself.

Properties of Ring Homomorphisms

Here we study some structure features of R and R' that are preserved by a homomorphism $\phi : R \to R'$.

Theorem 3.41. *Let ϕ be a ring homomorphism from a ring R into a ring R'. Then*

- *If 0 is the additive identity in R, then $\phi(0) = 0'$ is the additive identity in R'.*

- *If $a \in R$, then $\phi(-a) = -\phi(a)$.*

- *If S is a subring of R, then $\phi[S]$ is a subring of R'.*

- *If S' is a subring R', then $\phi^{-1}[S']$ is a subring of R.*

- *If R has unity 1, then $\phi(1)$ is unity for $\phi[R]$.(Subrings correspond to subrings and rings with unity correspond to rings with unity under a ring homorphism.)*

Proof. Let ϕ be a homomorphism of a ring R into R'. In particular ϕ can be viewed as a group homoorphism of $(R, +)$ into $(R', +')$. Then $\phi(0) = 0'$ is the identity element of R' and $\phi(-a) = -\phi(a)$.

Let S be a subring of R. Then S is a ring with respect to the operation on R. Now consider the addictive group $\langle S, +\rangle$. Then the set $\langle \phi[S], +']$ gives a subgroup of R'.

Let $a, b \in S$. Then $\phi(a)$, $\phi(b) \in \phi[S]$ and $\phi(a)\phi(b) = \phi(ab)$. Since $\phi(ab) \in \phi[S]$, $\phi(a)\phi(b) \in \phi[S]$. So $\phi[S]$ is closed under multiplication. Hence $\phi[S]$ is a subring of R'.

Let S' be a subring R'. Then $\langle \phi^{-1}[S'], +\rangle$ is a subgroup of $\langle R, +\rangle$. Let $a, b \in \phi^{-1}[S']$. Then $\phi(a)$, $\phi(b) \in S'$. Since S' is a ring, $\phi(a)\phi(b) \in S'$. But $\phi(a)\phi(b) = \phi(ab)$. This implies that $ab \in \phi^{-1}[S']$ and hence $\phi^{-1}[S']$ is closed under multiplication. Thus $\phi^{-1}[S']$ is a subring of R.

Suppose that R has unity 1. Then for all $r \in R$,

$$\phi(r) = \phi(1r) = \phi(r1) = \phi(1)\phi(r) = \phi(r)\phi(1).$$

So $\phi(1)$ is a unity for $\phi[R]$. □

Remark 3.42. *Note that if R has unity 1, then $\phi(1)$ is unity for $\phi[R]$ but not necessarily for R'. If R has unity 1, $S \neq \{0\}$ and ϕ is onto, then $\phi(1)$ is the unity of R'.*

Question 3.43. *Give an example of a ring homomorphism $\phi : R \to R'$ where R has unity 1 and $\phi(1) \neq 0'$, but $\phi(1)$ is not unity for R'.*

Solution. Let $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $\phi(a) = (a, 0)$. Then *phi* is a homomorphism. Then $\mathbb{Z}$ has unity 1. Now $\phi(1) = (1, 0)$ is not the unity. The unity in $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$. ■

Question 3.44. *Show that the feild $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.*

Solution. An isomorphism $\phi : \mathbb{R} \to \mathbb{C}$ maps the unity 1 if $\mathbb{R}$ into the multiplicative identity 1 of $\mathbb{C}$. Consequently it must map the additive inverse -1 of 1 in $\mathbb{R}$ into -1 in $\mathbb{C}$. Nore that -1 is not a square of any real number. But $-1 = i^2$ in $\mathbb{C}$. So these two fields are not isomorphic. ■

Next we define kernel of a homomorphism.

Definition 3.45. *Let a map $\phi : R \to R$ be a homomorphism of rings. The subring $\phi^{-1}[0'] = \{r \in R : \phi(r) = 0'\}$ is the kernel of ϕ, denoted by $Ker(\phi)$.*

Note that the kernel of the ring homomorphism ϕ is the kernel of the group homomorphism of $\langle R, + \rangle$ into $\langle R', + \rangle$ given by ϕ.

Theorem 3.46. *Let $\phi : R \to R'$ be a ring homomorphism and let $H = Ker(\phi)$. Let $a \in R$. Then $\phi^{-1}[\phi(a)] = a + H = H + a$, where $a + H = H + a$ is the coset containing a of the commutative additive group $\langle H, + \rangle$*

Proof. We have to show that

$$\{x \in R : \phi(x) = \phi(a)\} = H + a.$$

Let $y \in \{x \in R : \phi(x) = \phi(a)\}$. Then $\phi(y) = \phi(a)$. Then $\phi(y) + (-\phi(a)) = 0'$. We have $\phi(-a) = -\phi(a)$. So we have $\phi(y) + \phi(-a) = 0'$. Since ϕ is a homomorphism, We have $\phi(y) + \phi(-a) = \phi(y - a)$, so $\phi(y - a) = 0'$. This implies that $y - a \in H$. So $y - a = h$ for some $h \in H$, and $y = h + a \in H + a$. This shows that

$$\{x \in R : \phi(x) = \phi(a)\} \subseteq H + a.$$

Let $y \in H + a$. Then $y = h + a$ for some $h \in H$. Then

$$\phi(y) = \phi(h + a) = \phi(h) + \phi(a) = 0' + \phi(a) = \phi(a).$$

So $y \in \{x \in R : \phi(x) = \phi(a)\}$.
Simillarly we can easily prove $\{x \in R : \phi(x) = \phi(a)\} = a + H$. Hence the proof. □

Corollary 3.47. *A ring homomorphism $\phi : R \to R'$ is a one-to-one map if and only if $Ker(\phi) = \{0\}$.*

Proof. Suppose that $\phi : R \to R'$ is a one-to-one map. We have $\phi(0) = 0'$. Since ϕ is one to one, 0 is the only element mapped into $0'$ by ϕ. This implies that $Ker(\phi) = \{0\}$.

Suppose that $Ker(\phi) = \{0\}$. Then by previous theorem, $\phi^{-1}(\phi(a) = a + \{0\} = \{a\}$. So ϕ is one to one. □

Factor Rings

In section 1.3, we showed that if N is a normal subgroup of a group G, then we can create the factor groups G/N. Here we discuss an analogy in ring theory.

Theorem 3.48. *Let $\phi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by*

$$(a + H) + (b + H) = (a + b) + H$$

and the product of the cosets is defined by

$$(a + H)(b + H) = (ab) + H.$$

Also, the map $\mu : R/H \to \phi[R]$ *defined by* $\mu(a + H) = \phi(a)$ *is an isomorphism.*

Proof. The additive part of the theory is done in Theorem 1.22. So we check the multiplicative aspects.

Here we show that multiplication of cosets by choosing representatives is well defined. Let h_1, $h_2 \in H$ and consider the representatives $a+h_1$ of $a+H$ and $b+h_2$ of $b+H$. Let

$$c = (a + h_1)(b + h_2) = ab + ah_2 + h_1b + h_1h_2.$$

We show that $c \in ab+H$. We have $ab+H = \phi^{-1}[\phi(ab)]$, it is enough to show that $\phi(c) = \phi(ab)$. Since ϕ is a homomorphism and $\phi(h) = 0'$ for $h \in H$, we obtain

$$\begin{aligned}
\phi(c) &= \phi(ab + ah_2 + h_1b + h_1h_2) \\
&= \phi(ab) + \phi(ah_2) + \phi(h_1b) + \phi(h_1h_2) \\
&= \phi(ab) + \phi(a))0' + 0'\phi(b) + 0'0' \\
&= \phi(ab) + 0' + 0' + 0' \\
&= \phi(ab)
\end{aligned}$$

Thus the multiplication by choosing representatives is well defined.

To show that R/H is a ring, it remains to show that the associative property for multiplication and the distributive laws hold in R/H. Since

addition and multiplication are computed by choosing representatives, these properties follows from corresponding properties in $\mathbb{R}$.

In Theorem 1.22, we proved that the map μ is well defined, one-one and onto $\phi[R]$ and satisfies additive property for homomorphism. We have

$$\mu[(a+H)(b+H)] = \mu(ab+H) = \phi(ab) = \phi(a)\phi(b) = \mu(a+H)\mu(b+H).$$

Hence μ is an isomomorphism. □

Now we characterize those subrings H of a ring R such that the multiplication of additive cosets of H by choosing representatives is well defined.

Theorem 3.49. *Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equation*

$$(a+H)(b+H) = ab+H$$

if and only if $ah \in H$ and $hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof. First assume that $ah \in H$ and $hb \in H$ for all $a, b \in R$ and $h \in H$. Let h_1, $h_2 \in H$. Then $a+h_1$ and $b+h_2$ are two representatives of the cosets $a+H$ and $b+H$ containing a and b. Then

$$(a+h_1)(b+h_2) = ab + ah_2 + h_1b + h_1h_2$$

Since by our assumption, ah_2, h_1b and h_1h_2 are all in H. Hence $(a+h_1)(b+h_2) \in ab+H$.

Conversely suppose that multiplication of additive cosets of H is well defined by the equation

$$(a+H)(b+H) = ab+H.$$

Let $a \in R$. Consider the coset product $(a+H)H$. We compute this product in two ways by choosing two representatives. First we choose representatives $a \in (a+H)$ and $0 \in H$. Then we get $(a+H)H = a0 + H = 0 + H = H$. Choose $a \in a+H$ and $h \in H$, compute $(a+H)H$. We see that $ah \in H$ for any $h \in H$. Similarly by computing the product $H(b+H)$ in two ways, we get $hb \in H$ for any $h \in H$. □

We already studied that normal subgroups play an important role in group theory and using normal subgroups we can construct factor groups. Here we introduce analogous concepts for rings-ideals and factor rings. So the analogous substructure must be a subring H of a ring R such that $aH \subseteq H$ and $Hb \subseteq H$ for all $a, b \in R$.

Definition 3.50. *An additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a, b \in R$ is called an ideal.*

From the definition of an ideal, it follows that a nonempty subset N of a subring R is an ideal of R if it satisfies two conditions.
1. $m - n \in N$ whenever $m, n \in N$.
2. rn and nr are in N whenever $n \in N$ and $r \in R$.

Examples 3.51.
1. *For any positive integer n, the set $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$.*
2. *Let $R[x]$ denote the set of all polynomials with real coefficients and N be the set of all polynomials with constant term 0. Then N is an ideal in $R[x]$.*

Corollary 3.52. *Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with binary operations defined by*

$$(a+N) + (b+N) = (a+b) + N \text{ and } (a+N)(b+N) = ab + N.$$

The ring R/N in corollary 3.52 is the factor ring or quotient ring of R by N.

Fundamental Homomorphism Theorem

Analogous to Fundamental Homomorphism Theorem in group theory, here we give Fundamental Homomorphism Theorem for rings.

Theorem 3.53. *Let N be an ideal of a ring R. Then $\gamma : R \to R/N$ gives by $\gamma(x) = x + N$ is a ring homomorphism with kernel N.*

Proof. Let x, $y \in R/N$. Then

$$\gamma(x + y) = (x + y) + N = (x + N) + (y + N) = \gamma(x) + \gamma(y)$$

and

$$\gamma(xy) = (xy) + N = (x + N)(y + N) = \gamma(x)\gamma(y).$$

So γ is a homomorphism. □

Theorem 3.54. *Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then $\phi[R]$ is a ring and the map $\mu : R/N \to \phi[R]$ given by $\mu(x + N) = \phi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$,we have $\phi(x) = \mu\gamma(x)$*

Example 3.55. *We know that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. So we can form the factor ring $\mathbb{Z}/n\mathbb{Z}$. Recall that $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(m)$ is the reminder of m modulo n is a homomorphism and Ker(ϕ)=$n\mathbb{Z}$. Then by Theorem 3.54, the map $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ where $\mu(m+n\mathbb{Z})$ is the reminder of m modulo n is well defined and is an isomorphism.*

Thus we have every ring homomorphism with domain R gives rise to factor ring R/N and every factor ring R/N gives rise to a homomorphism

mapping R into R/N. We already mentioned that an ideal in ring theory is analogous to normal subgroup in the group theory.

Question 3.56. *Show that each homomorphism of a field is either one to one or maps everything onto* 0.

Solution. Let $\phi : F \to R$ be a homomorphism from a field F to a ring R and $N = ker(\phi)$. Let $N \neq \{0\}$. Then N contains a non zero element $a \in F$. Since F is a field, a is a unit. Since N is an ideal, $a^{-1}a = 1 \in N$. Let $x \in F$. Then $x1 = x \in N$. So $F = N$. Thus N is either $N = \{0\}$ or $N = F$. That is, either ϕ is either one to one or maps every thing onto 0. ■

Question 3.57. *Let R be a commutative ring and $a \in R$. Show that $I_a = \{x \in R : ax = 0\}$ is an ideal of R.*

Solution. Let $x, y \in I_a$. Then $ax = 0$ and $ay = 0$ and hence $a(x + y) = ax + ay = 0$. So $x + y \in I_a$. Also we have $a(xy) = (ax)y = 0y = 0$. So $xy \in I_a$. Since $a0 = 0$ and $a(-x) = -(ax) = -0 = 0$. So I_a is a subring of R.

Let $r \in R$. Then $a(xr) = (ax)r = 0r = 0$. So $xr \in I_a$. Since R is commutative, $a(rx) = r(ax) = r0 = 0$, $rx \in I_a$. Hence I_a is an ideal in R. ■

EXERCISES

1. Show that an intersection of ideals of a ring is an ideal.

2. Show that a factor ring of a field is either the trivial ring or is isomorphic to the field.

3. Show that if R is a ring with unity and N is an ideal of R such that $N \neq R$, then R/N is a ring with unity.

3.5 Group Presentations

Group presentation is one method of specifying a group by giving a set of generators for the group and relations that the generators to satisfy. Here the group is free on the generators subject to these relations.

Through out this section we denote the identity element in a group by 1.

Example 3.58. Suppose G has generators x and y and is free except for the relation $xy = yx$. The relation $xy = yx$ can be expressed as $xyx^{-1}y^{-1} = 1$. Since $xy = yx$, G must be abelian. Thus G is free abelian on two generators. Recall that an element $xyx^{-1}y^{-1}$ is a commutator of the group $F[\{x, y\}]$. If N is a normal subgroup of G, then G/N is abelian if and only if N contains the commutator subgroup. This implies that any normal subgroup containing $xyx^{-1}y^{-1}$ gives rise to an abelian factor group and thus contains the commutator subgroup. So the commutator subgroup of $F[\{x, y\}]$ is the smallest normal subgroup of $F[\{x, y\}]$ containing $xyx^{-1}y^{-1}$.

Let $F[A]$ be a free group. Here we form a new group as much like $F[A]$ but certain equations that the generators to satisfy. Note that these equations can be written in the form in which the right hand side is 1. We can denote these equations as $r_i = 1$ for $i \in I$ where $r_i \in F[A]$. If $r_i = 1$, then we have $x(r_i^n)x^{-1} = 1$ for any $x \in F[A]$ and $n \in \mathbb{Z}$. So any finite product of the form $\prod_j x_j(r_{i_j})x_j^{-1}$ where the r_{i_j} need not be distinct, will have to equal to 1 in the new group. We can easily verify that the set of all these finite products is a normal subgroup R of $F[A]$. Then the factor group $F[A]/R$ looks like $F[A]$, except that R has been collapsed to form the identity 1.

Definition 3.59. *Let A be a set and let $\{r_i\} \subseteq F[A]$. Let R be the least normal subgroup of $F[A]$ containing the r_i. An isomorphism ϕ of $F[A]/R$ onto a group G is a presentation of G. The sets A and $\{r_i\}$ give a group presentation. The set A is the set of generators for the presentation and each*

r_i is a ralator. Each $r \in R$ is a consequence of $\{r_i\}$. An equation $r_i = 1$ is a relation. A finite presentation is one in which both A and $\{r_i\}$ are finite sets.

Let a group presentation has generators x_j and relators r_j, we use the notation (x_j, r_i) or $(x_j, r_j = 1)$ to denote the group presentation and $F[\{x_j\}]/R$ as the group with presentation (x_j, r_i).

In Example 3.58, $\{x, y\}$ is the set of generators and $xyx^{-1}y^{-1}$ is the only relator. The equation $xyx^{-1}y^{-1} = 1$ or $xy = yx$ is a relation. This presentation is finite.

Isomorphic Presentation

Here we show that different group presentations may give isomorphic groups. In this case we say that the presentations are isomorphic.

Consider the group presentation with

$$A = \{a\} \quad \text{and } \{r_i\} = \{a^6\}.$$

We denote this presentation as

$$(a : a^6 = 1).$$

Note that this group is generated by one generator a, with the relation $a^6 = 1$. So this group is isomorphic to $\mathbb{Z}_6$.

Consider the group presentation with

$$A = \{a, b\} \quad \text{and } \{r_i\} = \{a^2, b^3, aba^{-1}b^{-1}\}.$$

That is the presentation is

$$(a, b : a^2, b^3, aba^{-1}b^{-1}).$$

Now $a^2 = 1$ implies that $a^{-1} = a$ and $b^3 = 1$ implies that $b^{-1} = b^2$. So every element in this group can be written as a product of non negative powers of a and b. From the relation $aba^{-1}b^{-1} = 1$ ($ab = ba$), we can write first all the factors involving a and then the factors involving b. So every element of the group is of the form $a^m b^n$. Since $a^2 = 1$ and $b^3 = 1$, there are just six elements in the group,

$$1, b, b^2, a, ab, ab^2.$$

Thus this presentation gives a group of six elements. Since $ab = ba$, the group is abelian. In this case also the group presentation is isomorphic to $\mathbb{Z}_6$. Hence the above two presentations are isomorphic.

Question 3.60. *Show that* $(x, y : y^2x = y, yx^2y = x)$ *is a presentation of the trivial group of one element.*

Solution. Here we show that $x = 1$ and $y = 1$ can be deduced from the relations $y^2x = y$ and $yx^2y = x$.

We have $y^2x = y$. Multiplication by y^{-1} on left side, we get $yx = 1$. Now substitute $yx = 1$ in $yx^2y = x$, we get $xy = x$. Then multiplying by x^{-1} on the left, we have $y = 1$. Now put $y = 1$ in $yx = 1$, we get $x = 1$. ■

Here we illustrate an application of group presentation.

We determine all groups order 10 upto isomorphism. By Fundamental Theorem of finitely generated abelian groups, every abelian group of order 10 is isomorphic to $\mathbb{Z}_{10}$. Suppose that G is non abelian of order 10. Since 5 divides 10, G has a normal subgroup H of order 5 by Sylow theory. Since order of H is 5, H is cyclic and let a be a generator of H. The factor group G/H is of order 2 and hence isomorphic to $\mathbb{Z}_2$. If $b \notin H$ and $b \in G$, then we must have $b^2 \in H$. Since every element of H except 1 has order 5, if $b^2 \neq 1$, then the order of b^2 is 5. Hence the order of b is 10. This implies that G is cyclic. This is a contradiction to our assumption. So $b^2 = 1$. Since H is a normal subgroup of G, $bHb^{-1} = H$. Consider $bab^{-1} \in bHb^{-1} = H$.

Then bab^{-1} equals a, a^2, a^3 or a^4. If $bab^{-1} = a$, then $ab = ba$ and hence G is abelian. This is not possible. Thus the possibilities for the presentations of G are

1. $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$,
2. $(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$,
3. $(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$.

Using the relation $ba = a^ib$ we can express every product of a's and b's in G in the form a^sb^t. So

$$S = \{a^0b^0, a^1b^0, a^2b^0, a^3b^0, a^4b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1, a^4b^1\}$$

includes all elements of G and all these elements in S need not be distinct.

The group presentation $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$ gives a group and using associative law we can easily show that this group is isomorphic to $\mathbb{Z}_2$.

We have

$$\begin{aligned} a = b^2a = (bb)a = b(ba) = b(a^2b) = (ba)(ab) \\ = (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2 = a^4. \end{aligned}$$

Hence in this case, $a = a^4$. That is, $a^3 = 1$. But $a^5 = 1$. Hence $a^5 = a^3$. This implies that $a^2 = 1$. Now $a^2 = a^3$ implies that $a = 1$. Hence every element in the group with presentation $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$ is equal to either 1 or b. In this case group is isomorphic to $\mathbb{Z}_2$.

Similarly the group presentation $(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$ gives a group and using associative law we can easily show that this group is isomorphic to $\mathbb{Z}_2$.

For

$$a = b^2a = (bb)a = b(ba) = b(a^3b) = (ba)(a^2b)$$

$$= (a^3b)(a^2b) = a^3(ba)(ab) = a^3(a^3b)(ab) = a(ba)b = a^4b^2$$
$$= a^4.$$

So there is only one choice $(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$ for a nonabelian group of order 10. This presentation does give a nonabelian group G of order 10 and is isomorphic to the dihedral group D_5 (for more details refer Text page 350).

EXCERCISE

1. Give a presentation of $\mathbb{Z}_4$ involving one generator, involving two generators, involving three generators.

2. Give a presentation of S_3 involving three generators.