U P RAJARSHI TANDON
OPEN UNIVERSITY
ALLAHABAD

DCEMM-109
ABSTRACT ALGEBRA

ABSTRACT ALGEBRA

Course Design Committee

Prof. Ashutosh Gupta Director, School of Science, UPRTOU, Prayagraj	**Chairman**
Prof. Sudhir Srivastav Professor, Dept. of Mathematics, DDU Gorakhpur University Gorakhpur	**Member**
Prof. P. K. Singh Dept. of Mathematics, University of Allahabad, Prayagraj	**Member**
Prof. Mona Khare Dept. of Mathematics, University of Allahabad, Prayagraj	**Member**
Dr. A. K. Pandey Associate Professor, E.C.C University of Allahabad, Prayagraj	**Member**
Dr. Vikas Singh Academic Consultant School of Science, UPRTOU, Prayagraj	**Member**
Dr. S. S. Tripathi Academic Consultant School of Science, UPRTOU, Prayagraj	**Member**

Course Preparation Committee

Dr. Kamran Alam Khan Assistant Professor (Mathematics) Ram Lubhai Sahani Govt. Girls Degree College, Pilibhit (U.P.)	**Author**
Dr. S. S. Tripathi Academic Consultant School of Science, UPRTOU, Prayagraj	**Editor**
Prof. Ashutosh Gupta Director, School of Computer and Information Science, UPRTOU, Prayagraj	

Faculty Members, School of Sciences

Prof. Ashutosh Gupta, Director, School of Science, UPRTOU, Prayagraj
Dr. Shruti, Asst. Prof., (Statistics), School of Science, UPRTOU, Prayagraj
Dr. Marisha Asst. Prof., (Computer Science), School of Science, UPRTOU, Prayagraj
Mr. Manoj K Balwant Asst. Prof., (Computer Science), School of Science, UPRTOU, Prayagraj
Dr. Dinesh K Gupta Academic Consultant (Chemistry), School of Science, UPRTOU, Prayagraj
Dr. S. S. Tripathi, Academic Consultant (Maths), Scool of Science, UPRTOU, Prayagraj
Dr. Dharamveer Singh, Academic Consultant (Bio-Chemistry), School of Science, UPRTOU, Prayagraj
Dr. R. P. Singh, Academic Consultant (Bio-Chemistry), School of Science, UPRTOU, Prayagraj
Dr. Susma Chuhan, Academic Consultant (Botany), School of Science, UPRTOU, Prayagraj
Dr. Deepa Chubey, Academic Consultant (Zoology), School of Science, UPRTOU, Prayagraj
Dr. Arvind Kumar Mishra, Academic Consultant (Physics), School of Science, UPRTOU, Prayagraj

Block-I

Groups and Subgroups

U P RAJARSHI TANDON
OPEN UNIVERSITY
ALLAHABAD

UGMM-109
ABSTRACT ALGEBRA

Block-I
Groups and Subgroups

Block-I **UGMM-109**

Introduction

Unit-1 In this unit, we introduce binary operations, Definition and examples of Groups, Abelian Groups, some special groups such as groups of Residue classes $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{U}_n$, the group of nth roots of unity, Quaternion group (Hamiltonian group), Klein's four group, Permutation group along with integral powers of an element and order of an element.

Unit-2 In this unit, we introduce the notion of homomorphism and isomorphism. We discuss subgroups with examples, subgroup generated by a subset of a group and cyclic groups with examples.

Unit-3 In the unit, we deal with coset decomposition, left cosets and right cosets of a subgroup, Lagrange's theorem, index of a subgroup, Euler's theorem and Fermat's theorem.

Unit-1: Elementary Group Theory

Structure

1.1 Introduction

Pure Mathematics studies abstract structures, forms and their properties. Abstract algebra is one of the subfields of pure Mathematics which deals with algebraic structures like groups, rings, fields, vector spaces, and so on. In this unit, we provide an exposition of some basic ideas of group theory.

The evolution of the idea of the group can be found in classical algebra (Lagrange, 1770), Number theory (Gauss, 1801), Geometry (Klein, 1874) and Analysis (Lie, 1874 Poincare and Klein, 1876). E. Galois was the first to introduce the word 'Group' in his work on the solutions of equations in around 1830. The modern axiomatic definition of an abstract group was given by walther Von Dyck in 1882 and independently by Heinrich weber in the same year.

The significance of group theory can be understood by the fact that it arises in a number of apparently unrelated disciplines such as physics, chemistry, biology, economics, computer science etc and within Mathematics groups appear in algebra, analysis, number theory, geometry and topology.

Let us begin with the definition of binary operation:

Definition: Let G be a non-empty set. A **binary operation** $*$ on G is a function $* : G \times G \longrightarrow G$ i.e., to each ordered pair $(a, b) \in G$ there exists an element $c \in G$ such that $*(a, b) = c$. We write $a * b$ for $*(a, b)$.

Hence a binary operation is a rule by which we combine any two elements a, b of G so as to get another element $c = a * b$ of G. A binary operation on a set G is also called a composition in G.

For example, the result of addition of two natural numbers is also a natural number, e.g. $3,4 \in \mathbb{N}$ and $3 + 4 = 7 \in \mathbb{N}$ i.e. $a + b \in \mathbb{N}$ for all $a, b \in \mathbb{N}$, hence the usual addition '$+$' is a binary operation on the set $\mathbb{N}$ of all natural numbers. Addition '$+$' is also a binary operation on the sets $\mathbb{Z}$ (Set of all integers), $\mathbb{Q}$ (the set of all rational numbers) and $\mathbb{R}$ (the set of all real numbers) etc. Thus a particular binary operation can be defined on different sets. Similarly several different binary

operations can be defined on a specific set. For example, addition, subtraction and multiplication are binary operations on $\mathbb{R}$.

If '$*$' is a binary operation on a set G, we say that G is **closed** with respect to '$*$'. So we can say that $\mathbb{R}$ is closed under addition, multiplication and subtraction.

Now you may ask a question: Is there an example of a binary operation under which one set is closed while some other is not? The answer is yes! There are many examples. For instance, the subtraction '$-$' is a binary operation on $\mathbb{Z}$, however it fails to be a binary operation on $\mathbb{N}$ as $3,5 \in \mathbb{N}$ but $3-5 \notin \mathbb{N}$.

Definition: A binary operation '$*$' on a non-empty set G is **associative** if

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

and is **commutative** if $a*b=b*a$ for all $a,b \in G$.

For example, the usual addition '$+$' is associative as well as commutative on $\mathbb{Z}$, i.e. $a+(b+c)=(a+b)+c$ and $a+b=b+a$ for all $a,b,c \in \mathbb{Z}$, However subtraction is neither associative nor commutative on $\mathbb{Z}$.

i.e. $a-(b-c) \neq (a-b)-c$ and $a-b \neq b-a$ for $a,b,c \in \mathbb{Z}$.

A set with one or more operations (unary, binary or other) obeying a particular collection of axioms is termed as **'algebraic structure'.** The examples include groupoids, semigroups, monoids, groups, rings, fields and so on. In this unit, we shall study the algebraic structure **'Group'** in details. Let us have a look at our objectives.

1.2 Objectives

After reading this unit, you should be able to:

- Understand the definition of a group and an abelian group
- Observe how sets form groups under different binary operations and how to construct composition tables for finite groups
- Discuss the elementary properties of a group
- Describe residue classes and related groups such as $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n, \mathbb{U}_n$
- Recognize different groups such as group of nth roots of unity, Quaternion group (Hamiltonian group), Klein's four group and permutation group
- Know about the integral powers of an element and order of an element

1.3 Groups

We have already seen that the usual addition '$+$' is a binary operation on the set $\mathbb{Z}$ of all integers, i.e. $a+b \in \mathbb{Z}$ for all $a,b \in \mathbb{Z}$. Also this operation is associative in $\mathbb{Z}$, i.e. $a+(b+c)=(a+b)+c$ for all $a,b,c \in \mathbb{Z}$. We also notice that the set $\mathbb{Z}$ has a special element '0' such that

$$a+0=a=0+a \quad \forall a \in \mathbb{Z}$$

and to each $a \in \mathbb{Z}$ there is an element $-a \in \mathbb{Z}$ such that

$$a+(-a)=0=(-a)+a$$

These properties are not unique to the set of integers with addition.

For example, if we take the set $\mathbb{Q}_{\neq 0}=\mathbb{Q}-\{0\}$ of all nonzero rational numbers with multiplication, we observe that the set $\mathbb{Q}_{\neq 0}$ is closed under multiplication, i.e. $a \cdot b \in \mathbb{Q}_{\neq 0}$ for all $a,b \in \mathbb{Q}_{\neq 0}$ and satisfies the following properties:

1. $a \cdot (b \cdot c)=(a \cdot b) \cdot c$ for all $a,b,c \in \mathbb{Q}_{\neq 0}$

2. There exists $1 \in \mathbb{Q}_{\neq 0}$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in \mathbb{Q}_{\neq 0}$
3. For each $a \in \mathbb{Q}_{\neq 0}$ there exists $1/a \in \mathbb{Q}_{\neq 0}$ such that $1/a \cdot a = 1 = a \cdot 1/a$

You will observe a structure and pattern in the properties satisfied by the elements of the sets $\mathbb{Z}$ and $\mathbb{Q}_{\neq 0}$ with respect to addition and multiplication respectively.

Now we take a very different example from the world of matrices. Suppose we have a set M of 2×2 matrices having their elements as integers. We observe that if we add any two such matrices, again we get same kind of matrix. For example if we take $A, B \in M$ such that $A = \begin{bmatrix} 1 & -2 \\ 5 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 1 \\ -4 & 0 \end{bmatrix}$, then

that $A + B = \begin{bmatrix} 1 & -2 \\ 5 & 3 \end{bmatrix} + \begin{bmatrix} 3 & 1 \\ -4 & 0 \end{bmatrix} = \begin{bmatrix} 4 & -1 \\ 1 & 3 \end{bmatrix} \in M$

This is true for all $A, B \in M$.

Now if we take $C = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$, then

$$(A + B) + C = \begin{bmatrix} 4 & -1 \\ 1 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 4 & 4 \end{bmatrix}$$

Also $A + (B + C) = \begin{bmatrix} 1 & -2 \\ 5 & 3 \end{bmatrix} + \left(\begin{bmatrix} 3 & 1 \\ -4 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & -2 \\ 5 & 3 \end{bmatrix} + \begin{bmatrix} 4 & 3 \\ -1 & 1 \end{bmatrix}$

$$= \begin{bmatrix} 5 & 1 \\ 4 & 4 \end{bmatrix}$$

Hence $(A + B) + C = A + (B + C)$. You can check for yourself that associativity of addition holds good for all $A, B \in M$

Since $0 \in \mathbb{Z}$, hence $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$. It is easy to see that $A + O = A = O + A$ for every $A \in M$.

For example $\begin{bmatrix} 5 & 1 \\ 4 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 4 & 4 \end{bmatrix}$

Also if $A = \begin{bmatrix} 1 & -2 \\ 5 & 3 \end{bmatrix} \in M$, then $-A = \begin{bmatrix} -1 & 2 \\ -5 & -3 \end{bmatrix} \in M$ and

$A + (-A) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$, Also $(-A) + A = O$.

Thus we see that the set M of 2×2 matrices having their elements as integers together with the addition (of matices) satisfies the same properties that are satisfied by $\mathbb{Z}$ with addition(of integers) and $\mathbb{Q} \neq 0$ with multiplication. So we can say that certain systems consisting of a set and a binary operation follow certain specific set of axioms. So if we take an arbitrary nonempty set G and a binary operation '$*$'satisfying above properties, we get an algebraic structure called 'group'.

Definition: A **group** is an ordered pair $(G,*)$ where G is a nonempty set and '$*$' is a binary operation on G satisfying the following axioms:

1. $a * b \in G$ for all $a, b \in G$ **(Closure Property)**
2. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$ **(Associative Law)**
3. There exists an element $e \in G$ called an identity element such that
   $a * e = a = e * a$ for all $a \in G$ **(Existence of Identity)**
4. For each $a \in G$ there exists an element $b \in G$called an inverse of 'a' such that
   $a * b = e = b * a$ and we write $b = a^{-1}$ **(Existence of Inverse)**

The group whose only element is the identity e will be denoted by $\{e\}$. It is called the **trivial group**.

If the set G is finite then the group $(G,*)$ is called a **finite group**, otherwise we call it an **infinite group**. The number of elements in a finite group is called the **order** of the group. An infinite group is said to be of infinite order.

Definition: A group $(G,*)$ is said to be **abelian** (or commutative) if the binary operation '$*$' is commutative, i.e. $a * b = b * a$ for all $a, b \in G$.

Examples: From above discussion it is clear that $(\mathbb{Z},+)$, $(\mathbb{Q},+)$,$(\mathbb{R},+)$ and $(\mathbb{C},+)$ are all infinite abelian groups with $e = 0$ and $a^{-1} = -a$. Also the set M of 2×2 matrices having their elements as integers is an abelian group with $e = O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the inverse of $A \in M$ is $-A$.

Similarly $(\mathbb{Q}_{\neq 0},\cdot)$, $(\mathbb{R}_{\neq 0},\cdot)$ and $(\mathbb{C}_{\neq 0},\cdot)$ are all infinite abelian groups with $e = 1$ and $a^{-1} = {}^{1}/_{a}$.

Do you know why $(\mathbb{N},+)$ is not a group? The answer is simple. Since there exists no natural number e qualifying as the identity element, i.e.

$\nexists e \in \mathbb{N}$ such that $e + a = a = a + e$. Here $e = 0$ but $0 \notin \mathbb{N}$

Also for any $a \in \mathbb{N}$, there is no 'b' in $\mathbb{N}$ such that $a + b = 0$ i.e. $b = -a$.

Does this mean that the sets of numbers create group structures only with usual addition or multiplication? No. That is not the case. For instance, you can check for yourself that the set $\mathbb{Q}^+$ of all positive rational numbers forms an abelian group with respect the composition $*$ given by $a * b = {}^{ab}/_{2}$ for all $a, b \in \mathbb{Q}^+$. Interestingly, $2 \in \mathbb{Q}^+$ is the identity element as

$$2 * a = {}^{2a}/_{2} = 1 = a * 2 \text{ for all } a \in \mathbb{Q}^+.$$

The inverse of $a \in \mathbb{Q}^+$ is ${}^{4}/_{a}$, since $a * {}^{4}/_{a} = 2 = {}^{4}/_{a} * a$. You can easily verify the other group axioms.

Now you are mature enough to understand the following example.

Consider a set $GL_2(\mathbb{R})$ of all 2×2 square matrices whose entries are real numbers and whose determinant is nonzero, i.e.

$$GL_2(\mathbb{R}) = \{A: A \text{ is an } 2 \times 2 \text{ matrix with entries from } \mathbb{R} \text{ and } \det(A) \neq 0\}$$

Hence if $= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$, then $a, b, c, d \in \mathbb{R}$ and $ad - bc \neq 0$. We can show that $GL_2(\mathbb{R})$ is a group under usual multiplication of matrices.

If $A, B \in GL_2(\mathbb{R})$, then AB is also a 2×2 matrix such that $\det(AB) = \det(A) \cdot \det(B) \neq 0$ since $\det(A) \neq 0$ and $\det(B) \neq 0$, hence $AB \in GL_2(\mathbb{R})$.

The product of matrices is associative, i.e. $A(BC) = (AB)C$

The identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element as $AI = A = IA$ for all $A \in GL_2(\mathbb{R})$ and the inverse of $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the matrix $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Obviously $A^{-1} \in GL_2(\mathbb{R})$ and $AA^{-1} = I = A^{-1}A$.

This is an example of a non-abelian group, since the matrix multiplication is not commutative in general, i.e. $AB \neq BA$. For example – Let $A = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \neq 0$, $B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \neq 0$ but $A.B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. This group is called the general linear group of degree 2. Similarly we can define general linear group of degree n, i.e. $GL_n(\mathbb{R})$ under matrix multiplication, where

$$GL_n(\mathbb{R}) = \{A: A \text{ is an } n \times n \text{ matrix with entries from } \mathbb{R} \text{ and } \det(A) \neq 0 \}$$

So far we have seen examples of infinite groups. You may ask if there are finite sets forming groups under certain binary operations. Yes, we have many interesting examples. The simplest are the trivial groups such as $(\{0\}, +)$ and $(\{1\},\cdot)$. The set of square roots of unity, i.e. $\{1, -1\}$ forms an abelian group with respect usual multiplication. There are other interesting examples of finite groups like the multiplicative group of nth roots of unity, Klein four group, quaternion group, Symmetric group on n symbols, groups of residue classes $\mathbb{Z}_n, \mathbb{Z}_p$and $\mathbb{U}_n$ etc which we shall discuss later in details.

For a finite group we may construct a table called a group table or composition table to tabulate the effect of a binary operation on its elements. If a group $(G,*)$ contains n elements, namely, $g_1, g_2, \ldots\ldots, g_n$, then its composition table is a square $n \times n$ matrix with (i,j)th entry $g_{ij} = g_i * g_j$.

$*$	g_1	g_2	…..	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	…..	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	…..	$g_2 * g_n$
⋮	⋮	⋮	⋮	⋮
g_n	$g_n * g_1$	$g_n * g_2$	…..	$g_n * g_n$

Usually the element $g_1$is taken as the identity element e. The composition table contains each element exactly once in each of its rows and columns. Since in a finite abelian group $(G,*)$ we have $g_i * g_j = g_j * g_i$ for all $g_i, g_j \in G$, the entries in the table are symmetric with respect to the diagonal that starts at the upper left corner and ends at the lower right corner.

Example: Let us construct a group table for the multiplicative group of cube roots of unity, i.e. $(\{1, \omega, \omega^2\},\cdot)$.

$\cdot$	1	ω	ω^2
1	$1 \cdot 1$	$1 \cdot \omega$	$1 \cdot \omega^2$
ω	$\omega \cdot 1$	$\omega \cdot \omega$	$\omega \cdot \omega^2$
ω^2	$\omega^2 \cdot 1$	$\omega^2 \cdot \omega$	$\omega^2 \cdot \omega^2$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

The group axioms can be verified directly from the table. The entries of the composition table are the elements of $G = \{1, \omega, \omega^2\}$ thereby indicating that the closure property is satisfied. The top row coincides with the first row corresponding to the element 1, i.e. 1 is the identity element. Also the identity 1 appears in the cells (1,1), (2,3) and (3,2) corresponding to the products $1 \cdot 1$, $\omega \cdot \omega^2$ and $\omega^2 \cdot \omega$ respectively. Hence $(1)^{-1} = 1$, $(\omega)^{-1} = \omega^2$ and $(\omega^2)^{-1} = \omega$. The commutativity is confirmed from the fact that the entries in the table are symmetric with respect to the diagonal from the cell (1,1) to (3,3).

Note: Instead of referring $(G,*)$ as group, we simply say that G is a group with the understanding that there is no confusion regarding the binary composition. Sometimes, it is convenient to denote the binary operation '$*$' by '$\cdot$'. Henceforth (except when necessary) we shall use the notation '$a \cdot b$' (or simply 'ab') for '$a * b$'.

1.4 Elementary properties of groups

Proposition 1.1 If G is a group, then

(1) The identity element of G is unique
(2) Each element of G has unique inverse in G
(3) $(a^{-1})^{-1} = a \quad \forall a \in G$
(4) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a, b \in G$

Proof: (1) Let e and f be two identities of G, then $ef = f$ as e is an identity. Also $ef = e$ as f is an identity. Therefore $f = e$, and the identity is unique.

(2) Let $a \in G$. Assume that b and c are both inverses of a in G, then we have $ab = e = ba$ and $ac = e = ca$. Now $b = be = b(ac) = (ba)c = ec = c$. Hence inverse of a is unique.

(3) b is the inverse of a if $ba = e = ab$ and we write $b = a^{-1}$. Also a is the inverse of b, i.e. $a = b^{-1}$, hence $a = b^{-1} = (a^{-1})^{-1}$

(4) we have $(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1}$, by associative law

$= (ae)a^{-1}$, since $bb^{-1} = e$

$= aa^{-1}$, since $ae = a$

$= e$

Also $(b^{-1}a^{-1})(ab) = b^{-1}[(a^{-1}a)b] = b^{-1}(eb) = b^{-1}b = e$

Hence $(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$, consequently $(ab)^{-1} = b^{-1}a^{-1}$.

Proposition 1.2 The left and right cancellation laws hold in a group G.

Proof: suppose $a, b, c \in G$ then a^{-1} exists. Now $ab = ac$

$\Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}a)c \Longrightarrow eb = ec \Longrightarrow b = c$

Similarly, from $ba = ca$ we can deduce $b = c$ upon multiplication on the right by a^{-1}.

Using the associative law and other axioms we can deduce the following result:

Proposition 1.3 If G is a group and $a, b \in G$, then each of the equations $ax = b$ and $ya = b$ has unique solution in G. (Prove it)

1.5 Some special groups

1.5.1 Residue classes and the groups $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n, \mathbb{U}_n$

Let n be a fixed positive integer, we define a relation '$\equiv$' on $\mathbb{Z}$ as follows-

$$a \equiv b \pmod{n} \text{ if and only if } n \text{ divides } (a - b)$$

The expression $a \equiv b \pmod{n}$ is read as " a is congruent to b modulo n".

Thus $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a - b = nq$ for some $q \in \mathbb{Z}$

or $a \equiv b \pmod{n} \Leftrightarrow a = b + nq$ for some $q \in \mathbb{Z}$. This relation is called the **relation of congruence modulo n** in the set of integers.

For example, 3 divides $15 = 17 - 2$. Hence we can write $17 \equiv 2 \pmod{3}$. Similarly $15 \equiv 3 \pmod{12}$. Does this remind you of any real life situation? Yes, your wall clock tells you that 10 o'clock (A.M.) plus 5 hours is 3 o'clock (P.M.), i.e. $10 + 5 \equiv 3 \pmod{12}$.

Proposition 1.4 The relation of congruence modulo n is an equivalence relation in the set $\mathbb{Z}$ of integers.

Proof: We have $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

(1) **Reflexivity:** Since $n|0$ i.e. $n|(a - a) \ \forall a \in \mathbb{Z}$,
hence $a \equiv a \pmod{n} \ \forall a \in \mathbb{Z}$

(2) **Symmetry:** $a \equiv b \pmod{n} \Rightarrow a = b + nq$ for some $q \in \mathbb{Z}$
$\Rightarrow b - a = -nq$ for some $q \in \mathbb{Z}$
$\Rightarrow n|(b - a)$
$\Rightarrow b \equiv a \pmod{n}$

(3) **Transitivity:** $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
$\Rightarrow a = b + nq_1, \ b = c + nq_2$ for some $q_1, q_2 \in \mathbb{Z}$
$\Rightarrow a = (c + nq_2) + nq_1$ for some $q_1, q_2 \in \mathbb{Z}$
$\Rightarrow a - c = n(q_2 + q_1)$ for some $q_1, q_2 \in \mathbb{Z}$
$\Rightarrow a \equiv c \pmod{n}$

Hence the relation of congruence modulo n is an equivalence relation in $\mathbb{Z}$. This equivalence relation decomposes $\mathbb{Z}$ into disjoint equivalence classes called the **congruence classes modulo n or residue classes modulo n.**

For any $a \in \mathbb{Z}$, we shall denote the congruence class of a by $[a]$. Thus

$$[a] = \{x \in \mathbb{Z}: x \equiv a \pmod{n}\}$$

$$= \{x \in \mathbb{Z}: \ x = a + nq, q \in \mathbb{Z}\}$$

$$= \{a + nq : q \in \mathbb{Z}\}$$

For example, if we take $n = 5$, the residue class modulo 5 of '0' will be

$$[0] = \{nq : q \in \mathbb{Z}\} = \{\ldots -10, -5, 0, 5, 10, \ldots\}$$

These residue classes have the following properties:

(1) $a \in [a]$ for any $a \in \mathbb{Z}$ (2) If $b \in [a]$, then $[a] = [b]$

(3) $[a] = [b]$ if and only if $a \equiv b \pmod{n}$

(4) Either $[a] = [b]$ or $[a] \cap [b] = \emptyset$

Thus we have $[a] = [a + n] = [a + 2n]$ and so on.

Similarly $[0] = [n] = [2n] = \ldots\ldots = [-n] = [-2n] = [-3n] = \ldots$

We can show that there are precisely n distinct residue classes, namely

$$[0], [1], \ldots\ldots, [n-1]$$

Let $a, b \in \{0, 1, \ldots\ldots, n-1\}$ such that $a > b$ then

$$[a] = [b] \Longrightarrow a \equiv b \pmod{n} \Longrightarrow n \text{ divides } (a - b),$$

Which is not possible since $a - b < n$. Therefore $[a] \neq [b]$ and thus the residue classes $[0], [1], \ldots\ldots, [n-1]$ are all distinct. Also if $a \in \mathbb{Z}$, then by division algorithm

$$a = nq + r, \text{ where } q, r \in \mathbb{Z} \text{ and } 0 \leq r < n$$

$$\Longrightarrow a \equiv r \pmod{n} \Longrightarrow [a] = [r]$$

Hence if $a \in \mathbb{Z}$, then $[a]$ is equal to one of the residue classes $[0], [1], \ldots\ldots, [n-1]$. The set of these n distinct residue classes is denoted by $\mathbb{Z}/n\mathbb{Z}$, i.e. $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots\ldots, [n-1]\}$.

We can define the addition operation on $\mathbb{Z}/n\mathbb{Z}$ as follows-

$$[a] + [b] = [a + b]$$

This addition is well defined i.e. if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ such that $[a_1] = [b_1]$ and $[a_2] = [b_2]$ then $[a_1 + a_2] = [b_1 + b_2]$. Since

$[a_1] = [b_1]$ and $[a_2] = [b_2] \Longrightarrow a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$

$\Longrightarrow a_1 = nq_1 + b_1$ and $a_2 = nq_2 + b_2$ for some $q_1, q_2 \in \mathbb{Z}$

$\Longrightarrow a_1 + a_2 = n(q_1 + q_2) + b_1 + b_2$

$\Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$

$\Longrightarrow [a_1 + a_2] = [b_1 + b_2]$

It can be immediately verified that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the addition of residue classes.

Proposition 1.5 $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the addition of residue classes.

Proof: we have $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots\ldots, [n-1]\}$

(1) Closure Property: If $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, then

$$[a] + [b] = [a + b]$$

since $a + b \equiv r \pmod{n}$, $0 \leq r < n$, hence $[a + b] \in \mathbb{Z}/n\mathbb{Z}$

(2) Associative Law: Let $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c]$$

$$= [a + b] + [c] = ([a] + [b]) + [c]$$

(3) Existence of identity: We have $[0] + [a] = [a] = [a] + [0]$

Hence $[0] \in \mathbb{Z}/n\mathbb{Z}$ is the identity element.

(4) Existence of inverse: Let $[a] \in \mathbb{Z}/n\mathbb{Z}$. Then a is an integer such that $0 \leq a < n$. Therefore $0 < n - a \leq n$, i.e. $[n - a] \in \{[1], [2], \dots, [n]\}$. Since $[n] = [0]$, hence $[n - a] \in \mathbb{Z}/n\mathbb{Z}$. Now $[a] + [n - a] = [0] = [n - a] + [a]$, therefore the inverse of $[a] \in \mathbb{Z}/n\mathbb{Z}$ is $[n - a] \in \mathbb{Z}/n\mathbb{Z}$.

(5) The commutative law: Let $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

Hence $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the addition of residue classes called the **additive group of residue classes modulo n**.

We can also define the multiplication of residue classes as follows-

$$[a][b] = [ab]$$

This multiplication is well defined in the set $\mathbb{Z}/n\mathbb{Z}$. Now the question arises: Do the nonzero residue classes $[1], \dots \dots, [n - 1]$ form a group under this multiplication?

Not necessarily. For example, in $\mathbb{Z}/6\mathbb{Z}$, $[4][3] = [12] = [0]$, hence nonzero elements can sometimes have a zero product. Also not all the nonzero residue classes are invertible (units) generally. They are all invertible only when $n = p$, a prime number. The set of all invertible elements (units) of $\mathbb{Z}/n\mathbb{Z}$ forms an abelian group with respect to multiplication of residue classes. This set of units is denoted by $(\mathbb{Z}/n\mathbb{Z})^{\times}$, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{[a] \in \mathbb{Z}/n\mathbb{Z} : [a] \text{ is invertible } \}$$

Now you will observe that an element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is invertible with respect to residue multiplication if and only if $\gcd(a, n) = 1$.

If $[a]$ is invertible, then there exists $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = [1]$, i.e. $ab \equiv 1 \pmod{n}$. Which implies that $ab = qn + 1$ for some $q \in \mathbb{Z}$, i.e. $\gcd(a, n) = 1$, by Bezout's Lemma. The lemma is – [**Bezout's Lemma** states that if x and y are nonzero integers and $g = \gcd(x, y)$, then there exist integers α and β such that $x\alpha + y\beta = g$. In other words, there exists a linear combination of x and y equal to g.]. Conversely, if $\gcd(a, n) = 1$, then by Bezout's Lemma, there exist integers x and y such that $ax + ny = 1$, i.e. $ax \equiv 1 \pmod{n}$ and so $[a][x] = [1]$ and it follows that $[a]$ is invertible. Hence we can define $(\mathbb{Z}/n\mathbb{Z})^{\times}$ as

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$$

$$= \{[a] \in \mathbb{Z}/n\mathbb{Z} : a \text{ and } n \text{ are co-prime}\}$$

Now we shall show that $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is indeed a group under multiplication of residue classes.

Proposition 1.6 $(\mathbb{Z}/n\mathbb{Z})^{\times}$is an abelian group under multiplication of residue classes.

Proof: We have $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \ a \text{ and } n \text{ are co-prime}\}$.

(1) Closure Property: Let $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$Then $[a][b] = [ab]$. Now $[ab] \neq [0]$ otherwise $n|ab$ which is not possible, since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. Therefore $[ab] = [r]$ where $1 \leq r < n$. Further if $\gcd(r, n) \neq 1$ then there exists some prime number p dividing both r and n. This gives $p|ab$ i.e. $p|a$ or $p|b$. Thus either p divides the HCF of a and n or HCF of b and n .which is not possible as $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. Therefore $\gcd(r, n) = 1$ and hence $[r] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

(2) Associativity: Let $[a], [b], [c] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Then we have

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]$$

(3) Existence of identity: since 1 is co-prime to n, hence $[1] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ and we have

$$[a][1] = [a1] = [a] = [1][a]$$

Therefore $[1]$ is the identity element.

(4) Existence of inverse: If $[a] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $\gcd(a, n) = 1$ and we have already seen that in this case $[a]$ is invertible.

(5) Commutativity: Let $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Then we have

$$[a][b] = [ab] = [ba] = [b][a]$$

Thus $(\mathbb{Z}/n\mathbb{Z})^{\times}$is a finite abelian group with respect to multiplication of residue classes. Now what is the order of this group? It is equal to the number of positive integers less than n and co-prime to n, i.e. **the Euler's totient function** $\varphi(n)$.

It is interesting to note that if $n = p$, a prime number, then the positive integers less than p and co-prime to p are $1,2, \ldots \ldots, p-1$. Hence we have

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \{[1], \ldots \ldots, [p-1]\}.$$

Now we shall discuss some other groups abstractly similar to $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^{\times}$, i.e. $\mathbb{Z}_n$ and $\mathbb{U}_n$.

Group of integers modulo n

Let a and b be any two integers and n be a fixed integer, we define a composition on the set of integers $\mathbb{Z}$ called **addition modulo n** $(+_n)$ as follows-

$$a +_n b = r, \qquad 0 \leq r < n$$

Where r is the least non-negative remainder when $a + b$ is divided by n.

For example, $3 +_5 4 = 2$, since 2 is the remainder (non-negative) when $3 + 4$ i.e. 7 is divided by 5. Also $(-25) +_3 6 = 2$ since $-25 + 6 = -19 = (-7)3 + 2$.

If $a +_n b = r$, then by division algorithm we can write

$$a + b = nq + r, \ 0 \leq r < n$$

For some integer q.

Hence $(a + b) - r$ is divisible by n, i.e. $r \equiv a + b \pmod{n}$ or

$$a +_n b \equiv a + b \pmod{n}$$

It can be easily seen that if $a \equiv b \pmod{n}$, then $a +_n c = b +_n c$.

Let $\mathbb{Z}_n = \{0,1, \ldots \ldots, n-1\}, n \geq 1$. Then we can show that $\mathbb{Z}_n$ forms an abelian group with respect to addition modulo n.

(1) Closure property: Let $a, b \in \mathbb{Z}_n$ then $a +_n b \equiv a + b \pmod{n} \in \mathbb{Z}_n$. Hence $\mathbb{Z}_n$ is closed under addition modulo n.

(2) Associativity: Let $a, b, c \in \mathbb{Z}_n$.Then

$$a +_n (b +_n c) = a +_n (b + c) \text{ as } b +_n c \equiv b + c \pmod{n}$$
$$= [a + (b + c)] \pmod{n}$$

$$= [(a + b) + c](\text{mod } n)$$
$$= (a + b)+_n c$$
$$= (a+_n b)+_n c$$

(3) Existence of identity: $0 \in \mathbb{Z}_n$ such that $a+_n 0 = a = 0+_n a \ \ \forall a \in \mathbb{Z}_n$, i.e. 0 is the identity element.

(4)Existence of inverse: Let $a \in \mathbb{Z}_n$. If $a = 0$, then it is the inverse of itself. Let $a \neq 0$. Then $n - a \in \mathbb{Z}_n$ is the inverse of $a \in \mathbb{Z}_n$ as

$$(n - a)+_n a = 0 = a+_n (n - a)$$

(5) Commutativity: Let $a, b \in \mathbb{Z}_n$. Then

$$a+_n b = a + b \ (\text{mod } n) = b+_n a$$

Therefore $(\mathbb{Z}_n, +_n)$ is a finite abelian group of order n. This group is usually referred to as the **group of integers modulo n**.

Note: ***Sometimes by the abuse of notation we write $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ and consider $\mathbb{Z}_n$ as the additive group of residue classes modulo n.***

Definition: Let a and b be any two integers and n be a fixed integer. The composition on the set of integers $\mathbb{Z}$ called **multiplication modulo n** ($\times_n$) is defined as follows-

For any two integers a and b and a fixed integer n,

$$a \times_n b = r, \ 0 \leq r < n$$

Where r is the least non-negative remainder when ab is divided by n.

For example, $7 \times_3 4 = 1$, since 1 is the remainder (non-negative) when 7×4 i.e. 28 is divided by 3. Obviously we have $a \times_n b \equiv ab \ (\text{mod } n)$. Also if $a \equiv b(\text{mod } n)$, then $a \times_n c = b \times_n c$.

The set of all invertible elements (units) of $\mathbb{Z}_n$ forms an abelian group with respect to multiplication modulo n. This set of units is denoted by $\mathbb{U}_n$, i.e.

$$\mathbb{U}_n = \{a \in \mathbb{Z}_n : a \text{ is invertible } \}$$

Following the same arguments as that given earlier in case of $\mathbb{U}(n)$, using Bezout's Lemma you can check for yourself that an element $a \in \mathbb{Z}_n$ is invertible with respect to multiplication modulo n if and only if $\gcd(a, n) = 1$.

Hence

$$\mathbb{U}_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1 \}$$
$$= \{a \in \mathbb{Z}_n : a \text{ and } n \text{ are co-prime}\}$$

Proposition 1.7 $(\mathbb{U}_n, \times_n)$ is a finite abelian group.

The proof is similar to that of proposition 1.6.

If p is a prime number, then the elements of $\mathbb{Z}_p$ co-prime to p are$1,2, \ldots \ldots, p - 1$.

Hence $\mathbb{U}_p = \{1,2, \ldots \ldots, p - 1\}$.

Proposition 1.8 $(\mathbb{U}_p, \times_p)$, p being prime, is a finite abelian group.

Proof: We have $\mathbb{U}_p = \{1,2, \ldots \ldots, p - 1\}$, where p is a prime number.

(1) Closure property: Let $a, b \in \mathbb{U}_p$. Then p is neither a divisor of a nor a divisor of b. Therefore $p \nmid ab$. Hence the remainder cannot be zero when ab is divided by p i.e. if $a \times_p b = r$, then $1 \leq r \leq p - 1$. Thus $a \times_p b \in \mathbb{U}_p$.

(2) Associativity: For all $a, b, c \in \mathbb{U}_p$,we have,

$$a \times_p (b \times_p c) = a \times_p (bc) \text{ ,since } b \times_p c \equiv bc \ (\text{mod } p)$$
$$= a(bc) \ (\text{mod } p)$$
$$= (ab)c \ (\text{mod } p)$$

$$= (ab) \times_p c$$
$$= (a \times_p b) \times_p c$$

(3) Existence of identity: $1 \in \mathbb{U}_p$ such that $1 \times_p a = a = a \times_p 1$ for all $a \in \mathbb{U}_p$. Hence 1 is the identity element.

(4) Existence of inverse: If $a \in \mathbb{U}_p$, then by closure property $a \times_p i \in \mathbb{U}_p$ for all $i \in \mathbb{U}_p$. Also $i \neq j \Longrightarrow a \times_p i \neq a \times_p j$ for $i, j \in \mathbb{U}_p$ for if $a \times_p i = a \times_p j$, then $ai - aj$ is divisible by p, i.e. $p|a(i-j)$. Which is not possible, since p cannot divide $(i-j)$ as either $i - j < p$ for $i > j$, or $j - i < p$ for $j > i$. Also $p \nmid a$. Hence all the products $a \times_p i \in \mathbb{U}_p$, $i \in \mathbb{U}_p$ are distinct elements of $\mathbb{U}_p$. Therefore there exists $i = k \in \mathbb{U}_p$ such that $a \times_p k = 1$, i.e. k is the inverse of a.

(5) Commutativity: For all $a, b \in \mathbb{U}_p$we have,

$$a \times_p b = ab \pmod{p}$$
$$= ba \pmod{p}$$
$$= b \times_p a$$

i.e. $(\mathbb{U}_p, \times_p)$ is a finite abelian group of order $p - 1$.

1.5.2 Group of nth roots of unity

Let us start with the square roots of unity. We have $(1)^{1/2} = \pm 1$, hence the set of square roots of unity is $\{-1,1\}$. You can check for yourself that this is an abelian group under multiplication. For the cube roots of unity, we have

$$(1)^{1/3} = (\cos 2r\pi + i \sin 2r\pi)^{1/3} = \cos\left(\frac{2\pi r}{3}\right) + i \sin\left(\frac{2\pi r}{3}\right), r = 0,1,2$$

i.e. $(1)^{1/3} = \cos(0) + i\sin(0), \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right), \cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right)$

$$= 1, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}$$

If we let $\omega = \frac{-1+i\sqrt{3}}{2}$, then simple calculation shows that

$$\omega^2 = \left(\frac{-1 + i\sqrt{3}}{2}\right)^2 = \frac{-1 - i\sqrt{3}}{2}$$

Thus the set of cube roots of unity is $\{1, \omega, \omega^2\}$. We have already seen that this set forms an abelian group under multiplication. Let us illustrate one more thing that will be useful in discussing the nth roots of unity.

$$\omega^t \omega^s = \omega^{t+s}$$

But since $\omega^3 = 1$, hence if $t + s = 3q + k$, where $0 \leq k < 3$, then $\omega^{t+s} = \omega^k$, i.e. $\omega^{t+s} = \omega^{t+s \,(\mathrm{mod} 3)}$.For instance $\omega^2\omega^2 = \omega^4 = \omega^{3(1)+1} = \omega^3\omega^1 = 1\omega = \omega$

Now we can generalize this concept to nth roots of unity. The set of nth roots of unity is given by

$$G = \{z \in \mathbb{C}: z^n = 1\}$$

It is easy to see that the solutions of the equation $z^n = 1$ are the numbers $e^{2r\pi i/n}, r = 0,1, \ldots, n-1$.

$$(1)^{1/n} = (\cos 2r\pi + i \sin 2r\pi)^{1/n}, r = 0,1, \ldots, n-1$$
$$= \cos\left(\frac{2\pi r}{n}\right) + i \sin\left(\frac{2\pi r}{n}\right), r = 0,1, \ldots, n-1$$
$$= e^{2r\pi i/n}, r = 0,1, \ldots, n-1$$

If we let $\zeta = e^{2\pi i/n}$, then the set of nth roots of unity can be written as

$$G = \{1 = \zeta^0, \zeta, \zeta^2, \ldots\ldots, \zeta^{n-1}\}$$

Proposition 1.9 The set of nth roots of unity forms a finite abelian group with respect to multiplication of complex numbers.

Proof: We have $G = \{1 = \zeta^0, \zeta, \zeta^2, \ldots\ldots, \zeta^{n-1}\}$, where $\zeta = e^{2\pi i/n}$.

(1) For $\zeta^t, \zeta^s \in G$, we have $\zeta^t\zeta^s = \zeta^{t+s}$. But $\zeta^n = 1$, hence $\zeta^{t+s} = \zeta^k$ where $k \equiv t + s \pmod{n}$, therefore $0 \leq k < n$ and $\zeta^k \in G$, i.e. $\zeta^t\zeta^s \in G$. Hence G is closed with respect to multiplication.

(2) The multiplication of complex numbers is associative.

(3) $1 \in G$ is the identity element.

(4) The inverse of 1 is 1 itself and ζ^{n-s} is the inverse element of $\zeta^s \in G$ $(1 \leq s \leq n-1)$, since $\zeta^{n-s}\zeta^s = \zeta^n = 1 = \zeta^s\zeta^{n-s}$ and $1 \leq n - s \leq n - 1$.

(5) The multiplication of complex numbers is commutative.

i.e. The set of nth roots of unity forms a finite abelian group of order n under multiplication.

1.5.3 Permutation group

Let S be a nonempty set. Then a one-one mapping of S onto itself (i.e. bijections from S to itself) is called a permutation. The set $A(S)$ of all permutations of S forms a group with respect to function composition$o$. Let us see how the group axioms are satisfied.

(1) Let $f: S \longrightarrow S$ and $g: S \longrightarrow S$ be any two permutations (bijections) of S, then $fog: S \longrightarrow S$ given by $(fog)(x) = f\{g(x)\}\ \forall x \in S$ is also a permutation (bijection) of S, i.e. $fog \in A(S)$.

(2) $(fog)oh = fo(goh)$ for all $f, g, h \in A(S)$

(3) The identity map $i: S \longrightarrow S$ given by $i(x) = x \quad \forall x \in S$ is the identity element as $(foi)(x) = f\{i(x)\} = f(x) \quad \forall x \in S$, and $(iof)(x) = i\{f(x)\} = f(x) \quad \forall x \in S$, i.e. $iof = f = foi$

(4) For every permutation $f: S \longrightarrow S$ there is an inverse function $f^{-1}: S \longrightarrow S$ such that $f^{-1}(y) = x$ whenever $y = f(x)$. Obviously f^{-1} is also a bijection on S, i.e. $f^{-1} \in A(S)$. Also $(fof^{-1})(y) = f\{f^{-1}(y)\} = f(x) = y = i(y)$,i.e. $fof^{-1} = i$. Similarly $f^{-1}of = i$. Hence $f^{-1} \in A(S)$ is the inverse element of $f \in A(S)$.

Thus $(A(S), o)$ is a group of permutations and is called the **symmetric group** on S. Subgroups of symmetric groups are called **Transformation groups** or **Permutation groups**.

Now there is an interesting case when the set S is finite. For instance suppose $S = \{1,2,3, \ldots, n\}$, then the group $A(S)$ of all permutations of S is denoted by S_n and is called **symmetric group of degree n**.

You may ask a question: How many elements does S_n have? Or equivalently, How many bijections can be defined from S to S? It is equivalent to counting the number of ways, in which we can permute the elements of the set S. For n elements this number is $n!$. Hence S_n is a group of order $n!$. For example, S_3 has $3! = 6$ elements. Suppose $f \in S_3$ such that $f(1) = 3, f(2) = 2, f(3) = 1$, then we use the following standard notation to denote this permutation:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

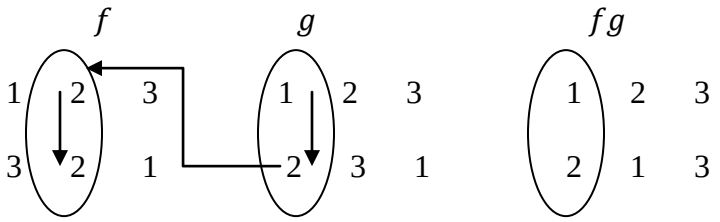
Let $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$. Then we usually denote the composition of f and g by fg, i.e. $fg = fog$. Now $(fg)(1) = (fog)(1) = f\{g(1)\} = f(2) = 2$

$$(fg)(2) = (fog)(2) = f\{g(2)\} = f(3) = 1$$
$$(fg)(3) = (fog)(3) = f\{g(3)\} = f(1) = 3$$

Hence we can write

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

Remember that the composition is applied from *right to left order*.



Example: Now we construct a composition table for S_3 and show that it is a finite nonabelian group of order 6 with respect to multiplication of permutations.

Let $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ such that

$f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $f_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$, $f_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$,

$f_5 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, $f_6 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$

Here we have $f_1 f_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = f_2$

$f_2 f_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = f_1$ and so on. So the composition table is

Product of permutations	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

From the composition table, we observe that

(1) All the entries of the table are the elements of S_3. Hence S_3 is closed under the multiplication of permutations.

(2) The composition of mappings is associative in general, hence this multiplication of permutations is an associative composition.

(3) We observe that $f_1 f_1 = f_1$, $f_1 f_2 = f_2 = f_2 f_1$, $f_1 f_3 = f_3 = f_3 f_1$,
$f_1 f_4 = f_4 = f_4 f_1$, $f_1 f_5 = f_5 = f_5 f_1$ and $f_1 f_6 = f_6 = f_6 f_1$. Therefore f_1 is the identity element.

(4) Also we have $f_1 f_1 = f_1 \Longrightarrow (f_1)^{-1} = f_1$,
$f_2 f_3 = f_1 = f_3 f_2 \Longrightarrow (f_2)^{-1} = f_3$, and $(f_3)^{-1} = f_2$, $f_4 f_4 = f_1 \Longrightarrow (f_4)^{-1} = f_4$, $f_5 f_5 = f_1 \Longrightarrow (f_5)^{-1} = f_5$ and $f_6 f_6 = f_1 \Longrightarrow (f_6)^{-1} = f_6$

Thus each element has its inverse in S_3.

This multiplication of permutations is not commutative as we see that $f_5 f_3 = f_4$ and $f_3 f_5 = f_6$. Thus $f_5 f_3 \neq f_3 f_5$.

Therefore S_3 is a finite nonabelian group of order 6 with respect to permutation multiplication.

Here you will notice that $(f_2)^{-1} = f_3$, i.e. $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$. Since interchanging the columns does not change the permutation, hence we can write $\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$ as $\begin{pmatrix}2 & 3 & 1\\ 1 & 2 & 3\end{pmatrix}$. Therefore we have $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}^{-1} = \begin{pmatrix}2 & 3 & 1\\ 1 & 2 & 3\end{pmatrix}$. So when we inverse the permutation, we simply interchange the rows in the standard notation. We shall study some other properties of these permutations in block-II.

1.5.4 Klein's four group

Consider a finite group $V = \{e, a, b, c\}$ of order 4 with the following composition table-

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

It is interesting to note that each element is the inverse of itself. From the composition table we also observe that this is an abelian group. This group is called the Klein's four group. You can check for yourself that the matrices $e = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $a = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, $b = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$, and $c = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ form a Klein's four group under multiplication.

1.5.5 Quaternion group (Hamiltonian group)

Consider a set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Define a multiplication '$\cdot$' called quaternion multiplication on Q_8 as follows-

$$i \cdot i = j \cdot j = k \cdot k = -1\ ,\ i \cdot j = k, j \cdot k = i, k \cdot i = j$$
$$j \cdot i = -k, k \cdot j = -i, ,\ i \cdot k = -j, (-1) \cdot (-1) = 1$$

and $1 \cdot a = a \cdot 1 = a$, $(-1) \cdot a = a \cdot (-1) = -a$ for all $a \in Q_8$.

Then Q_8 forms a non-abelian group under quaternion multiplication. This is an example of a more general group called **Hamiltonian** group. Every Hamiltonian group contains a copy of Q_8. You can check for yourself that the following matrices form a quaternion group.

$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \begin{bmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{bmatrix}, \begin{bmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \begin{bmatrix}-\sqrt{-1} & 0\\ 0 & \sqrt{-1}\end{bmatrix}, \begin{bmatrix}0 & -\sqrt{-1}\\ -\sqrt{-1} & 0\end{bmatrix}$

1.6 The integral powers and order of an element

Let $(G, *)$ be a group and $a \in G$. Then we define the positive powers of a as

$$a^n = a * a * \ldots * a \text{ upto } n \text{ factors}, n = 1,2,3, \ldots.$$

and $a^0 = e$ (the identity of G)

If n is a negative integer, then $n = -m$, $m = 1,2, \ldots\ldots$ and we have

$$a^n = a^{-m} = (a^m)^{-1} = (a * a * \ldots * a \text{ upto m factors})^{-1}$$

$$= a^{-1} * a^{-1} * \ldots * a^{-1} \text{ upto m factors} = (a^{-1})^m$$

Also for any two integers m, n, you can prove that

$$a^{n+m} = a^n * a^m \text{ and } (a^n)^m = a^{nm}$$

These two are the laws of indices in a group.

Hence for a group in which the composition is denoted multiplicatively, we have

$$a^n = aa \ldots a \text{ upto } n \text{ factors, } n = 1,2,3, \ldots. \text{ and } a^{-m} = (a^{-1})^m$$

And for a group $(G, +)$ in which the composition is denoted additively, we have

$$na = a + a + \cdots + a \text{ upto n terms and } (-m)a = m(-a)$$

Now we are in position to define the order of an element of a group.

Definition: Let G be a group and let $a \in G$. Then the **order** of a is the least positive integer n such that $a^n = e$(the identity of G). If there exists no positive integer n such that $a^n = e$, then a is said to be of infinite order or zero order. The symbol $o(a)$ is used to denote the order of a.

Example: consider the multiplicative group $G = \{1, -1, i, -i\}$. We have

(1) $o(1) = 1$

(2)$(-1)^1 = -1$, $(-1)^2 = 1$ hence $o(-1) = 2$

(3) $o(i) = 4$ since $i^4 = 1$ and for no positive integer m less than 4, $i^m = 1$ and similarly $o(-i) = 4$

Example: In $\mathbb{Z}_5$ i.e. $(\{0,1,2,3,4\}, +_5)$, we have

$2^1 = 2$, $2^2 = 2+_5 2 = 4$, $2^3 = 2+_5 2+_5 2 = 1$, $2^4 = 2+_5 2+_5 2+_5 2 = 3$,

$2^5 = 2+_5 2+_5 2+_5 2+_5 2 = 0$, hence $o(2) = 5$.

Example: In the additive group of integers $(\mathbb{Z}, +)$, we have $o(0) = 1$ and for any nonzero integer a, there does not exists a positive integer n such that $a + a + \cdots + a$ (upto n terms) $= 0$, hence $o(a)$ is infinite.

Naturally if $a^m = e$, then the order of a, say n, must divide m. Let us see how it goes.

Proposition 1.10 Let G be a group and $a \in G$ such that $o(a) = n$. If $a^m = e$, then n divides m.

Proof : By division algorithm, there exist integers q and r such that

$$m = nq + r \text{ where } 0 \leq r < n$$

Now $a^m = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$.

Therefore $a^m = e \Longrightarrow a^r = e$. Hence $r = 0$ because otherwise $r < n = o(a)$ such that $a^r = e$ which is not possible. Thus $m = nq$, i.e. n divides m.

Now an interesting question: Is there any relationship between the order of an element $a \in G$ and the order of a^{-1}? We have the following answer.

Proposition 1.11 The order of a^{-1} is the same as that of a.

Proof: Let us suppose that $o(a) = n$ and $o(a^{-1}) = m$.

Now $o(a) = n \Longrightarrow a^n = e \Longrightarrow (a^n)^{-1} = e^{-1} \Longrightarrow (a^{-1})^n = e$

But $(a^{-1}) = m$, hence n cannot be less than m, i.e. $n \geq m$

Also $o(a^{-1}) = m \Longrightarrow (a^{-1})^m = e \Longrightarrow (a^m)^{-1} = e \Longrightarrow a^m = e \Longrightarrow m \geq n$

Now $n \geq m$ and $m \geq n \Longrightarrow m = n$. Thus the order of a^{-1} is the same as that of a. If the order of a is infinite, then the order of a^{-1} is also infinite.

1.7 Summary

We conclude with summarizing what we have covered in this unit. We:

(1) Introduced a binary operation on a nonempty set as a function. Also discussed associative law and commutative law.

(2) Defined Group as an algebraic structure following axioms (i) Closure property (ii) Associative law (iii) existence of identity and (iv) existence of inverse. We defined abelian group as a group satisfying commutative law.

(3) Discussed various examples of groups and abelian groups.

(3) Discussed elementary properties of groups.

(4) Introduced the relation of congruence modulo n and the residue classes. We then discussed groups of residue classes $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^{\times}$. We also introduced operations addition modulo n $(+_n)$ and multiplication modulo n $(\times_n)$ and discussed the groups $\mathbb{Z}_n$ and $\mathbb{U}_n$. Discussed some other special groups such as Group of nth roots of unity, Permutation group, Klein's four group and Quaternion group (Hamiltonian group).

(5) Defined integral powers of an element $a \in G$ of a group $(G,*)$ as

$a^n = a * a * ... * a$ upto n factors, $n = 1,2,3, ...$ and $a^0 = e$ (the identity of G) . Then we introduced the notion of order of an element $a \in G$ as the least positive integer n such that $a^n = e$. We illustrated the concept with some examples.

1.8 Self assessment questions

(1) Define a binary operation $*$ on $\mathbb{Z}$ by $a * b = a + b - 2$. Show that $(\mathbb{Z},*)$ is an abelian group.

(2) Show that the set of all $m \times n$ matrices having their elements as real numbers is an infinite abelian group with respect to addition of matrices?

(3) Show that the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where $\alpha \in \mathbb{R}$ forms a group under matrix multiplication.

(4) Construct the composition table and show that the set of fourth roots of unity $\{1, -1, i, -i\}$ forms a group with respect to multiplication.

(5) Show that in a group G the left identity is also the right identity.

$$ea = a \Longrightarrow ae = a \text{ for all } a \in G$$

Also the left inverse of an element is also its right inverse.

$$a^{-1}a = e \Longrightarrow aa^{-1} = e$$

(6) Let $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where f_i $(i = 1,2, \dots, 6)$ are transformations on the set of complex numbers such that $f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = 1 - z$, $f_4(z) = \frac{z}{z-1}$, $f_5(z) = \frac{1}{1-z}$ and $f_6(z) = \frac{z-1}{z}$. Show that G forms a finite non-abelian group with respect to composite (product) of two functions.

(7) Construct a composition table for $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ under $+_6$ and show that $(\mathbb{Z}_6, +_6)$ is a finite abelian group.

(8) Show that $(\{1,3,4,5,9\}, \times_{11})$ is an abelian group.

(9) Show that the set V of all vectors in 3-dimensional space is an infinite abelian group under vector addition.

(10) Prove that a set G with a binary operation denoted multiplicatively is a group if and only if (i) the associative law holds (ii) for every pair of elements $a, b \in G$, the equations $ax = b$ and $ya = b$ have solutions in G.

(11) Let $f, g \in S_3$ such that $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
Compute (i) $fg^{-1}f$, (ii) f^3 and (iii) the orders of the elements f and g.
[Ans. (i) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ (iii) $o(f) = 3, o(g) = 2$]
(12) Show that the order of every element of a finite group is finite and is less than or equal to the order of the group.
(13) Let G be a group and $a, x \in G$. Then show that the orders of the elements a and $x^{-1}ax$ are the same.
(14) If a is an element of order n and p is prime to n, then show that $o(a^p) = n$.
(15) Prove that if G is an abelian group then $(ab)^n = a^n b^n$ for all $a, b \in G$ and for all integers n.
(16) Let G be a group and $a, b \in G$. Then $(ab)^2 = a^2 b^2$ if and only if the group G is abelian.

1.9 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

Unit-2: Homomorphism, Subgroups and Cyclic Groups

Structure

2.1 Introduction

In Unit 1, we defined and studied algebraic structure called group. We studied its properties and discussed many examples. To put it simply, a group is a non-empty set equipped with a binary operation satisfying certain axioms. Suppose we are given two different groups $(G,*)$ and $(G',*')$. Are there tools to check if they are structurally the same? Yes, we have some special mappings between the groups which can do this job, i.e. relate the group structure of G to the group structure of G' . For instance, consider the multiplicative group of fourth roots of unity, i.e. $G = \{1,-1,i,-i\}$ and additive group of integers modulo 4, i.e. $(\mathbb{Z}_4,+_4)$. These groups appear to be different in the sense they have different elements and they are groups under different binary operation. But if you look into the following composition tables of these groups, you find a common structure hidden in both the groups.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$+_4$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

Here you see that the composition tables for both the groups are identical. If we replace $1,-1,i,-i$ by 0,2,1,3 respectively in the composition table for G, we obtain the composition table for $\mathbb{Z}_4$. We can say that both the groups are abstractly identical.

Here we see that the element $i \in G$ corresponds to $1 \in \mathbb{Z}_4$ and $-i \in G$ corresponds to $3 \in \mathbb{Z}_4$. Interestingly, $i.(-i) = 1$ occupies the cell (3,4) in the composition table for G and $1+_4 3 = 0$ occupies the same cell position in the composition table for $\mathbb{Z}_4$. Thus $i.(-i)$ also corresponds to

$1+_4 3$. Thus if we define a function $f: G \longrightarrow \mathbb{Z}_4$ such that $f(1) = 0, f(-1) = 2,\ f(i) = 1$ and $f(-i) = 3$, then $f\{i.(-i)\} = f(1) = 0 = 1+_4 3 = f(i)+_4 f(-i)$

i.e. $f\{i.(-i)\} = f(i)+_4 f(-i)$. Similarly $f\{i.(-1)\} = f(i)+_4 f(-1)$ and so on. Thus there exists a function $f: G \longrightarrow \mathbb{Z}_4$ such that $f(xy) = f(x)+_4 f(y)$ for all $x, y \in G$. The mapping between the groups satisfying this composition preserving property is called a homomorphism. In our example, the homomorphism $f: G \longrightarrow \mathbb{Z}_4$ is one-to-one and onto. Such homomorphisms are called isomorphisms. In this unit, we shall define these mappings formally and discuss their properties.

One way to unravel the structure of a group is to study the subsets of that group which are groups themselves. Such subsets are called subgroups of that group. We shall study these subgroups in details and establish some criteria to decide when a given subset of a group is a subgroup. Finally, we discuss special groups which are generated by an element of that group. We call such groups 'cyclic' and they have some very interesting properties. So here we have the objectives of this unit-

2.2 Objectives

After reading this unit, you should be able to

- Define the concept of homomorphism and isomorphism
- Describe the isomorphic groups
- Define a subgroup of a given group
- Identify different subgroups
- Define a cyclic group
- Calculate number of generators of a cyclic group
- Find subgroups of a cyclic group
- Define the subgroups generated by a subset of a group.

2.3 Homomorphism and isomorphism

We are interested in mappings $f: G \longrightarrow G'$, such that we could get information (for example "of being abelian") about G' via f when information about G is given. One such mapping is homomorphism or group homomorphism. It is a mapping which respects binary operations defined on two groups. Let us define it more formally:

Definition: Let $(G,*)$ and $(G',*')$ be any two groups. A mapping $f: G \longrightarrow G'$is called **homomorphism** if it preserves the compositions in G and G', i.e.

$$f(a * b) = f(a) *' f(b) \text{ for all } a, b \in G$$

Here you see that the element $a * b$ belongs to G and the element $f(a) *' f(b)$ belongs to G'. Thus above equation gives a relation between these two binary operations $*$ and $*'$. In other words, this mapping f relates the two group structures.

When there is no confusion regarding the binary compositions, we denote both the group operations multiplicatively. So the above condition becomes

$$f(ab) = f(a)f(b) \text{ for all } a, b \in G$$

Definition: A homomorphism $f: G \longrightarrow G'$ is called an **epimorphism** iff f is surjective (i.e. onto) and then the group G' is said to be a **homomorphic image** of the group G.

Definition: A homomorphism $f: G \longrightarrow G'$ is called an **monomorphism** iff f is injective (i.e. one to one).

Definition: A homomorphism $f: G \longrightarrow G$ of a group G into itself is called an **endomorphism.**

Now we define a very important mapping between groups which makes two groups abstractly identical.

Definition: A mapping $f: G \longrightarrow G'$is called an **isomorphism** if

(1) f is a homomorphism, i.e. $f(ab) = f(a)f(b)$ for all $a, b \in G$

(2) f is a bijection, i.e. one to one and onto

Then the group G is said to be **isomorphic** to the group G' and we write $G \cong G'$.

An isomorphism of a group G onto itself is called an **automorphism** of G.

In other words, the groups G and $G'$are isomorphic if there is a bijection between them which preserves compositions. Abstractly isomorphic groups are regarded as same, i.e. if the group G has some property derivable from group axioms, then G' also has the same property. Let us illustrate these concepts with some examples.

2.4 Examples of homomorphism and isomorphism

Example 2.4.1 The mapping $f: \mathbb{C} \longrightarrow \mathbb{R}$ given by $f(z) = Re(z)$ for all $z \in \mathbb{C}$ is a homomorphism of the additive group of complex numbers onto the additive group of real numbers.

Let $z_1, z_2 \in \mathbb{C}$ such that $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then $f(z_1) = x_1$ and $f(z_2) = x_2$. Now $z_1 + z_2 = (x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2)$. Hence $Re(z_1 + z_2) = x_1 + x_2$. Therefore

$$f(z_1 + z_2) = x_1 + x_2 = f(z_1) + f(z_2)$$

Hence f is a homomorphism.

Example 2.4.2 Let us discuss an endomorphism of the additive group $\mathbb{Z}$ of integers.

Consider a mapping $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $f(x) = 2x$ for all $x \in \mathbb{Z}$.
For $x, y \in \mathbb{Z}$ We have

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

Hence f is a homomorphism of $\mathbb{Z}$ into itself, i.e. f is an endomorphism.

Example 2.4.3 Consider the multiplicative group $G = \{\dots, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, \dots\}$. The mapping $f: \mathbb{Z} \longrightarrow G$ defined by $f(x) = 3^x$ for all $x \in \mathbb{Z}$ is an isomorphism from the additive group $(\mathbb{Z}, +)$ onto the multiplicative group $(G, \cdot)$. Let us see how.

(1) f is a homomorphism, i.e. f preserves compositions: Let $x, y \in \mathbb{Z}$.

Then $f(x+y) = 3^{x+y} = 3^x \cdot 3^y = f(x) \cdot f(y)$

(2) f is a bijection: Let $a, b \in \mathbb{Z}$. Then

$$f(a) = f(b) \Longrightarrow 3^a = 3^b \Longrightarrow a = b$$

Hence f is one to one.

Also $y \in G$, then $y = f(x) \Longrightarrow y = 3^x \Longrightarrow x = \log_3 y$. Obviously $\log_3 y \in \mathbb{Z}$ for every $y \in G$, i.e. $y \in G \Longrightarrow \exists \log_3 y \in \mathbb{Z}$ such that $f(\log_3 y) = 3^{\log_3 y} = y$. Hence f is onto.

Therefore f is an isomorphism of $\mathbb{Z}$ onto G. Hence the additive group of integers is isomorphic to the multiplicative group G, i.e. $\mathbb{Z} \cong G$.

Example 2.4.4 The additive group of all real numbers $(\mathbb{R}, +)$ is isomorphic to the multiplicative group of all positive real numbers $(\mathbb{R}^+, \cdot)$. The exponential map $f: \mathbb{R} \longrightarrow \mathbb{R}^+$defined by $f(x) = e^x$ for all $x \in \mathbb{R}$ is an isomorphism.

(1) f is a homomorphism: Let $x, y \in \mathbb{R}$.

Then $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$

(2) f is a bijection: Let $a, b \in \mathbb{R}$. Then

$$f(a) = f(b) \Longrightarrow e^a = e^b \Longrightarrow \ln e^a = \ln e^b \Longrightarrow a = b$$

Hence f is one to one.

Also $y \in \mathbb{R}^+ \Longrightarrow \exists \ln y \in \mathbb{R}$ such that $f(\ln y) = e^{\ln y} = y$. Hence f is onto.

Therefore $\mathbb{R} \cong \mathbb{R}^+$.

Example 2.4.5 Now we show that the multiplicative group of nth roots of unity is isomorphic to the additive group of integers modulo n, i.e. $(\mathbb{Z}_n, +_n)$.

Let $G = \{1 = \zeta^0, \zeta, \zeta^2, \ldots\ldots, \zeta^{n-1}\}$ be the group of nth roots of unity, where $\zeta = e^{2\pi i/n}$. We have $\mathbb{Z}_n = \{0,1, \ldots, n-1\}$. Let us define a mapping $\varphi: G \longrightarrow \mathbb{Z}_n$ by $\varphi(\zeta^r) = r$, where $r = 0,1, \ldots, n-1$.

(1) φ is a homomorphism: Let $\zeta^r, \zeta^s \in G$, hence
$\varphi(\zeta^r \zeta^s) = \varphi(\zeta^{r+s}) = \varphi(\zeta^k) = k$ where $k \equiv r + s \pmod{n}$, i.e. $k = r +_n s$
Thus $\varphi(\zeta^r \zeta^s) = r +_n s = \varphi(\zeta^r) +_n \varphi(\zeta^s)$
(2) φ is a bijection: Let $\zeta^r, \zeta^s \in G$, then $\varphi(\zeta^r) = \varphi(\zeta^s) \Longrightarrow r = s$

$$\Longrightarrow e^{2\pi i r/n} = e^{2\pi i s/n}$$
$$\Longrightarrow \zeta^r = \zeta^s$$

Hence φ is one-one. Since the number of elements in G is equal to the number of elements in $\mathbb{Z}_n$, therefore φ must be onto. Thus φ is a bijection.
Therefore $\varphi: G \longrightarrow \mathbb{Z}_n$ is an isomorphism of G onto $\mathbb{Z}_n$, i.e. $G \cong \mathbb{Z}_n$.

2.5 Some properties of homomorphism

Proposition 2.1 Let f be a homomorphism of a group G into a group G', then

(i) The identity e of G is mapped onto the identity e' of G', i.e. $e' = f(e)$

(ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof (i) Let $a \in G$, then $f(a) \in G'$. Since e' is the identity of G', hence

$$e'f(a) = f(a) = f(ea) = f(e)f(a)$$

The right cancellation law in G' gives $e' = f(e)$.

(ii) We have $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$,

$$\Longrightarrow f(a^{-1}) = [f(a)]^{-1}.$$

Proposition 2.2 Let $f: G \longrightarrow G'$ be an isomorphism of a group G onto a group G'. Let $a \in G$, then $o(a) = o[f(a)]$.

Proof: Suppose $o(a) = n$ and $[f(a)] = m$. Then

$$a^n = e \Longrightarrow f(a^n) = f(e)$$

$$\Longrightarrow f(aa \ldots n \text{ times}) = e', \text{ since } e' = f(e)$$

$$\Longrightarrow f(a)f(a) \ldots . n \text{ times} = e', \text{ since } f \text{ is a homomorphism}$$

$$\Longrightarrow [f(a)]^n = e'$$

$$\Longrightarrow \ m \leq n$$

Example: Let $f: G \longrightarrow G'$ be defined as $f(x) = e', \forall\ x\ \in G$, then f is a homomorphism.

Again $o[f(a)] = m \Longrightarrow [f(a)]^m = e'$

$$\Longrightarrow f(a)f(a) \ldots . m \text{ times} = e'$$

$$\Longrightarrow f(aa \ldots m \text{ times}) = e'$$

$$\Longrightarrow f(a^m) = f(e) \text{ as } \ e' = f(e)$$

$$\Longrightarrow a^m = e \text{ , since } f \text{ is an isomorphism and hence one-one}$$

$$\Longrightarrow \ n \leq m$$

Thus $m \leq n$ and $n \leq m \Longrightarrow m = n$.

Example: Let $f: G \longrightarrow G'$ be defined as $f(x) = x, \forall\ x\ \in G$, then f is a isomorphism

We shall make a detailed study of homomorphism theorems in Block-II

2.6 Subgroups of a group

Sometimes you see a group inside the group table of a given group. For example, if you observe the group table of the multiplicative group $\{1, -1, i, -i\}$, the shaded section indicates the presence of another multiplicative group $\{-1,1\}$. This group is called a subgroup of the original group.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Now we shall make a detailed study of these subgroups.

Definition: Let $(G,*)$ be a group and H be a non-empty set subset of G then a binary operation $*_H: H \times H \longrightarrow H$ is said to be the restriction of '$*$' or **binary operation on H induced by '$*$'** if $a *_H b = a * b$ for all $a, b \in H$.

Definition: Let $(G,*)$ be a group and H be a non-empty set subset of G then H is said to be a **subgroup** of G, if

(1) H is closed with respect to $*$, i.e. $a * b \in H$ for all $a, b \in H$.

(2) H is itself a group with respect to binary operation '$*_H$' induced by **'$*$'.**

If H is a subgroup of G, we denote it as $H \leq G$. If H is a subgroup of G and $H \neq G$, we shall write $H < G$. Since the binary operation is restricted to a subset of G, we may denote both the operations **'$*$'** and '$*_H$' multiplicatively.

Example 2.6.1 The additive group of integers $(\mathbb{Z}, +)$ is a subgroup of additive group of rational numbers $(\mathbb{Q}, +)$, i.e. $\mathbb{Z} \leq \mathbb{Q}$. Similarly $\mathbb{Q} \leq \mathbb{R}$ under operation of addition.

Example 2.6.2 Consider the set $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ of all even integers. You can verify that it is a group under addition. Hence $E \leq \mathbb{Z}$.

What about the set O of odd integers? Certainly Not. Even the closure property is not satisfied, i.e. $3 + 5 = 8 \notin O$.

Example 2.6.3 The multiplicative group $\{-1,1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$**.**

Example 2.6.4 The subset $A_3 = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$ is a subgroup of symmetric group S_3.

Example 2.6.5 In unit 1, we have shown that the set $G = \{1 = \zeta^0, \zeta, \zeta^2, \ldots\ldots, \zeta^{n-1}\}$ of nth roots of unity forms a group under multiplication. It is a subgroup of the group $(\mathbb{C}_{\neq 0}, \cdot)$ of nonzero complex numbers under multiplication.

For any group G we have $G \subseteq G$, Hence G itself is a subgroup of G. Also if e is the identity element of G, the set $\{e\}$ is also a subgroup of G. These two subgroups G and $\{e\}$ are called **trivial or improper subgroups**. The subgroups other than these two are called **proper subgroups.**

Proposition 2.3 Let H be a subgroup of a group G. Then

(i) The identity of H is the same as that of G.

(ii) The inverse of $a \in H$ is the same as the inverse of a in G.

Proof: (i) Let e and e_H be the identities of G and H respectively. Let $a \in H$. Then $a \in G$ as $H \subseteq G$.

Now $ea = a$, since e is the identity of G.

Also $a \in H \Longrightarrow ae_H = a$, since e_H is the identity of H.

Therefore $e_H = ae \Longrightarrow e_H = e$, by left cancellation law in G.

(ii) Let $a \in H$. Let b be the inverse of a in H and c be its inverse in G. Then we have $ab = e$ and $ac = e$ (since e is the identity for both G and H).

Hence $= ac \Longrightarrow b = c$, by left cancellation law in G.

The subsets of a group are also quite interesting. A non-empty subset K of a group G is called a **complex** of G.

Definition: If H and $K$are two complexes of a group, then we define

$$HK = \{x \in G : x = hk, h \in H, k \in K\}$$

Since $h \in H, k \in K \Longrightarrow h, k \in G \Longrightarrow hk \in G$, hence $HK \subseteq G$.

and $H^{-1} = \{h^{-1} : h \in H\}$

We can show that the multiplication of complexes is associative.

If H_1, H_2 and $H_3$are any three complexes of G and $h_1 \in H_1, h_2 \in H_2$ and $h_3 \in H_3$, then $h_1(h_2h_3) \in H_1(H_2H_3)$. Since $h_1(h_2h_3) = (h_1h_2)h_3 \in (H_1H_2)H_3$, hence $H_1(H_2H_3) \subseteq (H_1H_2)H_3$. Similarly we can show that $(H_1H_2)H_3 \subseteq H_1(H_2H_3)$. Thus $H_1(H_2H_3) = (H_1H_2)H_3$.

Let us have some examples to illustrate these concepts. Consider the multiplicative group of fourth roots of unity,i.e. $G = \{1, -1, i, -1\}$. Let $H, K \subseteq G$, such that $H = \{1, i\}$, $K = \{i, -i, -1\}$. Then

$$HK = \{1i, 1(-i), 1(-1), ii, i(-i), i(-1)\} = \{i, -i, -1, 1\}$$

$$H^{-1} = \{1^{-1}, i^{-1}\} = \{1, -i\}$$

Proposition 2.4 $H_1$and H_2 are any two complexes of G, then $(H_1H_2)^{-1} = {H_2}^{-1}{H_1}^{-1}$.

Proof: Let $x \in (H_1H_2)^{-1}$ then there exist $h_1 \in H_1$, $h_2 \in H_2$ such that

$$x = (h_1h_2)^{-1} = {h_2}^{-1}{h_1}^{-1} \in {H_2}^{-1}{H_1}^{-1}$$

Hence $(H_1H_2)^{-1} \subseteq {H_2}^{-1}{H_1}^{-1}$. Similarly we can show that ${H_2}^{-1}{H_1}^{-1} \subseteq (H_1H_2)^{-1}$. Therefore $(H_1H_2)^{-1} = {H_2}^{-1}{H_1}^{-1}$.

Proposition 2.5 If H is any subgroup of a group G, then $H^{-1} = H$.

Proof: Let $h^{-1} \in H^{-1}$. Then $h \in H$. Since H is a subgroup, hence $h \in H \Longrightarrow h^{-1} \in H$. Thus $h^{-1} \in H^{-1} \Longrightarrow h^{-1} \in H$. Therefore $H^{-1} \subseteq H$.

Also $h \in H \Longrightarrow h^{-1} \in H \Longrightarrow (h^{-1})^{-1} \in H^{-1} \Longrightarrow h \in H^{-1}$, i.e. $H \subseteq H^{-1}$.

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

Now we shall prove an important criterion which may serve to test whether a given non-empty subset H of a group G is a subgroup of G.

Proposition 2.6 A non-empty subset H of a group G is a subgroup of G if and only if

$$a, b \in H \Longrightarrow ab^{-1} \in H \text{ for all a, b } \in H$$

Proof: Let us first suppose that H is a subgroup of G. Then

$$a \in H, b \in H \Longrightarrow a \in H, b^{-1} \in H$$

$$\Longrightarrow ab^{-1} \in H$$

Conversely, suppose that H is a non-empty subset of a group G such that

$$a, b \in H \Longrightarrow ab^{-1} \in H$$

Hence $a \in H, a \in H \Longrightarrow aa^{-1} \in H \Longrightarrow e \in H$, i.e. the identity element $e \in H$.

Now $e \in H, a \in H \Longrightarrow ea^{-1} \in H \Longrightarrow a^{-1} \in H$, each element of H has its inverse in H.

Also $a \in H, b \in H \Longrightarrow a \in H, b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} \in H$, by the given condition

$$\Longrightarrow ab \in H$$

Hence H is closed under composition in G.

The elements of H are none but the elements of G and the associative law holds in G, therefore it must also hold in H.

Thus we see that the given condition implies that H is a subgroup of G.

Note: In case of additive groups, we have $b^{-1} = -b$, hence above criterion becomes: A non-empty subset H of a group G is a subgroup of G if and only if

$$a, b \in H \Longrightarrow a - b \in H$$

Proposition 2.7 A non-empty finite subset H of a group G is a subgroup of G if and only if H is closed under given composition, i.e. $a, b \in H \Longrightarrow ab \in H$.

Proof: Suppose H is a subgroup of G, then obviously H is closed under given composition, i.e. $a, b \in H \Longrightarrow ab \in H$.

Conversely, suppose that H is a non-empty finite subset of a group G such that obviously H is closed under given composition, i.e. $a, b \in H \Longrightarrow ab \in H$. We show that H is a subgroup of G.

The associative law holds in H as it holds in G. Now it remains to show that $e \in H$ and $a \in H \Longrightarrow a^{-1} \in H$.

Let $a \in H$. Then by closure property (which is assumed here) all the elements a, a^2, a^3 ... belong to H. Since H is finite, hence all these elements are not distinct. Hence for some positive integers r and s $(r > s)$, we have

$$a^r = a^s \Longrightarrow a^{r-s} = e$$

Now $r - s > 0$ hence $a^{r-s} \in H$ (as all positive powers of a belong to H). Therefore $e \in H$.

Since $r - s > 0 \Longrightarrow r - s \geq 1 \Longrightarrow r - s - 1 \geq 0$.

Now $aa^{r-s-1} = a^{r-s} = e \Longrightarrow a^{r-s-1}$ is the inverse of a.

Thus H is a group in itself under the composition in G, i.e. H is a subgroup of G.

Example 2.6.6 For any $m \in \mathbb{N}$, $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

We shall use the above criterion to show that $m\mathbb{Z}$ is a subgroup.

Since $0 \in m\mathbb{Z}$, hence $m\mathbb{Z}$ is non-empty. Let $a, b \in m\mathbb{Z}$ then there exist $r, s \in \mathbb{Z}$ such that $a = mr$ and $b = ms$. Now $a - b = mr - ms = m(r - s) \in m\mathbb{Z}$ as $r - s \in \mathbb{Z}$. Hence $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Example 2.6.7 We have seen in unit 1 that the general linear group of degree n, i.e. $GL_n(\mathbb{R})$ is a group under matrix multiplication, where

$$GL_n(\mathbb{R}) = \{A : A \text{ is an } n \times n \text{ matrix with entries from } \mathbb{R} \text{ and } \det(A) \neq 0\}$$

Let us define a subset of $GL_n(\mathbb{R})$ as $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$ We shall show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$, then $\det(A) = 1$ and $\det(B) = 1$.

Now $\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\frac{1}{\det(B)} = 1$

Moreover $A, B \in SL_n(\mathbb{R}) \Longrightarrow A, B \in GL_n(\mathbb{R}) \Longrightarrow AB^{-1} \in GL_n(\mathbb{R})$, since $GL_n(\mathbb{R})$ is a group. Thus $AB^{-1} \in GL_n(\mathbb{R})$ such that $\det(AB^{-1}) = 1$. Hence $AB^{-1} \in SL_n(\mathbb{R})$, i.e. $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. This subgroup is called special linear group of degree n.

2.7 Properties of subgroups

Proposition 2.8 A non-empty subset H of a group G is a subgroup of G if and only if $HH^{-1} = H$

Proof: First suppose that H is a subgroup of G. Let $c \in HH^{-1}$ then $c = ab^{-1}$ for some $a, b \in H$. Now H is a subgroup, hence $a, b \in H \Longrightarrow ab^{-1} \in H$, i.e. $c \in H$. Thus $HH^{-1} \subseteq H$. Also if $h \in H$, then $h = he = he^{-1} \in HH^{-1}$, i.e. $H \subseteq HH^{-1}$. Therefore $HH^{-1} = H$.

Conversely, suppose that $HH^{-1} = H$, hence $HH^{-1} \subseteq H$. Now $ab^{-1} \in HH^{-1}$ for some $a, b \in H$. Since $HH^{-1} \subseteq H$, hence $ab^{-1} \in HH^{-1} \Longrightarrow ab^{-1} \in H$. Thus $a, b \in H \Longrightarrow ab^{-1} \in H$, i.e. H is a subgroup of G.

Proposition 2.9 If H_1 and H_2 are two subgroups of a group G, then H_1H_2 is a subgroup of G, if and only if $H_1H_2 = H_2H_1$.

Proof: Let us first suppose that $H_1H_2 = H_2H_1$. We know that H is a subgroup of G if $HH^{-1} = H$. Hence to show that H_1H_2 is a subgroup of G, we have to show that $(H_1H_2)(H_1H_2)^{-1} = H_1H_2$.

Now $(H_1H_2)(H_1H_2)^{-1} = (H_1H_2)(H_1H_2)^{-1}$

$= (H_1H_2)\left(H_2{}^{-1}H_1{}^{-1}\right)$ since $(H_1H_2)^{-1} = H_2{}^{-1}H_1{}^{-1}$

$= [H_1\left(H_2H_2{}^{-1}\right)]H_1{}^{-1}$ by associativity

$= (H_1H_2)H_1{}^{-1}$, since H_2 is a subgroup, $H_2H_2{}^{-1} = H_2$

$= (H_2H_1)H_1{}^{-1}$, since $H_1H_2 = H_2H_1$

$= H_2\left(H_1H_1{}^{-1}\right)$

$= H_2H_1$, since H_1 is a subgroup, $H_1H_1{}^{-1} = H_1$

$= H_1H_2$

Conversely, suppose that H_1H_2 is a subgroup of G. Then

$$(H_1H_2)^{-1} = H_1H_2 \Longrightarrow H_2{}^{-1}H_1{}^{-1} = H_1H_2 \Longrightarrow H_2H_1 = H_1H_2$$

This completes the proof.

We can infer the following result from above proposition-

If H_1 and H_2 are two subgroups of an abelian group G, then H_1H_2 is a subgroup of G.

Proposition 2.10 If H_1 and H_2 are subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof: Since $e \in H_1$ and $e \in H_2$, hence $e \in H_1 \cap H_2$. Hence $H_1 \cap H_2 \neq \emptyset$. Let $a, b \in H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$. Now H_1 and H_2 are subgroups, hence $a, b \in H_1 \Longrightarrow ab^{-1} \in H_1$ and $a, b \in H_2 \Longrightarrow ab^{-1} \in H_2$.

Finally $ab^{-1} \in H_1$ and $ab^{-1} \in H_2 \Longrightarrow ab^{-1} \in H_1 \cap H_2$.

Thus $a, b \in H_1 \cap H_2 \Longrightarrow ab^{-1} \in H_1 \cap H_2$, i.e. $H_1 \cap H_2$ is a subgroup of G.

Now you may ask whether the union of two subgroups is also a subgroup. Not necessarily. For example, $2\mathbb{Z}$ and $3\mathbb{Z}$ are subgroups of $\mathbb{Z}$ under addition. Now

$$2\mathbb{Z} \cup 3\mathbb{Z} = \{\dots, -4, -3, -2, 0, 2, 3, 4, \dots\}$$

You can observe that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not closed under addition as $3,4 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ but $3 + 4 = 7 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Therefore $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$. Hence If $H_1$and H_2 are subgroups of a group G, then $H_1 \cup H_2$ is not necessarily a subgroup of G. The next proposition tells you the situation in which $H_1 \cup H_2$ is a subgroup.

Proposition 2.11 The union of two subgroups is a subgroup if and only if one is contained in the other.

Proof Let $H_1$and H_2 be two subgroups of a group G. First suppose that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Then either $H_1 \cup H_2 = H_2$ or $H_1 \cup H_2 = H_1$. But $H_1$and H_2 be two subgroups and hence $H_1 \cup H_2$ is also a subgroup.

Conversely, suppose that $H_1 \cup H_2$ is also a subgroup. Now to prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$, assume on the contrary that $H_1 \nsubseteq H_2$ and $H_2 \nsubseteq H_1$.

$H_1 \nsubseteq H_2 \Longrightarrow$ there is an element $a \in H_1$ such that $a \notin H_2$

and $H_2 \nsubseteq H_1 \Longrightarrow$ there is an element $b \in H_2$ such that $b \notin H_1$

Now $a \in H_1$ and $b \in H_2 \Longrightarrow a, b \in H_1 \cup H_2 \Longrightarrow ab \in H_1 \cup H_2$ since $H_1 \cup H_2$ is a subgroup.

$ab \in H_1 \cup H_2 \Longrightarrow ab \in H_1$ or $ab \in H_2$

Since $a \in H_1 \Longrightarrow a^{-1} \in H_1$, hence if $ab \in H_1$, then we have

$$a^{-1} \in H_1, ab \in H_1 \Longrightarrow a^{-1}(ab) \in H_1 \Longrightarrow (a^{-1}a)b \in H_1 \Longrightarrow eb \in H_1 \Longrightarrow b \in H_1$$

Which is not possible as $b \notin H_1$.

Again if $ab \in H_2$ then

$$b \in H_2, ab \in H_2 \Longrightarrow b^{-1} \in H_2, ab \in H_2 \Longrightarrow (ab)b^{-1} \in H_2 \Longrightarrow a(bb^{-1}) \in H_2$$

$$\Longrightarrow ae \in H_2 \Longrightarrow a \in H_2$$

Which is also not possible as $a \notin H_2$. Hence our assumption that $H_1 \nsubseteq H_2$ and $H_2 \nsubseteq H_1$ is wrong and we must have either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proposition 2.12 Arbitrary intersection of subgroups of a group is a subgroup.

Proof: Let G be a group and let $\{H_t : t \in T\}$ be a family of subgroups of G. Where T is an index set. We have to show that the intersection of this family, $\bigcap_{t \in T} H_t$, is a subgroup of G. Since $e \in H_t$ for all $t \in T$, hence $e \in \bigcap_{t \in T} H_t$, i.e. $\bigcap_{t \in T} H_t$ is non-empty. Let $a, b \in \bigcap_{t \in T} H_t$,then $a, b \in H_t$ for all $t \in T$.

Now H_t is a subgroup for all $t \in T$, hence

$$a, b \in H_t \Longrightarrow ab^{-1} \in H_t \text{ for all} t \in T$$

$$\Longrightarrow ab^{-1} \in \bigcap_{t\in T} H_t$$

Thus $a, b \in \bigcap_{t\in T} H_t \Longrightarrow ab^{-1} \in \bigcap_{t\in T} H_t$. Consequently $\bigcap_{t\in T} H_t$ is a subgroup of G.

2.8 Cyclic Groups

Sometimes, you observe that every element of a group G can be written in the form of a^n for some $a \in G$, where n is any integer. For example, the multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity can be written as $G = \{i^4, i^2, i^1, i^3\}$. In this section, we shall study such groups.

Definition: A group G is called **cyclic** if every element of G is of the form a^n for some $a \in G$, where n is any integer. The element a is then called a **generator** of G. i.e.

$$G = \{a^n : n \in \mathbb{Z}\}$$

In additive notation, a group G is cyclic if $G = \{na : n \in \mathbb{Z}\}$. Thus a group G is cyclic if it can be generated by a single element. If G is cyclic group with a generator a, then we write $G = \langle a \rangle$ and say that G is generated by a.

A cyclic group may have more than one generator. For example, the group of cube roots of unity has ω and ω^2 as its generators, i.e.

$$G = \{1, \omega, \omega^2\} = \{\omega^3, \omega, \omega^2\} = \langle \omega \rangle$$

and $G = \{1, \omega, \omega^2\} = \{(\omega^2)^3, (\omega^2)^2, \omega^2\} = \langle \omega^2 \rangle$

Let us have some more examples.

Example 2.8.1

(1) The additive group of integers $\mathbb{Z}$ is a cyclic group as $\mathbb{Z} = \langle 1 \rangle$. Also since every integer x can be written as $(-x)(-1)$, hence $\mathbb{Z} = \langle -1 \rangle$.

(2) The additive group of integers modulo 6, i.e. $(\mathbb{Z}_6, +_6)$ is generated by 1 as $1 = 1^1$, $2 = 1 +_6 1 = 1^2$, $3 = 1^3$,$4 = 1^4$, $5 = 1^5$ and $0 = 1^6$. Here 5 is another generator as $1 = 5^5$, $2 = 5^4$, $3 = 5^3$, $4 = 5^2$, $5 = 5^1$, $0 = 5^6$.

(3) The group $\mathbb{U}_{10} = \{1,3,7,9\}$ under multiplication modulo10 is a cyclic group with generators 3 and 7 as $\mathbb{U}_{10} = \{1,3,7,9\} = \{3^4, 3^1, 3^3, 3^2\} = \langle 3 \rangle$. Also $\mathbb{U}_{10} = \{1,3,7,9\} = \{7^4, 7^3, 7^1, 7^2\} = \langle 7 \rangle$.

(4)The multiplicative group $G = \{1 = \zeta^0, \zeta, \zeta^2, \ldots\ldots, \zeta^{n-1}\}$ of nth roots of unity is cyclic with a generator $\zeta = e^{2\pi i/n}$.

(5) You can verify that the set of matrices

$$\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}\right\}$$

forms a cyclic group under matrix multiplication with generators $\begin{bmatrix}1 & -1\\ 1 & 0\end{bmatrix}$ and $\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}$.

2.9 Properties of cyclic groups

Proposition 2.13 Let $G = \langle a\rangle$ be a cyclic group with a generator 'a'. Then a^{-1} is also a generator of G, i.e. $G = \langle a^{-1}\rangle$.

Proof Let $x \in G$, then $x = a^r$ for some $r \in \mathbb{Z}$. Now we can write $x = a^r = (a^{-1})^{-r}$. Hence a^{-1} is also a generator of G, i.e. $G = \langle a^{-1}\rangle$.

Proposition 2.14 Every cyclic group is abelian.

Proof Let G be a cyclic group with a generator a, i.e. $G = \langle a\rangle$. Let $x, y \in G$, then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$.

Now $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$ for all $x, y \in G$.

Hence $G = \langle a\rangle$ is abelian.

Note: An abelien group need not be cyclic. For example the Kliens four group $V_4 = \{ e, a, b, c\}$ is abelian but not cyclic.

Proposition 2.15 Let $G = \langle a\rangle$ be a cyclic group generated by a. Then $o(G) = o(a)$, including the case when $o(G)$ is infinite.

Proof: Let $o(a) = n$. First suppose that n is finite, i.e. $n < \infty$. Then the elements $e = a^0, a^1, a^2, \dots\dots, a^{n-1}$ are all distinct, since if $a^r = a^s$, $0 \le r < s < n$, then $a^{r-s} = e$ where $r - s < n$. Which is not possible as n is the smallest positive integer satisfying this property. So G must have at least these n elements.

Now if a^t be any element of G, then by division algorithm, $t = nq + k$, where $0 \le k < n$. Therefore

$$a^t = a^{nq+k} = (a^n)^q a^k = e^q a^k = a^k \in \{e = a^0, a^1, a^2, \dots\dots, a^{n-1}\}$$

Thus each element of G is one of the elements $e = a^0, a^1, a^2, \dots\dots, a^{n-1}$, i.e. G has exactly n elements. Hence $o(G) = n$.

Next suppose that $o(a)$ is infinite, then there exists no integer n such that $a^n = e$. Hence all the powers of a are distinct elements of G, since if $a^r = a^s$, then $a^{r-s} = e$,which is not possible. Thus the order of G is infinite.

Proposition 2.16 A finite group G of order n is cyclic if and only if it contains an element of order n.

Proof First suppose that G is a cyclic group of order n generated by $a \in G$. Then by above proposition, $o(a) = n$.

Conversely, suppose that G is a finite group of order n containing an element b of order n. Then $H = \{b^r : r \in \mathbb{Z}\}$ is a subgroup of G having n distinct elements, i.e.

$$H = \{e = b^0, b^1, b^2, \dots\dots, b^{n-1}\}$$

Since $H \subseteq G$ and $o(H) = n$, $H = G$. Therefore G is a cyclic group generated by b.

Proposition 2.17 Let G be a group and $a \in G$. Then $H = \{a^r : r \in \mathbb{Z}\}$ is a cyclic subgroup of G.

Proof Let $x, y \in H$. Then there exist $r, s \in \mathbb{Z}$ such that $x = a^r$ and $y = a^s$.

Now $xy^{-1} = a^r(a^s)^{-1} = a^r a^{-s} = a^{r-s} \in H$

Hence H is a subgroup of G. Since H is cyclic, this subgroup is a cyclic subgroup of G generated by a.

Definition: A subgroup H of a group G is called a cyclic subgroup generated by a iff there exists an element $a \in G$ such that $H = \{a^r : r \in \mathbb{Z}\}$ and we write $H = \langle a \rangle$.

Proposition 2.18 Every subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group generated by an element $a \in G$. Let H be a subgroup of G. If $H = G$ or $H = \{e\}$, then obviously H is cyclic. Suppose that $H \neq G$ and $H (\neq \{e\})$.

Since $G = \langle a \rangle$, hence each element of H is of the form of a^r where $r \in \mathbb{Z}$. Now $a^r \in H \Longrightarrow (a^r)^{-1} \in H$, i.e. $a^{-r} \in H$. So H always contains positive powers of a. Let $\mathcal{P} = \{n \in \mathbb{Z}^+ : a^n \in H\}$. Then $\mathcal{P}$ is a non-empty set of positive integers. By well ordering principle, $\mathcal{P}$ has a minimum element m (say). Now we show that $H = \langle a^m \rangle$.

Since H is a subgroup and $a^m \in H$, hence $\langle a^m \rangle \leq H$. Let $a^t \in H$, then by division algorithm $t = mq + k$, $0 \leq k < m$.

Now $a^m \in H \Longrightarrow (a^m)^q = a^{mq} \in H \Longrightarrow (a^m)^{-q} = (a^{mq})^{-1} \in H$, hence

$a^k = a^{t-mq} = a^t(a^m)^{-q} \in H,\ k < m$

But m is the least positive integer such that $a^m \in H$, hence $k \not< m$, i.e. $k = 0$. Therefore $t = mq$ and so $a^t = (a^m)^q \in \langle a^m \rangle$. Hence $H \leq \langle a^m \rangle$, which gives $H = \langle a^m \rangle$, i.e. H is a cyclic subgroup of G with generator a^m.

However the converse is not true, i.e. there exist groups which are not cyclic but whose proper subgroups are all cyclic. For instance, the symmetric group S_3 is not cyclic but it has cyclic subgroups, namely,

$$\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle$$

Proposition 2.19 Let G be a cyclic group generated by a and $o(a) = n$ then

(i) G has exactly two generators namely a and a^{-1} if $o(a)$ is infinite (or equivalently G is an infinite cyclic group).

(ii) G is generated by a^m if and only if $(m, n) = 1$, i.e. m and n are relatively prime.

Proof (i) Suppose that $o(a)$ is infinite, i.e. $G = \langle a \rangle$ is an infinite cyclic group generated by a. Hence there does not exist any integer k such $a^k = e$. Now by closure property all the integral powers of a are elements of G, i.e. $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \in G$. No two distinct integral powers of a are equal, for if $a^r = a^s$, then $a^{r-s} = e$,which is not possible as $o(a)$ cannot be finite. Therefore we can write $G = \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$. Also $a^r \in G$ can be written as $a^r = (a^{-1})^{-r}$. Hence a^{-1} is also a generator of G.

Moreover , if a^m is a generator of G where $m \neq \pm 1$. Then $a \in G \Longrightarrow \exists k \in \mathbb{Z}$ such that $a = (a^m)^k = a^{mk}$. Since $m \neq \pm 1$, hence $mk \neq 1$. Therefore two distinct powers of a are equal. Thus we get a contradiction. Hence a^m cannot be a generator of G if $m \neq \pm 1$. Hence G has only two generators, namely a and a^{-1}.

(ii) First suppose that $(m, n) = 1$, then by Euclidean algorithm there exist integers x and y such that $mx + ny = 1$. Hence

$$a^{mx+ny} = a^1 \Longrightarrow a^{mx}a^{ny} = a$$

$$\Longrightarrow (a^m)^x(a^n)^y = a$$

$$\Longrightarrow (a^m)^x = a \text{ as } (a^n)^y = e^y = e$$

Thus each power of a can be expressed as some integral power of a^m, i.e. a^m is a generator of G.

Conversely, suppose that a^m is a generator of G. Hence we have $o(a^m) = n$. Let $(m, n) = d$. Then there exist integers b and c such that $m = bd$ and $n = cd$ and $(b, c) = 1$. Now $(a^m)^c = a^{mc} = a^{bdc} = (a^{dc})^b = (a^n)^b = e^b = e$. Hence $(a^m) \leq c$. Since $c = \frac{n}{d}$, hence if $d \neq 1$, then $c < n$. But then $o(a^m) < n$. Therefore we must have $d = 1$.

The implications of this proposition are interesting. This tells us that the number of generators of a finite cyclic group of order n is equal to number of integers less than n and relatively prime to n. The Euler's totient function $\varphi(n)$, by definition, represents this number.

For example, consider the group $\mathbb{U}_{18}$ under multiplication modulo18. It is a cyclic group of order 6 and we have

$$\mathbb{U}_{18} = \{1,5,7,11,13,17\}$$

Since $5^6 \equiv 1 \pmod{18}$, hence $o(5) = 6$. Therefore 5 is a generator of $\mathbb{U}_{18}$. Now 5^m will be a generator of $\mathbb{U}_{18}$, if m is relatively prime to 6. Since $\varphi(6) = 2$, hence there are two numbers relatively prime to 6,i.e. 1 and 5. Therefore the generators of $\mathbb{U}_{18}$ are 5 and 5^5, i.e. 5 and 11 as $5^5 \equiv 11 \pmod{18}$.

2.10 Subgroups generated by a subset of a group

In the formation of cyclic subgroups of a given group, we have a single element called generator to generate the entire subgroup. You will also notice that the cyclic subgroup $\langle a \rangle$ generated by any element a of a group G is the smallest subgroup of G which contains the set $\{a\}$, i.e. if H is any subgroup which contains $\{a\}$, then H also contain $\langle a \rangle$. We can generalize this

technique to generate a subgroup by an arbitrary subset of a group. So we give the following definition:

Definition: Let A be any subset of a group G. The smallest subgroup of G containing A is called the **subgroup generated by A** and is denoted by $\langle A \rangle$.

We have already seen that the arbitrary intersection of subgroups of a group is a subgroup. Now we show that if we have a family of all subgroups of G containing A, the intersection of this family is the smallest subgroup of G containing A.

Proposition 2.20 If A is any subset of a group G and $\mathcal{F}$ is the family of all subgroups of G containing A, i.e.$\mathcal{F} = \{H: H \leq G, A \subseteq H\}$, then the intersection of this family is the smallest subgroup of G generated by A.

Proof: This family $\mathcal{F}$ is non-empty as $G \in \mathcal{F}$. Let $K = \bigcap_{H \in \mathcal{F}} H = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$ be the intersection of the family of subgroups of a group G containing A. Now

$$A \subseteq H \text{ for all } H \in \mathcal{F} \Longrightarrow A \subseteq \bigcap_{H \in \mathcal{F}} H$$

We know that such an intersection is a subgroup of G. If M is any subgroup of G containing A, then $M \in \mathcal{F}$. Since K is the intersection of all such subgroups, hence each element of $\mathcal{F}$ must contain K, i.e. $K \subseteq M$. Hence K is the smallest subgroup of G generated by A.

In light of above proposition, we can write

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

When $A = \{a_1, a_2, \dots, a_n\}$, we write $\langle A \rangle = \langle a_1, a_2, \dots, a_n \rangle$. If A and B are two subsets of G, then we write $\langle A, B \rangle$ for $\langle A \cup B \rangle$.

If $A = \emptyset$, then $\langle A \rangle = \{e\}$. If $\langle A \rangle = G$, then we say that the group G is **generated by the set** A and the set A is called the **set of generators** of G. If A is finite and $\langle A \rangle = G$ then we say that G is finitely generated.

The following proposition gives an easier way to describe $\langle A \rangle$ than the previous definition.

Proposition 2.21 If A is a non-empty subset of a group G, then

$$\langle A \rangle = \{{a_1}^{n_1} {a_2}^{n_2} \dots {a_k}^{n_k} : k \in \mathbb{Z}^+, a_i \in A \text{ and } n_i = \pm 1 \text{ for each } i\}$$

Proof Let $K = \{{a_1}^{n_1} {a_2}^{n_2} \dots {a_k}^{n_k} : k \in \mathbb{Z}^+, a_i \in A \text{ and } n_i = \pm 1 \text{ for each } i\}$. Then K is the set of all finite products of elements of A and inverses of elements of A. Then $K \neq \emptyset$. Let $x, y \in K$ such that $x = {a_1}^{n_1} {a_2}^{n_2} \dots {a_k}^{n_k}$ and $y = {b_1}^{m_1} {b_2}^{m_2} \dots {b_s}^{m_s}$, then $xy^{-1} = {a_1}^{n_1} {a_2}^{n_2} \dots {a_k}^{n_k} {b_s}^{-m_s} {b_{s-1}}^{-m_{s-1}} \dots {b_1}^{-m_1}$. Hence xy^{-1} is a product of elements of A raised to powers ± 1, therefore $xy^{-1} \in K$. Thus K is a subgroup of G.

Let $a \in A$, then we can write $a = a^1 \in K$. Hence $A \subseteq K$. Since $\langle A \rangle$ is the smallest subgroup containing A, therefore $\langle A \rangle \subseteq K$. Now $\langle A \rangle$ is a group containing A, hence it contains elements of the form ${a_1}^{n_1}{a_2}^{n_2} \ldots {a_k}^{n_k}$, i.e. $K \subseteq \langle A \rangle$. Thus we have $K = \langle A \rangle$.

We observe that the products such as '$aaabbbaba^{-1}$' can be written as $a^3b^2aba^{-1}$. Hence we can also write

$$\langle A \rangle = \{{a_1}^{n_1}{a_2}^{n_2} \ldots {a_k}^{n_k} : k \in \mathbb{Z}^+, a_i \in A, a_i \neq a_{i+1} \text{ and } n_i \in \mathbb{Z} \text{ for each } i\}$$

Example 2.10.1

(1) Consider the symmetric group $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where
$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$,
$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
Then we observe that $f_6 f_2 = f_4$, ${f_2}^2 = f_3$, ${f_2}^3 = f_1$. Hence every member of S_3 is expressible as a product of members of $A = \{f_2, f_6\}$, i.e. $S_3 = \langle f_2, f_6 \rangle$.

(2) The quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is generated by the subset $A = \{i, j\}$ as $ij = k$, $i^3 = -i$, $j^3 = -j$, $k^3 = -k$, $i^2 = -1, i^4 = 1$. Thus $Q_8 = \langle i, j \rangle$.

(3) The set of integers $\mathbb{Z}$ is generated by $\{1\}$, i.e. $\mathbb{Z} = \langle 1 \rangle$.

2.11 Summary

In this unit, we have

(1) Defined homomorphism between groups $(G,*)$ and $(G',*')$ as a composition preserving mapping $f: G \longrightarrow G'$, i.e. $f(a * b) = f(a) *' f(b)$ for all $a, b \in G$.

(2) Defined isomorphism as a bijective homomorphism. The concept of isomorphic groups is discussed with examples. We have more to say on this topic in Block-II

(3) Defined subgroup of a group as a non-empty subset of the group which is a group in itself.

(4) Discussed the properties of subsets (complexes) and subgroups of a group

(5) Defined cyclic group with examples.

(6) Discussed the properties of cyclic group.

(7) Defined the subgroup generated by a subset as the smallest subgroup containing that subset.

2.12 Self assessment questions

(1) Show that the mapping $f: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$ defined by $f(x) = ln(x)$ for all $x \in \mathbb{R}^+$ is an isomorphism.

(2) Show that the additive group of integers $\mathbb{Z}$ is isomorphic to additive group $G = \{\ldots -2m, -m, 0, m, 2m, \ldots\}$ where m is a non-zero integer.

(3) Show that the multiplicative group $G = \{-1,1\}$ is isomorphic to the group (G', o) where $G' = \{f_1, f_2\}$, $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$, $f_2 : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f_1(x) = x$, $f_2(x) = 1 - x$.

(4) Show that the multiplicative group of cube roots of unity is isomorphic to the additive group of residue classes modulo 3.

(5) Show that all those elements of an abelian group G which satisfy the relation $a^2 = e$ constitute a subgroup of G.

(6) Show that every finite group of composite order possesses proper subgroups.

(7) Show that an infinite cyclic group is isomorphic to the additive group of integers.

(8) Show that any cyclic group of order 10 has four generators.

(9) Show that any two cyclic groups of the same order are isomorphic.

(10) Prove that

(i) In the group $\mathbb{Z}_{20}$, $\langle 8,14 \rangle = \{0,2,4, \dots ,18\}$

(ii) In the additive group of integers $\mathbb{Z}$, $\langle 4,19 \rangle = \mathbb{Z}$

(iii) In the additive group of real numbers $\mathbb{R}$,

$$\langle 2, \pi, \sqrt{3} \rangle = \{2a + b\pi + c\sqrt{3} : a, b, c \in \mathbb{Z}\}$$

(11) Does there exists a homomorphism between the Kliens four group V_4 and the additive group of integers?

2.13 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

Unit-3: Coset Decomposition of a Group

Structure

3.1 Introduction

In unit 1, we introduced the notion of congruence modulo n. Let $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{n}$ if and only if n divides $a - b$ or equivalently $a - b$ is an integral multiple of n. Thus $a \equiv b \pmod{n}$ if and only if $a - b \in n\mathbb{Z}$, the subgroup consisting of multiples of n. Hence we see that the congruence between two integers is closely related to the subgroup $n\mathbb{Z}$. Now we shall generalize this congruence relation to any group G and you will observe how a group can be partitioned using this congruence relation.

Definition: Let H be a subgroup of a group G. Let $a, b \in G$. Then a is said to be **left congruent to b modulo H** if and only if $a^{-1}b \in H$. Symbolically

$$a \equiv_L b \pmod{H} \quad \text{if and only if} \quad a^{-1}b \in H$$

and a is said to be **right congruent to b modulo H** if and only if $ab^{-1} \in H$. Symbolically

$$a \equiv_R b \pmod{H} \quad \text{if and only if} \quad ab^{-1} \in H$$

Now we shall see that these relations are equivalence relations in the group G.

Proposition 3.1 The relations subgroup $\equiv_R$ and $\equiv_L$ are equivalence relations in the group G.

Proof: We shall prove the result for $\equiv_R$. A similar proof can be given for $\equiv_L$.

(1) **Reflexivity:** Since H is a subgroup, hence

$$e \in H \Longrightarrow aa^{-1} \in H \Longrightarrow a \equiv_R a \pmod{H}$$

(2) Symmetry: $a \equiv_R b \pmod{H} \Longrightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H$, since H is a subgroup and $c \in H \Rightarrow c^{-1} \in H$
$\Rightarrow (b^{-1})^{-1}a^{-1} \in H$
$\Rightarrow ba^{-1} \in H$
$\Rightarrow b \equiv_R a \pmod{H}$

Transitivity: $a \equiv_R b \pmod{H}$ and $b \equiv_R c \pmod{H}$

$\Rightarrow ab^{-1} \in H$ and $bc^{-1} \in H$
$\Rightarrow (ab^{-1})(bc^{-1}) \in H$
$\Rightarrow a(b^{-1}b)c^{-1} \in H$ by associativity
$\Rightarrow (ae)c^{-1} \in H$
$\Rightarrow (ae)c^{-1} \in H$
$\Rightarrow ac^{-1} \in H$
$\Rightarrow a \equiv_R c \pmod{H}$

Hence the relation $\equiv_R$ is an equivalence relation on the group G. Similarly, we can show that $\equiv_L$is an equivalence relation on G.

We know that an equivalence relation on a non-empty set always determines a partition. Hence $\equiv_R$ defines a partition of G. Similarly $\equiv_L$ partitions G into cells or classes. In this unit, we shall define and study these classes in details. These equivalence classes are called **cosets** and this partitioning of group is called **coset decomposition of group.**

3.2 Objectives

After reading this unit, you should be able to

- Describe the left and right decomposition of a group
- Define left and right cosets of any subgroup.
- Illustrate properties of these cosets
- Prove the Lagrange's theorem
- Discuss applications of Lagrange's theorem
- Define the index of a subgroup in a group
- Prove the Euler's theorem and Fermat's theorem
- illustrate the application of Fermat's theorem to RSA cryptosystem

3.3 Coset decomposition of a group

We have seen that the relation $\equiv_R$ is an equivalence relation on the group G. Therefore it will partition the group G into disjoint equivalence classes. Let $a \in G$, then the equivalence class of a can be given as

$$[a] = \{x \in G : x \equiv_R a \pmod{H}\}$$

or $$= \{x \in G : xa^{-1} \in H\}$$

Let us take an example to illustrate the decomposition of a group induced by this equivalence relation. Consider the symmetric group$S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ of degree 3 where

$f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $f_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$, $f_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$,
$f_5 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, $f_6 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$

You can see that $H = \{f_1, f_4\}$ is a subgroup of S_3. Now

$$[f_1] = \{f \in S_3 : f{f_1}^{-1} \in H\}$$

Remember $fg = fog$ for $f, g \in S_3$.

$\therefore\ f_1{f_1}^{-1} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = f_1$,

$f_2{f_1}^{-1} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = f_2$,

Similarly, $f_3{f_1}^{-1} = f_3$, $f_4{f_1}^{-1} = f_4$, $f_5{f_1}^{-1} = f_5$, $f_6{f_1}^{-1} = f_6$.

Here $f_1{f_1}^{-1} = f_1 \in H$ and $f_4{f_1}^{-1} = f_4 \in H$. Therefore

$$[f_1] = \{f_1, f_4\} = H$$

Now $[f_2] = \{f \in S_3 : f{f_2}^{-1} \in H\}$

$$f_1{f_2}^{-1} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\begin{pmatrix}2 & 3 & 1\\ 1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = f_3$$

Using the composition table of the symmetric group S_3 given in unit 1, we can calculate these elements easily, i.e.

$f_2{f_2}^{-1} = f_2f_3 = f_1$,$f_3{f_2}^{-1} = f_3f_3 = f_2$, $f_4{f_2}^{-1} = f_4f_3 = f_6$, $f_5{f_2}^{-1} = f_5f_3 = f_4$,

and $f_6{f_2}^{-1} = f_6f_3 = f_5$.

Here since $f_2{f_2}^{-1} = f_1 \in H$ and $f_5{f_2}^{-1} = f_4 \in H$, therefore

$$[f_2] = \{f_2, f_5\}$$

Similarly $[f_3] = \{f_3, f_6\}$, $[f_4] = \{f_4, f_1\}$, $[f_5] = \{f_5, f_2\}$ and $[f_6] = \{f_6, f_3\}$.

Hence the disjoint equivalence classes are

$$[f_1] = [f_4] = \{f_1, f_4\}$$
$$[f_2] = [f_5] = \{f_2, f_5\}$$

and $$[f_3] = [f_6] = \{f_3, f_6\}$$

Therefore $S_3 = [f_1] \cup [f_2] \cup [f_3]$ or you can say $S_3 = [f_4] \cup [f_5] \cup [f_6]$ etc. This is the decomposition of the group S_3induced by $\equiv_R$. These equivalence classes are called **the right cosets of the subgroup H** in S_3.

You will observe that $[f_1] = \{f_1, f_4\} = \{f_1f_1, f_4f_1\}$ or $\{ff_1 : f \in H\}$

Similarly $[f_2] = \{f_2, f_5\} = \{f_1f_2, f_4f_2\}$ or $\{ff_2 : f \in H\}$ etc. Therefore we can write

$$[g] = \{fg : f \in H\} \text{ for any } g \in S_3$$

We can use this representation for any arbitrary group G. So if H is any subgroup of G, then its right coset in G generated by $a \in G$ is given by

$$[a] = \{ha : h \in H\}$$

We use the notation Ha for $[a]$ .Hence

$$Ha = \{ha : h \in H\}$$

Similarly we can also obtain left coset decomposition of a group G. This decomposition is induced by the relation $\equiv_L$. In that case, the equivalence classes are called the left cosets of the subgroup H in the group G and the left coset generated by $a \in G$ is denoted by aH. Therefore

$$aH = \{ah : h \in H\}$$

Now we are in position to define left and right cosets of a subgroup H abstractly.

3.4 Left and right cosets of a subgroup

Definition: Let $(G,*)$ be a group and H be any subgroup of G. Let $a \in G$. Then
$H * a = \{h * a : h \in H\}$ is called **a right coset of H in G generated by a.** Similarly the set $a * H = \{a * h : h \in H\}$ is called **a left coset of H in G generated by a.**
If e is the identity element of G, then $e * H = H = H * e$.

Example 3.1 Let $H = \{\dots, -4, -2, 0, 2, 4, \dots\}$. Obviously H is a subgroup of additive group of integers $\mathbb{Z}$. Let us construct right cosets of H in $\mathbb{Z}$

$$H + 0 = H$$
$$H + 1 = \{h + 1 : h \in H\}$$
$$= \{\dots, -3, -1, 1, 3, \dots\}$$
$$H + 2 = \{\dots -4, -2, 0, 2, 4, \dots\} = H$$
$$H + 3 = \{\dots, -3, -1, 1, 3, \dots\} = H + 1$$

Also $H + (-1) = \{\dots -5, -3, -1, 1, 3, \dots\} = H + 1$, and so on. Therefore the distinct right cosets of H in $\mathbb{Z}$ are H and $H + 1$. Obviously

$$\mathbb{Z} = H \cup (H + 1)$$

Also we observe that
(i) $a \in H + a$ (ii) $b \in H + a \Leftrightarrow H + a = H + b$
(iii) $H + a = H + b \Leftrightarrow a - b \in H$
(iv) Either $H + a = H + b$ or $(H + a) \cap (H + b) = \emptyset$
Later on, we shall prove these properties in general setting.
Similarly, we can obtain different left cosets of H in $\mathbb{Z}$.

Example 3.2 we know that $H = \{-1, 1\}$ is a subgroup of multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity.
The left cosets of H in G can be formed as follows-
$1H = H, = \{-i, i\}$, $(-1)H = \{1, -1\} = H$, and $(-i)H = \{i, -i\} = iH$
Obviously $G = H \cup (iH)$.

Note: Since it is convenient to use multiplication for the composition $*$, from now on (except when necessary) we shall denote $H * a$ by Ha and $a * H$ by aH.

Proposition 3.2 If $[a] = \{x \in G : x \equiv_R a \pmod{H}\}$, then $[a] = Ha$.

Proof: Let $h \in H$. Then

$$a(ha)^{-1} = a(a^{-1}h^{-1}) = (aa^{-1})h^{-1} = eh^{-1} = h^{-1} \in H$$

Now $ax^{-1} \in H \Leftrightarrow xa^{-1} \in H \Leftrightarrow x \equiv_R a \pmod{H}$, therefore $ha \equiv_R a \pmod{H}$ and hence $ha \in [a]$ for every $h \in H$, and so $Ha \subseteq [a]$.

Let $x \in [a]$. Then $xa^{-1} \in H$, i.e. there exists $h \in H$ such that $xa^{-1} = h$ or $(xa^{-1})a = ha \Longrightarrow x(a^{-1}a) = ha \Longrightarrow xe = ha \Longrightarrow x = ha$. Thus $x \in Ha$. Hence $[a] \subseteq Ha$. The two inclusions $[a] \subseteq Ha$ and $[a] \subseteq Ha$ imply that $[a] = Ha$.

Now we shall discuss some properties of cosets of a given subgroup H of a group G.

3.5 Properties of cosets

Let H be any subgroup of a group$G$.

(1) $h \in H \Longrightarrow hH = H = Hh$.

Proof: Let $h \in H$. Then $hh' \in hH$ for any $h' \in H$. By closure property, $hh' \in H$. Thus $hH \subseteq H$.

Also every element $h' \in H$ can be written as

$$h' = eh' = (hh^{-1})h' = h(h^{-1}h')$$

Since $h^{-1}h' \in H$, hence $h(h^{-1}h') \in hH$, i.e. $h' \in hH$

Thus $H \subseteq hH$. Now $hH \subseteq H$ and $H \subseteq hH \Longrightarrow hH = H$.

Similarly we can prove that $Hh = H$.

(2) $a \in Ha$ for any $a \in G$.

Proof: Since $e \in H$, hence $a = ea \in Ha$

(3) Let $a, b \in G$. Then $a \in Hb \Leftrightarrow Ha = Hb$

Proof: Let $a \in Hb$. Then there exists $h \in H$ such that $a = hb$.

Now $x \in Ha \Leftrightarrow x = h_1 a$ for some $h_1 \in H$

$\Leftrightarrow x = h_1(hb), \quad h, h_1 \in H$

$\Leftrightarrow x = (h_1 h)b$

$\Leftrightarrow x \in Hb$

Hence $Ha = Hb$.

Conversely, suppose that $Ha = Hb$. Since $a \in Ha$, hence $a \in Hb$.

(4) Let $a, b \in G$. Then $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Proof: Let $Ha = Hb$. Then $a \in Hb$, i.e. $a = hb$ for some $h \in H$.

Now $a = hb \Longrightarrow ab^{-1} = h \in H$, i.e. $ab^{-1} \in H$.

Conversely, suppose that $ab^{-1} \in H$. Then there exists $h \in H$ such that $ab^{-1} = h$ or $a = hb$. Since $hb \in Hb$, hence $a \in Hb$ and therefore $Ha = Hb$.

(5) Any two right cosets of H are either disjoint or identical.

Let Ha and Hb be any two right cosets of the subgroup H in G. If these are not disjoint then there exists $c \in Ha \cap Hb$, i.e. $c \in Ha$ and $c \in Hb$. Thus there exists $h_1, h_2 \in H$ such that $c = h_1 a$ and $c = h_2 b$. Therefore

$$h_1 a = h_2 b$$

$$\Longrightarrow a = {h_1}^{-1}(h_2 b)$$

$$\Longrightarrow a = ({h_1}^{-1} h_2) b \in Hb \text{ as } {h_1}^{-1} h_2 \in H$$

$$\Longrightarrow Ha = Hb \quad \text{since } a \in Hb \Leftrightarrow Ha = Hb$$

i.e. if the right cosets are not disjoint, they are identical.

(6) The group G is the union of all right cosets of H in G.

Proof: Since $x \in Ha \Longrightarrow x \in G$, for any $a \in G$, hence $Ha \subseteq G$ for any $a \in G$. Therefore

$$\bigcup_{a \in G} Ha \subseteq G$$

Let $x \in G$. Then Hx is a right coset of H in G and $x \in Hx$. Therefore

$$x \in G \Longrightarrow x \in Hx \subseteq \bigcup_{a \in G} Ha$$

i.e. $G \subseteq \bigcup_{a \in G} Ha$. Thus $G = \bigcup_{a \in G} Ha$.

(7) There is a one-to-one correspondence between any two right cosets of H in G.

Proof: Let $a, b \in G$. Then Ha and Hb are two right cosets of H in G. Define a mapping $f: Ha \longrightarrow Hb$ such that $f(ha) = hb$ for all $h \in H$. We show that f is a bijection.

(i) $\boldsymbol{f}$ **is one-to-one:** Let $h_1, h_2 \in H$. Then $h_1 a, h_2 a \in Ha$.

Now $f(h_1 a) = f(h_2 a) \Longrightarrow h_1 b = h_2 b \Longrightarrow h_1 = h_2 \Longrightarrow h_1 a = h_2 a$

(ii) $\boldsymbol{f}$ **is onto:** Let $hb \in Hb$. Then $h \in H$ and therefore $ha \in Ha$. Thus to each $hb \in Hb$,there exists $ha \in Ha$ such that $f(ha) = hb$.

Hence f is a bijection, i.e. there is a one-to-one correspondence between any two right cosets of H in G.

Similarly, we can prove results for left cosets. Thus we have

(1) $a \in aH$ for any $a \in G$.

(2) Let $a, b \in G$. Then $a \in bH \Leftrightarrow aH = bH$

(3) Let $a, b \in G$. Then $aH = bH \Leftrightarrow a^{-1} b \in H$.

(4) Any two left cosets of H are either disjoint or identical.

(5) The group G is the union of all left cosets of H in G.

(6) There is a one-to-one correspondence between any two left cosets of H in G.

Proposition 3.3 There is a one-to-one correspondence between the set of left cosets of H in G and the set of right cosets of H in G.

Proof: Let $\mathcal{L} = \{aH : a \in G\}$ and $\mathcal{R} = \{Ha : a \in G\}$ be the families of left cosets of H and right cosets of H in G respectively. Define $f : \mathcal{L} \longrightarrow \mathcal{R}$, such that

$$f(aH) = Ha^{-1} \text{ for all } a \in G.$$

First we show that f is well defined.

Let $aH \in \mathcal{L}$. Then $a \in G$ and therefore $a^{-1} \in G$. Hence $Ha^{-1} \in \mathcal{R}$. Further let $aH, bH \in \mathcal{L}$, then

$$\begin{aligned} aH = bH &\Longrightarrow a^{-1}b \in H \\ &\Longrightarrow Ha^{-1}b = H \qquad \text{as } h \in H \Longrightarrow Hh = H \\ &\Longrightarrow Ha^{-1} = Hb^{-1} \\ &\Longrightarrow f(aH) = f(bH) \end{aligned}$$

Thus f is a well defined map. Now we prove that f is a bijection from $\mathcal{L}$ onto $\mathcal{R}$.

(i) f is one-to-one: We have

$$\begin{aligned} f(aH) = f(bH) &\Longrightarrow Ha^{-1} = Hb^{-1} \\ &\Longrightarrow a^{-1}(b^{-1})^{-1} \in H \qquad \text{as } Hc = Hd \Leftrightarrow cd^{-1} \in H \\ &\Longrightarrow a^{-1}b \in H \\ &\Longrightarrow aH = bH \end{aligned}$$

(ii) f is onto: Let $Hb \in \mathcal{R}$. Then $b \in G$ and hence $b^{-1} \in G$. Therefore $b^{-1}H \in \mathcal{L}$. Now $f(b^{-1}H) = H(b^{-1})^{-1} = Hb$. i.e. f is onto.

Thus f is a well defined bijective mapping from $\mathcal{L}$ onto $\mathcal{R}$. Hence the result.

Definition: Let H and K be two (not necessarily distinct) subgroups of a group G and let $x \in G$.The set $HxK = \{hxk : h \in H, k \in K\}$ is called a double coset.

Proposition 3.4 Two double cosets are either disjoint or identical.

Proof: Let HaK and HbK be any two double cosets of a group G. If these are not disjoint, then there exists $c \in HaK \cap HbK$. Then $c = hak = h_1bk_1$ where $h, h_1 \in H$ and $k, k_1 \in K$.

Now $HcK = HhakK = HaK$, since $Hh = H$ and $kK = K$.

Also $cK = Hh_1bk_1K = HbK$, as $Hh_1 = H$ and $k_1K = K$.

Therefore we have $HaK = HcK = HbK$, i.e. $HaK = HbK$.

Now we shall prove an important theorem due to Lagrange.

3.6 Lagrange's Theorem

Theorem 3.1 The order of each subgroup of a finite group is a divisor of the order of the group.

Proof: Let G be a finite group of order n and H a subgroup of G. Let $o(H) = m$ and $H = \{h_1, h_2, \dots, h_m\}$. Hence $1 \leq m \leq n$. Let $a \in G$. Then Ha is a right coset of H in G. Define a function $f: H \longrightarrow Ha$ by $f(h) = ha$ for all $h \in H$. This mapping is a onto as if $ha \in Ha$ then $h \in H$ and $f(h) = ha$. Also f is one-one since $(h_i) = f(h_j) \Longrightarrow h_i a = h_j a \Longrightarrow h_i = h_j$, where $h_i, h_j \in H$. Hence H and Ha have the same number of elements, i.e. $o(Ha) = o(H) = m$.

Let $Ha_1, Ha_2, \dots, Ha_k$be the distinct right cosets of H in G. Then these k distinct right cosets are the distinct equivalence classes in G detemined by the relation of right congruence modulo H. Hence we have

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$$

$$\Longrightarrow o(G) = o(Ha_1) + o(Ha_2) + \cdots + o(Ha_k)$$

$$\Longrightarrow o(G) = m + m + \cdots + m \text{ upto } k \text{ terms}$$

$$\Longrightarrow o(G) = mk$$

$$\Longrightarrow n = km$$

Hence m divides n, i.e. $o(H)$ divides $o(G)$.

Let us illustrate the result with some examples. Consider the multiplicative group of fourth roots of unity, i.e. $G = \{1, -1, i, -i\}$. The group has a subgroup $H = \{1, -1\}$. Here $o(G) = 4$ and $o(H) = 2$. Obviously $o(H)$ divides $o(G)$. So that means if H is a subset of a group G such that $o(H)$ does not divide $o(G)$, then H cannot be a subgroup of G. Hence in above example, G cannot have a subgroup of order 3. Here you will observe one more thing that For instance, the subset $H_1 = \{i, -i\}$ of G is of order 2, i.e. divisor of $o(G)$, But H_1 is not a subgroup of G. So if $o(H)$ divides $o(G)$, it does not mean that H is definitely a subgroup of G.

Also the full converse of above theorem is not true. That is, if m divides $o(G)$, then it is not necessary that G has a subgroup of order m. However, for finite abelian groups the full converse of Lagrange's theorem is true, i.e. an abelian group has a subgroup of order m if m divides $o(G)$.

Another consequence of the theorem is that a group of prime order can have no proper subgroup as the only divisors of a prime number p are ± 1 and $\pm p$.

Now we derive some consequences of Lagrange's theorem.

Corollary 1 The order of every element of a finite group is a divisor of the order of the group.

Proof: Let G be a finite group of order n. Let a be an element of G of order m, i.e. $o(a) = m$. Consider a cyclic subgroup $\langle a \rangle$ of G generated by a. We show that $\langle a \rangle$ contains exactly m elements, namely, $e = a^0, a^1, a^2, \dots \dots, a^{m-1}$.

The elements $e = a^0, a^1, a^2, \dots\dots, a^{m-1}$ are all distinct, since if $a^r = a^s$, $0 \leq r < s < m$, then $a^{r-s} = e$ where $r - s < m$. Which is not possible as m is the smallest positive integer satisfying this property. So $\langle a \rangle$ must have at least these m elements.

Now if a^t be any element of $\langle a \rangle$, then by division algorithm, $t = mq + k$, where $0 \leq k < m$. Therefore

$$a^t = a^{mq+k} = (a^m)^q a^k = e^q a^k = a^k \in \{e = a^0, a^1, a^2, \dots\dots, a^{m-1}\}$$

Thus each element of $\langle a \rangle$ is one of the elements $e = a^0, a^1, a^2, \dots\dots, a^{m-1}$, i.e. $\langle a \rangle$ has exactly $\langle a \rangle$ elements. Hence $o(\langle a \rangle) = m$.

By Lagrange's theorem $o(\langle a \rangle) | o(G)$, i.e. $m | o(G)$ or $o(a) | o(G)$.

Corollary 2 Let G be a finite group and $a \in G$. Then $a^{o(G)} = e$.

Proof: Let $o(G) = n$ and $o(a) = m$. Then $o(\langle a \rangle) = m$ and by Lagrange's theorem $m | n$. Hence we have $n = mk$ for some positive integer k.

Since $o(a) = m$, hence $a^m = e$.

Now $a^n = a^{mk} = (a^m)^k = e^k = e$, i.e. $a^{o(G)} = e$.

Proposition 3.5 Every group of prime order is cyclic.

Proof: Let G be a finite group of prime order p. Then G must contain at least two elements. Let $a \in G$ such that $a \neq e$. Let $o(a) = m$. Then $m \geq 2$. Hence $o(\langle a \rangle) = m$, where $\langle a \rangle$ is a cyclic subgroup of G generated by a.

By Lagrange's theorem m must divide p. Since $m \geq 2$ and p is a prime number, hence we have $m = p$. Therefore $\langle a \rangle = G$, i.e. G is a cyclic group with a generator a.

Proposition 3.6 If H and K are finite subgroups of a group G, then

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

Proof: Let $D = H \cap K$. Then D is a subgroup of G. Also $D \subseteq K$, hence D is a subgroup of K. Let us decompose K into disjoint right cosets $Dk_1, Dk_2, \dots, Dk_t$ of D. Where $k_1, k_2, \dots, k_t$ are distinct elements of K. By Lagrange's theorem the number of such cosets is given by $t = \frac{o(K)}{o(D)}$ and we have

$$K = \bigcup_{m=1}^{t} Dk_m$$

Therefore

$$HK = H\left(\bigcup_{m=1}^{t} Dk_m\right) = \bigcup_{m=1}^{t} HDk_m = \bigcup_{m=1}^{t} Hk_m$$

as $D \subseteq H \Longrightarrow HD = H$.

Now we claim that the right cosets $Hk_1, Hk_2, \ldots, Hk_t$ are pairwise distinct. For if

$$Hk_i = Hk_j \Longrightarrow k_i {k_j}^{-1} \in H$$

But since $k_i {k_j}^{-1} \in K$, hence $k_i {k_j}^{-1} \in H \cap K = D \Longrightarrow Dk_i = Dk_j \Longrightarrow k_i = k_j$, a contradiction as all k_i's are assumed to be distinct. Therefore the right cosets $Hk_1, Hk_2, \ldots, Hk_t$ are pairwise distinct. Each of these cosets has $o(H)$ number of elements. Hence we have

$$o(HK) = t \times o(H) = \frac{o(K)}{o(D)} \times o(H) = \frac{o(H)o(K)}{o(H \cap K)}$$

3.7 Index of a subgroup

While proving the Lagrange's theorem you noticed that $k = \frac{n}{m}$ i.e. the number of right cosets of H in $G = \frac{o(G)}{o(H)}$. This number is called the index of H in G. For example, the index of the subgroup $H = \{1, -1\}$ in $G = \{1, -1, i, -i\}$ is 2.

But for an infinite group G the quotient $\frac{o(G)}{o(H)}$ does not make sense. So we have the following definition.

Definition : If G is a group and H a subgroup of G, the number of distinct left (right) cosets of H in G is called the **index** of H in G and is denoted by $[G:H]$ or $i_G(H)$. If the group G is finite then

$$[G:H] = \frac{o(G)}{o(H)}$$

Infinite groups may have subgroups of finite or infinite index. For example, the subgroup $\{0\}$ is of infinite index in the additive group $\mathbb{Z}$ and the subgroup $\langle 2 \rangle$, i.e. $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is of index 2 in $\mathbb{Z}$.

Proposition 3.7 If H and K are two subgroups of a finite group G such that $H \subseteq K$, then

$$[G:H] = [G:K][K:H]$$

Proof: Since H and K are subgroups of G and $H \subseteq K$, therefore H is also a subgroup of K. Then we have $[G:H] = \frac{o(G)}{o(H)}$ and $[G:K] = \frac{o(G)}{o(K)}$ and $[K:H] = \frac{o(K)}{o(H)}$.

Now $[G:H] = \frac{o(G)}{o(H)} = \frac{o(G)}{o(K)} \times \frac{o(K)}{o(H)} = [G:K][K:H]$.

Definition: Let G be a group and let p be a prime number. A group of order p^α for some $\alpha \geq 1$ is called a ***p*-group** and the subgroups of G which are p-groups are called ***p*-subgroups.**

If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a **Sylow *p*-subgroup** of G.

Now we state some important theorems without proof.

Cauchy's theorem: Let G be a finite group and p be a prime number dividing $o(G)$, then G has an element of order p.

Sylow's theorem: If G is a group of order $p^\alpha m$, where p is a prime number not dividing m, i.e. $p \nmid m$, then G has a Sylow p-subgroup and the number of Sylow p-subgroups of G, n_p, is of the form $n_p = 1 + kp$,i.e. $n_p \equiv 1 \pmod{p}$.

Consider the symmetric group S_3 on three symbols. We have $o(S_3) = 6 = 2 \times 3$. Since $2 \nmid 3$, hence S_3 must have a Sylow 2-subgroup.

We have $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$,where
$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$,
$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
Then using the composition table given in unit-1, we can show that the cyclic subgroup generated by f_4 is $\langle f_4 \rangle = \{f_1, f_4\}$ which is a Sylow 2-subgroup of S_3.

Similarly, the other two Sylow 2-subgroup of S_3 are $\langle f_5 \rangle = \{f_1, f_5\}$ and $\langle f_6 \rangle = \{f_1, f_6\}$. Hence there are three Sylow 2-subgroups of S_3. This is justified as

$3 \equiv 1 \pmod{2}$ **.**

Now we prove two very interesting and useful results.

3.8 Euler's theorem

Theorem 3.2 If n is a positive integer coprime (i.e. relatively prime) to a, then
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof: We know that $\mathbb{U}_n = \{[a] \in \mathbb{Z}_n : a \text{ and } n \text{ are co-prime}\}$ is a multiplicative group of residue classes modulo n. The order of $\mathbb{U}_n$ is $\varphi(n)$, the Euler's totient function. The identity of this group is $[1]$. If $[a] \in \mathbb{U}_n$, then by the corollary to Lagrange's theorem

$$[a]^{\varphi(n)} = [1] \Rightarrow [a][a] \ldots \text{ upto } \varphi(n) \text{times} = [1]$$
$$\Rightarrow [aa \ldots \text{ upto } \varphi(n) \text{times}] = [1]$$
$$\Rightarrow \left[a^{\varphi(n)}\right] = [1] ,$$
$$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n} \{\because [a] = [b] \Rightarrow a \equiv b \pmod{n}\}$$

Hence the result.

3.9 Fermat's theorem

This theorem is a direct consequence of the Euler's theorem, i.e. if p is a prime number then the number of positive integers less than and prime to p is $\varphi(p) = p - 1$ and by Euler's theorem we have $a^{p-1} \equiv 1 \pmod{p}$. This theorem is also called the Fermat's little theorem. We give a somewhat direct proof below.

Theorem 3.3 Let p be a prime number and let a be any integer not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof: Since a is not divisible by p, hence

$$\gcd(a, p) = 1$$

$$\Longrightarrow [a] \in \mathbb{Z}_p$$

Now $(\mathbb{Z}_p) = p - 1$, Hence by the corollary to Lagrange's theorem , we have

$$[a]^{p-1} = [1]$$

$$\Longrightarrow [a^{p-1}] = [1]$$

$$\Longrightarrow a^{p-1} \equiv 1 \pmod{p}$$

Corollary: Let p be a prime and let a be any integer. Then $a^p \equiv a \pmod{p}$

Proof: If $p|a$, then $p|a^p$, i.e. $p|a^p - a$. Therefore $a^p \equiv a \pmod{p}$.

(The other way to illustrate this case is that $p|a$, then $p|a^p \Longrightarrow [a] = [0] = [a^p]$, and hence $a^p \equiv a \pmod{p}$)

If $p \nmid a$ i.e. p is not a divisor of a. Then by Fermat's little theorem $a^{p-1} \equiv 1 \pmod{p}$. Multiplying both sides by a we get $a^p \equiv a \pmod{p}$.

Now We shall discuss some applications of theses theorems.

Example 3.3 Compute the remainder of $37^{49}$when divided by 7.

We have $37^{49} = (37^6)^8(37)$. Now by Fermat's theorem,

$$37^6 \equiv 1 \pmod{7}$$

$$\therefore 37^{49} \equiv (1)^8(37) \pmod{7}$$

$$\equiv 37 \pmod{7}$$

$$\equiv 2 \pmod{7}$$

Hence the remainder is 2.

Example 3.4 Show that $2^{913} - 1$ is not divisible by 13

We have $2^{913} - 1 = (2^{12})^{76}(12) - 1$

By Fermat's theorem, $2^{12} \equiv 1 (\text{mod } 13)$, so

$$2^{913} - 1 \equiv (1)^{76}(12) - 1 (\text{mod } 13)$$

$$\equiv 12 - 1 (\text{mod } 13)$$

$$\equiv 11 (\text{mod } 13)$$

Thus the remainder of $2^{913} - 1$ when divided by 13 is 11 and not zero, i.e. $2^{913} - 1$ is not divisible by 13.

Example 3.5 Show that for every integer n, the number $n^{33} - n$ is divisible by 15.

Since $15 = 5 \times 3$, we shall show that $n^{33} - n$ is divisible by both 3 and 5.

We have either $3|n$ or $3 \nmid n$

If $3|n$, then obviously 3 divides $n(n^{32} - 1) = n^{33} - n$.

If 3 does not divide n, then by Fermat's theorem

$$n^2 \equiv 1 \text{ (mod } 3)$$

Now $n^{32} - 1 = (n^2)^{16} - 1$, therefore we have

$$n^{32} - 1 \equiv (1)^{16} - 1 \text{ (mod } 3) \equiv 0 (\text{mod } 3)$$

Hence the remainder of $n^{32} - 1$ is zero when divided by 3, i.e. 3 divides $n^{32} - 1$ and hence $n(n^{32} - 1) = n^{33} - n$.

If $5|n$, then 5 divides $n(n^{32} - 1) = n^{33} - n$.

If 5 is not a divisor of n, then by Fermat's theorem

$$n^4 \equiv 1 \text{ (mod } 5)$$

Now $n^{32} - 1 = (n^4)^8 - 1$, therefore we have

$$n^{32} - 1 \equiv (1)^8 - 1 \text{ (mod } 5) \equiv 0 (\text{mod } 5)$$

Hence 5 divides $n^{32} - 1$, i.e. 5 divides $n(n^{32} - 1) = n^{33} - n$.

Thus $n^{33} - n$ is divisible by both 3 and 5, i.e. $n^{33} - n$ is divisible by 15.

Test for compositeness: The contrapositive of Fermat's little theorem can be used to test for compositeness of a number.

Let $n > 2$ be an odd positive integer. If There exists an integer a relatively prime to n for which $a^{n-1} \not\equiv 1 (\mathrm{mod}\, n)$, then n is necessarily a composite number.

Example 3.6 We have $680^{5460} \equiv 1162 \not\equiv 1 (\mathrm{mod}\, 5461)$. Hence the number 5461 is composite. In fact, $5461 = 43 \times 127$.

3.10 Application of Fermat's theorem to RSA cryptosystem

Cryptography is the study of tools and techniques required for secure communication in the presence of third parties. Its aim is to protect the sensitive information against the unauthorized access. First the ordinary information (plaintext) is encrypted to the form known as ciphertext. This ciphertext is sent to the receiver through a medium (channel) and then decrypted to get the original plaintext message. The encryption and decryption constitute a cryptosystem. The encryption and decryption processes require a word, number or phrase as a key.

In public key cryptosystems two different but mathematically related keys are used. The key that is made public is called public key while the key that is kept secret is called private key. The public key is used for encryption while the private key is used for decryption procedure. One such cryptosystem is RSA which was introduced by R.Rivest, A.Shamir and L.Adleman in 1978. It is based on the factoring of large numbers and the use of Fermat's little theorem.

Suppose Bob wants to send a message M to Alice using this cryptosystem. The steps involved in RSA algorithm can be listed as follows-

(1) Choose two distinct prime numbers p and q.

(2) Compute $n = pq$

(3) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+q) + 1$

Where $\varphi(n)$ is Euler's totient function.

(4) Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd\big(e, \varphi(n)\big) = 1$

(5) Find the multiplicative inverse d of e in $\mathbb{Z}_{\varphi(n)}$, i.e.

$$de \equiv 1 \left(\mathrm{mod}\, \varphi(n)\right)$$

(6) The Public key consists of n and e while the private key consists of n and d. The value e is announced as the public key exponent and the number d is kept as the private key exponent. The primes numbers p and q, and $\varphi(n)$ are also kept secret.

(7) Bob knows the public key (n, e) and turns the message M into an integer m such that $0 \leq m < n$

(8) The message is encrypted by raising m to eth power modulo n to obtain the ciphertext C, i.e.

$$C \equiv m^e \ (\mathrm{mod}\, n)$$

(9) Bob sends C to Alice. Now Alice recovers the original message as

$$m \equiv \sqrt[e]{C} \pmod{n}$$

Now the little Fermat's theorem comes into play. We shall show that decryption of C can be obtained as $m \equiv C^d \pmod{n}$, where d is the private key available to Alice.

Now $m \equiv C^d \pmod{n}$ is equivalent to $C^d \equiv m \pmod{n}$ or $(m^e)^d \equiv m \pmod{n}$

So we have to prove that $m^{ed} \equiv m \pmod{pq}$ as $n = pq$

We know that $a \equiv m \pmod{p}, a \equiv m \pmod{q} \Longrightarrow a \equiv m \pmod{pq}$. So to prove that $m^{ed} \equiv m \pmod{pq}$, we have to show that $m^{ed} \equiv m \pmod{p}$ and $m^{ed} \equiv m \pmod{q}$.

First we shall show that $m^{ed} \equiv m \pmod{p}$. We consider the following two cases:

Case I When $m \equiv 0 \pmod{p}$. Then $|m$, i.e. $m = ps$ for some integer s.

Now $m^{ed} = (ps)^{ed} = pp^{ed-1}s^{ed}$, i.e.$p|m^{ed}$. Hence $m^{ed} \equiv 0 \pmod{p}$.

Therefore $m^{ed} \equiv m \pmod{p}$.

Case II When $m \not\equiv 0 \pmod{p}$. Then $\gcd(m, p) = 1$ and by Fermat's little theorem we have

$$m^{p-1} \equiv 1 \pmod{p}$$

Now

$$de \equiv 1 \left(\mathrm{mod}\ \varphi(n)\right)$$

or $de - 1 = k\varphi(n)$ for some integer k

or $de - 1 = k(p-1)(q-1)$

or $de = 1 + k(p-1)(q-1)$

Thus we have $m^{ed} = m^{1+k(p-1)(q-1)}$

$$= mm^{k(p-1)(q-1)}$$

$$= m(m^{p-1})^{k(q-1)}$$

$$\Longrightarrow m^{ed} \equiv m\ (1)^{k(q-1)} (\mathrm{mod}\ p)\ , \text{since } m^{p-1} \equiv 1 \pmod{p}$$

$$\text{or } m^{ed} \equiv m \pmod{p}$$

Same reasoning implies $m^{ed} \equiv m \pmod{q}$. Therefore $m^{ed} \equiv m \pmod{pq}$ or $m^{ed} \equiv m \pmod{n}$. Hence the decryption of $C \equiv m^e \pmod{n}$ is obtained as $m \equiv C^d \pmod{n}$.

Let us illustrate the procedure with an example. Take $p = 61$ and $q = 53$. Then $n = pq = 61 \times 53 = 3233$. Therefore

$$\varphi(n) = \varphi(3233) = (61-1)(53-1) = 60 \times 52 = 3120$$

Choose $1 < e < 3120$ such that e is relatively prime to 3120. Take $e = 17$. The multiplicative inverse modulo 3120 of e is 2753, i.e.

$$17 \times 2753 \equiv 1(\text{mod } 3120)$$

Hence $d = 2753$. Therefore the encryption of the message m is

$$C \equiv m^e \pmod{n}, \text{ i.e. } C \equiv m^{17} \pmod{3233}$$

The decryption of C is $m \equiv C^d(\text{mod } n)$, i.e. $m \equiv C^{2753}(\text{mod } 3233)$.

For example, the encryption of $m = 65$ is $C \equiv 65^{17} \pmod{3233}$ or $C = 2790$.

The decryption of $C = 2790$ is $m \equiv 2790^{2753}(\text{mod } 3233)$ or $m = 65$.

Note: while doing computation, sometimes we need to calculate congruences of very large numbers. There are tricks to carry out such calculations. Let us take an example. Suppose we have to compute $320^{984}(\text{mod } 7)$.

We have $320 \equiv 5(\text{mod } 7)$ as 7 divides 315. Hence we can write

$$320^{984} \equiv 5^{984}(\text{mod } 7)$$

Now $984 = 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3$, therefore

$$5^{984} = 5^{2^9} \times 5^{2^8} \times 5^{2^7} \times 5^{2^6} \times 5^{2^4} \times 5^{2^3}$$

Now $5^2 = 25 \equiv 4(\text{mod } 7)$

$5^4 = 5^2 \times 5^2 \equiv 4 \times 4(\text{mod } 7) = 16(\text{mod } 7) \equiv 2(\text{mod } 7)$

$5^8 = 5^4 \times 5^4 \equiv 2 \times 2(\text{mod } 7) = 4(\text{mod } 7)$

$5^{16} = 5^8 \times 5^8 \equiv 4 \times 4(\text{mod } 7) = 16(\text{mod } 7) \equiv 2(\text{mod } 7)$

Similarly, $5^{32} \equiv 4(\text{mod } 7)$, $5^{64} \equiv 2(\text{mod } 7)$, $5^{128} \equiv 4(\text{mod } 7)$,

$5^{256} \equiv 2(\text{mod } 7)$ and $5^{512} \equiv 4(\text{mod } 7)$.

Therefore $5^{984} \equiv 4 \times 2 \times 4 \times 2 \times 2 \times 4(\text{mod } 7)$

$$= 8 \times 8 \times 8(\text{mod } 7) \equiv 1 \times 1 \times 1(\text{mod } 7) = 1(\text{mod } 7).$$

3.11 Summary

In this unit, we have

(1) Introduced the congruence relations $\equiv_L$ and $\equiv_R$ in a group G and proved that these are equivalence relations in G.

(2) discussed the coset decomposition of a group and defined left and right cosets of a subgroup in a group G.

(3) described the properties of cosets of a subgroup.

(4) proved the Lagrange's theorem.

(5) discussed various applications of Lagrange's theorem.

(6) defined the index of a subgroup in a group.

(7) stated Cauchy's theorem and Sylow's theorem without proof.

(8) proved Euler's theorem and Fermat's theorem and discussed various examples illustrating these theorems.

(9) described in details the application of Fermat's theorem in RSA cryptosytem.

3.12 Self assessment questions

(1) If a finite group G contains an element of even order, show that G must also be of even order.

(2) Let H be a subgroup of a group G and $a \in G$. Then $(Ha)^{-1} = a^{-1}H$

(3) If a finite group possesses an element of order 2, prove that it possesses an odd number of such elements.

(4) Prove that the only right (left) coset of a subgroup H in a group G which is also a subgroup of G is H itself.

(5) Prove that the intersection of two subgroups, each of finite index, is again of finite index.

(6) Show that every finite group of order less than six must be abelian.

(7)Use Lagrange's theorem to prove that a finite group cannot be expressed as the union of two of its proper subgroups.

(8) Show that all proper subgroups of a group of order 8 must be abelian.

(9) Let H and K are subgroups of a finite group G such that $o(H) = 3$, $o(K) = 5$. Find the order of HK. [Ans. 15]

(10) Show that 1763 is composite. [Hint: $2^{1762} \equiv 742 \pmod{1763}$]

(11) If p is a prime, prove that $(p-1)! \equiv -1 \pmod{p}$.

(12) Let G be a group of order 12. If Sylow 2-subgroup of G is cyclic, prove that G is cyclic.

(13) Let H be a subgroup of a group$G$. Let $x \in G$. Then $x^{-1}Hx = \{x^{-1}hx : h \in H\}$ is a subgroup of G.

(14) Prove that a group of prime order is cyclic.

3.13 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

U P RAJARSHI TANDON
OPEN UNIVERSITY
ALLAHABAD

UGMM-109
ABSTRACT ALGEBRA

ABSTRACT ALGEBRA

Block-II

Normal Subgroups and Symmetric Groups

Block-II
Normal Subgroups and Symmetric Groups

Unit-4

Normal Subgroups and Homomorphisms

Unit-5

Symmetric Groups and Automorphisms

Block-II **UGMM-109**

Introduction

Unit-4 In this unit, we introduce Normal subgroups and discuss various properties of normal subgroups. We define Quotient group, Conjugate elements, Normalizer of an element of a group and the Center of a group and the kernel of a homomorphism. We prove the fundamental theorem of homomorphism of groups. We illustrate the concept of direct and inverse image of a subgroup and normal subgroup under a homomorphism.

Unit-5 In this unit, we study symmetric group S_n in details. We discuss cycles, transpositions, decomposition of a permutation and the alternating group A_n. We prove the Cayley's theorem. We introduce the notion of automorphism and inner automorphism of groups with examples.

Unit-4: Normal Subgroups and Homomorphisms

Structure

4.1 Introduction

If a group G is abelian and H is a subgroup of G, then for any $x \in G$, we have $xH = Hx$. For example, the group of fourth roots of unity, $G = \{1, -1, i, -i\}$, is an abelian group and $H = \{1, -1\}$ is a subgroup of G. We observe that

$$iH = \{i1, i(-1)\} = \{i, -i\} = Hi$$

Similarly $(-i)H = H(-i)$, $1H = H1$ and $(-1)H = H(-1)$

Hence $xH = Hx$ for all $x \in G$.

If a group G is not abelian, then the condition $xH = Hx$ for all $x \in G$ is not always true for any subgroup H. However a group G may contain a subgroup H satisfying this condition.

For example, the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is a non-abelian group under quaternion multiplication. Let

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and $C = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$

We know that $G = \{\pm I, \pm A, \pm B, \pm C\}$ forms a quaternion group under matrix multiplication. You can verify that $\mathcal{H} = \{\pm I, \pm A\}$ is a subgroup of G.
Now you will observe that $x\mathcal{H} = \mathcal{H}x$ for all $x \in G$. For example, $B \in G$ and

$$B\mathcal{H} = \{BI, -BI, BA, -BA\} = \{B, -B, -C, C\}$$

and $$\mathcal{H}B = \{IB, -IB, AB, -AB\} = \{B, -B, C, -C\}$$

Thus $B\mathcal{H} = \mathcal{H}B$. Similarly $I\mathcal{H} = \mathcal{H}I$, $A\mathcal{H} = \mathcal{H}A$, $(-A)\mathcal{H} = \mathcal{H}(-A)$ and so on.

So it may happen that the group G is not abelian but it has a subgroup H such that $xH = Hx$ for all $x \in G$. Such subgroups are called **normal subgroups.** In this unit, we shall study normal subgroups in details. The cosets of a normal subgroup are special in a way that the set of all such cosets is a group with respect to multiplication of complexes. This group is called the **quotient group** or **factor group**.

We shall define an interesting equivalence relation called **relation of conjugacy** on a group. We shall also study some special subgroups such as **normalizer of an element of a group** and **center of a group**.

A homomorphism $f: G \longrightarrow G'$maps a subset of the group G onto the identity element of group G'. This subset is a normal subgroup of the group G and is called the **kernel of homomorphism** f. In this unit, we shall make a detailed study these concepts and then prove an important result called the fundamental theorem of homomorphism.

4.2 Objectives

After reading this unit, you should be able to

- Describe the normal subgroups of a group
- Discuss the Properties of Normal subgroups
- Define quotient group
- Define an equivalence relation called the relation of conjugacy on a group.
- Define the conjugate elements and self-conjugate elements of a group
- Illustrate the concepts such as the normalizer of an element of a group and the center of a group
- Define the kernel of a homomorphism
- Prove the fundamental theorem of Homomorphism
- Discuss the direct and inverse images of a subgroups and normal subgroups under a homomorphism

4.3 Normal subgroups of a group

Definition: A subgroup H of a group G is said to be a **normal subgroup** of G if

$$xhx^{-1} \in H \text{ for every } x \in G \text{ and for every } h \in H.$$

Since $xhx^{-1} \in xHx^{-1}$, hence we can say that H is a normal subgroup of G if

$$xHx^{-1} \subseteq H \text{ for every } x \in G$$

If H is a normal subgroup of a group G, we denote this by $H \lhd G$

Every group G has at least two normal subgroups namely G and $\{e\}$. These subgroups are called **trivial normal subgroups**. A group $G \neq \{e\}$ which does not have any non-trivial normal subgroup is called a **simple group**.

In example (given above), $\mathcal{H} = \{\pm I, \pm A\}$ is a non-trivial normal subgroup of the group $G = \{\pm I, \pm A, \pm B, \pm C\}$.

Example Let $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ be the symmetric group of order 6. where

$f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $f_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$, $f_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$,
$f_5 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, $f_6 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$
Then you can verify that $H = \{f_1, f_2, f_3\}$ is a normal subgroup of S_3.

Example Every subgroup of an abelian group is normal.
Let H be a subgroup of an abelian group$G$. Let $h \in H$ and $x \in G$. Then

$$xhx^{-1} = hxx^{-1} = he = h \in H$$

i.e. H is normal in G.
We have already seen this result in case of subgroup $H = \{1, -1\}$ of the abelian group $G = \{1, -1, i, -i\}$ of fourth roots of unity.
Now we shall discuss some important properties of normal subgroups.

4.4 Properties of Normal subgroups

Proposition: A Subgroup H of a group G is normal if and only if
$xHx^{-1} = H$ for all $x \in G$
Proof: First suppose that H is a subgroup of a group G such that
$xHx^{-1} = H$ for all $x \in G$
Then obviously $xHx^{-1} \subseteq H$ for all $x \in G$, i.e. H is a normal subgroup of G.
Conversely, suppose that H is a normal subgroup of a group G. Then
$xHx^{-1} \subseteq H$ for all $x \in G$
Since $x \in G \Longrightarrow x^{-1} \in G$, hence we have $x^{-1}H(x^{-1})^{-1} \subseteq H$, i.e.
$x^{-1}Hx \subseteq H$ for all $x \in G$
$\Longrightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$ for all $x \in G$
$\Longrightarrow (xx^{-1})H(xx^{-1}) \subseteq xHx^{-1}$ for all $x \in G$
$\Longrightarrow H \subseteq xHx^{-1}$ for all $x \in G$
Now the inclusions $xHx^{-1} \subseteq H$ and $H \subseteq xHx^{-1}\ \forall x \in G$ imply that
$xHx^{-1} = H$ for all $x \in G$

Proposition: A subgroup H of a group G is a normal subgroup of G if and only if each left coset of H in G is a right coset of H in G.
Proof: First suppose that H is a normal subgroup of a group G. Then by above proposition, we have $xHx^{-1} = H$ for all $x \in G \Longrightarrow (xHx^{-1})x = Hx$ for all $x \in G$, equivalently $xH = Hx$ for all $x \in G$ i.e. each left coset xH is the right coset Hx.
Conversely, suppose that H is a subgroup of a group G such that each left coset of H in G is also a right coset of H in G. Let $x \in G$. Then the left coset xH must be a right coset of H in G. Suppose $xH = Hy$ for some $y \in G$.
Now $x = xe \in xH$, hence $x \in Hy$. Also $x = ex \in Hx$. Thus the right cosets Hx and Hy both contain x. Since any two right cosets are either disjoint or identical, hence we have $Hx = Hy$. Therefore $xH = Hy = Hx$, i.e. $xH = Hx$ and so H is a normal subgroup of G.

Proposition: The intersection of any two normal subgroups of a group is a normal subgroup.

Proof: Let H and K be any two normal subgroups of a group G. Obviously, $H \cap K$ is a subgroup of G. Let $a \in H \cap K$ and $x \in G$. Now

$$a \in H \cap K \Longrightarrow a \in H \text{and } a \in K$$

Since H is normal in G, hence $a \in H, x \in G \Longrightarrow xax^{-1} \in H$. Also K is normal in G, therfore $a \in K, x \in G \Longrightarrow xax^{-1} \in K$.

Now $xax^{-1} \in H$ and $xax^{-1} \in K \Longrightarrow xax^{-1} \in H \cap K$.

Therfore $a \in H \cap K, x \in G \Longrightarrow xax^{-1} \in H \cap K$.

Hence $H \cap K$ is a normal subgroup of G.

Proposition: Let G be a group and H be a subgroup of G of index 2. Then H is a normal subgroup of G.

Proof: We shall prove that $xH = Hx$ for all $x \in G$.

If $x \in H$, then $xH = H = Hx$.

Suppose that $x \notin H$.Then $xH \neq H$. Since the index of H in G is two, hence there are only two distinct left cosets of H in G. So we have $G = xH \cup H$, where xH and H are disjoint.

Similarly, $Hx \neq H$ and $G = Hx \cup H$, where Hx and H are disjoint. Hence we have $G = xH \cup H = G = Hx \cup H$ such that $xH \cap H = \emptyset$ and $Hx \cap H = \emptyset$. Therfore $xH = Hx$.

In unit-2, we have defined the product of any two complexes H and K of a group G as follows-

$$HK = \{x \in G : x = hk, h \in H, k \in K\}$$

If we take $K = H$, we have

$$HH = \{hh' \in G : h, h' \in H\}$$

If H is a subgroup of G, then $hh' \in H$ and hence $HH \subseteq H$.

Also $h \in H \Longrightarrow h = he \in HH$, hence we have $H \subseteq HH$. Therefore $HH = H$.

Note: In general, for a group$(G,*)$, we define

$$H * K = \{x \in G : x = h * k, h \in H, k \in K\}$$

Where $H, K \subseteq G$. Hence in case of additive groups we write $H + K$ for $H * K$. We call $H + K$, the sum of H and K.

Now we prove an important result.

Proposition: A subgroup N of a group G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Proof: Let N be a normal subgroup of a group G. Let $x, y \in G$. Then Nx and Ny are two right cosets of N in G. Now

$$\begin{aligned}(Nx)(Ny) &= N(xN)y \\ &= N(Nx)y \text{ ,as } N \text{ is a normal subgroup} \\ &= NNxy \\ &= Nxy, \text{ as } NN = N\end{aligned}$$

Now $x, y \in G \Longrightarrow xy \in G$, therefore Nxy is a right coset of N in G, i.e. the product of two right cosets of N is again a right coset of N in G.

Conversely, suppose that N is any subgroup of G such that the product of any two right cosets of N in G is also a right coset of N in G. Let $x \in G$ and $a, b \in N$. Then $bx \in Nx$ and $ax^{-1} \in Nx^{-1}$and therefore $bxax^{-1} \in NxNx^{-1}$. If we take $a = b = e$ (identity), then $exex^{-1} \in NxNx^{-1}$, i.e. $e \in NxNx^{-1}$.

By assumption, the product of two right cosets $NxNx^{-1}$ is also a right coset and N is itself a right coset of N in G such that $e \in N$, hence we have $NxNx^{-1} = N$ for all $x \in G$ as two right cosets are either disjoint or identical.
Therefore $bxax^{-1} \in N$ for all $x \in G$.
$\Longrightarrow b^{-1}(bxax^{-1}) \in N$ for all $x \in G$, as N is a subgroup of G
$\Longrightarrow xax^{-1} \in N$ for all $x \in G$,by associativity and the inverse property $b^{-1}b = e$
Thus N is a normal subgroup of G.
Note: If the composition in G is addition, each right coset of N in G is denoted as $N + a$ and we define the addition of two right cosets as follows-

$$(N + a) + (N + b) = N + (a + b)$$

4.5 Quotient Group

If N is a normal subgroup of G, then for any $x \in G$, the left coset xN of N, and the right coset Nx of N are equal. So there is no need to specify these cosets separately. We shall say that Nx (or xN) is a coset of the normal subgroup N.

We have seen that we can define the product of two cosets Nx and Ny as follows-

$$(Nx)(Ny) = Nxy$$

The product Nxy is itself a coset of N. So if we collect all cosets of a normal subgroup$N$, this collection appears to be closed under coset multiplication provided this multiplication is well defined. We shall show that this multiplication is well defined.
Let $x, y, a, b \in G$ and $Nx = Na$, $Ny = Nb$. Hence $x \in Nx \Longrightarrow x \in Na$ and $y \in Ny \Longrightarrow y \in Nb$. Therefore there exist $n_1, n_2 \in N$ such that $x = n_1 a$ and $y = n_2 b$.
Now $(xy)(ab)^{-1} = (n_1 a n_2 b)(b^{-1}a^{-1}) = n_1 a n_2 b b^{-1} a^{-1} = n_1 a n_2 a^{-1}$
Since N is normal, hence $an_2a^{-1} \in N$. Therefore $(xy)(ab)^{-1} = n_1 a n_2 a^{-1} \in N$.
From unit-3, we know that "$hk^{-1} \in N \Longrightarrow Nh = Nk$", hence

$$(xy)(ab)^{-1} \in N \Longrightarrow N(xy) = N(ab)$$
$$\Longrightarrow (Nx)(Ny) = (Na)(Nb)$$

Hence the multiplication of cosets is well defined.
Now we shall prove that this set of all cosets is indeed a group under coset multiplication. This group is called the **quotient group** of G by N, and is denoted by G/N.

Proposition: Let G be a group and N be a normal subgroup of G. The set G/N of all cosets of N in G, is a group under coset multiplication defined as follows-

For any $Na, Nb \in G/N$, $(Na)(Nb) = Nab$

Proof: (1) Closure Law: We have already shown that this composition is well defined and G/N is closed under this composition.
(2) Associativity: Let $Na, Nb, Nc \in G/N$. Then

$$[(Na)(Nb)](Nc) = (Nab)(Nc) = N(ab)c$$

Also $(Na)[(Nb)(Nc)] = (Na)(Nbc) = Na(bc)$
Since $a, b, c \in G \Longrightarrow (ab)c = a(bc)$, hence

$$[(Na)(Nb)](Nc) = (Na)[(Nb)(Nc)]$$

(3) Existence of identity: Let e be the identity element of G. Then $N = Ne \in G/N$ and $(Na)N = (Na)(Ne) = Nae = Na$. Similarly$N(Na) = Na$.
Thus N is the identity element of G/N.
(4) Existence of inverse: Let $a \in G$. Then $a^{-1} \in G$ and hence $Na^{-1} \in G/N$.
Now $(Na)(Na^{-1}) = Naa^{-1} = Ne = N$ and $(Na^{-1})(Na) = Na^{-1}a = Ne = N$.
Therefore $(Na)^{-1} = Na^{-1} \in G/N$.
Hence G/N is a group.
Definition: Let G be a group and N be a normal subgroup of G. Then the set G/N of all cosets of N in G is a group under the composition defined by

$$(Na)(Nb) = Nab \text{ for all } Na, Nb \in G/N$$

This group is called the **factor group** or **quotient group** of G by N.
G/N is read as $\boldsymbol{G}$ **modulo** $\boldsymbol{N}$ or simply $\boldsymbol{G}$ **mod** $\boldsymbol{N}$
If the composition in G is addition, then we have

$$G/N = \{N + a : a \in G\}$$

and the composition in G/N is denoted additively, i.e.

$$(N + a) + (N + b) = N + (a + b) \text{ for all } N + a, N + b \in G/N$$

Example: Let $(\mathbb{Z}, +)$ be the additive group of integers. Then $H = \langle 2 \rangle$, i.e.
$H = \{\dots, -4, -2, 0, 2, 4, \dots\}$ is a subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, hence H is a normal subgroup of $\mathbb{Z}$.
The cosets of H in $\mathbb{Z}$ can be formed as follows-

$$H + 0 = H$$
$$H + 1 = \{h + 1 : h \in H\}$$
$$= \{\dots, -3, -1, 1, 3, \dots\}$$
$$H + 2 = \{\dots -4, -2, 0, 2, 4, \dots\} = H$$
$$H + 3 = \{\dots, -3, -1, 1, 3, \dots\} = H + 1$$

Also $H + (-1) = \{\dots -5, -3, -1, 1, 3, \dots\} = H + 1$, and so on. Therefore the distinct cosets of H in $\mathbb{Z}$ are H and $H + 1$. So the quotient group of $\mathbb{Z}$ by H is

$$\mathbb{Z}/H = \{H, H + 1\}$$

The subgroup $H = \langle 2 \rangle$ is also denoted as $2\mathbb{Z}$ and then we write

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

The quotient group of $\mathbb{Z}$ by $n\mathbb{Z}$ is denoted by $\mathbb{Z}/n\mathbb{Z}$. Now we show that $n\mathbb{Z}, n\mathbb{Z} + 1, \dots, n\mathbb{Z} + (n - 1)$ are the only n cosets of $n\mathbb{Z}$.
Let $m \in \mathbb{Z}$. Then by division algorithm

$$m = nq + r, \text{ where } 0 \leq r < n$$
$$\Longrightarrow m - r = nq \in n\mathbb{Z}$$
$$\Longrightarrow n\mathbb{Z} + m = n\mathbb{Z} + r$$

Since $0 \leq r < n$, hence for any $m \in \mathbb{Z}$, we have $n\mathbb{Z} + m \in \{n\mathbb{Z}, n\mathbb{Z} + 1, \dots, n\mathbb{Z} + (n - 1)\}$. Further these cosets are distinct as for no two distinct non-negative integers r and s both less than n, $r - s$ is a multiple of n, i.e. if $0 \leq r < s < n$, then $r - s \neq nq$ for some $q \in \mathbb{Z}$ and hence $n\mathbb{Z} + r \neq n\mathbb{Z} + s$. Therefore we have

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z} + 1, \dots, n\mathbb{Z} + (n - 1)\}$$

Since $n\mathbb{Z} + r$ and $n\mathbb{Z} + s$ are cosets, hence we have

$$n\mathbb{Z} + r = n\mathbb{Z} + s \Leftrightarrow r - s \in n\mathbb{Z} \Leftrightarrow r \equiv s \pmod{n}$$

Let $n\mathbb{Z} + r,\ n\mathbb{Z} + s \in \mathbb{Z}/n\mathbb{Z}$. Then
$(n\mathbb{Z} + r) + (n\mathbb{Z} + s) = n\mathbb{Z} + (r + s)$
Now if $n\mathbb{Z} + k \in \mathbb{Z}/n\mathbb{Z}$ such that $n\mathbb{Z} + (r + s) = n\mathbb{Z} + k$, then

$(r+s)-k \in \mathbb{Z}/n\mathbb{Z}$, i.e. $k \equiv r+s(\text{mod } n)$. Hence $k = r+_n s$.

$$\therefore (n\mathbb{Z}+r)+(n\mathbb{Z}+s) = n\mathbb{Z}+(r+s)(\text{mod } n) = n\mathbb{Z}+(r+_n s)$$

Here you note that the coset $n\mathbb{Z}+r$ is the same as the residue class $[r]$ (modulo n), i.e. $n\mathbb{Z}+r = [r] = \{x \in \mathbb{Z}: x \equiv r \ (\text{mod } n)\}$. This justifies the use of same notation $\mathbb{Z}/n\mathbb{Z}$ for both the additive group of residue classes modulo n and the quotient group $\mathbb{Z}$ modulo n.

Now we prove an interesting result.

Proposition: The quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}_n$of integers modulo n.

Proof: Define a mapping $f: \mathbb{Z}_n \longrightarrow \mathbb{Z}/n\mathbb{Z}$ such that $f(r) = n\mathbb{Z}+r$ for all $r \in \mathbb{Z}_n$.

Obviously the mapping f is a bijection and for all $r, s \in \mathbb{Z}_n$,we have

$$\begin{aligned} f(r+_n s) &= n\mathbb{Z}+(r+_n s) \\ &= n\mathbb{Z}+(r+s)(\text{mod } n) \\ &= (n\mathbb{Z}+r)+(n\mathbb{Z}+s) \\ &= f(r)+f(s) \end{aligned}$$

Thus f is an isomorphism of $\mathbb{Z}_n$ onto $\mathbb{Z}/n\mathbb{Z}$ and therefore $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Interestingly, if the group G is finite, then the order of a quotient group G/N can be obtained using Lagrange's theorem. Hence we have the following result.

Proposition: Let G be a finite group and N be a normal subgroup of G. Then

$$o(G/N) = \frac{o(G)}{o(N)}$$

Proof: By Lagrange's theorem the number of distinct cosets of N in G is equal to $o(G)/o(N)$. Therefore, we have

$$\begin{aligned} o(G/N) &= \text{number of distinct cosets of } N \text{ in } G \\ &= \frac{o(G)}{o(N)} \end{aligned}$$

We shall come back with more tools and techniques after studying center of group, kernel of homomorphism and the fundamental theorem of homomorphism. You will appreciate many interesting properties of quotient groups after studying the following sections.

4.6 Relation of conjugacy and conjugate elements

Definition: Let G be a group and $a, b \in G$. Then the element a is said to be a **conjugate** of b in G if there exists $x \in G$ such that $a = x^{-1}bx$.

If a is conjugate to b then symbolically we write $a \sim b$. This relation in G is called the **relation of conjugacy.**

Proposition: The relation of conjugacy is an equivalence relation on a group G.

Proof: (1) *Reflexivity*: Since $a = a^{-1}aa$, hence $a \sim a$.

(2) *Symmetry*: we have $a \sim b \Longrightarrow a = x^{-1}bx$ for some $x \in G$,

$$\Longrightarrow xax^{-1} = x(x^{-1}bx)x^{-1}$$

$$\Longrightarrow b = xax^{-1} = (x^{-1})^{-1}ax^{-1}$$

$$\Longrightarrow b = yay^{-1} \text{ where } y = x^{-1} \in G$$

$$\Rightarrow b \sim a$$

(3) *Transitivity*: We have

$$a \sim b, b \sim c \Rightarrow a = x^{-1}bx, b = y^{-1}cy \text{ for some } x, y \in G$$
$$\Rightarrow a = x^{-1}(y^{-1}cy)x = (x^{-1}y^{-1})c(xy) = (xy)^{-1}c(xy)$$
$$\Rightarrow a \sim c$$

Hence the relation of conjugacy is an equivalence relation on G. Therefore the group G is decomposed into equivalence classes under this equivalence relation. These equivalence classes are called the **conjugate classes**. For any $a \in G$, the conjugate class of a is denoted by $C(a)$ and

$$C(a) = \{b \in G : a \sim b\}$$

Therefore $C(a)$ consists of all elements of the form $x^{-1}ax$

i.e. $$C(a) = \{x^{-1}ax : x \in G\}$$

For example, $C(e) = \{x^{-1}ex : x \in G\} = \{x^{-1}x : x \in G\} = \{e\}$

Suppose G is a finite group and $C(a_1), C(a_2), \ldots, C(a_k)$ are the distinct conjugate classes of G. Then these classes are pairwise disjoint and their union is G.

$$G = C(a_1) \cup C(a_2) \cup \ldots \cup C(a_k)$$

If c_{a_i} denotes the number of elements in$C(a_i)$, then

$$o(G) = \sum_{i=1}^{k} c_{a_i}$$

In order to determine c_{a_i}, we first introduce the notion of the *normalizer* of an element of G.

4.7 Normalizer of an element of a group

Definition: Let G be a group and $a \in G$. Then the **normalizer of a** in G is defined as the set $N(a) = \{x \in G : ax = xa\}$.
For instance, $N(e) = \{x \in G : ex = xe\} = G$.
Also if G is abelian, then $ax = xa$ for all $x \in G$. Therefore $N(a) = G$ for all $a \in G$.
Proposition: The normalizer of an element in a group G is a subgroup of G.
Proof: Let $a \in G$. Then the normalizer of a in G,

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

If e is the identity of G then $ea = ae$, i.e. $e \in N(a)$. Hence $N(a)$ is non-empty. Let $x, y \in N(a)$. Then we have $ax = xa$ and $ay = ya$. Now

$$ay = ya \Rightarrow y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$$
$$\Rightarrow y^{-1}a = ay^{-1}$$
$$\Rightarrow y^{-1} \in N(a)$$

Therefore we have

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$$

$\Longrightarrow xy^{-1} \in N(a)$

Hence $x, y \in N(a) \Longrightarrow xy^{-1} \in N(a)$

Therefore $N(a)$ is a subgroup of G.

We are now in a position to count c_{a_i}, i.e. the number of elements in the conjugate class $C(a_i)$.

Proposition: If G is a finite group and $a \in G$, then

$$c_a = \frac{o(G)}{o[N(a)]}$$

Proof: First we show that there is a one-to-one correspondence between the conjugates of a and right cosets of $N(a)$.

Let $x, y \in G$ belong to the same right coset of $N(a)$ in G, i.e. there is some right coset $N(a)h$ of $N(a)$ in G such that $x, y \in N(a)h$. Then $N(a)x = N(a)h$ and $N(a)y = N(a)h$. Therefore $N(a)x = N(a)y$, i.e. $xy^{-1} \in N(a)$.

Now $xy^{-1} \in N(a) \Longrightarrow xy^{-1}a = axy^{-1}$

$\Longrightarrow x^{-1}(xy^{-1}a)y = x^{-1}(axy^{-1})y$

$\Longrightarrow y^{-1}ay = x^{-1}ax$

Thus if x, y belong to the same right coset of $N(a)$ in G, then x, y yield same conjugate of a. Similarly it can be shown that if x, y belong to different right cosets of $N(a)$ in G, then x, y give rise to different conjugates of a. Hence there is a one-to-one correspondence between the conjugates of a and right cosets of $N(a)$

Since $N(a)$ is a subgroup of G, hence by Lagrange's theorem the number of distinct right cosets of $N(a)$ in G is

$$\frac{o(G)}{o[N(a)]}$$

Now c_a = the number of distinct elements in $C(a)$

= the number of elements conjugate to a

= the number of distinct right cosets of $N(a)$ in G

= $\frac{o(G)}{o[N(a)]}$

Corollary: If G is a finite group, then

$$o(G) = \sum_a \frac{o(G)}{o[N(a)]}$$

where the sum runs over element a, taken one each from each conjugate class.

Proof: Let $C(a_1), C(a_2), \ldots, C(a_k)$ be the distinct conjugate classes of G and $o[C(a_i)] = c_{a_i}$.Then

$$o(G) = \sum_{i=1}^{k} c_{a_i} = \sum_{i=1}^{k} \frac{o(G)}{o[N(a_i)]}$$

We can write it simply as

$$o(G) = \sum_a \frac{o(G)}{o[N(a)]}$$

4.8 Center of a group

Let G be a group.The conjugate class of $a \in G$ in G is given as

$$C(a) = \{x^{-1}ax : x \in G\}$$

If a is the only element conjugate to itself, then $C(a) = \{a\}$. Such elements are called self-conjugate elements. Hence $a \in G$ is self-conjugate iff

$$a = x^{-1}ax \text{ for all } x \in G$$

or $$xa = ax \text{ for all } x \in G$$

The set of all self-conjugate elements of G is called the center of G. So we have the following definition-

Definition: Let G be a group. Then the **center** $Z(G)$ of G is defined by

$$Z(G) = \{z \in G : zx = xz \ \forall x \in G\}$$

Thus the center of a group G is the set of all those elements of G which commute with each element of G.

Proposition The center $Z(G)$ of a group G is a normal subgroup of G.

Proof: We have

$$Z(G) = \{z \in G : zx = xz \ \forall x \in G\}$$

First we show that $Z(G)$ is a subgroup of G.

Let $a, b \in Z(G)$. Then $ax = xa$ and $bx = xb$ for all $x \in G$.

Now $bx = xb \Longrightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1}$

$$\Longrightarrow (b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1})$$

$$\Longrightarrow exb^{-1} = b^{-1}xe$$

$$\Longrightarrow xb^{-1} = b^{-1}x$$

Hence $bx = xb$ for all $x \in G \Longrightarrow xb^{-1} = b^{-1}x$ for all $x \in G$.

Therefore $b^{-1} \in Z(G)$. Hence we have

$$(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}) \ \forall x \in G$$

$$\therefore a, b \in Z(G) \Longrightarrow ab^{-1} \in Z(G)$$

Thus $Z(G)$ is a subgroup of G.

Now we prove that $Z(G)$ is a normal subgroup of G. Let $z \in Z(G)$ and $\in G$. Then $xzx^{-1} = zxx^{-1} = ze = z \in Z(G)$.

Therefore $z \in Z(G)$ and $x \in G \Longrightarrow xzx^{-1} \in Z(G)$, i.e. $Z(G)$ is a normal subgroup of G.

Proposition Let G be a finite group and $Z(G)$ be the center of G. Then $a \in Z(G)$ if and only if $N(a) = G$. If G is finite, $a \in Z(G)$ if and only if $o[N(a)] = o(G)$.

Proof: If $a \in Z(G)$, then $xa = ax$ for all $x \in G$. By definition of $N(a)$, we have $N(a) = G$.

Conversely, suppose $N(a) = G$. Then $xa = ax$ for all $x \in G$, i.e. $a \in Z(G)$.

If the group G is finite, then $N(a) = G$ is equivalent to $o[N(a)] = o(G)$. Hence the result.

Proposition (The Class Equation) Let G be a finite group and $Z(G)$ be the center of G. Then

$$o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

Where the summation runs over elements taken one from each of those distinct conjugate classes which contain more than one element.

Proof: We have

$$o(G) = \sum_{a} \frac{o(G)}{o[N(a)]}$$

From above proposition, we know that $a \in Z(G) \Leftrightarrow o[N(a)] = o(G)$. Therefore the number of distinct elements in $C(a)$,

$$c_a = \frac{o(G)}{o[N(a)]} = 1$$

Hence the number of conjugate classes each having only one element is $o[Z(G)]$.
Therefore

$$o(G) = \sum_{a} \frac{o(G)}{o[N(a)]} = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

This equation is called the **class equation** of the group G. This equation plays an important role in the structure theory of non-abelian finite groups. In case of abelian groups, we have $Z(G) = G$ and hence $c_a = 1$ for all $a \in G$. Let us now discuss some applications of class equation.

Proposition If $o(G) = p^n$, where p is a prime number, then $Z(G) \neq \{e\}$.
Proof: Let $o[Z(G)] = z$. The class equation of the group G is

$$o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

$$\Longrightarrow p^n = z + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

Where the summation runs over elements taken one from each of those distinct conjugate classes which contain more than one element.

Now $a \notin Z(G) \Longrightarrow o[N(a)] \neq o(G)$. Therefore $o[N(a)] < o(G) = p^n$. Since $o[N(a)]$ is a subgroup of G, hence by Lagrange's theorem $o[N(a)]$ must divide $o(G)$, i.e. $o[N(a)] = p^{n_a}$ for some integer n_a such that $1 \leq n_a < n$. Therefore we have

$$p^n = z + \sum_{n_a<n} \frac{p^n}{p^{n_a}}$$

or

$$z = p^n - \sum_{n_a<n} \frac{p^n}{p^{n_a}}$$

Since $p|p^n$ and $p|\frac{p^n}{p^{n_a}}$ as $n_a < n$, therefore $p|z$. Since $e \in Z(G)$, hence $z \neq 0$. Thus z is a positive integer divisible by the prime number p. Therefore $z > 1$. Hence there must exist an element in $Z(G)$ besides e, i.e. $Z(G) \neq \{e\}$.

Corollary: If $o(G) = p^2$ where p is a prime number, then G is abelian.

Proof: In order to show that G is abelian, We shall show that $Z(G) = G$.

By above proposition, we have $Z(G) \neq \{e\}$. Hence we must have either $o[Z(G)] = p$ or $o[Z(G)] = p^2$.

If $o[Z(G)] = p$, then there exists $a \in G$ such that $a \notin Z(G)$. Now

$$z \in Z(G) \Longrightarrow zx = xz \; \forall x \in G$$

In particular,$za = az$ as $a \in G$. Therefore $z \in N(a)$. Also $a \in N(a)$, hence we have $Z(G) \subset N(a)$. Thus $N(a)$ is a subgroup of G such that $Z(G) \subset N(a)$. Hence we must have $o[N(a)] > o[Z(G)]$ such that $o[N(a)]|o(G)$ (by Lagrange's theorem), i.e. $o[N(a)] > p$ such that $o[N(a)]|p^2$. The only possibility is $o[N(a)] = p^2$, i.e. $N(a) = G$. Hence $a \in Z(G)$, a contradiction. Thus $o[Z(G)] \neq p$. Therefore the only possibility is that $o[Z(G)] = p^2 = o(G)$, i.e. $Z(G) = G$. Hence G is abelian.

So you have seen how the concept of center of a group is instrumental in discovering some important counting techniques. Now let us discuss some other applications of this concept.

The center $Z(G)$ of a group G is a normal subgroup of G. Hence $G/Z(G)$ is a quotient group. The quotient groups are important as we can deduce properties of the group by examining its quotient groups. Now we shall see how the quotient group $G/Z(G)$ helps us in revealing some information regarding G.

Proposition: Let $Z(G)$ be the center of a group G. If $G/Z(G)$ is cyclic, then G is abelian.

Proof: If $G/Z(G)$ is cyclic, then $G/Z(G) = \langle gZ(G) \rangle$ for some $g \in G$. Let $a, b \in G$. Then $aZ(G), bZ(G) \in G/Z(G)$. Therefore there exist integers m and n such that $aZ(G) = [gZ(G)]^m$ and $bZ(G) = [gZ(G)]^n$. Now

$$aZ(G) = [gZ(G)]^m \Longrightarrow aZ(G) = g^m Z(G)$$

Since $a \in aZ(G)$, hence there exists $z_1 \in Z(G)$ such that $a = g^m z_1$.

Similarly there exists $z_2 \in Z(G)$ such that $b = g^n z_2$. Now

$$\begin{aligned} ab &= (g^m z_1)(g^n z_2) \\ &= g^m(z_1 g^n)z_2, \quad \text{by associativity} \\ &= g^m(g^n z_1)z_2, \text{ since } z_1 \in Z(G) \Longrightarrow z_1 g^n = g^n z_1 \\ &= g^m(g^n z_1)z_2 \\ &= (g^m g^n)(z_1 z_2) \\ &= g^{m+n} z_1 z_2 \end{aligned}$$

Similarly $ba = g^{n+m} z_2 z_1 == g^{m+n} z_1 z_2$ as $z_1, z_1 \in Z(G) \Longrightarrow z_1 z_2 = z_2 z_1$

Therefore $ab = ba$, i.e. the group G is abelian.

Remark: In this case, we have $G = Z(G)$ and so $G/Z(G)$ is the trivial group.

4.9 Kernel of a homomorphism

In unit 2, we discussed the notion of group homomorphism.. Recall that a homomorphism of a group G into a group $G'$is a mapping $f: G \longrightarrow G'$ which preserves the compositions in G and G', i.e.

$$f(ab) = f(a)f(b) \text{ for all } a, b \in G$$

In this section, we shall introduce the notion of the kernel of a homomorphism and use this notion to obtain some important theorems on homomorphisms.

Definition: Let f be a homomorphism of a group G into a group G', then the kernel of f is the set of all those elements of G which are mapped onto the identity $e'$of G'. We shall denote the kernel of f by Ker$f$. Hence

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

Example 1 The mapping $f: \mathbb{R} \longrightarrow \mathbb{R}^+$ defined by $f(x) = e^x$ for all $x \in \mathbb{R}$ is a homomorphism of the additive group of all real numbers $(\mathbb{R}, +)$ onto the multiplicative group of all positive real numbers $(\mathbb{R}^+, \cdot)$ and

$$\text{Ker}f = \{x \in \mathbb{R}: f(x) = 1\} = \{0\}$$

Example 2 Let $(\mathbb{R}^*, \cdot)$ be the multiplicative group of all non-zero real numbers. The mapping $f: \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = |x|$ for all $x \in \mathbb{R}^*$ is a homomorphism with Ker$f = \{x \in \mathbb{R}^*: f(x) = 1\} = \{-1, 1\}$.

We shall now prove that the kernel of a homomorphism $f: G \longrightarrow G'$ is a normal subgroup of G.

Proposition Let f be a homomorphism of a group G into a group G', then the kernel of f is a normal subgroup of G.

Proof: We have

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

First we shall show that Ker$f$ is a subgroup of G. Since $f(e) = e'$, hence $e \in \text{Ker}f$. Therefore Ker$f$ is non-empty. Let $a, b \in \text{Ker}f$. Then $f(a) = e'$ and $f(b) = e'$. Now

$$f(ab^{-1}) = f(a)f(b^{-1}) \text{ as } f \text{ is a homomorphism}$$

$$= f(a)[f(b)]^{-1}, \quad \text{since } f(b^{-1}) = [f(b)]^{-1}$$

$$= e'(e')^{-1} = e'e' = e'$$

$$\Longrightarrow ab^{-1} \in \text{Ker}f$$

Hence Ker$f$ is a subgroup of G.

Now if $x \in G$ and $a \in \text{Ker}f$, then

$$f(xax^{-1}) = f(x)f(a)f(x^{-1}) = f(x)e'[f(x)]^{-1} = f(x)[f(x)]^{-1} = e'$$
$$\Longrightarrow xax^{-1} \in \text{Ker}f$$

Thus $x \in G$ and $a \in \text{Ker}f \Longrightarrow xax^{-1} \in \text{Ker}f$, i.e. Ker$f$ is a normal subgroup of G.

Now you will notice an interesting point. The homomorphism f is projecting the normal subgroup Ker$f$ of G onto the identity e' and hence we have

$$\text{Ker}f = f^{-1}(\{e'\})$$

you may ask if we have some expression for $f^{-1}(\{a'\})$ in terms of Ker$f$ for any $a' \in G'$. The following proposition answers this positively.

Proposition Let f be a homomorphism of a group G into a group G'. Let $K = \text{Ker}f$ and $a' = f(a) \in G'$ for some $a \in G$. Then

$$f^{-1}(\{a'\}) = Ka = aK$$

Proof: We have $f^{-1}(\{a'\}) = \{x \in G : f(x) = a'\} = \{x \in G : f(x) = f(a)\}$

Let $y \in Ka$. Then there exists $k \in K$ such that $y = ka$.

Now $f(y) = f(ka) = f(k)f(a) = e'f(a) = f(a) = a'$

$\Longrightarrow y \in f^{-1}(\{a'\})$

Hence we have $Ka \subseteq f^{-1}(\{a'\})$.

Now let $x \in f^{-1}(\{a'\})$. Then $f(x) = a' = f(a)$. We have

$$f(xa^{-1}) = f(x)f(a^{-1}) = f(a)[f(a)]^{-1} = e'$$

$$\Longrightarrow xa^{-1} \in \text{Ker}f = K$$

$$\Longrightarrow x \in Ka$$

Hence we have $f^{-1}(\{a'\}) \subseteq Ka$.

The two inclusions $Ka \subseteq f^{-1}(\{a'\})$ and $f^{-1}(\{a'\}) \subseteq Ka$ implies that

$$f^{-1}(\{a'\}) = Ka$$

Since $\text{Ker}f = K$ is a normal subgroup of G, hence $Ka = aK$. Therefore we have

$$f^{-1}(\{a'\}) = Ka = aK$$

From this proposition it is clear that for $a \in G$, the cosets $(\text{Ker}f)a$ and $a(\text{Ker}f)$ are equal, and are projected onto the single element $f(a)$ by the homomorphism f. Hence if $o(\text{Ker}f) = n$, then f maps n elements of $(\text{Ker}f)a$ onto the single element $f(a)$ of $f(G) \subseteq G'$, i.e. the homomorphism f is an n-to-1 mapping from G onto $f(G)$. Hence the size of $\text{Ker}f$ determines the nature of homomorphism f. Obviously if $o(\text{Ker}f) = 1$, then f will be a one-to-one mapping of G into G'. So we have the following proposition-

Proposition A homomorphism f of a group G into a group G' is a monomorphism if and only if $\text{Ker}f = \{e\}$.

Proof: Let us first suppose that f is a monomorphism, i.e. f is one-one. Let $x \in \text{Ker}f$, then

$$f(x) = e'$$

$$\Rightarrow f(x) = f(e) \text{ as } f(e) = e'$$

$$\Rightarrow x = e \text{ as } f \text{ is one-one}$$

Therefore $\text{Ker}f = \{e\}$.

Conversely, suppose that $\text{Ker}f = \{e\}$. Let $a, b \in \text{Ker}f$. Then

$$f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} = f(a)[f(b)]^{-1}$$

$$\Rightarrow f(a)[f(b)]^{-1} = e'$$

$$\Rightarrow f(a)f(b^{-1}) = e', \quad \text{since } [f(b)]^{-1} = f(b^{-1})$$

$$\Rightarrow f(ab^{-1}) = e', \text{ as } f \text{ is a homomorphism}$$

$$\Rightarrow ab^{-1} \in \text{Ker}f$$

$$\Rightarrow ab^{-1} = e, \text{ as } \text{Ker}f = \{e\}$$

$$\Rightarrow a = b$$

Hence f is one-one, i.e.f is a monomorphism.

Proposition Let G be a group and N a normal subgroup of G. Define a mapping $f: G \longrightarrow G/N$ by $f(x) = Nx$ for all $x \in G$.Then f is a homomorphism of G onto G/N and $\text{Ker}f = N$.
Proof: Let $x, y \in G$. Then

$$f(xy) = Nxy = (Nx)(Ny) = f(x)f(y)$$

Hence f is a homomorphism.
Now let $Nx \in G/N$. Then $x \in G$ and we have $f(x) = Nx$. Therefore f is onto.
Thus f is a homomorphism of G onto G/N.
We have Ker$f = \{x \in G: f(x) = N\}$. We shall prove that Ker$f = N$.
Let $x \in$ Ker$f$, then $f(x) = N$.
Now $f(x) = N \Longrightarrow Nx = N \Longrightarrow x \in N$
Hence Ker$f \subseteq N$.
Now suppose that $x \in N$. Then $Nx = N$. Therefore

$$f(x) = Nx = N$$
$$\Longrightarrow x \in \text{Ker}f$$

Thus $N \subseteq$ Ker$f$.
Consequently, Ker$f = N$.
The homomorphism $f: G \longrightarrow G/N$ defined by $f(x) = Nx$ for all $x \in G$ is called the **natural projection (homomorphism)** of G onto G/N.

4.10 Fundamental theorem of Homomorphism

This is an important result which tells us that every homomorphic image of a group G is isomorphic to some quotient group of G.
Theorem Let f be a homomorphism of a group G onto a group $G'$with kernel K. Then $G/K \cong G'$.
Proof: Since the kernel K of the homomorphism $f: G \longrightarrow G'$ is a normal subgroup of G, hence G/K is a quotient group. Define $\varphi: G/K \longrightarrow G'$ by

$$\varphi(Kx) = f(x) \text{ for all } x \in G$$

First we show that φ is well defined. Let $x, y \in G$. Then

$$\begin{aligned} Kx = Ky &\Longrightarrow xy^{-1} \in K \\ &\Longrightarrow f(xy^{-1}) = e' \\ &\Longrightarrow f(x)f(y^{-1}) = e' \\ &\Longrightarrow f(x)[f(y)]^{-1} = e' \\ &\Longrightarrow f(x) = f(y) \\ &\Longrightarrow \varphi(Kx) = \varphi(Ky) \end{aligned}$$

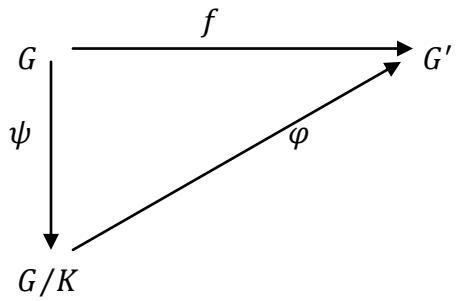
Consequently φ is well defined.
Now let $Kx, Ky \in G/K$. Then

$$\varphi[(Kx)(Ky)] = \varphi(Kxy) = f(xy) = f(x)f(y) = \varphi(Kx)\varphi(Ky)$$

Hence φ preserves compositions in G/K and G'.
Also $\varphi(Kx) = \varphi(Ky)$

$$\begin{aligned} &\Longrightarrow f(x) = f(y) \\ &\Longrightarrow f(x)[f(y)]^{-1} = e' \\ &\Longrightarrow f(x)f(y^{-1}) = e' \\ &\Longrightarrow f(xy^{-1}) = e' \\ &\Longrightarrow Kx = Ky \end{aligned}$$

Thus φ is one-one.
Since $f: G \longrightarrow G'$is onto, hence $y \in G' \Longrightarrow \exists x \in G$such that $y = f(x)$. Therefore $\varphi(Kx) = f(x) = y$, i.e. φ is onto.
Thus φ is an isomorphism of G/K onto $G'$and hence $G/K \cong G'$.
We can represent the result pictorially as follows-



We say that the above diagram commutes if $\varphi o\psi = f$.
Here $(\varphi o\psi)(x) = \varphi\{\psi(x)\} = \varphi(Kx) = f(x)$ for all $x \in G$, i.e. the diagram is commutative. The isomorphism φ is referred to as **natural or canonical isomorphism.** For a given homomorphism f, the mappings ψ and φ are uniquely determined by the fundamental theorem of homomorphism.

This theorem tells us that different homomorphic images $G'$of a group G can be expressed as different quotient groups G/K, where K is the kernel of the homomorphism. We know that for any normal subgroup N of G, the mapping $\psi: G \longrightarrow G/N$ defined by $\psi(x) = Nx$ for all $x \in G$ is a homomorphism of G onto G/N, i.e. G/N is a homomorphic image of G. Therefore there is a one-to-one correspondence between the normal subgroups of G and homomorphic images of G. Hence we can obtain all homomorphic images of a group G as follows-
(1) First find all normal subgroups of G
(2) For each normal subgroup N, construct the corresponding quotient group G/N.
(3)This set of quotient groups gives us all homomorphic images of G (upto isomorphisms).
Example Find all the homomorphisms from $\mathbb{Z}_6$ onto $\mathbb{Z}_5$.
Let $\varphi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_5$ be one such homomorphism with Ker$\varphi = K$. Then K is a normal subgroup of $\mathbb{Z}_6$. By Lagrange's theorem, order of K must divide the order of $\mathbb{Z}_6$. Since $o(\mathbb{Z}_6) = 6$, hence the order of $K = 1,2,3$ or 6.
From the fundamental theorem of homomorphism, we have

$$\mathbb{Z}_6/K \cong \mathbb{Z}_5$$
$$\Longrightarrow o(\mathbb{Z}_6/K) = o(\mathbb{Z}_5) = 5$$

If $o(K) = 1$, then

$$o(\mathbb{Z}_6/K) = \frac{o(\mathbb{Z}_6)}{o(K)} = \frac{6}{1} = 6$$

Hence we cannot have $\mathbb{Z}_6/K \cong \mathbb{Z}_5$.
Similarly, If $o(K) = 2$, then $o(\mathbb{Z}_6/K) = \frac{o(\mathbb{Z}_6)}{o(K)} = \frac{6}{2} = 3$. Hence $\mathbb{Z}_6/K \ncong \mathbb{Z}_5$
If $o(K) = 3$, then $o(\mathbb{Z}_6/K) = \frac{o(\mathbb{Z}_6)}{o(K)} = \frac{6}{3} = 2$, i.e. $\mathbb{Z}_6/K \ncong \mathbb{Z}_5$
If $o(K) = 6$, then $o(\mathbb{Z}_6/K) = \frac{o(\mathbb{Z}_6)}{o(K)} = \frac{6}{6} = 1$, i.e. $\mathbb{Z}_6/K \ncong \mathbb{Z}_5$
Therefore in all these cases we cannot have $\mathbb{Z}_6/K \cong \mathbb{Z}_5$. Hence there exists no homomorphism of $\mathbb{Z}_6$ onto $\mathbb{Z}_5$.

4.11 Direct and inverse images of a subgroup and normal subgroups

Let f be a homomorphism from a group G to a group G'. Let H be a subgroup of G and H' be a subgroup of G'. Then we define the **direct image** of H under f as follows-

$$f(H) = \{f(h) \in G' : h \in H\}$$

and the **inverse image** of H'as follows-

$$f^{-1}(H') = \{h \in G : f(h) \in H'\}$$

Now we shall study the properties $f(H)$ and $f^{-1}(H')$.

Property-1 $f(H)$ is a subgroup of G'.

Proof: Since $e \in H$, hence $e' = f(e) \in f(H)$. Hence $f(H)$ is non-empty. Let $a, b \in f(H)$. Then there exists $h, k \in H$ such that $a = f(h)$ and $b = f(k)$.

Now $ab^{-1} = f(h)[f(k)]^{-1} = f(h)f(k^{-1}) = f(hk^{-1})$

Since H is a subgroup of G, hence

$$h, k \in H \Longrightarrow hk^{-1} \in H$$
$$\Longrightarrow f(hk^{-1}) \in f(H)$$

Hence $ab^{-1} \in f(H)$. Thus $f(H)$ is a subgroup of G.

Property-2 If H is abelian, then $f(H)$ is abelian.

Proof: Suppose H is abelian. Let $a, b \in f(H)$. Then there exists $h, k \in H$ such that $a = f(h)$ and $b = f(k)$.

Since H is abelian, hence $hk = kh$. Therefore

$$ab = f(h)f(k) = f(hk) = f(kh) = f(k)f(h) = ba$$

Hence $f(H)$ is abelian.

Property-3 If H is normal in G, then $f(H)$ is normal in $f(G)$.

Proof: Let $a \in f(H)$ and $y \in f(G)$. Then there exist $h \in H$ and $x \in G$ such that $a = f(h)$ and $y = f(x)$.

Since H is normal in G, hence

$$h \in H \text{ and } x \in G \Longrightarrow xhx^{-1} \in H$$

Now $yay^{-1} = f(x)f(h)[f(x)]^{-1} = f(x)f(h)f(x^{-1}) = f(xhx^{-1}) \in f(H)$

Thus $f(H)$ is normal in $f(G)$.

Property-4 If H' be a subgroup of G', then $f^{-1}(H')$ is a subgroup of G.

Proof: We have

$$f^{-1}(H') = \{h \in G : f(h) \in H'\}$$

Since $e' = f(e) \in H'$, hence $e \in f^{-1}(H')$. Thus $f^{-1}(H')$ is non-empty. Let $h, k \in f^{-1}(H')$. Then $f(h), f(k) \in H'$ and therefore $[f(k)]^{-1} \in H'$. Now

$f(hk^{-1}) = f(h)f(k^{-1}) = f(h)[f(k)]^{-1} \in H'$. Hence by definition of $f^{-1}(H')$, we have $hk^{-1} \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is a subgroup of G.
Similarly we can prove the following properties:
Property-5 If H is cyclic, then $f(H)$ is cyclic.
Property-6 If H' be a normal subgroup of G', then $f^{-1}(H')$ is a normal subgroup of G.

4.12 Summary

In this unit, we have

(1) Defined the normal subgroup of a group G as a subgroup H of G such that
$$xHx^{-1} \subseteq H \text{ for every } x \in G$$
(2) Discussed various examples and properties of normal subgroups.
(3) Defined quotient group G/N of a group G and discussed examples and properties of quotient groups.

(4) Defined the relation of conjugacy $\sim$ in the group G as $a \sim b \Leftrightarrow a = x^{-1}bx$ for some $x \in G$ and proved that it is an equivalence relation in G.

(5) Defined the nomalizer $a \in G$ in the group G as the set
$$N(a) = \{x \in G : ax = xa\}$$
(6) Proved that the normalizer of an element is a subgroup of the group and obtained some other results related to $N(a)$.
(7) Defined the center of a group G as $Z(G) = \{z \in G : zx = xz \ \forall x \in G\}$. We then proved that the center of a group G is a normal subgroup of G. We discussed properties of $Z(G)$ and proved the class equation
$$o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$
(8) Defined the kernel of a homomorphism f as $\text{Ker}f = \{x \in G : f(x) = e'\}$ and proved that $\text{Ker}f$ is a normal subgroup of G. We proved results concerning $\text{Ker}f$.
(9) Proved the fundamental theorem of homomorphism, that is, every homomorphic image of a group G is isomorphic to some quotient group of G.
(10) Discuss the properties of direct image $f(H)$ of subgroup H and the inverse image $f^{-1}(H')$ of subgroup H' under the homomorphism f.

4.13 Self assessment questions

(1) Prove that the intercestion of any collection of normal subgroups is itself a normal subgroup.

(2) H is a normal subgroup of G and K is a subgroup of G such that $H \subseteq K \subseteq G$. Show that H is a normal subgroup of K.

(3) If H and K are normal subgroups of G, prove that HK is also a normal subgroup of G.

(4) Let H and K be normal subgroups of G such that $H \cap K = \{e\}$. Show that every element of H commutes with every element of K.

(5) Let H be the only subgroup of finite order n in a group G. Show that H is normal in G

(6) Let H be a subgroup of a group G such that $x^2 \in H \ \ \forall x \in G$. Show that H is a normal subgroup of G.

(7) Show that the set of all $n \times n$ matrices with determinant 1 forms a normal subgroup of $GL_n(\mathbb{R})$.

(8) Show that every quotient group of an abelian group is abelian and the converse is not true.

(9) Show that every quotient group of a cyclic group is cyclic and the converse is not true.

(10) Let G be a non-abelian group of order p^3, where p is a prime number. Show that the center of G has exactly p elements.

(11) Let f be a homomorphism of a group G into a group G'. Show that $f(G)$ is a subgroup of G'.

(12) Show that every homomorphic image of an abelian group is abelian and the converse is not true.

(13) Show that the mapping $f: \mathbb{C} \longrightarrow \mathbb{R}$ given by $f(z) = Re(z)$ is a homomorphism. Where $\mathbb{C}$ and $\mathbb{R}$ are the additive groups of complex numbers and real numbers respectively. Find $\mathrm{Ker}f$.

[HINT: $\mathrm{Ker}f$ consists of $z \in \mathbb{C}$ such that $Re(z) = 0$]

(14) Let f be a homomorphism of a group G onto a group G' and $H = \mathrm{Ker}f$. Let K'be any normal subgroup of $G'$and $K = \{x \in G: f(x) \in K'\} = f^{-1}(K')$. Show that K is a normal subgroup of G containing H and $G/K \cong G'/K'$.

(15) Let H and K be two normal subgroups of G such that $H \subseteq K$. Show that K/H is a normal subgroup of G/H and

$$G/K \cong (G/H)/(K/H)$$

(16) Let H be a normal subgroup of a group G, and K be any subgroup of G. Show that $K/H \cap K \cong HK/H$.

(17) Show that it is impossible to find a homomorphism of $\mathbb{Z}$ onto $S_n (n > 2)$.

(18) Show that $Q_8/\{1, -1\}$ is isomorphic to Klein's four group V.

(19) Show that $\mathbb{Z}_n$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z})$.

(20) Show that every abelian group of order pq where p and q are distinct primes is cyclic.

4.14 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

(6) Lang, S. (1965): Algebra, Reading, Massachusetts, Addison-Wesley.

Unit-5: Symmetric Groups and Automorphisms

Structure

5.1 Introduction

You have already studied permutations and symmetric groups in unit-1. In this unit, we shall study symmetric groups on finite sets in details We shall also study some basic concepts related to permutations such as cycles, transpositions, orbits, decomposition of a permutation into disjoint transpositions, cyclic permutations, even and odd permutations and alternating group. Permutation groups are of great importance as we shall see that every finite group is isomorphic to some permutation group. This famous result is known as Cayley's theorem after the English mathematician Arthur Cayley. We shall prove the Cayley's theorem. You will be surprised to know that some specific permutation groups were the only groups studied by the mathematicians in the beginning of group theory.

In unit-2, we introduced the notion of an automorphism. Recall that an isomorphism of a group G onto itself is called an automorphism of G. We shall make a detailed study of automorphisms and inner automorphisms of groups.

5.2 Objectives

After reading this unit, you should be able to

- Define and discuss the Symmetric group of degree n
- Illustrate the concept of cycles, transpositions and orbits
- Describe the decomposition of a permutation into transpositions
- Define even and odd permutation
- Describe the Alternating group
- Prove the Cayley's theorem

- Define the automorphism and inner automorphism of groups

5.3 Symmetric group

In unit-1, we have introduced the notion of a permutation of a nonempty set. Recall that a one-one mapping of a non-empty set S onto itself (i.e. bijections from S to itself) is called a **permutation**.

Let $S = \{a_1, a_2, \dots, a_n\}$ and f be a permutation of S such that

$$f(a_1) = b_1, f(a_2) = b_2, \dots\dots, f(a_n) = b_n$$

where $b_1, b_2, \dots, b_n$ is some arrangement of the elements $a_1, a_2, \dots, a_n$. Then f is represented as follows-

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

This notation is known as *2-rowed notation* for f. The elements of S can be put in any order in the first row. For example, If $S = \{1,2,3,4\}$, we have

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \text{ etc}$$

We have already explained the method of multiplication of two permutations in unit-1.

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}$ and $g = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ g(a_1) & g(a_2) & \dots & g(a_n) \end{pmatrix}$. Then the product fg of permutations f and g is defined as follows-

$$fg = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ (fog)(a_1) & (fog)(a_2) & \dots & (fog)(a_n) \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f\{g(a_1)\} & f\{g(a_1)\} & \dots & f\{g(a_1)\} \end{pmatrix}$$

Here you should remember that the composition is applied from *right to left order*.

The set $A(S)$ of all permutations of S forms a group with respect to composition of functions and is called the **symmetric group**. Subgroups of symmetric groups are called **Transformation groups** or **Permutation groups**. A symmetric group on a finite set with n elements is called **symmetric group of degree n** and is denoted by $\boldsymbol{S_n}$. Since the number of bijections from S onto itself is $n!$, hence S_n is a group of order $n!$.

The symmetric groups S_1 and S_2 are abelian groups, since the groups of order 1 and 2 are always abelian and here we have $o(S_1) = 1$ and $o(S_2) = 2$. However for $n > 2$, the commutative law is not satisfied in general, hence $S_n (n > 2)$ is non-abelian.

Corollary For a finite group G, we have $a^{o(G)} = e$. Hence for the symmetric group S_n of degree n, we have

$$f^{o(S_n)} = f^{n!} = I$$

Note: There is no loss of generality if we take the set S as $\{1,2, \dots, n\}$ in place of $\{a_1, a_2, \dots, a_n\}$. This can be justified as follows.

Suppose $S = \{a_1, a_2, \dots, a_n\}$ and $f \in S_n$ such that $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$.

Since b_i is one of the elements of S, there exists some integer m_i such that $b_i = a_{m_i}$ $(1 \le m_i \le n)$. Therefore

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{m_1} & a_{m_2} & \dots & a_{m_n} \end{pmatrix}$$

Corresponding to this permutation we can define a permutation on $\{1,2,\dots,n\}$ as follows-

$$\begin{pmatrix} 1 & 2 & \dots & n \\ m_1 & m_2 & \dots & m_n \end{pmatrix}$$

This is a permutation of $\{1,2,\dots,n\}$ is determined by f.

Also if we are given a permutation of $\{1,2,\dots,n\}$, then we can define corresponding permutation on $S = \{a_1, a_2, \dots, a_n\}$. So for the sake of convenience we can take permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ m_1 & m_2 & \dots & m_n \end{pmatrix}$ in place of $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{m_1} & a_{m_2} & \dots & a_{m_n} \end{pmatrix}$.

From now on, we shall take $S = \{1,2,\dots,n\}$ in place of $S = \{a_1, a_2, \dots, a_n\}$.

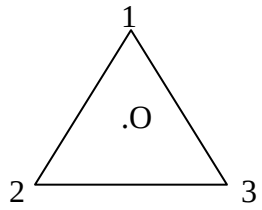
The following example will give you an idea how concrete situations could be represented using permutations.

Example (Symmetry group of an equilateral triangle)

In unit-1 we have discussed the symmetric group S_3 on three symbols. Let us see how this symmetric group is related to the symmetries of an equilateral triangle. Let us discuss the group D_3 of symmetries of an equilateral triangle, i.e. the third dihedral group. Consider an equilateral triangle with vertices labeled as 1, 2 and 3 counterclockwise around the triangle starting with 1 on the top vertex. The operations that leave a geometrical figure invariant are called the symmetry operations of the figure. The symmetry operations of an equilateral triangle are-

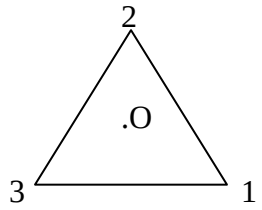
(1) The identity ρ_0 corresponding to rotation of the triangle about the axis normal to the plane of the triangle passing through its geometric centre O by an angle of 2π. In terms of permutation, it is given by the identity permutation, i.e.

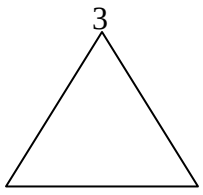
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$



(2) The operations ρ_1 and ρ_2 corresponding to rotations of the triangle about the axis normal to the plane of the triangle passing through its geometric centre O by angles of $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$ respectively. In terms of permutations, these are expressed as follows-

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





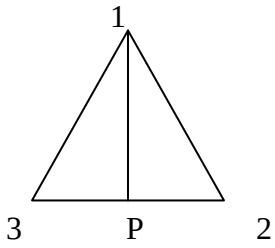
$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

.O

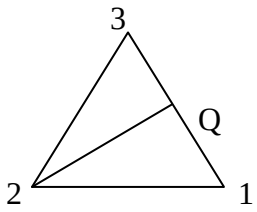
1 2

(3) The operations μ_1, μ_2 and μ_3 corresponding to reflections about the perpendicular lines 1P, 2Q and 3R respectively. These symmetry operations are described by the following permutations-

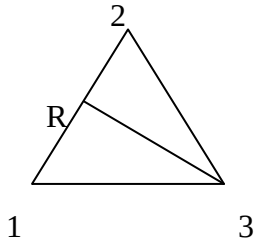
$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$



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



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



In this example, the elements of S_3 act on the set of vertices of the equilateral triangle. The concept of group action is an important one, and you will learn more about it in advanced courses. Moreover, here you see that the dihedral group D_3 is isomorphic to the symmetric group S_3.

5.4 Cycles and Transpositions

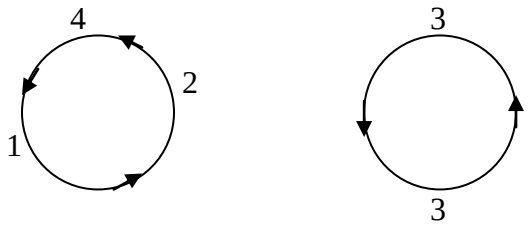
Let $S = \{1,2,3,4\}$ and $f \in S_4$ such that

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

Hence we have $f(1) = 2, f(2) = 4, f(3) = 3$ and $f(4) = 1$, i.e. f takes 1 to 2, 2 to 4 and 4 to 1. The remaining symbol 3 is taken to itself, i.e.

$$1 \longrightarrow 2 \longrightarrow 4 \longrightarrow 1 \text{ and } 3 \longrightarrow 3$$

This can be visualized as follows



Since 3 is left fixed by the permutation f, we can use the following one-row notation to represent this permutation

$$f = (1\ 2\ 4)$$

Such permutations are called cyclic permutations. Thus we have the following definition:

Definition Let $S = \{1,2,\dots,n\}$ be a finite set. A permutation f of S is said to be a **cyclic permutation** or a **cycle of length m** or **m-cycle** if there exist elements $x_1, x_2, \dots, x_m \in S$ such that $f(x_1) = x_2, f(x_2) = x_3, \dots, f(x_{m-1}) = x_m, f(x_m) = x_1$ and for any $y \in S$, $y \neq x_j$ $(1 \leq j \leq m)$, $f(y) = y$.This cyclic permutation f is represented by one-row notation as $(x_1\ x_2 \dots\ x_m)$. The number m is called the length of the cycle f.

Example: Let $S = \{1,2,3,4,5\}$. Then the permutation denoted by 4-cycle $f = (2\ 1\ 5\ 4)$ can be expressed as

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

We also note that the cycles $(1\ 5\ 4\ 2)$, $(5\ 4\ 2\ 1)$ and $(4\ 2\ 1\ 5)$ represent the same permutation. Therefore

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

By definition, cycle of length 1 is the identity permutation. In above example, we have

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

You will observe that $(1) = (2) = (3) = (4) = (5)$.

Definition A cycle of length 2 is called a **transposition.**

Example Let $S = \{1,2,3,4\}$. Then the cycle $(1\ 3)$ is a transposition of S. Similarly $(1\ 2), (1\ 4), (2\ 3)$ and $(3\ 4)$ are transpositions of S. Can you find all possible transpositions of S? How many transpositions are there in all?

We multiply cycles by multiplying the corresponding permutations. For example, suppose $S = \{1,2,3,4,5,6\}$. Let $f = (2\ 5)$ and $g = (4\ 3\ 6)$, then

$$fg = (2\ 5)(4\ 3\ 6)$$

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

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

Example Let $S = \{1,2,3,4,5\}$. The inverse of the cycle (1 2 3 4) is the cycle (4 3 2 1), since

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

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

$\Longrightarrow (1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1)$

We can generalize this result to any cycle of length n, i.e.

$$(1\ 2 \ldots \ldots\ n)^{-1} = (n\ \ n-1 \ldots . . 2\ 1)$$

Definition Two cycles $(i_1\ i_2 \ldots\ i_k)$ and $(j_1\ j_2 \ldots\ j_r)$ are said to be disjoint if

$$\{i_1\ i_2 \ldots\ i_k\} \cap \{j_1\ j_2 \ldots\ j_r\} = \emptyset$$

For example, if $S = \{1,2,3,4,5,6\}$, then the cycles (2 3 5) and (4 1) are disjoint.

Proposition Any two disjoint cycles commute.

Proof: Let $S = \{1,2, \ldots, n\}$. Let $f = (i_1\ i_2 \ldots\ i_k)$ and $g = (j_1\ j_2 \ldots\ j_r)$ be any two disjoint cycles. Let $l \in S$. If $l \in \{i_1\ i_2 \ldots\ i_k\}$, then there exists $i_p (1 \leq p \leq k)$ such that $l = i_p$. Then $f(l) = f(i_p) \in \{i_1\ i_2 \ldots\ i_k\}$. Since f and g are disjoint, hence $g(l) = g(i_p) = i_p = l$. Also $g(f(l)) = g(f(i_p)) = f(i_p) = f(l)$

Now

$$(fg)(l) = f(g(l)) = f(l)$$

and

$$(gf)(l) = g(f(l)) = f(l)$$

Therefore $(fg)(l) = (gf)(l)$.

Similarly, if $l \in \{j_1\ j_2 \ldots\ j_r\}$, then $f(l) = l$ and $f(g(l)) = g(l)$. Therefore

$$(fg)(l) = f(g(l)) = g(l)$$

and

$$(gf)(l) = g(f(l)) = g(l)$$

Thus $(fg)(l) = (gf)(l)$.

Now let $l \notin \{i_1\ i_2 \ldots\ i_k, j_1\ j_2 \ldots\ j_r\}$, then $f(l) = g(l) = l$. Hence

$$(fg)(l) = f(g(l)) = f(l) = l$$

$$(gf)(l) = g\big(f(l)\big) = g(l) = l$$

$\Longrightarrow (fg)(l) = (gf)(l)$

Thus we have shown that $(fg)(l) = (gf)(l)\ \forall l \in S$, i.e. $fg = gf$.

5.5 Orbits

Let S be a non-empty set. Let $f \in A(S)$. Define a relation $\equiv_f$ on S as follows:

For any $a, b \in S$, $a \equiv_f b$ if and only if $b = f^n(a)$ for some integer n.

Now we prove that the relation $\equiv_f$ is an equivalence relation on S.

Reflexivity: Since $f^0(a) = I(a) = a\ \forall a \in S$, hence $a \equiv_f a$ for all $a \in S$

Symmetry: $a \equiv_f b \Longrightarrow b = f^n(a)$ for some integer n

$$\Longrightarrow f^{-n}(b) = a$$

$$\Longrightarrow b \equiv_f a$$

Transitivity: $a \equiv_f b,\ b \equiv_f c \Longrightarrow b = f^n(a), c = f^m(b)$ for some integers m, n

$$\Longrightarrow c = f^m\big(f^n(a)\big) = f^{m+n}(a)$$

$$\Longrightarrow a \equiv_f c$$

Therefore the relation $\equiv_f$ is an equivalence relation on S. This relation induces a decomposition of S into equivalence classes called orbits. So we have the following definition:

Definition Let S be a non-empty set and $f \in A(S)$. Let $s \in S$. Then the orbit of s under f is defined as follows

$$O_s = \{x \in S : s \equiv_f x\} = \{x \in S : x = f^n(s) \text{ where n is some integer}\}$$

O_s is called the f-orbit of s.

We can write

$$O_s = \{f^n(s) : \text{where n is some integer}\}$$

Hence the f-orbit of s consists of all elements $f^n(s)$, $n = 0, \pm 1, \pm 2, \ldots\ldots$ This appears to be an infinite set but this is not the case as the following proposition shows.

Proposition Let S be a finite set and $f \in A(S)$. Let $s \in S$. Then there exists a positive integer k such that the f-orbit of s is given by

$$O_s = \{s, f(s), f^2(s), \ldots, f^{k-1}(s)\}$$

Proof: Since S is a finite set, the symmetric group $A(S)$ is of finite order. Therefore if $f \in A(S)$, the order of f is also finite. Let $o(f) = l$. Then

$$f^l = I \Longrightarrow f^l(x) = I(x) = x \text{ for all } x \in S$$

Obviously $f^l(s) = s$. Now l is the smallest positive integer satisfying $f^l(x) = x$ for all x But l may not be the smallest positive integer satisfying $f^l(s) = s$ (why?). Let k be the smallest positive integer such that $f^k(s) = s$.

Then $s = f^0(s), f(s), f^2(s), \ldots., f^{k-1}(s)$ are all distinct, for if $f^i(s) = f^j(s)$, $0 \leq i < j \leq k-1$, then $f^{j-i}(s) = s$ where $0 < j - i \leq k - 1$ contradicting the fact that k is the smallest such positive integer satisfying this condition.

Now suppose $t \in O_s$. Then $t = f^m(s)$ for some integer m. By division algorithm, we have

$$m = qk + r, \text{ where } 0 \leq r < k$$

So we have $t = f^m(s) = t = f^{qk+r}(s) = f^r\left(f^{kq}(s)\right) = f^r(s)$ as$f^k(s) = s \Longrightarrow f^{kq}(s) = s$, i.e. $= f^r(s)$, where $0 \leq r < k$. Thus t is one of the elements $s = f^0(s), f(s), f^2(s), \ldots., f^{k-1}(s)$. Hence $s, f(s), f^2(s), \ldots., f^{k-1}(s)$ are the only distinct elements in O_s, i.e.

$$O_s = \{s, f(s), f^2(s), \ldots., f^{k-1}(s)\}$$

Corollary: The cyclic permutation $f = (x_1\ x_2 \ldots\ x_m)$ is the cycle $\left(x_1\ f(x_1)\ f^2(x_1)\ \ldots. f^{m-1}(x_1)\right)$.

Proof: Let $S = \{1,2, \ldots, n\}$ be a finite set and $f = (x_1\ x_2 \ldots\ x_m)$ be a cyclic permutation of S. Then $f(x_1) = x_2, f(x_2) = x_3, \ldots, f(x_{m-1}) = x_m, f(x_m) = x_1$ and for any $y \in S$, $y \neq x_j$ $(1 \leq j \leq m)$, $f(y) = y$.

Obviously $x_3 = f(x_2) = f^2(x_1)$, $x_4 = f(x_3) = f^3(x_1)$, and so on. Therfore $x_m = f^{m-1}(x_1)$. Since $f(x_m) = x_1$, hence $x_1 = f^m(x_1)$. Hence we can write the cyclic permutation $(x_1\ x_2 \ldots\ x_m)$ as $\left(x_1\ f(x_1)\ f^2(x_1)\ \ldots. f^{m-1}(x_1)\right)$.

5.6 Decomposition of a permutation

Let $S = \{1,2, \ldots, n\}$ be a finite set. A cyclic permutation on S is represented by a single cycle. If a permutation f on S is not cyclic, then for any $s \in S$, there exists a positive integer m such that $\{s, f(s), f^2(s), \ldots., f^{m-1}(s)\}$ is an f-orbit of S. We can define a cycle of permutation f corresponding to this orbit. So we have the following definition-

Definition Let $S = \{1,2, \ldots, n\}$ be a finite set and $f \in S_n$. Then for any $s \in S$, there exists a positive integer m such that $\left(s\ f(s)\ f^2(s)\ \ldots. f^{m-1}(s)\right)$ is a cyclic permutation corresponding to the orbit $\{s, f(s), f^2(s), \ldots., f^{m-1}(s)\}$. This cyclic permutation is called a **cycle of the permutation** f.

Also if $\sigma(s)$ denotes the cycle $\left(s\ f(s)\ f^2(s)\ \ldots.f^{m-1}(s)\right)$ of f, then for any $t \in \{s, f(s), f^2(s), \ldots., f^{m-1}(s)\}$ we have $\sigma(t) = \sigma(s)$.

Suppose f be a permutation on $S = \{1,2,3,4,5,6\}$ such that

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

Then the orbit of 1 consists of $1, f(1) = 5, f^2(1) = f(5) = 3, f^3(1) = f(3) = 1$, i.e. 1,5,3. Hence (1 5 3) is a cycle of f.

The orbit of 2 contains only 2 as $f(2) = 2$, i.e. (2) is a cycle of f.

Since the orbit of 1 contains 3 and 5, hence the orbits of 3 and 5 are the same as that of 1.

The orbit of 4 consists of $4, f(4) = 6, f^2(4) = f(6) = 4$. Hence (4 6) is a cycle of f. Also the orbit of 6 is the same as that of 4.

Therefore the cycles of f are (2), (1 5 3) and (4 6).

Here you observe that any two cycles of f are disjoint. Hence we have the following proposition-

Proposition Any two cycles of a permutation of a finite set are disjoint.

Proof: Let $S = \{1,2, \ldots, n\}$ be a finite set and $f \in S_n$. The f-orbits of elements in S are equivalence classes. Hence any two orbits such as $\{s, f(s), f^2(s), \ldots., f^{m-1}(s)\}$ and $\{t, f(t), f^2(t), \ldots., f^{m-1}(t)\}$ are either identical or disjoint, i.e. distinct orbits are disjoint. Therefore the distinct cycles $\left(s\ f(s)\ f^2(s)\ \ldots.f^{m-1}(s)\right)$ and $\left(t\ f(t)\ f^2(t)\ \ldots.f^{m-1}(t)\right)$ are disjoint.

Now if you multiply these disjoint cycles in any order, the result is the permutation. Let us verify it for the permutation f described above.

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

Therefore

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

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

$$= f$$

Since any two disjoint cycles commute, hence

$$f = (1\ 5\ 3)(2)(4\ 6) = (2)(1\ 5\ 3)(4\ 6) = (2)(4\ 6)(1\ 5\ 3) \text{ etc.}$$

Therefore we have the following result.

Proposition Every non-identity permutation of a finite set can be written uniquely as a product of disjoint cycles, each of length> 1, upto rearrangement of cycles.

Proof: Let $S = \{1,2, \dots, n\}$ be a finite set and $f \in S_n$ be a non-identity permutation of S. Let $\sigma_1, \sigma_2, \dots . \sigma_i, \dots \sigma_k$ be all pairwise disjoint cycles of f. Let $x \in S$. Then there exists cycle σ_i such that $\sigma_i = \left(s\, f(s)\, f^2(s)\, \dots . f^{m-1}(s)\right)$ and $x = f^j(s)$ for some $0 \leq j \leq m-1$. Then $f(x) = f^{j+1}(s)$ if $j < m-1$ and $f(x) = s$ if $j = m-1$. Therefore $f(x) = \sigma_i(x)$. Since σ_i has no element common with other cycles, the elements of σ_i are left fixed by the cycles $\sigma_1, \sigma_2, \dots . \sigma_{i-1}, \sigma_{i+1} \dots \sigma_k$. Hence we have

$$\sigma_1 \sigma_2 \dots . \sigma_i \dots \sigma_k(x) = \sigma_i(x) = f(x)$$

Therefore $f = \sigma_1 \sigma_2 \dots \sigma_k$.

Since f is a non-identity permutation, hence there must exist cycles of length greater than one among $\sigma_1, \sigma_2, \dots, \sigma_k$. Now a cycle of length one represents an identity permutation, we can drop such cycles from the product $\sigma_1 \sigma_2 \dots \sigma_k$. Hence we can write f as a product of disjoint cycles of length greater than one as

$$f = \alpha_1 \alpha_2 \dots \alpha_l$$

Where $\alpha_i \in \{\sigma_1, \sigma_2, \dots, \sigma_k\}$, $1 \leq i \leq l$, are cycles of length greater than one.

To prove uniqueness, suppose if possible $f = \beta_1 \beta_2 \dots \beta_r$, where β's are some disjoint cycles of length> 1.

Let $\beta_h = \left(t\, f(t)\, f^2(t)\, \dots . f^{p-1}(t)\right)$. If t is not an element of any α_i , then t is left fixed by each α_i. Then $f(t) = \alpha_1 \alpha_2 \dots \alpha_l(t) = t$. Which is not possible as the orbit of t contains distinct elements $t, f(t), f^2(t), \dots, f^{p-1}(t)$, i.e. $t \neq f(t)$. Hence our assumption that t is not an element of any α_i, is wrong. Hence t is an element of some α_i, say α_u. Hence t is common to the orbits corresponding to the cycles α_u and β_h, therefore these orbits are identical. consequently $\beta_h = \alpha_u$. Thus each $\beta_j (1 \leq j \leq r)$ is equal to some $\alpha_i (1 \leq i \leq l)$. Since all α's are disjoint, each β_j is equal to α_i for unique i. Similarly each α_i is equal to β_j for unique j. Thus there is a one-to-one correspondence between α's and β's such that corresponding cycles are equal and $l = r$. This proves the uniqueness of the product.

Now we shall prove an interesting result.

Proposition Let $S = \{1,2, \dots, n\}$. Then

$$(1\ 2 \dots n) = (1\ n)(1\ n-1) \dots (1\ 3)(1\ 2)$$

Proof Let $\psi_i = (1\ i+1)$. Then

$$\psi_{n-1} \dots \psi_2 \psi_1 = (1\ n)(1\ n-1) \dots (1\ 3)(1\ 2)$$

Since $\psi_1(1) = 2$ and $\psi_j(2) = 2$ for all $j \neq 1$, hence

$$\psi_{n-1} \dots \psi_2 \psi_1(1) = \psi_{n-1} \dots \psi_2(2) = 2$$

Also $\psi_1(2) = 1$, $\psi_2(1) = 3$ and $\psi_j(3) = 3$ for all $j \neq 2$, hence

$$\psi_{n-1} \dots \psi_2\psi_1(2) = \psi_{n-1} \dots \psi_3\psi_2(1) = \psi_{n-1} \dots \psi_3(3) = 3$$

Now $\psi_1(3) = 3$, $\psi_2(3) = 1$, $\psi_3(1) = 4$ and $\psi_j(4) = 4$ for all $j \neq 3$, hence

$$\psi_{n-1} \dots \psi_2\psi_1(3) = 4$$

and so on, and finally

$$\psi_{n-1} \dots \psi_2\psi_1(n) = 1$$

Thus we see that the product $\psi_{n-1} \dots \psi_2\psi_1$ takes 1 to 2, 2 to 3, 3 to 4, and so on, and finally n to 1. Hence $\psi_{n-1} \dots \psi_2\psi_1 = (1\ 2 \dots n)$.

In this way, every cycle can be expressed as a product of transpositions. Since every permutation is product of disjoint cycles, we have

Corollary combining above two propositions we can say that

Every permutation of a finite set S having more than one element is a product of transpositions.

However the representation of a permutation as product of transposition is not unique. For example,

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

5.7 Even and odd permutations

We have seen that a permutation is a product of transpositions. The number of transpositions in the product may be even or odd. Suppose a permutation has a representation as a product of even number of transpositions, you may ask whether it is possible to express it as a product of odd number of transposition in some other representation. The answer is no. Let us see why this is not possible.

Consider a polynomial $p(x_1, x_2, \dots, x_n) = \prod_{i<j}(x_i - x_j)$. Let $f \in S_n$. Suppose f acts on $p(x_1, x_2, \dots, x_n)$ by the rule

$$\prod_{i<j}(x_i - x_j) \mapsto \prod_{i<j}(x_{f(i)} - x_{f(j)})$$

For instance, if $f = (3\ 4) \in S_4$ is a transposition, then f takes

$$p(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

into $(x_{f(1)} - x_{f(1)})(x_{f(1)} - x_{f(1)})(x_{f(1)} - x_{f(1)})(x_{f(1)} - x_{f(1)})$

$$\times \left(x_{f(1)} - x_{f(1)}\right)\left(x_{f(1)} - x_{4f(1)}\right)$$

i.e. $(x_1 - x_2)(x_1 - x_4)(x_1 - x_3)(x_2 - x_4)(x_2 - x_3)(x_4 - x_3) = -p(x_1, x_2, x_3, x_4)$

Hence the action of a transposition changes the sign of the polynomial. You can verify it for any transposition $(r\ s)$. Therefore if a permutation f is expressed as a product of even number of transpositions, it leaves $p(x_1, x_2, \dots, x_n)$ fixed (i.e. unchanged) and if any representation of f is a product of odd number of transpositions, it changes the sign of the polynomial $p(x_1, x_2, \dots, x_n)$. Hence if a permutation is expressed as a product of transpositions, the number of transpositions is either always even or always odd.

Now if $\sigma \in S_n$ is any permutation on n-symbols, then

$$\sigma[p(x_1, x_2, \dots, x_n)] = \pm\, p(x_1, x_2, \dots, x_n)$$

If we denote $p(x_1, x_2, \dots, x_n)$ by Δ, then

$$\sigma(\Delta) = \pm\, \Delta$$

Let us define a function $\chi: S_n \longrightarrow \{-1,1\}$ such that

$$\chi(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

Then χ is called the **alternating map** of degree n or the signature function or simply the sign function. $\chi(\sigma)$ is called the sign of σ. A simple formula for $\chi(\sigma)$ is given as

$$\chi(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Let us discuss the nature of the map $\chi: S_n \longrightarrow \{-1,1\}$.

Proposition: The alternating map $\chi: S_n \longrightarrow \{-1,1\}$ is a surjective homomorphism such that $\chi(f) = \pm 1$ for all $f \in S_n$.

Proof: Let $f, g \in S_n$. Then

$$\chi(fg) = \prod_{1 \le i < j \le n} \frac{(fg)(i) - (fg)(j)}{i - j}$$

$$= \prod_{1 \le i < j \le n} \frac{f\{g(i)\} - f\{g(j)\}}{i - j}$$

$$= \prod_{1 \le i < j \le n} \frac{f\{g(i)\} - f\{g(j)\}}{g(i) - g(j)} \cdot \prod_{1 \le i < j \le n} \frac{g(i) - g(j)}{i - j}$$

$$= \prod_{1 \le i < j \le n} \frac{f\{g(i)\} - f\{g(j)\}}{g(i) - g(j)} \cdot \chi(g)$$

Since g is a bijection on $\{1,2, \dots, n\}$ and $1 \le i < j \le n$, hence $g(i)$ and $g(j)$ take all possible pair of distinct values from $\{1,2, \dots, n\}$. Therefore

$$\prod_{1\le i<j\le n} \frac{f\{g(i)\}-f\{g(j)\}}{g(i)-g(j)} = \chi(f)$$

Hence $\chi(fg) = \chi(f)\cdot\chi(g)$, i.e. the alternating map $\chi: S_n \longrightarrow \{-1,1\}$ is a homomorphism.

Now let $t \in S_n$ be a transposition such that $t = (p\ q)$, $p < q$.

$$\chi(t) = \prod_{1\le i<j\le n} \frac{t(i)-t(j)}{i-j}$$

This product has the following types of factors-

(1) factor involving both p and q, i.e.

$$\frac{t(p)-t(q)}{p-q}$$

Since $t(p) = q$ and $t(q) = p$, we have $\frac{t(p)-t(q)}{p-q} = -1$.

(2) factor that contains neither p nor q, i.e.

$$\frac{t(i)-t(j)}{i-j};\ \text{where}\ \ i,j \neq p,q$$

Then $t(i) = i$ and $t(j) = j$. Thus $\frac{t(i)-t(j)}{i-j} = 1$

(3) factors such as

$$\frac{t(i)-t(p)}{i-p}\cdot\frac{t(i)-t(q)}{i-q} = \frac{i-q}{i-p}\cdot\frac{i-p}{i-q} = 1, \text{where } i < p$$

$$\frac{t(p)-t(i)}{p-i}\cdot\frac{t(i)-t(q)}{i-q} = \frac{q-i}{p-i}\cdot\frac{i-p}{i-q} = 1, \text{where } p < i < q$$

$$\frac{t(p)-t(i)}{p-i}\cdot\frac{t(q)-t(i)}{q-i} = \frac{q-i}{p-i}\cdot\frac{p-i}{q-i} = 1, \text{where } i > q$$

Therefore we have

$$\chi(t) = \prod_{1\le i<j\le n} \frac{t(i)-t(j)}{i-j} = -1$$

Let $f \in S_n$. Since every permutation is a product of transpositions, hence there exist transpositions $t_1, t_2, \dots, t_k$ such that

$$f = t_1 t_2 \dots t_k$$

$\Longrightarrow \chi(f) = \chi(t_1 t_2 \dots t_k) = \chi(t_1)\chi(t_2) \dots \chi(t_k)$ as χ is a homomorphism

$\Longrightarrow \chi(f) = (-1)^k$

$\Longrightarrow \chi(f) = \pm 1$

Hence χ is a homomorphism of S_n onto the multiplicative group $\{-1,1\}$.

The implications of above proposition are interesting. If a permutation f is a product of even number of transpositions, i.e. $f = t_1 t_2 \dots t_k$, where k is even, then

$$\chi(f) = (-1)^k = 1$$

and if the permutation f is a product of odd number of transpositions, i.e. k is odd, then

$$\chi(f) = (-1)^k = -1$$

Corollary: Let $f \in S_n$ such that

$$f = t_1 t_2 \dots t_k = \alpha_1 \alpha_2 \dots \alpha_r$$

Where $t_1, t_2, \dots, t_k$and $\alpha_1, \alpha_2, \dots, \alpha_r$ are transpositions. Then $k \equiv r \pmod 2$.

Proof: From above proposition, we have

$$\chi(f) = \chi(t_1)\chi(t_2) \dots \chi(t_k) = \chi(\alpha_1)\chi(\alpha_2) \dots \chi(\alpha_r)$$

$\Longrightarrow (-1)^k = (-1)^r$

$\Longrightarrow k \equiv r \pmod 2$

That means k and r both are simultaneously even or simultaneously odd.

Now we are in position to define even and odd permutations.

Definition: A permutation $f \in S_n$ is said to be an **even permutation** if it can be represented as a product of an even number of transpositions, otherwise it is said to be an **odd permutation.**

In other words, f is called an even permutation if $\chi(\sigma) = 1$ and an odd permutation if $\chi(\sigma) = -1$.

For example, $f = (1\ 2\ 4\ 6\ 3) \in S_6$ is an even permutation as

$$f = (1\ 3)(1\ 6)(1\ 4)(1\ 2)$$

and we have

$$\chi(f) = \chi[(1\ 3)(1\ 6)(1\ 4)(1\ 2)]$$

$$= \chi[(1\ 3)] \cdot \chi[(1\ 6)] \cdot \chi[(1\ 4)] \cdot \chi[(1\ 2)]$$

$$= (-1) \cdot (-1) \cdot (-1) \cdot (-1)$$

$= 1$

Also $g = (1\ 3\ 6)(4\ 2) \in S_6$ is an odd permutation as

$$g = (1\ 6)(1\ 3)(4\ 2)$$

and
$$\chi(g) = \chi[(1\ 6)(1\ 3)(4\ 2)]$$
$$= \chi[(1\ 6)] \cdot \chi[(1\ 3)] \cdot \chi[(4\ 2)]$$
$$= (-1) \cdot (-1) \cdot (-1)$$
$$= -1$$

Obviously every transposition is an odd permutation and the identity permutation is an even permutation. You will also observe that the product of two even or product of two odd permutations is even and product of an even and an odd permutation is odd.

Also since $(1\ 2\ \ldots r) = (1\ r)(1\ r-1)\ \ldots (1\ 2)$, hence an r-cycle is odd if r is even and an r-cycle is even if r is odd.

5.8 Alternating group

We have seen that the alternating map $\chi: S_n \longrightarrow \{-1,1\}$ is a surjective homomorphism and $\chi(f) = 1$ if $f \in S_n$ is an even permutation. The kernel of this homomorphism is

$$\text{Ker}\chi = \{f \in S_n : \chi(f) = 1\}$$
$$= \{f \in S_n : f \text{ is an even permutation}\}$$

Since $\text{Ker}\chi$ is a normal subgroup of S_n. Hence the subset of S_n containing all even permutations is a normal subgroup of S_n. So we have the following definition-

Definition: The group of all even permutations of degree n is called the **alternating group** of degree n and is denoted by A_n.

Since $\text{Ker}\chi = A_n$, hence by fundamental theorem of homomorphism

$$S_n/A_n \cong \{-1,1\}$$
$$\Longrightarrow o(S_n/A_n) = 2$$
$$\Longrightarrow \frac{o(S_n)}{o(A_n)} = 2$$
$$\Longrightarrow o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}$$

Hence there are $n!/2$ even permutations and the rest $n!/2$ are odd.

Example Let us determine the alternating group A_3 of degree 3. We have $S_3 = \{I, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\}$. The even permutations are $I, (1\ 2\ 3)$ and $(1\ 3\ 2)$, since the identity permutation is always even and we have $(1\ 2\ 3) = (1\ 3)(1\ 2)$ and $(1\ 3\ 2) = (1\ 2)(1\ 3)$. Hence $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

5.9 Cayley's theorem

In 1878 the English mathematician Arthur Cayley published an important result which had tremendous influence in the development of group theory. He noticed from the group table that multiplication by any group element permuted the group elements and therefore any group can be considered as an abstractly similar copy of some permutation group. In other words, every group is isomorphic to some group of permutations. We now proceed to prove the Cayley's theorem.

Theorem Every group is isomorphic to a permutation group.

Proof: Let G be a group and let $A(G)$ be the group of all permutations of G. Let $a \in G$. Define a map $f_a: G \longrightarrow G$ by $f_a(x) = ax\ \forall x \in G$. The map f_a is called the left multiplication by a.

f_a is one-one: Let $x, y \in G$. Then $f_a(x) = f_a(y) \Longrightarrow ax = ay \Longrightarrow x = y$

f_a is onto: Suppose $y \in G$, then $a^{-1}y \in G$ such that

$$f_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = ey = y$$

Hence f_a is a permutation of G, i.e. $f_a \in A(G)$.

Now for any $a, b, x \in G$, we have

$$(f_a o f_b)(x) = f_a[f_b(x)] = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$$

This shows that $f_a o f_b = f_{ab}$. Define $\psi: G \longrightarrow A(G)$ by $\psi(a) = f_a\ \forall a \in G$. Then for $a, b \in G$, we have

$$\psi(a) = \psi(b) \Longrightarrow f_a = f_b$$

$$\Longrightarrow f_a(e) = f_b(e)$$

$$\Longrightarrow ae = be$$

$$\Longrightarrow a = b$$

i.e. ψ is injective. Also $\psi(ab) = f_{ab} = f_a o f_b = \psi(a) o \psi(b)\ \ \forall a, b \in G$. Thus ψ is a one-one homomorphism of G into $A(G)$, i.e. G is isomorphic to the subgroup $\psi(G)$ of $A(G)$. This proves the theorem.

Note: If the group G is finite containing n elements, then $A(G)$ is isomorphic to S_n and therefore G is isomorphic to a subgroup of S_n.

Example Let $G = \{1, \omega, \omega^2\}$ be the multiplicative group of cube roots of unity. Then $f_1(x) = 1 \cdot x = x \ \forall x \in G$, hence $f_1 = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix} = I$,

$f_\omega(x) = \omega \cdot x \ \forall x \in G$, hence $f_\omega = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix} = (1\ \omega\ \omega^2)$

$f_{\omega^2}(x) = \omega^2 \cdot x \ \forall x \in G$, hence $f_{\omega^2} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix} = (1\ \ \omega^2\ \omega)$

By Cayley's theorem G is isomorphic to the permutation group $\{I, (1\ \omega\ \omega^2), (1\ \ \omega^2\ \omega)\}$. Since $\{I, (1\ \omega\ \omega^2), (1\ \ \omega^2\ \omega)\} \cong A_3$, therefore $G \cong A_3$.

5.10 Automorphisms and Inner automorphisms of groups

In unit-2, we introduced the concept of an isomorphism. Recall that An isomorphism of a group G onto itself is called an **automorphism** of G.

Example The mapping $f: (\mathbb{R}_{\neq 0}, \cdot) \longrightarrow (\mathbb{R}_{\neq 0}, \cdot)$ such that $f(x) = \frac{1}{x}$ for all $x \in \mathbb{R}_{\neq 0}$ is an automorphism of $\mathbb{R}_{\neq 0}$.

Obviously, f is one-one and onto. Let $x, y \in \mathbb{R}_{\neq 0}$. Then

$$f(x \cdot y) = \frac{1}{xy} = \frac{1}{x} \cdot \frac{1}{y} = f(x) \cdot f(y)$$

Let $Aut(G)$ be the set of all automorphisms of a group G. Let $f \in Aut(G)$. Since every automorphism is a one-one mapping of Gonto itself, hence $f \in A(G)$. Therefore $Aut(G) \subseteq A(G)$. We shall show that $Aut(G)$ is a group with respect to composition of functions. Since the identity map $I \in Aut(G)$, hence $Aut(G)$ is non-empty.

(1) *Closure Property*: Let $f, g \in Aut(G)$. Then f and g are both one-one mappings of G onto itself. Therefore the composition fog is also a one-one mapping of G onto itself. Also we have

$(fog)(xy) = f[g(xy)] = f[g(x)g(y)]$, as g is an automorphism

$= f[g(x)]f[g(y)]$, as f is an automorphism

$= (fog)(x)(fog)(y)$

$\Longrightarrow fog \in Aut(G)$

(2) *Associativity*: Since $Aut(G) \subseteq A(G)$ and the composition of mappings is associative in $A(G)$, the composition is also associative in $Aut(G)$.

(3) *Existence of identity*: If $I: G \longrightarrow G$ is the identity map, i.e. $I(x) = x \ \forall x \in G$, then I is an automorphism of G and $foI = f = Iof \ \ \forall f \in Aut(G)$. Thus I is the identity of $Aut(G)$.

(4) *Existence of Inverse*: Let $f \in Aut(G)$. Since f is one-one and onto, we can define $f^{-1}: G \longrightarrow G$ such that $f^{-1}(y) = x$ whenever $y = f(x)$. Obviously f^{-1} is also one-one mapping of G onto itself. Let $x_1, x_2 \in G$ such that $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Then $f^{-1}(y_1) = x_1$ and $f^{-1}(y_2) = x_2$. Now

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) = f[f^{-1}(y_1)f^{-1}(y_2)]$$

$$\Longrightarrow f^{-1}(y_1 y_2) = f^{-1}(y_1)f^{-1}(y_2)$$

Hence f^{-1} is an isomorphism of G onto itself, i.e. f^{-1} is an automorphism of G.

Therefore $f^{-1} \in Aut(G)$. Also we have $fof^{-1} = I = f^{-1}of$, i.e. f^{-1} is the inverse of f in $Aut(G)$.

Thus $Aut(G)$ is a group.

For an abelian group G, you will observe that the map $x \mapsto x^{-1}$ is an automorphism of a group G and this map is different from the identity map. For a non-abelian group G, an automorphism of G can be obtained by congjugation by a fixed element in G.

Let $a \in G$ be fixed element. Let us define a function $f_a: G \longrightarrow G$ given by $f_a(x) = axa^{-1} \ \ \forall x \in G$. We can verify that this is an automorphism of the group G.

(1) f_a *is one-one*: Let $x, y \in G$. Then

$$f_a(x) = f_a(y) \Longrightarrow axa^{-1} = aya^{-1}$$

$$\Longrightarrow x = y, \ \text{ by cancellation laws in } G$$

Hence f_a is one-one.

(2) f_a *is onto*: Let $y \in G$. Then $a^{-1}ya \in G$ such that

$$f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$$

$\therefore \ f_a$ is onto G.

(3) Let $x, y \in G$. Then $f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y)$

This proves that f_a is an automorphism of G. This automorphism is called an inner automorphism corresponding to a.

Definition: Let a be an element of a group G. The automorphism $f_a: G \longrightarrow G$ given by $f_a(x) = axa^{-1} \ \ \forall x \in G$ is called an **inner automorphism** corresponding to a. The set of all inner automorphisms of a group G is denoted by $Inn(G)$.

Obviously for an abelian group, every inner automorphism turns out to be the identity map. However a non-abelian group G has non-trivial automorphisms. The following result shows that for a non-abelian group G, $Inn(G)$ is a not a trivial group.

Proposition Let G be a group. Then $Inn(G)$ is a normal subgroup of $Aut(G)$ and $Inn(G) \cong G/Z(G)$, where $Z(G)$ denotes the center of G.

Proof: We have $e \in G$, hence $f_e(x) = exe^{-1} = x \ \forall x \in G$. Thus $f_e = I \in Inn(G)$, i.e. $Inn(G) \neq \emptyset$.

First we shall show that every element $f_a \in Inn(G)$ has its inverse in $Inn(G)$.

Since $a \in G \Longrightarrow a^{-1} \in G$, hence for any $x \in G$, we have $(f_a o f_{a^{-1}})(x) = f_a[f_{a^{-1}}(x)] = f_a[a^{-1}x(a^{-1})^{-1}] = f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x = I(x)$.

i.e. $(f_a o f_{a^{-1}})(x) = I(x) \ \ \forall x \in G \Longrightarrow f_a o f_{a^{-1}} = I$

Similarly $f_{a^{-1}} o f_a = I$. Therefore $f_a o f_{a^{-1}} = I = f_{a^{-1}} o f_a$

$$\Longrightarrow (f_a)^{-1} = f_{a^{-1}} \in Inn(G)$$

Now for $a, b \in G$, we have

$$(f_a o f_b)(x) = f_a[f_b(x)] = f_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(b^{-1}a^{-1})$$

$$= (ab)x(ab)^{-1} = f_{ab}(x) \ \ \forall x \in G$$

i.e. $(f_a o f_b)(x) = f_{ab}(x) \quad \forall x \in G$

$$\Longrightarrow f_a o f_b = f_{ab} \in Inn(G)$$

Therefore $f_a o (f_b)^{-1} = f_a o f_{b^{-1}} = f_{ab^{-1}} \in Inn(G)$, i.e. $Inn(G)$ is a subgroup of $Aut(G)$.

To show that $Inn(G)$ is a normal subgroup of $Aut(G)$, we prove that

$$f_a \in Inn(G), \rho \in Aut(G) \Longrightarrow \rho o f_a o \rho^{-1} \in Inn(G)$$

For $x \in G$, we have

$$(\rho o f_a o \rho^{-1})(x) = (\rho o f_a)[\rho^{-1}(x)] = \rho[a\rho^{-1}(x)a^{-1}] = \rho(a)\rho[\rho^{-1}(x)]\rho(a^{-1}) = \rho(a)x[\rho(a)]^{-1}$$
$$= f_{\rho(a)}(x)$$

$$\Longrightarrow \rho o f_a o \rho^{-1} = f_{\rho(a)} \in Inn(G)$$

Hence $Inn(G)$ is a normal subgroup of $Aut(G)$.

Now to prove the remaining part of the proposition, consider the mapping

$\psi: G \longrightarrow Inn(G)$ defined by $\psi(a) = f_a$ for all $a \in G$.

Let $a, b \in G$. Then $\psi(ab) = f_{ab} = f_a o f_b = \psi(a) o \psi(b)$. Thus ψ is a homomorphism. Now $f_a \in Inn(G) \Longrightarrow \exists a \in G$ such that $\psi(a) = f_a$. Hence ψ is onto $Inn(G)$. Therefore $Inn(G)$ is a homomorphic image of G. By the fundamental theorem of homomorphism, $G/\text{Ker}\psi \cong Inn(G)$.

Now $\text{Ker}\psi = \{x \in G : \psi(x) = I\}$. Hence

$$a \in \text{Ker}\psi \Leftrightarrow \psi(a) = I$$

$$\Leftrightarrow f_a = I$$

$$\Leftrightarrow f_a(x) = I(x) \text{ for all } x \in G$$

$$\Leftrightarrow axa^{-1} = x \text{ for all } x \in G$$

$$\Leftrightarrow ax = xa \text{ for all } x \in G$$

$$\Leftrightarrow a \in Z(G)$$

Thus $\text{Ker}\psi = Z(G)$. This proves the proposition.

5.11 Summary

In this unit, we have

(1) Proved that the set of all permutations on a finite set S forms a group with respect to composition of mappings and defined the symmetric group S_n.

(2) Defined cycles, transpositions and orbits and proved that a permutation can be represented as a product of transpositions.

(3) Defined alternating map $\chi : S_n \longrightarrow \{-1, 1\}$ and proved that it is a surjective homomorphism such that $\chi(f) = \pm 1$ for all $f \in S_n$.

(4) Defined even and odd permutations and proved that the subset of S_n containing all even permutations is a normal subgroup of S_n. This group of all even permutations is called the alternating group A_n.

(5) Discussed and proved the Cayley's theorem, i.e. every group is isomorphic to a permutation group.

(6) Defined automorphism of a group G as an isomorphism of G onto itself and proved that the set $Aut(G)$ of all automorphisms of a group G is a group with respect to composition of functions.

(7) Defined inner automorphism corresponding to $a \in G$ as the automorphism $f_a : G \longrightarrow G$ given by $f_a(x) = axa^{-1} \quad \forall x \in G$ and proved that the set $Inn(G)$ of all inner automorphisms of a group G is a normal subgroup of $Aut(G)$ and $Inn(G) \cong G/Z(G)$, where $Z(G)$ denotes the center of G.

5.12 Self assessment questions

(1) Let $S = \{1,2,3,4,5,6,7\}$. Express the following permutations of S as products of disjoint cycles (i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 2 & 3 & 6 & 7 \end{pmatrix}$ (ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 4 & 2 & 1 & 7 & 3 \end{pmatrix}$

[Ans: (i)$f = (1\ 4\ 2)(3\ 5)$ (ii) $= (1\ 5)(2\ 6\ 7\ 3\ 4)$]

(2) If $f = (1\ 3)(\ 4\ 5\ 6)$ and $g = (1\ 3\ 4)$, determine $fg^{-1}f^{-1}$.

[Ans: $g^{-1}f^{-1} = (1\ 3\ 5)$]

(3) Decompose the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 2 & 3 & 7 & 6 \end{pmatrix}$ into transpositions.

[Ans: $= (1\ 3)(1\ 5)(2\ 4)(6\ 7)$]

(4) Let $f \in S_n$ be a cycle of length r. Prove that $o(f) = r$.

(5) Let $f = \alpha_1\alpha_2 \dots \alpha_k$ be a permutation on $S = \{1,2, \dots, n\}$.Where $\alpha_1, \alpha_2, \dots, \alpha_k$ are pairwise disjoint cycles of lengths $m_1, m_2, \dots, m_k$ respectively. Prove that $o(f) = [m_1, m_2, \dots, m_k]$ the least common multiple of $m_1, m_2, \dots, m_k$.

(6) Prove that S_7 contains no elements of order 8.

(7) Show that $K = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a normal subgroup of S_4. Also show that K is isomorphic to the Klein's four group V_4.

(8) Show that $S_4/V_4 \cong S_3$

(9) Prove that there are only two groups of order six, one is cyclic and other is isomorphic to S_3.

(10) Prove that A_n is simple for $n \geq 5$.

(11) Show that (i) $Aut(S_3) \cong S_3$ (ii) $Aut(V_4) \cong S_3$ (iii) $Inn(Q_8) \cong V_4$

5.13 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Lang, S. (1965): Algebra, Reading, Massachusetts, Addison-Wesley.

ABSTRACT ALGEBRA

Block-III

Rings and Fields

ALLAHABAD

Block-III
Rings and Fields

Unit-6

Rings and Fields

Unit-7

Homomorphisms and Embedding of rings

Unit-8

Ideals

Block-III **UGMM-109**

Introduction

Unit-6 In this unit, we introduce an algebraic structure with two binary operations called ring. We define ring with examples and discuss various properties of rings. We define zero divisors and then introduce rings without zero divisors. Some special rings such as integral domain, division ring and field are studied. We introduce subring and subfield with examples.

Unit-7 In this unit, we define characteristic of an integral domain. We study homomorphism and isomorphism of rings, Kernel of a homomorphism, direct and inverse images of subring and subfield under homomorphism. We discuss the embedding of a ring into another ring and the field of fractions of an integral domain.

Unit-8 In this unit, we deal with the left ideal, right ideal, principal ideal, prime ideal and maximal ideal with examples. We define quotient ring and prove the fundamental theorem of homomorphism for rings and fields.

Unit-6: Rings and Fields

Structure

6.1 Introduction

Recall that a set with one or more operations (unary, binary or other) obeying a particular collection of axioms is termed as 'algebraic structure'. In previous blocks, you have studied an algebraic structure called 'group'. A group is a non-empty set equipped with a binary operation satisfying axioms: closure property, associativity, existence of identity and existence of inverse. Let us take an example to show how we can equip a non-empty set with two binary operations.

Consider the set $\mathbb{Z}$ of integers with two binary operations, namely the addition and multiplication. We know that $(\mathbb{Z}, +)$ is an abelian group, i.e.

(1) $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$

(2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$.

(3) There exists $0 \in \mathbb{Z}$ such that $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$.

(4) To each $a \in \mathbb{Z}$, there is an element $-a \in \mathbb{Z}$ such that

$$a + (-a) = 0 = (-a) + a$$

(5) $a + b = b + a$ for all $a, b \in \mathbb{Z}$

The set $\mathbb{Z}$ fails to form a group under multiplication, however it is closed under multiplication and the associative law holds in it, i.e.

(6) $a \cdot b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$

(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{Z}$

Moreover you will see that these two operations are interrelated by distributive law-

(8) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{Z}$

and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathbb{Z}$

This algebraic framework forms a model for abstract definition of an algebraic structure called **ring**. In this unit, you will study different types of rings in details.

Not all rings follow commutativity of multiplication. We shall introduce some special rings in which commutative law of multiplication holds and which contains multiplicative identity, i.e. unity. In a ring, sometimes it happens that $a \neq 0, b \neq 0$ but $ab = 0$. Such elements are called divisors of zero. Commutative rings with unity and without zero divisors are called **integral domains**. As the name suggests, these rings share many properties with the integers.

Some rings have unity and in some rings every nonzero element has multiplicative inverse. A ring with unity is called a **division ring** if its nonzero elements form a group under multiplication. A Commutative division ring is called a **field.** We shall study these structures with examples and prove some interesting results.

You will see how the study of groups provides parallels to study rings. The notions of **subring** and **subfield** are quite similar to that of a subgroup you studied in unit-2. We shall discuss these concepts and establish some results.

Let us first discuss the objectives of this unit.

6.2 Objectives

After reading this unit, you should be able to

- Understand the definition of ring and observe how different sets equipped with two binary operations form rings.
- Discuss the elementary properties of rings
- Describe rings with or without zero divisors with examples
- Define different types of rings such as integral domains, division rings and fields
- Describe subrings and subfields with examples

6.3 Rings

The German mathematician David Hilbert introduced the term *Zahlring* (number ring) in his 1897 paper "The theory of algebraic number fields". Actually the abstract definition of ring stemmed from two independently developed theories: commutative ring theory and noncommutative ring theory. Let us first discuss the abstract definition of a ring.

Definition A ring $(R, +, \cdot)$ is an algebraic structure consisting of a non-empty set R equipped with two binary operations '$+$' and '$\cdot$', called addition and multiplication respectively, such that the following axioms are satisfied:

(1) $a + b \in R$ for all $a, b \in R$
(2) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$
(3) $a + b = b + a$ for all $a, b \in R$
(4) There is an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$
(5) For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$
(6) $a \cdot b \in R$ for all $a, b \in R$
(7) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$

(8) For all $a, b, c \in R$, $a.(b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$
The additive identity 0 of R is called the *zero* of the ring R.
We can say that the triple $(R, +, \cdot)$ is a ring if
(1) $(R, +)$ is an abelian group.
(2) $(R, \cdot)$ is a semigroup.
(3) The left distributive law and the right distributive law hold.
Remarks 1. we shall denote $a + (-b)$ by $a - b$.
2. For the sake of convenience, sometimes we denote $a \cdot b$ by ab.
3. Instead of saying that $(R, +, \cdot)$ is a ring, we simply say that R is a ring with the understanding that there is no confusion regarding the binary compositions '$+$' and '$\cdot$'.

The multiplication operation in a ring needs not to be commutative as we shall see in example 6.3.2 and example 6.3.8. Also the multiplicative identity may or may not exist. So we have the following definitions:

Definition A ring $(R, +, \cdot)$ is called **commutative** if
$a \cdot b = b \cdot a$ for all $a, b \in R$
Definition A ring $(R, +, \cdot)$ is said to be a **ring with identity (or unity)** if there exists $1 \in R$ such that
$a \cdot 1 = a = 1 \cdot a$ for all $a \in R$
This element 1 is called the unity or identity of the ring R.

Let us illustrate these concepts with some examples.
The simplest ring is the zero ring, where $R = \{0\}$ is the trivial group and multiplication is defined by $ab = 0$ for all $a, b \in R$. This is the only ring where $1 = 0$.
Example 6.3.1 We have already seen that the set $\mathbb{Z}$ of integers is a ring under usual addition and multiplication. Also we have
$ab = ba$ for all $a, b \in \mathbb{Z}$
and $1 \in \mathbb{Z}$ such that $a1 = a = 1a$ for all $a \in \mathbb{Z}$.
i.e. $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unity. You can check for yourself that $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are also commutative rings with unity.

Now we give an example of a non-commutative ring with unity involving matrices.
Example 6.3.2 The set $M_n(\mathbb{Z})$, $n \geq 2$, of all square matrices of order $n \times n$ with entries in $\mathbb{Z}$ is a noncommutative ring with unity under the addition '$+$' and multiplication '$\cdot$' defined as follows-
Let $A, B \in M_n(\mathbb{Z})$ such that $A = [a_{ij}]$ and $B = [b_{ij}]$, where $a_{ij}, b_{ij} \in \mathbb{Z}$. Then
$$A + B = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$
and $$AB = [c_{ij}] \text{ where } c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$
Since $a_{ij} + b_{ij} \in \mathbb{Z}$ and $\sum_{j=1}^{n} a_{ij} b_{jk} \in \mathbb{Z}$ for all $1 \leq i \leq n$ and $1 \leq j \leq n$, hence
$A + B \in M_n(\mathbb{Z})$ and $AB \in M_n(\mathbb{Z})$ for all $A, B \in M_n(\mathbb{Z})$. Also we observe that
(1) $A + (B + C) = (A + B) + C$ for all $A, B, C \in M_n(\mathbb{Z})$
(2) $A + B = B + A$ for all $A, B \in M_n(\mathbb{Z})$
(3) If O is the null matrix of order $n \times n$, then
$A + O = A$ for all $A \in M_n(\mathbb{Z})$
(4) To each $A = [a_{ij}] \in M_n(\mathbb{Z})$ there exists $-A = [-a_{ij}] \in M_n(\mathbb{Z})$ such that

$$A + (-A) = [a_{ij} + (-a_{ij})] = O$$

(5) Since the multiplication of matrices is associative, hence

$$A(BC) = (AB)C \text{ for all } A, B, C \in M_n(\mathbb{Z})$$

(6) Also the multiplication of matrices is distributive with respect to matrix addition. Hence

$A(B + C) = AB + AC$ and $(A + B)C = AC + BC$ for all $A, B, C \in M_n(\mathbb{Z})$

(7) Let $I = [a_{ij}]$ such that $a_{ij} = 1$ for $i = j$ and $a_{ij} = 0$ for $i \neq j$, i.e. I is the $n \times n$ identity matrix. Then

$$AI = A = IA \text{ for all } A \in M_n(\mathbb{Z})$$

i.e. the identity matrix is the unity.

We know that the matrix multiplication is not commutative in general. Hence $M_n(\mathbb{Z})$ is a noncommutative ring with unity for $n \geq 2$.

Similarly, you can check that $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are also noncommutative rings with unity. In fact, if R is any ring, then $M_n(R)$, $n \geq 2$, is a noncommutative ring with unity.

Example 6.3.3 Let $(R, +, \cdot)$ be any ring. Let X be any non-empty set. The collection, R^X, of all functions $f: X \longrightarrow R$ is a ring with respect to pointwise addition and multiplication defined as follows:

$$(f \oplus g)(x) = f(x) + g(x) \text{ for all } x \in X$$

and $$(f \odot g)(x) = f(x) \cdot g(x) \text{ for all } x \in X$$

Since R is a ring and $f(x), g(x) \in R$ for all $x \in X$, hence $f(x) + g(x) \in R$ and $f(x) \cdot g(x) \in R$ for all $x \in X$. Therefore $f \oplus g \in R^X$ and $f \odot g \in R^X$. Also for all $x \in X$, we have

(1) $$\begin{aligned}[(f \oplus g) \oplus h](x) &= (f \oplus g)(x) + h(x) \\ &= [f(x) + g(x)] + h(x) \\ &= f(x) + [g(x) + h(x)], \text{ since } f(x), g(x), h(x) \in R \\ &= f(x) + (g \oplus h)(x) \\ &= f(x) + (g \oplus h)(x) \\ &= [f \oplus (g \oplus h)](x)\end{aligned}$$

i.e. $(f \oplus g) \oplus h = f \oplus (g \oplus h)$

(2) $$\begin{aligned}(f \oplus g)(x) &= f(x) + g(x) \\ &= g(x) + f(x), \text{ since } f(x), g(x) \in R \text{ and } R \text{ is a ring} \\ &= (g \oplus f)(x)\end{aligned}$$

i.e. $f \oplus g = g \oplus f$

Similarly, you can see that other axioms of a ring hold in R^X. The zero of R^X is the mapping $\bar{0}: X \longrightarrow R$ given by $\bar{0}(x) = 0 \ \forall x \in X$.

You will also note that R^X is commutative if and only if R is commutative. Also R^X has unity if and only if R has unity. If 1 is unity of R, then the unity of R^X is the mapping $i: X \longrightarrow R$ given by $i(x) = 1 \ \forall x \in X$.

Let us have another interesting example involving mappings.

Example 6.3.4 Let $End(G)$ denote the set of all endomorphisms of an abelian group $(G, +)$. Then $End(G)$ is a ring under the addition and multiplication defined by

$$(f \oplus g)(x) = f(x) + g(x) \text{ for all } x \in G$$

and $$(f \odot g)(x) = f\{g(x)\} \text{ for all } x \in G$$

An endomorphism of a group G is a homomorphism of G into itself. Let $f, g \in End(G)$. Then for all $x, y \in G$, we have

$$(f \oplus g)(x+y) = f(x+y) + g(x+y)$$
$$= [f(x) + f(y)] + [g(x) + g(y)]$$

Since G is abelian, hence

$$(f \oplus g)(x+y) = [f(x) + g(x)] + [f(y) + g(y)]$$
$$= (f \oplus g)(x) + (f \oplus g)(y)$$

i.e. $f \oplus g$ is an endomorphism of G. Hence $f \oplus g \in End(G)$.

Also $(f \odot g)(x+y) = f\{g(x+y)\}$
$= f\{g(x) + g(y)\}$
$= f\{g(x)\} + f\{g(y)\}$
$= (f \odot g)(x) + (f \odot g)(y)$

Hence $f \odot g \in End(G)$.

It can be readily checked that $End(G)$ is a ring.

Now we give an example of a commutative ring which does not have an identity.

Example 6.3.5 The set $2\mathbb{Z}$ of all even integers is a commutative ring without unity under usual addition and multiplication.

Example 6.3.6 The set $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ forms a commutative ring with unity under addition modulo 6 and multiplication modulo 6.

Let us have a look at the composition tables for $+_6$ and $\times_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We know that $(\mathbb{Z}_6, +_6)$ is an abelian group.

From the composition table for $\times_6$, we see that $\mathbb{Z}_6$ is closed under $\times_6$, i.e.

$a \times_6 b \in \mathbb{Z}_6$ for all $a, b \in \mathbb{Z}_6$.

Also we have

$$a \times_6 (b \times_6 c) = (a \times_6 b) \times_6 c \quad \text{for all } a, b, c \in \mathbb{Z}_6$$

Further $a \times_6 (b +_6 c) = a \times_6 (b + c)$ as $b +_6 c \equiv b + c \pmod 6$
$= a(b + c) \pmod 6$
$= ab + ac \pmod 6$
$= ab +_6 ac$
$= a \times_6 b +_6 a \times_6 c$

Similarly, you can show that $(a +_6 b) \times_6 c = a \times_6 c +_6 b \times_6 c$

Also $1 \in \mathbb{Z}_6$ is the unity as $a \times_6 1 = a = 1 \times_6 a$ for all $a \in \mathbb{Z}_6$ and

$a \times_6 b = b \times_6 a$ for all $a, b \in \mathbb{Z}_6$

Therefore $(\mathbb{Z}_6, +_6, \times_6)$ is a commutative ring with unity. In general, $(\mathbb{Z}_n, +_n, \times_n)$ is a commutative ring with unity.

Example 6.3.7 The set $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\}$ of residue classes modulo n is a commutative ring with unity $[1]$ under the addition and multiplication of residue classes given by

$$[a] + [b] = [a + b], \quad \text{where } a + b \equiv a + b \pmod{n}$$
$$[a][b] = [ab], \quad \text{where } ab \equiv ab \pmod{n}$$

Now we shall give an example created by Irish mathematician William Rowan Hamilton which is historically important in noncommutative ring theory and has many applications in algebra, number theory, geometry and mechanics.

Example 6.3.8 (Ring of real Hamilton Quaternions) Let

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Where $a_1 + b_1 i + c_1 j + d_1 k = a_2 + b_2 i + c_2 j + d_2 k$ if and only if $a_1 = a_2, b_1 = b_2, c_1 = c_2, d_1 = d_2$.

Define addition and multiplication on $\mathbb{H}$ as follows

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k)$$
$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i$$
$$+ (a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2)j + (a_1 d_2 + b_1 c_2 + d_1 a_2 - c_1 b_2)k$$

This multiplication follows from the distributive law and the relations

$$i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1, \; i \cdot j = -j \cdot i = k,$$
$$j \cdot k = -k \cdot j = i, \; k \cdot i = -i \cdot k = j$$

You can verify that $\mathbb{H}$ is a noncommutative ring with zero, $0 = 0 + 0i + 0j + 0k$ and unity, $1 = 1 + 0i + 0j + 0k$.

Similarly, you can define ring of rational Hamilton Quaternions by taking $a, b, c, d \in \mathbb{Q}$.

Example 6.3.9 (Ring of Gaussian integers) Gaussian integers are complex numbers $a + ib$ such that $a, b \in \mathbb{Z}$. Let

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$$

Consider addition and multiplication of Gaussian integers $a_1 + ib_1$ and $a_2 + ib_2$ induced by those in the set $\mathbb{C}$ of complex numbers, i.e.

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$$
$$(a_1 + ib_1)(a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(b_1 a_2 + a_1 b_2)$$

You can verify for yourself that $\mathbb{Z}[i]$ is indeed a commutative ring with unity.

Example 6.3.10 The set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a commutative ring with unity under addition and multiplication induced by those in $\mathbb{R}$.

Solution Let $a_1 + b_1\sqrt{2}, \; a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Define addition and multiplication operations in $\mathbb{Q}[\sqrt{2}]$ as induced by those in $\mathbb{R}$, i.e.

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$
$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2}$$

Since $a_1 + a_2,\ b_1 + b_2,\ a_1a_2 + 2b_1b_2,\ a_1b_2 + b_1a_2 \in \mathbb{Q}$, hence $\mathbb{Q}[\sqrt{2}]$ is closed under these operations.

Now the elements of $\mathbb{Q}[\sqrt{2}]$ are real numbers. Therefore the associative law and commutative law of addition and multiplication must hold in $\mathbb{Q}[\sqrt{2}]$, i.e. for all $x, y, z \in \mathbb{Q}[\sqrt{2}]$, we have

(1) $x + (y + z) = (x + y) + z$

(2) $x + y = y + x$

(3) $x(yz) = (xy)z$

(4)$xy = yx$

Also the multiplication is distributive over addition. Hence for all $x, y, z \in \mathbb{Q}[\sqrt{2}]$, we have $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

The element $0 + 0\sqrt{2}$ is the zero element of $\mathbb{Q}[\sqrt{2}]$ and $1 + 0\sqrt{2}$ is the identity (unity). Thus $\mathbb{Q}[\sqrt{2}]$ is a commutative ring with unity under addition and multiplication induced by those in $\mathbb{R}$.

Example 6.3.11 Let $(R_i, \oplus_i, \odot_i), i = 1,2, \dots, n$ be rings. Let

$$R_1 \times R_2 \times \dots \times R_n = \{(a_1, a_2, \dots, a_n) : a_1 \in R_1, a_2 \in R_2 \ \dots, a_n \in R_n\}$$

Then $R_1 \times R_2 \times \dots \times R_n$ is a ring with respect to the following operations (verify):

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 \oplus_1 b_1, a_2 \oplus_2 b_1, \dots, a_n \oplus_n b_1)$$

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1 \odot_1 b_1, a_2 \odot_2 b_1, \dots, a_n \odot_n b_1)$$

This ring is called the *direct product* of $R_1, R_2, \dots, R_n$.

Now we give an important example of ring of polynomials.

Example 6.3.12 Let R be a ring and x be an indeterminate. A polynomial $f(x)$ with coefficients in R is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ \dots + a_{n-1}x^{n-1} + a_n x^n + \ \dots$$

Where $a_i \in R$ and all except finite number of a_i's are equal to zero. If $a_n \neq 0$ and $a_i = 0$, for all $i > n$, then the polynomial is said to be of degree n.

Let $R[x]$ be the set of all such polynomials. Let $f(x), g(x) \in R[x]$ such that $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$. We define polynomial addition and multiplication as follows:

$$f(x) + g(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$f(x)g(x) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} c_i x^i$$

Where $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

You can verify that $R[x]$ is a ring under polynomial addition and multiplication.

6.4 Properties of rings

If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group. Hence R enjoys all the properties of an additive abelian group. Let us see what else we have for a ring.

Proposition Let $(R, +, \cdot)$ be a ring with 0 as its zero. Then for all $a, b, c \in R$, we have
(i) $a0 = 0a = 0$ for all $a \in R$
(ii) $a(-b) = (-a)b = -(ab)$ for all $a, b \in R$
(iii)$(-a)(-b) = ab$ for all $a, b \in R$
(iv) $a(b - c) = ab - ac$ for all $a, b, c \in R$
(v) $(b - c)a = ba - ca$ for all $a, b, c \in R$
Proof (i) We have $a0 = a(0 + 0)$

$= a0 + a0$, by left distributive law

$\Rightarrow 0 + a0 = a0 + a0$, $\{\because 0 + 0a = 0a\}$

$\Rightarrow 0 = a0$, by right cancellation law for addition in the group $(R, +)$

Similarly $0a = 0$.
Hence $a0 = 0a = 0$ for all $a \in R$.
(ii) We have $a[(-b) + b] = a0$

$\Rightarrow a(-b) + ab = 0$, by left distributive law and using (i)

$\Rightarrow a(-b) = -(ab)$

Also $[(-a) + a]b = 0b$

$\Rightarrow (-a)b + ab = 0$, by right distributive law and using (i)

$\Rightarrow (-a)b = -(ab)$

Hence $a(-b) = (-a)b = -(ab)$ for all $a, b \in R$
(iii) We have $(-a)(-b) = -[(-a)b]$ by (ii)

$\Rightarrow = -[-(ab)]$

$\Rightarrow = ab$

(iv)We have $a(b - c) = a[b + (-c)]$

$= ab + a(-c)$

$= ab + [-(ac)]$

$= ab - ac$

Similarly we can prove (v).

Proposition If R is a ring such that $a^2 = a \ \ \forall a \in R$, then
(i) Each element of R is its own inverse, i.e. $a + a = 0 \ \ \forall a \in R$
(ii) $a + b = 0 \Rightarrow a = b$
(iii) R is a commutative ring.
Proof: (i) Since $a \in R$, hence $a + a \in R$. Therefore

$(a + a)^2 = a + a$

$\Rightarrow \ (a + a)(a + a) = a + a$

$\Rightarrow \ a(a + a) + a(a + a) = a + a$ by right distributive law

$\Rightarrow \ (a^2 + a^2) + (a^2 + a^2) = a + a$ by left distributive law

$\Rightarrow \ (a + a) + (a + a) = a + a$, since $a^2 = a$

$\Rightarrow \ (a + a) + (a + a) = (a + a) + 0$

$\Rightarrow \ a + a = 0$, by left cancellation law for addition in R

(ii) We have,

$a + b = 0 \Rightarrow a + b = a + a$ as $a + a = 0$

$\Rightarrow b = a$, by left cancellation law for addition in R

(iii) We have

$(a + b)^2 = a + b \Rightarrow (a + b)(a + b) = a + b$

$\Rightarrow a(a + b) + b(a + b) = a + b$, by right distributive law

$\Longrightarrow (a^2 + ab) + (ba + b^2) = a + b$, by left distributive law
$\Longrightarrow (a + ab) + (ba + b) = a + b$, since $a^2 = a$, $b^2 = b$
$\Longrightarrow a + (ab + ba) + b = a + b$, by associativity of addition
$\Longrightarrow (ab + ba) + a + b = a + b$, by commutativity of addition
$\Longrightarrow (ab + ba) + (a + b) = 0 + (a + b)$
$\Longrightarrow ab + ba = 0$, by right cancellation law
$\Longrightarrow ab = ba$, since $a + b = 0 \Longrightarrow a = b$

Hence R is a commutative ring.

Definition An element $a \in R$ is called an **idempotent** element if $a^2 = a$. A ring R is a **Boolean ring** if every element of R is idempotent.
In light of above proposition we can say that every Boolean ring is commutative.

Remark Let R be a ring. If n is a positive integer, we define

$$na = a + a + \ \dots\dots, n \text{ times}$$

If n is a negative integer,i.e. $n = -m$, where m is a positive integer, then we define

$$na = (-m)a = -(ma) = m(-a)$$

and hence $na = (-a) + (-a) + \ \dots\dots, m$ times
Also if m and n are integers, then

$$ma + na = (m + n)a,\ m(na) = (mn)a$$

Now we shall prove that the binomial theorem holds in commutative rings.
Proposition Let R be a commutative ring. Then for all $a, b \in R$ and given positive integer n, we have

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \ \dots\dots + b^n$$

Proof We shall prove it by mathematical induction.
For $n = 1$, the result is obviously true, i.e. $(a + b)^1 = a^1 + b^1$.
Suppose that the result is true for $n = m$.

$$(a + b)^m = \sum_{r=0}^{m} \binom{m}{r} a^{m-r}b^r$$

Now

$$(a + b)^{m+1} = (a + b)^m(a + b) = \left[\sum_{r=0}^{m} \binom{m}{r} a^{m-r}b^r\right](a + b)$$

Since R is commutative, hence

$$(a + b)^{m+1} = \sum_{r=0}^{m} \binom{m}{r} a^{m-r+1}b^r + \sum_{r=0}^{m} \binom{m}{r} a^{m-r}b^{r+1}$$

$$= a^{m+1} + \sum_{r=1}^{m}\binom{m}{r}a^{m-r+1}b^r + \sum_{r=0}^{m-1}\binom{m}{r}a^{m-r}b^{r+1} + b^{m+1}$$

$$= a^{m+1} + \sum_{r=1}^{m}\binom{m}{r}a^{m-r+1}b^r + \sum_{r=1}^{m}\binom{m}{r-1}a^{m-r+1}b^r + b^{m+1}$$
$$= a^{m+1} + \sum_{r=1}^{m}\left[\binom{m}{r} + \binom{m}{r-1}\right]a^{m-r+1}b^r + b^{m+1}$$
$$= a^{m+1} + \sum_{r=1}^{m}\binom{m+1}{r}a^{m-r+1}b^r + b^{m+1}$$
$$= \sum_{r=0}^{m+1}\binom{m+1}{r}a^{m+1-r}b^r$$

Hence the result is also true for $n = m + 1$.

6.5 Rings with or without zero divisors

Consider the example 6.3.6, $(\mathbb{Z}_6, +_6, \times_6)$ is a commutative ring with unity. Here you will observe that $2 \times_6 3 = 0$, $3 \times_6 2 = 0$, i.e. $a \neq 0, b \neq 0$ but we have $a \times_6 b = 0 = b \times_6 a$. Also in example 6.3.2, if $A, B \in M_2(\mathbb{Z})$ such that

$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, then $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$ and $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq O$.

Therefore in a ring, it may happen that $a \neq 0, b \neq 0$ but $ab = 0$ and $ba \neq 0$. So we have the following definition:

Definition Let R be a ring. An element $a \in R$ is called a **left zero divisor**, if there exists $b \in R$, $b \neq 0$ such that $ab = 0$. Also $a \in R$ is called a **right zero divisor**, if there exists $b \in R$, $b \neq 0$ such that $ba = 0$.

Obviously 0 is always a left as well as right zero divisor in any given ring. 0 is called a *trivial zero divisor*. In example 6.3.6, the element $2 \in \mathbb{Z}_6$ is a left as well as right zero divisor. In example 6.3.2, $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z})$ is a left zero divisor.

A non-zero element of a ring R which is a left (right) zero divisor is called a proper left (right) zero divisor of R. If a ring R has no proper left or right zero divisors, then it is called a **ring without zero divisors**.

For example, the ring $\mathbb{Z}$ of integers is a ring without zero divisor.

Suppose a ring R has no proper left zero divisors. Let b be a right zero divisor. Then there exists $a \neq 0$ in R such that $ab = 0$. Then we must have $b = 0$ for otherwise a will become a proper left zero divisor. Hence R has no proper right zero divisor. Therefore

R has no proper left zero divisors $\Longrightarrow$ R has no proper right zero divisors

Similarly, you can show that

R has no proper right zero divisors $\Longrightarrow$ R has no proper left zero divisors

Now suppose that R has no proper left zero divisors. If $a, b \in R$ such that $ab = 0$, then we must have either $a = 0$ or $b = 0$. Let us see how:

Suppose $ab = 0$. If $a = 0$, then there is nothing to show. If $a \neq 0$, then a cannot be a proper left zero divisor hence we must have $b = 0$.

Hence if R is without zero divisors, then

$$ab = 0 \Longrightarrow a = 0 \text{ or } b = 0$$

or equivalently, $a \neq 0, b \neq 0 \Longrightarrow ab \neq 0$

6.6 Integral domain, division ring and field

Rings without zero divisors are special and have many interesting properties. These rings are discussed at length in this section.

Definition A commutative ring R with unity $1 \neq 0$ is called an **integral domain** if it contains no proper zero divisors.

However, some authors do not include the existence of unity as a necessary condition to define integral domain and simply define integral domain as a commutative ring without zero divisors.

Example 6.6.1 Since for any two integers a, b; we have $ab = 0 \Longrightarrow a = 0$ or $= 0$, hence the ring $\mathbb{Z}$ of integers is an integral domain.

Example 6.6.2 The ring $\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is an integral domain. **Solution** From example 6.3.10, We know that $\mathbb{Q}[\sqrt{2}\,]$ is a commutative ring with unity $1 + 0\sqrt{2}$.

Let $x, y \in \mathbb{Q}[\sqrt{2}\,]$ such that $x = a_1 + b_1\sqrt{2}$ and $y = a_2 + b_2\sqrt{2}$ .Then

$$xy = 0 \Longrightarrow (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = 0 + 0\sqrt{2}$$
$$\Longrightarrow (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} = 0 + 0\sqrt{2}$$
$$\Longrightarrow a_1a_2 + 2b_1b_2 = 0, a_1b_2 + b_1a_2 = 0$$

Which is possible only when either $a_1 = 0, b_1 = 0$ or $a_2 = 0, b_2 = 0$, i.e. either $x = 0$ or $y = 0$.

Hence the ring $\mathbb{Q}[\sqrt{2}\,]$ is without zero divisors. Therefore $\mathbb{Q}[\sqrt{2}\,]$ is an integral domain.

Example 6.6.3 We have seen that the ring $(\mathbb{Z}_6, +_6, \times_6)$has zero divisors. Hence it is not an integral domain. However from the following composition table we observe that the ring $(\mathbb{Z}_5, +_5, \times_5)$ is without zero divisors

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

i.e. $a \times_5 b = 0 \Longrightarrow a = 0$or $b = 0$

Hence $(\mathbb{Z}_5, +_5, \times_5)$ is a commutative ring with unity and without zero divisors, i.e. it is an integral domain.

What do you say about $(\mathbb{Z}_n, +_n, \times_n)$? The following proposition gives the answer.

Proposition The ring $(\mathbb{Z}_n, +_n, \times_n)$ is an integral domain if and only if n is prime.

Proof: Suppose that n is a prime number and $a, b \in \mathbb{Z}_n$ such that $a \times_n b = 0$. Then n divides ab. Since n is a prime, hence $n|ab \Longrightarrow n|a$ or $n|b$. Now $0 \leq a \leq n - 1$ and $0 \leq b \leq n - 1$. Therefore $n|a \Longrightarrow a = 0$. Similarly $n|b \Longrightarrow b = 0$.

Thus $a \times_n b = 0 \Longrightarrow a = 0$ or $b = 0$, i.e. $\mathbb{Z}_n$ is an integral domain.

Conversely, suppose that $(\mathbb{Z}_n, +_n, \times_n)$ is an integral domain and n is not prime. Let $n = pq$ such that $1 < p < n$ and $1 < q < n$ but then $p, q \in \mathbb{Z}_n$ such that $p \neq 0, q \neq 0$ and $p \times_n q = pq \pmod{n} = 0$, i.e. $\mathbb{Z}_n$ has zero divisors, a contradiction. Hence n must be a prime.

Proposition The cancellation laws hold in an integral domain.

Proof Let R be an integral domain, i.e. R is a commutative ring with unity and without zero divisors. Let $a \neq 0$ and $ab = ac$. Then

$$ab - ac = 0$$
$$\Longrightarrow ab + a(-c) = 0$$
$$\Longrightarrow a[b + (-c)] = 0$$
$$\Longrightarrow b + (-c) = 0 \quad \text{as } a \neq 0$$
$$\Longrightarrow b = c$$

Similarly, if $a \neq 0$, then $ba = ca \Longrightarrow b = c$.

So far we have not talked about the multiplicative inverses of the elements of a ring. However, we know that the multiplicative inverses of elements do exist in some rings. For example, the non-zero elements in $(\mathbb{Z}_5,\ +_5,\ \times_5)$ have multiplicative inverses, i.e. $1 \times_5 1 = 1$, $2 \times_5 3 = 1 = 3 \times_5 2$ and $4 \times_5 4 = 1$. These elements are called *units*. So we have the following definition-

Definition Let R be a ring with unity $1 \neq 0$. An element u of R is called a **unit** (or invertible) in R if there exists some $v \in R$ such that $uv = 1 = vu$. The set of units of R is denoted by $R^\times$.

Now we shall show that $R^\times$ forms a group under multiplication.

Proposition Let R be a ring with unity. The multiplication in R induces a multiplication in the set $R^\times$ of units with respect to which $R^\times$ is a group.

Proof: Since the unity is the multiplicative inverse of itself, hence $1 \in R^\times$. Let $a, b \in R^\times$. Then there exist elements $c, d \in R$ such that $ac = 1 = ca$ and $bd = 1 = db$. Let $dc = h$. Now $(ab)h = abdc = ac = 1$ and $h(ab) = dcab = db = 1$. Thus $(ab)h = 1 = h(ab)$, i.e. ab is a unit in R. Hence $ab \in R^\times$.

Now $a \in R^\times$ implies that there exists $c \in R$ such that $ac = 1 = ca$. Thus c is a unit in R, i.e. $c \in R^\times$. The associativity holds in $R^\times$ as it holds in R. This shows that $R^\times$ is a group with respect to the induced multiplication.

Example 6.6.4 The units of the ring $\mathbb{Z}$ are 1 and -1, i.e. $\mathbb{Z}^\times = \{-1, 1\}$

Example 6.6.5 In unit-1, you have seen that the set of all invertible elements (units) of $\mathbb{Z}/n\mathbb{Z}, (n \geq 2)$ forms an abelian group with respect to multiplication of residue classes. This set of units is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} : [a] \text{ is invertible}\}$$

Also we proved that $[a] \in \mathbb{Z}/n\mathbb{Z}$ is invertible with respect to residue multiplication if and only if $\gcd(a, n) = 1$. Hence

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} :\ a \text{ and } n \text{ are co-prime}\}$$

Therefore in the ring $\mathbb{Z}/n\mathbb{Z}$ the elements $[a]$ for which a and n are co-prime are units. You can verify that every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor. For example, in the ring $\mathbb{Z}/8\mathbb{Z}$, the units are [1], [3], [5] and [7]. The zero divisors are [0], [2], [4] and [6].

Note: From unit-1**,** we know that the set of all invertible elements (units) of $\mathbb{Z}_n$ forms an abelian group with respect to multiplication modulo n and is denoted by $\mathbb{U}_n$. Where $\mathbb{U}_n = \{a \in \mathbb{Z}_n : a \text{ and } n \text{ are co-prime}\}$.

Hence for the ring $(\mathbb{Z}_n,\ +_n,\ \times_n)$, we have $(\mathbb{Z}_n)^\times = \mathbb{U}_n$.

Now let us define some special rings which contain units.

Definition A ring R with unity $1(\neq 0)$ is called a **division ring** (or **skew field**) if every nonzero element of R is a unit (invertible). In other words, A ring with unity is a division ring if its nonzero elements form a group under multiplication.

In a division ring $(R,\ +,\ \cdot)$, $R - \{0\}$ is a group with respect to multiplication induced by '$\cdot$' i.e. $R^\times = R - \{0\}$.

Definition A commutative ring R with unity $1(\neq 0)$ is called a **field** if every nonzero element of R is a unit (invertible). In other words, a field is a commutative division ring. In this way, every field is a division ring.

Please be careful while using the words *unit* and *unity*. Unity is the multiplicative identity element, while a unit is an element having a multiplicative inverse. Now let us illustrate the concepts of division ring and field with examples.

It is obvious that the ring $\mathbb{Z}$ of integers is not a division ring and hence not a field as its nonzero elements do not have multiplicative inverses. The rings $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are all fields. Now we give an example of a division ring which is not a field.

Example 6.6.6 You have seen in example 6.3.8 that the ring of real Hamilton Quaternions $\mathbb{H}$ is a noncommutative ring with unity.

Let $a + bi + cj + dk$ be a nonzero element of $\mathbb{H}$. Then $a - bi - cj - dk$ is also a nonzero element of $\mathbb{H}$. By the definition of quaternion multiplication, we have

$$\begin{aligned}&(a + bi + cj + dk) \cdot (a - bi - cj - dk)\\ &= (a^2 + b^2 + c^2 + d^2) + (-ab + ba - cd + cd)i + (-ac + ac - db + bd)j\\ &\quad +(-ad - bc + da + cb)k\\ &= (a^2 + b^2 + c^2 + d^2)\end{aligned}$$

Hence

$$(a + bi + cj + dk) \cdot \frac{(a - bi - cj - dk)}{(a^2 + b^2 + c^2 + d^2)} = 1$$

$$\Longrightarrow (a + bi + cj + dk)^{-1} = \frac{(a - bi - cj - dk)}{(a^2 + b^2 + c^2 + d^2)}$$

Thus each nonzero element of $\mathbb{H}$ is invertible. This makes the ring of real Hamilton Quaternions $\mathbb{H}$ a division ring. However It is not a field as it is not commutative.

Example 6.6.7 The ring $(\mathbb{Z}_5, +_5, \times_5)$ is a field.

As you have seen earlier in example 6.6.3 that $(\mathbb{Z}_5, +_5, \times_5)$ is a commutative ring with unity. From the composition table, we observe that every nonzero element has a multiplicative inverse, i.e. $1 \times_5 1 = 1$, $2 \times_5 3 = 1 = 3 \times_5 2$ and $4 \times_5 4 = 1$. Thus $(\mathbb{Z}_5, +_5, \times_5)$ is a field. This is an example of a finite field.

Example 6.6.8 The ring $\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

Solution From example 6.3.10, We know that $\mathbb{Q}[\sqrt{2}\,]$ is a commutative ring with unity $1 + 0\sqrt{2}$. Let $a + b\sqrt{2}$ be a non-zero element of $\mathbb{Q}[\sqrt{2}\,]$. Then at least one of a and b is not zero. Now

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

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

Now $a, b \in \mathbb{Q}$, hence $a^2 - 2b^2 = 0 \Longrightarrow a = 0, b = 0$. This is not possible. Therefore $a^2 - 2b^2 \neq 0$. Hence

$$(a + b\sqrt{2})^{-1} = \frac{(a - b\sqrt{2})}{(a^2 - 2b^2)} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}\,]$$

This shows that every nonzero element in $\mathbb{Q}[\sqrt{2}\,]$ is a unit, i.e. $\mathbb{Q}[\sqrt{2}\,]$ is a field.

Proposition Every field is an integral domain.

Proof Let $(F, +, \cdot)$ be a field. Then F is a commutative ring with unity $1 \neq 0$ such that every nonzero element of F is invertible. To show that F is an integral domain, we have to show that F is without zero divisors.

Let $a, b \in F$ such that $ab = 0$.
If $a \neq 0$, then there exists $a^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1}a$.
Then $ab = 0 \Longrightarrow a^{-1}(ab) = a^{-1}0$
$\Longrightarrow (a^{-1}a)b = 0$
$\Longrightarrow b = 0$
Similarly, if $b \neq 0$, then you can show that $ab = 0 \Longrightarrow a = 0$
Thus $ab = 0 \Longrightarrow a = 0$ or $b = 0$, i.e. F is without zero divisors and hence an integral domain.
Now you may ask whether the converse is true. It is true but only for finite integral domains. Hence we have the following proposition.

Proposition Every finite integral domain is a field.
Proof : Let $R = \{a_1, a_2, \dots, a_n\}$ be a finite integral domain with n distinct elements. Then R will be a commutative ring with unity $1 \neq 0$. To prove that R is a field, we show that every nonzero element of R is a unit. Let $a \neq 0$ be a nonzero element of R. Since R is closed under multiplication, hence $aa_1, aa_2, \dots, aa_n$ are elements of R. All these elements are distinct. For if $aa_i = aa_j$, $i \neq j$ then the cancellation law in R gives $a_i = a_j$, a contradiction. Since $1 \in R$, hence one of the products $aa_1, aa_2, \dots, aa_n$ must be equal to 1. Therefore there exists a unique element $a_k \in R$, $1 \leq k \leq n$, such that $aa_k = 1$. Since R is commutative, hence $aa_k = 1 = a_k a$, i.e. a is invertible. Hence R is a field.

6.7 Subrings and subfields

The notion of a subring in ring theory is analogous to that of a subgroup in group theory. We have seen that the set $2\mathbb{Z}$ of all even integers is a ring under usual addition and multiplication and $2\mathbb{Z} \subset \mathbb{Z}$. Soon we shall see that $2\mathbb{Z}$ is a subring of the ring $\mathbb{Z}$ of integers. Also we shall demonstrate that $\mathbb{Z}$ is a subring of the ring $\mathbb{Q}$ of rational numbers. In a similar fashion we can define a subfield of a given field.

Definition A non-empty subset S of a ring R is called a subring of R if S is closed under the addition and multiplication compositions in R and S itself is a ring under the induced addition and multiplication compositions.
Since $S \subseteq R$, hence the properties such as associative law, commutative law and distributive law hold good in S as they hold good in R. So we need to check only few conditions in order to show that S is a subring of R. Let us establish this criterion.
Proposition A non-empty subset S of a ring R is a subring of R if and only if $a - b \in S$ and $ab \in S$ for all $a, b \in S$.
Proof First suppose that S is a subring of R. Then S is a group under induced addition '$+$'. Let $a, b \in S$. Then $-b \in S$ and hence $a + (-b) \in S$, i.e. $a - b \in S$. Also S is closed under induced multiplication. Hence $ab \in S$.
Conversely, suppose that S is a non-empty subset of R such that $a - b \in S$ and $ab \in S$ for all $a, b \in S$.
Now the condition $a - b \in S$ for all $a, b \in S$ implies that $(S, +)$ is a subgroup of $(R, +)$. Since commutativity of addition holds in R, it will hold in S as well. Hence $(S, +)$ is an abelian group under induced addition.

The condition $ab \in S$ for all $a, b \in S$ implies that S is closed under induced multiplication. The remaining properties such as associativity of multiplication and the distributive laws hold in S since they hold in R. Thus S is a ring under induced addition and multiplication. Hence S is a subring of R.

Now we shall apply this result to check whether a given subset of ring is a subring.

Example 6.7.1 $\mathbb{Z}$ is a subring of the ring $\mathbb{Q}$.

Obviously we have $a - b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$ and hence the result.

Example 6.7.2 Let S be a set of all 2×2 matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ where $a, b \in \mathbb{R}$. Then S is a subring of $M_2(\mathbb{R})$.

Let $A, B \in S$ such that $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$. Then

$$A - B = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in S$$

Also

$$AB = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 & 0 \end{bmatrix} \in S$$

Hence S is a subring of $M_2(\mathbb{R})$.

Example 6.7.3 $2\mathbb{Z}$ is a subring of the ring $\mathbb{Z}$ of integers.

Let $a, b \in 2\mathbb{Z}$. Then $a = 2x, b = 2y$ where $x, y \in \mathbb{Z}$. Now

$a - b = 2x - 2y = 2(x - y) \in 2\mathbb{Z}$ and $(2x)(2y) = 2(2xy) \in 2\mathbb{Z}$.

Hence $2\mathbb{Z}$ is a subring of the ring $\mathbb{Z}$ of integers.

Here you will notice one interesting thing that $\mathbb{Z}$ is a ring with unity, however $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ without unity. Thus subring of a ring with unity may not have unity. Also it may happen that a subring may have unity which is different from the unity of the ring. So we have the following example.

Example 6.7.4 $\mathbb{Z} \times \mathbb{Z} = \{(m, n) : m, n \in \mathbb{Z}\}$ is a ring under following addition and multiplication

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$$
$$(m_1, n_1)(m_2, n_2) = (m_1 m_2, n_1 n_2)$$

The unity of this ring is $(1,1)$.

We have $\mathbb{Z} \times \{0\} \subset \mathbb{Z} \times \mathbb{Z}$. Let $(m_1, 0), (m_2, 0) \in \mathbb{Z} \times \{0\}$. Then

$$(m_1, 0) - (m_2, 0) = (m_1 - m_2, 0) \in \mathbb{Z} \times \{0\}$$

and

$$(m_1, 0)(m_2, 0) = (m_1 m_2, 0) \in \mathbb{Z} \times \{0\}$$

Hence $\mathbb{Z} \times \{0\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. Now

$$(m, 0)(1,0) = (m, 0) = (1,0)(m, 0)$$

Therefore $(1,0)$ is the unity of $\mathbb{Z} \times \{0\}$ which is different from the unity of $\mathbb{Z} \times \mathbb{Z}$.

Example 6.7.5 The set of Gaussian integers

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$$

is a subring of the complex numbers $\mathbb{C}$.

Note $\{0\}$ and R are subrings of any ring R. Subring $\{0\}$ is called the *trivial* subring of R.

You have seen while studying group theory that the intersection of two subgroups is again a subgroup. We have similar result for subrings.

Proposition The intersection of two subrings is a subring.

Proof: Let S_1 and S_2 be any two subrings of a ring R. We have $0 \in S_1 \cap S_2$, hence $S_1 \cap S_2$ is a non-empty subset of R. Let $a, b \in S_1 \cap S_2$. Then $a, b \in S_1$ and $a, b \in S_2$. Since S_1 and S_2 are subrings of R, hence we have

$$a, b \in S_1 \Longrightarrow a - b \in S_1 \text{ and } ab \in S_1$$
$$a, b \in S_2 \Longrightarrow a - b \in S_2 \text{ and } ab \in S_2$$

Now $a - b \in S_1$ and $a - b \in S_2 \Longrightarrow a - b \in S_1 \cap S_2$

and $ab \in S_1$ and $ab \in S_2 \Longrightarrow ab \in S_1 \cap S_2$

Therefore $S_1 \cap S_2$ is a subring of R.

Now we shall define the notion of a subfield of a given field.

Definition A non-empty subset K of a field F is said to be a **subfield** of F if K is closed with respect to the addition and multiplication compositions in F and K itself is a field under the induced addition and multiplication compositions.

Let us establish the following important characterization of a subfield.

Proposition Any subset K of a field F, containing at least two elements, is a subfield of F if and only if

(i) $a \in K, b \in K \Longrightarrow a - b \in K$

(ii) $a \in K, 0 \neq b \in K \Longrightarrow ab^{-1} \in K$

Proof: Suppose that K is a subfield of F. Then $(K, +)$ is an abelian group. Let $a, b \in K$. Then $-b \in K$ and hence $a + (-b) \in K$, i.e. $a - b \in K$.

Also every nonzero element of K is a unit. Hence $0 \neq b \in K \Longrightarrow b^{-1} \in K$. Now K is closed under multiplication, hence $a \in K, b^{-1} \in K \Longrightarrow ab^{-1} \in K$.

Conversely suppose that the conditions (i) and (ii) hold. Now the condition (i) implies that $(K, +)$ is a subgroup of $(F, +)$. Since commutativity of addition holds in F, it will hold in K as well. Hence $(K, +)$ is an abelian group under induced addition.

Let $0 \neq a \in K$, then from (ii), we have $aa^{-1} \in K$, i.e. $1 \in K$, hence the unity exists. Again from (ii) we have $1 \in K, 0 \neq a \in K \Longrightarrow 1a^{-1} \in K$, i.e. $a^{-1} \in K$. Hence each nonzero element of K has multiplicative inverse.

Now $a \in K, 0 \neq b \in K \Longrightarrow a \in K, b^{-1} \in K \Longrightarrow a(b^{-1})^{-1} \in K$, by (ii).

$$\Longrightarrow ab \in K$$

If $b = 0$, then $ab = 0 \in K$. Hence we have $ab \in K \; \forall a, b \in K$.

The remaining properties of a field such as associativity of multiplication, commutativity of multiplication and the distributive laws hold in K since they hold in F. Thus K is a Field under induced addition and multiplication. Hence K is a subfield of F.

Example The field $\mathbb{Q}$ of rational numbers is a subfield of the field $\mathbb{R}$ of real numbers. Also the field $\mathbb{R}$ of real numbers is a subfield of the field $\mathbb{C}$ of complex numbers.

6.8 Summary

In this unit, we have

(1) Discussed the notion of a ring with examples.
(2) Defined zero divisors and introduced rings with zero divisors.
(3) Defined integral domain, division ring and field with examples.

(4) Proved that the ring $(\mathbb{Z}_n, +_n, \times_n)$ is an integral domain if and only if n is prime.
(5) Proved that the cancellation laws hold in an integral domain.
(6) Proved that every field is an integral domain and every finite integral domain is a field.
(7) Introduced the notion of a subring and subfield with examples and proved that the intersection of two subrings is a subring.

6.9 Self assessment questions

(1) Let G be an additive abelian group. Define an operation in G by $ab = 0$ for all $a, b \in G$. Prove that $(G, +, .)$ is a ring.

(2) Show that the power set $\mathcal{P}(A)$ of a given set A forms a Boolean ring under the compositions:

$$X + Y = (X - Y) \cup (Y - X) \text{and} \quad XY = X \cap Y \text{ for all } X, Y \in \mathcal{P}(A)$$

(3) Show that any ring $(R, +, .)$ in which $a + b = ab$ for all $a, b \in R$ is the zero ring.

(4) Show that the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a commutative ring with unity under addition and multiplication induced by those in $\mathbb{R}$.

(5) Let $(R, +, .)$ be a ring. Prove that $\mathbb{Z} \times R$ is a ring with unity under the operations $\oplus$ and $\odot$ given by

$$(m, a) \oplus (n, b) = (m + n, a + b)$$

and

$$(m, a) \odot (n, b) = (mn, mb + na + ab)$$

(6) Let $D[0,1]$ denote the set of all real valued differentiable functions on $[0,1]$. Show that it is a commutative ring with respect to pointwise addition and pointwise multiplication.

(7) Show that $R = \{0,2,4\}$ is a subring of the ring $\mathbb{Z}_6$.

(8) Show that for each positive integer n, the set $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(9) Prove that a ring can have at most one unity.

(10) Let R be a ring. Let $m, n \in \mathbb{Z}$ and $a, b \in R$. Show that –
(i) $(ma)(nb) = (mn)(ab)$
(ii) $m(ab) = (ma)b = a(mb)$

(11) Let R be a ring and $a \in R$. Show the set $S = \{x \in R : ax = 0\}$ is a subring of R.

(12) Let R be a ring. The *center* of R is the set $\{x \in R : ax = xa \quad \forall a \in R\}$. Prove that the center of a ring is a subring of R.

(13) Show that every nonzero element of the ring $(\mathbb{Z}_n, +_n, \times_n)$ is either a unit or a zero-divisor.

(14) Prove that the sets of idempotents of a commutative ring is closed under multiplication.

(15) Prove that the only idempotents in an integral domain are 0 and 1.

(16) Let d be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}\,] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ is a field.

6.10 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

(6) Lang, S. (1965): Algebra, Reading, Massachusetts, Addison-Wesley.

(7) Barshay, J. (1969): Topics in ring theory, N.Y., W.A. Benjamin Inc.

(8) Burtan, D. M. (1968): A first course in Rings and Ideals, Reading, MA., Addison-Wesley.

Unit-7: Homomorphisms and Embedding of rings

Structure

7.1 Introduction

In unit 6, we introduced the notion of a ring. You studied different types of rings such as integral domain, division ring and field and their properties. We begin this unit by associating a special number with an integral domain. You will see that for an integral domain R there may exist a positive integer n such that $na = 0$ for all $a \in R$. The smallest such integer, if it exists, is called the characteristic of the integral domain. Otherwise the integral domain is said to be of characteristic zero. We shall illustrate this concept with examples.

Next we shall define the concept of a homomorphism for a ring. You have already studied these composition preserving mappings for groups. Since in rings we have two operations, so we have two conditions, i.e. for a mapping f from a ring R to a ring $R'$to be a homomorphism, we must have

(i) $f(a+b) = f(a) + f(b)$ (ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

If f is a bijection, we call it an isomorphism. The isomorphic rings are abstractly identical in the same way the isomorphic groups are. We shall study different ring homomorphisms with examples. We shall define kernel of a ring homomorphism as we did for group homomorphism. Similar to the notion of a normal subgroup in group theory, we shall introduce the concept of an ideal here. However a detailed study of ideals is the central theme of our next unit. The direct and inverse images of subring and subfield will be discussed.

You know that a field has richer structure than an integral domain. How can we enlarge an integral domain to a field? The answer is the concept of embedding of rings. We shall discuss different procedures of embedding one ring into another. You will see that an integral domain can be embedded in a field. This special field is called the field of fractions or field of quotients of the corresponding integral domain. The motivation comes from the construction of rational numbers by integers. So the natural example of a field of fractions is $\mathbb{Q}$ which embeds the integral domain $\mathbb{Z}$

of integers. You will observe that the field of fractions is the smallest field containing the given integral domain.

7.2 Objectives

After reading this unit, you should be able to

- Define and illustrate the concept of characteristic of a ring.
- Define and discuss different homomorphisms of rings such as monomorphisms, epimorphisms, isomorphisms, endomorphisms, and automorphisms.
- Discuss the kernel of a ring homomorphism.
- Obtain properties of direct and inverse images of subrings and subfields.
- Define embedding of rings and discuss different procedures of embedding one ring into another.
- Describe the embedding of an integral domain in a field and define the field of fractions or quotients.
- Discuss results concerning the field of fractions.

7.3 Characteristic of an integral domain

Let us consider the integral domain $(\mathbb{Z}_5,\ +_5,\ \times_5)$. We observe that

$1(1) = 1,\ 2(1) = 1+_5 1 = 2,\ 3(1) = 1+_5 1+_5 1 = 3,$

$4(1) = 1+_5 1+_5 1+_5 1 = 4,\ 5(1) = 1+_5 1+_5 1+_5 1+_5 1 = 0$, hence the additive order of 1 is 5, i.e. $o(1) = 5$.

Also $1(2) = 2,\ 2(2) = 4,\ 3(2) = 1,\ 4(2) = 3,\ 5(2) = 0$, hence $o(2) = 5$.

Similarly $o(3) = 5,\ o(4) = 5$. Interestingly, the additive order of each element of the integral domain $\mathbb{Z}_5$ is the same. Let us see whether it is true for all integral domains.

Let $(R, +,\ .)$ be an integral domain. We shall see that

$$ma = 0 \Leftrightarrow mb = 0 \text{ for all } a, b \in R - \{0\}.$$

We have $(ma)b = (a + a + \cdots m \text{ times})b$
$= ab + ab + \cdots\ m \text{ times},$ by distributive law
$= a(b + b + \cdots\ m \text{ times})$, by distributive law
$= a(mb)$

If $ma = 0$, then $a(mb) = (ma)b = 0b = 0$. Since $a \neq 0$ and R is an integral domain, hence $mb = 0$. Similarly $mb = 0 \Longrightarrow ma = 0$.

Thus $ma = 0 \Leftrightarrow mb = 0$ for all $a, b \in R - \{0\}$. That means

In an integral domain the additive order of any two nonzero elements are same.

This promotes the following definition.

Definition Let $(R, +, .)$ be an integral domain. The smallest positive integer n, if it exists, such that $na = 0$ for all $a \in R$ is called the **characteristic** of the integral domain R. If no such positive integer exists, then R is said to be of characteristic zero.

Examples

(i) The characteristic of the integral domain $(\mathbb{Z}_5, +_5, \times_5)$ is 5.

(ii) The characteristic of the integral domain $\mathbb{Z}$ is zero.

(iii) The characteristic of the integral domain $\mathbb{Q}$ is zero.

Now we shall prove a result that puts some restrictions on the characteristic of an integral domain.

Proposition The characteristic of an integral domain is either zero or a prime number.

Proof Let R be an integral domain. Let R have finite characteristic n.. We shall prove that n is a prime number. Suppose on the contrary that n is not prime. Then $n = pq$, where $1 < p < n$ and $1 < q < n$. Let $a \neq 0$. Since R is an integral domain, hence $a^2 = aa \neq 0$. Now the order of each nonzero element of an integral domain is the same. Hence $o(a) = o(a^2) = n$.

$$\begin{aligned} \therefore na^2 = 0 &\Longrightarrow (pq)a^2 = 0 \\ &\Longrightarrow (pq)(aa) = 0 \\ &\Longrightarrow (pa)(qa) = 0 \\ &\Longrightarrow \text{Either } pa = 0 \text{ or } qa = 0 \end{aligned}$$

This is a contradiction to our assumption that n is the order of a. Hence n must be prime.

Note: Since every field is an integral domain, hence the characteristic of a field is either 0 or prime number.

Corollary If R is a finite integral domain, then the characteristic of R divides $o(R)$.

Proof Let R be a finite integral domain with n elements, i.e. $o(R) = n$. Since R is finite, hence the order of its elements cannot be infinite. Then the characteristic of R is a prime number p (say). Hence the additive order of every nonzero element of R is also p. By Lagrange's theorem, order of an element divides the order of the group, i.e. p divides n.

Example Let $(R, +, .)$ be an integral domain of characteristic p. Then show that

$$(a + b)^p = a^p + b^p \text{ for all } a, b \in R.$$

Solution: We have

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ \ldots\ldots + b^p$$

Now p divides $\binom{p}{r}$ for all $r,\ 1 \leq r \leq p - 1$. Hence $\binom{p}{r} = mp$ for some positive integer m. Therefore for all $r,\ 1 \leq r \leq p - 1$, we have

$$\binom{p}{r} a^{p-r}b^r = mpa^{p-r}b^r = mpc$$

where $c = a^{p-r}b^r \in R$. Since p is the characteristic of R, hence $pc = 0$. Therefore $\binom{p}{r}a^{p-r}b^r = 0$ for all $r,\ 1 \leq r \leq p - 1$. This gives

$$(a + b)^p = a^p + b^p$$

Proposition The order of a finite field is p^n for some prime p and $n > 0$.

Proof Let F be a finite field. Then its characteristic is a prime number p (say). Hence the additive order of each nonzero element is also p, i.e. $(F, +)$ is a p-group. Now any prime q other than p cannot divide $o(F)$. For otherwise, by Cauchy's theorem, F will contain an element of order $q(\neq p)$. Which is not possible as each element of F has the same order p. So we must have $o(F) = p^n$ for some $n > 0$.

7.4 Homomorphism and isomorphism of rings

In unit 2, we introduced the notion of a homomorphism for groups as a mapping satisfying the composition preserving property. In a similar way, we can define homomorphism for a ring.

Definition Let R and R' be any two rings. A mapping $f: R \longrightarrow R'$ is called a **ring homomorphism** or simply a homomorphism if it satisfies the following properties:

(i) $f(a+b) = f(a) + f(b)$ (ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

A homomorphism is called a **monomorphism** if it is one-one and **epimorphism** if it is onto. A bijective homomorphism is called an **isomorphism.** A homomorphism of a ring R into itself is called an **endomorphism**. An isomorphism of a ring R onto itself is called an **automorphism.**

Let us illustrate these concepts with some examples.

Example 7.4.1 The mapping $f: \mathbb{Z} \longrightarrow \mathbb{Z}_n$ given by

$$f(a) = a(\text{mod } n) \text{ for all } a \in \mathbb{Z}$$

is a ring homomorphism.

Solution: Let $a, b \in \mathbb{Z}$. Then

$$f(a+b) = (a+b)(\text{mod } n)$$
$$= a(\text{mod } n) +_n b(\text{mod } n)$$
$$= f(a) +_n f(b)$$

and

$$f(ab) = (ab)(\text{mod } n)$$
$$= a(\text{mod } n) \times_n b(\text{mod } n)$$
$$= f(a) \times_n f(b)$$

Example 7.4.2 The mapping $\varphi: \mathbb{R}[x] \longrightarrow \mathbb{R}$ given by $\varphi[f(x)] = f(1)\ \forall f(x) \in \mathbb{R}[x]$ is a ring homomorphism.

Solution: Let $f(x), g(x) \in \mathbb{R}[x]$ such that $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$. The evaluation of $f(x)$ at $1 \in \mathbb{R}$ is given by $f(1) = \sum_{i=0}^{\infty} a_i$. Hence

$$\varphi[f(x)] = f(1) = \sum_{i=0}^{\infty} a_i$$

Now $f(x) + g(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$. Therefore

$$\varphi[f(x) + g(x)] = \sum_{i=0}^{\infty} (a_i + b_i)$$
$$= \sum_{i=0}^{\infty} a_i + \sum_{i=0}^{\infty} b_i$$

$$= f(1) + g(1)$$

$$= \varphi[f(x)] + \varphi[g(x)]$$

Also $f(x)g(x) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} c_i x^i$, Where $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.
Hence

$$\varphi[f(x)g(x)] = \varphi\left(\sum_{i=0}^{\infty} c_i x^i\right)$$
$$= \sum_{i=0}^{\infty} c_i$$
$$= \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)$$
$$= \left(\sum_{i=0}^{\infty} a_i\right)\left(\sum_{i=0}^{\infty} b_i\right)$$
$$= f(1)g(1)$$
$$= \varphi[f(x)]\varphi[g(x)]$$

Hence φ is a ring homomorphism.

Example 7.4.3 Let $f: \mathbb{C} \longrightarrow \mathbb{C}$ be a mapping from the ring of complex numbers to itself such that $f(z) = \bar{z}$ for all$z \in \mathbb{C}$. Then f is a ring homomorphism.
Solution: Let $z_1, z_2 \in \mathbb{C}$. Then

$$f(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z_1} + \bar{z_2} = f(z_1) + f(z_2)$$

and

$$f(z_1 z_2) = \overline{z_1 z_2} = \bar{z_1}\bar{z_2} = f(z_1)f(z_2)$$

This proves that f is a ring homomorphism.

Example 7.4.4 Let us discuss the endomorphisms of the ring $\mathbb{Z}$ of integers. In unit 2, we have seen that the mapping $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $f(x) = 2x$ for all $x \in \mathbb{Z}$ is an endomorphism of the additive group $\mathbb{Z}$ of integers. But it is not a ring homomorphism as $f(1) = 2 \cdot 1 = 2$ and hence

$$2 = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = 2 \cdot 2 = 4$$

which is not possible. So what kind of endomorphisms of the ring $\mathbb{Z}$ we can have?
Suppose $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ is a ring homomorphism, i.e. an endomorphism. Then f is a group homomorphism from $\mathbb{Z}$ to itself. Thus there exists $m \in \mathbb{Z}$ such that $f(x) = mx$ for all $x \in \mathbb{Z}$. Now $f(1) = m \cdot 1 = m$, Since f is a ring homomorphism, hence $m = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = m \cdot m = m^2$. Therefore $m^2 = m$. This gives $m = 0$ or $m = 1$. Hence f is either zero homomorphism or identity homomorphism.
Example 7.4.5 From unit 6, we know that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}: a, b \in \mathbb{Z}\}$ is a ring under addition and multiplication of real numbers.
The mapping $f: \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{2}]$ given by $f(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of $\mathbb{Z}[\sqrt{2}]$.
f is one-one: Let $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then

$$f(a_1 + b_1\sqrt{2}) = f(a_2 + b_2\sqrt{2}) \Longrightarrow a_1 - b_1\sqrt{2} = a_2 - b_2\sqrt{2}$$
$$\Longrightarrow a_1 = a_2,\ b_1 = b_2$$
$$\Longrightarrow a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$$

f is onto: Suppose $a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then $a, b \in \mathbb{Z}$ which implies that $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Hence for $a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, there exists $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that $f(a + b\sqrt{2}) = a - b\sqrt{2}$, i.e. f is onto.

f is a homomorphism: Let $x, y \in \mathbb{Z}[\sqrt{2}]$ such that $x = a_1 + b_1\sqrt{2}$ and $y = a_2 + b_2\sqrt{2}$. Then $f(x) = a_1 - b_1\sqrt{2}$ and $f(y) = a_2 - b_2\sqrt{2}$. Now

$$\begin{aligned} f(x+y) &= f\left[\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right)\right] \\ &= f\left[(a_1 + a_2) + (b_1 + b_2)\sqrt{2}\right] \\ &= (a_1 + a_2) - (b_1 + b_2)\sqrt{2} \\ &= \left(a_1 - b_1\sqrt{2}\right) + \left(a_2 - b_2\sqrt{2}\right) \\ &= f(x) + f(y) \end{aligned}$$

Also

$$\begin{aligned} f(xy) &= f\left[\left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right)\right] = f\left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}\right] \\ &= \left[(a_1a_2 + 2b_1b_2) - (a_1b_2 + b_1a_2)\sqrt{2}\right] \\ &= \left(a_1 - b_1\sqrt{2}\right)\left(a_2 - b_2\sqrt{2}\right) \\ &= f(x)f(y) \end{aligned}$$

Hence f is an automorphism of $\mathbb{Z}[\sqrt{2}]$.

Example 7.4.6 Let R be a ring with unity e. Then the mapping $f: \mathbb{Z} \longrightarrow R$ given by $f(n) = ne\ \forall n \in \mathbb{Z}$ is a ring homomorphism.

Let $m, n \in \mathbb{Z}$. There arise three cases.

Case I when both m and n are nonnegative. Then

$$\begin{aligned} f(m+n) &= (m+n)e \\ &= e + e + \cdots \ (m+n)\text{times} \\ &= (e + e + \cdots \ m \text{ times}) + (e + e + \cdots \ n \text{ times}) \\ &= me + ne \\ &= f(m) + f(n) \end{aligned}$$

Case II when both m and n are negative. Then

$$\begin{aligned} f(m+n) &= (m+n)e \\ &= (-m-n)(-e) \\ &= (-m)(-e) + (-n)(-e) \\ &= me + ne \\ &= f(m) + f(n) \end{aligned}$$

Case III when one of m and n is nonnegative, say $m \geq 0, n < 0$. Then

$$\begin{aligned} f(m+n) &= (m+n)e = [m-(-n)]e \\ &= e + e + \cdots \ [m-(-n)]\text{times} \\ &= (e + e + \cdots \ m \text{ times}) - (e + e + \cdots \ (-n) \text{ times}) \\ &= me - (-n)e \\ &= me + ne \\ &= f(m) + f(n) \end{aligned}$$

Now in a ring R, we have $(ma)(na) = (mn)(ab)$ for all $a, b \in R$ and for all $m, n \in \mathbb{Z}$. Hence we have

$$f(mn) = (mn)e = (mn)(ee) = (me)(ne) = f(m)f(n)$$

Thus f is a ring homomorphism.

[Note: Here we denote unity by e instead of 1 in order to differentiate it from $1 \in \mathbb{Z}$]

7.5 Some properties of ring homomorphism

In unit 2 you have seen that a group homomorphism f has the properties such as $e' = f(e)$ and $f(a^{-1}) = [f(a)]^{-1}$. Since a ring R is an additive abelian group $(R, +)$, hence a ring homomorphism shares similar properties.

Proposition: Let f be a homomorphism of a ring R into a ring R'. Then
(i) $f(0) = 0'$, where 0 and $0'$are the zero elements of R and R'respectively.
(ii) $f(-a) = -f(a)$
(iii)$f(a - b) = f(a) - f(b)$
(iv)$f(na) = nf(a)$
for all $a, b \in R$ and $n \in \mathbb{Z}$.
Proof: (i) Let $a \in R$. Then $f(a) \in R'$.
Now $f(a) + 0' = f(a)$
$= f(a + 0)$
$= f(a) + f(0)$, since f is a homomorphism
Therefore by left cancellation law in the additive group $(R, +)$, we have
$$0' = f(0)$$
(ii) $f(0) = 0' \Longrightarrow f[a + (-a)] = 0'$
$\Longrightarrow f(a) + f(-a) = 0'$
$\Longrightarrow f(-a) = -f(a)$
(iii) Let $a, b \in R$. We have
$$f(a - b) = f[a + (-b)] = f(a) + f(-b) = f(a) - f(b)$$
(iv) Let $n \in \mathbb{Z}$. If n is a positive integer, then
$f(na) = f(a + a + \cdots n \text{ times})$
$= f(a) + f(a) + \cdots n \text{ times}$, since f is a homomorphism
$= nf(a)$
If n is a negative integer, i.e. $n = -m$ (say), then
$$f(na) = f[(-m)a] = f[-(ma)] = -f(ma) = -mf(a) = nf(a)$$

Proposition Let f be a homomorphism of a ring R onto a ring R'. Let 1 be the unity of R and $R' \neq \{0\}$. Then $f(1)$ is the unity of R'.
Proof Let $y \in R'$. Since f is onto, hence there exists $x \in R$ such that $y = f(x)$.
Now $yf(1) = f(x)f(1) = f(x1) = f(x) = y$. Also $f(1)y = f(1)f(x) = f(1x) = f(x) = y$.
Hence $f(1)$ is the unity of R'.

7.6 Kernel of a homomorphism

You are familiar with the concept of the kernel of a group homomorphism. Now we shall give a similar definition for the kernel of a ring homomorphism.
Definition Let f be a homomorphism of a ring R into a ring R'. **Kernel** of the homomorphism f is defined as the set
$$\text{Ker } f = \{x \in R : f(x) = 0'\}$$
In case of group homomorphism, you observed that the kernel of a homomorphism is a normal subgroup. Here we have a similar notion that we call "ideal". So let us define ideals for a ring. You will learn more about ideals in the next unit.

Definition A non-empty subset A of a ring R is called an **ideal** if

$a, b \in A \Longrightarrow a - b \in A$ and $a \in A, r \in R \Longrightarrow ar \in A$ and $ra \in A$

Example The set E of even integers is an ideal of the ring $\mathbb{Z}$ of integers.

Let $a, b \in E$. Then $a = 2m$ and $b = 2n$ for some $m, n \in \mathbb{Z}$. Now

$$a, b \in E \Longrightarrow a - b = 2m - 2n = 2(m - n) \in E$$

and $a \in E, r \in \mathbb{Z} \Longrightarrow ar = (2m)r = 2mr \in E, ra = r(2m) = 2rm \in E$.

Now we shall show that Ker f is an ideal of R.

Proposition Let f be a homomorphism of a ring R into a ring R'. Then the kernel of the homomorphism f is an ideal of R.

Proof We have Ker $f = \{x \in R: f(x) = 0'\}$. Since $f(0) = 0'$, hence $0 \in$ Ker f. Hence Ker f is non-empty. Let $a, b \in$ Ker f. Then $f(a) = 0'$ and $f(b) = 0'$. Now

$$f(a - b) = f(a) - f(b) = 0' - 0' = 0'$$
$$\Longrightarrow a - b \in \text{Ker } f$$

Let $r \in R$. Then

$$f(ar) = f(a)f(r) = 0'f(r) = 0'$$
$$\Longrightarrow ar \in \text{Ker } f$$

Also
$$f(ra) = f(r)f(a) = f(r)0' = 0'$$
$$\Longrightarrow ra \in \text{Ker } f$$

Hence $a, b \in$ Ker $f \Longrightarrow a - b \in$ Ker f and $a \in$ Ker $f, r \in R \Longrightarrow ar \in$ Ker f and $ra \in$ Ker f.

Therefore Ker f is an ideal of R.

One more result is similar to that of group theory:

Proposition Let f be a homomorphism of a ring R into a ring R'. Then f is injective if and only if Ker $f = \{0\}$.

Proof First suppose that f is an injective homomorphism. Let $a \in$ Ker f. Then

$$f(a) = 0'$$
$$\Longrightarrow f(a) = f(0) \quad \text{as } f(0) = 0'$$
$$\Longrightarrow a = 0 \quad \text{as } f \text{ is one-one}$$

Therefore Ker $f = \{0\}$.

Conversely, suppose that Ker $f = \{0\}$. To show that f is an injective, let $a, b \in R$. Then

$$f(a) = f(b) \Longrightarrow f(a) - f(b) = 0'$$
$$\Longrightarrow f(a - b) = 0' \text{ as } f \text{ is a homomorphism}$$
$$\Longrightarrow a - b \in \text{Ker } f$$
$$\Longrightarrow a - b = 0 \quad \text{as Ker } f = \{0\}.$$
$$\Longrightarrow a = b$$

Hence f is an injective homomorphism of R into R'.

7.7 Direct and inverse images of subring and subfield

Let f be a homomorphism of a ring R into a ring R'. Let S be a subring (or subfield) of R. We define the **direct image** of S under f as follows-

$$f(S) = \{f(a) \in R': a \in S\}$$

Let K be a subring (or subfield) of R'. Then the **inverse image** of K is defined as follows-

$$f^{-1}(K) = \{r \in R : f(r) \in K\}$$

Similarly we can define the direct images and inverse images of ideals. Let us prove some results related to these concepts.

Proposition Let f be a homomorphism of a ring R into a ring R'. If S is a subring of R, then $f(S)$ is a subring of R'.

Proof Let $x, y \in f(S)$. Then $x = f(a)$ and $y = f(b)$ for some $a, b \in S$. Obviously $a - b \in S$ and $ab \in S$. Now

$$x - y = f(a) - f(b) = f(a - b) \in f(S)$$

and $xy = f(a)f(b) = f(ab) \in f(S)$.

Hence $f(S)$ is a subring of R'.

Proposition Suppose f is a homomorphism of a ring R onto a ring R'. If A is an ideal of R, then $f(A)$ is an ideal of R'.

Proof Let $x, y \in f(A)$. Since f is onto, hence $x = f(a)$ and $y = f(b)$ for some $a, b \in A$. Let $r \in R$. Hence $a - b \in A$ and $ra \in A$, $ar \in A$. Suppose $k = f(r) \in R'$. Now

$$x - y = f(a) - f(b) = f(a - b) \in f(A)$$

and $kx = f(r)f(a) = f(ra) \in f(A)$, $xk = f(a)f(r) = f(ar) \in f(A)$

Hence $f(A)$ is an ideal of R'.

Proposition Every homomorphic image of a commutative ring is commutative.

Proof Let R be a commutative ring and R' be a homomorphic image of R under the homomorphism f. Then f is onto and $R' = f(R)$.

Let $x, y \in R'$. Then $x = f(a)$ and $y = f(b)$ for some $a, b \in R$. Now

$$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$$

Hence R', i.e. $f(R)$ is a commutative ring.

Proposition Let K be an ideal of R'. Then $f^{-1}(K)$ is an ideal of R.

Proof We have

$$f^{-1}(K) = \{r \in R : f(r) \in K\}$$

Since $0' = f(0) \in K$, hence $0 \in f^{-1}(K)$. Therefore $f^{-1}(K)$ is non-empty. Let $a, b \in f^{-1}(K)$. Then $f(a), f(b) \in K$. Now K is an ideal of R', hence

$$f(a) - f(b) \in K$$
$$\Rightarrow f(a - b) \in K \quad \text{as } f \text{ is a homomorphism}$$
$$\Rightarrow a - b \in f^{-1}(K), \text{ by definition of } f^{-1}(K)$$

Let $r \in R$. Then$f(r) \in R'$. Since K is an ideal of R', hence

$$f(a) \in K, f(r) \in R' \Rightarrow f(a)f(r) \in K$$
$$\Rightarrow f(ar) \in K$$
$$\Rightarrow ar \in f^{-1}(K)$$

Also $f(a) \in K, f(r) \in R' \Rightarrow f(r)f(a) \in K \Rightarrow f(ra) \in K \Rightarrow ra \in f^{-1}(K)$.

Therefore $f^{-1}(K)$ is an ideal of R.

7.8 Embedding of a ring into another ring

A ring R is said to be embedded in a ring R'if there is a subring S of R'such that R is isomorphic to S. In other words, a ring R can be embedded in a ring R' if there exists a monomorphism of R into R'.

For example, the ring $\mathbb{R}$ of real numbers can be embedded in the ring $\mathbb{C}$ of complex numbers. As you can see that the map $f: \mathbb{R} \longrightarrow \mathbb{C}$ given by $f(a) = (a, 0)\ \forall a \in \mathbb{R}$ is a monomorphism.

Sometimes it is easier to deduce the structure of embedded ring R by using the properties of the ring R' embedding it. There are many ways we can embed a ring in another ring. You will see that

(1) Every ring can be embedded in a ring with unity

(2) A ring can be embedded in a ring of endomorphism of some abelian group.

(3) An integral domain can be embedded in a field

We shall discuss the first two embeddings in this section. Our next section is devoted to the last one where we shall construct a field in which a given integral domain can be embedded.

Let $(R, +, .)$ be a ring. Then we can show that

$$R \times \mathbb{Z} = \{(a, n): a \in R, n \in \mathbb{Z}\}$$

is a ring with unity under the addition and multiplication defined as under:

$$(a, n) + (b, m) = (a + b, n + m)$$

and

$$(a, n)(b, m) = (ab + nb + ma, nm)$$

for all $(a, n), (b, m) \in R \times \mathbb{Z}$.

Since R is a ring, hence $a + b \in R$, $ab \in R$ and $nb, ma \in R$. Therefore $ab + nb + ma \in R$. Hence $(a + b, n + m) \in R \times \mathbb{Z}$ and $(ab + nb + ma, nm) \in R \times \mathbb{Z}$. Thus $R \times \mathbb{Z}$ is closed under the addition and multiplication defined above. Let $\bar{0}$ be the zero element of R. Then $(\bar{0}, 0) \in R \times \mathbb{Z}$ and

$$(\bar{0}, 0) + (a, n) = (\bar{0} + a, 0 + n) = (a, n)$$

Also

$$(a, n) + (\bar{0}, 0) = (a + \bar{0}, n + 0) = (a, n)$$

Thus $(\bar{0}, 0)$ is the additive identity of $R \times \mathbb{Z}$.

Now $(\bar{0}, 1) \in R \times \mathbb{Z}$ such that

$$(a, n)(\bar{0}, 1) = (a\bar{0} + n\bar{0} + 1a, n1) = (\bar{0} + \bar{0} + a, n) = (a, n)$$

Similarly, $(\bar{0}, 1)(a, n) = (a, n)$. Therefore $(\bar{0}, 1)$ is the multiplicative identity of $R \times \mathbb{Z}$.

You can check that other properties of a ring are satisfied by $R \times \mathbb{Z}$ under under the addition and multiplication defined above. Thus $R \times \mathbb{Z}$ is a ring with unity $(\bar{0}, 1)$. Now we shall prove our main result.

Proposition Every ring can be embedded in a ring with unity.

Proof: Let R be a ring. We know that $R \times \mathbb{Z}$ is a ring with unity $(\bar{0}, 1)$. Let us define a mapping $f: R \longrightarrow R \times \mathbb{Z}$ by $f(a) = (a, 0)\ \forall a \in R$. We shall show that f is a monomorphism.

Let $a, b \in R$. Then

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

and $$f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a)f(b)$$

since $(a, 0)(b, 0) = (ab + 0b + 0a, 00) = (ab + \bar{0} + \bar{0}, 0) = (ab, 0)$

Hence f is a homomorphism of R into $R \times \mathbb{Z}$.

Now $f(a) = f(b) \Longrightarrow (a, 0) = (b, 0) \Longrightarrow a = b$

$\therefore$ f is one-one, i.e. f is a monomorphism of R into $R \times \mathbb{Z}$. Hence R is embeddable in $R \times \mathbb{Z}$.

Let us now discuss the embedding of a ring in a ring of endomorphism of some abelian group. Let $End(G)$ denote the set of all endomorphisms of an abelian group $(G,+)$. In unit 6, we have seen that $End(G)$ is a ring under the addition and multiplication defined by

$$(f \oplus g)(x) = f(x) + g(x) \text{ for all } x \in G$$

and $$(f \odot g)(x) = f\{g(x)\} \text{ for all } x \in G$$

For the sake of convenience we shall write $f + g$ for $f \oplus g$ and fg for $f \odot g$.

You will observe that $End(G)$ is a ring with unity I, where $I: G \longrightarrow G$ is the identity mapping given by $I(x) = x \; \forall x \in G$. We shall show that a ring R is embeddable in some $End(G)$.

Proposition Every ring$(R,+,.)$ with unity can be embedded in a ring of endomorphisms of the additive abelian group $(R,+)$.

Proof Let us denote the additive group $(R,+)$ by R^+. The ring of endomorphisms of R^+ is $End(R^+)$. Define $f: R \longrightarrow End(R^+)$ by $f(r) = \varphi_r \; \forall r \in R$ such that $\varphi_r: R^+ \longrightarrow R^+$ is given by $\varphi_r(a) = ra \; \forall a \in R^+$. Obviously, $ra \in R^+$ and

$$\varphi_r(a+b) = r(a+b) = ra + rb = \varphi_r(a) + \varphi_r(b) \text{ for all } a, b \in R^+$$

Hence φ_r is an endomorphism of R^+, i.e. $\varphi_r \in End(R^+)$. Therefore the mapping f is justified.

To prove that f is a homomorphism, let $r, s \in R$. Then for all $a \in R^+$, we have

$$\begin{aligned} \varphi_{r+s}(a) &= (r+s)a \\ &= ra + sa \\ &= \varphi_r(a) + \varphi_s(a) \\ &= (\varphi_r + \varphi_s)(a) \end{aligned}$$

$$\Longrightarrow \varphi_{r+s} = \varphi_r + \varphi_s$$

Therefore

$$f(r+s) = \varphi_{r+s} = \varphi_r + \varphi_s = f(r) + f(s)$$

Also for all $a \in R^+$, we have

$$\varphi_{rs}(a) = (rs)a = r(sa) = \varphi_r(sa) = \varphi_r\{\varphi_s(a)\} = (\varphi_r\varphi_s)(a)$$

$$\Longrightarrow \varphi_{rs} = \varphi_r\varphi_s$$

Therefore $f(rs) = \varphi_{rs} = \varphi_r\varphi_s = f(r)f(s)$

Hence f is a homomorphism of R into $End(R^+)$.

Finally, $f(r) = f(s) \Longrightarrow \varphi_r = \varphi_s$

$$\begin{aligned} &\Longrightarrow \varphi_r(a) = \varphi_s(a) \text{ for all } a \in R^+ \\ &\Longrightarrow ra = sa \text{ for all } a \in R^+ \\ &\Longrightarrow r1 = s1 \text{ as } 1 \in R^+ \text{ since } 1 \in R \\ &\Longrightarrow r = s \end{aligned}$$

Thus f is one-one and so f is a monomorphism of R into $End(R^+)$, i.e.

$$R \cong f(R) \subseteq End(R^+)$$

Consequently R is embeddable in $End(R^+)$.

Corollary Every ring can be embedded in a ring of endomorphism of some additive group.

Proof We know that a ring R can be embedded in a ring $R'(= R \times \mathbb{Z})$ with unity and there exists a monomorphism $f: R \longrightarrow R'$ such that $f(a) = (a, 0) \; \forall a \in R$. Let us denote the additive abelian group $(R',+)$ by R'^+. Then by above proposition, the ring R' with unity can be embedded in a ring of endomorphism of the additive group $R'^+$and there exists a monomorphism $g: R' \longrightarrow End(R'^+)$ such that $g(r) = \varphi_r \; \forall r \in R'$. Then the composition map $gf: R \longrightarrow End(R'^+)$ given by $(gf)(a) = g\{f(a)\} \; \forall a \in R$ is a homomorphism. Since f and g both are one-one, hence gf is also one-one, i.e. gf is a monomorphism of R into $End(R'^+)$. Hence $R \cong gf(R) \subseteq End(R'^+)$. Thus R is embeddable in $End(R'^+)$.

Note: Some authors use the notation $Hom(R^+, R^+)$ for $End(R^+)$.

7.9 The field of quotients (fractions) of an integral domain

In this section we shall discuss how an integral domain can be embedded in a field. Suppose we are given an integral domain. You may ask, is it possible to construct a field embedding this integral domain as a subring? In other words, is it possible to extend an integral domain to a field?

We know that in a field every non-zero element is invertible however in an integral domain it is not always the case. For example, in $\mathbb{Z}$ the elements are not invertible. That means the equation $ax = b,\ a \neq 0$ with integer coefficients does not have solution in $\mathbb{Z}$. But the equation has a solution in the field $\mathbb{Q}$ of rational numbers. So at least in this case it appears that we can construct $\mathbb{Q}$ such that $\mathbb{Z}$ can be embedded into it. Now you will see that we can always embed an integral domain in a field.

Theorem Every integral domain can be embedded in a field.

Proof Let D be an integral domain with at least two elements and let $D_0 = D - \{0\}$. Then $D \times D_0 = \{(a, b): a, b \in D, b \neq 0\}$.

The proof consists of three parts. First we shall define a relation '$\sim$' on $D \times D_0$ such that $(a, b) \sim (c, d)$ if and only if $ad = bc$. We shall show that '$\sim$' is an equivalence on $D \times D_0$. Next we shall construct a family F of all equivalence classes and define addition and multiplication in it such that F becomes field. Finally, we shall prove that D can be embedded in F.

Let us first show that the relation '$\sim$' on $D \times D_0$ as defined above is an equivalence relation.

Reflexivity: Since D is an integral domain, hence $ab = ba$ for all $a, b \in D$. Therefore by definition of '$\sim$' we have

$$(a, b) \sim (a, b) \text{ for all } (a, b) \in D \times D_0$$

Symmetry: $(a, b) \sim (c, d) \Rightarrow ad = bc$

$$\Rightarrow cb = da$$
$$\Rightarrow (c, d) \sim (a, b)$$

Transitivity: $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$

$\Rightarrow ad = bc$ and $cf = de$

$\Rightarrow adf = bcf$ and $bcf = bde$

$\Rightarrow adf = bde$

$\Rightarrow afd = bed$ as D is commutative

$\Rightarrow af = be$ as $d \neq 0$ and cancellation law holds in D_0

$\Rightarrow (a, b) \sim (e, f)$

Hence '$\sim$' is an equivalence relation on $D \times D_0$. This relation decomposes $D \times D_0$ into disjoint equivalence classes. Let us denote the equivalence class of (a, b) by a/b. Hence

$$a/b = \{(c, d) \in D \times D_0 : (c, d) \sim (a, b)\}$$

Obviously $a/b = c/d$ if and only if $(a, b) \sim (c, d)$, i.e. $ad = bc$

Let F be the family of all equivalence classes a/b of $D \times D_0$, i.e.

$$F = \{a/b : (c, d) \in D \times D_0\}$$

Let us define addition and multiplication in F as follows:

$$a/b + c/d = (ad + bc)/bd$$
$$(a/b)(c/d) = ac/bd$$

You will observe that theses operations are inspired by addition and multiplication of rational numbers.

Since D is an integral domain, $b \neq 0, d \neq 0 \Longrightarrow bd \neq 0$. Hence $(ad + bc)/bd$ and $ac/bd \in F$. Now we shall show that these operations are well defined, i.e. they are independent of the representation of equivalence classes. Hence we show that if $a/b = a'/b'$and $c/d = c'/d'$ then $a/b + c/d = a'/b' + c'/d'$ and $(a/b)(c/d) = (a'/b')(c'/d')$.

We have $a/b = a'/b'$and $c/d = c'/d'$

$$\Longrightarrow ab' = ba' \text{ and } cd' = dc'$$
$$\Longrightarrow ab'dd' = ba'dd' \text{ and } bb'cd' = bb'dc'$$
$$\Longrightarrow ab'dd' + bb'cd' = ba'dd' + bb'dc'$$
$$\Longrightarrow adb'd' + bcb'd' = bda'd' + bdb'c' \text{ as } D \text{ is commutative}$$
$$\Longrightarrow (ad + bc)b'd' = bd(a'd' + b'c')$$
$$\Longrightarrow (ad + bc)/bd = (a'd' + b'c')/b'd'$$
$$\Longrightarrow a/b + c/d = a'/b' + c'/d'$$

Also $a/b = a'/b'$and $c/d = c'/d'$

$$\Longrightarrow ab' = ba' \text{ and } cd' = dc'$$
$$\Longrightarrow ab'cd' = ba'dc'$$
$$\Longrightarrow (ac)(b'd') = (bd)(a'c')$$
$$\Longrightarrow ac/bd = a'c'/b'd'$$
$$\Longrightarrow ac/bd = a'c'/b'd'$$
$$\Longrightarrow (a/b)(c/d) = (a'/b')(c'/d')$$

You will observe that if $a \in D_0$, then $0/a \neq a/a$ as $0a \neq aa$. Hence $0/a$ and a/a are two distinct elements of F, i.e. F has at least two elements. Also we have $0/a = 0/b$ for all $a, b \in D_0$ and $ac/bc = a/b$ for any $c \in D_0$.

Now we shall show that F is a field under the addition and multiplication defined above.

(1) *Associativity of addition*: For all $a/b\,, c/d\,, e/f \in F$, we have

$$\begin{aligned} a/b + (c/d + e/f) &= a/b + (cf + de)/df \\ &= \{a(df) + b(cf + de)\}/b(df) \\ &= \{(ad + bc)f + (bd)e\}/(bd)f \\ &= (ad + bc)/bd + e/f \\ &= (a/b + c/d) + e/f \end{aligned}$$

(2) *Commutativity of addition*: For all $a/b\,, c/d \in F$, we have

$$\begin{aligned} a/b + c/d &= (ad + bc)/bd \\ &= (cb + da)/db \\ &= c/d + a/b \end{aligned}$$

(3) *Existence of zero element*: We have $0/a \in F$ for $0 \neq a \in D$ such that

$$0/a + c/d = (0d + ac)/ad = (0 + ac)/ad = ac/ad = c/d$$

Hence $0/a$ is the zero element of F. Also if $0 \neq b \in D$, then

$$0/a = 0/b \text{ as } 0b = a0$$

Let us denote $0/a$ (or $0/b$) by 0.

(4) *Existence of additive inverse*: If $a/b \in F$, then $(-a)/b \in F$ such that

$$a/b + (-a)/b = \{ab + b(-a)\}/bb = (ab - ba)/b^2 = 0/b^2$$

Since $0/b^2 = 0$, hence $a/b + (-a)/b = 0$. Therefore

$$-(a/b) = (-a)/b \in F$$

(5) *Associativity of multiplication*: For all $a/b\,, c/d\,, e/f \in F$, we have

$$[(a/b)(c/d)](e/f) = (ac/bd)(e/f) = (ac)e/(bd)f$$

$$= a\,(ce)/b(df) = (a/b)(ce/df) = (a/b)[(c/d)(e/f)]$$

(6) *Commutativity of multiplication*: For all $a/b\,, c/d \in F$, we have

$$(a/b)(c/d) = ac/bd = ca/db = (c/d)(a/b)$$

(7) *Existence of unity*: Let $0 \neq a \in D$, then $a/a \in F$ such that

$$(a/a)(c/d) = ac/ad = c/d$$

Also

$$(c/d)(a/a) = ca/da = c/d$$

Hence $a/a \in F$ is the multiplicative identity, i.e. unity for F. Let us denote it by 1.

(8) *Existence of multiplicative inverse of non-zero elements*: Let $0 \neq a/b \in F$. Now $a/b \neq 0 \Longrightarrow a \neq 0, b \neq 0 \Longrightarrow b/a \neq 0$ and

$$(a/b)(b/a) = ab/ba = ab/ab = a/a = 1$$

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

(9) *Distributivity*: For all $a/b\,, c/d\,, e/f \in F$, we have

$$(a/b)[(c/d) + (e/f)] = (a/b)(cf + de/df) = a(cf + de)/b(df)$$
$$= (acf + ade)/(bdf) = (acf + ade)b/(bdf)b$$
$$= (acfb + adeb)/bdfb = \{(ac)(bf) + (ae)(bd)\}/(bd)(bf)$$
$$= (ac/bd) + (ae/bf) = (a/b)(c/d) + (a/b)(e/f)$$

Hence $(F, +, .)$ is a field.

Now we shall show that D can be embedded in F. Define $\varphi: D \longrightarrow F$ by

$$\varphi(x) = xa/a \;\; \forall x \in D \text{ where } 0 \neq a \in D$$

Then for $x, y \in D$, we have

$$\varphi(x) = \varphi(y) \Longrightarrow xa/a = ya/a$$
$$\Longrightarrow xaa = aya$$
$$\Longrightarrow xa^2 = ya^2$$
$$\Longrightarrow xa^2 - ya^2 = 0$$
$$\Longrightarrow (x - y)a^2 = 0$$
$$\Longrightarrow x - y = 0, \text{ as } a^2 \neq 0$$
$$\Longrightarrow x = y$$

Hence φ is one-one.

Also $\varphi(x + y) = (x + y)a/a = (x + y)a^2/a^2 = (xa^2 + ya^2)/a^2$
$$= (xaa + aya)/aa = (xa/a) + (ya/a) = \varphi(x) + \varphi(y)$$

and $\varphi(xy) = (xy)a/a = (xy)a^2/a^2 = (xa)(ya)/aa$
$$= (xa/a)(ya/a) = \varphi(x)\varphi(y)$$

Thus φ is a monomorphism of D into F. Hence $D \cong \varphi(D) \subseteq F$, i.e. D can be embedded in a field F.

This field F is called the **field of quotients** or the field of fractions of D.

Let $x/y \in F$. Then $x, y \in D$ and $y \neq 0$ and

$$x/y = xaa/aya = (xa/a)(a/ya) = (xa/a)(ya/a)^{-1} = \varphi(x)[\varphi(y)]^{-1}$$

So we have the following definition:

Definition Let D be an integral domain with more than one element. A **field of quotients (or field of fractions)** of D is a pair (F, φ) consisting of a field F and a monomorphism $\varphi: D \longrightarrow F$ such that every element $u = x/y$ of F is expressible as $\varphi(x)[\varphi(y)]^{-1}$ for some $x, y \in D$ with $y \neq 0$.

Proposition Let D be an integral domain and (F, φ) be its field of fraction. Let K be a field and ψ be an injective homomorphism from D to K.Then there exists unique homomorphism f from F to K such that $fo\varphi = \psi$.

Proof Since $D \cong \psi(D) \subseteq K$, hence the field K contains an isomorphic copy of the integral domain D. Now ψ is injective, therefore $\psi(y) \neq 0$ whenever $y \neq 0$. Let us define a map $f: F \longrightarrow K$ by

$$f(x/y) = \psi(x)[\psi(y)]^{-1} \text{ for all } x, y \in D \text{ and } y \neq 0$$

Then the mapping is well defined as

$$\begin{aligned} x/y = u/v &\Longrightarrow xv = yu \\ &\Longrightarrow \psi(xv) = \psi(yu) \\ &\Longrightarrow \psi(x)\psi(v) = \psi(y)\psi(u) \\ &\Longrightarrow \psi(x)[\psi(y)]^{-1} = \psi(u)[\psi(v)]^{-1} \\ &\Longrightarrow f(x/y) = f(u/v) \end{aligned}$$

$$\begin{aligned} \text{Now } f(x/y + u/v) &= f(xv + yu/yv) = \psi(xv + yu)[\psi(yv)]^{-1} \\ &= [\psi(xv) + \psi(yu)][\psi(y)\psi(v)]^{-1} \\ &= [\psi(x)\psi(v) + \psi(y)\psi(u)][\psi(v)]^{-1}[\psi(y)]^{-1} \\ &= \psi(x)[\psi(y)]^{-1} + \psi(u)[\psi(v)]^{-1} \\ &= f(x/y) + f(u/v) \end{aligned}$$

$$\begin{aligned} \text{and } f[(x/y)(u/v)] &= f(xu/yv) = \psi(xu)[\psi(yv)]^{-1} \\ &= \psi(x)\psi(u)[\psi(v)]^{-1}[\psi(y)]^{-1} \\ &= \psi(x)[\psi(y)]^{-1}\psi(u)[\psi(v)]^{-1} \\ &= f(x/y)\, f(u/v) \end{aligned}$$

Hence f is a homomorphism.

Now if $f(x/y) = 0 \Longrightarrow \psi(x)[\psi(y)]^{-1} = 0 \Longrightarrow \psi(x) = 0\psi(y) = 0$

Since ψ is an injective homomorphism, hence $\psi(x) = 0 \Longrightarrow x = 0$

Thus $x/y = 0/y = 0$. Hence $f(x/y) = 0 \Longrightarrow x/y = 0$. Therefore $\text{Ker} f = \{0\}$, i.e. f is injective.

Now (F, φ) is the field of fractions of D, hence $f: F \longrightarrow K$ is an injective homomorphism such that $fo\varphi = \psi$. Also $\varphi(D)$ generates the field F as $x/y \in F \Longrightarrow x/y = \varphi(x)[\varphi(y)]^{-1}$. Thus if $f': F \longrightarrow K$ is some other injective homomorphism such that $f'o\varphi = \psi$, then $f' = f$.

It is clear from above result that any field K containing an isomorphic copy of integral domain D must also contain an isomorphic copy of the field of fractions F. Since the injective homomorphism $f: F \longrightarrow K$ is unique, this establishes the uniqueness of the field of fractions.

Note: Since $D \cong \varphi(D)$, we can identify D with $\varphi(D)$. Hence $\varphi(x)$ and $\varphi(y)$can be identified as x and y. Therefore any element x/y of F can be expressed as xy^{-1}. In this case, D is itself regarded as a subring of F.

In view of above result we can say that if K is any field containing an integral domain D, then K contains a subfield isomorphic to the field of fractions F of D. In other words, the field of fractions F of an integral domain D is the smallest field containing D.

Proposition The fields of fractions of isomorphic integral domains are isomorphic.

Proof Let D_1 and D_2 be two isomorphic integral domains and $f: D_1 \longrightarrow D_2$ be the isomorphism. Let F_1 and F_2be the fields of fractions of D_1 and D_2 respectively. Define a mapping$\varphi: F_1 \longrightarrow F_2$by $\varphi(x/y) = f(x)/f(y)$ where $x, y \in D_1$ and $y \neq 0$. Obviously $f(y) \neq 0$.

Let $f(x)/f(y) \in F_2$, then $f(x), f(y) \in D_2$ and $f(y) \neq 0$. Since f is an isomorphism, hence $x, y \in D_1$ and $y \neq 0$. This implies that $x/y \in F_1$ and $\varphi(x/y) = f(x)/f(y)$. Therefore φ is onto.

$$\begin{aligned} \text{Now } \varphi(x/y) = \varphi(u/v) &\Longrightarrow f(x)/f(y) = f(u)/f(v) \\ &\Longrightarrow f(x)f(v) = f(y)f(u) \\ &\Longrightarrow f(xv) = f(yu) \\ &\Longrightarrow xv = yu \text{ as } f \text{ is one-one} \end{aligned}$$

$$\Longrightarrow x/y = u/v$$

Hence φ is one-one.

Also $\varphi(x/y + u/v) = \varphi(xv + yu/yv) = f(xv + yu)/f(yv)$

$$= \{f(xv) + f(yu)\}/f(y)f(v) = \{f(x)f(v) + f(y)f(u)\}/f(y)f(v)$$

$$= f(x)/f(y) + f(u)/f(v) = \varphi(x/y) + \varphi(u/v)$$

Similarly, you can check that $\varphi[(x/y)(u/v)] = \varphi(x/y)\varphi(u/v)$

Therefore φ is an isomorphism, i.e. $F_1 \cong F_2$.

Examples

(1) If F is a field then its field of fractions is F itself.

(2) The field of fractions of the integral domain $\mathbb{Z}$ is the field $\mathbb{Q}$ of rational numbers.

(3) The field of fraction of the integral domain $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is the field $\mathbb{Q}[\sqrt{2}\,] = \{x + y\sqrt{2} : x, y \in \mathbb{Q}\}$.

7.10 Summary

In this unit, we have

(1) Defined the Characteristic of an integral domain and proved that the characteristic of an integral domain is either zero or a prime number.

(2) Defined and illustrated the homomorphism and isomorphism of rings and discussed their properties.

(3) Defined kernel of a homomorphism and proved that the kernel of a homomorphism f is an ideal.

(4) Proved results concerning the direct and inverse images of subring and subfield.

(5) Discussed embedding of rings and proved that every ring can be embedded in a ring with unity.

(6) Proved that every ring can be embedded in a ring of endomorphism of some additive group.

(7) Discussed the embedding of an integral domain in a field and defined the field of fractions of an integral domain. We also showed that the field of fractions F of an integral domain D is the smallest field containing D.

7.11 Self assessment questions

(1) Let f be a non-zero ring homomorphism from an integral domain D_1 of characteristic p to an integral domain D_2. Show that the characteristic of D_2 is also p.

(2) Show that the field $\mathbb{R}$ of real numbers is not isomorphic to the field $\mathbb{C}$ of complex numbers.

(3) Let F be a field of characteristic $p \neq 0$. Show that there is an injective homomorphism from $\mathbb{Z}_p$ to F.

(4) Let R be a ring and $M = \left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in R\right\}$. Show that M is a ring under addition and multipliacation of matrices and $f: M \longrightarrow R$ given by $f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) = a$ for all $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in M$ is an isomorphism.

(5) If f is a homomorphism from a ring R into a ring S and g is a homomorphism from S into a ring T, show that gof is a homomorphism from R into T.

(6) Show that $f: \mathbb{C} \longrightarrow M_2(\mathbb{R})$ given by $f(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a monomorphism.

(7) Let $\mathbb{Z}^+$ denotes the additive abelian group $(\mathbb{Z}, +)$. Show that

$$End(\mathbb{Z}^+) \cong (\mathbb{Z}, +, .)$$

(8) Determine the field of quotient of the integral domain containing rational numbers of the form of $m/10^n$, $(m, n \in \mathbb{Z})$. [Ans. $\mathbb{Q}$]

7.12 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

(6) Lang, S. (1965): Algebra, Reading, Massachusetts, Addison-Wesley.

(7) Barshay, J. (1969): Topics in ring theory, N.Y., W.A. Benjamin Inc.

(8) Burtan, D. M. (1968): A first course in Rings and Ideals, Reading, MA., Addison-Wesley.

Unit-8: Ideals

Structure

8.1 Introduction

In unit 7, we introduced the notion of an ideal of a ring R. Recall that a non-empty subset A of a ring R is called an ideal if

$a, b \in A \Longrightarrow a - b \in A$ and $a \in A, r \in R \Longrightarrow ar \in A$ and $ra \in A$

In this unit, we shall see how the notion of an ideal is evolved by defining an equivalence relation on the elements of a ring. You have studied similar equivalence relation on a group in unit 3.

The ideals are similar to normal subgroups you studied in group theory. You have seen that a quotient group is defined as a group of cosets of a given normal subgroup. Since a ring $(R, +, \cdot)$ is an abelian additive group and an ideal I of R is an additive subgroup of R, hence I is normal in R and R/I is a quotient group. The addition in R/I is defined as follows:

$(a + I) + (b + I) = (a + b) + I$ for all $a, b \in R$

We then require multiplication composition to be defined on R/I in order to make it a ring. So we define multiplication composition on R/I as follows:

$(a + I)(b + I) = ab + I$ for all $a, b \in R$

You will see that R/I is indeed a ring under these two compositions. This ring is called a quotient ring of R modulo I.

The construction of quotient ring together with the concept of homomorphism naturally leads you to the fundamental theorem of homomorphism. This theorem is similar to that you have proved for groups, i.e. every homomorphic image of a group is isomorphic to a quotient group. So we shall prove the theorem for rings and discuss its consequences. Then we shall discuss some special ideals namely the principal ideals, prime ideals and maximal ideals.

Let us first discuss the objectives of this unit-

8.2 Objectives

After reading this unit, you should be able to

- Define left ideal, right ideal and ideal of a ring.
- Discuss different properties of ideals.
- Define quotient rings with example.
- Prove the Fundamental theorem of homomorphism for rings and some isomorphism theorems.
- Define and discuss principal ideals, prime ideals and maximal ideals with examples.

8.3 Ideals

Let us see what concepts really motivate the definition of an ideal. In unit 6, we have defined subrings analogous to subgroups in group theory. Following this analogy further, we can define equivalence relations on the elements of a ring R as follows:

Let S be a subring of a ring R. Let $a, b \in R$. Then a is said to be **left congruent to b modulo S** if and only if $a - b \in S$ and $x(a-b) \in S$ for all $x \in R$. Symbolically

$a \equiv_l b \pmod{S}$ if and only if $a - b \in S$ and $x(a-b) \in S$ for all $x \in R$

and a is said to be **right congruent to b modulo S** if and only if $a - b \in S$ and $(a-b)x \in S$ for all $x \in R$.Symbolically

$a \equiv_r b \pmod{S}$ if and only if $a - b \in S$ and $(a-b)x \in S$ for all $x \in R$

The element a is said to be **congruent to b modulo S** if a is both right and left congruent to b modulo S and then we write $a \equiv b \pmod{S}$. Now we shall prove that $\equiv_r$ and $\equiv_l$ are equivalence relations on R. Let us first consider the relation $\equiv_r$. Let $a, b, c \in R$.

Reflexivity: For all $a \in R$, we have $a - a = 0 \in S$ and $(a-a)x = 0 \in S$ for all $x \in R$. Hence $a \equiv_r a \pmod{S}$ for all $a \in R$

Symmetry: $a \equiv_r b \pmod{S} \Rightarrow a - b \in S$ and $(a-b)x \in S$ for all $x \in R$

$\Rightarrow b - a = -(a-b) \in S$ and $(b-a)x = -(a-b)x \in S$ for all $x \in R$

$\Rightarrow b \equiv_r a \pmod{S}$

Transitivity: $a \equiv_r b \pmod{S}$, $b \equiv_r c \pmod{S} \Rightarrow a - b \in S$, $b - c \in S$ and $(a-b)x \in S$, $(b-c)x \in S$ for all $x \in R$.

Since S is a subring, hence $a - b \in S, b - c \in S \Rightarrow (a-b) + (b-c) \in S$

$$\Rightarrow a - c \in S$$

Also $(a-b)x \in S$, $(b-c)x \in S \Rightarrow (a-b)x + (b-c)x \in S$

$$\Rightarrow (a-c)x \in S$$

Therefore $a \equiv_r c \pmod{S}$. Hence $\equiv_r$ is an equivalence relation on R. Similarly you can verify that $\equiv_l$ and hence the relation of congruence modulo S is an equivalence relation on the ring R. These equivalence relations partition the ring into equivalence classes which motivates the definition of some important objects in ring theory called the ideals. Let us first discuss the equivalence classes for the relation $\equiv_r$.

Let $x \in R$. We define a subset $x + S$ as follows:

$$x + S = \{x + s : s \in S\}$$

We shall show that if S is a subring of R such that $a \in S, y \in R \Rightarrow ay \in S$ then the equivalence class of $x \in R$ under the relation $\equiv_r$is $x + S$.

The equivalence class of $x \in R$ under $\equiv_r$ is given by

$$[x]_r = \{z \in R : z \equiv_r x (\text{mod } S)\}$$

Let $y \in [x]_r$. Then $y \equiv_r x (\text{mod } S) \Rightarrow y - x \in S \Rightarrow y \in S + x \Rightarrow y \in x + S$ as $S + x = x + S$. Thus $y \in [x]_r \Rightarrow y \in x + S$. Hence $[x]_r \subseteq x + S$.

Again $u \in x + S \Rightarrow u - x \in S$. Now by our hypothesis

$$u - x \in S, y \in R \Rightarrow (u - x)y \in S$$
$$\Rightarrow u \equiv_r x (\text{mod } S)$$
$$\Rightarrow u \in [x]_r$$

This gives $x + S \subseteq [x]_r$. Hence $[x]_r = x + S$.

You can verify that the converse is also true, i.e. if $[x]_r = x + S$ for all $x \in R$, then $ay \in S$ for all $a \in S, y \in R$. Similarly, if $[x]_l$ is the equivalence class of $x \in R$ under $\equiv_l$, then you can show that if S is a subring of R such that $a \in S, y \in R \Rightarrow ya \in S$ then $[x]_l = x + S$ and conversely.

Also if S is a subring of R such that for all $a \in S, y \in R \Rightarrow ya \in S, ay \in S$ then for every $x \in R$ the equivalence class $[x]$ under the relation congruence modulo S is equal to $x + S$, i.e. $[x] = x + S = S + x$ and conversely.

All this stuff motivates us to define an ideal of a ring.

Definition Let R be a ring and I be a non-empty subset of R. Then

(i) I is called a **left ideal** of R if I is a subring of R and $rI \subseteq I$ for all $r \in R$.

i.e. $a, b \in I \Rightarrow a - b \in I$ and $a \in I, r \in R \Rightarrow ra \in I$

(ii) I is called a **right ideal** of R if I is a subring of R and $Ir \subseteq I$ for all $r \in R$.

i.e. $a, b \in I \Rightarrow a - b \in I$ and $a \in I, r \in R \Rightarrow ar \in I$

(iii) I is called an **ideal (**or **two-sided ideal)** of R if I is both left and right ideal of R, i.e. $a, b \in I \Rightarrow a - b \in I$ and $a \in I, r \in R \Rightarrow ra \in I$ and $ar \in I$

Thus we can say that a non-empty subset $I$of a ring R is said to be an ideal of R if $(I, +)$ is a subgroup of the additive group $(R, +)$ and $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.

Here you will notice that every subring is not an ideal as an ideal has a stronger closure property than a subring, i.e. an ideal I is closed (under multiplication) not just by elements of I but by all the elements of R.

Also it is obvious that for commutative rings left, right and two-sided ideal are all identical.

Examples

(1) R and $\{0\}$ are ideals of any ring R. The ideal $\{0\}$ is called the *trivial ideal* and the ideal R is called *improper* ideal.

(2) For any positive integer n, the set $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
Let $x, y \in n\mathbb{Z}$. Then $x = na, y = nb$ for some $a, b \in \mathbb{Z}$. Now
$x - y = na - nb = n(a - b) \in n\mathbb{Z}$ as $a - b \in \mathbb{Z}$
Let $r \in \mathbb{Z}$ and $x \in n\mathbb{Z}$ then $rx = r(na) = n(ra) \in n\mathbb{Z}$,by the commutativity and associativity of multiplication in $\mathbb{Z}$.
Similarly, $xr = (na)r = n(ar) \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(3) $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Since $2/3 \in \mathbb{Q}$, $5 \in \mathbb{Z}$ but $(2/3)5 = 10/3 \notin \mathbb{Z}$.

(4) Let R be a ring. You can verify that the subring $I = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in R\right\}$ of $M_2(R)$ is a right ideal but not a left ideal.
Since $0 \in R$, hence $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$. Thus I is non-empty. Let $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in I$.

Then $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in I$

If $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(R)$, then $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ 0 & 0 \end{bmatrix} \in I$

Hence I is a right ideal of $M_2(R)$. But I is not a left ideal of $M_2(R)$, since for non-zero elements a, b, r of R such that $ra \neq 0$ and $rb \neq 0$, we have

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} pa & pb \\ ra & rb \end{bmatrix} \notin I$$

Similarly you can verify that $\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in R\right\}$ is a left ideal but not a right ideal of $M_2(R)$ and $\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a, b \in R\right\}$ is neither a left ideal nor a right ideal of $M_2(R)$.

Let us discuss some results concerning ideals.

Proposition Let R be a ring and $a \in R$. Then $Ra = \{ra : r \in R\}$ is a left ideal of R.

Proof Let $r_1a, r_2a \in Ra$ where $r_1, r_2 \in R$. Then

$$r_1a - r_2a = (r_1 - r_2)a \in Ra \text{ as } r_1 - r_2 \in R$$

Also for $r \in R$, we have

$$r(r_1a) = (rr_1)a \in R \text{ as } rr_1 \in R$$

Hence Ra is a left ideal of R.

Proposition A commutative ring R with unity is a field if and only if its only ideals are $\{0\}$ and R.

Proof First suppose that the only ideals of R are $\{0\}$ and R. In order to show that R is a field, we have to show that every non-zero element of R is a unit. Let $0 \neq a \in R$. Then by above proposition, the set Ra is a left ideal of R. Since R is commutative, it is also a right ideal of R. Thus Ra is an ideal of R. Now $1 \in R$, hence $1a = a \in Ra$. Therefore $Ra \neq \{0\}$. Hence we have $Ra = R$. Now

$1 \in R \Longrightarrow 1 \in Ra$. That means there exists an element $b \in R$ such that $ba = 1$, i.e. a is a unit. Thus R is a field.

Conversely, suppose that R is a field. Let A be a nontrivial ideal of R, $A \neq \{0\}$. Let $a \in A$. Then $a \in R$. Since every element of R is a unit, hence there exists $b \in R$ such that $ab = 1$. Now A is an ideal, hence

$$a \in A, b \in R \Longrightarrow ab \in A \Longrightarrow 1 \in A$$

Let r be any element of R. Then

$$1 \in A, r \in R \Longrightarrow 1r \in A \Longrightarrow r \in A$$

Thus A contains every element of R, i.e. $A = R$. Therefore the only ideals of R are $\{0\}$ and R.

Definition A ring R is said to be **simple** if it has no proper nontrivial ideals, i.e. its only ideals are $\{0\}$ and R.

Example $M_2(\mathbb{Q})$ is a simple ring.

Solution Let E_{ij} denote the 2×2 matrix whose $(i,j)^{th}$ element is 1 and all other elements are zero. Then $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. Obviously $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E_{11} + E_{22}$.

Let Γ be an ideal of $M_2(\mathbb{Q})$ such that $\Gamma \neq \{0\}$. Then there exists a matrix $A \in \Gamma$ such that $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. By the theory of matrices we know that there exist non-singular matrices P and Q in $M_2(\mathbb{Q})$ such that

$$PAQ = \begin{cases} I \text{ if the rank of } A \text{ is } 2 \\ E_{11} \text{ if the rank of } A \text{ is } 1 \end{cases}$$

Since Γ is an ideal, hence

$$P \in M_2(\mathbb{Q}), A \in \Gamma \Longrightarrow PA \in \Gamma$$

Therefore $Q \in M_2(\mathbb{Q}), PA \in \Gamma \Longrightarrow PAQ \in \Gamma$

Hence either $PAQ = I \in \Gamma$ or $PAQ = E_{11} \in \Gamma$.

If $I \in \Gamma$, then $I \in \Gamma, N \in M_2(\mathbb{Q}) \Longrightarrow IN = N \in \Gamma$, i.e. $\Gamma = M_2(\mathbb{Q})$.

If $E_{11} \in \Gamma$, then $E_{21}E_{11}E_{11}E_{12} = E_{22} \in \Gamma$ as Γ is an ideal of $M_2(\mathbb{Q})$.

Now $E_{11} \in \Gamma, E_{22} \in \Gamma \Longrightarrow E_{11} + E_{22} \in \Gamma \Longrightarrow I \in \Gamma$ as $E_{11} + E_{22} = I$. Then again we have $\Gamma = M_2(\mathbb{Q})$. Therefore $M_2(\mathbb{Q})$ is simple.

Proposition A division ring is a simple ring

Proof We shall show that a division ring has no proper nontrivial ideals. Let A be a nontrivial ideal of a division ring R, i.e. $A \neq \{0\}$. Let $0 \neq a \in A$. Since R is a division ring, a must be a unit in R. Therefore there exists $b \in R$ such that $ab = 1$. Now $a \in A,\ b \in R \Longrightarrow ab \in A \Longrightarrow 1 \in A$. Also $1 \in A,\ r \in R \Longrightarrow 1r = r \in A$. Thus $A = R$. Hence R has no proper nontrivial ideals, i.e. R is simple.

Now we shall discuss some properties of ideals.

8.4 Some properties of ideals

Proposition Intersection of two right (left) ideals of a ring R is a right (left) ideal of R.

Proof Let A and B be any two right ideals of a ring R. Since $0 \in A$ and $0 \in B$, hence $0 \in A \cap B$. Thus $A \cap B$ is nonempty. Let $x, y \in A \cap B$. Then $x, y \in A$ and $x, y \in B$. Now A and B are right ideals, hence $x, y \in A \Longrightarrow x - y \in A$ and $x, y \in B \Longrightarrow x - y \in B$.Therefore $x - y \in A \cap B$.

Also $r \in R$ and $x \in A \Longrightarrow xr \in A$ and $r \in R$ and $x \in B \Longrightarrow xr \in B$. Therefore $xr \in A \cap B$.Thus we have shown that

$$x, y \in A \cap B, r \in R \Longrightarrow x - y \in A \cap B \text{and } xr \in A \cap B$$

Therefore $A \cap B$ is a right ideal of R. Similarly we can show that the intersection of two left ideals of a ring is also a left ideal.

Proposition Intersection of any non-empty family of right (left) ideals of a ring R is a right (left) ideal of R.

Proof Let $\{A_t : t \in \Lambda\}$ be a non-empty family of right ideals of a ring R. Since $0 \in A_t\ \forall t \in \Lambda$, hence $0 \in \bigcap_{t\in\Lambda} A_t$. Therefore $\bigcap_{t\in\Lambda} A_t$ is non-empty. Let $x, y \in \bigcap_{t\in\Lambda} A_t$. Then $x, y \in A_t\ \forall t \in \Lambda$. Since A_t is an ideal for all $t \in \Lambda$, hence

$$x, y \in A_t \Longrightarrow x - y \in A_t \text{ for all } t \in \Lambda$$
$$\Longrightarrow x - y \in \bigcap_{t\in\Lambda} A_t$$

Also $x \in A_t, r \in R \Longrightarrow xr \in A_t \quad \forall t \in \Lambda$

$$\Longrightarrow xr \in \bigcap_{t\in\Lambda} A_t$$

Hence $\bigcap_{t\in\Lambda} A_t$ is a right ideal of R. Similar proof can be given for left ideals.

Now what do you say about the union of two ideals? For example, $4\mathbb{Z}$ and $5\mathbb{Z}$ are ideals of the ring $\mathbb{Z}$ of integers. Is $4\mathbb{Z} \cup 5\mathbb{Z}$ an ideal of $\mathbb{Z}$? The answer is no. let us see how. We have $4 \in 4\mathbb{Z}$ and $5 \in 5\mathbb{Z}$, therefore $4,5 \in 4\mathbb{Z} \cup 5\mathbb{Z}$. But $5 - 4 = 1 \notin 4\mathbb{Z} \cup 5\mathbb{Z}$. Hence $4\mathbb{Z} \cup 5\mathbb{Z}$ is not an ideal of $\mathbb{Z}$. Now we prove the following result which gives the necessary and sufficient condition for a union of two ideals to be an ideal of the given ring.

Proposition Let A and B be any two ideals of a ring R. Then $A \cup B$ is an ideal of R if and only if either $A \subseteq B$ or $B \subseteq A$.

Proof First suppose that $A \subseteq B$. Then $A \cup B = B$, i.e. $A \cup B$ is an ideal of R.

If $B \subseteq A$, then $A \cup B = A$ is an ideal of R. Therefore if $A \subseteq B$ or $B \subseteq A$, then $A \cup B$ is an ideal of R.

Conversely, suppose that $A \cup B$ is an ideal of R. Assume on the contrary that A is not contained in B and B is not contained in A, i.e. $A \nsubseteq B$ and $B \nsubseteq A$. Then there exist $x \in A$ and $y \in B$ such that $x \notin B$ and $y \notin A$. Then $x, y \in A \cup B$. Since $A \cup B$ is an ideal, hence $x - y \in A \cup B$. Therefore either $x - y \in A$ or $x - y \in B$.

If $x - y \in A$, then $y = x - (x - y) \in A$. This contradicts the fact that $y \notin A$.

Similarly if $x - y \in B$, then $x = (x - y) + y \in B$. Which is against the fact that $x \notin B$. Hence our assumption is wrong. Therefore either $A \subseteq B$ or $B \subseteq A$.

Now we define the sum of two ideals as follows:

Definition Let A and B be any two ideals of a ring R. Then the sum of ideals A and B is defined as follows:

$$A + B = \{a + b : a \in A, b \in B\}$$

Proposition Let A and B be any two ideals of a ring R. Then $A + B$ is an ideal of R containing both A and B.

Proof Since $0 \in A$ and $0 \in B$, hence $0 = 0 + 0 \in A + B$. Therefore $A + B$ is nonempty. Let $x, y \in A + B$. Then $x = a + b$, $y = a' + b'$ where $a, a' \in A$ and $b, b' \in B$. Then $a - a' \in A$ and $b - b' \in B$ and we have

$$x - y = (a + b) - (a' + b') = (a - a') + (b - b') \in A + B$$

Also for $r \in R$, we have $xr = (a + b)r = ar + br \in A + B$ as $ar \in A$ and $br \in B$. Similarly, $rx = r(a + b) = ra + rb \in A + B$. Hence $A + B$ is an ideal of R.

Now $a \in A$ and $0 \in B \Longrightarrow a + 0 \in A + B$, i.e. $a \in A + B$. Thus $A \subseteq A + B$. Similarly $0 \in A$ and $b \in B \Longrightarrow b = 0 + b \in A + B$. Hence $B \subseteq A + B$.

Definition Let A and B be any two ideals of a ring R. Then the product AB of A and B is defined as the set of all those elements of R which can be written as finite sums of elements of the form ab where $a \in A$ and $b \in B$, i.e.

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_1, a_2, .., a_n \in A, b_1, b_2, .., b_n \in B\}$$

Proposition Let A and B be any two ideals of a ring R. Then the product AB is an ideal of R.

Proof Since $0 = 00 \in AB$, hence AB is nonempty. Let $x, y \in AB$ such that $x = \sum_{i=1}^{n} a_i b_i$ and $y = \sum_{j=1}^{m} a_j' b_j'$, where $a_i, a_j' \in A$, $b_i, b_j' \in B$. Then

$$\begin{aligned} x - y &= (a_1b_1 + a_2b_2 + \cdots + a_nb_n) - (a_1'b_1' + a_2'b_2' + \cdots + a_m'b_m') \\ &= a_1b_1 + a_2b_2 + \cdots + a_nb_n + (-a_1')b_1' + (-a_2')b_2' + \cdots + (-a_m')b_m' \end{aligned}$$

Since $a_j' \in A \Longrightarrow -a_j' \in A$, hence $x - y \in AB$.

Let $r \in R$. Then $rx = \sum_{i=1}^{n} r(a_ib_i) = \sum_{i=1}^{n} (ra_i)b_i \in AB$ as $ra_i \in A$ for all $i = 1,2,..,n$. Also $xr = \sum_{i=1}^{n} (a_ib_i)r = \sum_{i=1}^{n} a_i(b_ir) \in AB$ as $b_ir \in B$ for all $i = 1,2,..,n$. Hence AB is an ideal of R.

So now we can define AA as $\{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_1, a_2, .., a_n,\ b_1, b_2, .., b_n \in A\}$. We denote AA by A^2. For any positive integer n, we define $A^n = AA \ldots A$ (n times). We assume $A^1 = A$. If R is a ring with unity, then we define $A^0 = R$.

You can verify that $A^nA^m = A^{m+n}$ and $(A^n)^m = A^{nm}$ for any positive integers m, n.

Definition An ideal A of a ring R is said to be **nilpotent** if $A^n = \{0\}$ for some positive integer n.

Example Let $U_2(\mathbb{Z})$ be the ring of all 2×2 upper triangular matrices over integers. Let $A = \left\{\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z}\right\}$ be a subset of $U_2(\mathbb{Z})$. You can verify that A is an ideal of $U_2(\mathbb{Z})$. Let $\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in A$ then

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

Hence $A^2 = \{0\}$. Thus A is nilpotent.

Definition An element a of a ring R is said to be a **nilpotent** if $a^n = 0$ for some positive integer n.

Now you can verify that the collection of all nilpotent elements in a commutative ring R is an ideal.

Let R be a commutative ring. Let

$$A = \{a \in R : a^n = 0 \text{ for some positive integer n }\}$$

Obviously $0 \in A$. Let $a, b \in A$, then $a^n = 0$ and $b^m = 0$ for some positive integers n and m.

Since R is a commutative ring, hence

$$(a-b)^{n+m} = \sum_{r=0}^{n+m} (-1)^r \binom{n+m}{r} a^{n+m-r}b^r$$

When $r \leq m$, then $a^{n+m-r}b^r = a^n a^{m-r}b^r = 0$

When $r > m$, i.e. $r = m + q$ where $q = 1,2, \ldots n$, then

$$a^{n+m-r}b^r = a^{n+m-r}b^{m+q} = a^{n+m-r}b^m b^q = 0$$

Hence we have $(a-b)^{n+m} = 0 \Longrightarrow a - b \in A$

Also if $r \in R$ and $a \in A$, then $a^n = 0$ for some positive integers n and

$$(ra)^n = r^n a^n = 0$$

$$\Longrightarrow ra \in A$$

Also $ar \in A$ as R is commutative. Thus A is an ideal of R. This ideal is called the **nilradical** of R.

You can observe that every nilpotent ideal is a nilradical. Suppose A is a nilpotent ideal, then $A^n = \{0\}$ for some positive integer n. Now

$$a \in A \Longrightarrow a^n \in A^n \Longrightarrow a^n = 0$$

Hence A is a nil radical.

Therefore in above example the nilpotent ideal $A = \left\{\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z}\right\}$ of $U_2(\mathbb{Z})$ is a nilradical.

Proposition Let R be a commutative ring and A an ideal of R. Then

$$\sqrt{A} = \{a \in R : a^n \in A \text{ for some positive integer n }\}$$

is an ideal of R.

Proof: Since $0 \in A$, hence $0 \in \sqrt{A}$. Therefore $\sqrt{A}$ is non-empty. Let $a, b \in \sqrt{A}$. Then $a^n, b^m \in A$ for some positive integers n and m.

Since R is a commutative ring, hence

$$(a-b)^{n+m} = \sum_{r=0}^{n+m} (-1)^r \binom{n+m}{r} a^{n+m-r}b^r$$

Let $s + t = n + m$. Now A is an ideal, hence we have $a^s b^t = a^n(a^{s-n}b^t) \in A$ for $s \geq n$, and $a^s b^t = (a^s b^{t-m})b^m \in A$ for $t \geq m$.

Hence we have $(a-b)^{n+m} \in A \Longrightarrow a - b \in \sqrt{A}$

Also if $r \in R$ and $a \in \sqrt{A}$, then $a^n \in A$ for some positive integers n and

$$(ra)^n = r^n a^n \in A$$
$$\Rightarrow ra \in \sqrt{A}$$

Also $ar = ra \in \sqrt{A}$ as R is commutative. Thus $\sqrt{A}$ is an ideal of R. This ideal is called the **radical** of R.

8.5 Quotient rings

In unit 4, you have seen that if N is a normal subgroup of a group G, then the set of all cosets of N forms a group called the quotient group G/N under coset multiplication. In ring theory, the ideals play the same role as normal subgroups do in group theory. So for a given ideal S of a ring R, we can define quotient ring R/S.

In section 8.3, we have seen that if S is a subring of R then the relation of congruence modulo S is an equivalence relation on the ring R. This equivalence relation partitions the ring into equivalence classes and if $a \in S, y \in R \Rightarrow ya \in S, ay \in S$ then for every $x \in R$ the equivalence class $[x]$ under the relation congruence modulo S is equal to $x + S$, i.e. $[x] = x + S = S + x$ and conversely. In other words, if S is an ideal of R, then for every $x \in R$ we have $[x] = x + S = S + x$. Let R/S be the set of all equivalence classes for the relation of congruence modulo S. Then

$$R/S = \{r + S : r \in R\}$$

Since S is an additive subgroup of R, we can define the quotient group $(R/S, +)$ under the addition given by $(a + S) + (b + S) = (a + b) + S$ for all $a, b \in R$. Now we want to make R/S a ring. So we define multiplication composition on R/S as follows:

$$(a + S)(b + S) = ab + S$$

First we shall show that this multiplication is well defined.

Let $a + S = a' + S, b + S = b' + S$ for some $a, b, a', b' \in R$.

$\Rightarrow a - a' \in S, b - b' \in S$

$\Rightarrow a - a' = u, b - b' = v$ for some $u, v \in S$

$\Rightarrow a = u + a', b = v + b'$

$\Rightarrow ab = (u + a')(v + b') = uv + ub' + a'v + a'b'$

Since S is an ideal, hence $a'v \in S, ub' \in S, uv \in S$ and therefore $uv + ub' + a'v \in S$. Thus

$$ab - a'b' = uv + ub' + a'v \in S$$
$$\Rightarrow ab + S = a'b' + S$$
$$\Rightarrow (a + S)(a' + S) = (b + S)(b' + S)$$

Hence the multiplication in R/S is well defined. Now we shall show that R/S is a ring with respect to addition and multiplication defined above.

Proposition Let R be a ring and S be an ideal of R. Then R/S is a ring under the addition and multiplication defined as follows:

$$(a + S) + (b + S) = (a + b) + S$$
$$(a + S)(b + S) = ab + S$$

For all $a + S, b + S \in R/S$

Proof: The addition and multiplication are well defined and $(R/S, +)$ is an abelian group. Also by definition R/S is closed under multiplication, hence we shall prove the remaining properties of a ring for R/S.

Associativity of multiplication: Let $a+S, b+S, c+S \in R/S$. Then

$$\begin{aligned}(a+S)[(b+S)(c+S)] &= (a+S)(bc+S)\\ &= a(bc)+S\\ &= (ab)c+S \text{ as } a(bc)=(ab)c \text{ in } R\\ &= (ab+S)(c+S)\\ &= [(a+S)(b+S)](c+S)\end{aligned}$$

Distributive Laws: we have

$$\begin{aligned}(a+S)[(b+S)+(c+S)] &= (a+S)[(b+c)+S]\\ &= a(b+c)+S\\ &= (ab+ac)+S\\ &= (ab+S)+(ac+S)\\ &= (a+S)(b+S)+(a+S)(c+S)\end{aligned}$$

Similarly, we can show that

$$[(b+S)+(c+S)](a+S) = (b+S)(a+S)+(c+S)(a+S)$$

Hence $(R/S, +, \cdot)$ is a ring.

Definition Let R be a ring and S be any ideal of R. Then $R/S = \{r+S : r \in R\}$ forms a ring with respect to the binary compositions '$+$' and '$\cdot$' defined as follows

$$(a+S)+(b+S) = (a+b)+S$$
$$(a+S)(b+S) = ab+S$$

for all $a, b \in R$. This ring $(R/S, +, \cdot)$ is called the **quotient ring** of R with respect to the ideal S or **quotient ring of R modulo S**.

Obviously R/S is commutative if R is commutative. Also if R has a unity 1, then R/S has unity $1+S$.

Examples

(1) We know that $n\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$ of integers. Hence $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring. Where

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$$

Here you will observe that the compositions '$+$' and '$\cdot$' are modulo n arithmetic and $r+n\mathbb{Z} = [r] = \{x \in \mathbb{Z} : x \equiv r \pmod{n}\}$.

For instance, suppose $n=4$. Then $\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z})\}$.

Now $(2+4\mathbb{Z})+(3+4\mathbb{Z}) = (2+3)+4\mathbb{Z} = 5+4\mathbb{Z} = 1+4\mathbb{Z}$

$$(2+4\mathbb{Z})(3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2+4\mathbb{Z}$$

You can make composition tables to verify that $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ is a ring.

(2) In unit 7, you have seen that if f be a homomorphism of a ring R into a ring R', then the kernel Ker f of the homomorphism f is an ideal of R. Therefore $R/\text{Ker } f$ is a quotient ring.

Proposition Let N be an ideal of a ring R. Then the mapping $\pi: R \longrightarrow R/N$ given by $\pi(r) = r+N$ is an epimorphism with kernel N.

Proof Since N is an ideal of a ring R, hence R/N is a quotient ring. Let $r+N \in R/N$. Then $r \in R$ and $\pi(r) = r+N$. Therefore π is onto.

Let $r, s \in R$. Then

$$\pi(r+s) = (r+s)+N = (r+N)+(s+N) = \pi(r)+\pi(s)$$

and

$$\pi(rs) = rs+N = (r+N)(s+N) = \pi(r)\pi(s)$$

Hence π is a homomorphism of R onto R/N, i.e. π is an epimorphism. This map is called canonical or natural epimorphism.

Now Ker $\pi = \{r \in R : \pi(r) = N\} = \{r \in R : r+N = N\} = \{r \in R : r \in N\} = N$

8.6 Fundamental theorem of homomorphism

In unit 4 we proved fundamental theorem of homomorphism for groups. Now we shall prove a similar result for rings.

Theorem Every homomorphic image of a ring R is isomorphic to some quotient ring.

Proof Let f be a homomorphism of a ring R onto a ring R'. Then R' is a homomorphic image of the ring R. Let $N = \text{Ker } f$. Then N is an ideal of R and R/N is a quotient ring. Define $\varphi: R/N \longrightarrow R'$ by $\varphi(r+N) = f(r)$ for all $r+N \in R/N$. Then for $r+N, s+N \in R/N$, we have

$$\begin{aligned} r+N = s+N &\Leftrightarrow r-s \in N \\ &\Leftrightarrow f(r-s) = 0 \\ &\Leftrightarrow f(r) - f(s) = 0 \\ &\Leftrightarrow f(r) = f(s) \\ &\Leftrightarrow \varphi(r+N) = \varphi(s+N) \end{aligned}$$

Hence φ is well-defined and one-one.

Now $\varphi[(r+N)+(s+N)] = \varphi[(r+s)+N] = f(r+s)$

$$= f(r) + f(s) = \varphi(r+N) + \varphi(s+N)$$

$$\varphi[(r+N)(s+N)] = \varphi(rs+N)$$

$$= f(rs) = f(r)f(s) = \varphi(r+N)\varphi(s+N)$$

Hence φ is a monomorphism.

Let $b \in R'$. Since f is onto, hence there exists $a \in R$ such that $b = f(a)$. Now $a+N \in R/N$ and we have $\varphi(a+N) = f(a) = b$. Thus φ is onto R'. Hence φ is an isomorphism of R/N onto R', i.e. $R/N \cong R'$.

This theorem is also called **"*The first isomorphism theorem for rings*".**

Theorem (*Correspondence Theorem*) Let R and S be rings and $f: R \longrightarrow S$ be an epimorphism. Then there exists a one-to-one correspondence between the collection of ideals of R containing Ker f and the collection of ideals of S.

Proof Let $K = \text{Ker } f$. Let $\mathfrak{I}(R)$ be the collection of all ideals of R containing K and $\mathfrak{I}(S)$ be the collection of all ideals of S. Define $\varphi: \mathfrak{I}(R) \longrightarrow \mathfrak{I}(S)$ by $\varphi(I) = f(I)$ for all $I \in \mathfrak{I}(R)$. Since f is a homomorphism, hence $f(I)$ is an ideal of S. Therefore $f(I) \in \mathfrak{I}(S)$.

Let $A, B \in \mathfrak{I}(R)$. Then $\varphi(A) = \varphi(B) \Longrightarrow f(A) = f(B)$.

We shall prove that $A = B$. Let $a \in A$. Then $f(A) = f(B)$ implies that there exists $b \in B$ such that $f(a) = f(b)$. Which gives

$f(a) - f(b) = 0 \Longrightarrow f(a-b) = 0 \Longrightarrow a-b \in \text{Ker } f = K \subseteq B$

Now $b \in B,\ a-b \in B \Longrightarrow a = (a-b)+b \in B$. Thus $a \in A \Longrightarrow a \in B$, i.e. $A \subseteq B$. Similarly, $B \subseteq A$. Thus $A = B$. Therefore we have shown that

$$\varphi(A) = \varphi(B) \Longrightarrow f(A) = f(B) \Longrightarrow A = B$$

Hence φ is one-one.

Let $N \in \mathfrak{I}(S)$. Since f is an epimorphism, hence $f^{-1}(N)$ is an ideal of R containing K. Let $f^{-1}(N) = M$. Then $\varphi^{-1}(N) = f^{-1}(N) = M$. Now

$$f[f^{-1}(N)] = N \cap f(R) = N \Longrightarrow f(M) = N$$

Hence $N = f(M) = \varphi(M)$. Thus φ is onto. Hence φ is a one-to-one correspondence between $\mathfrak{I}(R)$ and $\mathfrak{I}(S)$.

8.7 Isomorphism theorems

Now we prove some important results called "*The second isomorphism theorem for rings*" and called "*The third isomorphism theorem for rings*".

Theorem (*The second isomorphism theorem for rings*) Let A be an ideal and B be a subring of a ring R. Then

$$(A+B)/A \cong B/(A \cap B)$$

Proof $A+B$ is a subring of R containing A. Since A is an ideal of R, therefore A is an ideal of $A+B$. Hence the quotient ring $(A+B)/A$ is defined. Also $A \cap B$ is an ideal of B, i.e. the quotient ring $B/(A \cap B)$ is also defined.
Define a map $f: B \longrightarrow (A+B)/A$ by $f(b) = b + A$ for all $b \in B$.
Let $b_1, b_2 \in B$. Then

$$f(b_1 + b_2) = (b_1 + b_2) + A = (b_1 + A) + (b_2 + A) = f(b_1) + f(b_2)$$
$$f(b_1 b_2) = b_1 b_2 + A = (b_1 + A)(b_2 + A) = f(b_1) f(b_2)$$

Hence f is a homomorphism.
Let $x + A \in (A+B)/A$. Then there exist $a \in A$ and $b \in B$ such that $x = a + b$. Hence $x + A = a + b + A = b + a + A = b + A = f(b)$. Thus f is onto.
Also if Ker f is the kernel of the homomorphism f, then

$$\begin{aligned} b \in \text{Ker } f &\Leftrightarrow f(b) = A \\ &\Leftrightarrow b + A = A \\ &\Leftrightarrow b \in A \\ &\Leftrightarrow b \in A \cap B \text{ as } b \in B \end{aligned}$$

Hence Ker $f = A \cap B$. Therefore by fundamental theorem of homomorphism

$$(A+B)/A \cong B/(A \cap B)$$

Theorem (*The third isomorphism theorem for rings*) Let A and B be ideals of a ring R such that $B \subseteq A$, then

$$R/A \cong (R/B)/(A/B)$$

Proof Since $B \subseteq A$, hence B is an ideal of A. Hence the quotient ring A/B is defined. Also A/B is an ideal of R/B.
Define a map $f: R/B \longrightarrow R/A$ by $f(r+B) = r + A$ for all $r \in R$. Then the mapping is well defined as

$$\begin{aligned} r + B = s + B &\Longrightarrow r - s \in B \\ &\Longrightarrow r - s \in A \quad \text{as } B \subseteq A \\ &\Longrightarrow r + A = s + A \\ &\Longrightarrow f(r+B) = f(s+B) \end{aligned}$$

Now $f[(r+B) + (s+B)] = f[(r+s) + B]$
$= (r+s) + A$
$= (r + A) + (s + A)$
$= f(r+B) + f(s+B)$
and $f[(r+B)(s+B)] = f[rs + B]$
$= rs + A$
$= (r + A)(s + A)$

$$= f(r+B)f(s+B)$$

Therefore f is a homomorphism.

Let $r+A \in R/A$. Then $r \in R$. Therefore $r+B \in R/B$ and $r+A = f(r+B)$. Hence f is onto. Thus f is an epimorphism.

Now if Ker f is the kernel of the homomorphism f, then

$$r+B \in \text{Ker } f \Leftrightarrow f(r+B) = A$$
$$\Leftrightarrow r+A = A$$
$$\Leftrightarrow r \in A$$
$$\Leftrightarrow r+B \in A/B$$

Hence Ker $f = A/B$. Therefore by fundamental theorem of homomorphism

$$R/A \cong (R/B)/(A/B)$$

8.8 Principal ideals

Definition Let S be a non-empty subset of a ring R. Then an ideal of R generated by S is defined as

$$\langle S\rangle = \cap \{I : S \subseteq I; I \text{ is an ideal of } R\}$$

If $S = \{a_1, a_2, \dots, a_n\}$, then the ideal generated by S is denoted by $\langle a_1, a_2, \dots, a_n\rangle$. An ideal $\langle a\rangle$ generated by a single element a of R is called a **principal ideal** generated by a.

In other words, ideal A is generated by S if $S \subseteq A$ and for any ideal B of $S \subseteq B \Longrightarrow A \subseteq B$. Obviously $\langle S\rangle$ is the smallest ideal of R containing S.

Let R be a commutative ring with unity. Let $a \in R$. Then you can verify that the set $Ra = \{ra : r \in R\}$ is a principal ideal of R generated by a. We have already seen that Ra is a left ideal of R. Since R is commutative, hence Ra is also a right ideal. Thus Ra is an ideal of R. Now $1 \in R \Longrightarrow a = 1a \in Ra$. If S is any ideal of R containing a, then $a \in S$, $r \in R \Longrightarrow ra \in S$. Hence $Ra \subseteq S$. Therefore Ra is the smallest ideal containing a, i.e. $Ra = \langle a\rangle$.

We can generalize this process and show that if R is a commutative ring with unity and $a_1, a_2, \dots, a_n \in R$, then

$$Ra_1 + Ra_2 + \cdots + Ra_n = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_1, r_2, .. r_n \in R\}$$

is an ideal of R generated by $a_1, a_2, \dots, a_n$, i.e.

$$Ra_1 + Ra_2 + \cdots + Ra_n = \langle a_1, a_2, \dots, a_n\rangle$$

Proposition Let A and B be any two ideals of a ring R. Then $A + B = \langle A \cup B\rangle$.

Proof We have seen that $A + B$ is an ideal of R containing A and B. Now $A \subseteq A + B$, $B \subseteq A + B \Longrightarrow A \cup B \subseteq A + B$. Let S be any ideal of R such that $A \cup B \subseteq S$. Let $u \in A + B$. Then there exists $a \in A$ and $b \in B$ such that $u = a + b$. Now $a \in A$, $b \in B \Longrightarrow a, b \in A \cup B \Longrightarrow a, b \in S \Longrightarrow a + b \in S \Longrightarrow u \in S$. Hence $A + B \subseteq S$. Consequently , by definition $A + B = \langle A \cup B\rangle$.

Examples

(i) The trivial ideal $\{0\}$ and the ideal R are principal ideals as $\langle 0\rangle = \{0\}$ and $\langle 1\rangle = R$.

(ii) Consider the ring $\mathbb{Z}$ of integers. You will observe that every ideal of $\mathbb{Z}$ is a principal ideal. Suppose A is any non-trivial ideal of $\mathbb{Z}$. By well ordering principle, the positive integers in A must have a least element u(say). Suppose $n \in A$. Then by division algorithm, there exists integers q and r such that $n = qa + r$, where $0 \leq r < a$. Now A is an ideal, hence

$$a \in A, q \in \mathbb{Z} \Longrightarrow qa \in A$$

and

$$n \in A, qa \in A \Longrightarrow n - qa \in A$$

$$\Rightarrow r \in A$$

But a is least positive integer in A. Hence we have $r = 0$. Thus $n = qa$.

Therefore $A = \{qa : q \in \mathbb{Z}\}$. Suppose B is any other ideal of $\mathbb{Z}$ containing a, then $a \in B$, $q \in \mathbb{Z} \Rightarrow qa \in B$, i.e. $A \subseteq B$. Hence $A = \langle a \rangle$.

So every ideal of $\mathbb{Z}$ is a principal ideal. You can verify that $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = \{2q : q \in \mathbb{Z}\}$,i.e. the ring of even integers forms an ideal of $\mathbb{Z}$. Moreover you will also observe that $\langle n \rangle = \{nq : q \in \mathbb{Z}\} = n\mathbb{Z}$. Thus every ideal of the ring $\mathbb{Z}$ of integers is of the form of $n\mathbb{Z}$.

All this leads to the following definitions:

Definition A commutative ring R with unity is said to be a **principal ideal ring** if every ideal of R is a principal ideal.

Definition A **principal ideal domain (P.I.D.)** is an integral domain in which every ideal is a principal ideal.

Thus the integral domain $\mathbb{Z}$ of integers is a P.I.D.

You have seen that the only ideals of a field F are $\{0\}$ and F. Now $\{0\} = \langle 0 \rangle$ and $F = \langle 1 \rangle$. Hence every field is a P.I.D.

8.9 Prime ideals

The concept of prime ideal is similar to the notion of prime numbers in integers.

Definition Let R be a commutative ring. An ideal P of R is called a **prime ideal** if $P \neq R$ and $a, b \in R$, $ab \in P \Rightarrow a \in P$ or $b \in P$.

Consider the ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers. If $n = 0$, then $\langle 0 \rangle$ is a prime ideal since $a, b \in \mathbb{Z}$, $ab \in \langle 0 \rangle \Rightarrow a = 0$ or $b = 0$ as $\mathbb{Z}$ is an integral domain. Let $n \neq 0$. Since we require $n\mathbb{Z} \neq \mathbb{Z}$, hence $n \neq 1$. Then by above definition $n\mathbb{Z}$ is a prime ideal if the product ab of two integers a and b whenever belongs to $n\mathbb{Z}$, either we have $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. In other words, $n|ab \Rightarrow n|a$ or $n|b$. Hence n must be a prime number. Thus the prime ideals of $\mathbb{Z}$ are $\langle 0 \rangle$ and $p\mathbb{Z}$ (p is prime).

In fact, you will notice that in any integral domain$\langle 0 \rangle$ is a prime ideal. Now we shall see how we can characterize a prime ideal with the notion of quotient ring. For the sake of simplicity, we shall use the bar notation for the congruence classes modulo N, i.e. we shall denote $r + N \in R/N$ by $\bar{r}$.

Proposition An ideal P of a commutative ring R is prime if and only if the quotient ring R/P is an integral domain.

Proof First suppose that R/P is an integral domain. Then for all $a, b \in R$

$$\begin{aligned} ab \in P &\Rightarrow ab + P = P \\ &\Rightarrow (a + P)(b + P) = P \\ &\Rightarrow \bar{a}\bar{b} = \bar{0} \\ &\Rightarrow \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0} \text{ as } R/P \text{ is without zero divisors} \\ &\Rightarrow a \in P \text{ or } b \in P \end{aligned}$$

Hence P is a prime ideal.

Conversely, suppose that P is a prime ideal. Then

$$\begin{aligned} \bar{a}\bar{b} = \bar{0} &\Rightarrow (a + P)(b + P) = P \\ &\Rightarrow ab + P = P \\ &\Rightarrow ab \in P \\ &\Rightarrow a \in P \text{ or } b \in P \text{ as } P \text{ is a prime ideal} \\ &\Rightarrow \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0} \end{aligned}$$

Hence R/P is without zero divisors.
Now R is commutative $\Longrightarrow R/P$ is commutative. Thus R/P is a commutative ring without proper zero divisors, i.e. R/P is an integral domain.

8.10 Maximal ideals

We have seen that the quotient ring R/P is an integral domain when P is a prime ideal. You may ask when a quotient ring becomes a field. The notion of maximal ideals gives the answer. Let us first define a maximal ideal for a ring. By the notation $A \subset B$, we shall mean $A \subsetneq B$.
Definition Let R be a ring. An ideal $M \neq R$ of R is said to be a **maximal ideal** of R if there exists no ideal J of R such that $M \subset J \subset R$. In other words, An ideal M of a ring R is a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.
In a division ring D, the ideal $\langle 0\rangle$ is a maximal ideal. Since $0 \neq 1 \in D$, hence $\langle 0\rangle \neq D$. Let J be any non-trivial ideal of D. Then there exists $x \in J$ such that $x \neq 0$. Since D is a division ring hence x must be a unit, i.e. there exists $y \in D$ such that $xy = 1$. Since $xy \in J \Longrightarrow 1 \in J$, hence $J = D$. Therefore $\langle 0\rangle$ is a maximal ideal of D.
Example The ideal $\langle p\rangle$ is a maximal ideal of $\mathbb{Z}$ for each prime integer p.
Let J be an ideal of $\mathbb{Z}$ such that $\langle p\rangle \subset J$. Then there exists an integer $n \in J$ such that $n \notin \langle p\rangle$. Hence p does not divide n, i.e. $\gcd(n,p) = 1$. Hence there exist $u, v \in \mathbb{Z}$ such that $nu + pv = 1$. Since J is an ideal, hence $n \in J, u \in \mathbb{Z} \Longrightarrow nu \in J$ and $p \in \langle p\rangle \subset J, v \in \mathbb{Z} \Longrightarrow pv \in J$. Also $nu, pv \in J \Longrightarrow nu + pv \in J$, i.e. $1 \in J$. Therefore $J = \mathbb{Z}$. Hence $\langle p\rangle$ is a maximal ideal of $\mathbb{Z}$.
Example In the ring $2\mathbb{Z}$ of even integers, the principal ideal $\langle 4\rangle$ is a maximal ideal. We have $\langle 4\rangle \neq 2\mathbb{Z}$ and if J is any ideal of $2\mathbb{Z}$ such that $\langle 4\rangle \subset J$, then there exists $a \in J$ such that $a \notin \langle 4\rangle$. Hence a is an even integer which is not a multiple of 4 i.e. $a = 4n + 2$ for some integer n. Now $4n \in \langle 4\rangle \Longrightarrow 4n \in J$ as $\langle 4\rangle \subset J$. Therefore $a \in J, 4n \in J \Longrightarrow a - 4n \in J$, i.e. $2 \in J$. Since J is an ideal, hence every even integer belongs to J. Therefore $J = 2\mathbb{Z}$. Consequently, $\langle 4\rangle$ is a maximal ideal of $2\mathbb{Z}$.
Example Let R be a ring of all real valued continuous functions on the closed interval $[0,1]$. Let $M = \{f \in R : f(1/3) = 0\}$. Then M is a maximal ideal of R.
First we show that M is an ideal of R. If h is a real valued function such that $h(x) = 0$ for all $x \in [0,1]$, then $h \in R$. Obviously $h(1/3) = 0$, hence $h \in M$. Hence M is non-empty. Let $f, g \in M$. Then

$$(f - g)(1/3) = f(1/3) - g(1/3) = 0 - 0 = 0$$
$$\Longrightarrow f - g \in M$$

Let $u \in R$. Then $(uf)(1/3) = u(1/3)f(1/3) = u(1/3).0 = 0 \Longrightarrow uf \in M$
Since R is commutative, hence $fu = uf \in M$. Hence M is an ideal of R.
Now there exists $\rho \in R$ such that $\rho(x) = 1$ for all $x \in R$. Obviously $\rho \notin M$. Therefore $M \neq R$. Let J be an ideal of R such that $M \subset J$. Then there exists $\lambda \in J$ such that $\lambda \notin M$. Hence $\lambda(1/3) \neq 0$. Let $\lambda(1/3) = k$ where $k \neq 0$. Define $\beta(x) = k$ for all $x \in [0,1]$. Then $\beta \in R$. Now

$$(\lambda - \beta)(1/3) = \lambda(1/3) - \beta(1/3) = 0 \Longrightarrow \lambda - \beta \in M \Longrightarrow \lambda - \beta \in J$$

Therefore $\lambda \in J, \lambda - \beta \in J \Longrightarrow \beta = \lambda + (\lambda - \beta) \in J$.
If we define $\gamma(x) = 1/k$ for all $x \in [0,1]$. Then $\gamma \in R$. Therefore

$$(\gamma\beta)(x) = \gamma(x)\beta(x) = 1 = \rho(x) \Longrightarrow \gamma\beta = \rho$$

Now $\gamma \in R, \beta \in J \Longrightarrow \gamma\beta \in J$ as J is an ideal. Thus $\rho = \gamma\beta \in J$. But ρ is the unity of R. Hence we have $J = R$. Consequently, M is a maximal ideal of R.

Proposition An ideal M of a commutative ring R with unity is a maximal ideal if and only if R/M is a field.

Proof First suppose that M is a maximal ideal of R. Since R is a commutative ring with unity, hence R/M is a commutative quotient ring with unity $1+M$. To prove that R/M is a field, we have to show that each non-zero element $a+M$ of R/M is a unit. Since $a+M \neq M$, hence $a \notin M$. Now Ra is an ideal of R and $a = 1a \in Ra$. Therefore $a \in M + Ra$. But $a \notin M$, hence $M \subset M + Ra$. The ideal M is maximal, hence $M + Ra = R$. Since $1 \in R$, hence there exists $m \in M$ and $r \in R$ such that $m + ra = 1$. Therefore

$$1 - ra = m \in M \Longrightarrow 1 + M = ra + M = (r + M)(a + M)$$
$$\Longrightarrow \bar{1} = \bar{r}\bar{a}$$

Since R/M is commutative, $\bar{r}\bar{a} = 1 = \bar{a}\bar{r}$. Hence $\bar{a} = a + M$ is a unit. Thus R/M is a field.

Conversely, suppose that R/M is a field. Hence $\bar{1} \neq \bar{0}$, i.e. $1 + M \neq M$. Therefore $1 \notin M$, i.e. $M \neq R$. Let J be an ideal of R such that $M \subset J$. To prove that M is maximal, we shall show that $J = R$. Let $a \in J$ such that $a \notin M$. Then $a + M \neq M$, i.e. $\bar{a} \neq \bar{0}$. Since R/M is a field, hence $\bar{a}$ must be a unit, i.e. there exists $\bar{b} \in R/M$ such that

$$\bar{a}\bar{b} = \bar{1} \Longrightarrow (a + M)(b + M) = 1 + M \Longrightarrow ab + M = 1 + M \Longrightarrow 1 - ab \in M$$

Now $M \subset J$, hence $1 - ab \in J$. Since J is an ideal and $a \in J$, hence $ab \in J$. Thus we have $(1 - ab) + ab \in J \Longrightarrow 1 \in J$. Therefore $J = R$, i.e. M is maximal in R.

You have seen that an ideal P of a commutative ring R is prime if and only if the quotient ring R/P is an integral domain. Since every field is an integral domain, hence we have the following result:

Proposition Let R be a commutative ring with unity. Then every maximal ideal of R is a prime ideal.

Proof Let M be a maximal ideal of R. Then R/M is a field. Since every field is an integral domain, hence R/M is an integral domain. Thus M is a prime ideal of R.

However the converse of this proposition is not true. $\mathbb{Z}$ is an integral domain and $\langle 0 \rangle$ is a prime ideal of $\mathbb{Z}$, but $\langle 0 \rangle$ is not maximal as $\langle 0 \rangle \subset \langle 2 \rangle \subset \mathbb{Z}$.

8.11 Summary

In this unit, we have

(1) Defined relations of congruence modulo a subring S on a given ring R and proved that these are equivalence relations on R.
(2) Defined left ideal, right ideal and ideal of a ring with examples.
(3) Defined simple ring and proved that a division ring is a simple ring.
(4) Proved that a commutative ring R with unity is a field if and only if its only ideals are $\{0\}$ and R.
(5) Defined quotient ring with examples.
(6)Proved the fundamental theorem of homomorphism for rings (first isomorphism theorem for the rings), i.e. every homomorphic image of a ring R is isomorphic to some quotient ring.
(7) Proved the second isomorphism theorem and the third isomorphism theorem for rings.
(8) Defined principal ideal, prime ideal and maximal ideal with examples.
(9) Proved that an ideal P of a commutative ring R is prime if and only if the quotient ring R/P is an integral domain.

(10) Proved that an ideal M of a commutative ring R with unity is a maximal ideal if and only if R/M is a field.
(11) Proved that every maximal ideal of commutative ring R with unity is a prime ideal.

8.12 Self assessment questions

(1) Let R be a ring with unity. If R has no right ideals except R and $\{0\}$, show that R is a division ring.
(2) Let A be an ideal of R such that $A \neq R$. Show that if R has unity then $1 \notin A$.
(3) Let R be a commutative ring and A an ideal of R. Prove that (i) $A \subseteq \sqrt{A}$ (ii)$\sqrt{\sqrt{A}} = \sqrt{A}$ (iii) if R has unity and $\sqrt{A} = R$, then $A = R$.
(4) Let E be the ring of even integers. Prove that the set of all matrices of the form $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ where each element is of the form of $4n$, $(n \in \mathbb{Z})$ is an ideal of $M_2(E)$, the ring of 2×2 matrices over E.
(5) Prove that if R is a ring with more than one element such that $aR = R$ for every non-zero element a of R then R is a division ring.
(6) If a ring R is finitely generated, then prove that each proper ideal of R is contained in a maximal ideal.
(7) Prove that a nontrivial ideal I of a Boolean ring R is prime if and only if I is a maximal ideal.
(8) If A,B and C are ideals of a ring R prove that $A(B + C) = AB + AC$.
(9)Let A be a right ideal and B be a left ideal of a ring R Show that $AB \subseteq A \cap B$.
(10) If A,B, C are ideals of a ring R such that $B \subseteq A$ then prove that

$$A \cap (B + C) = B + (A \cap C)$$

(11) In a ring R define $S = \{ab - ba: a, b \in R\}$. Show that for any ideal A of R, the quotient ring R/A is commutative if and only if $S \subseteq A$.
(12) Let for a $p(\neq 0) \in \mathbb{Z}$, $\langle p \rangle = \{pn: n \in \mathbb{Z}\}$. Show that $\mathbb{Z}/\langle p \rangle$ is a field if and only if p is a prime number.
(13) Let $f: R \longrightarrow S$ be an epimorphism. Let A and B are ideals in R and U, V are ideals in S. Prove that
(i) $f(A + B) = f(A) + f(B)$
(ii) $f(AB) = f(A)f(B)$
(iii) $f^{-1}(U + V) = f^{-1}(U) + f^{-1}(V)$
(iv) $f^{-1}(UV) \supseteq f^{-1}(U)f^{-1}(V)$
(14) Let N be an ideal of R. Prove that there is a one-to-one correspondence between ideals of R containing N and ideals of R/N.
(15) If A and B are ideals of a ring R, define $A: B = \{r \in R: rB \subseteq A\}$. Show that $A: B$ is an ideal of R.
(16) Let R be a ring and S a subring. Let P be a prime ideal of R. Show that $P \cap S$ is a prime ideal of S.
(17) Show that the intersection of a maximal ideal of a ring with a subring need not be maximal ideal of the subring whereas it remains prime ideal.
(18) Let R be a commutative ring with unity. Let A be an ideal of R. Then $\sqrt{A}$ is the intersection of all prime ideals containing A.

8.13 Further readings

(1) Herstein, I.N. (1993): Topics in Algebra, Wiley Eastern Limited, New Delhi.

(2) Fraleigh, J.B. (2003): A first course in abstract Algebra, New Delhi, Pearson Education, Inc.

(3) Dummit, D.S. and Foote, R.M. (2009): Abstract Algebra, New Delhi, Wiley India (P) Ltd.

(4) Artin, M.(1996): Algebra, New Delhi, Prentice Hall of India.

(5) Birkhoff,G. and MacLane,S (1965): A survey of modern Algebra, Macmillan, N.Y.

(6) Lang, S. (1965): Algebra, Reading, Massachusetts, Addison-Wesley.

(7) Barshay, J. (1969): Topics in ring theory, N.Y., W.A. Benjamin Inc.

(8) Burtan, D. M. (1968): A first course in Rings and Ideals, Reading, MA., Addison-Wesley.