PREFACE

In a bid to standardize higher education in the country, the University Grants Commission (UGC) has introduced Choice Based Credit System (CBCS) based on five types of courses viz. *core, discipline specific, generic elective, ability and skill enhancement* for graduate students of all programmes at Honours level. This brings in the semester pattern, which finds efficacy in sync with credit system, credit transfer, comprehensive continuous assessments and a graded pattern of evaluation. The objective is to offer learners ample flexibility of choose from a wide gamut of courses, as also to provide them lateral mobility between various educational institutions in the country where they can carry their acquired credits. I am happy to note that the University has been recently accredited by National Assessment and Accreditation Council of India (NAAC) with grade ''A''.

UGC (Open and Distance Learning Programmes and Online Programmes) Regulations, 2020 have mandated compliance with CBCS for U.G. programmes for all the HEIs in this mode. Welcoming this paradigm shift in higher education, Netaji Subhas Open University (NSOU) has resolved to adopt CBCS from the academic session 2021–22 at the Under Graduate Degree Programme level. The present syllabus, framed in the spirit of syllabi recommended by UGC, lays due stress on all aspects envisaged in the curricular framework of the apex body on higher education. It will be imparted to learners over the six semesters of the Programme.

Self Learning Materials (SLMs) are the mainstay of Student Support Services (SSS) of an Open University. From a logistic point of view, NSOU has embarked upon CBCS presently with SLMs in English/Bengali. Eventually, the English version SLMs will be trnslated into Bengali too, for the benefit of learners. As always, all of our teaching faculties contributed in this process. In addition to this we have also requisitioned the services of best academics in each domain in preparation of the new SLMs. I am sure they will be of commendable academic support. We look forward to proactive feedback from all stakeholders who will participate in the teaching-learning based on these study materials. It has been a very challenging task well executed, and I congratulate all concerned in the preparation of these SLMs.

I wish the venture a grand success.

Professor (Dr.) Subha Sankar Sarkar
Vice-Chancellor

Netaji Subhas Open University
Under Graduate Degree Programme
Choice Based Credit System (CBCS)
Subject : Honours in Mathematics (HMT)
Course : Group Theory
Course Code : CC-MT-10

First Print : March, 2022

Printed in accordance with the regulations of the Distance
Education Bureau of the University Grants Commission

Netaji Subhas Open University
Under Graduate Degree Programme
Choice Based Credit System (CBCS)
Subject : Honours in Mathematics (HMT)
Course : Group Theory
Course Code : Core Course CC-MT-10

: Course Writer :
Mr. Chandan Kumar Mondal
Netaji Subhas Open University

: Course Editor :
Prof. Kajal De
Netaji Subhas Open University

: Format Editor :
Mr. Chandan Kumar Mondal
Netaji Subhas Open University

Notification

Kishore Sengupta
Registrar

Netaji Subhas
Open University

UG : Mathematics
(HMT)

Course : Group Theory
Course Code : CC-MT-10

Unit - 1 ❑ Set Relation and Mappings

Structure

1.1 Objectives

The following are discussed here:

* Definition of set and subset

* Elementary operations on sets, De Morgan's law, Cartesion product

* Definition of relation

* Relfexive, Symmetric, transitive and equivalance relation

* Equivalance class

* Defintion of function/ mapping

* Onto mapping, one-one mapping and bijective mapping

1.2 Introduction

Set theory is the branch of mathematical logic that studies sets, which can be informally described as collections of objects. Although objects of any kind can be collected into a set, set theory, as a branch of mathematics, is mostly concerned with those that are relevant to mathematics as a whole. In this unit, some basic introduction of set theory along with the concept of relation and mappingare to be discussed.

1.3 Sets

A set is a collection of objects, called the elements or members of the set. The objects could be anything (planets, squirrels, characters in Shakespeare's plays, orother sets) but for us they will be mathematical objects such as numbers, or sets of numbers. We write $x \in X$ if x is an element of the set X and $x \notin X$ if x is not an element of X.

Sets are determined entirely by their elements. Thus, the sets X, Y are equal, written $X = Y$, if

$$x \in X \quad \text{if and only if} \quad x \in Y.$$

It is convenient to define the empty set, denoted by $\varnothing$, as the set with no elements. (Since sets are determined by their elements, there is only one set with no elements!) If $X \neq \varnothing$, meaning that X has at least one element, then we say that X is nonempty.

We can define a finite set by listing its elements (between curly brackets). For example,

$$X = \{2, 3 , 5, 7, 11\}$$

is a set with five elements. The order in which the elements are listed or repetitions of the same element are irrelevant. Alternatively, we can define X as the set whose elements are the first five prime numbers. It doesn't matter how we specify the elements of X, only that they are the same.

Infinite sets can't be defined by explicitly listing all of their elements. Nevertheless, we will adopt a realist (or "platonist") approach towards arbitrary infinite sets and regard them as well-defined totalities. In constructive mathematics and computer science, one may be interested only in sets that can be defined by a rule or algorithm — for example, the set of all prime numbers — rather than by infinitely many arbitrary specifications.

1.3.1 Numbers : The infinite sets we use are derived from the natural and real numbers, about which we have a direct intuitive understanding.

Our understanding of the natural numbers 1, 2, 3, . . . derives from counting.We denote the set of natural numbers by

$$\mathbb{N} = \{1, 2 , 3, . . . \}.$$

We define $\mathbb{N}$ so that it starts at 1. In set theory and logic, the natural numbers are defined to start at zero, but we denote this set by $\mathbb{N}_0 = \{0 , 1, 2, . . . \}$. Historically, the number 0 was later addition to the number system, primarily by Indian mathematicians in the 5th century AD. The ancient Greek mathematicians, such as Euclid, defined a number as a multiplicity and didn't consider 1 to be a number either.

Our understanding of the real numbers derives from durations of time and lengths in space. We think of the real line, or continuum, as being composed of an (uncountably) infinite number of points, each of which corresponds to a real number, and denote the set of real numbers by $\mathbb{R}$.

We denote the set of (positive, negative and zero) integers by

$$\mathbb{Z} = \{. . . ,-3,-2,-1, 0, 1, 2, 3, . . . \},$$

and the set of rational numbers (ratios of integers) by

$$\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}.$$

The letter "Z" comes from "zahl" (German for "number") and "Q" comes from "quotient." These number systems are discussed further in unit 2.

Although we will not develop any complex analysis here, we occasionally make use of complex numbers. We denote the set of complex numbers by

$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\} ,$$

where we add and multiply complex numbers in the natural way, with the additional identity that $i^2 = -1$, meaning that i is a square root of -1. If $z = x + iy \in \mathbb{C}$, we call $x = \Re z$ the real part of z and $y = \Im z$ the imaginary part of z, and we call

$$| z | = \sqrt{x^2 + y^2}$$

the absolute value, or modulus, of z. Two complex numbers $z = x + iy$, $w = u + iv$ are equal if and only if $x = u$ and $y = v$.

1.3.2 Subsets : A set A is a subset of a set X, written $A \subseteq X$, if every element of A belongs to X; that is, if

$$x \in A \text{ implies that } x \in X.$$

We also say that A is included in X. For example, if P is the set of prime numbers, then $P \subseteq \mathbb{N}$, and $\mathbb{N} \subseteq \mathbb{R}$. The empty set $\varnothing$ and the whole set X are subsets of any set X. Note that $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$; we often prove the equality of two sets by showing that each one includes the other.

If $A \neq X$ but $A \subseteq X$, then A is called a proper subset of X and is denoted by $A \subset X$. In our notation, $A \subseteq X$ does not imply that A is a proper subset of X (that is, a subset of X not equal to X itself), and we may have $A = X$.

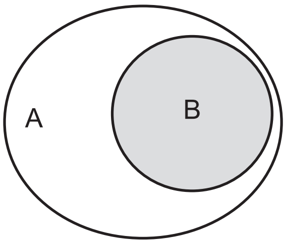


***Fig. 1.1* : Venn diagram of set A with a subset B**

Definition 1.3.3 : The power set $P(X)$ of a set X is the set of all subsets of X.

Example 1.3.4 : If $X = \{1, 2, 3\}$, then

$$P(X) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}\} .$$

The power set of a finite set with n elements has 2^n elements because, in defining a subset, we have two independent choices for each element (does it belong to the subset or not?). In Example 1.3.4, X has 3 elements and $P(X)$ has $2^3 = 8$ elements.

The power set of an infinite set, such as $\mathbb{N}$, consists of all finite and infinite subsets and is infinite.

We imagine that a general subset $A \subseteq \mathbb{N}$ is "defined" by going through the elements of $\mathbb{N}$ one by one and deciding for each $n \in \mathbb{N}$ whether $n \in A$ or n not belongs to A.

If X is a set and P is a property of elements of X, we denote the subset of X consisting of elements with the property P by $\{x \in X : P(x)\}$.

Example 1.3.5 : The set

$$\{n \in \mathbb{N} : n = k^2 \text{ for some } k \in \mathbb{N}\}$$

is the set of perfect squares $\{1, 4, 9, 16, 25, \ldots\}$. The set

$$\{x \in \mathbb{R} : 0 < x < 1\}$$

is the open interval (0, 1).

1.3.6 Set operations : The intersection $A \cap B$ of two sets A, B is the set of all elements that belong to both A and B; that is

$$x \in A \cap B \text{ if and only if } x \in A \text{ and } x \in B.$$

Two sets A, B are said to be disjoint if $A \cap B = \varnothing$; that is, if A and B have no elements in common.

The union $A \cup B$ is the set of all elements that belong to A or B; that is

$$x \in A \cup B \text{ if and only if } x \in A \text{ or } x \in B.$$

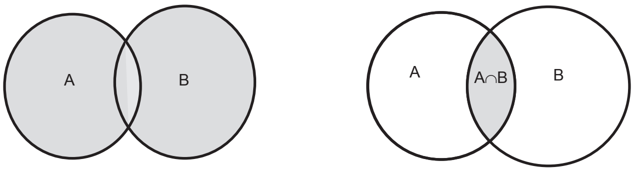


***Fig. 1.2* : Union of A and B** **Intersection of A and B**

Note that we always use 'or' in an inclusive sense, so that $x \in A \cup$ B if x is an element of A or B, or both A and B. (Thus, $A \cap B \subset A \cup B$.)

The set-difference of two sets B and A is the set of elements of B that do not belong to A,

$$B \setminus A = \{x \in B : x \notin A\} \ .$$

If we consider sets that are subsets of a fixed set X that is understood from the context, then we write $\mathrm{A}^c = X \setminus A$ to denote the complement of $A \subset X$ in X. Note that $(A^c)^c = A$.

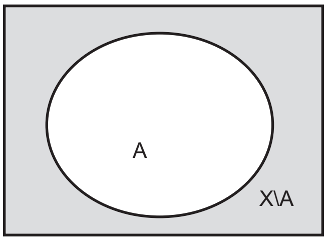


***Fig. 1.3* : Complement of A**

Example 1.3.7 : If

$$A = \{2, 3, 5, 7, 11\}, \qquad B = \{1, 3, 5, 7, 9, 11\}$$

then

$$A \cap B = \{3, 5, 7, 11\}, \ \ A \cup B = \{1, 2, 3, 5, 7, 9, 11\}.$$

Thus, $A \cap B$ consists of the natural numbers between 1 and 11 that are both prime and odd, while $A \cup B$ consists of the numbers that are either prime or odd (or both). The set differences of these sets are

$$B \setminus A = \{1, 9\}, \qquad A \setminus B = \{2\} \ .$$

Thus, $B \setminus A$ is the set of odd numbers between 1 and 11 that are not prime, and $A \setminus B$ is the set of prime numbers that are not odd.

If $A, B \subset X$, we have De Morgan's laws:

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c$$

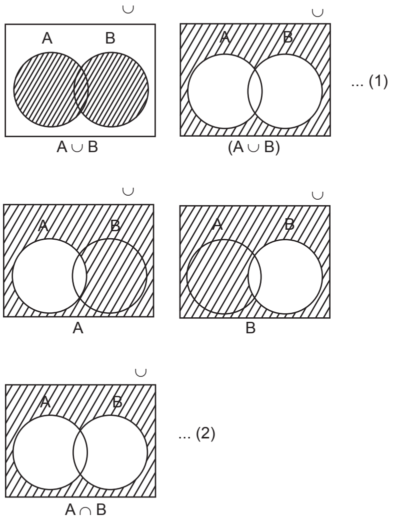


Fig. 1.4 : **De Morgan's laws**

The Cartesian product $X \times Y$ of sets X, Y is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. If $X = Y$, we often write $X \times X = X^2$. Two ordered pairs (x_1, y_1), (x_2, y_2) in $X \times Y$ are equal if and only if $x_1 = x_2$ and $y_1 = y_2$. Thus, $(x, y) \neq (y, x)$ unless $x = y$. This contrasts with sets where $\{x, y\} = \{y, x\}$.

Example 1.3.8 : If $X = \{1, 2, 3\}$ and $Y = \{4 , 5\}$ then

$$X \times Y = \{(1, 4), (1, 5), (2, 4) , (2, 5), (3, 4), (3, 5)\} .$$

Example 1.3.9 : The Cartesian product of $\mathbb{R}$ with itself is the Cartesian plane $\mathbb{R}^2$ consisting of all points with coordinates (x, y) where $x, y \in \mathbb{R}$.

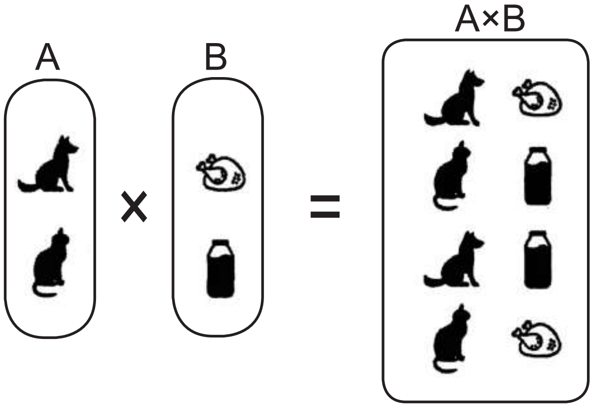


Fig. 1.5 : **Cartesian Product of Two Sets.**

The Cartesian product of finitely many sets is defined analogously.

Definition 1.3.10 : The Cartesian products of n sets X_1 , X_2, . . . , X_n is the set of ordered n-tuples,

$X_1 \times X_2 \times . . . \times X_n = \{(x_1, \text{x}_2 , . . . , x_n) : x_i \in X_i$ for $i = 1, 2, . . . , n\}$, where $(x_1, x_2 , . . . , x_n) = (y_1, y_2 , . . . , y_n)$ if and only if $x_i = y_i$ for every $i = 1 , 2, . . . , n$.

1.4 Relations

A relation R on two non-empty sets X and Y is a rule that associates some or all the elements of X with some elements or element of Y . We write xRy if $x \in X$ and $y \in Y$ are related. One can also define relations on more than two sets, but we shall consider only binary relations and refer to them simply as relations. If $X = Y$, then we call R a relation on X

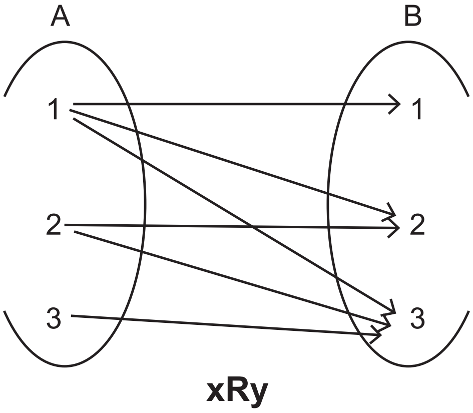


Fig. 1.6 **: A relation between A and B**

The relation R between two non-empty sets X and Y is a subset of X × Y, i.e.,

$$R = \{(x, y) : xRy, \quad x \in X \text{ and } y \in Y \} \subseteq X \times Y.$$

Example 1.4.1 : Suppose that S is a set of students enrolled in a university and B is a set of books in a library. We might define a relation R on S and B by :

$$s \in S \text{ has read } b \in B.$$

In that case, sRb if and only if s has read b. Another, probably inequivalent, relation is:

$$s \in S \text{ has checked } b \in B \text{ out of the library.}$$

Example 1.4.2 : Let S be the set of balls in a box. Now define a relation R on S by

$$xRy \text{ if and only if } x \text{ and } y \text{ have the same colour.}$$

When used informally, relations may be ambiguous (did s read b if she only read the first page?), but in mathematical usage we always require that relations are definite, meaning that one and only one of the statements "these elements are related" or "these elements are not related" is true.

The graph G_R of a relation R on X and Y is the subset of $X \times Y$ defined by

$$G_R = \{(x, y) \in X \times Y : xRy\}.$$

This graph contains all of the information about which elements are related.

Definition 1.4.3 : A relation R on a set S is said to be reflexive if

$$xRx \text{ for all } x \in S.$$

Example 1.4.4 : The relation R defined on the set of real numbers $\mathbb{R}$ by

$$xRy \text{ if and only if } x - y \geq 0.$$

Then the relation R is reflexive on $\mathbb{R}$.

Example 1.4.5 : Let S be the set of all students in a class. Now a reflexive relation R is defined on S by

$$xRy \text{ if and only if } x \text{ and } y \text{ obtain same marks.}$$

Not all relations satisfy the reflexive condition, see the following example.

Example 1.4.6 : Consider the relation R on the set of integers $\mathbb{Z}$ defined by

$$xRy \text{ if and only if } x + y = 1.$$

This relation is not reflexive.

Definition 1.4.7 : A relation R on a set S is said to be symmetric if

$$xRy \text{ implies } yRx \quad \forall x, y \in S.$$

Example 1.4.8 : The relation R defined on the set of real numbers $\mathbb{R}$ by

$$xRy \text{ if and only if } x \text{ and } y \text{ have a common divisor other than } 1.$$

Then the relation R is symmetric on $\mathbb{R}$.

Example 1.4.9 : Let S be the set of all students in a school. Now a relation R is defined on S by

$$xRy \text{ if and only if } x \text{ and y are from different classes.}$$

This relation is symmetric but not reflexive.

Definition 1.4.10 : A relation R on a set S is said to be transitive if

$$xRy \text{ and } yRz \text{ implies } xRz \quad \forall x, y, z \in S.$$

Example 1.4.11 : The relation R defined on the set of integers $\mathbb{Z}$ by

$$xRy \text{ if and only if } x < y.$$

Then the relation R is transitive on $\mathbb{R}$ although it is neither reflexive nor symmetric.

1.4.12 : Equivalence relations : Equivalence relations decompose a set into disjoint subsets, called equivalence classes. We begin with an example of an equivalence relation on $\mathbb{N}$.

Example 1.4.12.1 : Fix $N \in \mathbb{N}$ and say that $m\ R\ n$ if

$$m \equiv n \ (\text{mod } N),$$

meaning that m - n is divisible by N . Two numbers are related by R if they have the same remainder when divided by N . Moreover, N is the union of N disjoint sets, consisting of numbers with remainders 0, 1,. . .$N - 1$ modulo N .

Definition 1.4.12.2 : An equivalence relation R on a set X is a binary relation on X such that for every $x, y, z \in X$:

(a) $x\ R\ x$ (reflexivity);

(b) if $x\ R\ y$ then $y\ R\ x$ (symmetry);

(c) if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$ (transitivity).

Example 1.4.12.3 : The relation R on the set of integers defined by

$$x\ R\ y \text{ if and only if } x - y \text{ is divisible by 2.}$$

This relation is reflexive since $x - x = 0$ is divisible by 2. It is easy to check that this relation is symmetric and also transitive. Therefore, it is an equivalence relation.

Example 1.4.12.4 : The relation R on the set of balls in a box, S, defined by

$$x\ R\ y \text{ if and only if both } x \text{ and } y \text{ has same colour.}$$

This relation is an equivalence relation (check it !).

Example 1.4.12.5 : The relation R on the set of all triangles in the plane, K, defined by

$$x\ R\ y \text{ if and only if both } x \text{ and } y \text{ has same area.}$$

This relation is an equivalence relation .

Example 1.4.12.6 : If we define a relation R on $\mathbb{R}$ by

$$x\ R \text{ y if and only if } x < y.$$

Then this relation is not equivalence as the it breaks the reflexive and symmetric conditions.

For each $x \in X$, the set of elements equivalent to x,

$$[x/R] = \{y \in X : x\ R\ y\} \ ,$$

is called the equivalence class of x with respect to R When the equivalence relation is understood, we write the equivalence class $[x/ R]$ simply as $[x]$. The set of equivalence classes of an equivalence relation R on a set X is denoted by X/ R. Note that each element of X/ R is a subset of X, so X/ R is a subset of the power set $P(X)$ of X.

The following theorem is the basic result about equivalence relations. It says that an equivalence relation on a set partitions the set into disjoint equivalence classes.

Theorem 1.4.12.7 : Let R be an equivalence relation on a set X. Every equivalence class is non-empty, and X is the disjoint union of the equivalence classes of R.

Proof. If $x \in X$, then the reflexive of R implies that $x \in [x]$. Therefore every equivalence class is non-empty and the union of the equivalence classes is X.

To prove that the union is disjoint, we show that for every $x, y \in X$ either $[x] \cap [y] = \varnothing$ (if $x \not R\ y$) or $[x] = [y]$ (if $x\, R\, y$).

Suppose that $[x] \cap [y] \neq \varnothing$. Let z $\in [x] \cap [y]$ be an element in both equivalence classes. If $x_1 \in [x]$, then $x_1\, R\, z$ and $z\, R\, y$, so $x_1\, R\, y$ by the transitivity of R and therefore $x_1 \in [y]$. It follows that $[x] \subset [y]$. A similar argument applied to $y_1 \in [y]$ implies that $[y] \subset [x]$, and therefore $[x] = [y]$. In particular, $y \in [x]$, so $x\, R\, y$. On the other hand, if $[x] \cap [y] = \varnothing$, then y does not belong to $[x]$ since $y \in [y]$, so $x \not R\ y$. □

There is a natural projection $\pi : X \to X / R$ given by $\pi\,(x) = [x]$, that maps each element of X to the equivalence class that contains it. Conversely, we can index the collection of equivalence classes

$$X/ R = \{[a] : a \in A\}$$

by a subset A of X which contains exactly one element from each equivalence class. It is important to recognize, however, that such an indexing involves an arbitrary choice of a representative element from each equivalence class, and it is better to think in terms of the collection of equivalence classes, rather than a subset of elements.

Example 1.4.12.8 : The equivalence classes of $\mathbb{N}$ relative to the equivalence relation $m\, R\, n$ if $m \equiv$ n (mod 3) are given by

$$I_0 = \{3, 6, 9, \ldots\}, I_1 = \{1, 4, 7, \ldots\}, I_2 = \{2, 5, 8, \ldots\}.$$

The projection $\pi : \mathbb{N} \to \{I_0, I_1, I_2\}$ maps a number to its equivalence class e.g. $\pi\,(101) = I_2$. We can choose $\{1,2, 3\}$ as a set of representative elements, in which case

$$I_0 = [3], \qquad I_1 = [1], \qquad I_2 = [2],$$

but any other set $A \subset \mathbb{N}$ of three numbers with remainders 0, 1, 2 (mod 3) will do. For example, if we choose $A = \{7 , 15, 101\}$, then

$$I_0 = [15], \qquad I_1 = [7], \qquad I_2 = [101],$$

1.5 Functions

A function $f : X \to Y$ between sets X and Y assigns to each $x \in X$ a unique element $f(x) \in Y$. Functions are also called maps, mappings, or transformations. The set X on which f is defined is called the domain of f and the set Y in which it takes its values is called the codomain. We write $f : x \to f(x)$ to indicate that f is the function that maps x to $f(x)$.

Definition 1.5.1 : A function f between two sets X and Y is a subset $f \subseteq X \times Y$ such that

(i) For all $x \in X$, there exists $y \in Y$ such that $(x, y) \in f$

(ii) For any $x \in X$, if there exists $y, y' \in Y$ such that $(x, y), (x, y') \in f$ then $y = y'$.

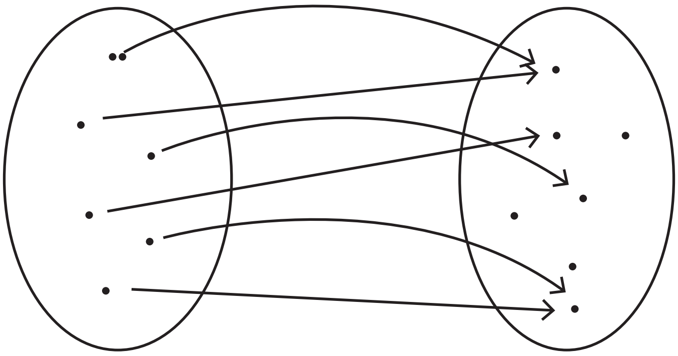


Fig. 1.7 : $X \xrightarrow{\quad f \quad} Y$

Example 1.5.2 : The identity function $\text{id}_x : \text{X} \to \text{X}$ on a set X is the function $\text{id}_x : x \mapsto x$ that maps every element to itself.

Example 1.5.3 : Let $A \subset X$. The characteristic (or indicator) function of A,

$$\chi_A : X \to \{0 , 1\},$$

is defined by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Specifying the function χ_A is equivalent to specifying the subset A.

Example 1.5.4 : Let A, B be the sets in Example 1.4. We can define a function $f : A \to B$ by

$$f(2) = 7, \quad f(3) = 1, \quad f(5) = 11, \quad f(7) = 3, \quad f(11) = 9,$$

and a function $g : B \to A$ by

$$g(1) = 3, \quad g(3) = 7, \quad g(5) = 2, \quad g(7) = 2, \quad g(9) = 5, \quad g(11) = 11.$$

Example 1.5.5 : The square function $f : \mathbb{N} \to \mathbb{N}$ is defined by

$$f(n) = n^2,$$

which we also write as $f : n \to n^2$. The equation $g(n) = \sqrt{n}$, where $\sqrt{n}$ is the positive square root, defines a function $g : \mathbb{N} \to \mathbb{R}$, but $h(n) = \pm \sqrt{n}$ does not define a function since it doesn't specify a unique value for $h(n)$. Sometimes we use a convenient oxymoron and refer to h as a multi-valued function.

One way to specify a function is to explicitly list its values, as in Example 1.5.4 Another way is to give a definite rule, as in Example 1.5.5 If X is infinite and f is not given by a definite rule, then neither of these methods can be used to specify the function. Nevertheless, we suppose that a general function $f : X \to Y$ may be "defined" by picking for each $x \in X$ a corresponding value $f(x) \in Y$.

If $f : X \to Y$ and $U \subset X$, then we denote the restriction of f to U by $f|_U : U \to Y$, where $f|_U(x) = f(x)$ for $x \in U$.

In defining a function $f : X \to Y$, it is crucial to specify the domain X of elements on which it is defined. There is more ambiguity about the choice of codomain, however, since we can extend the codomain to any set $Z \supset$Y and define a function $g : X \to Z$ by $g(x) = f(x)$. Strictly speaking, even though f and g have exactly the same values, they are different functions since they have different codomains. Usually, however, we will ignore this distinction and regard f and g as being the same function.

The graph of a function $f : X \to Y$ is the subset G_f of $X \times Y$ defined by

$$G_f = \{(x, y) \in X \times Y : x \in X \text{ and } y = f(x)\} .$$

For example, if $f : \mathbb{R} \to \mathbb{R}$, then the graph of f is the usual set of points (x, y) with $y = f(x)$ in the Cartesian plane $\mathbb{R}^2$. Since a function is defined at every point in its domain, there is some point $(x, y) \in G_f$ for every $x \in X$, and since the value of a function is uniquely defined, there is exactly one such point. In other words, for each $x \in X$ the "vertical line" $L_x = \{(x, y) \in X \times Y : y \in Y\}$ through x intersects the graph of a function $f : X \to Y$ in exactly one point : $L_x \cap G_f = (x, f(x))$.

Definition 1.5.6 : The image, of a function f : X → Y is the set of values

$$\text{Img}(f) = \{y \in Y : y = f(x) \text{ for some } x \in X\} .$$

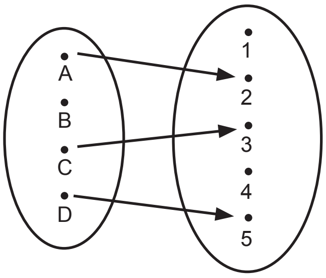
	Domain	{A,B,C,D}
	Image	{2,3,5}
	Codomain	{2,2,3,4,5}

Fig. 1.8 **: Function**

Definition: function $f : X \to Y$ is said to

• Onto or surjective if the image of f is the whole Y, i.e.,

$$Img(f) = Y$$

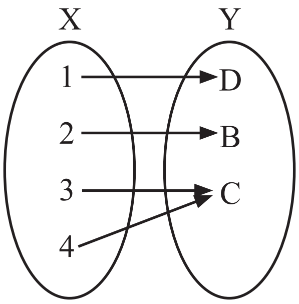


Fig. 1.9 **: Onto**

• One-one or injective if each point in the image of f in Y has a unique pre-image in X, i.e.,

$$f(x) = f(y) \textit{ implies } x = y \quad \forall x, y \in X.$$

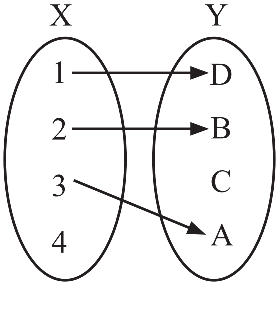


Fig. 1.10 **: One-one**

- Bijective if *f* is both onto and one-one.

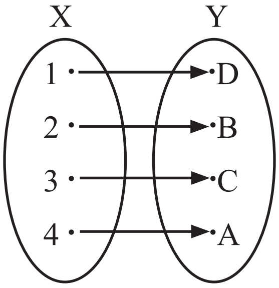


Fig. 1.11 **: Bijective**

1.6 Summary

In this chapter, we have discussed the preliminary concept in set, relation and functions. Various elementary operations in sets such as union, intersection etc are discussed. Various types of relations are presented and also some clasification of functions are described in pictorial notion.

1.7 Worked examples

1. Determine whether each of the following relations are reflexive, symmetric and transitive :

(i) Relation R in the set $A = \{1, 2, 3 \ldots 13, 14\}$ defined as

R = $\{(x, y): 3x - y = 0\}$

(ii) Relation R in the set N of natural numbers defined as

R = $\{(x, y): y = x + 5$ and $x < 4\}$

(iii) Relation R in the set $A = \{1, 2, 3, 4, 5, 6\}$ as

R = $\{(x, y)$: y is divisible by x$\}$

(iv) Relation R in the set Z of all integers defined as

R = $\{(x, y)$: $x - y$ is as integer$\}$

Solution :

(i) $A = \{1, 2, 3 \ldots 13, 14\}$

$R = \{(x, y): 3x - y = 0\}$

$\therefore$ R = $\{(1, 3), (2, 6), (3, 9), (4, 12)\}$

R is not reflexive since $(1, 1), (2, 2) \ldots (14, 14) \notin$ R.

Also, R is not symmetric as $(1, 3) \in R$, but $(3, 1) \notin R$. $[3(3) - 1 \neq 0]$

Also, R is not transitive as $(1, 3), (3, 9) \in R$, but $(1, 9) \notin R$.

Hence, R is neither reflexive, nor symmetric, nor transitive.

(ii) $R = \{(x, y): y = x + 5 \text{ and } x < 4\} = \{(1, 6), (2, 7), (3, 8)\}$

It is seen that $(1, 1) \notin R$.

$\therefore$ R is not reflexive. Now $(1, 6) \in R$ But, $(1, 6) \notin R$.

$\therefore$ R is not symmetric. Now, since there is no pair in R such that (x, y) and $(y, z) \in R$, then (x, z) cannot belong to R. Therefore, R is not transitive.

Hence, R is neither reflexive, nor symmetric, nor transitive.

(iii) $A = \{1, 2, 3, 4, 5, 6\}$

$R = \{(x, y): y \text{ is divisible by } x\}$

We know that any number (x) is divisible by itself.

$\Rightarrow (x, x) \in R$

$\therefore$ R is reflexive. Now,

$(2, 4) \in R$ [as 4 is divisible by 2] But, $(4, 2) \notin R$. [as 2 is not divisible by 4]

$\therefore$ R is not symmetric.

Let $(x, y), (y, z) \in R$. Then, y is divisible by x and z is divisible by y. $\therefore z$ is divisible by x.

$\Rightarrow (x, z) \in R$

$\therefore$ R is transitive.

Hence, R is reflexive and transitive but not symmetric.

(iv) $R = \{(x, y): x - y \text{ is an integer}\}$

Now, for every $x \in \mathbf{Z}$, $(x, x) \in R$ as $x - x = 0$ is an integer.

$\therefore$ R is reflexive.

Now, for every $x, y \in \mathbf{Z}$ if $(x, y) \in R$, then $x - y$ is an integer.

$\Rightarrow -(x - y)$ is also an integer.

$\Rightarrow (y - x)$ is an integer.

$\therefore$ $(y, x) \in R$. Hence, R is symmetric.

Now, Let (x, y) and $(y, z) \in R$, where $x, y, z \in \mathbf{Z}$.

$\Rightarrow (x - y)$ and $(y - z)$ are integers.

$\Rightarrow x - z = (x - y) + (y - z)$ is an integer.

$\therefore$ $(x, z) \in$ R. Hence, R is transitive.

Hence, R is reflexive, symmetric, and transitive.

2. Show that the relation R in the set R of real numbers, defined as R = {(a, b): a $\leq$ b^2} is neither reflexive nor symmetric nor transitive.

Solution :

R = $\{(a, b)\text{: } a \leq b^2\}$

$$\left(\frac{1}{2},\frac{1}{2}\right) \notin \mathbf{R}\text{, since } \frac{1}{2} > \left(\frac{1}{2}\right)^2 = \frac{1}{4}$$

It can be observed that

$\therefore$R is not reflexive.

Now, (1, 4) $\in$ R as $1 < 4^2$ But, 4 is not less than 1^2.

$\therefore$ (4, 1) $\notin$ R

$\therefore$ R is not symmetric.

Now, (3, 2), (2, 1.5) $\in$ R (as $3 < 2^2 = 4$ and $2 < (1.5)^2 = 2.25$) But, $3 > (1.5)^2 = 2.25$

$\therefore$ (3, 1.5) $\notin$ R

$\therefore$ R is not transitive.

Hence, R is neither reflexive, nor symmetric, nor transitive.

1.8 Model Questions

A 1. *Do the following relations represent functions? Why?*

(a) $f : \mathbb{Z} \to \mathbb{Z}$ *defined by*

i. $f = \{(x, 1) : 2$ *divides* $x\} \cup \{(x,5) : 3 \text{ divides } x\}$.

ii. $f = \{(x, 1) : x \in S\}$ [$\{(x, -1) : x \in S^c\}$, *where* $S = \{n^2 : n \in \mathbb{Z}\}$ and $S^c = \mathbb{Z} \setminus S$.

iii. $f = \{(x, x^3) : x \in \mathbb{Z}\}$.

(b) $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f = \{(x, \pm \sqrt{x}) : x \in \mathbb{R}^+\}$, *where* $\mathbb{R}^+$ i*s the set of all positive real numbers.*

(c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f = \{(x, \sqrt{x}) : x \in \mathbb{R}\}$.

(d) $f : \mathbb{R} \to \mathbb{C}$ defined by $f = \{(\text{x}, \sqrt{x}) : x \in \mathbb{R}\}$.

(e) $f : \mathbb{R}^- \to \mathbb{R}$ defined by $f = \{(x, \log_e |x|) : x \in \mathbb{R}^-\}$, where $\mathbb{R}^-$ is the set of all negative real numbers.

(f) $f : \mathbb{R} \to \mathbb{R}$ defined by $f = \{(x, \tan x) : x \in \mathbb{R}\}$.

2. Let $f : X \to Y$ be a function. Then f^{-1} is a relation from Y to X. Show that the following results hold for f^{-1} :

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ for all $A, B \subseteq Y$.

(b) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$ for all $A, B \subseteq Y$.

(c) $f^{-1}(\varnothing) = \varnothing$.

(d) $f^{-1}(Y) = X$.

(e) $f^{-1}(Y \setminus B) = X \setminus (f^{-1}(\mathrm{B}))$ for each $B \subseteq Y$.

3. Let $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1, x \geq 0\}$. It is a relation from $\mathbb{R}$ to $\mathbb{R}$. Draw a picture of the inverse of this relation.

B Determine the equivalence relation among the relations given below. Further, for each equivalence relation, determine its equivalence classes.

1. $R = \{(a, b) \in \mathbb{Z}^2 : a \leq \mathrm{b}\}$ on $\mathbb{Z}$.

2. $R = \{(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^* : a$ divides $b\}$ on $\mathbb{Z}^*$, where $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

3. Recall the greatest integer function $f : \mathbb{R} \to \mathbb{Z}$ given by $f(x) = [x]$ and let $\mathbb{R} = \{(a, b) \in \mathbb{R} \times \mathbb{R} : [a] = [b]\}$ on $\mathbb{R}$.

4. For $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ and $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, let

(a) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : x_1^2 + x_2^2 = y_1^2 + y_2^2 \}$.

(b) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : x = \alpha y$ for some $\alpha \in \mathbb{R}^*\}$.

(c) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : 4x_1^2 + 9x_2^2 = 4y_1^2 + 9y_2^2\}$.

(d) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : x - y = \alpha(1, 1)$ for some $\alpha \in \mathbb{R}^*\}$.

(e) Fix $c \in \mathbb{R}$. Now, define $\mathbb{R} = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : y_2 - x_2 = c(y_1 - x_1)\}$.

(f) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : |x_1| + |x_2| = \alpha(|y_1| + |y_2|)\}$, for some number $\alpha \in \mathbb{R}^+$.

(g) $R = \{(x, y) \in \mathbb{R}^2 \times \mathbb{R}^2 : x_1 x_2 = y_1 y_2\}$.

5. For $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$, let $S = \{x \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$. Then, are the relations given below an equivalence relation on S?

(a) $R = \{(x, y) \in S \times S : x_1 = y_1, x_2 = -y_2\}$.

(b) $R = \{(x, y) \in S \times S : x = -y\}$.

6. Let f, g be two equivalence relations on $\mathbb{R}$. Then, prove/disprove the following statements.

(a) $f \circ g$ is necessarily an equivalence relation.

(b) $f \cap g$ is necessarily an equivalence relation.

(c) $f \cup g$ is necessarily an equivalence relation.

(d) $f \cup g^c$ is necessarily an equivalence relation. ($g^c = (\mathbb{R} \times \mathbb{R}) \setminus g$)

7 a. Find an example of two nonempty sets A and B for which $A \times B = B \times A$ is true.

b. Prove $A \cup \phi = A$ and $A \cap \phi = \phi$.

c. Prove $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

d. Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

e. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

f. Prove $A \subset B$ if and only if $A \cap B = A$.

g. Prove $(A \cap B)' = A' \cup B'$.

h. Prove $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

i. Prove $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

j. Prove $(A \cap B) \setminus B = \phi$.

k. Prove $(A \cup B) \setminus B = A \setminus B$.

l. Prove $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

m. Prove $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

n. Prove $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

8. Prove the relation defined on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ is an equivalence relation.

9. Let $f : A \to B$ and $g : B \to C$ be maps.

(a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.

(b) If $g \circ f$ is onto, show that g is onto.

(c) If $g \circ f$ is one-to-one, show that f is one-to-one.

(d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.

(e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

10. Define a function on the real numbers by

$$f(x) = \frac{x+1}{x-1}$$

What are the domain and range of f? What is the inverse of f ? Compute $f \circ f^{-1}$ and $f^{-1} \circ f$.

11. Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$.

(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Give an example in which equality fails.

(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(e) Prove $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

12. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$

(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

13. Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. Show that $\sim$ is reflexive and transitive but not symmetric.

14. Show that an $m \times n$ matrix gives rise to a well-defined map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Unit - 2 ❑ Introduction to Groups

Structure

2.1 Objectives

The followings are discussed here :

- Definition of binary operation along with examples
- Definition of group
- Basic properties of group
- Definition of subgroups, centralizer, normalizer, center of a group
- Order of a group and order of an element

2.2 Introduction

Group theory, in modern algebra, is the study of groups, which are systems consisting of a set of elements and a binary operation that can be applied to two elements of the set, which together satisfy certain axioms. Groups are vital to modern algebra; their basic structure can be found in many mathematical phenomena. Groups can be found in geometry, representing phenomena such as symmetry and certain types of transformations. In this unit, we introduce the concept of group and subgroup and demonstrate this concept through some examples.

2.3 Binary Operation

Definition 2.3.1 : Let S be a set. The the binary operation * on S is a map

$$* : S \times S \to \mathrm{S}\ (x, y) \to x * y.$$

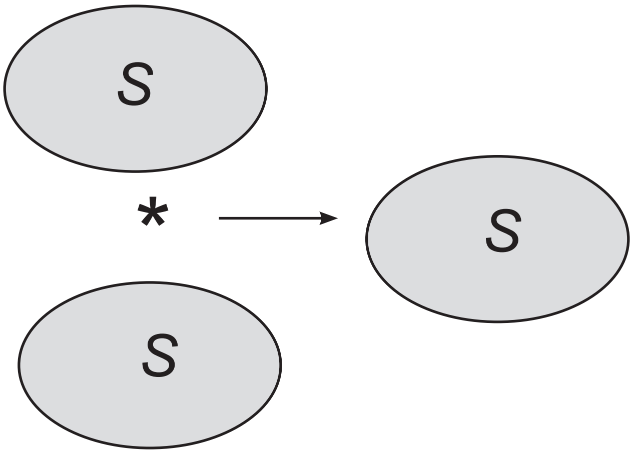


Fig. 2.1 : **Binary operation on *S*.**

Example 2.3.2 : The arithmetic operations +,−,×, ... are binary operations on suitable sets of numbers such as $\mathbb{R}$, $\mathbb{Q}$ etc.

Example 2.3.3 : Matrix addition and multiplication are binary operations on the set of all $n \times n$ matrices.

Example 2.3.4 : Vector addition and subtraction are binary operations on $\mathbb{R}^n$.

Example 2.3.5 : The vector product, or cross product, $(a, b, c) \times (x, y, z) = (bz - cy, cx - az, ay - bx)$ is a binary operation on $\mathbb{R}^3$.

Example 2.3.6 : Composition of symmetries is a binary operation on the set of symmetries of a triangle, square, cube,...

In the definition of binary operation, for any two elements from a set, the element produced by applying binary operation on them is also an element of the same set, i.e., $a * b \in S$ whenever $a \in S$ and $b \in S$. This property is sometimes expressed as : S **is closed with respect to** '$*$'. The notion becomes important when we consider restricting a binary operation to subsets of the set on which it was originally defined.

Let T be a subset of S and S is closed under the binary operation *. Then $T \times T \subset S \times S$. Now we consider the restriction of the map $* : S \times S \rightarrow S$ to $T \times T$. Then it is not always true that for any $x * y \in T$ whenever $x, y \in T$.

For example, take $S = \mathbb{N}$ and define a binary operation * on S as follows :

for any

$$n * m = n + m + 1 \quad \text{for any } n, m \in S.$$

Then S is closed under *. But if we consider the set of even number $E \subset S$, then E is not closed under the restricted binary operation * from S. Hence, we say the following definition :

Definition 2.3.7 : Let the set S is closed under the binary operation *. Then we say that a subset T of S is closed under the restricted binary operation *

if

$$x * y \in T \quad \text{whenever } x, y \in T.$$

Example 2.3.8 : The set of all non-singular (non-zero determinant) $n \times n$ real matrices is denoted by $GL(n, \mathbb{R})$. Now this set $GL(n, \mathbb{R})$ closed under matrix multiplication. Again, consider the subset $SL(n, \mathbb{R})$ of $GL(n, \mathbb{R})$, the of all matrices whose determinant is 1. This subset is also closed under matrix multiplication.

Example 2.3.9 : Let C be the set of all concentric circles with center at the origin. A circle in C with radius r is denoted by a_r. Now the binary operation is defined by

$$a_r * a_t = a_{r+t} .$$

The set C is closed under the binary operation *.

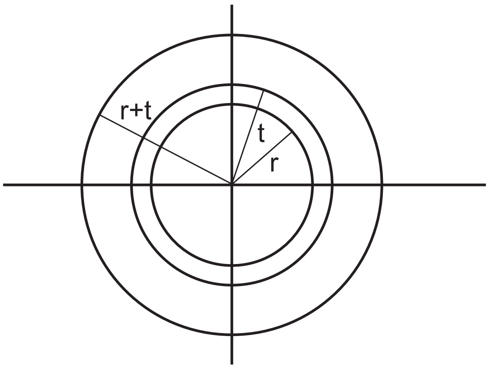


***Fig. 2.2* : Binary operation on concentric circles**

Binary operation can also be imposed on real life objects, see the following example:

Example 2.3.10 : Let A be the set of all students in a class. Now define the binary operation on A as follows: for any $x, y \in A$,

$$x * y = \begin{cases} x & \text{if age of } x \geq \text{age of } y \\ y & \text{otherwise} \end{cases}$$

Definition 2.3.11 : A binary operation * on a set S is said to be commutative if $x * y = y * x$ for all $x, y \in S$.

In general binary operation may not be commutative, see the following example:

Example 2.3.12 : Let $M(n, \mathbb{R})$ be the set of all real $n \times n$ matrices. The binary operation addition is commutative on M (n, $\mathbb{R}$). But the binary operation multiplication is not commutative on M (n, $\mathbb{R}$).

2.4 Definition of Group

Definition 2.4.1 : Let G be a non-empty set * be a binary operation defined in such a way that the following four rules are true :

1. * is closed in G, i.e., if $a, b \in G$ then $a * b \in G$.
2. * is associative, i.e., $a * (b * c) = (a * b) * c$ for $a, b, c \in G$.
3. G contains an identity element e, i.e.,
$$a * e = e * a = a \text{ for all } a \in G.$$
4. Inverse exists in G, i.e., for any $a \in G$ there exists an inverse element $a' \in G$ such that
$$a * a' = a' * a = e.$$

Then the pair (G, *) is called a group with the binary operation &.

In multiplicative notation the inverse of an element a is denoted by a^{-1}. If G is commutative with respect to the binary operation *, then (G, *) is called the abelian group.

Example 2.4.2 : The set of real numbers $\mathbb{R}$, integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, complex numbers $\mathbb{C}$ forms a group under the binary operation '+'. The identity element is 0 and for each element x, the inverse is $-x$.

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

Table 2.1 : Multiplication table

Example 2.4.3 : The set of all $m \times n$ real matrix is denoted by M (m, n). Then M (m, n) forms a group under matrix addition. Hence, the identity element is the zero matrix. This is an abelian group.

Example 2.4.4 : The set $GL(n, \mathbb{R})$ forms a group under matrix multiplication. Let A, $B \in \mathrm{GL}(n, \mathbb{R})$. Then $det\ (A) \neq 0$ and $det\ (B) \neq 0$. Now $det\ (AB) = det\ (A) * \det\ (B) \neq 0$. Hence, $A * B \in GL(n, \mathbb{R})$. The matrix multiplication is associative. The identity matrix In acts as identity element. For any element $A \in GL(n, \mathbb{R})$, the inverse is A^{-1}. Hence, $GL(n, \mathbb{R})$ is a group under matrix multiplication. But this group is not abelian, since matrix multiplication is not commutative.

Example 2.4.5 : Let $G = \{e, a, b, c\}$ with multiplication as defined by the table 2.1 From the table, we observe that

1. G is closed under composition.
2. e is the identity element.
3. $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$ and $c^{-1} = c$.
4. the multiplication is commutative.

It can be checked that the multiplication is associative. Thus, $(G,*)$ is anabelian group. This group is called Klein's 4-group. The multiplication table 2.1 is known as Cayley table of a group.

Example 2.4.6 : The set $C[a, b]$ is the set of all continuous functions on $[a, b]$. Let f, $g \in C[a, b]$. The binary operation + defined by

$$(f + g)(x) = f(x) + g(x)\ \forall x \in [a, b].$$

Then $f + g$ is also continuous. The binary operation + is also associative. The identity function i is the identity element and for any $f \in C[a, b]$, the inverse is $-f$. Therefore, $C\,[a, b]$ forms a group under addition +. In fact it abelian.

Example 2.4.7 : In the Euclidean plane, let G_p be the set of all rotations about a fixed point p. If two rotations differ by a multiple of 2π then we say that they are equal. If α and β are two elements of G_P then α o β is the rotation obtained by first applying β and then applying α. Thus, G_P is closed under composition. Again functional composition is associative. An identity element of G_P is the rotation of 0°. Each rotation has an inverse : rotation of the same magnitude in the opposite direction. Finally, as an operation on G_P , composition is commutative. Therefore, G_P is a group with respect to the rotation about the point p.

Example 2.4.8 : The subset $\{1,-1, i,-i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, whereas the ainverse of i is $-i$, and vice versa.

Example 2.4.9 : In the example 2.3.7, the set C does not form a group under the given binary operation as the inverse of any non-zero element does not exists (why?).

Example 2.4.10 : The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} * \sqrt{2} = 2$, so S is not closed under multiplication.

Example 2.4.11 : The set $\mathbb{Z}n = \{1, 2, ..., n - 1\}$ for $n \geq 1$ is group under integer modulo n. For any $j > 0$ in $\mathbb{Z}n$, the inverse of j is $n - j$. This group is called *integer modulo n* group.

Example 2.4.12 : For $n > 1$, we define $U(n)$, to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n.

For $n = 10$, we have $U(10) = \{1, 3, 7, 9\}$. The Cayley table for $U(10)$ is

Mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Table 2.2

(Recall that ab mod n is the unique integer r with the property $a.b = nq + r$, where $0 \le r < n$ and $a.b$ is ordinary multiplication.) In the case that n is prime, then $U(n) = \{1, 2, ..., n - 1\}$.

In his classic book *Lehrbuch der Algebra*, published in 1895, Heinrich Weber gave an extensive treatment of the groups $U(n)$ and described them as the most important examples of finite Abelian groups.

Example 2.4.13 : Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ $K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, where $i^2 = -1$. Then the relations $I^2 = J^2 = K^2 = -1$, $IJ = K, JK = I, KI = J, JI = -K, KJ = -I, IK = -J$ hold. The set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is a group called the quaternion group. Notice that Q_8 is non-abelian.

Example 2.4.14 : Let $\mathbb{C}^*$ be the set of nonzero complex numbers. Under the operation of multiplication $\mathbb{C}^*$ forms a group. The identity is 1. If $z = a + ib$ is a nonzero complex number, then

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

is the inverse of z. It is easy to see that the remaining group axioms hold.

Example 2.4.15 : (Direct product of groups). Let $(G_1, *_1), \dots (G_n, *_n)$ be groups. Then the direct product $G = G_1 \times G_2 \times \dots \times G_n$ is the set of n-tuples $(g_1, g_2, \dots, g_n)$ where $g_i \in G_i$ with operation defined componentwise :

$$(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n).$$

It is a routine checkup that $G = (G_1, *_1) \times \dots \times (G_n, *_n)$ forms a group under the binary operation defined above.

2.5 Basic properties of groups

Proposition 2.5.1 : *The identity element e of a group is unique, i.e., there exists only one e such that $ex = xe = x$ for all $x \in G$.*

Proof. Suppose both e and e' are the identity element. Then $xe = ex = x$ and $xe' = e'x = x$ for all $x \in G$. We need to show that $e = e'$. If we think e as identity then $ee' = e'$ and if we think e' as identity, then $ee' = e'$. Therefore, combining them we get $e = e'$. □

Similarly we can say that

Proposition 2.5.2 : *Inverse of an element is also unique.*

Proof. Let g' and g'' be two identity elements of g. Then $g'g = e$ and $g''g = e$. We want to show that $g' = g''$. Now $g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''$. Hence, $g' = g''$. □

Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
R*	Multiplication	1	x	$1/x$	Yes
C*	Multiplication	1	$a + bi$	$\frac{1}{a^2+b^2}a - \frac{1}{a^2-b^2}bi$	Yes
$GL(2,F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, gcd $(k, n) = 1$	Solution to kx mod n=1	Yes
R^n	Componentwise addition	(0,0, ...,0)	$(a_1, a_2, ..., a_3)$	$(-a_1, -a_2, ..., -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - a}$, L	No

Fig. 2.3

Proposition 2.5.3 : Let G be a group. then for any two elements $a, b \in G$, $(ab)^{-1} = b^{-1} a^{-1}$.

Proof. Let $a, b \in G$. Then $abb^{-1} a^{-1} = aea^{-1} = e$. Similarly, $b^{-1} a^{-1} ab = e$. Therefore, $(ab)^{-1} = b^{-1} a^{-1}$. □

Proposition 2.5.4 : In a group G, right and left cancellation law holds, i.e., $ba = bc$ implies $a = c$ and $ab = cb$ implies $a = c$.

Proof. Taking inverse of b in both sides of $ba = bc$ we get

$$b^{-1} ba = b^{-1} bc =) ea = ec.$$

which implies that $a = c$. The right cancellation can be proved similarly. □

Definition 2.5.5 : (Order of a Group). The number of elements of a group G (finite or infinite) is called the order of the group G and it is denoted by $|G|$.

Example 2.5.6 : The group of integers $\mathbb{Z}$ under addition is of infinite order.

Example 2.5.7 : The group $\mathbb{Z}_{10}$ is of order 10. The group $U(7)$ is of order 6.

Definition 2.5.8 : (Order of an element). The order of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$). If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

Example 2.5.9 : Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. under multiplication modulo 15. This group has order 8. Then for any element, say 7, $7^1 = 7$, $7^2 = 4$, $7^3 = 13$, $7^4 = 1$. Hence, the order of 7 is 4. Similarly, the order of 11 is 2.

Example 2.9.10 : The order of Q_8 is 8. In this group order of each element, except identity, are of order 4.

Proposition 2.5.11 : Let G be a group and g be an element of order m. Then $g^i \neq g^j$ for $i \neq j$ and $1 \leq i, j \leq m$. And if g is of infinite order, then all the elements $g, g^2, ..., g^n, ...$ are distinct.

Proof. For the first proof let us assume that $g^i = g^j$ for some $i \neq j$ and $1 \leq i, j \leq m$. Suppose $i < j$, then $g^{j-i} = e$. But $j - i < n$. Which contradicts that $|g| = n$. Hence, our assumption is wrong.

For the second proof, suppose $g^i = g^j$ for some $i, j \geq 1$ and $i \neq j$. Assume that $j > i$, then it implies that $g^{j-i} = e$. Which contradicts that g has infinite order.

The question naturally arises :

Given a set A, can we define a binary operation on A which makes A a group?.

In case of empty set it is not possible. But in case of non-empty set, fortunately, this question has an affirmative answer if we assume the *Axiom of Choice*[1] (which is done in most of mainstream mathematics, but may not be done in the more foundational parts). To answer this first we need to prove the following theorem:

Theorem 2.5.12 : Let A be a non-empty set and G be a group such that there exists a bijection $f : A \to G$. Then a group structure can be defined on A.

Proof. First we define a binary operation on A. Let $a, b \in A$. Then the binary operation $a * b$ on A is defined by

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

Since f is a bijection, this binary operation is well-defined. It is clear that A is closed under the binary operation *. The operation is associative since G is a group and f is a bijection. Let $e_{\text{A}} = f^{-1}(e)$, e be the identity element of G. Then for any $a \in A$.

$$a * e_{\text{A}} = f^{-1}(f(\text{a})f(e_{\text{A}})) = f^{-1}(f(a)e) = f^{-1}(f(a)) = a = e_{\text{A}} * a.$$

Which shows that $e_{\text{A}}$is the identity element in A. Now what is the inverse of an element $a \in A$? The inverse is $a' = f^{-1}(f(a)^{-1})$. Here $f(a)^{-1}$ means inverse of the element $f(a)$ in the group G. Then

$$\begin{aligned} a * a' &= f^{-1}(f(a)f(a')) \\ &= f^{-1}(f(a)f(f^{-1}(f(a)^{-1}))) \\ &= f^{-1}(f(a)f(a)^{-1}) \\ &= f^{-1}(e) = e_{\text{A}}. \end{aligned}$$

Similarly, we can show that $a' * a = e_{\text{A}}$. Therefore, e_{A} is the identity element of A. Thus $(A, *)$ is a group.

Now come to our main question. If A is finite, having n-number of elements, then there is a bijection between A and $\mathbb{Z}_n$. Then by the above theorem, A can be given a group structure. If A is countably infinite, then A forms a group under the binary operation which can be constructed from the bijection between A and $\mathbb{Z}$. And in case when A is uncountable, the same thing can also be done by the bijection between A and R.

2.6 Subgroups

Sometimes we wish to investigate smaller groups sitting inside a larger group. The set of even integers $2\mathbb{Z} = \{...-2, 0, 2, 4...\}$ is a group under the operation of addition. This smaller group sits naturally inside of the group of integers under addition.

[1] The Axiom of Choice states that for any family of nonempty disjoint sets, there exists a set that consists of exactly one element from each element of the family.

Definition 2.6.1 : We define a **subgroup** *H* of a group *G* to be a subset *H* of *G* such that when the group operation of *G* is restricted to *H*, *H* is a group in its own right.

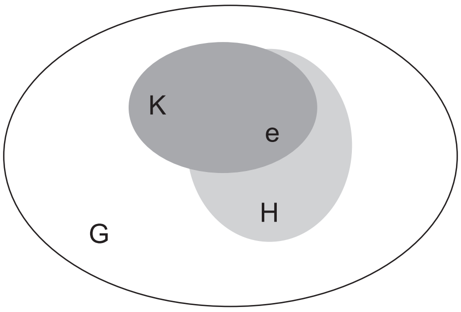


Fig. 2.4 **: Group G with two subgroups H and K**

Observe that every group *G* with at least two elements will always have at least two subgroups, the subgroup consisting of the identity element alone and the entire group itself. The subgroup $H = \{e\}$ of a group *G* is called the trivial subgroup. A subgroup that is a proper subset of *G* is called a proper subgroup. In many of the examples that we have investigated up to this point, there exist other subgroups besides the trivial and improper subgroups. The set of rationals $\mathbb{Q}$, the set of integers $\mathbb{Z}$ are subgroups of $\mathbb{R}$ under addition.

Example 2.6.2 : The set of non-zero complex numbers $\mathbb{C}^*$ is a group under multiplication and also the set $H = \{\pm 1, \pm i\}$ is also a group under multiplication. Since $H \subset \mathbb{C}^*$, *H* is a subgroup of $\mathbb{C}^*$.

Example 2.6.3 : The set of all 2 × 2-matrix with determinant 1 is the set

$$SL(2, \mathbb{R}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1\right\}$$

Then $SL(2, \mathbb{R})$ closed under multiplication, since for $A, B \in SL(2, \mathbb{R})$ implies $AB \in SL(2, \mathbb{R})$ as $det\,(AB) = 1$.

Since the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has determinant 1, *I* is the identity element for $SL(2, \mathbb{R})$. For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$, the inverse is $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ which also belongs to $SL(2, \mathbb{R})$. Therefore, $SL\,(2, \mathbb{R})$ is a group under matrix multiplication. Also $SL(2, \mathbb{R}) \subset GL\,(2, \mathbb{R})$, so $SL(2, \mathbb{R})$ is a subgroup of $GL(2, \mathbb{R})$.

Theorem 2.6.4 : (Two-steps test). Let G be a group and H be a non-empty subset of G. If $ab \in G$ whenever $a, b \in G$ and $a^{-1} \in H$ whenever $a \in H$, then H is a subgroup of G.

Proof. Since H is a subset of G and G is a group, the binary operation on H is associative. Let $a \in H$. Then $a^{-1} \in H$ from the hypothesis. Now $aa^{-1} = e \in H$. Hence, H contains the identity element. Also from the hypothesis inverse of each element of H exists in H. So, H is a subgroup of G.

Theorem 2.6.5 : (One-steps test). Let G be a group and H be a non-empty subset of G. If $ab^{-1} \in G$ whenever $a, b \in G$, then H is a subgroup of G.

Proof. Let $a, b \in H$. Then by the hypothesis $ab^{-1} \in H$ also $ba^{-1} \in H$. Now

$$e = (ab^{-1})(ba^{-1}) \in H,$$

So, H contains identity element. Also for a $\in H$, a^{-1} belongs to H, since $a^{-1} = \mathrm{ea}^{-1}$. Which implies that $ab = a(b^{-1})^{-1} \in H$ for $anb \in H$. Therefore, H is a subgroup of G.

Example 2.6.6 : For any $a \in G$. The set $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G. For any $p, q \in \langle a \rangle$, $p = a^k$ and $q = a^t$ for some $k, t \in \mathbb{Z}$. Now $pq^{-1} = a^k a^{-t} = ak^{-t} \in \langle a \rangle$. So, by the above theorem it is proved that hai is a subgroup of G. In fact this group is generated by one element a. This type of group is called cyclic group and it will be discussed in detail in next chapter.

Example 2.6.7 : Let G be a group of non-zero real numbers under multiplication,

$$H = \{x \in G : x = 1 \text{ or } x \text{ is irrational}\} \text{ and}$$

$$K = \{x \in G : x \geq 1\}.$$

Now H is not a subgroup of G since $\sqrt{2} \in H$ but $\sqrt{2} . \sqrt{2} \notin H$. Similarly, it can be shown that K is also not a subgroup of G.

Example 2.6.8 : (Centralizer of an element). Let G be a group and $a \in G$. Now consider the set

$$C_a = \{x \in G : xa = ax\}.$$

This set is non-empty, since $ea = ae$. Let $x, y \in C_a$. Then $xa = ax$ and $ya = ay$. Now

$$\begin{aligned}(xy^{-1})\, a\, (xy^{-1})^{-1} &= xy^{-1}\, ayx^{-1} \\ &= x(y^{-1} y)\, ax^{-1} \\ &= axx^{-1} = a.\end{aligned}$$

Which implies that

$$(xy^{-1})\, a = a\, (xy^{-1}).$$

Therefore, $xy^{-1} \in C_a$, whenever $x, y \in C_a$. So, C_a is a subgroup of G. This subgroup is called centralizer of a.

Example 2.6.9 : (Center of a group). The center of a group G is defined by

$$Z(G) = \{a \in G : ax = xa \; \forall x \in G\}.$$

Now $Z(G) \neq \phi$, since $e \in Z(G)$. By using the same arguments of the above example it can be proved that $Z(G)$ is a subgroup of G (Complete the proof). This group in fact is the largest abelian subgroup of G. If G is abelian, then $Z(G) = G$.

Example 2.6.10 : (Normalizer of a subgroup). Let H be a subgroup of G. Now consider the set

$$N(H) = \{x \in G : xHx^{-1} \subseteq H\} = \{x \in G : xhx^{-1} \in H \; \forall h \in H\}.$$

Now $e \in N(H)$. Let $x, y \in N(H)$. Then $xhx^{-1} \in H$ and $yhy^{-1} \in H$ for all $h \in H$. Now for all $h \in H$,

$$\begin{aligned}(xy)\,h\,(xy)^{-1} &= (xy)\,h\,(y^{-1}x^{-1})\\ &= x\,(yhy^{-1})\,x^{-1}\\ &= xh_1x^{-1} \in H\end{aligned}$$

Thus $xy \in N(H)$, whenever $x, y \in N(H)$. Again $x^{-1}\,h\,(x^{-1})^{-1} = x^{-1}hx = (xh^{-1}\,x^{-1})^{-1} = h'^{-1} \in H$, since $xh^{-1}x^{-1} \in H$. Therefore, $x^{-1} \in N(H)$ for $x \in N(H)$. Hence, $N(H)$ is a subgroup of G. This group is called normalizer of H in G.

Proposition 2.6.11 : Let H and K be two subgroups of G. Then $H \cap K$ is also a subgroup of G.

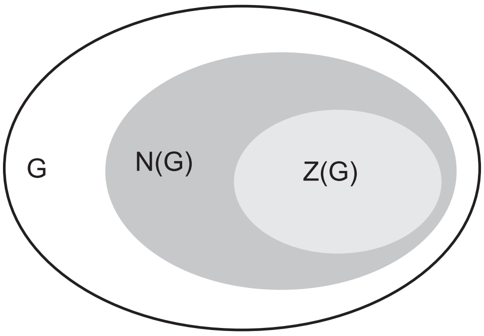


***Fig. 2.5*: Group, Normal subgroup and center of a group**

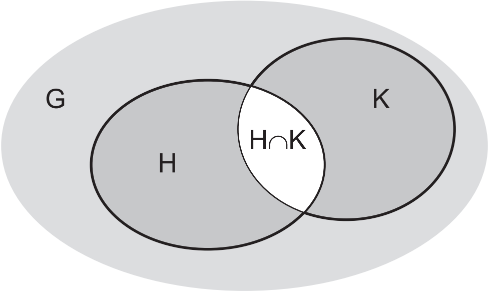


***Fig. 2.6* : Intersection of two subgroups**

Proof. Since H and K are two subgroups of G, $H \cap K$ contains the identity element e. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Hence, $ab^{-1} \in H$ and $ab^{-1} \in K$. Which implies that $ab^{-1} \in H \cap K$. Therefore, $H \cap K$ is a subgroup of G. □

The above theorem can also be extend in case of finite sum, i.e., if $H_1, H_2, ..., H_n$ are subgroups of G, then $\bigcap_{i=1}^{i=n} H_i$ is also a subgroup of G. Can we extend this theorem in case of infinite sum? Yes it is possible and the proof is same as the finite one.

Union of two subgroups may not be a subgroup. For example let $G = \mathbb{Z}$. Then $3\mathbb{Z}$ and $5\mathbb{Z}$ are subgroups of $\mathbb{Z}$. Now $3 \in 3\mathbb{Z} \cup 5\mathbb{Z}$ and $5 \in 3\mathbb{Z} \cap 5\mathbb{Z}$. But $3 + 5 = 8 \notin 3\mathbb{Z} \cap 5\mathbb{Z}$.

2.7 Summary

In this unit, we have mainly studied the concept of group along with various kinds of subgroups such as normalizer of a group, centralizer of a group. We have seen that the examples of groups are abundance in nature.

2.8 Worked examples

1. Let x and y be elements in a group G such that $xy \in Z(G)$. Prove that $xy = yx$.

Solution : Since $xy = x^{-1}x(xy)$ and $xy \in Z(G)$, we have $xy = x^{-1}x(xy) = x^{-1}(xy)x = (x^{-1}x)$ $yx = yx$.

2. Let G be a group with exactly 4 elements. Prove that G is Abelian.

Solution : Let a and b be non identity elements of G. Then e, a, b, ab, and ba are elements of G. Since G has exactly 4 elements, $ab = ba$. Thus, G is Abelian.

3. Let a be an element in a group. Prove that $(a^n)^{-1} = (a^{-1})^n$ for each $n \geq 1$.

Solution : We use Math. induction on n. For $n = 1$, the claim is clearly valid. Hence, assume that $(a^n)^{-1} = (a^{-1})^n$. Now, we need to prove the claim for $n + 1$. Thus, $(a^{n+1})^{-1} = (aa^n)^{-1} = (a^n)^{-1}\, a^{-1} = (a^{-1})^n\, a^{-1} = (a^{-1})^{n+1}$.

4. Let H and D be two subgroups of a group such that neither $H \subset D$ nor $D \subset H$. Prove that $H \cup D$ is never a group.

Solution : Deny. Let $a \in H \setminus D$ and let $b \in D \setminus H$. Hence, $ab \in H$ or $ab \in D$. Suppose that $ab = h \in H$. Then $b = a^{-1}h \in H$, a contradiction. In a similar argument, if $ab \in D$, then we will reach a contradiction. Thus, $ab \notin H \cup D$. Hence, our denial is invalid. Therefore, $H \cup$ D is never a group.

5. Give an example of a subset of a group that satisfies all group-axioms except closure.

Solution : Let $H = 3Z$ and $D = 5Z$. Then H and D are subgroups of Z. Now, let $C = H \cup D$. Then by the previous question, C is never a group since it is not closed.

6. Let $H = \{a \in Q : a = 3^n\, 8^m$ for some n and m in Z}. Prove that H under multiplication is a subgroup of $Q \setminus \{0\}$.

Solution : Let $a, b \in H$. Then $a = 3^{n1}\, 8^{n2}$ and b $= 3^{m1}\, 8^{m2}$ for some $n_1, n_2, m_1, m_2 \in Z$. Now, $a^{-1}\, b = 3^{m1 - n1}\, 8^{\,m2 - n2} \in H$. Thus, H is a subgroup of $Q \setminus \{0\}$ by Theorem 12..29..71.

7. Let a, x be elements in a group G. Prove that $ax = xa$ if and only if $a^{-1}x = xa^{-1}$.

Solution : Suppose that $ax = xa$. Then $a^{-1}x = a^{-1}xaa^{-1} = a^{-1}axa^{-1} = exa^{-1} = xa^{-1}$. Conversely, suppose that $a^{-1}x = xa^{-1}$. Then $ax = axa^{-1}a = aa^{-1}xa = exa = xa$.

8. Let $H = \{x \in C : x^{301} = 1\}$. Prove that H is a subgroup of C $\setminus$ {0} under multiplication.

Solution : First, observe that H is a finite set with exactly 301 elements. Let $a, b \in H$. Then $(ab)^{301} = a^{301}b^{301} = 1$. Hence, $ab \in H$. Thus, H is closed. Hence, H is a subgroup of $C \setminus \{0\}$.

9. Let $H = \{A \in GL(608, Z_{89})$: det(A) = 1}. Prove that H is a subgroup of GL(608, Z_{89}).

Solution : First observe that H is a finite set. Let $C, D \in H$. Then $det(CD) = det(C)\, det(D) = 1$. Thus, $CD \in H$. Hence, H is closed. Thus, H is a subgroup of $GL(608, Z_{89})$.

10. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(a\, .\, b)^n = a^n\, .\, b^n$.

Solution : We resort to induction to prove that the result holds for positive integers. For $n = 1$, we have $(a\, .\, b)^1 = a\, .\, b = a^1\, .\, b^1$. So the result is valid for the base case. Suppose result holds for $n = k - 1$, i.e. $(a\, .\, b)^{k-1} = a^{k-1}\, .\, b^{k-1}$.

We need to show result also holds good for $n = k$. We have

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

So the result holds for $n = k$ too. Therefore, result holds for all $n \in \mathbb{N}$. Next suppose $n \in \mathbb{Z}$. If $n = 0$, then $(a.b)^0 = e$ where e the identity element. Therefore $(a \,.\, b)^0 = e = e \,.\, e = a^0 \,.\, b^0$. So the result is valid for $n = 0$ too. Next suppose n is a negative integer. So $n = -m$, where m is some positive integer. We have

$$\begin{aligned} (a \,.\, b)^n &= (a \,.\, b)^{-m} \\ &= ((a \,.\, b)^{-1})^m \text{ by definition of the notation} \\ &= (b^{-1} \,.\, a^{-1})^m \\ &= ((a^{-1}) \,.\, (b^{-1}))^m \\ &= (a^{-1})^m \,.\, (b^{-1})m \text{ as the result is valid for positive integers} \\ &= (a^{-m}) \,.\, (b^{-m}) \\ &= a^n \,.\, b^n \end{aligned}$$

So the result is valid for negative integers too. Hence the result that $(a \,.\, b)^n = a^n \,.\, b^n$ holds in an abelian group for all $n \in \mathbb{Z}$.

11. If G is a group in which $(a \,.\, b)^i = a^i \,.\, b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

Solution : Let n, n+1, n+2 be some three consecutive integers. Therefore we have

$$(a \,.\, b)^n = a^n \,.\, b^n \qquad (1)$$

$$(a \,.\, b)^{n+1} = a^{n+1} \,.\, b^{n+1} \qquad (2)$$

$$(a \,.\, b)^{n+2} = a^{n+2} \,.\, b^{n+2} \qquad (3)$$

Using (2) we have

$$\begin{aligned} & (a \,.\, b)^{n+1} = a^{n+1} \,.\, b^{n+1} \\ \Rightarrow\; & (a \,.\, b)^n \,.\, (a \,.\, b) = a^{n+1} \,.\, (b^n \,.\, b) \\ \Rightarrow\; & (a^n \,.\, b^n) \,.\, (a \,.\, b) = (a^{n+1} \,.\, b^n) \,.\, b, \text{ Using (1)} \\ \Rightarrow\; & ((a^n \,.\, b^n) \,.\, a) \,.\, b = (a^{n+1} \,.\, b^n) \,.\, b \end{aligned}$$

$$\Rightarrow \; (a^n \,.\, b^n) \,.\, a = (a^n \,.\, a) \,.\, b^n$$

$$\Rightarrow \; a^n \,.\, (b^n \,.\, a) = a^n \,.\, (a \,.\, b^n)$$

$$\Rightarrow \; b^n \,.\, a = a \,.\, b^n \qquad (4)$$

Again using (3), analogously we have

$$b^{n+1} \,.\, a = a \,.\, b^{n+1}$$

$$\Rightarrow \; b \,.\, (b^n \,.\, a) = a \,.\, b^{n+1}$$

$$\Rightarrow \; b \,.\, (a \,.\, b^n) = a \,.\, b^{n+1}, \text{ Using (4)}$$

$$\Rightarrow \; (b \,.\, a) \,.\, b^n = (a \,.\, b) \,.\, b^n$$

$$\Rightarrow \; b \,.\, a = a \,.\, b$$

So we have $a \,.\, b = b \,.\, a \; \forall \; a, b \in G$. And hence G is abelian.

12. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

Solution : We prove the result by contradiction. Note that G is a finite group. Suppose there is no element x satisfying $x^2 = e$ except for $x = e$. Thus if some $g \neq e$ belongs to G, then $g^2 \neq e$, i.e. $g \neq g^{-1}$. It means every non-identity element g has another element g^{-1} associated with it. So the non-identity elements can be paired into mutually disjoint subsets of order 2. We can assume the count of these subsets equals to some positive integer n as G is a finite group. But then counting the number of elements of G, we have $o(G) = 2n + 1$, where 1 is added for the identity element. So G is a group of odd order, which is not true. Hence there must exist an element $a \neq e$ such that $a^2 = e$ for G is a group of even order.

13. Let : P be the set of all real numbers except the integer 1. Let the operation '$*$' be defined by $a * b = a + b - ab$ for all $a, b \in P$. Show that $(P,*)$ is a group.

Solution : (i) Closure Property: Let $a, b \in P$.

So, a and b are two real numbers and $a \neq 1, b \neq 1$.

Now, $a * b = a+b - ab$ which is a real number and $a + b - ab \neq 1$, because $a + b - ab = 1 \Rightarrow b(1 - a) = 1 - a \Rightarrow b = 1$, since $a \neq 1$. But $b \neq 1$.

Therefore, $a * b$ is a real number and $a * b \neq 1$. So, $a * b \in P \; \forall \; a, b \in P$.

Hence P is closed under the binary operation '$*$'.

(ii) Associative Property : Let $a, b, c \in P$, where $a, b, c \in R$ and $a \neq 1, b \neq 1, c \neq 1$.

Now, $a * (b * c) = a * (b + c - bc) = a + b + c - bc - a\,(c + c - bc)$

$$= a + b + c - bc - ab - ac + abc$$

$(a * b) * c = (a + b - bc) * c \; = a + b - bc + c - (a + b - ab)\, c$

$$= a + b + c - ab - ac - bc + abc$$

Therefore, $a * (b * c) = (a * b) * c \ \forall\ a, b, c \in P$.

So, associative property is satisfied w.r.t. the binary operation '$*$'.

(iii) Identity Property : $0 \in P$.

Now, $0 * a = 0 + a - 0.\ a\ = a\ \forall\ a \in P$.

So 0 is the left identity element in : under the binary operation '$*$'.

(iv) Inverse Property : Let b be an element in P such that $b * a = 0$.

Now, $b * a = 0 \Rightarrow b + a - ba = 0 \Rightarrow b(1 - \mathrm{a}) = -\mathrm{a} \Rightarrow b = \dfrac{a}{a-1}$, since ≠ 1

Since $\dfrac{a}{a-1}$ is a real number as $a \neq 1$ and $\dfrac{a}{a-1} \neq 1$, so $b = \dfrac{a}{a-1} \in P$.

Therefore, for any element a in P, $\exists$ an element $\dfrac{a}{a-1}$ in P such that $\dfrac{a}{a-1} * a = 0$.

So, $\dfrac{a}{a-1}$ is the left 0-inverse in P under the binary operation '$*$'.

Therefore, $(P, *)$ is a group.

14. Let (G, o) be a group and $a, b \in G$. If o(a) = 3 and $aoboa^{-1} = b^2$, find the order of b if b is not the identity element of G.

Solution : $aoboa^{-1} = b^2 \Rightarrow a^2oboa^{-2} = aob^2oa^{-1}$

$= (aoboa^{-1})\ o\ (aoboa^{-1})$ since 'o' is associative.

$= b^2ob^2 = b^4$

$\Rightarrow a^3oboa^{-3} = aob^4oa^{-1} = (aoboa^{-1})\ \mathrm{o}\ (aoboa^{-1})\ \mathrm{o}\ (aoboa^{-1})\ \mathrm{o}\ (aoboa^{-1})$

$= b^2ob^2ob^2ob^2 = b^8$

or, $b = b^8 \Rightarrow b^7 = e$.

Since $b \neq e$ and 7 is prime, so $o\ (b) = 7$.

2.9 Model Questions

1. In each case, find the inverse of the element under the given operation.

i) 17 in $\mathbb{Z}_{20}$.

ii) 2, 7 and 8 in $U(9)$.

2. Prove that for a group G,

$$Z(G) = \bigcap_{a \in G} C_a$$

3. List all the elements of $U(20)$.
4. Let a, b be any two elements of an aleblian group and n be an integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-abelian groups?
5. Prove that a group G is abelian iff
$$(ab)^{-1} = a^{-1} b^{-1}, \forall a, b \in G.$$
6. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.
7. Prove that in a group $(ab)^2 = a^2b^2$ iff $ab = ba$.
8. Prove that if G is a group with the property that the square of every element is the identity, then G is abelian.
9. Let $a.b \in G$. Find $x \in G$ such that $xabx^{-1} = ba$.
10. For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$. [For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.] List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$. Prove that $U_{\mathrm{k}}(n)$ is a subgroup of $U(n)$. Let $H = \{x \in U(10) \mid x \bmod 3 = 1\}$. Is H a subgroup of $U(10)$?
11. Suppose that a is a group element and $a^6 = e$. What are the possibilities for |a|? Provide reasons for your answer.
12. If a is a group element and a has infinite order, prove that $a^m \neq a^n$ when $m \neq n$.
13. For any group elements a and b, prove that $|ab| = |ba|$.
14. Show that if a is an element of a group G, then $|a| \leq |G|$.
15. Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. [Hence, $U(14)$ is cyclic.] Is $U(14) = \langle 11 \rangle$?
16. Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]
17. Suppose n is an even positive integer and H is a subgroup of Z_n. Prove that either every member of H is even or exactly half of the members of H are even.
18. Let n be a positive even integer and let H be a subgroup of Z_n of odd order. Prove that every member of H is an even integer.
19. Prove that for every subgroup of D_n, either every member of the subgroup is a rotation or exactly half of the members are rotations.

20. Let H be a subgroup of D_n of odd order. Prove that every member of H is a rotation.

21. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

22. For every even integer n, show that D_n has a subgroup of order 4.

23. Suppose that H is a proper subgroup of Z under addition and H contains 18, 30, and 40. Determine H.

24. Suppose that H is a proper subgroup of Z under addition and that H contains 12, 30, and 54. What are the possibilities for H?

25. Suppose that H is a subgroup of Z under addition and that H contains 2^{50} and 3^{50}. What are the possibilities for H?

26. Prove that the dihedral group of order 6 does not have a subgroup of order 4.

27. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

28. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

29. Prove the right and left cancellation laws for a group G; that is, show that in the group G, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for elements $a, b, c \in G$.

30. Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

31. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.

32. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

33. Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$.

34. Find all the subgroups of the symmetry group of an equilateral triangle.

35. Compute the subgroups of the symmetry group of a square.

36. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}*$.

37. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

38. Let $\mathrm{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that T is a subgroup of $\mathbb{C}^*$.

39. Let G consist of the 2×2 matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $SL_2(\mathbb{R})$.

40. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Unit - 3 ❑ Cyclic Groups and Cyclic Subgroups

Structure

3.1 Objectives

The followings are discussed here:

- Definition of cyclic group
- Examples of cyclic group
- Basic properties of cyclic group
- Euler Phi function
- Roots of unity

3.2 Introduction

Cyclic group is the basic building block of group theory. In this unit we discuss the notion of cyclic group. The generators of a cyclic group is also derived. Finally, as an application of cyclic group, the circle group and the root of unity are discussed.

3.3 Definition and examples

Definition 3.3.1 : A group G is called cyclic if there exists an element $g \in G$ such that

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

The element g is called the generator of G. The generator may not be unique. If G is cyclic and generated by g then G can be written as $\langle g \rangle$.

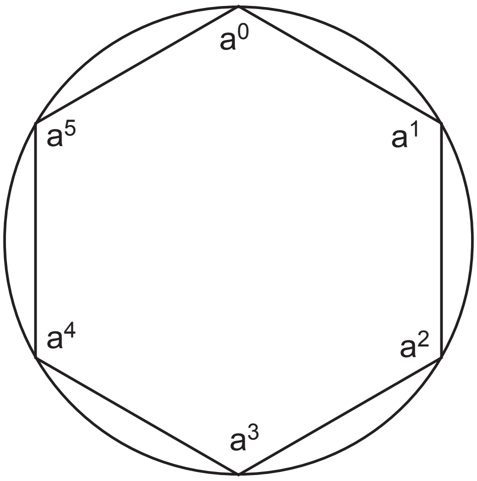


***Fig. 3.1* : Cyclic group generated by a**

Example 3.3.2 : Any integer n 2 Z can be expressed as

$$n = 1 + 1 + ... + 1(n \text{ times}), \text{ when } n \text{ is positive.}$$

Also

$$n = (-1) + (-1) + ... + (-1)(|n| \text{ times}), \text{ when } n \text{ is negative.}$$

Which implies that both 1 and −1 are generators of the infinite cylic group $\mathbb{Z}$.

Example 3.3.3 : $\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$ with addition modulo n is a finite cyclic group. In this group 1 and $-1 = n - 1$ are the generators.

For example $\mathbb{Z}_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$. To verify that $\mathbb{Z}_8 = \langle 3\rangle$, we note that $\langle 1\rangle = \{3, 3 + 3, 3 + 3 + 3, ...\} = \{3, 6, 1, 4, 7, 2, 5, 0\}$. On the other hand 2 is not a generator (check it).

Example 3.3.4 : $U(12) = \{1, 5, 7, 11\}$, in this case $\langle 1\rangle = 1$, $\langle 5\rangle = \{1, 5\}$, $\langle 7\rangle = \{1, 7\}$ and $\langle 11\rangle = \{1, 11\}$. Therefore, $U(12)$ is not cyclic. But note that $U(10)$ is cyclic and generated by 3 and 7.

Example 3.3.5 : The group $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(m, n) : m \in \mathbb{Z}_2, n \in \mathbb{Z}_3\}$ is a cyclic group. The binary operation is component wise addition

$$(m, n) + (m', n') = (m + m', n + n').$$

In this group the element (1, 1) has order 6.

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

$$\begin{aligned}(1, 1) + (1, 0) &= (0, 1)\\(1, 1) + (0, 1) &= (1, 2)\\(1, 1) + (1, 2) &= (0, 0).\end{aligned}$$

Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group of order 6. Be careful, in general it is not true that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

3.4 Properties of Cyclic Group

Since the elements of a cyclic group are the powers of an element, properties of cyclic groups are closely related to the properties of the powers of an element.

Theorem 3.4.1 : Every cyclic group is Abelian.

Proof. Let G be a cyclic group generated by g. Take $a, b \in G$. Then $a = g^n$ and $b = g^m$. Now

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba.$$

Which implies that G is Abelian.

The converse of the above theorem need not be true always, check that (hints: try)

Theorem 3.4.2 : Every subgroup of a cyclic group is cyclic.

Proof. The main tools used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If $H = \{e\}$, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as an for some integer n. We can assume that $n > 0$. Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well-Ordering. We claim that $h = a^m$ is a generator for H. We must show that every $h_0 \in H$ can be written as a power of h. Since $h_0 \in H$ and H is a subgroup of G, $h_0 = a^{\text{k}}$ for some positive integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$a^k = a^{mk+r} = (a^m)^k a^r = h^q a^r.$$

So $a^r = a^k h^{-q}$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that a^m was in H; consequently, $r = 0$ and so $k = m^q$. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h.

Corollary 3.4.3 : The subgroups of $\mathbb{Z}$ is exactly $n\mathbb{Z}$ for $n = 1, 2, ...$

Theorem 3.4.4 : Let a $\in G$ such that $|a| = n$. Then for any $k \in \mathbb{N}$

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

2. $|a^k| = \dfrac{n}{\gcd(n,k)}$.

This theorem is related to the order of a^k and the groups generated by it. They will help us to find generators of a cyclic group

Proof. 1. Let $d = gcd(n, k)$. So, in particular, d is a divisor of k so there exists an integer r such that $k = dr$. So, $a^k = (a^d)r$. This implies that $a^k \in \langle a^d\rangle$, i.e., $\langle a^k\rangle \subseteq \langle a^{gcd(n,k)}\rangle$.

Conversely, with d as above we know there exist integers s and t such that $d = ns + kt$. So,

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

Therefore, $a^d \in \langle a^k\rangle$ and so $\langle a^d\rangle \subseteq \langle a^k\rangle$ by closure.

2. It is clear that $(a^d)^{\frac{n}{d}} = a^n = e$, so that $|a^d| \le \frac{n}{d}$. We can not have $|a^d| < \frac{n}{d}$. If we did, then there exists $i < \frac{n}{d}$ such that $|a^d| = i$, then $a^{di} = e$ and $di < n$ which contradicts that $|a| = n$. Thus, $|a^d| = \frac{n}{d}$. This is true for every positive divisor of n and $gcd(n, k)$ is such a divisor. So, we have $|a^k| = |\langle a^k\rangle| = |\langle a^{gcd(n,k)}\rangle| = \dfrac{n}{\gcd(n,k)}$. □

Theorem 3.4.5 : Let $G = \langle a\rangle$ be a cyclic group of order n. If G contains an element b of order n, then $\langle b\rangle = G$.

Proof. Since $b \in$ G and $|b| = n$. Then $\langle b\rangle$ contains n number of distinct elements. Again $\langle b\rangle \subseteq G$. Hence, $\langle b\rangle = G$. □

Definition 3.4.6 : (Euler Phi Function). Let $n \in \mathbb{Z}^+$. The Euler Phi function of n, denoted by $\phi(n)$ is the number of positive integers less than n and relatively prime to n and we set $\phi(1) = 1$.

Example 3.4.7 : The following table shows the value of ϕ for different n.

n	1	2	3	4	5	6	7	8
ϕ	1	1	2	2	4	2	6	8

Example 3.4.8 : By definition $|U(n)| = \phi(n)$.

3.5 The Circle Group and the Roots of Unity

The multiplicative group of the complex numbers, $\mathbb{C}^+$, possesses some interesting subgroups. Whereas $\mathbb{Q}^+$ and $\mathbb{R}^+$ have no interesting subgroups of finite order, $\mathbb{C}^+$ has many. We first consider the **circle group**,

$$S = \{z \in \mathbb{C} : |z| = 1\}.$$

Proposition 3.5.1 : The circle group is a subgroup of $\mathbb{C}^+$.

Although the circle group has infinite order, it has many interesting infinite subgroups. Suppose that $H = \{1,-1, i,-i\}$. Then H is a subgroup of the circle group. Also, 1, −1, i, and $-i$ are exactly those complex numbers that satisfy the equation $z^4 = 1$. The complex numbers satisfying the equation $z^n = 1$ are called the ***n*th roots of unity**.

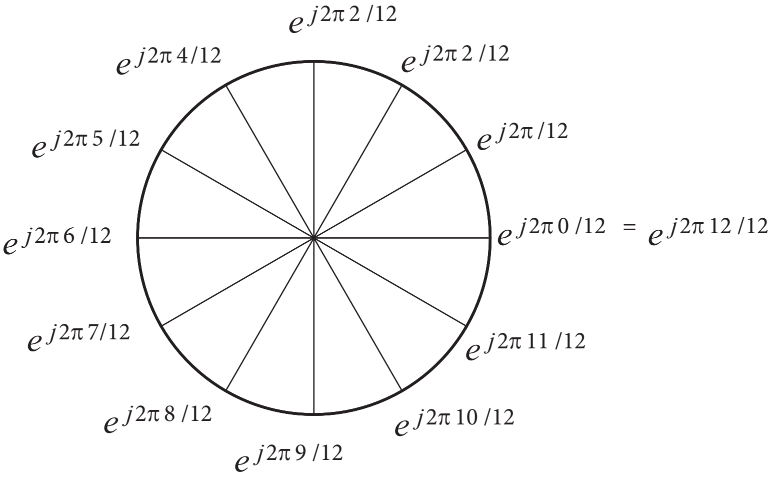


Fig. 3.2

Theorem 3.5.2 : If $z^n = 1$, then the nth root of unity are

$$z = \exp\left(\frac{2k\pi}{n}\right),$$

where $k = 0, 1, ..., n - 1$. Furthermore, the nth roots of unity form a cyclic subgroup of $\mathbb{S}$ of order n.

Proof. By DeMoivre's Theorem

$$z^n = exp\left(n\frac{2k\pi}{n}\right) = exp(2k\pi) = 1$$

The z's are distinct since the numbers $2k\pi/n$ are all distinct and are greater than or equal to 0 but less than 2π. The fact that these are all of the roots of the equation $z^n = 1$ follows from from fundamental theorem of algebra, which states that a polynomial of degree n can have at most n roots. We will leave the proof that the nth roots of unity form a cyclic subgroup of $\mathbb{S}$ as an exercise. □

A generator for the group of the nth roots of unity is called a primitive nth root of unity.

3.6 Summary

In this unit, we have introduced the concept of cyclic group. We have showed that a subgroup of a cyclic group is cyclic. Also we have studied that for each divisor of the order of a cyclic group there exists a unique cyclic subgroup of that order.

3.7 Worked examples

1. Find all generators of Z_{22}.

Solution : Since $|Z_{22}| = 22$, if a is a generator of Z_{22}, then $|a|$ must equal to 22. Now, let b be a generator of Z_{22}, then $b = 1^b = b$. Since $|1| = 22$, we have $|b| = |1^b| = 22/gcd(b, 22) = 22$. Hence, b is a generator of Z_{22} iff $gcd(b,22) = 1$. Thus, 1,3,5,7,9,11,13,15,17,19,21 are all generators of Z_{22}.

2. Let $G = (a)$, a cyclic group generated by a, such that $|a| = 16$. List all generators for the subgroup of order 8.

Solution : Let H be the subgroup of G of order 8. Then $H = (a^2) = (a^{16/8})$ is the unique subgroup of G of order 8 by Theorem 3.2.5. Hence,$(a^2)^k$ is a generator of H iff $gcd(k,8) = 1$. Thus, $(a^2)^1 = a^2$, $(a^2)^3 = a^6$, $(a^2)^5 = a^{10}$, $(a^2)^7 = a^{14}$.

3. Suppose that G is a cyclic group such that $|G| = 48$. How many subgroups does G have?

Solution : Since for each positive divisor k of 48 there is a unique subgroup of order k by Theorem 3.2.5, number of all subgroups of G equals to the number of all positive divisors of 48. Hence, Write $48 = 3^1 2^3$. Hence, number of all positive divisors of 48 = $(1+1)(3+1) = 8$. If we do not count G as a subgroup of itself, then number of all proper subgroups of G is $8 - 1 = 7$.

4. Let a be an element in a group,and let i, k be positive integers. Prove that $H = (a^i) \cap (a^k)$ is a cyclic subgroup of (a) and $H = (a^{lcm(i,k)})$.

Solution : Since (a) is cyclic and H is a subgroup of (a), H is cyclic by Theorem 3.2.2. By Theorem 1.2.18 we know that $\text{lcm}(i, k) = ik/gcd(i, k)$.

Since $k/\mathrm{gcd}(i,k)$ is an integer, we have $a^{lcm(i,k)} = (a^i)^{k/gcd(i,k)}$. Thus, $(a^{lcm\ (i,k)}) \subset (a^i)$. Also, since $k/gcd(i, k)$ is an integer, we have $a^{lcm(i,k)} = (a^k\ )^{i/gcd(i.k)}$. Thus, $(a^{lcm(i,\ k)}) \subset (a^k)$. Hence, $(a^{lcm\ (i,\ k)}\ ) \subset H$. Now, let $h \in H$. Then $h = a^j = (a^i)^m = (a^k)^n$ for some j, m, $n \in Z$. Thus, i divides j and k divides j. Hence, $lcm(i,k)$ divides j.

Thus, $h = a^j = (a^{lcm(i,k)})^c$ where $j = lcm(i,k)c$. Thus, $h \in (a^{lcm(i,k)})$. Hence, $H \subset (a^{lcm(i,k)})$. Thus, $H = (\mathrm{a}^{lcm(i,k)})$.

5. Let a be an element in a group. Describe the sub-group $H = (a^{12}) \cap (a^{18})$.

Solution : By the previous Question, H is cyclic and $H = (a^{lcm(12,18)} = (a^{36})$.

6. Let $G = (a)$, and let H be the smallest subgroup of G that contains am and an. Prove that $H = (a^{gcd(n,\ m)})$.

Solution : Since G is cyclic, H is cyclic by Theorem 3.2.2. Hence, $H = (a^k)$ for some positive integer k. Since $a^n \in H$ and $a^m \in H$, k divides both n and m. Hence, k divides $gcd(n,m)$. Thus, $a^{gcd(n,m)} \in H = (a^k)$. Hence, $(a^{gcd(n,m)}) \subset H$. Also, since $gcd(n,m)$ divides both n and m, $a^n \in (a^{gcd(n,m)})$ and $a^m \in (a^{gcd(n,m)})$. Hence, Since H is the smallest subgroup of G containing a^n and a^m and a^n, $a^m \in (a^{gcd(n,m)}) \subset H$, we conclude that $H = (a^{gcd(n,m)})$.

7. Let G be an infinite cyclic group. Prove that e is the only element in G of finite order.

Solution : Since G is an infinite cyclic group, $G = (a)$ for some $a \in G$ such that $|(a)|$ is infinite. Now, assume that there is k an element $b \in G$ such that $|b| = m$ and $b \neq e$. Since $G = (a)$, $b^k = a$ for some $k \geq 1$.

Hence, $e = b^m = (a^k)^m = a^{km}$. Hence, $|a|$ divides km.

a contradiction since $|a|$ is infinite. Thus, e is the only element in G of finite order.

8. Let $G = (a)$ be *a* cyclic group. Suppose that G has a finite subgroup H such that $H \neq \{e\}$. Prove that G is a finite group.

Solution : First, observe that H is cyclic by Theorem 3.2.2. Hence, $H = (a^n)$ for some positive integer n. Since H is finite and $H = (a^n)$, $Ord(a^n) = |H| = m$ is finite. Thus, (a^n) $m = a^{nm} = e$. Hence, $|a|$ divides n^m. Thus, $(a) = G$ is a finite group.

9. Let a be an element in a group G such that $|a|$ is infinite. Prove that (a), (a^2), (a^3), ... are all distinct subgroups of G, and Hence, G has infinitely many proper subgroups.

Solution : Suppose that $(a^i) = (a^k)$ for some positive integers i, k such th at $k > i$.

Thus, $a^i = (a^k)^m$ for some $m \in Z$. Hence, $a^i = a^{km}$. Thus, $a^{i\ km} = e$. Since $k > i$, $km \neq i$ and therefore $i - km \neq 0$. Thus, $|\ a\ |$ divides $i - km$. Hence, $|a|$ is finite, a contradiction.

10. Let *G* be a group containing more than 12 elements of order 13. Prove that *G* is never cyclic.

Solution : Suppose that *G* is cyclic. Let a $\in$ *G* such that $|a| = 13$. Hence, (a) is a finite subgroup of *G*. Thus, *G* must be finite by the previous Question. Hence, by Theorem 3.2.5 there is exactly ϕ (13) = 12 elements in *G* of order 13. A contradiction. Hence, *G* is never cyclic.

3.8 Model Questions

1. Find all generators of the cyclic group $\mathbb{Z}_{28}$.
2. In $\mathbb{Z}_{30}$ find the order of the subgroup $\langle 18\rangle$ and $\langle 24\rangle$.
3. Show that any cyclic group of even order has exactly one element of order 2.
4. Show that $\mathbb{Q}^+$ is not a cyclic group.
5. Let *G* be an abelian group of order 15. Show that if you can find an element *a* of order 5 and an element *b* of order 3, then *G* must be cyclic.
6. Let $H = \left\{\pm 1, \pm i, \pm\frac{\sqrt{2}}{2}, \pm\frac{\sqrt{2}}{2}i\right\}$ is a cyclic subgroup of $\mathbb{C}^+$.
7. Let $H = \left\{\begin{bmatrix}1 & m & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \in GL_3(\mathbb{Q}) : m \in \mathbb{Z}\right\}$ and $K = \left\{\begin{bmatrix}1 & 0 & n\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \in\right.$ $GL_3(\mathbb{Q}) : n \in \mathbb{Z}$ } are cyclic groups of $GL_3(\mathbb{Q})$.
8. Prove that $\mathbb{Z}_p$ does not have any non-trivial subgroup if p is prime.
9. Let *G* be an abelian group. Show that the elements of finite order in *G* form a subgroup. This subgroup is called the torsion subgroup of *G*.
10. Find all generators of $\mathbb{Z}_{48}$.
11. Prove that the following groups are not cyclic:

    (i) $\mathbb{Z}_2 \times \mathbb{Z}_2$

    (ii) $\mathbb{Z}_2 \times \mathbb{Z}$

    (iii) $\mathbb{Z} \times \mathbb{Z}$

12. Prove that the cyclic subgroup $\langle a \rangle$ is the smallest subgroup of G containing $a \in G$.

13. If a cyclic group has an element of infinite order, how many elements of finite order does it have?

14. Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation $x^{35} = e$. Prove that G is cyclic. Does your argument work if 35 is replaced with 33?

15. Let G be a group and let a be an element of G.

    a. If $a^{12} = e$, what can we say about the order of a?

    b. If $a^m = e$, what can we say about the order of a?

    c. Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a \rangle = G$.

16. Prove that a group of order 3 must be cyclic.

17. Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? Why? Describe all the subgroups of Z. Let a be a group element with infinite order. Describe all subgroups of $\langle a \rangle$.

18. For any element a in any group G, prove that $\langle a \rangle$ is a subgroup of $C(a)$ (the centralizer of a).

19. If d is a positive integer, $d \neq 2$, and d divides n, show that the number of elements of order d in D_n is ϕ (d). How many elements of order 2 does D_n have?

20. Find all generators of Z. Let a be a group element that has infinite order. Find all generators of $\langle a \rangle$.

21. Prove that C^*, the group of nonzero complex numbers under multiplication, has a cyclic subgroup of order n for every positive integer n.

22. Let a be a group element that has infinite order. Prove that $\langle a^i \rangle = \langle a^j \rangle$ if and only if $i = \pm j$.

23. List all the elements of order 8 in $Z_{8000000}$. How do you know your list is complete? Let a be a group element such that $|a| = 8000000$. List all elements of order 8 in $\langle a \rangle$. How do you know your list is complete?

24. Suppose that G is a group with more than one element. If the only subgroups of G are $\{e\}$ and G, prove that G is cyclic and has prime order.

25. Let G be a finite group. Show that there exists a fixed positive integer n such that $a^n = e$ for all a in G. (Note that n is independent of a.)

26. Determine the subgroup lattice for Z_{12}. Generalize to Z_{p^2q}, where p and q are distinct primes.

27. Determine the subgroup lattice for Z_8. Generalize to Z_{p^n}, where p is a prime and n is some positive integer.

28. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

29. List all of the elements in each of the following subgroups.

    (a) The subgroup of $\mathbb{Z}$ generated by 7

    (b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

    (c) All subgroups of $\mathbb{Z}_{12}$

    (d) All subgroups of $\mathbb{Z}_{60}$

    (e) All subgroups of $\mathbb{Z}_{13}$

    (f) All subgroups of $\mathbb{Z}_{48}$

    (g) The subgroup generated by 3 in $U(20)$

    (h) The subgroup generated by 5 in $U(18)$

    (i) The subgroup of $\mathbb{R}*$ generated by 7

    (j) The subgroup of $\mathbb{C}*$ generated by i where $i^2 = -1$

    (k) The subgroup of $\mathbb{C}*$ generated by $2i$

    (l) The subgroup of $\mathbb{C}*$ generated by $(1+i)/\sqrt{2}$

    (m) The subgroup of $\mathbb{C}*$ generated by $(1+\sqrt{3}i)/2$

30. Find the subgroups of $GL_2(\mathbb{R})$ generated by each of the following matrices

    (a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ (e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

    (b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

31. Find the order of every element in $\mathbb{Z}_{18}$.

32. Find the order of every element in the symmetry group of the square, D_4.

33. What are all of the cyclic subgroups of the quaternion group, Q_8?

34. List all of the cyclic subgroups of $U(30)$.

35. List every generator of each subgroup of order 8 in $\mathbb{Z}_{32}$.

36. Find all elements of finite order in each of the following groups. Here the "*" indicates the set with zero removed.

    (a) $\mathbb{Z}$ (b) $\mathbb{Q}^*$ (c) $\mathbb{R}^*$

37. If $a^{24} = e$ in a group G, what are the possible orders of a?

38. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

39. For $n \leq 20$, which groups $U(n)$ are cyclic? Make a conjecture as to what is true in general. Can you prove your conjecture?

3.9 Solutions of some selected problems

1. { 1, 3, 5, 9, 11 , 13, 15, 17, 19, 21, 23, 25, 27}

2. 5, 5

10. All the elements less than and prime to 48.

13. Only one

15. (a) order of a may be 1, 2, 3, 4, 6 or 12

    (b) order of a may be all the divisors of m

17. Use the fact that all the subgroups of a cyclic group are cyclic

20. $\{+1, -1\}$

23. Use theorem 3.4.3

29. (a) $\{7n : n \in Z\}$

    (b) {0, 6, 12, 15, 6, 21}

30. (a) $\{\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} : a \in R\}$

31. use theorem 3.4.3

36. (a) 0

    (b) $\{+1, -1\}$

    (c) $\{+1, -1\}$

37. All the divisors of 24

38. Z_2

Unit - 4 ❑ Cosets and Normal Subgroups

Structure

4.1 Objectives

The followings are discussed here:

- Definition of cosets and examples
- Definition of normal subgroup and normalizer
- Basic properties of normal group
- Lagrange's theorem

4.2 Introduction

In this unit, we prove the single most important theorem in finite group theory—Lagrange's Theorem. In his book on abstract algebra, I. N. Herstein likened it to the ABC's for finite groups. But first we introduce a new and powerful tool for analyzing a group—the notion of a coset. This notion was invented by Galois in 1830, although the term was coined by G. A. Miller in 1910.

4.3 Definition and concept

The Euclidean plane $\mathbb{R}^2$ forms a group under component wise addition, i.e., for any two $(a, b), (c, d) \in \mathbb{R}^2$, then

$$(a, b) + (c, d) = (a + c, b + d).$$

Now the subset $X = \{(x, 0) : x \in R\}$ is a subgroup of $\mathbb{R}^2$ which is nothing but the x axis (check it!). If we take any element $(a, b) \in \mathbb{R}^2$ which is not in X, then the set

$$H(a, b) = (a, b) + X = \{(a + x, b) : x \in \mathbb{R}\}$$

is parallel to x-axes and looks like the set X, see Figure 4.1. Also it can be seen that if we choose an element from X, i.e., of the form $(a, 0)$, then $H_{(a,0)}$ is X itself. Therefore, we conclude that either $H_{(a,b)} = X$ or $H_{(a,b)} \bigcap X = \phi$. Since the collection of all straight lines, parallel to x-axes covers the whole Euclidean plane, it implies that $\bigcup_{(a,b)\in\mathbb{R}^2} H_{(a,b)} = \mathbb{R}^2$. Hence, the collection $\{H_{(a,b)}\}$ forms a partition of the Euclidean plane. If we take the collection

$$H_{(a,b)} = X + (a, b) = \{(x + a, b) : x \in \mathbb{R}\}$$

then we also get the same image as the figure 4.1 for the commutativity of the addition in $\mathbb{R}^2$. In group theoretic language this type of element is called coset, more specifically left-coset. Here comes the formal definition.

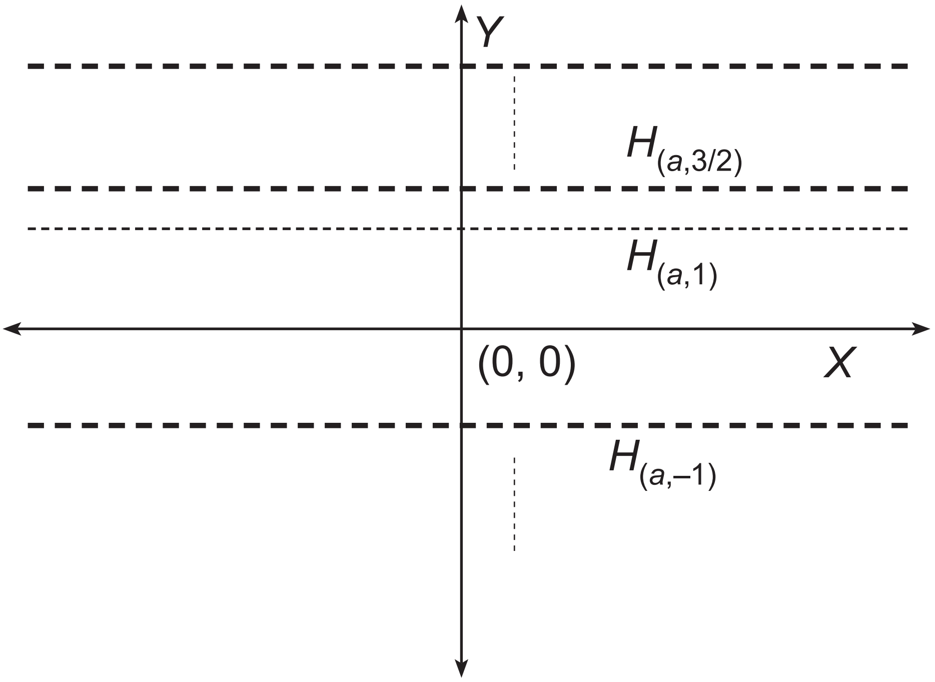


Fig. 4.1

Definition 4.3.1 : Let G be a group. Now take an element $a \in G$, then the set aH defined by

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

is called the left coset. Similarly we can define the right-coset Ha.

Example 4.3.2 : Consider the subgroup $H = \langle 3 \rangle$ of $\mathbb{Z}_6$. The cosets are

$$0 + H = \{0, 3\} = 3 + H$$
$$1 + H = (123)H = \{(13), (123)\}$$
$$2 + H = (132)H = \{(23), (132)\}$$

Example 4.3.3 : Let $G = S_3$ and $H = \{(1), (12)\}$. Then the left cosets of H in G are

$$(1)H = (12)H = \{(1), (1, 2)\}$$
$$(13)H = (123)H = \{(13), (123)\}$$
$$(23)H = (132)H = \{(23), (132)\}$$

The right cosets are

$$H(1) = H(12) = \{(1), (1, 2)\}$$
$$H(13) = H(132) = \{(13), (132)\}$$
$$H(23) = H(123) = \{(23), (123)\}.$$

Note that, except for the coset of the elements in H, the left and right cosets are different.

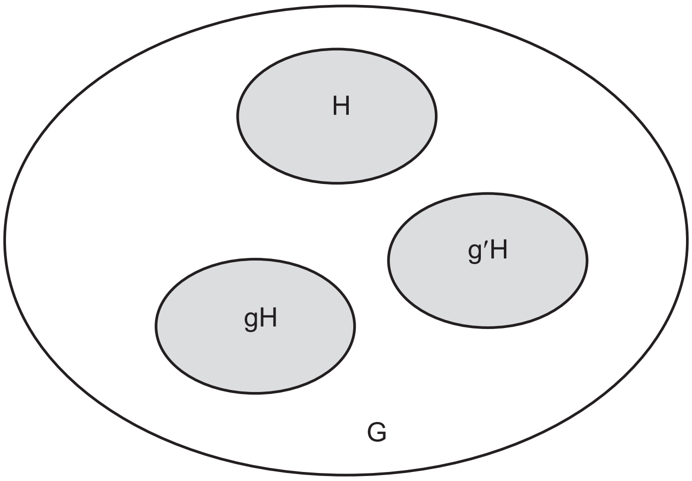


Fig. 4.2 **: Group G and cosets gH and g′H of the subgroup H**

Proposition 4.3.4 (Properties). *Let H and K be two subgroups of G and $a, b \in G$. Then*

1. $a \in aH$.

2. $aH = H$ if and only if $a \in H$.

3. $aH = bH$ if and only if $a \in bH$.

4. $aH = bH$ or $aH \cap bH = \phi$.

5. $aH = bH$ if and only if $a^{-1}b \in H$.

6. $|aH| = |bH|$.

Proof. 1. Since H contains the identity element e, which implies $a.e = a \in aH$.

2. Suppose $aH = H$, then $e = ah$ for some $h \in H$. Therefore, $a = eh^{-1} = h^{-1} \in H$. Conversely, suppose $a \in H$. Then $aH \subset H$. Let $h \in H$. Then h can be expressed as $h = aa^{-1}h = ah_1 \in aH$ for some $h_1 \in H$. Which implies $H \subseteq aH$. Hence, $aH = H$.

3. This part can be easily deduced from 1. and 2.

4. Let $aH \bigcap bH \neq \phi$. Take $x \in aH \bigcap bH$. Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. So, we get $a = bh_2h_1 \in bH$. Hence, from (3) we say that $aH = bH$. Therefore, either $aH \bigcap bH = \phi$ or $aH = bH$.

5. Let $aH = bH$. Then $b = ah$ for some $h \in H$. Which implies that $a^{-1}b = h \in H$. Conversely, let $a^{-1}b \in H$. Then $b \in aH$. So, from (3) we get $aH = bH$.

6. Define a function $f : aH \rightarrow bH$ by $f(ah) = bh$. (Check it!) This function is bijective. Hence, aH and bH has same number of elements. □

From (3) of the Proposition 4.4, it is clear that cosets makes partition of the group G. But we know that for any partition there must be a equivalence relation. Now we define the equivalence relation.

Let H be a subgroup of the group G. For any $a, b \in G$, a is related to b, $a \sim b$ if and only if $a^{-1}b \in H$.

This relation is reflective, i.e., $a \sim a$ since $a^{-1}a = e \in H$. This relation is also symmetric. Now for any $a, b, c \in G$ such that $a \sim$ b and $b \sim$ c, we get $a^{-1}b \in H$ and $b^{-1}c \in h$. Hence, $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. Which implies that $a \sim c$. Therefore, the relation $\sim$ is transitive. Hence $\sim$ is an equivalence relation.

Consider the equivalence class $[a]$ of $a \in g$, i.e.,

$$[a] = \{b \in G : a \sim b\}.$$

Theorem 4.3.5 : *The equivalence class [a] is nothing but the left coset aH.*

Proof. Since the relation $\sim$ is reflective, $[a] \neq \phi$. Let $b \in [a]$. Then $a \sim b$, i.e., a^{-1}b $\in H$. Which implies that $b \in aH$. Hence, $[a] \subseteq aH$.

Again take $b \in aH$. Then $b = ah$ for some $h \in H$. Which implies that $a^{-1}b = h \in H$. Therefore, $a \sim b$. So, $b \in [a]$. Therefore, $aH \subseteq [a]$. Hence, we get $[a] = aH$. □

This theorem makes it clear why the cosets partition the whole group. Note that the above result holds if we replace 'left' with 'right'.

Definition 4.3.6 : Let G be a group and H be a subgroup. The number of left cosets of H in G is called index of H in G and denoted by $[G : H]$.

Example 4.3.7 : From the previous example we get $[\mathbb{Z}_6, H] = 3$ and $[S_3, H] = 3$.

Theorem 4.3.8 : *Let H be a subgroup of G. Then the number of left cosets of H in G is same as the number of right cosets of H in G.*

Proof. Let L_H and R_H be the number of left cosets and right cosets of H in G respectively. Now we define a bijection between L_H and R_H. Consider the function

$$\varphi : L_H \to R_H$$

defined by

$$\varphi(gH) = Hg^{-1}.$$

First, we will show that this map is well-defined. Suppose $g_1H = g_2H$. Then by proposition 4.4, $Hg_1^{-1} = Hg_2^{-1} = \varphi(g_1H) = \varphi(g_2H)$. Thus, φ is well defined.

Let $\varphi(g_1H) = \varphi(g_2H)$ for some $g_1, g_2 \in G$. Then, $Hg_1^{-1} = Hg_2^{-1}$. Again, the proposition 4.4 implies that $g_1H = g_2H$. Hence, the function φ is injective. The function φ is obviously surjective. Therefore, φ is a bijection so the result holds. □

The above theorem implies that in the definition of index of a subgroup H in the group G we can replace the term 'left cosets' with 'right cosets' also.

4.4 Lagrange's Theorem

We're finally ready to state Lagrange's Theorem, which is named after the Italian born mathematician Joseph Louis Lagrange.

Theorem 4.4.1 (Lagrange's Theorem). *Let G be a finite group and H be a subgroup of G. Then* $|G|/|H| = [G : H]$. *In particular,* $|H|$ *divides* $|G|$.

Proof. The group G is partitioned into $[G : H]$ number of left-cosets and each left coset has $|H|$ numbers of element by the proposition 4.4. Hence, $|G| = |H|[G : H]$. □

The converse of Lagrange's Theorem is not true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n. It can be seen by an example: A_4 has no subgroup of order 6. But there are some partial converse to Lagranges Theoem. For finite abelian group the full converse is true, i.e., for each divisor of $|G|$, we have a subgroup of that order.

Theorem 4.4.2 (Cauchy's Theorem). *If G is a finite group and p is a prime dividing* $|G|$, *then G has an element of order p.*

Proof. The proof is out of the scope of this book.

We'll now examine a host of consequence of Lagrange's Theorem.

Corollary 4.4.3 : Suppose G is a finite group and $g \in$ G. Then

1. $|g|$ *divided* $|G|$.

2. $g|G| = e$.

3. *If* $|G|$ *is a prime, then G is cyclic and every element g ≠ e of G is a generator of G.*

Proof. 1. Consider the cyclic group $\langle g\rangle$ generated by g. Then $\langle g\rangle$ has order $|g|$. Now by Lagrange's theorem $|\langle g\rangle|$ divides $|G|$, hence, $|g|$ divides $|G|$.

2. Since $|g|||G|$. So $|G| = m|g|$ for some integer m. Now $g^{|G|} = (g^{|g|})^m = e^m = e$.

3. Let $g \in G$ be an non-identity element. Now $|g|$ divides $|G|$. But $|G|$ is a prime number. So either $|g|$ is one or $|G|$. But $|g| \neq 1$ since g is not the identity. Therefore, $|g| = |G|$. Therefore, g is a generator of G. Since g is arbitrary, so every element $g \neq \phi$ of G is a generator of G and G is cyclic. □

Corollary 4.4.4 : Let H and K be subgroups of G such that $K \subset$ H $\subset$ G. Then $[G : K] = [G : H][G : K]$.

Proof. By, Lagrange's Theorem we have

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

Theorem 4.4.5 : (Fermat's Little Theorem). *For every integer a and every prime p,*

$$a^p \equiv a \bmod p.$$

Proof. By division algorithm, $a = pm + r$ where $0 \le r < p$. Thus $a \equiv r$ mod p, and it suffices to prove that $r^p \equiv r$ mod p. If $r = 0$ the result is trivial, so we may assume that $r \in U(p) = \{1, 2, ..., p - 1\}$. Hence, $r^{p-1} \equiv 1$ mod p and therefore, $r^p \equiv r$ mod p.

4.5 Normal Subgroups

Normal subgroups was introduced by Evariste Galois in 1831 as a tool for deciding whether a polynomial is solvable by radical or not. Galois noted that a subgroup H of a group G of permutation induced two decompositions of G into what we call left cosets and right cosets. If the two decompositions coincide, that is, if the left cosets are the same as the right cosets, Galois called the decomposition proper. Thus a subgroup giving a proper decomposition is what we called normal subgroup.

Definition 4.5.1 : A subgroup H of G is called normal, denoted by $H \lhd G$, if $gH = Hg$ for all $g \in G$, i.e., left-coset and right-coset are equal.

You should think of a normal subgroup in this way: You can switch the order of a product of an element a from the group and an element h from the normal subgroup

H, but you must "fudge" a bit on the element from the normal subgroup H by using some h' from H rather than h. That is, there is an element h' in H such that $ah = h'a$. Likewise, there is some h'' in H such that $ha = ah''$. (It is possible that $h' = h$ or $h'' = h$, but we may not assume this.)

Proposition 4.5.2 : *Let G be a group and H be a subgroup with index* 2. *Then H is normal in G.*

Proof. Let $g \in G - H$ so, ny hypothesis, there are two left cosets of H in G, they are eH and gH. Since $eH = H$ and the cosets partition G, we must have $gH = G - H$. Now the two right cosets of H in G are He and Hg. Since $He = H$, we again must have $Hg = G - H$. Combining these gives, $gH = Hg$ for all $g \in G$. Hence, H is normal in G.

Example 4.5.3 : Every subgroup of an abelian group G is normal.

Example 4.5.4 : $G = S_3$, $H = \langle(1, 2, 3)\rangle = \{e, (1, 2, 3), (1, 3, 2)\}$. Now $[G : H] = 2$, so H is normal in G.

Let $g = (1, 2)$. Then

$$gH = \{(1, 2), (1, 2)(1, 2, 3), (1, 2)(1, 3, 2)\} = \{(1, 2), (2, 3), (1, 3)\}$$
$$Hg = \{(1, 2), (1, 2, 3)(1, 2), (1, 3, 2)(1, 2)\} = \{(1, 2), (1, 3), (2, 3)\}.$$

this example shows that if H is normal in G, then $gH = Hg\ \forall g \in G$ but it is not true that $gh = hg$ for all $h \in H$.

There are several equivalent formulations of the definition of normality. Normal subgroup can also be expressed in terms of conjugacy relation.

In a group G, two elements g and h are said to be conjugate if

$$h = xgx^{-1} \text{ for some } x \in G.$$

The conjugacy relation in G is an equivalence relation (Check it !). The conjugacy class of $g \in G$ is denoted by

$$[g] = \{xgx^{-1} : x \in G\}.$$

Example 4.5.5 : In S_3, what are the conjugates of (1, 2)? We make a table of $\sigma(1, 2)\sigma^{-1}$ for all $\sigma \in S_3$.

σ	(1)	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
$\sigma(1, 2)\sigma^{-1}$	(1,2)	(1,2)	(2,3)	(1,3)	(2,3)	(1,3)

The idea of conjugation can be applied not just to elements, but to subgroups. If H is a subgroup of G and $g \in G$, the set

$$\mathrm{gHg}^{-1} = \{ghg^{-1} : h \in H\}$$

is the conjugacy class of g in H.

Proposition 4.5.6 : *The conjugacy class gHg^{-1} is a subgroup of G.*

Proof. Since $e \in H$, which implies $e \in gHg^{-1}$. So $gHg^{-1} \neq \phi$. Let $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. Now, $xy^{-1} = gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2{}^{-1}g^{-1} = g(h_1h_2{}^{-1})g^{-1} \in gHg^{-1}$. Therefore, gHg^{-1} is a subgroup of G.

Theorem 4.5.7 : *A subgroup H of G is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.*

Proof. Let H is normal in G. Then $gH = Hg$ for all $g \in G$. Now for any $h \in H$, there exists h′ $\in H$ such that $gh = h'g$. Which implies that $ghg^{-1} = h' \in H$. Hence, $gHg^{-1} \subseteq H$ for all $g \in G$.

Conversely, let $gHg^{-1} \subseteq H$ for all $g \in G$. Then for any $gh \in gH$ there exists $h' \in H$ such that $gh = h'g$ from the hypothesis. Hence, $gH \subseteq Hg$. Similarly, we can show $Hg \subseteq gH$. Therefore, $gH = Hg$ for all $g \in G$. Hence, H is normal in G. □

Definition 4.5.8 : Let H and K be subgroups of a group G and define

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

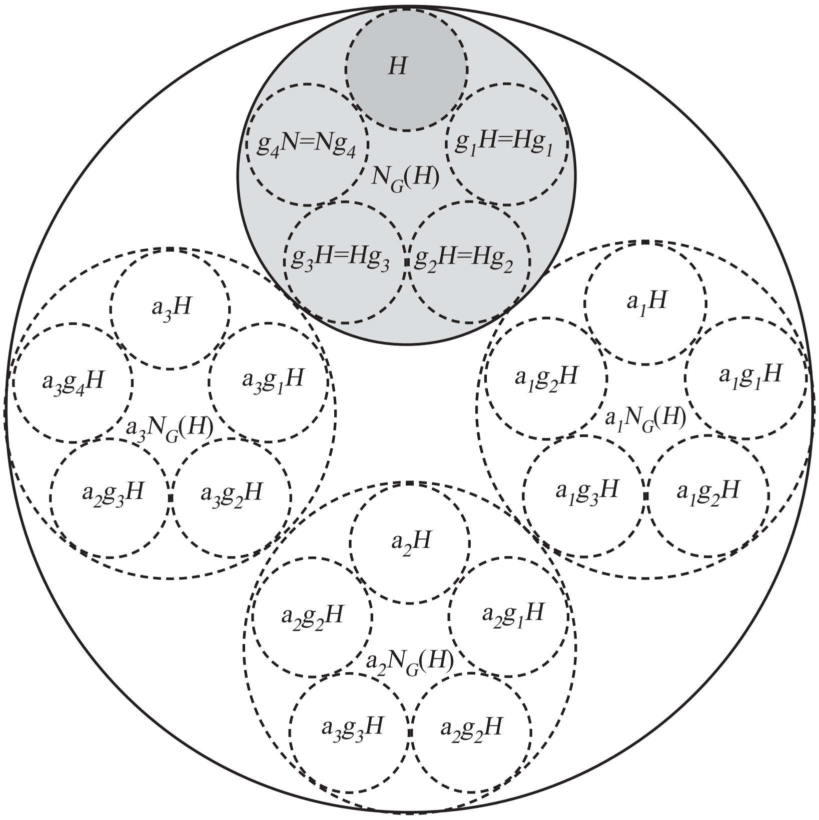


***Fig. 4.3* : Abstract visualization of the relationships $H \Delta N_GH \Delta G$**

Proposition 4.5.9 : *If H and K are finite subgroups of a group, then*

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

Proof. Notice that HK is a union of left cosets of K, namely,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of distinct left cosets of the from hK, $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \bigcap K \Leftrightarrow h_1(H \bigcap K) = h_2(H \bigcap K).$$

Thus the number of distinct cosets of the from hK, for $h \in H$ is the number of distinct cosets $h(H \bigcap K)$, for $h \in H$. The latter number, by Lagrange's theorem, equals $\frac{|H|}{|H \cap K|}$. Thus HK consists of $\frac{|H|}{|H \cap K|}$ number of cosets of K which proves the result. □

4.6 Summary

In this unit, we have studied the concept of cosets and normal subgroup. We have showed that the cosets partion the whole group. We have also discussed the Lagrange's theorem.

4.7 Worked examples

1. **List the cosets of $\langle 9 \rangle$ in $Z_{16}^{\times}$, and find the order of each coset in $Z_{16}^{\times}/\langle 9 \rangle$.**

Solution: $Z_{16}^{\times} = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

$\langle 9 \rangle = \{1, 9\}$ $3\langle 9 \rangle = \{3, 11\}$ $5\langle 9 \rangle = \{5, 13\}$ $7\langle 9 \rangle = \{7, 15\}$

Now the order of aN is the smallest positive integer n such that $a^n \in$ N.

The coset $3\langle 9 \rangle$ has order 2 since $3^2 = 9$ and 9 belongs to the subgroup $\langle 9 \rangle$. (We could have used either element of the coset to do the calculation.) The coset $5\langle 9 \rangle$ also has order 2, since $5^2 = 9$. The coset $7\langle 9 \rangle$ has order 2 since $7^2 = 1$.

2. **List the cosets of $\langle 7 \rangle$ in $Z_{16}^{\times}$. Is the factor group $Z_{16}^{\times}/\langle 7 \rangle$ cyclic?**

Solution: $Z_{16}^{\times} = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

$\langle 7 \rangle = \{1, 7\}$ $3\langle 7 \rangle = \{3, 5\}$ $9\langle 7 \rangle = \{9, 15\}$ $11\langle 7 \rangle = \{11, 13\}$

Since $3^2 \notin \langle 7 \rangle$, the coset $3\langle 7 \rangle$ does not have order 2, so it must have order 4, showing that the factor group is cyclic.

3. Show that the subgroup {id, (1 3)} of S_3 is not normal.

Solution: Here's the multiplication table for S_3, the group of permutations of $\{1, 2, 3\}$.

	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)	(1 2)
id	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3 2)	id	(1 2)	(2 3)	(1 3)
(1 3 2)	(1 3 2)	id	(1 2 3)	(1 3)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3)	(1 2)	id	(1 2 3)	(1 3 2)
(1 3)	(1 3)	(1 2)	(2 3)	(1 3 2)	id	(1 2 3)
(1 2)	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)	id

We have to find an element $g \in S_3$ such that

$$g\{\text{id}, (1\ 3)\}g^{-1} \not\subset \{\text{id}, (1\ 3)\}.$$

There are several possibilities. For example,

$(1\ 2)\{\text{id}, (1\ 3)\}(1\ 2)^{-1} = (1\ 2)\{\text{id}, (1\ 3)\}(1\ 2) = \{(1\ 2)\text{id}(1\ 2), (1\ 2)(1\ 3)(1\ 2)\} = \{\text{id}, (2\ 3)\}$.

Since $\{\text{id}, (2\ 3)\} \not\subset \{\text{id}, (1\ 3)\}$, the subgroup $\{\text{id}, (1\ 3)\}$ is not normal in S_3. □

4. Let G and H be groups. Let $G \times \{1\} = \{(g, 1) \mid g \in G\}$.

Prove that $G \times \{1\}$ is a normal subgroup of the product $G \times H$.

Solution: First, I'll show that it's a subgroup. Let $(g_1, 1), (g_2, 1) \in \text{G} \times \{1\}$, where g_1, $g_2 \in G$. Then

$$(g_1, 1) \cdot (g_2, 1) = (g_1g_2, 1) \in \text{G} \times \{1\}.$$

Therefore, $G \times \{1\}$ is closed under products.

The identity $(1, 1)$ is in $G \times \{1\}$.

If $(g, 1) \in G \times \{1\}$, the inverse is $(g, 1)^{-1} = (g^{-1}, 1)$, which is in $G \times \{1\}$.

Therefore, $G \times \{1\}$ is a subgroup.

To show that $G \times \{1\}$ is normal, let $(a, b) \in G \times H$, where $a \in G$ and $b \in H$. I must show that

$$(a, b)(G \times \{1\})(a, b)^{-1} \subset G \times \{1\}.$$

We can show one set is a subset of another by showing that an element of the first is an element of the second. An element of $(a, b)(G \times \{1\})(a, b)^{-1}$ looks like $(a, b)(g, 1)(a, b)^{-1}$, where $(g, 1) \in G \times \{1\}$. Now

$$(a, b)(g, 1)(a, b)^{-1} = (a, b)(g, 1)(a^{-1}, b^{-1}) = (aga^{-1}, b(1)b^{-1}) = (aga^{-1}, 1).$$

$aga^{-1} \in G$, since $a, g \in$ G. Therefore, $(a, b)(g, 1)(a, b)^{-1} \in G \times \{1\}$. This proves that $(a, b)(G \times \{1\})(a, b)^{-1} \subset G \times \{1\}$. Therefore, $G \times \{1\}$ is normal.

5. The cosets of the subgroup $\langle 19 \rangle$ in U_{20} are

$$\langle 19 \rangle = \{1, 19\}$$

$$3 \cdot \langle 19 \rangle = \{3, 17\}$$

$$7 \cdot \langle 19 \rangle = \{7, 13\}$$

$$9 \cdot \langle 19 \rangle = \{9, 11\}$$

(a) Compute $\{3, 17\} \cdot \{9, 11\}$.

(b) Compute $\{3, 17\}^{-1}$.

(c) Compute $\{9, 11\}^3$.

Solution: (a) Take an element (it doesn't matter which one) from each coset, say $3 \in \{3, 17\}$ and $11 \in \{9, 11\}$.

Perform the operation on the elements you chose. In this case, it's multiplication:

$$3 \cdot 11 = 33 = 13.$$

Find the coset containing the answer: $13 \in \{7, 13\}$.

Hence,

$$\{3, 17\} \cdot \{9, 11\} = \{7, 13\}. \qquad \square$$

(b) Take an element (it doesn't matter which one) from the coset, say $3 \in \{3, 17\}$.

Perform the operation on the elements you chose. In this case, it's finding the inverse (use the Extended Euclidean Algorithm, or trial and error):

$$3^{-1} = 7.$$

Find the coset containing the answer: $7 \in \{7, 13\}$.

Hence,

$$\{3, 17\}^{-1} = \{7, 13\}. \qquad \square$$

(c) Take an element (it doesn't matter which one) from the coset, say $11 \in \{9, 11\}$.

Perform the operation on the elements you chose. In this case, it's cubing:

$$11^3 = 1331 = 11.$$

Find the coset containing the answer: $11 \in \{9, 11\}$.

Hence,

$$\{9, 11\}^3 = \{9, 11\}. \qquad \square$$

6. **Let *G* be a group of order 24. What are the possible orders for the subgroups of *G*.**

   Solution: Write 24 as product of distinct primes. Hence, $24 = (3)(2^3)$. By Theorem 1.2.27, the order of a subgroup of *G* must divide the order of *G*. Hence, We need only to find all divisors of 24. By Theorem 1.2.17, number of all divisors of 24 is $(1 + 1)(3 + 1) = 8$. Hence, possible orders for the subgroups of *G* are : 1,3,2,4,8,6,12,24.

4.8 Model Questions

1. Let *G* be a finite group. If $a, b \in G$ such that $|a| = 5$ and $|b| = 7$, then show that $|G| \geq 35$.
2. Suppose that *G* is a finite group with 60 elements. What are the orders of possible subgroups of *G*?
3. Prove or disprove: Every subgroup of the integers has finite index.
4. Prove or disprove: Every subgroup of the integers has finite order.
5. List the left and right cosets of the subgroups $\langle 8 \rangle$ in $\mathbb{Z}_{18}$.
6. List the left and right cosets of the subgroups $\langle 3 \rangle$ in U_8.
7. List the left and right cosets of the subgroups $3\mathbb{Z}$ in $\mathbb{Z}$.
8. Describe the left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$.
9. Show that the integers have infinite index in the additive group of rational numbers.
10. Let *a* and *b* be elements of a group *G* and *H* and *K* be subgroups of *G*. If $aH = bK$, prove that $H = K$.
11. If *H* and *K* are subgroups of *G* and g belongs to *G*, show that $g(H \cap K) = gH \cap gK$.
12. Let *a* and *b* be nonidentity elements of different orders in a group *G* of order 155. Prove that the only subgroup of *G* that contains *a* and *b* is *G* itself.
13. Let *H* be a subgroup of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication. If $\mathbf{R}^+ \subseteq H \subseteq \mathbf{R}^*$, prove that $H = \mathbf{R}^+$ or $H = \mathbf{R}^*$.
14. Let $\mathbf{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbf{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.
15. Let *G* be a group of order 60. What are the possible orders for the subgroups of *G*?

16. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?
17. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.
18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)}$ mod $n = 1$.
19. Compute 5^{15} mod 7 and 7^{13} mod 11.
20. Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.
21. Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $gm = e$, prove that $g = e$.
22. Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.
23. For any integer $n \geq 3$, prove that D_n has a subgroup of order 4 if and only if n is even.
24. Let p be a prime and k a positive integer such that a^k mod $p = a$ mod p for all integers a. Prove that $p - 1$ divides $k - 1$.
25. Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.
26. Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

4.9 Solutions of some selected problems

2. Use Lagrange's theorem
5. {0, 8, 16 ,6, 14,4,
7. Z_3
8. R^*
14. The coset $(3 + 4i)H$ is the circle with center at the origin and radius $|3 + 4i|$.
15. Use Lagrange's theorem
16. 42*n where $1 < n < 10$.
22. 1

Unit - 5 ❑ Permutation Groups

Structure

5.1 Objective

The followings are discussed here:

- Definition of permutation group
- Operation on permutation
- Cyclic notation of permutation
- Transposition
- Alternation group

5.2 Introduction

Permutation groups are central to the study of geometric symmetries and to Galois theory, the study of finding solutions of polynomial equations. They also provide abundant examples of nonabelian groups. In this chapter, we shall deal with various concepts of permutations.

5.3 Definitions and Notation

Let X be a set. Then any bijection on X is called a permutation. We have already seen that the set of all permutation S_X forms a group under functional composition. If

X is finite, then we can assume that $X = \{1, 2, ..., n\}$. In this case we write S_n instead of S_X. The following theorem says that S_n is a group. We call this group the symmetric group on n letters. This group has $n!$ numbers of element, i.e., $|S_n| = n!$.

5.3.1 Notation :

Suppose $X = \{1, 2, 3, 4, 5\}$ and consider the permutation σ defined by $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 5$, $\sigma(4) = 1$ and $\sigma(5) = 4$. This permutation can also be expressed in array notation by writing

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

where the top row represent the original elements and the bottom row represents what each element is mapped to. Note that some texts use square brackets. This is one of the notations of a permutation. Below, we will see there is another way to represent permutations. Let us look at some specific examples.

Example 5.3.2 : Let $A = \{1, 2, 3, 4\}$. And suppose that $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$ ans then we would write

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

and to indicate the action of α on an element, say 2, we would write

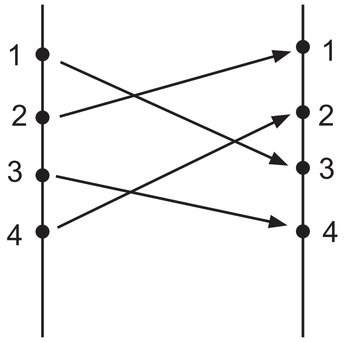


Fig. 5.1 : **Visualization of σ**

$$\sigma(2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}(2) = 1 \cdot$$

Example 5.3.3 : Any symmetry of an equilateral triangle is also a permutation. Let ΔABC be an equilateral triangle whose vertices are marked as A,B,C counterclockwise. Then each symmetry represents a permutation on the set $\{A, B, C\}$, see Figure 5.2:

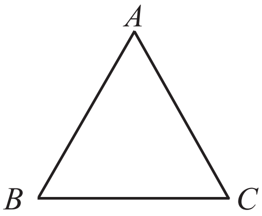
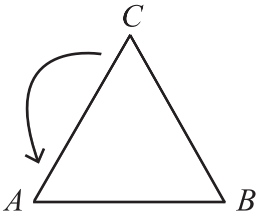
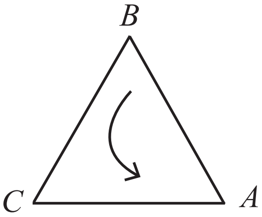
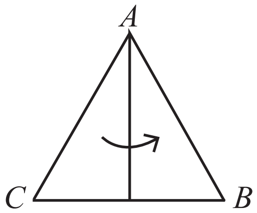
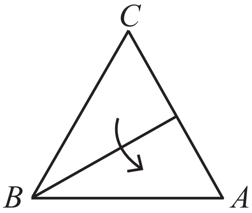
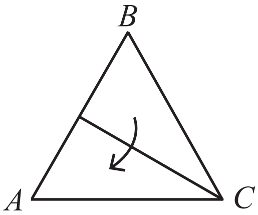
Group of Permutation of $\{A, B, C\}$	Group of Symmetries of an Equilateral Triangle	Interpretation
$p_1 = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ $(A)(B)(C)$		Do nothing
$p_2 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ (ABC)		Counterclockwise rotation of 120°
$p_3 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$ (ACB)		Counterclockwise rotation of 240°
$p_4 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ $(A)(BC)$		Flip through vertex A
$p_5 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$ $(AC)(B)$		Flip through vertex B
$p_6 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$ $(AB)(C)$		Flip through vertex C

***Fig. 5.2* : Symmetries of an equilateral triangle**

Example 5.3.4 : The identity permutation on A = {1, 2, 3, ..., n} is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 2 & 3 & 4 & \cdots & n \end{pmatrix},$$

in other words, it does not change anything.

5.4 Operation on Permutation

Above we said that Sn was a group under composition. Let us look in more detail at composition of permutations. Composition of permutations written in array notation is performed from right to left, that is the permutation on the right is performed first.

Let $A = \{1, 2, ..., n\}$ and $\sigma, \beta \in S_n$. Then the composition σβ is the functional composition. This composition can be written in cyclic notation as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \beta(1) & \beta(2) & \beta(3) & \cdots & \beta(n) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \beta\sigma(1) & \beta\sigma(2) & \beta\sigma(3) & \cdots & \beta\sigma(n) \end{pmatrix}.$$

Example 5.4.1 : Let $A = \{1, 2, 3, 4\}$ and $\sigma, \beta \in S_4$ defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Then

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

And

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

Example 5.4.2 : Consider two permutations

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Then

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

5.4.3 Inverse of Permutations :

If a permutation σ maps n_i to n_j, then the inverse permutation σ^{-1} maps n_j back to n_i. In other words, the inverse of a permutation can be found by simply interchanging the top and bottom rows of the permutation σ and (for convenience in reading) reordering the top row in numerical order 1, 2, ..., n.

For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \Rightarrow \sigma^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

Here, $\sigma(1) = 5$ so $\sigma^{-1}(5) = 1$.

5.5 Cyclic Notation

The notation that we have used to represent permutations up to this point is cumbersome, to say the least. To work effectively with permutation groups, we need a more streamlined method of writing down and manipulating permutations. The cycle notation was introduced by the French mathematician Cauchy in 1815. The notation has the advantage that many properties of permutations can be seen from a glance. We now present this notation.

Definition 5.5.1 : Let $A = \{1, 2, ..., n\}$. A permutation $\sigma \in S_n$ is a cycle of length k if there exists elements $a_1, a_2, ..., a_k \in A$ such that

$$\begin{gathered} \sigma(a_1) = a_2 \\ \sigma(a_2) = a_3 \\ . \\ . \\ . \\ \sigma(a_k) = a_1, \end{gathered}$$

and $\sigma(x) = x$ for all other elements $x \in A$. We write them as $(a_1, a_2, ..., a_k)$.

Example 5.5.2 : Let $A = \{1, 2, 3, 4, 5\}$ and $\sigma \in S_5$ defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

Then this permutation can be expressed in cyclic notation as (1, 3, 5, 4). Observe that there are also some other cyclic notations of this permutation as:

$$(1, 3, 5, 4) = (3, 5, 4, 1) = (5, 4, 3, 1) = (4, 1, 3, 5).$$

Bur we usually prefer the notation in ascending order.

Definition 5.5.3 When two cycles have no elements in common, they are said to be disjoint.

Example 5.5.4 The permutation

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

can be represented by (1, 2)(3, 4, 6)(5) and (1, 2)(3, 4, 6) if we omit the 1-cycle.

Note. *If you wanted to dial the telephone number* 413−2567 *but accidentally dialed* 314 − 5267, *then you permuted the digits according to* (2, 5)(3, 4).

Theorem 5.5.5 Let σ be any elements of S_n.

Then σ may be expressed as a product of disjoint cycles. This factorisation is unique. ignoring 1-cycles, up to order. Teh **cycle type** *of σ is the lengths of the corresponding cycles.*

Proof. We first prove the existence of such a decomposition. Let $a_1 = 1$ and define a_k recursively by the formula

$$a_{i+1} = \sigma(a_i).$$

Consider the set

$$\{a_i \mid i \in \mathbb{N}\}.$$

As there are only finitely many integers between 1 and n, we must have some repetitions, so that $a_i = a_j$, for some $i < j$. Pick the smallest i and j for which this happens. Suppose that $i \neq 1$. Then $\sigma(a_{i-1}) = a_i = \sigma(a_{j-1})$. As σ is injective, $a_{i-1} = a_{j-1}$. But this contradicts our choice of i and j. Let τ be the k-cycle $(a_1, a_2, \ldots, a_j)$. Then $\rho = \sigma\tau^{-1}$ fixes each element of the set

$$\{a_i \mid i \leq j\}.$$

Thus by an obvious induction, we may assume that ρ is a product of $k - 1$ disjoint cycles $\tau_1, \tau_2, \ldots, \tau_{k-1}$ which fix this set.

But then

$$\sigma = \rho\tau = \tau_1\tau_2 \ldots \tau_k,$$

where $\tau = \tau_k$.

Now we prove uniqueness. Suppose that $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$ and $\sigma = \tau_1\tau_2 \ldots \tau_l$ are two factorisations of σ into disjoint cycles. Suppose that $\sigma_1(i) = j$. Then for some p, $\tau_p(i) \neq i$. By disjointness, in fact $\tau_p(i) = j$. Now consider $\sigma_1(j)$. By the same reasoning, $\tau_p(j) = \sigma_1(j)$. Continuing in this way, we get $\sigma_1 = \tau_p$. But then just cancel these terms from both sides and continue by induction. □

Example 5.5.6 : Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Look at 1. 1 *is sent to* 3. *But* 3 *is sent back to* 1. *Thus part of the cycle decomposition is given by the transposition* (1, 3). *Now look at what is left* {2, 4, 5}. *Look at* 2. *Then* 2 *is sent to* 4. *Now* 4 *is sent to* 5. *Finally* 5 *is sent to* 2. *So another part of the cycle type is given by the* 3-*cycle* (2, 4, 5).

It is claimed then that

$$\sigma = (1, 3)(2, 4, 5) = (2, 4, 5)(1, 3).$$

This is easy to check. The cycle type is (2, 3).

Lemma 5.5.7 : *Let* $\sigma \in S_n$ *be a permutation, with cycle type* $(k_1, k_2, \ldots k_l)$. *The order of* σ *is the least common multiple* of $k_1, k_2, \ldots, k_l$.

Proof. Let k be the order of σ and let $\sigma = \tau_1\tau_2 \ldots \tau_l$ be the decomposition of σ into disjoint cycles of lengths $k_1, k_2, \ldots, k_l$.

Pick any integer h. As $\tau_1, \tau_2, \ldots, \tau_l$ are disjoint, it follows that

$$\sigma^h = \tau_1^h \tau_2^h \cdots \tau_l^h.$$

Moreover the RHS is equal to the identity, iff each individual term is equal to the identity.

It follows that

$$\tau_i^k = e.$$

In particular k_i divides k. Thus the least common multiple, m of $k_1, k_2, \ldots, k_l$ divides k. But $\sigma^m = \tau_1^m \tau_2^m \tau_3^m \cdots \tau_l^m = e$. Thus m divides k and so $k = m$. □

5.6 Transpositions

A 2-cycle is called a ***transposition***.

Since

$$(a_1, a_2, \ldots, a_n) = (a_1a_n)(a_1a_{n-1}) \ldots (a_1a_3)(a_1a_2),$$

any cycle can be written as the product of transpositions, leading to the following proposition.

Proposition 5.6.1 : Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Definition 5.6.2 : A permutation is said to be even if it can be expressed as the product of an even number of transpositions, and odd if it can be expressed as the product of an odd number of transpositions.

5.7 The Alternating Groups

One of the most important subgroups of S_n is the set of all even permutations, A_n. The group A_n is called the ***alternating group on*** *n* ***letters***.

Theorem 5.7.1 : *The set* A_n *is a subgroup of* S_n.

Proof. Since the product of two even permutations must also be an even permutation, A_n is closed. The identity is an even permutation and therefore is in A_n. If σ is an even permutation, then

$$\sigma = \sigma_1\sigma_2 \ldots \sigma_r,$$

where σ_i is a transposition and r is even. Since the inverse of any transposition is itself,

$$\sigma^{-1} = \sigma_r\sigma_{r-1} \ldots \sigma_1$$

is also in A_n. □

Proposition 5.7.2 : *The number of even permutations in* S_n, $n \geq 2$, *is equal to the number of odd permutations; hence, the order of* A_n *is* $n!/2$.

Proof. Let A_n be the set of even permutations in S_n and B_n be the set of odd permutations. If we can show that there is a bijection between these sets, they must contain the same number of elements. Fix a transposition σ in S_n. Since $n \geq 2$, such a σ exists. Define

$$\lambda_\sigma : A_n \to B_n$$

by

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Suppose that $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Then $\sigma\tau = \sigma\mu$ and so

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Therefore, λ_σ is one-to-one. We will leave the proof that λ_σ is surjective to the reader. □

Example 5.7.3 : The group A_4 is the subgroup of S_4 consisting of even permutations. There are twelve elements in A_4:

(1) (12)(34) (13)(24) (14)(23)
(123) (132) (124) (142)
(134) (143) (234) (243).

5.8 Summary

In this unit, we have studied various concept of permutation group. We have showed that a permutation can be expressed as the product of transpositions. The concept of alternating group is also discussed in this unit.

5.9 Worked Examples

1. **Find the orbit and cycles of the following permutations:**

(a) $\begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} & \mathbf{9} \\ \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{1} & \mathbf{6} & \mathbf{7} & \mathbf{9} & \mathbf{8} \end{pmatrix}$

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

Solution:

(a) Clearly $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$ = (1, 2, 3, 4, 5)(6)(7)(8, 9). So orbit of 1, 2, 3, 4 and 5 is the set {1, 2, 3, 4, 5}; orbit of 6 is 6; orbit of 7 is 7; orbit of 8 and 9 is the set {8, 9}. Also (1, 2, 3, 4, 5) and (8, 9) are its cycles.

(b) Again $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ = (1, 6, 2, 5)(3, 4). So the orbit of 1, 2, 5 and 6 is the set {1, 2, 5, 6}; and the orbit of 3 and 4 is the set {3, 4}. Also (1, 6, 2, 5) and (3, 4) are its cycles.

2. **Write the permutation in the worked example 1 as the product of disjoint cycles.**

Solution: We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$ = (1, 2, 3, 4, 5)(6)(7)(8, 9)

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

3. **Express as the product of disjoint cycles:**

(a) (1, 5)(1, 6, 7, 8, 9)(4, 5)(1, 2, 3).

(b) (1, 2)(1, 2, 3)(1, 2).

Solution:

(a) Let (1, 5)(1, 6, 7, 8, 9)(4, 5)(1, 2, 3) = τ . So we have $\tau = \tau_1\tau_2\tau_3\tau_4$, where

$\tau_1 = (1, 5)$, $\tau_2 = (1, 6, 7, 8, 9)$, $\tau_3 = (4, 5)$ and $\tau_4 = (1, 2, 3)$. Now

$$\begin{aligned}\tau(1) &= \tau_1\tau_2\tau_3\tau_4(1)\\ &= \tau_1(\tau_2(\tau_3(\tau_4(1))))\\ &= \tau_1(\tau_2(\tau_3(2)))\\ &= \tau_1(\tau_2(2))\\ &= \tau_1(2)\\ &= 2\end{aligned}$$

Repeating analogously, we have $\tau(2) = 3$; $\tau(3) = 6$; $\tau(6) = 7$; $\tau(7) = 8$; $\tau(8) = 9$; $\tau(9) = 5$; $\tau(5) = 4$; and $\tau(4) = 1$. Thus we have $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 6 & 1 & 4 & 7 & 8 & 9 & 5 \end{pmatrix}$ $= (1, 2, 3, 6, 7, 8, 9, 5, 4)$.

(b) Proceeding as in part (a), we have $(1, 2)(1, 2, 3)(1, 2) = (1, 3, 2)$.

4. **Prove that $(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$.**

   Solution: One can easily check $(1, 2, \ldots, n)(n, n-1, \ldots, 1) = I$, where I is the identity permutation. Hence $(1, 2, \ldots, n)^{-1} = (n, n-1, \ldots, 1)$.

5. **Show that A_3, the set of even permutations of {1,2,3} is a cyclic group with respect to the product of permutations. Find a generator of this cyclic group. Answer with reason.**

   Solution: The set of even permutations of $\{1,2,3\}$ is $A_3 = \rho_0, \rho_1, \rho_2$ where

   $$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

   Find the composition table and prove that the set A_3, the set of even permutations of $\{1,2,3\}$ is a commutative group with respect to the product of permutations.

   The order of this group is 3 and since 3 is a prime number, so A_3 is a cyclic group.

   Since $o(\rho_1) = 3$ and $o(A_3) = 3$, so ρ_1 is a generator of this group.

6. **Let $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. Find the smallest positive integer k such that $a^k = e$ in S_4.**

   Solution: S_4 is the symmetric group with respect to the multiplication of permutations of the set $\{1,2,3,4\}$ and e be the identity element in S_4.

   Now, $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ \ 3\ \ 2)$ which is a cycle of length 3.

   So $o(a) = 3$.

   Therefore, 3 is the least positive integer such that $a^3 = e$ in S_4.

7. **Prove that α = (3, 6, 7, 9, 12, 14) $\in S_{16}$ *is* not a prod-uct of 3-*cycles*.**

   Solution: Since α = (3, 14)(3, 12)...(3, 6) is a product of five 2-cycles, α is an odd cycle. Since each 3-cycle is an even cycle by the previous problem, a permutation that is a product of 3-cycles must be an even permutation. Thus, α is never a product of 3-cycles.

5.10 Model Questions

1. Write the following permutations in cycle notation.

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

2. Compute each of the following.

   (a) (1345)(234) (i) $(123)(45)(1254)^{-2}$

   (b) (12)(1253) (j) $(1254)^{100}$

   (c) (143)(23)(24) (k) |(1254)|

   (d) (1423)(34)(56)(1324) (l) $|(1254)^2|$

   (e) (1254)(13)(25) (m) $(12)^{-1}$

   (f) $(1254)(13)(25)^2$ (n) $(12537)^{-1}$

   (g) $(1254)^{-1}(123)(45)(1254)$ (o) $[(12)(34)(12)(47)]^{-1}$

   (h) $(1254)^2(123)(45)$ (p) $[(1235)(467)]^{-1}$

3. Express the following permutations as products of transpositions and identify them as even or odd.

   (a) (14356) (d) (17254)(1423)(154632)

   (b) (156)(234)

   (c) (1426)(142) (e) (142637)

4. Find $(a_1, a_2, \ldots, a_n)^{-1}$.

5. List all of the subgroups of S_4. Find each of the following sets.

   (a) $\{\sigma \in S_4 : \sigma(1) = 3\}$

   (b) $\{\sigma \in S_4 : \sigma(2) = 2\}$

   (c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

   Are any of these sets subgroups of S_4?

6. Find all of the subgroups in A_4. What is the order of each subgroup?
7. Find all possible orders of elements in S_7 and A_7.
8. Show that A10 contains an element of order 15.
9. Does A_8 contain an element of order 26?
10. Find an element of largest order in S_n for $n = 3, \dots, 10$.
11. Let $\sigma \in S_n$. Prove that σ can be written as the product of at most $n - 1$ transpositions.
12. Let $\sigma \in S_n$. If σ is not a cycle, prove that σ can be written as the product of at most $n - 2$ transpositions.
13. If σ can be expressed as an odd number of transpositions, show that any other product of transpositions equaling σ must also be odd.
14. If σ is a cycle of odd length, prove that σ^2 is also a cycle.
15. Show that a 3-cycle is an even permutation.
16. Prove that in A_n with $n \geq 3$, any permutation is a product of cycles of length 3.
17. Prove that any element in S_n can be written as a finite product of the following permutations.

    (a) (12), (13), . . . , (1n)

    (b) (12), (23), . . . , (n – 1, n)

    (c) (12), (12 . . . n)

5.11 Solution of some selected problems

1. (a) (1 2 4 5 3)

   (b) (1 4)(3 5)

   (c) (1 3)(2 5)

   (d) (2 4)
2. (a) (1 4) (3 2)
3. (a) (1 6)(1 5)(1 3)(1 4)
4. $(a_n, a_{n-1}, \dots, a_2, a_1)$

Unit - 6 ❑ Quotient Groups and Group Homomorphism

Structure

6.1 Objective

The followings are discussed here:

- Definition of quotient group
- Definition of group homomorphism, isomorphism and automorphism
- Properties of homomorphism
- Kernel of a homomorphism
- First, second and third isomorphism theorem
- Inner automorphism

6.2 Introduction

We have yet to explain why normal subgroups are of special significance. The reason is simple. When the subgroup *H* of *G* is normal, then the set of left (or right) cosets of *H* in *G* is itself a group—called the factor group of *G* by *H* (or the quotient group of *G* by *H*). Quite often, one can obtain information about a group by studying one of its factor groups. One of the important concept of group theory is the concept of homomorphism. Homomorphism is the natural group theoretic mapping between two groups preserving the binary compositions. The study of homomorphism reveals various properties of a group.

6.3 Quotient group

Theorem 6.3.1 : Let G be a group and H be normal subgroup of G. Then the set

$$G/H = \{gH : g \in G\}$$

is a group under the operation $g_1H * g_2H = g_1g_2H$ of order $[G : H]$.

Proof. This operation must be shown to be well-defined; that is, group multiplication must be independent of the choice of coset representative. Let $aH = bH$ and $cH = dH$. We must show that

$$aH * cH = acH = bH * dH = dbH.$$

Now $a = bh_1$ and $c = dh_2$ for some $h_1, h_2 \in H$. Then,

$$\begin{aligned} acH &= bh_1dh_2H \\ &= bh_1dH \\ &= bh_1Hd \\ &= bHd \\ &= bdH. \end{aligned}$$

Hence, the binary operation is well defined. Now the element eH acts as the identity element, since $aH * eH = eH * aH = aH$ for all $a \in G$. Associativity property holds automatically as G is a group. Now for any element $aH \in G/H$, the inverse element is $a^{-1}H$, since $aH * a^{-1}H = a^{-1}H * aH = eH$.

Hence, G/H forms a group. Since the number of cosets of H in G is $[G : H]$, therefore the order of the group G/H is $[G : H]$. □

Definition 6.3.2 : For a normal subgroup H of a group G, the set

$$G/H = \{gH : g \in G\}$$

with the binary operation $g_1H * g_2H = g_1g_2H$ is called Quotient group or Factor group.

Although the concept of quotient group is now considered to be fundamental to the study of groups, it is a concept which was unknown to early group theorists.It emerged relatively late in the history of the subject: toward the end of the 19th century. The main reason for this delay is that in order to give a recognizably modern definition of a quotient group, it is necessary to think of groups in an abstract way. Therefore the development of the concept of quotient group is closely linked with the abstraction of group theory.

This process of abstraction took place mainly during the period 1870-1890 and was carried out almost exclusively by German mathematicians. Thus by 1890 the development and understanding of the concept of quotient group had largely been completed.

Example 6.3.3 : Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$. Then the cosets of $3\mathbb{Z}$ are $0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$ and $2 + 3\mathbb{Z}$. The group $\mathbb{Z}/3\mathbb{Z}$ is given by the multiplication table below Since $|\mathbb{Z}/3\mathbb{Z}| = 3$ so $\mathbb{Z}/3\mathbb{Z}$ is isomorphic to $\mathbb{Z}_3$.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

Fig. 6.1

Theorem 6.3.4 : The quotient group of a cyclic group is cyclic.

Proof. Let H be a subgroup of G and $G = \langle a\rangle$. Then we will show that aH is a generator of G/H. Let $gH \in G/H$. Then $g = a^k$ for some integer k.

Now

$$\begin{aligned}(aH)^k &= aH * aH * \ldots * aH \ (k \text{ times})\\ &= a^kH = gH.\end{aligned}$$

Hence, G/H is a cyclic group generated by aH. □

6.4 Group Homomorphism

Definition 6.4.1 (Homomorphisms). A mapping φ from a group (G, o) to a group $(H, *)$ is called a homomorphsim if it preserves the group operation, i.e., $\varphi(\text{a o b}) = \varphi(a) * \varphi(\text{b})$ for all $a, b \in G$.

Definition 6.4.2 : If φ is a homomorphism of G into H, the kernel of φ, Ker_φ, is defined by $Ker_\varphi = \{x \in G : \varphi(x) = e', e' = \text{identity element of } H\}$.

Proposition 6.4.3 : *Let G and H be groups and let* $\varphi : G \to H$ *be a homomorphism.*

(i) $\varphi(e) = e'$, *where e and e′ are the identities of G and H, respectively.*

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ *for all* $g \in G$.

(iii) $\varphi(g^n) = \varphi(g)^n$ *for all* $g \in G$.

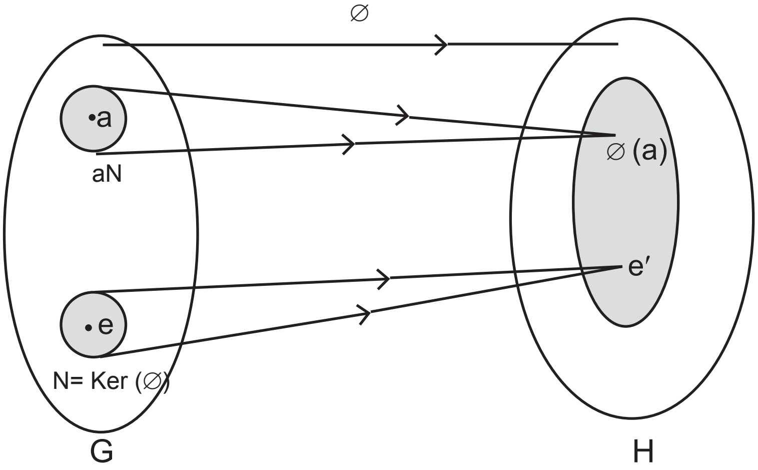


***Fig. 6.2* : Homomorphism φ : G → H**

Proof. (i) *Since* $\varphi(e) = \varphi(e \text{ o } e) = \varphi(e) * \varphi(e)$, *the cancellation laws shows that* $\varphi(e) = e'$.

(ii) $\varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ and, by part (i), $\varphi(e) = e'$, we get

$$e' = \varphi(g)\varphi(g^{-1}).$$

Now multiplying both sides on the left by $\varphi(g)^{-1}$, we get the result.

(iii) This can be easily deduced by using induction and (i) and (ii). □

Proposition 6.4.4 : *Let* φ *be a homomorphism from* (G, o) *to* $(H, \cdot)$*. Then*

(i) kernel of φ, ker_φ, *is a normal subgroup of G,*

(ii) image of φ, Im_φ, *is a subgroup of H.*

Proof. (i) Since $\varphi(e) = e'$, so ker_φ is non-empty. Let $a, b \in ker_\varphi$. Then $\varphi(a \circ b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e' \cdot e' = e'$. Therefore, $a \circ b^{-1} \in Ker_\varphi$. Hence, ker_φ is a subgroup of G.

Now to prove ker_φ is normal, take $x \in G$. Then, for any $q \in ker_\varphi$,

$$\begin{aligned}\varphi(x \circ q \circ x^{-1}) &= \varphi(x) \cdot \varphi(q) \cdot \varphi(x^{-1}) \\ &= \varphi(x) \cdot e' \cdot \varphi(x)^{-1} \\ &= e'.\end{aligned}$$

Hence, $xker_\varphi x^{-1} \subseteq ker_\varphi$ for all $x \in G$. Therefore, ker_φ is a normal subgroup of G.

(ii) Since $\varphi(e) = e'$, the identity of H lies in Im_φ, so Im_φ is nonempty. Let $x, y \in Im_\varphi$. Then there exists $a, b \in G$ such that $\varphi(a) = x$ and $\varphi(b) = y$.

Now by using homomorphim and proposition 6.5, we get

$$x \cdot y^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a \cdot b^{-1}).$$

Therefore, $x \cdot y^{-1} \in Im_\varphi$. So, Im_φ forms a subgroup of H. □

Theorem 6.4.5 : *A* homomorphism $\varphi : G \to H$ is injective if and only if $\text{Ker}_\varphi = \{e\}$.

Proof. Suppose φ is injective, and let $a \in Ker_\varphi$. Then $\varphi(e) = e' = \varphi(x)$.

Hence, $x = e$. Therefore, $ker_\varphi = \{e\}$.

Conversely, suppose $ker_\varphi = \{e\}$ and $x, y \in G$ such that $\varphi(x) = \varphi(y)$.

Then

$$\varphi(x \circ y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} = e'.$$

Therefore, $x \circ \mathrm{y}^{-1} \in ker_\varphi$. But $ker_\varphi = \{e\}$. Hence $x \circ y^{-1} = e$, i.e., $x = y$. □

Definition 6.4.6 (Isomorphism). A homomorphism φ from a group G to a group H is called isomorphism if φ is one-to-one and onto map.

If there is an isomorphism from a group G to a group H, we say that G and H are isomorphic and write $G \approx H$.

Philosophical considerations give isomorphism a particular importance. Abstract algebra studies groups but does not care what their elements look like. Accordingly, isomorphic groups are regarded as instances of the same "abstract" group. For example, the dihedral groups of various triangles are all isomorphic, and are regarded as instances of the "abstract" dihedral group D_3.

Example 6.4.7 : Let G be the real numbers under addition and let H be the positive real numbers under multiplication. Then G and H are isomorphic under the mapping $\varphi(x) = 2^x$. To prove that this map is onto-to-one, suppose $2x = 2y$. Which implies that $\log_e 2^x = \log_e 2^y$, and therefore $x = y$. For "onto," we must find for any positive real number y some real number x such that $\varphi(x) = y$, that is, $2x = y$. Now, solving for x gives $\log_2 y$. Again,

$$\varphi(x + y) = 2x + y = 2x \cdot 2y = \varphi(x) \cdot \varphi(y) \; \forall x, y \in G.$$

Therefore, G is isomorphic to H.

Example 6.4.8 : Any infinite cyclic group is isomorphic to $\mathbb{Z}$. Indeed, if a is a generator of the cyclic group, the mapping $a^k \to k$ is an isomorphism. Similarly, any finite cyclic group $\langle a \rangle$ of order n is isomorphic to $\mathbb{Z}_n$ and the isomorphism is defined by $a_k \to k \bmod n$.

Example 6.4.9 : The groups $U(5)$ and $U(10)$ are isomorphic, since both of them are cyclic groups of order 4.

Example 6.4.10 : $U(10)$ and $U(12)$ are not isomorphic, although they have same number of elements. First observe that, $x^2 = 1$ for all $x \in U(12)$. Now, suppose that $\varphi : U(10) \to U(12)$ is an isomorphism. Then,

$$\varphi(9) = \varphi(3) \cdot \varphi(3) = 1$$

and

$$\varphi(1) = 1.$$

Thus, $\varphi(9) = \varphi(1)$, but $9 \neq 1$. which contradicts the assumption that φ is one-to-one.

Example 6.4.11 : The quotient group $(\mathbb{R}/\mathbb{Z}, +) = \{r + \mathbb{Z} : r \in [0, 1)\}$ is isomorphic to the circle group S of complex numbers of absolute value 1. The isomorphism is given by $r + \mathbb{Z} \mapsto e^{i2\pi r}$.

Example 6.4.12 : There is no isomorphism from $\mathbb{Q}$, the group of rational number under addition, to $\mathbb{Q}^*$, the group of nonzero rational numbers under multiplication. Suppose there is an isomorphism φ. Then there exists a rational number a such that $\varphi(a) = -1$. But then,

$$-1=\varphi(a)=\varphi\left(\frac{1}{2}a+\frac{1}{2}a\right)=\varphi\left(\frac{1}{2}a\right)\cdot\varphi\left(\frac{1}{2}a\right)=\left[\varphi\left(\frac{1}{2}a\right)\right]^2.$$

However, no rational number squared is −1.

Theorem 6.4.13 (Properties of Isomorphism). *Suppose* φ *is an isomorphism from a group G to a group H. Then*

1. *For any elements a and b in G, a and b commute if and only if* $\varphi(a)$ *and* $\varphi(b)$ *commute.*
2. $G = \langle a\rangle$ *if and only if* $H = \langle\varphi(a)\rangle$.
3. $|a| = |\varphi(a)|$ *for all* $a \in G$, *i.e., isomorphism preserves order.*
4. *For a fixed integer k and a fixed group element b in G, the equation* $x^k = b$ *has the same number of solutions in G as does the equation* $x^k = \varphi(b)$ *in H.*
5. *If G is finite, then G and H has same number of elements of every order.*

Proof. Property 1 can be easily proved by using the property of isomorphism. Let $G = \langle a\rangle$. Take $q \in H$, then $p = \varphi^{-1}(q) \in G$. Hence, $p = a^k$ for some $k > 0$. Now, $q = \varphi(p) = \varphi(a^k) = \varphi(a)^k$. Hence, the second statement follows.

Third statement follows directly from the second one.

Forth statement follows from oder preserving property of isomorphism.

From third one, the fifth statement follows. □

Theorem 6.4.14 : *Let H be a normal subgroup of G. Then the mapping* $f : G \to G/H$ *defined by* $f(x) = xH$ *for* $x \in G$ *is an onto homomorphism with kernel H.*

Proof. Let us take two elements $x, y \in G$. Then $f(x) = xH$ and $f(y) = yH$.

Now

$$\begin{aligned} f(xy) &= xyH \\ &= (xH) * (yH) \\ &= f(x)f(y), \end{aligned}$$

which shows that f is a homomorphism.

Now the identity element of G/H is H. Hence, $ker_f = \{x \in G : f(x) = H\} = \{x \in G : xH = H\}$. Therefore, from the property of cosets, $Ker_f = H$. □

Theorem 6.4.15 (First Isomorphism Theorem). *Let* $\varphi : G \to G'$ *be an onto homomorphism. Then* G/Ker_φ *is isomorphic to* G', *i.e.,* $G/ker_\varphi \simeq G'$.

Proof. Since $H = Ker_\varphi$, H is normal subgroup of G. Let us define a mapping $f : G/H \to G'$ by $f(aH) = \varphi(a)$, $aH \in G/H$.

First we show that f is well defined in the sense that if $aH = bH$, then $f(aH) = f(bH)$. Now

$$\begin{aligned} aH = bH &\Rightarrow a^{-1}b \in H \\ &\Rightarrow \varphi(a^{-1}b) = e' \text{ Since } H = Kar_{\varphi} \\ &\Rightarrow \varphi(a^{-1})\varphi(b) = e' \\ &\Rightarrow \varphi(a) = \varphi(b) \\ &\Rightarrow f(aH) = f(bH), \end{aligned}$$

where e' is the identity of G'. So f is well defined.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & G \\ G/H \arrow[ur, "f"'] & \end{tikzcd}$$

Fig. 6.3 : **First Isomorphism Theorem**

Again for aH, $bH \in G/H$, we get

$$\begin{aligned} f(aH * bH) &= f(abH) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= f(aH)f(bH). \end{aligned}$$

Which shows that f is homomorphism.

Let $aH \in Ker_f$. Then $f(aH) = \varphi(a) = e'$. Which shows that $a \in Ker_{\varphi} = H$. Hence, $aH = H$. Thus, Ker_f only the identity element. So, f is one-one. Finally, f is onto, because each element of G' is of the form $\varphi(a)$ for some $a \in G$. And since $\varphi(a) = f(aH)$, the pre-image of $\varphi(a)$ is aH in G/H. Thus f is an isomorphism from G/H to G'. □

Example 6.4.16 : Let $\varphi : GL_n(\mathbb{R}) \to \mathbb{R} - \{0\} = \mathbb{R}^*$ defined by $\varphi(A) = det(A)$. Then φ is a homomorphism with kernel $SL_n(\mathbb{R})$. Therefore, by First isomoprhism theorem $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.

Example 6.4.17 : Those who learn some complex analysis, might know the Möbius transformation on the complex plane $\mathbb{C}$. The Möbius transformation looks like

$$A(z) = \frac{az+b}{cz+d} \tag{6.1}$$

where $ad - bc \neq 0$. Let M be the set of all Möbius transformation on $\mathbb{C}$.

Then M forms a group under the functional composition. Now consider the function $\varphi : GL_2(\mathbb{R}) \to M$ defined by

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

where A is the Möbius transformation defined in (6.1). Since composition of two Möbius transformations is same as product of their respective matrices, the function φ is a homomorphism. Also φ is onto. What is the kernel of φ? Or said differently, for what values of a, b, c, d, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gives the identity operator? It it only possible when $c = b = 0$ and $a = d = \lambda$ for $\lambda \in \mathbb{R}*$. Hence, the kernel is

$$ker_{\varphi} = \{\lambda I : \lambda \in \mathbb{R}^*\},$$

where I is the 2×2 identity matrix. Now by First Isomorphism theorem, we get

$$GL_2(\mathbb{R})/Ker_{\varphi} \simeq M.$$

The group $GL_2(\mathbb{R})/Ker_{\varphi}$ is called Projective General Linear group and is denoted by $PGL_2(\mathbb{R})$.

We have seen that the symmetric group S_n of all the permutations of n objects has order $n!$, and that the dihedral group D_3 of symmetries of the equilateral triangle is isomorphic to S_3, while the cyclic group C_2 is isomorphic to S_2. We now wonder whether there are more connections between finite groups and the group S_n. There is in fact a very powerful one, known as Cayley's Theorem.

Theorem 6.4.18 (Cayley's Theorem). *Any group G is isomorphic to a subgroup of Sym(G), where Sym(G) is the group of all bijections of G.*

Proof. The proof has been omitted. □

Theorem 6.4.19 (Second isomorphism Theorem). *Let H be a subgroup of G (not necessarily normal in G) and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and*

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

Theorem 6.4.20 (Correspondence Theorem). *Let N be a normal subgroup of a group G. Then $H \mapsto N/N$ is one-to-one correspondence between the set of subgroups H containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of H correspond to normal subgroups of G/N.*

Theorem 6.4.21 (Third Isomorphism Theorem). *Let G be a group and N and H be normal subgroups of G with $N \subset H$. Then*

$$\frac{G}{H} \cong \frac{G/N}{H/N}.$$

6.5 Automorphism

Definition 6.5.1 : An endomorphism of a group G, denoted by $End(G)$, is a homomorphism of G into G; an automorphism of a group G, denoted by $Aut(G)$, is an isomorphism of G onto itself.

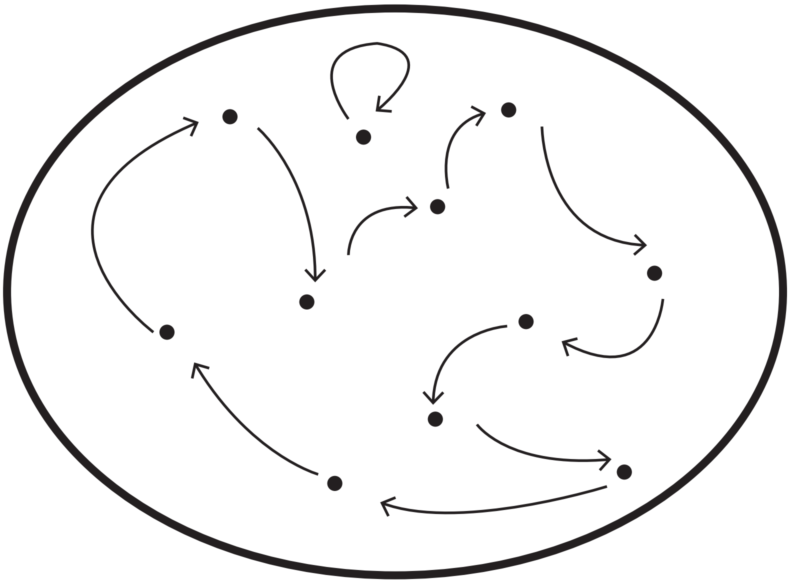


Fig. 6.4 : **Automorphism of *G***

Example 6.5.2 : Let G be a group. The identity mapping on G is an automorphism of G. This is called the identity automorphism and denoted by I_G.

Example 6.5.3 : Let G be an abelian group and the mapping $f : G \to G$ defined by $f(a) = a^{-1}$, $a \in G$. Then f is an automorphism.

Example 6.5.4 : Let $G = (\mathbb{C}, +)$ and the mapping $f : G \to G$ defined by $f(z) = \overline{z}$, $z \in G$. Then f is an automorphism.

Proposition 6.5.5 : *The $Aut(G)$ forms a group under composition.*

Proof. Since identity function $id_G \in Aut(G)$, so $Aut(G) \neq \phi$. Let $f, g \in Aut(G)$. Then it can conclude that $f \circ g$ is also a homomorphism. Also we know that composition of two bijective functions is also bijective. Therefore, $f \circ g$ is also an isomorphism. So, $f \circ g \in Aut(G)$.

The function composition automatically satisfies associativity property. The identity function I_G is the identity element.

Let $f \in Aut(G)$. Then the inverse function f^{-1} of f is the inverse element of $Aut(G)$. Hence $Aut(G)$ forms a group under composition. □

However, the class of abelian group is a little limited, and we should like to have some automorphism of non-abelian groups. Strangely enough the task of finding automorphism of non-abelian groups is easier than for abelian groups.

Let G be a group and $g \in G$. Then consider the mapping $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}, x \in G$.

Theorem 6.5.6 : The mapping I_g is an automorphism for each $g \in G$.

Proof. I_g is injective, because

$$I_g(x_1) = I_g(x_2) \Rightarrow gx_1g^{-1} = gx_2g^{-1} \Rightarrow x_1 = x_2.$$

I_g is onto, because an arbitrary element y in G has a pre-image of $g^{-1}yg$ in G.

Therefore, I_g is an bijection.

Let $x, y \in G$. Then

$$I_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = I_g(x)I_g(y).$$

Hence, I_g is a homomorphism. Thus I_g is an automorphism. □

Definition 6.5.7 : The automorphism I_g defined by $I_g(x) = gxg^{-1}$, $x \in G$ is said to be the inner automorphism of G determined by g.

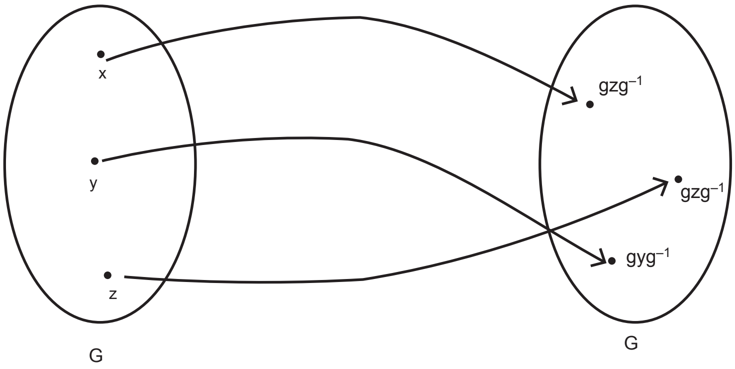


Fig. 6.5 : **Inner automorphism I_g**

The set of all inner automorphism of a group G is denoted by $Inn(G)$.

If G is abelian, then each mapping I_g for all $g \in G$ is simply the identity mapping. But if G is non-abelian, then there must be al least two distinct elements $g, x \in G$, such that $gx \neq xg$. Hence, the mapping I_g is non-trivial. Thus, the automorphism of non-abelian group is more interesting than that of abelian group.

Theorem 6.5.8 : *The inner automorphism $Inn(G)$ is a normal subgroup of $Aut(G)$.*

Proof. Since I_e is contained in $Inn(G)$, $Inn(G) \neq \phi$. Take Ig_1 , $Ig_2 \in Inn(G)$.

Then

$$\begin{aligned}(Ig_1 \circ Ig_2)(x) &= Ig_1(g_2xg_2^{-1}) = g_1(g_2xg_2^{-1})g_1^{-1}\\ &= (g_1g_2)x(g_1g_2)^{-1}\\ &= I_{g1g2}(x),\ \forall x \in G.\end{aligned}$$ □

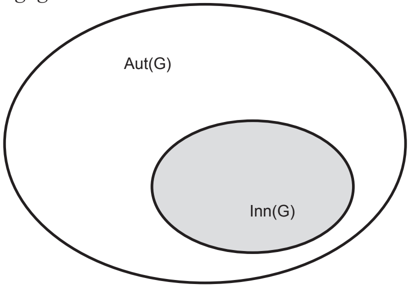


Fig. 6.6 **: Automorphism and inner automorphism of *G***

6.6 Summary

This unit deals with the concept of quotient group , homomorphism and isomorphism. The most important topic in this unit are the isomorphism theorems. The concept of automorphism and inner automorphism have been discussed.

6.7 Worked Examples

1. **Let *G* be a finite cyclic group of order n. Prove that $G \cong Z_n$.**

   Solution: Since G is a finite cyclic group of order n, we have $G = (a) = \{a^0 = e, a^1, a^2, a^3, ..., a^{n-1}\}$ for some $a \in G$. Define $\Phi : G \to Z_n$ such that $\Phi(a^i) = i$. By a similar argument as in the previous Question, we conclude that $G \cong Z_n$.

2. **Let *k, n* be positive integers such that *k* divides *n*. Prove that $Z_n/(k) \cong Z_k$.**

   Solution: Since Z_n is cyclic, we have $Z_n/(k)$ is cyclic by Theorem 5.1.2. Since Ord$((k)) = n/k$, we have order$(Z_n/(k)) = k$. Since $Z_n/(k)$ is a cyclic group of order k, $Z_n/(k) \cong Z_k$ by the previous Question.

3. Prove that Z under addition is not isomorphic to Q under addition.

Solution: *Since Z is cyclic and Q is not cyclic, we conclude that Z is not isomorphic to Q.*

4. Consider the group $\mathbb{R}^3$. *Let* H = $\{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + 2x_2 - x_3 = 0\}$. Show that H is a normal subgroup of $\mathbb{R}^3$. Show that $\mathbb{R}^3/H \simeq \mathbb{R}$.

Proof. The identity of the additive group $\mathbb{R}^3$ is $0 = (0, 0, 0)$. Notice that $0 \in H$ so $H \neq \varnothing$. Let $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ be two elements of H.

Then $x_1 + 2x_2 - x_3 = 0$ and $y_1 + 2y_2 - y_3 = 0$. It f ollows that the coordinates of $z = x - y = (x_1 - y_1, x_2 - y_2, x_3 - y_3)$ satisfy

$$(x_1 - y_1) + 2(x_2 - y_2) - (x_3 - y_3) = (x_1 + 2x_2 - x_3) + (y_1 + 2y_2 - y_3) = 0.$$

So $x - y \in H$ if $x, y \in H$. This directly proves that H is a subgroup of $\mathbb{R}^3$. Since $\mathbb{R}^3$ is abelian, any subgroup is automatically normal.

Alternatively, we can argue as follows: Now define $f : \mathbb{R}^3 \to \mathbb{R}$ by

$$f(x_1, x_2, x_3) = x_1 + 2x_2 - x_3.$$

Let $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ be two elements of $\mathbb{R}^3$. Then we verify that

$$\begin{aligned} f(x + y) &= f(x_1 + y_1, x_2 + y_2, x_3 + y_3) \\ &= (x_1 + y_1) + 2(x_2 + y_2) - (x_3 + y_3) \\ &= (x_1 + 2x_2 - x_3) + (y_1 + 2y_2 - y_3) \\ &= f(x) + f(y). \end{aligned}$$

So f is a group homomorphism. Looking at the definition of H, we notice $H = ker(f)$.

Since the kernel of any homomorphism is a normal subgroup, we find that H is a normal subgroup of $\mathbb{R}^3$. Given any $x \in \mathbb{R}$, we notice that $f(x, 0, 0) = x$, so f is an onto homomorphism. Thus by the first isomorphism theorem, we get an isomorphism $\mathbb{R}^3/H \simeq \mathbb{R}$.

5.a) Describe the set *Hom*($\mathbb{Z}^+$, $\mathbb{Z}^+$) of all homomorphisms $f : \mathbb{Z}^+ \to \mathbb{Z}^+$. Which of them are injective? which are surjective, which are authomorphisms?

b) Use the results of (a) to determine the group of automorphisms *Aut*($\mathbb{Z}^+$).

Solution:

a) Let $z \in Z$ we have two cases:

i) If $z \in Z_+$—set of non-negative integers.

Since 1 is the generator for z under addition

$$z = 1 + 1 + ... + 1(z \text{ times})$$

since f is a homomorphism;

$f(z) = f(1 + 1 + ... + 1) = f(1) + f(1) + ... + f(1) = zf(1)$

Let $f(1) = a \in Z$ then it follows that $f(z) = az$

ii) If $z \in Z$—set of negative integers –1 is also a generator for Z under addition:

$$z = -1 -1 - ... -1 = (-1) + (-1) + ... + (-1)(-z \text{ times})$$

As from the hyopthesis, f is a homomorphism;

$f(z) = f(-1 -1 ... -1) = f(-1) + f(-1) + ... + f(-1) = zf(-1)$

But $f(1) = a \Rightarrow f(-1) = -a \Rightarrow f(z) = -az$.

$\therefore$ we have proved that any homomorphism $f : Z^+ \to Z^+$ is of the form $f(z) = az$ where $a = f(1)$

Suppose that $f(z_1) = f(z_2)$) $az_1 = az_2 \Rightarrow z_1 = z_2$ when $a \neq 0 \Rightarrow f(z) = az$ is injective when $a \neq 0$.

When $a = \pm 1$, $f(z) = az = \pm z$ and f is surjective.

$\therefore$ Hom$(\mathbb{Z}^+,\mathbb{Z}^+) = \{f : Z^+ \to Z^+ : f(z) = az, z \in Z, a = f(1)\}$

b) $Aut(\mathbb{Z}^+) = \{f : Z^+ \to Z^+, f(z) = z, f(z) = -z\} = \langle f(z) = -z \rangle$

$\therefore Aut(\mathbb{Z}^+) \simeq C_2$.

6.8 Model Questions

1. Prove that $\det(AB) = \det(A) \det(B)$ for $A,B \in GL_2(\mathbb{R})$. This shows that the determinant is a homomorphism from $GL_2(\mathbb{R})$ to $\mathbb{R}^*$.
2. Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

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

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

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

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

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

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

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

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

(e) $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ defined by

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

where $M_2(\mathbb{R})$ is the additive group of 2 × 2 matrices with entries in $\mathbb{R}$.

3. Let A be an $m \times n$ matrix. Show that matrix multiplication, $x \mapsto Ax$, defines a homomorphism $\phi : \mathbb{R}^n \to \mathbb{R}^m$.
4. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be given by $\phi(n) = 7n$. Prove that ϕ is a group homomorphism. Find the kernel and the image of ϕ.
5. Describe all of the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.
6. Describe all of the homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$.
7. In the group $\mathbb{Z}_{24}$, let $H = \langle 4 \rangle$ and $N = \langle 6 \rangle$.

   (a) List the elements in HN (we usually write $H + N$ for these additive groups) and $H \cap N$.

   (b) List the cosets in HN/N, showing the elements in each coset.

   (c) List the cosets in $H/(H \cap N)$, showing the elements in each coset.

   (d) Give the correspondence between HN/N and $H/(H \cap N)$ described in the proof of the Second Isomorphism Theorem.
8. If G is an abelian group and $n \in N$, show that $\phi : G \to G$ defined by $g \mapsto g^n$ is a group homomorphism.
9. If $\phi : G \to H$ is a group homomorphism and G is abelian, prove that $\phi(G)$ is also abelian.
10. If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.
11. Show that a homomorphism defined on a cyclic group is completely determined by its action on the generator of the group.
12. Let G be a group of order p^2, where p is a prime number. If H is a subgroup of G of order p, show that H is normal in G. Prove that G must be abelian.
13. If a group G has exactly one subgroup H of order k, prove that H is normal in G.

14. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

15. Let G be a finite group and N a normal subgroup of G. If H is a subgroup of G/N, prove that $\phi^{-1}(H)$ is a subgroup in G of order $|H| \cdot |N|$, where $\phi : G \to G/N$ is the canonical homomorphism.

16. Let G_1 and G_2 be groups, and let H_1 and H_2 be normal subgroups of G_1 and G_2 respectively. Let $\phi : G_1 \to G_2$ be a homomorphism. Show that ϕ induces a natural homomorphism $\phi : (G_1/H_1) \to (G_2/H_2)$ if $\phi(H_1) \subseteq H_2$.

17. If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \times G/K$.

18. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism. Let H_1 be a normal subgroup of G_1 and suppose that $\phi(H_1) = H_2$. Prove or disprove that $G_1/H_1 \cong G_2/H_2$.

19. Let $\phi : G \to H$ be a group homomorphism. Show that ϕ is one-to-one if and only if $\phi^{-1}(e) - \{e\}$.

20. Given a homomorphism $\phi : G \to H$ define a relation $\sim$ on G by $a \sim b$ if $\phi(a) = \phi(b)$ for $a, b \in G$. Show this relation is an equivalence relation and describe the equivalence classes.

Automorphisms

1. Let $Aut(G)$ be the set of all automorphisms of G; that is, isomorphisms from G to itself. Prove this set forms a group and is a subgroup of the group of permutations of G; that is, $Aut(G) \leq S_G$.

2. An ***inner automorphism*** of G,
$$i_g : G \to G,$$
is defined by the map
$$i_g(x) = gxg^{-1},$$
for $g \in G$. Show that $i_g \in Aut(G)$.

3. The set of all inner automorphisms is denoted by $Inn(G)$. Show that $Inn(G)$ is a subgroup of $Aut(G)$.

4. Find an automorphism of a group G that is not an inner automorphism.

5. Let G be a group and ig be an inner automorphism of G, and define a map
$$G \to Aut(G)$$

by

$$g \mapsto i_g.$$

Prove that this map is a homomorphism with image $Inn(G)$ and kernel $Z(G)$. Use this result to conclude that

$$G/Z(G) \cong Inn(G).$$

6. Compute $Aut(S_3)$ and $Inn(S_3)$. Do the same thing for D_4.
7. Find all of the homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$. What is $Aut(\mathbb{Z})$?
8. Find all of the automorphisms of $\mathbb{Z}_8$. Prove that $Aut(\mathbb{Z}_8) \cong U(8)$.
9. For $k \in \mathbb{Z}_n$, define a map $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ by $a \mapsto ka$. Prove that ϕ_k is a homomorphism.
10. Prove that ϕ_k is an isomorphism if and only if k is a generator of $\mathbb{Z}_n$.
11. Show that every automorphism of $\mathbb{Z}_n$ is of the form ϕ_k, where k is a generator of $\mathbb{Z}_n$.
12. Prove that $\psi : U(n) \to Aut(\mathbb{Z}_n)$ is an isomorphism, where $\psi : k \mapsto \phi_k$.

6.9 Solutions of some selected problems

2. (a) $Ker(\phi) = \{1\}$

   (b) $Ker(\phi) = \{0\}$

   (e) $Ker(\phi)\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R) : b = 0\right\}$

4. $Ker(\phi) = \{0\}$, $Img(\phi) = 7Z$

Automorphism

7. All homomorphisms from Z to Z are of the type $n \to an$ for some fixed $a \in Z$. $Aut(Z) = Z_2$.

Further Reading

Further reading

[1] Dummit, David Steven, and Richard M. Foote. Abstract algebra. Vol. 3. Hoboken: Wiley, 2004.

[2] Fraleigh, John B. A first course in abstract algebra. Pearson Education India, 2003.

[3] Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.

[4] Herstein, Israel N. Topics in algebra. John Wiley & Sons, 2006.

[5] Lang, Serge. Undergraduate algebra. Springer Science & Business Media, 2005.

[6] Mapa, Sadhan Kumar. Higher Algebra, Abstract and Linear. Dipali Mapa, 2003.

[7] Rotman, Joseph J. A first course in abstract algebra. Pearson College Division, 2000.

[8] Chakraborty, A. Modern algebra. Sarat Book House (Levant Pub.)

NOTES

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

NOTES