THEORY OF GROUPS

Abdul Majeed Ph.D
Professor of Mathematics,
Department of Mathematics, FAST National University,
of
Computer and Emerging Sciences, Lahore Campus,
Faisal Town, Lahore.
Formerly
Professor of Mathematics
and
Chairman Department of Mathematics
and
Former Dean, Faculty of Science,
University of the Punjab, Lahore.

ILMI KITAB KHANA
Kabir Street, Urdu Bazar, Lahore-54000

Title : **Ilmi Theory of Groups**

Author : **Abdul Majeed**
Professor of Mathematics
Department of Mathematics,
FAST National University
of Computer and Emerging
Sciences, Lahore Campus.

Publisher : **Ilmi Kitab Khana**
Kabir Street, Urdu Bazar, Lahore-54000
Phone: 042-5018291, 7353510, 7248129

Printed at : **Al-Hajaz Printers**
Darbar Market, Lahore.
Phone: 7238009

Edition : **2013**

Price : **Rs. 200/-**

Foreword

Group theory is known as a powerful tool in various branches of mathematics and physics. It is particularly valuable in the study of symmetries that occur in nature and that can be analyzed by the theory in the visual and abstract sense. Its applications are manifold: in applied mathematics, physics, computer science, coding theory, chemistry and engineering. Because of its abstract nature, it develops the power of thinking coherently, analyze an argument logically and interpret a situation in a mathematically exact manner.

The book is especially designed for use as a text book for a complete advanced group theory course for students of M.A./M.Sc./ M.Phil (Mathematics) of Pakistani Universities. Its first few chapters cover the group theory requirements for an elementary abstract algebra course.

It is self-contained and self sufficient in the treatment of topics included in it. Its contents can meet the requirement for a two term course in group theory.

This book is an outcome of lectures delivered by the author to the graduate students of mathematics at Punjab University, Lahore, during the past several years and now at FAST National University of Computer and Emerging Sciences, Lahore Campus, for its M. S./Ph. D. classes.

The plan of the book as follows. The first three chapters are of elementary nature and deal with essentials of set theory including relations and functions, some of specific type, later used to relate various classes of groups. The novice may enjoy reading these chapters just because of the new treatment using ordered pairs.

A person having elementary knowledge about sets, relations and functions can straight away start from chapter *IV*.

Introduction of the concept of groups is given in chapter *IV*. This chapter contains a detailed discussion on the nature of subgroups of a group, a description of generators and relations for a group, the cyclic groups and the group of symmetries of some geometrical figures.

Chapter *V* contains one the most important theorems of group theory namely the Theorem of Lagrange. This theorem gives a relationship between the order of a finite group and that of its subgroups. The concept of normalizer and centralizer of a (subset) of a group also are discussed in

detail in this chapter. The notions of conjugate elements and conjugate subgroups of a group, together with their properties, are explained here. The concept of double coset in a group, which is a generalization of that of a coset, is a part of this chapter.

In Chapter *VI* we develop the concept of a normal subgroup of a group and give a method of forming a new class of groups called quotient groups. The relation of homomorphism between groups is examined and the fundamental theorem of homomorphisms is proved in this chapter.

As a part of new groups from old, we discuss the automorphism groups of a group and invariance of a subgroup of a group under the effect of automorphisms of that group.

Direct products and semidirect products of groups form the contents of Chapter *VII*. These also relate to forming new groups from old.

Permutations are the source of all developments of the theory. These are the groups of bijective mappings of a set. In Chapter *VIII* we discuss the elementary properties of groups of permutations. The last section of this chapter gives a brief account of the alternating group A_n, its generators and its simplicity (the characteristic property of having no normal subgroup) for $n \geq 5$. Some other classes of permutations, like transitive and primitive groups are also discussed.

Chapter IX relates the finite groups and their subgroups. These relations are obtained in the form of Sylow Theorems. Some consequences of these theorems are also examined here.

The idea of group actions has been developed and used to prove a number of results in groups theory. This concept forms the core of Chapter *X*. An action of a group G on a set X, which may itself be a group, is a special type of mapping from (G, X) to X. A simple example is the action of a permutation group G on a set X. This action is just a permutation of X. Orbits, stabilizers, and the Orbit-Stabilizer Theorem, together with their applications to the problems of groups, are the significant topics discussed in this chapter.

Normal series in groups and its special types like composition series and chief series are introduced in Chapter *XI*.

Solvable groups and nilpotent groups are considered in Chapters *XII* and *XIII*.

Chapters *XIV* and *XV* contain discussion of free groups, free products of groups, generalized free products of groups and other group theoretic

constructions. All these constructions yield new groups from the known ones.

Basic properties of linear groups are examined in Chapter *XVI*. Linear groups are also called matrix groups. Group representations which are just expressions of a group in terms reducible and irreducible representations and their applications, including a brief introduction of characters of representations, are discussed here.

The book has been written in an easily readable style. Attempt has been made to express the difficult ideas in a simpler and comprehensible manner.

In a sense, the book, the first of its kind in Pakistan, is a revised and extended version of my old book, The Theory of Groups. That book proved to be very popular with the students of post graduate classes of Pakistani Universities. I am sure that the present edition will be even more useful to the graduate students who want to specialize in Group Theory.

The material covered in the book provides sufficient necessary background for initiating research in some of the branches of group theory.

30-July, 2008 **Abdul Majeed**

Acknowledgements

The book exhibits a strong influence of the work and personality of some of the persons I have had the occasion to work with. These include my teachers Professor B. H. Neumann, FRS, Professor Hanna Neumann, Ph.D., D.Sc. of the Australian National University, Canberra, Australia and Professor John D. Dixon, FRSC (Fellow Royal Society of Canada) and Distinguished Professor at Carleton University, Ottawa, Canada.

I also express my gratitude to the FAST National University of Computer and Emerging Sciences, Lahore Campus, for making my task easier by providing me facilities to work in an excellent environment.

I have greatly benefitted from the books in the bibliography. But I feel satisfied by the fact that the book has been written by me in a very simple and easily comprehensible style. The subject is abstract and needs detailed explanation of almost all arguments in the proofs by carefully chosen words and illustrations by examples relevant to the concepts.

In the end I express my profound gratitude to Mr. Javed Iqbal, Proprietor Ilmi Kitab Khana, Lahore for his continued help in the preparation of this book.

I also thank Mr. M. Maqsood Bhutta for his help for carefully typing the manuscript.

I also thank my M. Phil Ph. D. students for their assistance in managing the manuscript in a much nicer manner.

30-July, 2008 Abdul Majeed

CONTENTS

Foreword (iii)
Acknowledgements (iv)

Chapter - I

BASIC CONCEPTS OF SET THEORY 1

1.1. Sets 1
1.2. Subset of a Set 3
1.3. Operations on Sets 5
1.4. Some Fundamental Results 8
1.5. Cartesian Product of Sets 11
Exercises 13

Chapter - II

RELATIONS ON SETS 17

2.1. Definitions 17
2.2. Types of Relations 18
2.3. Mappings or Functions 27
2.4. Theorems on Mappings 37
Exercises 42

Chapter - III

ALGEBRAIC OPERATIONS 47

3.1. Algebraic Operations 47
3.2. Algebraic Systems 52
3.3. Relations Between Algebraic Systems 56
Exercises 59

Chapter - IV

GROUPS 63

4.1. Definition and Consequences 63
4.2. Subgroups 71
4.3. Subgroup Lattices 75
4.4. Relations Between Groups 77
4.5. Systems of Generators and Relations in a Group 83
4.6. Cyclic Groups 88
4.7. Groups and Symmetries 97
Exercises 105

Chapter - V

COMPLEXES IN GROUPS 113

5.1. Complexes and Coset Decomposition of a Group **113**
5.2. Lagrange's Theorem **118**
5.3. Normalizers and Centralizers **130**
5.4. Conjugacy Relation in Groups **134**
5.5. Double Cosets **139**
Exercises **145**

Chapter - VI

NORMAL SUBGROUPS, FACTOR GROUPS 149

6.1. Normal Subgroups **150**
6.2. Quotient or Factor Groups **156**
6.3. Automorphism Group of a Group **165**
6.4. Commutator or Derived Subgroups **173**
6.5. Characteristic and Fully Invariant Subgroups **177**
Exercises **180**

Chapter - VII

PRODUCTS OF GROUPS 187

7.1. Direct Product of Groups **187**
7.2. Normal (or Semi-Direct) Products **195**
7.3. Holomorph of a Group **203**
7.4. Generalized Dihedral Group **204**
Exercises **205**

Chapter - VIII

GROUPS OF PERMUTATIONS 209

8.1. Symmetric or Permutation Groups **209**
8.2. Permutability of Permutations **213**
8.3. Cyclic Permutations and Orbits **214**
8.4. Order of a Permutation **219**
8.5. Transpositions, Even and Odd Permutations **220**
8.6. Generators of the Symmetric and Alternating Group **225**
8.7. Orbits, Stabilizer Subgroup and Transitive Groups **232**
Exercises **241**

Chapter - IX

SYLOW THEOREMS 245

9.1. Cauchy's Theorem for Abelian and Non-abelian Groups **246**
9.2. Sylow Theorems **248**
9.3. Miscellaneous Theorems **253**
Exercises **260**

Chapter - X

GROUP ACTIONS 263

10.1. Group Action **263**
10.2. A Basic Theorem **269**
10.3. Orbits and Transitive Actions **272**
10.4. Stabilizers **277**
10.5. Mappings Between G-Sets: The Orbit Stabilizer Theorem **280**
10.6. Applications to Group Theory **283**
Exercises **290**

Chapter - XI

SERIES IN GROUPS 293

11.1. Zassenhaus' Butterfly Lemma **293**
11.2. Normal Series **295**
11.3. Composition Series **302**
11.4. Chief or Principal Series **309**
Exercises **311**

Chapter - XII

SOLVABLE GROUPS 313

12.1. Solvable Groups **313**
12.2. Theorems on Solvable Groups **314**
Exercises **319**

Chapter - XIII

NILPOTENT GROUPS 321

13.1. Nilpotent Groups **321**
13.2. Finite Nilpotent Groups **329**
13.3. Upper Central Series **331**
13.4. The Frattini Subgroup **334**
13.5. Supersolvable Groups **338**
Exercises **342**

Chapter - XIV

FREE GROUPS AND FREE PRODUCTS OF GROUPS 345

14.1. Free Groups: Basic Theory **345**
14.2. Free Products of Groups **353**
Exercises **359**

Chapter - XV

SOME OTHER GROUP CONSTRUCTIONS 361

15.1. Generalized Free Product of Groups **361**
15.2. Permutational Product of Group **371**
15.3. Generalized Direct Product of Group **376**
15.4. Cartesian Product of Groups **379**
15.5. Wreath Product of Groups **381**
Exercises **385**

Chapter - XVI

LINEAR GROUPS 387

16.1. The General Linear Group **387**
16.2. Representations of Groups **390**
16.3. Group Algebras and Representation Modules **394**
16.4. Maschke's Theorem **403**
16.5. Group Characters **410**
16.6. Character Tables **414**
16.7. Lifted Characters **420**
Exercises **424**

Chapter - I

BASIC CONCEPTS OF SET THEORY

Set theory has been usefully employed in various branches of mathematical and social sciences. Specifically it forms a basis of all the fundamental concepts of mathematics specially algebra, topology and functional analysis. It is obviously impossible to give a complete discussion on various aspects of set theory, or, for that matter, to achieve coherent exposition of such a formalistic discipline. However, we shall try to present a summary of some of the basic aspects of the subject.

1.1. SETS

1.1. Sets and Their Description:

By a set we shall simply mean a *collection S of objects.* The objects in *S* are called *elements* of *S*. If a certain object '*a*' is in S then we write $a \in S$ (read as '*a* belongs to S', '*a* is a member of S, or '*a* is an element of S'). If an object *a* is not in S then we write $a \notin S$ (read as '*a* does not belong to S').

By a set we also mean a collection S of objects with a certain property which states whether or not a certain object belongs to S. This characteristic property which determines the set must be such that it can be used to decide, for every element, whether the element is in the set or not in it.

There are two ways to describe a set. The first is by writing down in parenthesis all the elements of that set explicitly. This is done mostly for the set consisting of a finite number of elements. When such a description is not possible or practical then we may, instead, indicate a characteristic property, which can enable us to determine whether or not a given object is a member of that set. More precisely if $P(x)$ is a proposition about a variable x, the collection of all elements x for which the statement $P(x)$ is true is denoted by

$$\{x : P(x)\}$$

read as 'the set of all x such that $P(x)$ is true'. This notation is usually called the *set builder notation.*

Certain sets may be describable in both ways.

We use the letters

$$A, B, C, X, Y, Z, \ldots \text{ etc.}$$

to denote a set.

1.1.1 Examples:

(i) The set M of students in a class of Mathematics in a post graduate class of a university. This set can be represented by:

M = {s: s is a student of a class of Mathematics in a post graduate class of a university}.

(ii) The set $\boldsymbol{Z}$ of integers, the set $\boldsymbol{Q}$ of rational numbers, the set $\boldsymbol{R}$ of real numbers, and the set $\boldsymbol{C}$ of complex numbers.

(Hereafter the letters $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, and $\boldsymbol{C}$ will denote number systems as indicated unless otherwise mentioned).

($\boldsymbol{Z}^+$, $\boldsymbol{Q}^+$, $\boldsymbol{R}^+$ shall stand for the sets of non-zero positive elements of these sets).

(iii) The set $\boldsymbol{C}_4$ consisting of the complex numbers 1, −1, i, −i, that is;

$$\boldsymbol{C}_4 = \{1, -1, i, -i\}.$$

(iv) The *solution set S* of a cubic equation. Here

$$S = \{\alpha \in C : \alpha \text{ is a root of } a_0x^3 + a_1x^2 + a_2x + a_3 = 0\}.$$

(v) The set P of all points in a circle of unit radius.

This set can be represented by the equation

$$P = \{(x, y) : x, y \in R, x^2 + y^2 < 1\}.$$

(vi) The set ℓ of all points on a line $y = mx + c$. This set has a representation.

$$\ell = \{(x, mx + c) : m, c, x, \text{ real numbers and } m, c, \text{ fixed}\}.$$

(vii) The set ϕ of positive integers less than − 1.

If Z^+ denotes the set of non-negative integers then ϕ can also, among many other ways, be described as:

$$\phi = \{x : x \in Z^+, x < -1\}.$$

1.2. SUBSET OF A SET

1.2.1 Subsets and Relations Between Them:

Let A be a set. By a *subset of* A we mean a set B all of whose elements are elements of A. B is a subset of a set A if every element of B is also an element of A.

A is then called a *superset* of B.

Usually when we discuss a subset in a particular situation, we talk of the subset with respect to a superset called the universal set for all subsets under discussion in that situation. It is denoted by the letter U. For example a universal set for the set of M.Sc (Mathematics) students in a university may be taken as the set U of all students of that university.

If B is a subset of A then we write $B \subseteq A$ (or $A \supseteq B$), read as 'B is contained in A' (or 'A contains B').

The symbol $\subseteq$ is called the *inclusion symbol.*

The *inclusion relation*, that is, the relation of 'being a subset of a set' is transitive. This means that if C is a subset of B and B is a subset of A then C is a subset of A. However the *membership relation*, that is, the relation of 'being an element of' is not transitive. Thus if an object b is a member of a set B and the set B is a member of a set A, then it is not always true that b should be a member of A. For example let $B = \{a, b, c\}$ and $A = \{u, v, B\}$. Then $b \in B$ but $b \notin$ A.

Two sets A and B are said to be *equal* if they consist of the same elements, and we write $A = B$.

Thus the sets A and B are equal if and only if every element of B is an elements of A *i.e.*, $B \subseteq A$ and conversely every element of A is an element of B *i.e.*, $A \subseteq B$.

A set which contains no element is called an *empty* (*vacous or null*) set. It is denoted by the symbol ϕ and is taken as a subset of every set. There is no logical difficulty in this assumption. For if S is any set then on the hypothesis that ϕ is not a subset of S implies the existence of an

element in ϕ which is not an element of S and this contradicts the definition of ϕ as a set containing no element.

A set B is called *proper subset of a set A* if B is a subset of A and $B \neq \phi$ and $B \neq A$, otherwise B is an *improper* subset of A.

The *power set* P(A) of a set A is the collection of all subsets of A. Both the empty set and the set A are members of $P(A)$.

1.2.1 Examples:

(a) The set E of even integers is a subset is a subset of the set $\boldsymbol{Z}$ of all integers.

(b) The set M of students in a Mathematics class of a University is a subset of the set U of all students in that University.

(c) The set

$B = \{(x, y): x, y \in \boldsymbol{R}, x^2 + y^2 = 1\}$

is a subset of the set

$C = \{(x, y): x, y \in \boldsymbol{R}, x^2 + y^2 \leq 1\}$

(d) Let A = {1, 2, 3, {1, 2, 3}} and B = {1, 2, 3}. Then B is both a subset and a member of A.

(e) Let $A = \{x : x \in \boldsymbol{R}, x - 1 = 0\}$, $B = \{x : x \in \boldsymbol{R}, x^2 - 1 = 0\}$,

$C = \{x : x \in \boldsymbol{R}, x^3 - 1 = 0\}$.

Then A = C and C is a subset of B.

(f) Let A = {a, b, c}. Then

P(A) = {$\{\phi\}, \{a\}, \{b\}; \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}$}

(g) The power set of the empty set ϕ is the set $\{\phi\}$ consisting of the set ϕ. Thus the power set of an empty set is not empty.

(i) The following sets are all equal (why?).

$A = \{x : x \in \boldsymbol{Z} \text{ and } x^2 < 0\}$, $B = \{x : x \in \boldsymbol{Z}, x \neq x\}$,

$C = \{x : x \text{ is a rational solution of } x^2 + x + 1 = 0\}$.

1.3. OPERATIONS ON SETS

1.3.1 Concepts of Union and Intersection of Sets:

Let Ω be a non-empty collection of sets. By the *union* of the sets in Ω we mean a set, to be denoted by $\cup\ \Omega$, whose elements are *all* the elements of the sets in Ω. Thus

$$\cup\,\Omega = \{x : x \in A, A \in \Omega\}.$$

If Ω consists of a finite number of sets $A_1, A_2, ..., A_n$, then we write.

$$\cup\,\Omega = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n.$$

In particular if A and B are sets then their union is a set $A \cup B$ whose elements are elements of A or elements of B, that is

$$A \cup B = \{x\,;\, x \in A \text{ or } x \in B\}.$$

Dual to the concept of union of sets is the concept of *intersection of sets.*

Let Ω be a non-empty collection of sets. The *intersection of the members* of Ω is a set, to be denoted by $\cap\,\Omega$, consisting of those elements which are common to *every* member of Ω. Thus

$$\cap\,\Omega = \{x : x \in A \text{ for } \textit{every } A \in \Omega\}.$$

Again, for the particular case when Ω consists of a finite number of sets only, say $A_1, A_2, ..., A_n$, then.

$\cap\,\Omega = \bigcup_{i=1}^{n} A_i = \{x : x \in A_i\ i = 1, 2, ..., n\}$, and for only two sets A and B,

$$A \cap B = \{x : x \in A \textit{ and } x \in B\}.$$

It is possible that the intersection of the members of Ω is the empty set ϕ. This is always so in the case when a member of Ω is itself empty. However, only here, we do not define the intersection of an empty collection of sets.

The union of an empty collection is the empty set ϕ.

It is easy to see that the intersection of a non-empty collection is a subset of every member of that collection.

The sets in a non-empty collection Ω are said to be *disjoint* if $A \cap B$ is the empty set ϕ for all $A, B \in \Omega$.

In particular the sets A and B are disjoint if $A \cap B = \phi$. Otherwise, they are said to be *overlapping*.

At times we shall resort to an indexing set to define the notion of union and intersection of sets. Let I be a set. With each $i \in I$ we associate a set A_i. Then

$$\Omega = \{A_i : i \in I\}$$

is said to be an *indexed family* of sets, and I is called the *indexing set.*

With this notation it is customary to denote the union and intersection of the family Ω by

$$\bigcup_{i \in I} A_i \text{ and } \bigcap_{i \in I} A_i$$

respectively.

By a *partition* of a set A we mean a collection of subsets A_α of A (α belonging to some indexing set I) such that.

(i) any two subsets of the collection are disjoint *i.e.*,

$$A_\alpha \cap A_\beta = \phi, \alpha \neq \beta, \alpha, \beta, \in I.$$

(ii) $\bigcup_{\alpha \in I} A_\alpha = A.$

For any two sets A and B we define another concept, called the *complement* of B with respect to A, as follows:

The *complement* of a set B relative to a set A is the totality of all elements of A which are not members of B. We denote it by $A \setminus B$ (read as "A minus B"). Thus

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

$A \setminus B$ is also called the difference of A and B.

Another way of representing a set is by using a diagram to represent the elements of the set.

In this case the universal set is taken as the set of points in a rectangle, circle or ellipse or any simply closed figure, supposed to

represent the objects of the set. The subsets of the set are then shown by closed curves, again usually circles or smaller rectangles.

Under this method a subset B of a set A is indicated as shown in the following diagram.

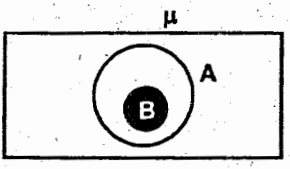


Figure 1.3.1

Such pictures are called *Venn diagrams* (after the British Mathematician John Venn) .

The notion of a Venn diagram helps to define another concept.

Let A and B be any sets. By the *symmetric difference* between A and B we mean a set $A \oplus B$ given by the equation:

$$A \oplus B = (A \setminus B) \cup (B \setminus A).$$

Using Venn diagram (which is a pictorial representation of sets), **$A \oplus B$ is as shown in figure.**

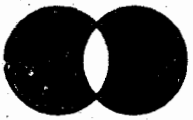


Figure 13.2. The shaded area is $A \oplus B$.

For any three sets A, B and C,

$$(A \oplus B) \oplus C = A \oplus (B \oplus C) \qquad (1.3.1)$$

Hence the relation $\oplus$ is associative.

This can be proved by the following pictorial representation of the two sides.

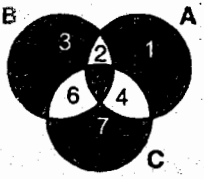


Figure 1.3.3. Shaded area showing $A \oplus B \oplus C$

Here $A \oplus B$ consists of the regions 1, 4, 3, 6, $B \oplus C$ consists of the regions 2, 3, 4, 7, So $A \oplus (B \oplus C)$ consists of the regions 1, 3, 5, 7 and $(A \oplus B) \oplus C$ also consists of the regions 1, 3, 5, 7. Hence the relation (1.3.1).

1.3.1 Examples:

(i) If $A_n = \left\{x \in \boldsymbol{R} : -\frac{1}{n} < x < \frac{1}{n} \text{ for all } n \in Z^+\right\}$.

Then $\cup \{A_n : n \in Z^+\} = \cup \{x : x \in A_n \text{ for some } n \in Z^+\} = A_1$

and $\cap \{A_n : n \in Z^+\} = \cap \{x : x \in A_n \text{ for every } n \in Z^+\} = \{0\}$.

(ii) Let

$C_0 = \{0, \pm 3, \pm 6, ...\} = \{3k : k \in Z\}$

$C_1 = \{..., -5, -2, 1, 4, 7, ...\} = \{3k + 1 : k \in Z\}$

$C_2 = \{..., -4, -1, 2, 5, 8, ...\} = \{3k + 2 : k \in Z\}$

Then $C_0 \cup C_1 \cup C_2 = Z$, $C_i \cap C_j = \phi$, $i \neq j$, $i, j = 0, 1, 2$.

Therefore, the subsets C_0, C_1, C_2 of Z define a partition of Z.

(iii) Let R_i be the set of students in the ith row of a class M of Mathematics and suppose that there are n distinct rows. Then $\bigcup_{i=1}^{n} R_i = M$, the set of students of the class of Mathematics, and

$R_i \cap R_j = \phi$, $i \neq j$, $i, j = 1, 2, ..., n$.

The collection of all R_i's, is therefore, a partition of M.

(iv) Let $A = \{\phi\}$, $B = \phi$. Then $A \cup B = \{\phi\}$ and $A \cap B = \phi$.

(Observe that A is a set consisting of an element namely the set ϕ. A set consisting of a single element is called a *singleton*)

1.4. SOME FUNDAMENTAL RESULTS

A few of the results related with the above definitions are enunciated in the following theorems.

1.4.1 Theorem:

For any sets A, B, C

(a) (Idempotent laws)

$A \cup A = A$

$$A \cap A = A$$

(b) (Commutative laws)

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

(c) (Associative laws)

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

The proofs of the above are straightforward and are left to the reader as exercises.

1.4.2 Theorem (Distributive laws):

For any sets A, B, C,

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof: We prove (a) only and leave the second to the reader as an exercise.

(a) Since

$$B \cap C \subseteq B, B \cap C \subseteq C,$$

we have

$$A \cup (B \cap C) \subseteq A \cup B \text{ and } A \cup (B \cap C) \subseteq A \cup C.$$

Hence

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \qquad (1.4.2)$$

Two show that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cup C)$,

let $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$, that is, $x \in A$ or $x \in B$ and $x \in A$ or $x \in C$

If $x \in A$, then $x \in A \cup (B \cap C)$, and if $x \notin A$, then $x \in B$ and $x \in C$ simultaneously. Thus $x \in B \cap C$ and again $x \in A \cup (B \cap C)$.

Hence

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C) \qquad (1.4.3)$$

Combining (1.4.2) and (1.4.3), we have,

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

1.4.3 THEOREM (De Morgan's Formula):

For any sets A, B, C,

(a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

(b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Proof

(a) Let $x \in A \setminus (B \cup C)$. Then $x \in A$ and $x \notin B$ and $x \notin C$ *i.e.*, $x \in A$ and $x \notin B \cup C$.

i.e., $x \in A, x \notin B$ and $x \in A, x \notin C$

i.e., $x \in A \setminus B$ and $x \in A \setminus C$

i.e., $x \in (A \setminus B) \cap (A \setminus C)$

Hence $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ (1.4.4)

Similarly one can prove that

Similarly one can prove that

$(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$ (1.4.5)

Combining (1.4.4) and (1.4.5) we get the desired result.

(b) This is left as an exercise to the reader.

1.5. CARTESIAN PRODUCT OF SETS

1.5.1 Ordered Pairs and Cartesian Products

A set of the form $\{\{x\}, \{x, y\}\}$ is called an *ordered pair*. This definition, which was historically important in reducing the theory of relations to the theory of sets, is due to Kuratowski. We shall denote this ordered pair by (x, y). Thus

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

The following theorem shows that the fundamental axiom on the equality of two ordered pairs is satisfied.

1.5.1 Theorem

Two ordered pairs (x, y) and (x_1, y_1) are equal if and only if

$$x = x_1, y = y_1$$

Proof:

The necessity of the condition is obvious.

For sufficiency, suppose that

$$(x, y) = \{\{x\}, \{x, y\}\} = \{\{x_1\}, \{x_1, y_1\}\}, \text{ (equal as sets)}$$
$$= (x_1, y_1)$$

Then we have the following two cases to discuss.

(a) $\{x\} = \{x_1\}, \{x, y\} = \{x_1, y_1\}$, (equal as sets)

(b) $\{x\} = \{x_1, y_1\}, \{x, y\} = \{x_1\}$.

If (a) holds then, since $\{x\} = \{x_1\}$, we have $x = x_1$ and so

$\{x, y\} = \{x_1, y_1\}$, with $x = x_1$, implies $y = y_1$.

If (b) holds then, from

$$\{x\} = \{x, x\} = \{x_1, y_1\},$$

we have

$$x = x_1 \text{ and } x = y_1. \tag{1.5.1}$$

Similarly $\{x, y\} = \{x_1\} = \{x_1, x_1\}$ implies

$$x_1 = x \text{ and } x_1 = y. \tag{1.5.2}$$

Hence (1.5.1) and (1.5.2) yield

$$x = x_1 = y = y_1 \text{ that is } x = x_1, y = y_1.$$

In general, an ordered n-tuple is written as $(x_1, x_2, ..., x_n)$. The element x_i is called the ith *component* or the ith *coordinate*, of the ordered n-tuple. We can now define the *cartesian product* of sets as follows:.

Let $A_1, A_1, ..., A_n$ be non-empty sets. By the *cartesian product* of $A_1, A_2, ..., A_n$, we mean a set P consisting of all ordered n-tuples

$$(a_1, a_2, ... a_n) ; a_i \in A_i, i = 1, 2, ..., n,$$

and denote it by

$$A_1 \times A_2 \times ... \times A_n.$$

Symbolically

$$P = A_1 \times A_2 \times ... \times A_n.$$

$$= \{(a_1, a_2, ..., a_n); a_i \in A_i, i = 1, 2, ..., n\}.$$

If any one of the A_i's is empty then their cartesian product is taken to be the empty set ϕ.[1]

In the particular case when $A_1 = A_2 = ... = A_n = A$ then P is called the nth *cartesian power* of A and is denoted by A^n.

Thus

$$A^n = \{(a_1, a_2, ..., a_n): a_i \in A \text{ for } i = 1, 2, ..., n\}.$$

The subset

$$D = \{(a, a, ..., a): a \in A\}$$

of A^n is called the *diagonal* of A^n.

---

[1]. More generally let $X = \{A_\alpha : \alpha \in I\}$ be a family of sets. The cartesian product of the family X is the set of all functions $f: I \to \cup A_\alpha$ such that $f(\alpha) \in A_\alpha$ for all $\alpha \in I$ and is denoted by

$$\Phi = \prod_{\alpha \in I} A_\alpha.$$

1.5.1 Example

(i) Let $A = \{a, b, c\}$, $B = \{1, 2\}$, then

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

and $B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$.

Note that the sets $A \times B$ and $B \times A$ are not equal.

(ii) Let $\boldsymbol{R}$ be the set of real numbers. The nth cartesian power $\boldsymbol{R}^n$ of $\boldsymbol{R}$ is called the *cartesian* n-*space*.

When n = 2 one obtains the ordinary cartesian plane $\boldsymbol{R}^2$. Thus

$$\boldsymbol{R}^2 = \{(x, y); x, y \in \boldsymbol{R}\}$$

EXERCISES

1. Verify the following relations for arbitrary sets.
   (a) $A \cup A = A = A \cap A$
   (b) $A \cap B \subseteq A \subseteq A \cup B$
   (c) $A \cup (B \setminus A) = A \cup B$.
   (d) $(A \setminus B) \cup (A \setminus C) = A \setminus (B \cap C)$.

2. Using any property of integers that may be needed, show that $\{x \in \mathbf{Z}: \exists\ m \in \mathbf{Z}$ with $x = 6m\} = \{y \in \mathbf{Z}: \exists\ p, q \in \mathbf{Z}$ with $y = 2p$ or $y = 3q\}$.

3. Show that a set consisting of n elements has exactly 2^n subsets.

4. A board of five members reaches its decision by a simple majority vote.
   What are the winning coalitions? (Hint. : Find all subsets consisting of 3 members or more).

5. Let $A_1, A_2, ..., A_n$ be a partition of a set X and B be any subset of X. Prove that:

$$\{A_1 \cap B, A_2 \cap B, ..., A_n \cap B\}$$

is a partition of B.

6. Let X be a set and P a collection of certain subsets of X. For $A, B \in P$, put

$$A \oplus B = (A \setminus B) \cup (B \setminus A)$$

and $A \otimes B = A \cap B$

Show that

(i) $A \oplus B = (A \cup B) \setminus (A \cap B)$

(ii) $A \oplus A = \phi$

(iii) $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$

7. Let $A \times B$ denote the cartesian product of A and B. Show that, for any non-empty A, B, C, D,

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

(ii) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(iii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

(iv) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

(v) $A \cap B = \phi$ implies $(A \times B) \cap (B \times A) = \phi$

(vi) $A \times B = B \times A$ if and only if $A = B$.

8. For any two sets A and B, prove that $A = (A \cap B) \cup (A \setminus B)$ is a partition of A.

9. Let $\{A_n : n \in \mathbf{Z}^+\}$ be a family of subsets of a set A.

Define a new family $\{B_n\}$ as follows

$$B_1 = A_1, B_n = A_n \setminus \bigcup_{k=1}^{n-1} A_k, n > 1.$$

Prove that all the B_n, $n \in Z^+$ are disjoint sets and that

$$\bigcup_{n \in \mathbf{Z}^+} A_n = \bigcup_{n \in \mathbf{Z}^+} B_n.$$

10. Can you explain the following situations (paradoxes)?

(i) A barber in a certain town shaves everyone who do not shave themselves, and only those. Who shaves the barber?

(ii) A fisherman, having caught a fish, tells the fish that if it cannot tell the fisherman what he is going to do with it then

he will eat it, otherwise, he will let it go. The fish answers "you are going to eat me". What can the fisherman do with the fish?

(The situation described by the statements given above describe what is known as the *Russels' Paradox*, after the famous British Mathematician - Philosopher Bertrand Russel. This paradox only mentions that a set cannot be an element of itself.)

Chapter - II

RELATIONS ON SETS

The concept of relations is one of the basic ideas of Mathematics. Algebraists constantly deal with the relation of equality and of isomorphism between various algebraic systems. Topologists use this notion in homotopy and isotopy theory. The functional relation is fundamental not only in Mathematics but in other natural and social sciences. We now describe it and discuss its various types.

2.1. DEFINITIONS

2.1.1. Binary Relations:

Let A and B be sets and $A \times B$ be their cartesian product. A subset R of $A \times B$ is called a *relation* from A to B.

If a pair $(a, b) \in R$, $a \in A$, $b \in B$ then a is said to be an *R-relative* of b and is written as $a\ R\ b$. If $(a, b) \notin R$ then we write $a \not R\ b$ (read as 'a is not an R-relative of b').

A relative R from A to B is said to be *empty* or *nullary* if $R = \phi$ and *full* it $R = A \times B$.

When R is a relation from A to B then the sets

$$D_R = \{a \in A: (a, b) \in R \text{ for some } b \in B\}$$

and

$$R_R = \{b \in B: (a, b) \in R \text{ for some } a \in A\}$$

are subsets of A and B and are called the *domain* and *range* of the relation R respectively. The relation R is clearly a subset of $D_R \times R_R$ but, in general, may not coincide with it.

By a *binary relation* R on (or in) a set A we mean a subset of $A \times A = A^2$. *Ternary, quaternary* and, in general, an n-ary relation on a set A can similarly be defined as a subset of A^3, A^4 respectively. §

One can easily see that the study of binary relations on A is simply the study of subsets of $A \times A$.

One can also speak about inclusion of a binary relation R in a binary relation R′ their intersection and union in the ordinary sense of inclusion, intersection and union of sets. Also the *complement of a binary relation R* is the subset.[1]

$$\tilde{R} = (A \times A) \setminus R$$

and, for any $(a, b) \in A \times A$, $(a, b) \in \tilde{R}$ if and only of $(a, b) \notin R$.

Let R and S be two relations on A. Then one can talk about the ***product*** **R.S of R and S in the following sense**

For $a, b \in A$, we say that $(a, b) \in R.S$ if and only if there exists a $c \in A$ such that $(a, c) \in R$ and $(c, b) \in S$.

A binary relation I is called the *identity relation on* A if

$$I = \{(a, a) ; a \in A\}.$$

Thus the diagonal of $A \times A$ defines the identity relation.

The *inverse of binary* relation R on A is the binary relation

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

Clearly $I.R = R.I = R$.

2.2. TYPES OF RELATIONS

A relation on a set A may or may not satisfy some specified conditions. Relations which do have certain additional properties are of relatively greater significance. A few of such relations are the following:

2.2.1. Reflexive relations:

A relation R on a set A is *reflexive* if R contains the identity relation I.

Thus R is reflexive if and only if $(a, a) \in R$ for all $a \in A$.

[1] The fact that a relation R from A to B is a particular case of a relation on a set follows from the fact that R is a relation on $A \cup B$.

2.2.2. Symmetric relations:

A relation R on A is *symmetric* if and only if $R = R^{-1}$, that is, R is symmetric if, for all $a, b \in A$, $(a, b) \in R$, implies $(b, a) \in R$ and conversely.

2.2.3. Transitive relations:

A relation R on A is said to be *transitive* if $R.R \subseteq R$.

Thus R is transitive if, for $a, b, c \in A$, $(a, b) \in R$, $(b, c) \in R$ implies $(a, c) \in R$.

2.2.4. Anti-symmetric relations:

An *anti-symmetric* relation on A is a relation R such that $R \cap R^{-1} \subseteq I$.

Thus a relation R is anti-symmetric if, for $a, b, \in A$, $(a, b) \in R$, $(b, a) \in R$ implies $a = b$

Among the various types of relations given above the relations which have the properties 2.2.1, 2.2.2, 2.2.3 and 2.2.1, 2.2.3, 2.2.4 are more important and are frequently used. Such relations are called *equivalence relations* and *order relations* respectively. A brief description of these is given below:

2.2.5. Equivalence relations:

A relation R on a set A is called an *equivalence relation* if and only if R is reflexive, symmetric and transitive.

The identity relation and the full relation on a set A are equivalence relations.

Equivalence relations on a set A are usually denoted by the symbol '~' (pronounced as 'tilde'), rather than by R, as a set of ordered pairs of elements of A.

Thus if R is an equivalence relation on A and $(a, b) \in R$ then we shall write $a \sim b$ and read it as 'a is related to b'.

With this notation the definition of an equivalence relation becomes:

A relation '~' on a set A is an equivalence relation if and only if for all $a, b, c \in A$,

(i) $a \sim a$

(ii) $a \sim b$ implies $b \sim a$

(iii) $a \sim b$ and $b \sim c$ implies $a \sim c$.

Let R be an equivalence relation on a set A and a be one of the members of A. Then a is related to some element of A, at least to a, by the reflexive property of R.

The set of those elements of A which are related to (also called *equivalent* to, in the case of an equivalence relation) a fixed element a of A under the relation R is called an *equivalence class* determined by the element a and is denoted by C_a. Thus

$$C_a = \{b \in A ; (a, b) \in R\}$$

For each $a \in A$, the equivalence class C_a is non-empty because, by the reflexive property of R, at least $(a, a) \in R$ and $a \in C_a$. The element a is called a ***representative element*** of C_a.

It is important to note that any pair of elements in an equivalence class are equivalent to each other.

The collection of all equivalence classes of a set A under an equivalence relation R is called the *quotient set* or the *factor set* of A determined by R. It is denoted by A/R.

We recall that a partition of a set A is a collection

$$\Omega = \{A_\alpha : A_\alpha \subseteq A, \alpha \in I\}$$

of subset of A such that

(i) $A_\alpha \cap A_\beta = \phi$, $A_\alpha, A_\beta \in \Omega$, $\alpha \neq \beta$, $\alpha, \beta \in I$

(ii) $\bigcup_{\alpha \in I} A_\alpha = A$.

The following fundamental theorem establishes a relationship between the partitions of A and the equivalence relations which can be defined on A.

2.2.6 Theorem: Each equivalence relation on a set A determines a partition of A and, conversely, every partition of A defines an equivalence relation on A.

Proof: Suppose that R is an equivalence relation on A and Ω the collection of equivalence classes of A determined by R. Then

$$\cup \Omega \subseteq A \qquad 2.2.6\ (i)$$

because each member of Ω is subset of A. Also, as R is reflexive, the pair $(a, a) \in R$ for all $a \in A$. Hence every $a \in A$ is in an equivalence class C_a, the equivalence class determined by a. Thus $a \in \cup \Omega$ for all $a \in A$. Hence

$$A \subseteq \cup \Omega \qquad 2.2.6\ (ii)$$

From (1) and (2) we have $A = \cup \Omega$ 2.2.6 (*iii*)

Further let C_a, C_b, $a, b \in A$, be *distinct* equivalence classes in Ω. We show that $C_a \cap C_b = \phi$. Suppose otherwise and let $x \in C_a \cap C_b$. Then $x \in C_a$ and $x \in C_b$ *i.e.*, $(a, x) \in R$ and $(b, x) \in R$. As R is symmetric, $(x, b) \in R$, By the transitivity of R, $(a, x) \in R$, $(x, b) \in R$ imply $(a, b) \in R$. Thus $b \in C_a$.

Now let $y \in C_b$. Then $(b, y) \in R$. Once again, by the transitivity of R, $(a, b) \in R$, $(b, y) \in R$ imply $(a, y) \in R$. Thus $y \in C_a$. Hence $C_b \subseteq C_a$. Similarly $C_a \subseteq C_b$. Hence $C_a = C_b$ which is a contradiction to our supposition that C_a and C_b are distinct. Therefore

$$C_a \cap C_b = \phi, \text{ for all } a, b \in A, a \neq b. \qquad 2.2.6\ (iv)$$

Equation 2.2.6 (iii) and 2.2.6 (iv) show that Ω is a partition of A. Hence every equivalence relation defines a partition of A.

Conversely, let the collection Ω of subset of A be a partition of A. Define a relation R on A as follows:

For two elements $a, b \in A$, $(a, b) \in R$ if and only if a and b are in the same member of Ω.

As Ω is a partition of A, every $a \in A$ is in some member of Ω. So $(a, a) \in R$ for all $a \in A$. Hence R is reflexive.

Moreover if $(a, b) \in R$ *i.e.*, a and b belong to the same member of Ω then b and a belong to the same member. Hence $(b, a) \in R$. Thus R is symmetric.

Next if $(a, b) \in R$ and $(b, c) \in R$ then a and b belong to the same member of Ω and b, c belong to the same member of Ω. Hence a, c belong to the same member of Ω. Thus $(a, c) \in R$ and R is transitive.

Hence R is an equivalence relation on A.

So very partition of A defines an equivalence relation on A.

2.2.7. Examples:

(*i*). The subsets ϕ and $A \times A$ of $A \times A$ are relations on A. These are called the *nullary* and the *full* relations on A, respectively. The latter is an equivalence relation.

(*ii*) Let $\boldsymbol{R} \times \boldsymbol{R} = \{(x, y) : x, y \in \boldsymbol{R}\}$ be the Cartesian plane and

$$X = \boldsymbol{R} \times \boldsymbol{R} \setminus \{O\}$$

where $O = \{(0, 0)\}$. Define a relation P on X as follows:

For $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$ in X, $(z_1, z_2) \in P$ if and only if there exists a non-zero real number λ such that $x_2 = \lambda x_1$, $y_2 = \lambda y_1$.

We show that P is an equivalence relation on X.

(a) P is reflexive because for any $z = (x, y) \in X$, $x = 1.\ x$, $y = 1.y$. Hence $(z, z) \in P$, for all $z \in X$.

(b) Let $(z_1, z_2) \in P$. Then $x_2 = \lambda x_1$, $y_2 = \lambda y_1$, for some $\lambda \neq 0$. Hence $x_1 = (1/\lambda)\, x_2$, $y_1 = (1/\lambda)\, y_2$. Thus $(z_2, z_1) \in P$ and P is symmetric.

(c) Let $(z_1, z_2) \in P$, $(z_2, z_3) \in P$, $z_3 = (x_3, y_3)$. Then there exist non-zero real numbers λ, ρ such that

$$x_2 = \lambda x_1,\ y_2 = \lambda y_1,\ x_3 = \rho x_2,\ y_3 = \rho y_2$$

Hence $$x_3 = (\rho\lambda)\, x_1,\ y_3 = (\rho\lambda)\, y_1,\ \rho\lambda \neq 0$$

so that $(z_1, z_3) \in P$. Hence P is transitive.

The equivalence classes determined by P are straight lines passing through the origin. The corresponding factor set X/P is called the *one dimensional projective space*.

(*iii*) Let $\boldsymbol{Z}$ be the set of integers and R be a relation defined on $\boldsymbol{Z}$ as follows:

For $m, n \in Z$, $(m, n) \in R$ if and only if m is less than or equal to n.

Then R is reflexive, anti-symmetric and transitive but is not symmetric. Hence R is not an equivalence relation on Z.

(*iv*) Let S be a set. Define a relation E on S as follows:

For $a, b \in$ S, $(a, b) \in E$ if and only if $a = b$ where '=' is the ordinary sign of equality.

The E is an equivalence relation on S and Ω the members of the factor set are all the singleton subset of S.

A comparison of this relation with the definition of an equivalence relation shows that an equivalence relation is a generalisation of the concept of ordinary equality relation.

(*v*) For a fixed integer n, define a relation R on the set Z of integers as follows:

For $a, b \in Z$, $(a, b) \in$ R, if and only if $a - b$ is a multiple of (or, what is the same thing, is divisible by) n. Then R is reflexive symmetric and transitive and therefore is an equivalence relation. This is the usual congruence relation '=' defined on integers. If $a, b \in Z$ are related under this relation then we write:

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

(read as "a is congruent to b modulo n").

The equivalence classes are the subsets $C_0, C_1, \ldots, C_{n-1}$ of Z consisting of integers leaving 0, 1, 2, ..., n − 1 as remainders respectively after division by n. The corresponding factor set is denoted by Z_n.

(*vi*) The usual geometrical relations of 'being congruent to' and of 'being similar' on the set T of all triangles in a plane are equivalence relations.

(*vii*) Let M denote the set of the students in a class of Mathematics. Define a relation R on M as follows:

For $a, b \in$ M, $(a, b) \in$ R if and only if a and b are of the same height.

Then R is an equivalence relation on M.

Likewise the relations of 'being of the same age', 'sitting in the same row' and of 'having the same father' are equivalence relations on M.

(*viii*) *The adjacency matrix.* There is another way to specify a relation R on a set X. This is to represent R with a matrix called its *adjacency matrix.* This representation matrix has rows and columns indexed by the elements of X listed in some arbitrary but fixed order. Each entry of the matrix is either 0 or 1. For two elements x, y of X the intersection of the row indexed by x and the column indexed by y is taken as 1 if $(x, y) \in R$. Otherwise it is taken as 0.

As an illustration let

$$X = \{x, y, z\}$$

and

$$R = \{(x, x), (x, y), (y, x), (y, y), (z, z)\}$$

Then the adjacency matrix of R is:

$$\begin{array}{c} \\ x \\ y \\ z \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Some properties of the relation R can be immediately verified from its adjacency matrix. For instance R is reflexive if all entries in the main diagonal are 1. R is symmetric if the matrix is symmetric which is the case if the entries at the (x, y) and (y, x) positions are the same. To verify the transitive property needs more care.

2.2.8 Order Relations:

Let A be a set. A relation R on A is called an *order relation* (or, to be more explicit, *a partial order relation*) if R is reflexive, transitive and anti-symmetric.

Thus a relation R, which is usually denoted by the symbol '$\leq$', is a partial order on A if and only if

(i) $a \leq a$ for all $a \in$ A.

(ii) $a \leq b$, $b \leq c$ implies $a \leq c$ for all $a, b, c \in$ A.

(iii) $a \leq b$ and $b \leq a$ implies $a = b$ for all, $a, b \in A$.

If $\leq$ is a partial order on A and $a \leq b$ for some $a, b \in A$, then we, sometime, also say that 'a precedes b'.

The set A together with the order relation $\leq$ is called a *partially ordered* set. That is the pair (A, $\leq$) is called a partially ordered set or a *poset.*

The elements a and b in a partially ordered set A are called *comparable* if and only if either $a \leq b$ or $b \leq a$.

A partially ordered set A is said to be *totally* (*simply* or *linearly*) ordered if any two elements in A are comparable.

The corresponding order relation is called *a total* (*simple linear*) order. A totally ordered set is also known as a *chain.*

2.2.9 The Hasse diagram

An interesting way to describe an order relation is by using the *Hasse diagram* (named after *Helmut Hasse*, a 20th century German number theorist). The *Hasse diagram* of a partial order R on X consists of a number of points on a plane, Each of these points represents an element of X. The points are placed in such a way that a line may be drawn going in the upward direction from each element x of X to each of its immediate successor missing the arrows implied by the transitive property. We then draw these lines.

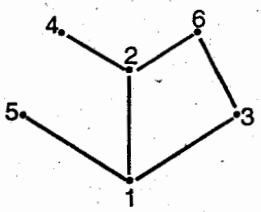
For example let

$$X = \{1, 2, 3, 4, 5, 6\}$$

and R be given by

$$R = \{(x, y) \in R \Leftrightarrow x \text{ divides } y\}.$$

Then the Hasse diagram of R is:



2.2.10. Examples of order relations:

1. The usual $\leq$ relation on the set $\boldsymbol{Z}$ (respectively $\boldsymbol{Q}$ and $\boldsymbol{R}$) of integers (rational and real numbers) is a partial order on $\boldsymbol{Z}$ (respectively $\boldsymbol{Q}$ and $\boldsymbol{R}$).

2. In the set **Z** of integers, define a relation R as follows:

'For $a, b \in \mathbf{Z}$, $(a, b) \in$ R if and only if 'a divides b'.

Then R is a partial order on **Z**. (Here by 'a divides b' we mean that there exists an integer $c \in \mathbf{Z}$ such that $b = ca$).

- R clearly is not a total order because, for instance, the integers 4 and 6 are not comparable.

3. Let P(A) be the *power set* of A. Each element of P(A) is a subset of A. The inclusion relation $\subseteq$ *i.e.,* for any two members S, T of P(A), *i.e.,* $S \subseteq T$, is a partial order on P(A):

4. The family S of all real valued sequences $\{s_n\}$ can be partially ordered in the following way:

Given the sequences $\{s_n\}$ and $\{t_n\}$, "we say that $\{s_n\}$ is less or equal to $\{t_n\}$ if there exists an integer k such that $s_n \leq t_n$ for all $n \geq k$". This defines a partial order in S.

Let A be a partially ordered set with $\leq$ as an order relation. An element $a \in$ A is called the *least element* of A if $a \leq x$ for all $x \in$ A. Analogously an element $b \in$ A is called the *greatest element* of A if $x \leq b$ for all $x \in$ A.

A set A is said to be *well-ordered* if every non-empty subset of it has a least element. An example of a set which is well ordered is the set **N** of all natural numbers under the usual ordering by magnitude, because it has a least element, namely 1. So every non-empty subset K of N contains an element m such that $m \leq k$ for all $k \in$ K.

This fact is known as 'The Well Ordering Principle'.

One of the most important applications of this fact is to establish the *principle of mathematical induction.* This principle provides a basis of a method of proof called the *proof* by *mathematical induction.*

2.2.11. Theorem:

(The principle of mathematical induction).

Let S be a subset of the set N of natural numbers such that

(i) $1 \in$ S and

(ii) whenever the integer $n \in$ S, $n + 1 \in$ S.

Then $S = N$.

Proof: Let $U = N \setminus S$. We shall show that $U = \phi$. Suppose that $U \neq \phi$.

Then, by the well ordering of N, U has a least element, say, a. Since $1 \in S$, $a \neq 1$ and so $a > 1$. Consequently

$$0 < a - 1 < a.$$

Since a is supposed to be the smallest integer in U, $a - 1$ is not in U and so $a - 1$ is in S. By (ii), $a - 1 + 1 = a \in S$, which is a contradiction to our supposition that $a \in U$. Hence $U = \phi$, as required.

About the well ordering of a set it would, however, be worthwhile to remember the famous result of set theory that every set can be well ordered. The proof of this theorem is beyond the scope of this book.

2.3. MAPPINGS OR FUNCTIONS

Mathematicians in general and algebraists in particular constantly deal with relation between sets satisfying certain additional properties. A special and perhaps the most important type of relations from a set A to a set B is the relation called a *mapping or a function from A to B.* In what follows, we shall briefly discuss the concept of mappings and a few of their special types. We shall, however, avoid defining a function or a mapping as a 'rule of correspondence'. Instead we define a mapping in terms of ordered pairs. Various results associated with the concept of mappings shall also be proved by making use of the notion of ordered pairs.

Let A and B be non-empty sets. *A mapping (or function) φ from A to B,* written as $\varphi : A \to B$, is a subset of $A \times B$ such that

(i) $D_\varphi = \{a \in A : (a, b) \in \varphi \text{ for some } b \in B\} = A$

and

(ii) $(a, b) \in \varphi$ and $(a, b) \in \varphi$ for $b, b' \in B$ imply $b = b'$.

If φ is a mapping from A to B and $(a, b) \in \varphi$ then $b \in B$ is called *the image of a* in A under φ and is written as

$$b = \varphi(a)$$

A mapping can also be defined by writing down the images of each element of A under φ.

Let $\varphi : A \to B$ be a mapping from A to B. Then

$$R_\varphi = \{b \in B; (a, b) \in \varphi \text{ for some } a \in A\}$$

is a subset of B and is called the *range of* φ.

When B = A we then say φ is a mapping from A to A.

It is important to note the following facts about a mapping φ *from* A to B.

(i) For any element $a \in A$ there is *precisely one* $b \in B$ such that $(a, b) \in \varphi$

(ii) Different elements of A may have only one $b \in B$ as their φ-relative, that is, for different $a, a' \in A$, there may be just one $b \in B$ such that both (a, b) and (a', b) are in φ.

Two mappings φ and ψ from A to B are said to be *equal* if and only if they are equal as subsets of $A \times B$. We then write $\varphi = \psi$. Since φ and ψ are mappings from A to B, A is the domain of both ϕ and ψ. So the sole requirement for the equality of mappings φ and ψ is that whenever, for any $a \in A$, $(a, b) \in \varphi$ for some $b \in B$ then $(a, b) \in \psi$ and conversely. In other words φ is equal to ψ if and only if

$$\varphi(a) = \psi(a)$$

for all $a \in A$.

Given any non-empty set A, the *identity mapping* $i_A : A \to A$ is simply the *identity relation on A.*

Recall that the identity relation is the diagonal of $A \times A$. Thus a mapping $i_A : A \to A$ is the identity mapping if and only if

$$i_A = \{(a, a) : a \in A\}$$

i.e., $i_A = a$ for all $a \in A$.

2.3.1. Examples:

1. Let $\boldsymbol{R}$ be the set of real numbers. Then the subsets

(a) $\varphi_1 = \{(x, e^x) : x \in \boldsymbol{R}\}$, (b) $\varphi_2 = \{(x, x^2) : x \in \boldsymbol{R}\}$

(c) $\varphi_3 = \{(x, mx + c) ; x \in \mathbf{R}$ and m, c fixed elements in $\boldsymbol{R}\}$,

are mapping from $\boldsymbol{R}$ to $\mathbf{R}$. These are usually written as:

$$\varphi_1(x) = ex,\ \varphi_2(x) = x^2,\ \varphi_3(x) = mx + c$$

for all $x \in \mathbf{R}$, respectively.

However the subset

$$\varphi = \{(x, \log x)\};\ x \in \boldsymbol{R}, x > 0\}$$

of $\boldsymbol{R} \times \boldsymbol{R}$ is not a function from $\boldsymbol{R}$ to $\boldsymbol{R}$ because in this case $D_\varphi \neq \boldsymbol{R}$. But if $x \in \boldsymbol{R}^+$, the set of non-zero positive real numbers, then, of course, φ is a function from $\boldsymbol{R}^+$ to $\boldsymbol{R}$.

For fixed $c \in \boldsymbol{R}$, the function $\varphi_c = \{(x, c)\ ;\ x \in \boldsymbol{R}\}$ is called the *constant mapping*. Its usual representation is

$$\varphi_c(x) = c \text{ for all } x \in \boldsymbol{R}.$$

When $c = 0$ we obtain the *zero function*.

2. Let $\mathbf{Z}$ be the set of integers. Then the subset

$$f = \{((m, n), m + n) : m, n \in \mathbf{Z}\}$$

of $(\mathbf{Z} \times \mathbf{Z}) \times \mathbf{Z}$ is a function from $\mathbf{Z}^2$ to $\mathbf{Z}$. This function can be represented by

$$f(m, n) = m + n\ ;\ m, n \in \mathbf{Z}.$$

3. Let A and B be non-empty sets and $A \times B$ their cartesian product. The subsets

$$\pi_A = \{((a, b), a) : a \in A, b \in B\}$$

$$\pi_B = \{((a, b), b) : a \in A, b \in B\}$$

of $(A \times B) \times A$ and $(A \times B) \times B$ respectively, define functions

$\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ given by

$$\pi_A(a, b) = a,\ \pi_B(a, b) = b.$$

These mappings are called *projections* of $A \times B$ onto A and B respectively.

4. For non-empty sets A and B, one may consider the collection B^A of all functions from A to B. B^A is the set of those subsets of $A \times B$ which are functions from A to B.

5. The function $f : N \to X$, where N is the set of natural numbers and X any non-empty set, given by

$$f(n) = x_n \in X$$

is called a *sequence* in X. If $X = \boldsymbol{R}$, the set of real numbers, then f is called a *sequence of real numbers.* The element x_n which is the image of $\in N$ is called the *nth term* of the sequence.

2.3.2. Types Of Mappings:

Mappings from a set A to a set B assume greater significance from the point of view of their application when some additional properties are satisfied by them. A few such mappings are described below.

2.3.2.1 Surjective or Onto Mappings:

A mapping φ from A to B is said to be *subjective* or *onto* if $R_\varphi = B$.

Thus φ is surjective if and only if, for every $b \in B$, there is an element $a \in A$ such that $(a, b) \in \varphi$, *i. e.*, for every $b \in B$ and some $a \in A$.

$$b = \varphi(a)$$

Hence φ is surjective if every element of B is the image of some element from A.

3.3.2 Examples:

1. The identity mapping $i_A : A \to A$ is surjective.

2. The mapping $\pi_A : A \times B \to A$, and $\pi_B : A \times B \to B$ given by

$$\pi_A(a, b) = a, \pi_B(a, b) = b, a \in A, b \in B$$

are surjective.

3. The mapping $\phi : \boldsymbol{R}^+ \to \boldsymbol{R}$ given by

$$\varphi(x) = \log x$$

is surjective. However the mapping $\psi : \boldsymbol{R} \to \boldsymbol{R}$ given by

$$\psi(x) = e^x$$

is not surjective because no negative real number is of the form e^x.

4. Let $\boldsymbol{Z}_n$ be the factor set of the set $\boldsymbol{Z}$ of integers determined by the relation of congruence modulo n. Elements of $\boldsymbol{Z}_n$ are equivalence classes $C_0, C_1, C_2, ..., C_{n-1}$.

Each class contains integers which leave the same remainder after division by n. The mapping $\varphi : Z \to Z_n$ given by:

$$\phi(m) = C_{r(m)}$$

where $r(m)$is the remainder after division of m by n, is surjective.

5. Let $\Omega = \{A_\alpha ; \alpha \in I\}$be a collection of non-empty disjoint subsets of X and $X = \cup A_\alpha$. Let P be a subset of $X \times \Omega$ defined as follows:

$$(x_\alpha, A_\alpha) \in P \text{ if and only if } x_\alpha \in A_\alpha$$

Then P defines a surjective mapping from X onto Ω given also by:

$$P(x_\alpha) = A_\alpha, x_\alpha \in A_\alpha, \alpha \in I.$$

2.3.4 Injective or One-One Mappings:

Let $\varphi : A \to B$ be a mapping. We call φ *injective or a one-one mapping* if $(a, b) \in \varphi$, $(a', b) \in \varphi$ implies $a = a'$.

Thus, for an injective mapping, distinct elements has distinct images, that is if for a, a' in A, $a \neq a'$ implies $\varphi(a) \neq \varphi(a')$.

Or equivalently: for a, $a' \in A$, $\varphi(a) = \varphi(a')$ implies $a = a'$.

2.3.5. Exmaples:

(i) The mapping $\alpha : Z \to Z$ given by:

$$\alpha(n) = 2n$$

is injective; Here $\alpha(m) = \alpha(n)$ implies $2m = 2n$ which, in turn, gives $m = n$.

(ii) The identity mapping $i_A : A \to A$ is injective.

(iii) The mappings $\varphi : R \to R^+$ and $\psi : R+ \to R$, given by $\varphi(x) = e^x, x \in \mathbf{R}$, $\psi(x) = \log x, \in \mathbf{R}^+$

are injective. To see that φ is injective, let $\varphi(x) = \varphi(y)$, $x, y \in \mathbf{R}$.

Then $e^x = e^y$ so that $e^{x-y} = 1 = e^0$.

Since x, y are real numbers the last equation implies that

$$x - y = 0 \text{ i. e., } x = y$$

2.3.6. One-One Correspondence (or Bijective Mappings)

A mapping $\varphi : A \to B$ which is injective as well as surjective is called a *bijective mapping* or a *one-one correspondence.*

The sets A and B having a one-one correspondence between them are called *equivalent (equipotent or, sometimes, equinumerous)* sets.

Thus two set A and B are said to be equivalent if there is a bijection φ from A to B. We then also say that A and B have the same cardinal number.

The *cardinal number* of a set A is denoted by $|A|$ or # A.

For each $n \in N$, a subset of N consisting of all natural number $\leq n$ is called the *ordinal n.*

A set A is said to be *finite* if there is a bijection between A and the ordinal n for some $n \in N$.

Otherwise A is said to be infinite.

If A and B are sets such that $|A| > |B|$, then, for any surjective mapping $\varphi : A \to B$, there are $a_1, a_2, \in A, a_1 \neq a_2$ such that $\varphi(a_1) = \varphi(a_2)$.

Thus, in case $|A| > |B|$, at least one pair of distinct elements of A must by associated with one and the same element of B under φ.

This simple fact is know as the '*pigeonhole principle*'. Because of this principle, if there are more letters than the pigeonholes then at least one pigeonhole must contain two letters. This principle has many applications in mathematics.

2.3.7. Examples:

1. The sets Z of integers and E of even integers, under the mapping φ given by:

$$\varphi(n) = 2n, n \in Z$$

are equivalent

2. The set R^+ of non-zero positive integers and R of real numbers under the mappings given by:

$$\varphi(x) = \log x, \qquad x \in R^+$$

or

$$\psi(x) = e^x, \qquad x \in R$$

are equivalent

3. Let X be a subset of R^2 given by:

$$X = \{(x, 0) : x \in R\}$$

The X and R are equivalent sets under the mapping $\varphi : X \to R$ given by:

$$\varphi(x, 0) = x \in R.$$

2.3.8. Restriction And Extension Of a Mapping:

Let $\varphi : A \to B$ be a mapping and A' a non-empty subset of A. Then $A' \times B$ is a subset of $A \times B$.

The subset

$$\varphi' = \varphi \cap (A' \times B)$$

of $A' \times B$ defines a mapping from A' to B and is called the *restriction of* φ to A'.

The restriction of $\varphi : A \to B$ to $A' \subseteq A$ is denoted by $\varphi/_{A'}$ (read as 'φ restricted to A'). It is given by the condition

$$\varphi/_{A'}(a) = \varphi'(a) = \varphi(a)$$

for all $a \in A'$.

If $\varphi' = \varphi/_{A'}$ is the restriction of φ to A' then φ is said to be an *extension of* φ', It is obvious that, for each function $\varphi : A \to B$, there is just one restriction of φ to a subset A' of A. However there can be more than one extensions of a mapping.

2.3.9. Example:

Let $f : R \to R$ be a mapping and $N \subset R$ be the set of natural numbers. Then the function $g : N \to R$ such that

$$g(n) = f(n)$$

for all $n \in N$ is the restriction of f to N. The function g is the restriction of f and defines a sequence of real numbers.

2.3.10. Composition of mappings: Product Mapping:

Let $\varphi : A \to B$ and $\psi : B \to C$ be mappings. Let α be the subset of $A \times C$ such that $(a, c) \in \alpha$ if and only if there exists a $b \in B$ such that $(a, b)\ \varphi$ and $(b, c) \in \psi$. Then α is called the composition of the mappings ϕ and ψ or the *product mapping* of φ and ψ and is denoted by $\psi.\ \varphi$ or

simply by $\psi\varphi$. Thus a mapping $\alpha = \psi\varphi : A \to C$ is the product mapping of φ and ψ if and only if

$$\alpha(a) = (\psi\varphi)(a) = \psi(\varphi(a))$$

for all $a \in A$.

2.3.11. Examples:

1. Let $f : R \to R$ and $\in' : R^+ \to R$ be the mappings given by:

$$\in(x) = e^x \text{ for all } x \in R$$

and

$$\in'(x) = \log x \text{ for all } x \in R^+.$$

The product mapping $(\in' \in)$ and $(\in \in')$ of $\in$ and $\in'$, and of $\in'$ and $\in$ respectively are given by:

$$(\in'\in)(x) = \in'(e^x) = \log e^x = x \log e = x = i_R(x), \text{ for all } x \in R,$$

$$(\in\in')(x) = \in(\in'(x)) = \in(\log x) = e^{\log x} = x = i_R + (x),$$

for all $x \in R^+$, respectively.

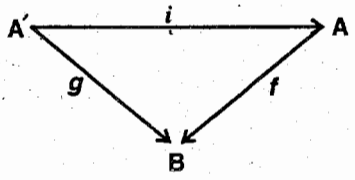
These product mappings are from $R \to R$ and $R^+ \to R^+$ and both are equal to the identity mapping on R and R^+ respectively.

2. Let $f : A \to B$ be a mapping and $g = f|_{A'}$, the restriction of f to a subset A′ of A. If $i : A' \to A$ denotes the *inclusion map i.e.,* the mapping such that $i(a') = a'$ for all $a' \in A'$, then the product of the mappings i and f is the mapping g because

$$(fi)(a') = f(i(a') = f(a') = g(a')$$

for all $a' \in A'$. Hence $g = fi$

This situation is represented by the accompanying diagram. In such a case the diagram A′ AB is said to be *commutative.*



3. For a fixed pair a, b of real numbers let f_{ab}; $R \to R$ be given by:

$$f_{ab}(x) = ax + b, x \in R.$$

Then $f_{ba}(x) = bx + a$.

The product $f_{ba} \cdot f_{ab}$ of f_{ab} and f_{ba} is a mapping from $R \to R$ given by:

$$(f_{ba} \cdot f_{ab})(x) = f_{ba}(ax + b) = b(ax + b) + a \quad (1)$$

Similarly $f_{ab} \cdot f_{ba}$ is given by

$$f_{ab} \cdot f_{ba}(x) = f_{ab}(bx + a) = a(bx + a) + b \quad (2)$$

Comparing (1) and (2) it is important to notice that

$$(f_{ba} \cdot f_{ab}) = b_{ax} + b^2 + a \neq abx + a^2 + b = f_{ab} \cdot f_{ba}(x)$$

for all $x \in R$.

Hence, in general, $f_{ba} \cdot f_{ab} \neq f_{ab} \cdot f_{ba}$

4. Let $A = \{a, b, c\}$, $B = \{x, y\}$, $C = \{1, 2, 3\}$ and let $f : A \to B$ and $g : B \to C$ be given by the subsets

$$f = \{(a, x), (b, y), (c, y)\}, g = \{(x, 1), (y, 2)\}$$

of $A \times B$ of $B \times C$, respectively. Then the subset

$$h = \{(a, 1), (b, 2), (c, 2)\}$$

of $A \times C$ defines the product mapping $g \cdot f$ of f and g.

2.3.12. Inverse of a Mapping:

Let $\varphi : A \to B$ be a mapping and $R_\varphi \subseteq B$ be the range of φ. For any $b \in R_\varphi$ let A_b be the subset of A consisting of all those $a \in A$ for which $(a, b) \in \varphi$. Then A_b is called the *inverse image set* of b under φ.

Suppose that is φ injective. Then $A_b = \{a\}$. So the subset

$$\varphi' = \{(b, a) ; (a, b) \in \varphi\}$$

of $(R_\varphi \times A) \subset B \times A$ defines a function from R_φ to A given by $\varphi'(b) = a$.

If φ is surjective as well then $R_\varphi = B$ and φ' is a mapping from B to A. In this case we call φ' the *inverse mapping of* φ. Thus:

The *inverse of a bijective mapping* $\varphi : A \to B$ is a mapping $\varphi' : B \to A$ such that $(b, a) \in \varphi'$ if and only if $(a, b) \in \varphi$, $a \in A$, $b \in B$.

It is usually denoted by φ^{-1}.

If φ^{-1} is the inverse mapping of φ then the product mapping $(\varphi^{-1}\ \varphi)$: $A \to A$ and $(\varphi\ \varphi^{-1})$: $B \to B$ are the identity mappings i_A and i_B of A and B respectively.

For if $a \in A$, then $(a, b) \in \varphi$ and $(b, a) \in \varphi^{-1}$ implies $(a, a) \in \varphi^{-1}\varphi$. Similarly if $b \in B$, then $(b, a) \in \varphi^{-1}$, $(a, b) \in \varphi$ implies $(b, b) \in \varphi\varphi^{-1}$ so that $\varphi^{-1}\varphi$ and $\varphi\varphi^{-1}$ are the identity relations on A and B respectively.

2.3.13. Examples:

The mapping $\in : R \to R^+$ and $\in' : R^+ \to R$ given by

$$\in(x) = e^x$$

for all $x \in R$, and

$$\in'(x) = \log x$$

for all $x \in R^+$, are inverses of each other.

2.3.14. Surjective Mappings and Factor Sets

Let $\varphi : A \to B$ be a surjective mapping. Then, for each $b \in B$, there is an $a \in A$ such that $\varphi(a) = b$. The set

$$\varphi^{-1}(b) = \{a' \in A : \varphi(a') = b\}$$

is then a subset of A and contains a. $\varphi^{-1}(b)$ is called the *fiber over the element b of B.*

Define a relation ~ on A as follows.

For $a_1, a_2 \in A$ we say that $a_1 \sim a_2$ if and only if $\varphi(a_1) = \varphi(a_2)$.

Clearly ~ is reflexive, symmetric and transitive and hence is an equivalence relation. We denote the equivalence class containing an element a of A of by $\bar{a}$ and the corresponding factor set consisting of all these equivalence classes by A / ~.

Note that, for each $a \in A$, $\bar{a}$ is a subset of A and consists of those elements a' of A for which $\varphi(a') = \varphi(a)$. Thus the equivalence class determined by a in A is the fiber $\varphi^{-1}(b)$, $b = \varphi(a) \in B$ given above. We write

$$\varphi^{-1}(b) = \bar{a} \text{ if and only if } \varphi(a) = b$$

for some $a \in A$, $b \in B$. we then have the following theorem.

2.3.15. Theorem: Every surjective mapping $\varphi : A \to B$ can be expressed as a product of a surjective and a bijective mapping.

Proof: Let ~ be the equivalence relation determined by φ. Let A / ~ denote the corresponding factor set. Define a mapping $v : A \to A / \sim$ as follows.

For each $a \in A$ we write $v(a) = \bar{a}$ where $\bar{a}$ is the equivalence class in A / ~ determined by a.

Clearly v is surjective. Consider the mapping $\bar{\varphi} : \bar{A} / \sim \to B$ defined by

$$\bar{\varphi}(\bar{a}) = b = \varphi(a), \bar{a} \in A/\sim, a \in A, b \in B.$$

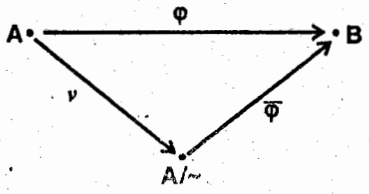
Then $\bar{\varphi}$ is surjective because each $b = \bar{\varphi}(\bar{a}) = \varphi(a) \in B$ is the image of some $\bar{a} \in A / \sim$. Also, for $a, a' \in A$,

$$\bar{\varphi}(\bar{a}) = \bar{\varphi}(\bar{a}')$$

implies $\varphi(a) = \varphi(a')$. Thus $\bar{a} = \bar{a}'$ because $a \in \bar{a}'$ and $a' \in \bar{a}$. Hence $\bar{\varphi}$ is bijective. Moreover

$$(\bar{\varphi} v)(a) = \bar{\varphi}(v(a)) = \bar{\varphi}(\bar{a}) = b = \varphi(a)$$

for all $a \in A$. Hence $\varphi = \bar{\varphi} . v$



so that φ has been factored as a product of a surjective and bijective mapping.

2.4. THEOREMS ON MAPPINGS

In this section we discuss a few results connected with the definitions of mappings given above. These theorems give necessary and sufficient conditions for mapping to be of a particular type.

Let $\varphi : A \to B$ be a mapping. A mapping $\varphi' : B \to A$ (respectively $\varphi'' : B \to A$) is called a *left (respectively right) inverse of* φ if and only if and only if $\varphi'\varphi = i_A$ (respectively $\varphi\,\varphi'' = i_B$).

We then have the following:

2.4.1. Theorem:

Let φ be a mapping from A to B. Then:

(i) φ is injective if and only if φ has a left inverse.

(ii) φ is surjective if and only if φ has a right inverse.

(iii) φ is bijective if and only if φ has both a left and *a* right inverse.

Proof:

(i) Suppose that φ is injective and let

$$\varphi' = \{(b, a) : (a, b) \in \varphi\}$$

Then φ' is a mapping from R_φ to A because $D_{\varphi'} = R_\varphi$ and $(b, a') \in \varphi'$, $(b, a'') \in \varphi'$ implies $(a', b) \in \varphi$, $(a'', b) \in \varphi$ which, by the injectivity $\overline{\varphi}(\overline{a})$ of φ, implies $a' = a''$. Moreover, for any $a \in A$, $(a, b) \in \varphi$, $(b, a) \in \varphi'$ implies $(a, a) \in \varphi'$. φ so that $\varphi'. \varphi = i_A$.

Conversely, let φ' be the left inverse of φ, *i.e.*, $\varphi' . \varphi = i_A$. Suppose $(a', b) \in \varphi$, $(a'', b) \in \varphi$. Then $(b, a') \in \varphi'$ and $(b, a'') \in \varphi'$ because only then (a' , a') and (a'' , a'') will belong to $\varphi' . \varphi = i_A$. Since φ' is a function, $(b, a') \in \varphi'$, $(b, a'') \in \varphi'$ implies $a' = a''$. Thus φ is injective.

(ii) Suppose that φ is surjective *i. e.*, for each $b \in B$, there is an $a \in A$ such that $(a, b) \in \varphi$. Define $\varphi'' : B \to A$ as follows:

For any $b \in B$, we take $(b, a) \in \varphi''$, where a is one of the elements of A, if and only if $(a, b) \in \varphi$

Then for each $b \in B$ there is an $a \in A$ such that $(b, a) \in \varphi''$, $(a, b) \in \varphi$.

This implies $(b, b) \in \varphi. \varphi''$. Hence $\varphi . \varphi'' = i_B$. Thus φ has a right inverse.

Conversely, let $\varphi : A \to B$ have a right inverse $\varphi'' : B \to A$, that is, $\varphi . \varphi'' = i_B$. Then, for any $b \in B$, $(b, b) \in \varphi . \varphi''$. By definition of the product of φ'' and φ, there is an $a \in A$ such that $(b, a) \in \varphi''$ and $(a, b) \in \varphi$. Thus, for each $b \in B$, there is an $a \in A$ such that $(a, b) \in \varphi$. Hence φ is surjective.

The proof for (iii) follows from (i) and (ii).

From the above theorem it follows that a bijective mapping $\varphi : A \to B$ has a left inverse φ' as well as a right inverse φ'' and the two are equal because these were defined analogously. Put $\varphi' = \varphi'' = \varphi^{-1}$. Then φ^{-1} is simply the inverse of φ and satisfies the equations $\varphi - 1 \cdot \varphi = i_A$ and $\varphi\, \varphi^{-1} = i_B$.

Henceforth we shall write $\varphi . \psi$ as $\varphi\, \psi$.

2.4.2 Theorem:

Let $\varphi : A \to B$ and $\psi ; B \to C$ be mappings. Then

(i) $\psi\varphi$ is injective if both φ and ψ are injective.

(ii) $\psi\varphi$ is surjective if both φ and ψ are surjective.

Proof:

(i) Let $\varphi : A \to B$ and $\psi : B \to C$ be injective mappings. For some c $\in$ C, let $(a, c), (a', c), \in \psi\varphi$ for $a, a' \in A$. Then by definition of the product mapping, there exist $b, b' \in B$ such that $(a, b) \in \varphi$, $(b, c) \in \psi$ and $(a', b') \in \varphi$, $(b', c) \in \psi$. As ψ is injective, $(b, c) \in \psi$, $(b', c) \in \psi$ implies $b = b'$. Also, as φ is injective, $(a, b) \in \varphi$, $(a', b) \in \varphi$ implies $a = a'$. Thus $(a, c) \in \psi\varphi$, $(a', c) \in \psi\varphi$ implies $a = a'$, Consequently $\psi\varphi$ is injective.

(ii) Let φ and ψ be surjective. Since ψ is surjective, for any $c \in C$, there is a $b \in B$ such that $(b, c) \in \psi$. Also, as φ is surjective, there is an $a \in$ such that $(a, b) \in \varphi$. But from $(a, b) \in \varphi$, $(b, c) \in \psi$ we get $(a, c) \in \psi\varphi$. Thus for any $c \in C$, there is an $a \in A$ such that $(a, c) \in \psi\varphi$. Hence $\psi\varphi$ is surjective.

2.4.3. Corollary: The product of two bijective mappings is bijective.

2.4.4. Theorem: (Associative law of product of mappings).

For any three mappings

$$f : A \to B, g : B \to C, h : C \to D,$$

$$h(gf) = (hg)f$$

Proof: It is clear that both $h(g\,f)$ and $(hg)f$ are subset of $A \times D$. For the equation

$$h(g\,f) = (h\ g)\,f \qquad (1)$$

to hold, we must show that the two are equal as subset of A × D. Let $(a, d) \in h(gf)$. Then there is a $c \in C$ such that $(a, c) \in gf$, $(c, d) \in h$. Also then there is a $b \in B$ such that $(a, b) \in f$, $(b, c) \in g$. So $(a, d) \in h(gf)$ implies there elements $b \in B$ and $c \in C$ such that $(a, b) \in f$, $(b, c) \in g$ and $(c, d) \in h$. This implies that $(a, b) \in f$ and $(b, d) \in (h\ g)$ so that $(a, d) \in (h\ g)f$.

Hence

$$h(gf) \subseteq (h\ g)f.$$

Likewise

$$(h\ g)f \subseteq h(gf)$$

Thus (1) holds.

Alternatively: For each $a \in A$,

$$(h(gf))(a) = h(gf(a)), \text{ by definition of composition of mappings}$$
$$= h(g(f(a)))$$
$$= (hg)(f(a))$$
$$= ((hg)f)(a)$$

Hence $h(gf) = (hg)f$.

Remarks:

(a) For the particular case when B = C = D = A we have f, g, h as mappings from A to A satisfying the *associative law*.

(b) Take $h = g = f$. Then $(ff)f$ and $f(ff)$ represent the same functions and are usually written as fff. For the sake of brevity we shall write f^3 for fff and in general f^n for $ff \ldots f$ (n-times).

It is convenient and useful to take f^0 as the identity mapping on A.

On particular interest among the mappings between sets are the bijective mappings of a set A. Let us denote by S_A the set of all such mappings of A. Then we have the following important result about S_A.

2.4.5. Theorem:

The set S_A of all bijective mappings on A has the following characteristics:

(i) For any two mappings f and g in S_A, their product $gf \in S_A$.

(ii) Associative law holds in S_A, that is, for any three mappings f, g, h in S_A,

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

(iii) The identity mappings i_A of A is in SA and satisfies the equation

$$f.\ i_A = f,\ i_A.f = f$$

for all $f \in S_A$.

(iv) For each $f \in S_A$, there is an $f^{-1} \in S_A$ such that

$$f.f^{-1} = f^{-1}.f = i_A.$$

Proof: The conditions (i) and (ii) follow from Corollary 2.3.5.3 to Theorem 2.3.5.2 and theorem 2.3.5.4 respectively.

For (iii) we have already seen that the identity mapping i_A defined by the diagonal of $A \times A$ is bijective and so is in S_A. Also any $f \in S_A$ consists of elements of the form $(a, a') \in A \times A$, $a, a' \in A$. As $(a, a') \in f$, $(a', a') \in i_A$, so $(a, a') \in i_A.f$, so $f \subseteq i_A.f$. Also, for $(a, a') \in i_A.f$, there is an $a' \in A$ such that $(a, a') \in f$ and $(a', a') \in i_A$ so that $(a, a') \in f$. Hence $i_A.f \subseteq f$. Therefore $f = i_A.f$. Likewise $f.\ i_A = f$.

For (iv) let $f \in S_A$. Then the inverse f^{-1} of f is bijective.

Hence $f^{-1} \in S_A$. The equation

$$f^{-1}.f = f.f^{-1} = i_A$$

then follows by the definition of f^{-1}

2.4.5 (1) ***Illustration:***

Let $A = \{a_1, a_2, a_3\}$. The mappings $\varphi : A \to$ and $\psi : A \to A$ given by:

$$\varphi(a_1) = a_2,\ \varphi(a_2) = a_3,\ \varphi(a_3) = a1 \qquad (1)$$

and

$$\psi(a_1) = a_2,\ \psi(a_2) = a_1,\ \psi(a_3) = a_3, \qquad (2)$$

are obviously bijective and hence are in S_A. Also

$$\varphi^3(a_1) = \varphi^2(\varphi(a_1)) = \varphi^2(a_2) = \varphi(\varphi(a_2)) = \varphi(a_3) = a_1$$

Similarly

$$\varphi^3(a_2) = a_2,\ \varphi^3(a_3) = a_3.\ \text{Thus}\ \varphi^3 = i_A.$$

Likewise

$$\psi^2 = (\phi\,\psi)^2 = i_A,$$

Here the mapping $\phi\,\psi$ is the product of the mapping ψ and φ *i.e.*, $\varphi\,\psi$ is defined by:

$$(\varphi\ \psi)(a_1) = \varphi(a_2) = a_3,\ (\varphi\ \psi)(a_2) = \varphi(\psi(a_2)) = \varphi(a_1) = a_2 \text{ and}$$
$$(\varphi\ \psi)(a_3) = a_1 \qquad (3)$$

The mapping $\psi\,\varphi$ is given by

$$(\psi\,\varphi)(a_1) = a_1,\ (\psi\,\varphi)(a_2) = a_3,\ (\psi\,\varphi)(a_3) = a_2 \qquad (4)$$

From (3) and (4) we observe that:

$$\varphi\,\psi \neq \psi\,\varphi$$

One can show that the elements of S_A are precisely

$$i_A,\ \varphi,\ \varphi^2,\ \psi,\ \varphi\,\psi,\ \varphi^2\,\psi.$$

EXERCISES

1. Eight articles are purchased. The first two articles cost Rs. 100 each and the prices, because of quantity discount, decrease 5 rupees with each additional article purchased. Show the relation of articles to prices.
2. Give an example in a set of:
   (i) a relation which is reflexive and symmetric but not transitive,
   (ii) a relation which is symmetric and transitive but not reflexive,
   (iii) a relation which is transitive and reflexive but not symmetric,
   (iv) a relation which is reflexive and transitive but not anti-symmetric,

3. Prove or disprove: Every transitive relation on a set X with more than 2 points is reflexive.

4. Let R_1 be the relation 'is a brother of' and R_2 the relation 'is a sister of' on the set U of students of a university. Find $R_1 \cup R_2$ and $R_1 \cap R_2$.

5. Let R and S be equivalence relations in a set. Show that $R \cap S$ is an equivalence relation.

6. Which of the following are equivalence relations.
   (a) the relation of parallelism in the set of lines in a Euclidean plane.
   (b) the relation of having the same number of elements in a collection of finite sets.
   (c) the relation of 'living in the same hostel' in the set B of all the resident students of a university.

7. Let R be a reflexive relation in a set X. Verify that R is an equivalence relation if and only if $R.R^{-1} = R$.

8. Which of the following are mappings and why?
   (a) The subset $\{(x^2, x) ; x \in R\}$ of $R \times R$
   (b) The subsets $[\{(1, a), (2, c)\}, \{(1, a), (2, a)\}], [\{(1, a),(1, b), (2, c)\}]$
   of $A \times B$ where $A = \{1, 2\}$ $B = \{a, b, c\}$.

9. Let $f: A \to B$ be a function. For each $b \in R_f$, let:
   $A_b = \{a \in A : f(a) = b\} = f^{-1}(b)$.
   Show that $\{A_b : b \in R_f\}$ is a partition of A. Hence deduce that every function on a set A defines an equivalence relation on A.

10. Let A be a set consisting of m elements and B a set consisting of n elements. Show, by induction on m, that there are n^m mappings from A to B. How many of these are surjective, injective and bijective?

11. Dealing 13 cards from a 52-card deck to each of the four bridge players is a surjective mapping of a set of 52 elements to a set of 4 elements. How many such mappings are there?

12. Which of the following mappings from $\boldsymbol{R}$ to $\boldsymbol{R}$ are surjective?

(i) $f(x) = x^2 + 2$, (ii) $f(x) = x \sin x$

(ii) $f(x) = x - \dfrac{1}{x^2 + 1}$

13. A mapping $\varphi : \boldsymbol{R} \to \boldsymbol{R}$ is linear if $\varphi(x) = ax + b$, $x \in \boldsymbol{R}$ and a, b fixed elements of $\mathbf{R}$. Find all linear mappings which are : (i) surjective, (ii) injective, and (iii) bijective.

14. Let f be a mapping from X to Y and A, B subset of X. Show that

$$f(A \cup B) = f(A) \cup f(B)$$

and $f(A \cap B) \subseteq f(A) \cap f(B)$.

Also if f is injective then

$$f(A \cap B) = f(A) \cap f(B)$$

15. Let f be as in exercise 14 and be a bijection. Then show that

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$$

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

16. Let X be a set. For an arbitrary subset A of X, define a mapping: $\chi_A : X \to R$ by:

$$\chi_A(x) = 1 \text{ if } x \in A$$

$$= 0 \text{ if } x \in X \setminus A$$

The function χ_A so defined is called the *characteristic function* of the subset A in X. Verify that

$$\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$$

$$\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$$

17. Let $I = \{x \in \boldsymbol{R} : a < x < b, a, b \in \boldsymbol{R} \text{ and fixed}\}$. Define a mapping $f : I \to \boldsymbol{R}$ by:

$$f(x) = \frac{x - c}{x - a} \qquad a < x \leq c$$

$$= \frac{x-c}{b-x} \qquad c \leq x < b$$

where c denotes the arithmatic mean of a and b. Show that f is a one-one correspondence between I and $\boldsymbol{R}$.

18. For a function $f: A \to A$, let f^n denote $f.f. \ldots f$ (n-times).

Suppose that $f^n = i_A$. Show that f is bijective.

19. Justify the following restatement of theorem 2.2.6.

Let A be a set.

There is a one-one correspondence between the equivalence relations on A and the partitions of A.

20. Let f be a bijective mapping of a set A and $f' = \{(y, x) : (x, y) \in f, x, y \text{ in } A\}$. Show that $f \,.\, f'$ and $f' \,.\, f$ define equivalence relations on A.

[Hint: Here $f.f' = f'f = i_A$ is the identity relation on A.]

21. Determine all the bijective mappings of a set consisting of (i) three elements, (ii) four elements, and (iii) a set consisting of n elements.

Chapter - **III**

ALGEBRAIC OPERATIONS

In elementary Mathematics one constantly deals with the familiar notions of sum, difference; product and quotient of ordinary real numbers. These concepts have much wider meaning in the superstructure of Algebra and are particular forms of an idea connected with a special type of relation in a set. These relations are called algebraic operations.

3.1. ALGEBRAIC OPERATIONS

By an *algebraic operation* or, to be more exact, *an n-ary algebraic operation* in a set A we mean a mapping $\alpha : A^n \to A$.

Thus an n-ary algebraic operation in A is a function α which associates with each element $(a_1, .., a_n)$ of A^n a uniquely determined element, say a, of A. The element of A associated with an ordered n-tuple $(a_1, .., a_n)$ under α is given by :

$$\alpha (a_1, .., a_n) = a$$

or by:

$$a_1 \alpha a_2 \alpha ... \alpha a_n = a.$$

The algebraic operations corresponding to n = 1, 2, 3, 4, etc. are respectively called *unary, binary, ternary, quaternary* etc. In our context, however, we shall be concerned with unary and binary algebraic operations only and refer to them as unary and binary operations respectively.

Thus a *binary operation* on set A is a function $\alpha : A^2 \to A$. This function associates with each ordered pair $(a_1, a_2) \in A^2$, a unique element of A and is denoted by :

$$a_1 \alpha a_2$$

It should be kept in mind that the element of A associated with the pair (a_2, a_1) under α may be different from the one associated with the pair (a_1, a_2). Thus the element $a_1 \alpha a_2$ is, in general, not equal to $a_2 \alpha a_1$.

In practice, for the sake of convenience, we use the familiar symbols of addition and multiplication namely the symbols +, . , × etc., for α

If we denote α by the symbol '+' we shall call it *addition*, and if the symbols '.' or '×' are used, the corresponding algebraic operation will be called multiplication. In the latter case, even the symbols . and × are usually omitted. Thus the element corresponding to the pair (a_1, a_2) will be denoted by $a_1 + a_2$ and by $a_1 . a_2$ or simply $a_1 a_2$ according as the algebraic operation is termed as addition or multiplication respectively. The elements $a_1 + a_2$ and $a_1 . a_2$ are called the '*sum*' and '*product*' of a_1, a_2 respectively.

3.1.1. Examples:

1. Let Z be the set of integers and let $\alpha : Z \times Z \to Z$ be given by:

$$\alpha (m, n) = m + n \; ; m, n \in Z.$$

Then α is an algebraic operation in Z. It is, in fact, the ordinary addition in Z. Here we have associated, with each pair m, n, a uniquely determined element namely their usual sum $m + n$. Similarly ordinary multiplication is an algebraic operation in Z. It is defined by the function

$\mu : Z \times Z \to Z$ given by

$\mu (m, n) = m . n.$

Likewise, ordinary addition and ordinary multiplication in the sets Q and R of rationals and real numbers respectively, are algebraic operations.

2. Let $V_3 (R)$ be the real 3-diensional space. Elements of $V_3 (R)$ are ordered triples (x_1, x_2, x_3), $x_i \in R$, i = 1, 2, 3.

The function which associates with each pair $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ of $V_3 (R)$ the element $x + y$ given by the equation.

$$x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

defines an algebraic operation in V_3 ($\boldsymbol{R}$). This operation is called the *usual addition of vectors in* V_3 ($\boldsymbol{R}$).

3. Let A = $\{a, b, c\}$. A binary algebraic operation in A is a certain subset of (A × A) × A. The following subsets define algebraic operations in A.

$\alpha_1 = \{((a, a), a), ((a, b), b), ((a, c), c), ((b, a), b), ((b, c), a),$

$((c, a), c), ((c, b), a), ((c, c), b)\}$.

$\alpha_2 = \{((a, a), a), ((a, b), a), ((a, c), a), ((b, a), a), ((b, b), b),$

$((b, c), c), ((c, a), a), ((c, b), c), ((c, c), b)\}$.

A simple way of describing the above algebraic operation on A will be given in 3.2.5.

REMARKS:

(i) If an algebraic operation α is defined in a set A then we say that *A is closed under the algebraic operation* α or simply *closed under* α. For instance the sets $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ are closed under ordinary addition and multiplication.

(ii) Let α be an algebraic operation in A. For a subset A′ of A the mapping $\alpha|_{A'}$ may not be an algebraic operation in A′. If $\alpha|_{A'}$ is an algebraic operation in A′ then it is called the *induced algebraic operation of A in A′*. For example, ordinary addition is the induced algebraic operation in the set $\boldsymbol{N}$ of natural numbers considered as a subset of the set $\boldsymbol{Z}$ of integers. However *ordinary subtraction* is not an algebraic operation in $\boldsymbol{N}$.

3.1.2. Commutative algebraic operations:

Under an algebraic operation α in A, the element associated with $(a_1, a_2) \in A \times A$ under α may be different from the one associated with (a_2, a_1). If α is such that one and the same element is associated with the pairs (a_1, a_2) and (a_2, a_1) under α for all $a_1, a_2 \in A$ then α is called a *commutative algebraic operation. Thus* α is commutative if and only if

$$a_1 \alpha a_2 = a_2 \alpha a_1$$

for all $a_1, a_2 \in A$.

3.1.3. Examples:

1. The ordinary addition and multiplication in the sets $\boldsymbol{Z}$ of integers, $\boldsymbol{Q}$ of rational numbers, $\boldsymbol{R}$ of real numbers and $\boldsymbol{C}$ of complex numbers are commutative operations.

   Recall that addition and multiplication in $\boldsymbol{C}$ are defined by:

   $$z + z' = (x, y) + (x', y') = (x + x', y + y')$$

   $$z \times z' = (x, y) \,.\, (x', y') = (xx' - yy', xy' + yx')$$

   for all $z, z' \in \boldsymbol{C}$.

   However ordinary subtraction is an algebraic operation in $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ but is not commutative.

   Similarly ordinary division in these in the sets $\boldsymbol{Q}$, $\boldsymbol{R}$, and $\boldsymbol{C}$ excluding the number '0' from each of them, is an algebraic operation which is not commutative.

2. Multiplication of mappings in the set S_A of all bijective mappings of the set $A = \{a, b, c\}$ is not commutative. Here the mappings $\varphi, \psi \in S_A$ given by:

   $$\varphi(a) = b, \varphi(b) = c, \varphi(c) = a$$

   and

   $$\psi(a) = a, \psi(b) = c, \psi(c) = b$$

   do not satisfy the equation

   $$\varphi \psi = \psi \varphi.$$

3. The *vector product* in the three dimensional Euclidean space $\mathbf{V}_3(\boldsymbol{R})$ is a binary operation in it and is not commutative because

   $$\boldsymbol{a} \times \boldsymbol{b} \neq \boldsymbol{b} \times \boldsymbol{a} \text{ for } \boldsymbol{a}, \boldsymbol{b} \in \mathbf{V}_3(\boldsymbol{R}).$$

   However the usual *component-wise addition* or multiplication of vectors in $\mathbf{V}_3(\mathbf{R})$ are commutative operations.

4. The solution set $S = \{\pm 1, \pm i\}$ of the equation $x^4 = 1$ has the usual multiplication of complex numbers as a commutative algebraic operation.

3.1.4. Associative algebraic operations:

Let α be an algebraic operation on a set A. For $a_1, a_2, a_3 \in$ A, the element in A taken for $(a_1 \alpha a_2) \alpha a_3$ may not be the same as that taken for $a_1 \alpha (a_2 \alpha a_3)$. If α is such that

$$(a_1 \alpha a_2) \alpha a_3 = a_1 \alpha (a_2 \alpha a_3)$$

for all $a_1, a_2, a_3 \in$ A, then α is called an *associative algebraic operation.* Replacing α by the symbols for addition and multiplication, the corresponding equations will be

$$(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$$

and

$$(a_1 . a_2) . a_3 = a_1 . (a_2 . a_3)$$

respectively.

Using induction on n one can easily verify the generalised associative law:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{m} a_i \cdot \prod_{j=m+1}^{n} a_j.$$

With the help of the above result the product

$(...((a_1 a_2) a_3) a_4 ...) a_n)$ of $a_1, a_2, ..., a_n$ is usually written as

$$a_1 a_2 ... a_n$$

without using the parenthesis.

The following rules of exponenciation are easily verifiable

I. $a^m . a^n = a^{m+n}$, $m, n \in Z$.

II. $(a^m)^n = a^{mn}$, $m, n \in Z$.

3.1.5. Examples:

(i) The usual addition and multiplication in Z, Q, R and C are associative operations but the usual subtraction in these sets is not.

(ii) Let P = $\{(a, b) ; a, b \in R\}$. Define an algebraic operation in P by:

$$u . v = (a, b) (c, d) = (ac, bc + d), \text{ for } u, v \in P$$

Then '.' is an associative operation in P.

(iii) Let R^+ be the set of non-zero positive real numbers. The algebraic operation '.' in R^+, defined by:

$$x \cdot y = y^x$$

for $x, y \in R^+$ is *not* associative.

(iv) Let Ω be an arbitrary collection of sets. For any $A, B \in \Omega$ the equation

$$A \oplus B = (A \setminus B) \cup (B \setminus A)$$

defines an algebraic operation $\oplus$ in Ω which is associative.

3.2. ALGEBRAIC SYSTEMS

A non-empty set A with an algebraic operation is called an **algebraic system**. Let α be an algebraic operation on a set A. If, for each pair a, b in A, the equations

$$x \alpha a = b, a \alpha y = b$$

have unique solutions in A then we say that an *inverse algebraic operation* is defined in A.

The solutions of the above equations are written as:

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

respectively.

Some examples of algebraic systems with an inverse algebraic operation are given below:

A *groupoid* is a non-empty set G with a binary operation '*'.

A semi-group is a non-empty set G with an associative binary operation '*'.

Both these are algebraic systems.

3.2.1. Examples:

1. Ordinary division is the inverse of the algebraic operation of multiplication in the following sets.

   (i) The set Q' of all non-zero rational numbers and the set R' of all non-zero real numbers.

   (ii) The set R^+ of all non-zero positive real numbers.

(iii) The set $\mathbf{C} = \{2^n ; n \in Z\}$.

2. Let M_n be the set of all n × n matrices with entries from $\boldsymbol{R}$. The usual addition of matrices given by:

$$A + B = (a_{ij} + b_{ij}),\ A = (a_{ij}),\ B = (b_{ij})$$

is an algebraic operation in M_n. The inverse of this operation is the usual subtraction of matrices. Thus the equations

$$X + A = B \quad \text{and} \quad A + Y = B$$

have the unique solutions

$$X = B - A = (b_{ij} - a_{ij}),\ Y = -A + B = (-a_{ij} + b_{ij}).$$

3. The set $\boldsymbol{N}$ of natural numbers does not admit the inverse operation of the algebraic operation of addition in $\boldsymbol{N}$.

3.2.2. Unit element and inverse of an element in a set:

Let A be a set with an algebraic operation α. If there are elements e_1, e_2 in A such that

$$e_1 \alpha a = a,\ a \alpha e_2 = a$$

for all $a \in A$, then e_1, e_2 are called *a left* and *a right unit* (*identity or neutral)* elements in A respectively.

An element $e \in A$ which is both a left and a right unit is simply called a *unit element* or *an identity in A.*

A semi-group with an identity element is called a *Monoid.*

A set with a certain algebraic operation may or may not have a unit element, For example, the set $\boldsymbol{N}$ of natural numbers under addition does not have a unite element. It certainly has a unit element namely '1' under multiplication.

An element $a' \in A$ is called a *left inverse* of an element $a \in A$ if $a' \alpha a = e$.

A *right inverse* is similarly defined.

The following theorem establishes the uniqueness of the identity and the inverse of each element in a set.

3.2.3. Theorem:

(i) In a set A with an algebraic operation α, a left identity is the same as a right identity.

(ii) In a set A with an associative algebraic operation α and an identity element e, a left inverse of an element is equal to its right inverse.

Proof:

(i) Let e' be a left identity and e'' a right identity of A. Then

$$e' \alpha e'' = e', \quad \because e'' \text{ is a right identity}$$

$$= e'', \quad \because e' \text{ is a left identity}$$

Hence $e' = e'' = e$ (say). This e is the unique identity element of A.

(ii) For any $a \in A$, let $a', a'' \in A$ be the left and right inverses of a respectively. Then, using the associative property of α, we have,

$$a' \alpha a \alpha a'' = a' \alpha (a \alpha a'')$$

$$= a' \alpha e \quad (\because a'' \text{ is the right inverse of } a)$$

$$= a'$$

and

$$a' \alpha a \alpha a'' = (a' \alpha a) \alpha a''$$

$$= e \alpha a'' \quad (\because a' \text{ is the left inverse of } a)$$

$$= a''$$

Hence $a' = a''$.

Making use of the above theorem we write $a' = a'' = a^{-1}$. Then a^{-1} is both the left and right inverse of a and is called the *inverse of a*. It has the property that

$$a \alpha a^{-1} = a^{-1} \alpha a = e$$

The inverse of the inverse of a is a itself as can be easily verified. Also we define a^0 and a^{-n} by:

$$a^0 = e$$

and

$$a^{-n} = a^{-1} . a^{-1} \ldots a^{-1} \text{ (n-times)}.$$

The inverse of the product $a_1 . a_2 \ldots a_n$ of $a_1, a_2, \ldots, a_n \in A$ is $a_n^{-1} . a_{n-1}^{-1} \ldots a_2^{-1} . a_1^{-1}$. This follows by actually multiplying the two expressions. In particular,

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

A groupoid, in which the equations $ax = b$ and $ya = b$ have unique solutions, is called a *quasi-group*.

A quasi-group with an identity is called a *loop*.

3.2.4. Cayley's algebraic operation tables:

It is often convenient to represent the elements associated with the pairs (a, b) of a finite set A under an algebraic operation α by a table. Let

$$A = \{a_1, a_2, \ldots, a_n\}$$

We prepare a table consisting of n^2 squares and write down the elements of A above the horizontal and across the vertical lines emanating from the upper left corner. The element associated with the pair a_i, a_j under α is then written in the square which occurs at the intersection of the ith row and jth column of squares. This table is called Cayley's *algebraic operation table*. When completed, such a table makes it easier to verify certain statements about the elements of A and the algebraic operation α. For example such a table makes it 'simpler' to verify the associative or commutative property of the operation, to find the identity element and the inverse of a certain element.

3.2.5. Examples:

The algebraic operations defined on a set A consisting of the elements a, b, c, in example 3.1.2 (3), can be given by the following tables. The algebraic operations on A are written at left upper corners of the table.

I.

α_1	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

II.

α_2	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

are the Cayley's table for A corresponding to the algebraic operations α_1 and α_2 or simply the α_1, α_2 - tables for A.

Similarly the addition table for $V = \{0, a, b, a + b\}$ having the equations $2a = 2b = 2(a + b) = 0$; and the multiplication table for $C = \{\pm 1, \pm i\}$ are;

III.

+	0	a	b	$a+b$
0	0	a	b	$a+b$
a	a	0	$a+b$	b
b	b	$a+b$	0	a
$a+b$	$a+b$	b	a	0

IV.

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

Observe that in table III we have taken a + b equal to b + a. (Why)?

3.3. RELATIONS BETWEEN ALGEBRAIC SYSTEMS

In what follows, by a set we shall always mean a non-empty set with some algebraic operation defined in it. The algebraic operation will be denoted by any symbols '+' '.' '×' etc.

The following paragraphs describe some particular types of relations between sets.

Let A, A′ be sets with '.' and '×' as algebraic operations respectively:

(1) Then:

A mapping $\varphi : A \to A'$ is called a *homomorphism* if

$$\varphi(a \,.\, b) = \varphi(a) \times \varphi(b)$$

An injective homomorphism φ: $A \to A'$ is called a *monomorphism* or an *embedding* of A in A′.

(2) A sujective homomorphism from A to A′ is called an epimorphism or a monic.

A bijictive homomorphism from A to A′ is called an *isomorphism.* Thus:

A bijective mapping $\varphi : A \to A'$ is called an *isomorphism* if the equation

$$\varphi(a.\, b) = \varphi(a) \times \varphi(b)$$

holds for all $a, b \in A$.

The sets A and A′ are then called isomorphic and we write $A \cong A'$ (read as 'A is isomorphic to A'').

The relation of isomorphism is fundamental in the whole of Mathematics. Its importance in algebra is too great to be emphasised. It is easy to verify that the relation of 'being isomorphic to' between sets is an equivalence relation and therefore partitions the whole collection of sets into mutually exclusive equivalence classes of isomorphic sets. In order to discuss various 'structural properties' inherent in each member of an equivalence class it is enough to examine only a member of this class with regard to these properties thereby making the study of these sets easier.

To prove that two infinite sets are isomorphic we define a mapping between these, verify the bijective property for that mapping and then examine equation (I). For finite sets, however, it is convenient to use Cayley's table to verify equation (I) after defining a bijective mapping between these sets.

3.3.1. Examples:

1. The sets $\boldsymbol{R}$ of real numbers under addition and $\boldsymbol{R}^+$ of non-zero positive real numbers under multiplication are isomorphic.

The mapping $\in : \boldsymbol{R} \to \boldsymbol{R}^+$ given by:

$$\in (x) = e^x.$$

for all x in $\mathbf{R}$ is an isomorphism because:

(a) $\in$ is injective. Here

$$\in (x_1) = \in (x_2) \to e^{x1} = e^{x2} \to x_1 = x_2 \text{ for all}$$

x_1, x_2 in $\boldsymbol{R}$.

$\in$ is surjective because every y in $\boldsymbol{R}^+$ is the image of an $x = \log y$ in $\boldsymbol{R}$ under $\in$.

Hence $\in$ is bijective.

(b) for all x_1, x_2 in R,

$$\in (x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = \in (x_1) \cdot \in (x_2).$$

2. The mapping φ from the set $\boldsymbol{Z}$ of integers under addition to the set $\boldsymbol{E}$ of even integers under addition, given by:

$$\varphi (n) = 2n, n \in Z$$

is an isomorphism.

3. Let A be a set with multiplication as an algebraic operation and let

$$P = \{(a, a'); a, a' \in A\}.$$

Define an algebraic operation '$\times$' in P as follows:

For (a, a'), (a_1, a_1') in P, we put

$$(a, a') \times (a_1, a_1') = (a \cdot a_1, a' \cdot a_1')$$

Then the *diagonal* $D = \{(a, a) : a \in A\}$ is isomorphic to A.

4. The sets $A = \{a, b, c, d\}$ and $C = \{1, -1, i, -i\}$, with the following Cayley's tables, are isomorphic:

(A)

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(C)

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

The mapping $\varphi : A \to C$ given by :

$$\varphi (a) = 1, \varphi (b) = i, \varphi (c) = -1, \varphi (d) = -i$$

is an isomorphism. To check equation (I) we have to verify it for every pair of elements in A. For instance

$$\varphi(b + c) = \varphi(d) = -i$$

and

$$\varphi(b) \times \varphi(c) = i \times -1 = -i$$

and similarly for other pairs.

EXERCISES

1. Let A = $\{a, b, c\}$ and P (A), the power set of A. List all the elements of P (A). Show that the usual intersection, $\cap$, and union, $\cup$, of sets in P (A) are algebraic operations. What are the Cayley's tables for these operations? Find the identity elements, if any, with respect to these operations.

2. How many algebraic operations are there for a set consisting of three elements? List two algebraic operation which are (i) non-commutative but associative, (ii) non-associative, (iii) neither commutative nor associative.

3. Let A be a set, P (A) its power set. Define an algebraic operation $\oplus$ in P (A) as follows:

   For X, Y $\in$ P (A), we put

   $$X \oplus Y = (X \setminus Y) \cup (Y \setminus X)$$

   Show that

   (i) $\oplus$ is an associative binary operation, *i.e.*,

   $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$ for all X, Y, Z $\in$ P (A).

   (ii) $\oplus$ is commutative *i.e.*, $X \oplus Y = Y \oplus X$ for all X, Y $\in$ P (A)

   (iii) the empty set ϕ is the identity element with respect to '$\oplus$'.

   (iv) the inverse of X $\in$ P (A) is X itself.

4. In the set $\boldsymbol{R}$ of real numbers, define an algebraic operation α by:

   $$\alpha(x, y) = x - y.$$

   Show, by examples, that

(a) α is not associative,

(b) α is not commutative.

5. Define an algebraic operation μ in the set $\boldsymbol{R'}$ of all non-zero real numbers by:

$$\mu(x, y) = x \cdot \frac{1}{y} = \frac{x}{y} = xy^{-1}$$

Show, by examples, that

(i) μ is not associative,

(ii) μ is not commutative.

6. Let $\boldsymbol{R}^+$ denote the set of non-zero positive real numbers. Define an algebraic operation '.' on $\boldsymbol{R}^+$ by:

$$x.y = y^x ; x, y \in \boldsymbol{R}^+.$$

Show that

(i) '.' is not commutative,

(ii) '.' is not associative,

(iii) $1 \in \mathbf{R}^+$ is a left identity but not a right identity.

7. Define an algebraic operation '*' on the set $\boldsymbol{N}$ of natural numbers by:

$$m * n = m + n + mn, m, n \in \boldsymbol{N}$$

Show that '*' is an associative binary operation.

Find the identity element, if any, with respect to *.

8. On the set $\boldsymbol{Q}$ of rational numbers define a binary operation '*' by:

$$a * b = a + b + ab$$

Show that

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

(ii) 0 is the identity element in $\boldsymbol{Q}$ under '*'.

(iii) each $a \in \boldsymbol{Q}, a \neq -1$, has an inverse

$$a^{-1} = \frac{a}{1 + a}$$

9. Let $\mathbf{X} = \{(a, b);\ a, b \in \boldsymbol{R},\ a \neq 0\}$. Define an algebraic operation '$\otimes$' in $\mathbf{X}$ by:

$$(a, b) \otimes (c, d) = (ac, bc - d)$$

Examine whether $\otimes$ is associative.

Show that (1, 0) is a right identity but not a left identity.

Is there also a left identity?

10. In a non-empty set A, define an algebraic operation by:

$$\alpha\,(a, b) = a, \quad a, b \in \mathrm{A}.$$

Prove that α is associative and every element of A is a right identity under α. Is there a left identity?

Chapter - IV

GROUPS

By a mathematical system or an algebraic system we shall mean a non-empty set with one or more binary operations. In this chapter, we shall examine one of the basic and fundamental mathematical systems namely groups. This concept forms an intrinsic as well as an essential part of algebra. Group theory originated mainly from the study of theory of a particular geometry invariant. Groups have found applications in various branches of pure and applied sciences. For example in theoretical physics one comes across the groups of linear operators, different types of orthogonal groups, the symmetry groups and various rotation groups. Similarly in chemistry one has to deal with crystallographic groups. We now describe this concept in detail.

4.1. DEFINITION AND CONSEQUENCES

4.1.1. Definition I:

A pair (G, .) where G is a non-empty set and '.' an algebraic operation in G is a group if and only if:

(i) the algebraic operation '.' is associative, *i.e.*,

$(a \,.\, b) \,.\, c = a.\, (b.\, c)$

for all $a, b, c \in G$.

(ii) with respect to '.' there is an identity element in G, that is, an element $e \in G$ satisfying the equations

$a.\, e = e.\, a = a$

for all $a \in G$.

(iii) for each $a \in G$ there is an $a' \in G$ such that

$a.\, a' = a' \,.\, a = e$.

a' is called the *inverse* of a in G and is denoted by a^{-1}.

The conditions given in definition I for a group can be weakened to the following:

Definition II:

A group is an ordered pair (G, .) where G is a non-empty set and '.' an algebraic operation in G satisfying the following properties, called the *group axioms*.

(i′) '.' is an associative operation.

(ii′) There is a left identity in G. That is, an element e in G exists such that

$$e \,.\, a = a$$

for all $a \in G$.

(iii′) Each $a \in G$ has a left inverse a' in G *i.e.*, for each $a \in G$ there is $a' \in G$ such that

$$a' \,.\, a = e$$

Let us show that the two definitions are equivalent.

Obviously definition II is a part of definition *I*.

Conversely, to prove the equivalence of (i′) (ii′) and (iii′) with (i), (ii) and (iii) respectively we have to show, using (i′), that e is also a right identity in G and that a' is a right inverse of a.

Since $a \in G$ has a left inverse a' in G, there is a left inverse a'' of a' in G satisfying $a''\, a' = e$. But then

$$\begin{aligned} aa' &= e\,(aa') \\ &= (a''\, a')\,(aa') \\ &= a''\,(a'\, a)\, a', \text{ by (i′)} \\ &= a''\,(ea'), \text{ by (iii′)} \\ &= a''\, a', \text{ by (ii′)} \\ &= e \end{aligned}$$

Hence a' is a right inverse as well and (iii) is satisfied.

Also

$$ae = a\,(a'\, a) \text{ by (iii′)}$$

$= (aa')\, a$, by (i')

$= ea$, as shown above,

$= a$ by (ii').

Hence e is also a right identity and (ii) is satisfied. Therefore the two definitions are equivalent.

If, in addition to the above requirements, the algebraic operation '.' is commutative then (G, .) is called a *commutative* or *abelian group*. Thus an abelian group is a group (G, .) in which the equation

$$a \,.\, b = b \,.\, a$$

is satisfied for all $a, b \in G$.

Henceforth, a group shall be denoted simply by a set G, it being always understood that there is an algebraic operation in G. G will be called a *group under addition* or *a group under multiplication* according as the algebraic operation in G is termed as 'addition' or 'multiplication' respectively. If no mention of the algebraic operation is made then G will be understood to be a group under multiplication. The product of any two elements a, b in G will then be denoted by $a \,.\, b$ or simply by ab.

An element x of a set G with a binary operation is said to be *idempotent* if $x^2 = x$:

The only idempotent element in a group is its identity.

For if x is an idempotent element in a group G, then

$$x^2 = x$$

implies

$$x^{-1} x^2 = x^{-1} x,$$

that is,

$$x = e$$

The *number of elements* in a group is called the *order* of that group.

A group is finite if and only if its order is finite; otherwise it is called an *infinite group*. (See the examples given below.)

Let a be an element of a group G. A non-zero positive integer n is called the *order of* a if $a^n = e$ and n is the least such integer.

An element a is of *finite* or *infinite* order according as an integer n with the above property exists or does not exist.

The order of the identity element e in a group G is taken as 1.

If the order of a is n, that is $a^n = e$, then the elements

$$e = a^0, a^1, ..., a^{n-1}.$$

are all distinct.

Also then $a^k = e$ if and only if k is divisible by n.

For if $a^k = e$ then, since k can be written as

$$k = nq + r, \qquad 0 \leq r < n,$$

we have

$$\begin{aligned} e = a^k &= a^{nq+r} \\ &= (a^n)^q . a^r \\ &= e . a^r \\ &= a^r \end{aligned}$$

But, since a has order n and $r < n$, we must have $r = 0$ otherwise a will have order a number smaller than n. Hence $k = nq$.

Conversely, if k = nq then $a^k = a^{nq} = (a^n)^q = e^q = e$.

A group all of whose elements are of finite order is called a *periodic* group. A finite group is obviously periodic. There are infinite periodic groups as well (*e.g.*, see example 4.1.2 (4) below).

A group in which every element except the identity e has infinite order is known as a *torsion free* (*a-periodic* or *locally infinite*).

A group having elements both of finite as well as of infinite order is called a *mixed* group.

4.1.2. Theorem: A non-empty set G with an associative binary operation is a group if and only if the left and right cancellation laws hold in G, that is,

$$ab = ac, ba = ca \Rightarrow b = c$$

for all $a, b, c, \in$ G.

Proof: Suppose that G is a group, finite or infinite. Then each element a of G has an inverse $= a^{-1}$ in G. So

$$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$$
$$\Rightarrow (a^{-1}a)\,b = (a^{-1}a)\,c, \text{ by associative law}$$
$$\Rightarrow eb = ec$$
$$\Rightarrow b = c$$

similarly

$$ba = ca \Rightarrow b = c$$

Conversely, suppose that G is a finite non-empty set with an associative binary operation and, in G, the left and right cancellations laws are satisfied. We have only to show that G has the identify element and an inverse for each of its elements. So suppose that

$$ab = ac \Rightarrow b = c$$

Consider the mapping $\alpha : G \to G$ given by:

$$\alpha(b) = ab \text{ for all } b \in G,\ a \in G \text{ is arbitrary but fixed } 4.1.2(1).$$

Then α is injective because; for $b, c \in G$,

$$\alpha(b) = \alpha(c) \Rightarrow ab = ac \Rightarrow b = c \qquad \text{by } 4.1.2\ (1)$$

We show that α is surjective as well. For this let $a \in G$. We show that there is an element $b \in G$ such that

$$\alpha(b) = a. \qquad 4.1.2\ (2)$$

Let us write α^2 for $\alpha \cdot \alpha$ and so on α^k for $\alpha \cdot \alpha \ldots \alpha$ (k-times). Then, applying α successively on a, the elements

$$\alpha(a), \alpha^2(a) = \alpha(\alpha(a)), \ldots, \alpha^k(a), \ldots$$

cannot all be distinct because G is finite. Hence, for some natural numbers m and n, $m > n$,

$$\alpha^m(a) = \alpha^n(a). \qquad 4.1.2\ (3)$$

Also note that if $\alpha(a) = a'$, $\alpha^2(a) = a''$, then, by (1), we have:

$$\alpha^2(a) = a'' = ab \cdot b = \alpha(a') = a'b = \alpha^2(a)$$

implies

$$\alpha(a) = ab = a' = \alpha(a)$$

So, from 4.1.2 (2) we can cancel α successively n-times. That is

$$\alpha^{m-n}(a) = a$$

That is

$$\alpha(\alpha^{m-n-1}(a)) = a$$

But

$$\alpha^{m-n-1}(a) = b$$

for some $b \in G$. Hence

$$\alpha(b) = a$$

for some $b \in G$. So α is surjective and therefore bijective.

Since, for each $x \in G$, $\alpha(x) = ax \in G$, there is a unique $b \in G$ such that

$$ax = b \qquad 4.1.2\ (3)$$

So the equation 4.1.2 (3) has a unique solution. Similarly, by symmetry,

$$xa = b \qquad 4.1.2\ (4)$$

has a unique solution. The unique solution of the equations

$$ax = a \text{ and } xa = a$$

is the identity element e of G and, for $b = e$ in 4.1.2 (3) and 4.1.2 (4), the unique solution of

$$ax = e \text{ and } xa = e$$

is the inverse of a for each $a \in G$.

Hence G is a group.

4.1.3. Examples:

1. The sets $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ of integers, rationals, reals and of complex numbers respectively are groups under ordinary addition. These groups are all torsion *free*

2. The sets $\boldsymbol{Q'}$, $\boldsymbol{R'}$, $\boldsymbol{R^+}$, $\boldsymbol{C'}$ of non-zero rationals, reals, positive reals and complex numbers respectively form groups under ordinary multiplication. All these except $\boldsymbol{R^+}$ are not torsion free. (In $\boldsymbol{Q'}$, $\boldsymbol{R'}$, $\boldsymbol{C'}$, the element -1 is of order 2.)

3. The set C_n of all nth roots of unity for a fixed positive integer n is a group under the usual multiplication of complex numbers.

   Its elements are of the form

$C_k = e^{2k\pi i/n}$, $k = 0, 1, 2, ..., n-1$.

It is a finite group of order n.

4. The set P of all the nth roots of unity for n = 1, 2, ..., is a group under complex multiplication. It is an infinite periodic group.

5. The set S_A of all bijective mappings of a non-empty set A under the usual multiplication of mappings is a group. In particular the set

$$I_A, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi$$

of bijective mappings of the set $A = \{a, b, c\}$ is a group. Here φ and ψ are as given in example 3.2.1 (2).

The mappings φ and ψ satisfy the equations

$$\varphi^3 = \psi^2 = (\varphi\psi)^2 = I_A.$$

This group is non-abelian. In fact it is the smallest non abelian group. That is, every group whose order is < 6 is abelian.

6. For any non-zero positive integer n, the collection M_n of all $n \times n$ matrices form a group under matrix addition. The zero matrix is the identity under addition and each $A = (a_{ij}) \in M_n$ has $-A = (-a_{ij})$ as its additive inverse.

A matrix A is *non-singular* if its determinant is not zero. The collection M'_n of all $n \times n$ non-singular matrices form a group under matrix multiplication. Here the unity matrix I_n, with all the main diagonal elements as '1' and zero elsewhere, is the identity and each $A \in M'_n$ has $A' = (A_{ji}/\det A)$ as its multiplicative inverse. A_{ij} is the cofactor of a_{ij} in the determinant det (A) of A.

7. For any non-zero positive integer n let

$$\boldsymbol{Z}_n = \{0, 1, 2, ..., n-1\}.$$

Define addition in $\boldsymbol{Z}_n$ as follows:

For $a, b \in \boldsymbol{Z}_n$, we put

$$a + b = r$$

where r is the remainder obtained after dividing the ordinary sum of a and b by n. It is easy to verify that Z_n is a group under this 'addition'.

8. The '*quaternions*' $\pm I, \pm i, \pm j, \pm k$. satisfying the equations: $i^2 = j^2 = k^2 = -I$, $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$ form a group Q called the *group of quaternions*. This is a non-abelian group of order 8. The elements of Q are special cases of the so called *quaternions* $aI + bi + cj + dk$, where I, i, j, k follow the multiplication rules given above, discovered by W.R. Hamilton (1805-65). Hamilton discovered these quaternions in his efforts to represent 3-dimensional forces by some suitable elements.

The matrices

$$a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

satisfy the equations

$$a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1}$$

and form a group Q* consisting of the elements

$\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

The groups Q and Q* are isomorphic.

9. The set $\mathbf{V}_3(\boldsymbol{R})$ of all vectors in the three diamensional Euclidean space is a group under the 'vector addition' defined by:

$$\boldsymbol{x} + \boldsymbol{y} = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

for $\boldsymbol{x} = (x_1, x_2, x_1)$, $\boldsymbol{y} = (y_1, y_2, y_3)$ in $\mathbf{V}_3$ in $\mathbf{V}_3$ $(\boldsymbol{R})$. The zero vector $\boldsymbol{0} = (0, 0, 0)$ is the identity and each $\boldsymbol{x} = (x_1, x_2, x_3)$ has $-\boldsymbol{x} = (-x_1, -x_2, -x_3)$ as its additive inverse.

10. ***Group of Mobius Transformations***: Let $\boldsymbol{C} \cup \{\infty\}$ be the extended complex plane. Consider the set M of all bilinear transformations,

$\mu : \boldsymbol{C} \cup \{\infty\} \to \boldsymbol{C} \cup \{\infty\}$ defined by

$$\mu(z) = \frac{az+b}{cz+d},\ ad-bc \neq 0,\ z \in C \cup \{\infty\}$$

and a, b, c, d are themselves complex numbers. Multiplication of mappings in M is their successive application. The mapping

$I : C \cup \{\infty\} \to C \cup \{\infty\}$ given by

$I(z) = z$ for all $z \in C \cup \{\infty\}$

is the identity element of M. Also for each μ in M, its inverse is the mapping

$\mu' : C \cup \{\infty\} \to C \cup \{\infty\}$ given by

$$\mu'(z) = \frac{dz-b}{-cz+a}$$

Hence M is a group, called the *group of Mobius transformations.*

Of particular intereset are those mappings μ in M,

$$\mu(z) = \frac{az+b}{cz+a}$$

with $ad - bc = 1$. Such mappings also form a group. Both these groups are closely related respectively to the groups

$$M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in C \text{ and } ad-bc \neq 0.\right\}$$

and

$$M^* = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in C \text{ and } ad-bc = 1.\right\}$$

under matrix multiplication.

4.2. SUBGROUPS

A subset H of a group G is called a *subgroup* of G if and only if H is itself a group under the *same* algebraic operation as defined in G.

According to this definition, an arbitrary subset of a group need not necessarily be a subgroup of that group. The algebraic operation in G induces in a subgroup H an algebraic operation and it is with regard to this operation that H has to satisfy all the axioms of a group.

Thus a subset H of a group G may itself be a group under an operation different from that in G but may not be regarded as a subgroup of G.

For instance the set

$$C = \{\pm 1, \pm i\}$$

is a subset of the group $\boldsymbol{C}$ of complex numbers under addition, it is itself a group under the complex multiplication but is not a subgroup of $\boldsymbol{C}$.

Every group G has at least two subgroups namely the subset E, consisting of the identity element e alone, of G and the whole of G itself. E is called the *unit (identity* or *trivial)* subgroup of **G**.

A subgroup of G different from E and G is called a *proper subgroup* of G.

It is easy to see that the relation of 'being a subgroup of a group is a transitive relation. Thus if H is a subgroup of a group K and K is a subgroup of a group G then H is a subgroup of the group G.

The concept of subgroup is important in the whole of group theory. Most of the problems in group theory are concerned with the determination of subgroups G having certain specified properties.

4.2.1. Examples:

1. The set $\boldsymbol{R}^+$ of all non-zero positive real numbers under multiplication is a subgroup of the group $\boldsymbol{R}'$ of all non-zero real numbers under multiplication.

2. The set $\boldsymbol{Z}$ of integers under addition is a subgroup of the group $\boldsymbol{Q}$ of rational under addition, $\boldsymbol{Q}$ is a subgroup of the group $\boldsymbol{R}$ of real numbers under addition and $\boldsymbol{R}$ is a subgroup of the group $\boldsymbol{C}$ of complex numbers under addition.

3. The subset $\{i_A, \varphi, \varphi^2\}$ of the group

$$S_A = \{i_A, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi\} \text{ with } \varphi^3 = \psi^2 = (\varphi\psi)^2 = i_A$$

is a subgroup of S_A.

4. The set $\{\pm 1\}$ is a subgroup of the group $\mathbf{Q}'$ of non-zero rationals under ordinary multiplication. It also is a subgroup of the group $\{\pm 1, \pm i\}$ under complex multiplication.

The following theorem gives a necessary and sufficient condition for a subset of a group to be a subgroup.

4.2.2. Theorem: A non empty subset H of a group G is a subgroup of G if and only if, for any pair $a, b \in H$, $ab^{-1} \in H$; $a \neq e \neq b$

Proof: Suppose that H is a subgroup of a group G. Then H is itself a group under the same algebraic operation as defined in G. The element ab^{-1}, being the product of two elements a and b^{-1} of H, is in H.

Conversely, if, for each pair $a, b \in H$, $ab^{-1} \in H$, then, putting $b = a$, we have $ab^{-1} = aa^{-1} = e \in H$. The element e is the identity element of G and, since the equation $a.e = a$ is satisfied for all $a \in G$, it is satisfied in the subset H of G so that e is the identity element H. Taking $a = e$, we have, for any $b \in H$, $e.b^{-1} = b^{-1} \in H$. Hence every element of H has an inverse in H. Moreover, for any two elements $a, b \in H$, a, b^{-1} H. Hence $ab = a(b^{-1})^{-1} \in H$. Thus H is closed under the induced algebraic operation.

The associativity of the induced operation in H follows from that of the algebraic operation in G.

Therefore H is a subgroup.

One can easily establish the equivalence of the following condition for a subset H of a group G to be subgroup with that given in Theorem 4.2.2.

4.2.3. Theorem: A non-empty subset H of a group G is a subgroup of G if and only if, for any pair, $a, b \in H$, $ab \in H$ and for each $a \in H$, $a^{-1} \in H$.

Analogous to the intersection of sets one has the *intersection of subgroups of a group* G. Thus by the intersection $\cap \Omega$ of a collection Ω of subgroups of a group G we mean a subset of G all of whose elements are common to each member of the collection.

4.2.4. Theorem: Let Ω be a collection of subgroups of a group G. Then the intersection $\cap \Omega$ of the members of Ω is a subgroup of G.

Proof: Let $H = \cap \Omega$ and $a, b \in H$. Then $a, b \in A$ for each member subgroup $A \in \Omega$. Hence $ab^{-1} \in A$ for each $A \in \Omega$. Therefore $ab^{-1} \in \cap \Omega = H$. Thus H is a subgroup of G.

The intersection of a collection of subgroups of a group G is obviously the *largest subgroup of G* that is contained in every member of

the collection. The intersection of *all* the subgroup of G is, of course, the identity subgroup of G.

4.2.5. Theorem: Let A be an abelian group and F the set of all elements of finite order in A. Then F is a subgroup of A.

Proof: Let $a, b \in F$. Then there exist integers m and n such that

$$a^m = 1,\ b^n = 1,\ 1 \text{ being the identity in F.}$$

So
$$\begin{aligned}(ab)^{mn} &= ab \,.\, ab \,...\, ab \qquad (mn \text{ times})\\ &= a^{mn} \,.\, b^{mn}\\ &= (a^m)^n \,.\, (b^n)^m\\ &= 1 \,.\, 1\\ &= 1.\end{aligned}$$

Hence ab has finite order and so belongs to F. Moreover, if $a \in F$ and $a^m = 1$, then

$$\begin{aligned}(a^{-1})^m &= a^{-1} \,.\, a^{-1} \,...\, a^{-1} \qquad (m\text{–times})\\ &= a^{-m}\\ &= (a^m)^{-1}\\ &= 1\end{aligned}$$

So $a^{-1} \in F$. Hence F is a subgroup of A.

4.2.6. Theorem: The union $H_1 \cup H_2$ of two subgroups H_1, H_2 of a group G is a subgroup of G if and only of either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof: Clearly if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$, then $H_1 \cup H_2 = H_2$ or H_1 and so is a *subgroup of G.*

On the other hand, suppose that $H_1 \cup H_2$ is a subgroup of G, and let

$$H_1 \not\subseteq H_2,\ H_2 \not\subseteq H_1.$$

Let $a \in H_1 \backslash H_2$, $b \in H_2 \backslash H_1$. Since $a, b \in H_1 \cup H_2$ and $H_1 \cup H_2$ is a subgroup, $ab \in H_1 \cup H_2$. That is $ab \in H_1$ or $ab \in H_2$. Suppose that $ab \in H_1$. Then

$$b = a^{-1}(ab) \in H_1, \because H_1 \text{ is a subgroup,}$$

a contradiction. Similarly $ab \in H_2$ implies that $a = (ab)\, b^{-1} \in H_2$, a contradiction. Hence $H_1 \setminus H_2 = \phi$ or $H_2 \setminus H_1 = \phi$ so that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

An element x of order 2 in a group G is called an *involution.*

2.7. Theorem: Every group of even order has at least one *involution.*

Proof: Let G be a group of order $2n$. Let

$$A = \{x \in G : x^2 = e\},\ B = \{y \in G : y^2 \neq e\}.$$

Then, of course,

$$A \cup B = G \text{ and } A \cap B = \phi$$

If $B = \phi$ then $G = A$. So A and therefore G also contains an involution.

So let $B \neq \phi$ and let $y \in B$. Then, as $y^2 \neq e$, $y \neq y^{-1}$. But then $(y^{-1})^2 \neq e$ so that $y^{-1} \in B$. So, for each $y \in B$, y^{-1} also belongs to B. Thus the number of elements in B is even. Since the order of G is even and

$$|G| = |A| + |B|,$$

$|G|$ being the order of G, so the number of elements in A also is even.

Since $e^2 = e$, $e \in A$, $A \neq \phi$. Hence $|A| \geq 2$. Thus A and so also G contains an involution.

4.3. SUBGROUP LATTICES

By a *Lattice* we mean a partially ordered set $(L, \leq)$ in which any two elements a and b have the greatest lower bound and the least upper bound in L. Here the greatest lower bound and least upper bound of a and b are denoted by

$$a \wedge b \text{ and } a \vee b$$

respectively. For example the collection P(A) of all subsets of a non-empty set A is a lattice under a partial order which is the set inclusion.

Let G be a group and H, K be subgroups of G. Then, only here, we take $H \cup K$ as the subgroup of G which is the intersection of all subgroups S of G which contain both H and K. $H \cup K$, in this case, is *not* the set-theoretic *union*. We take

$$H \cap K \text{ and } H \cup K$$

as the greatest lower bound and the least upper bound of the subgroups H and K respectively. That is, $H \cup K$ is the smallest subgroup of G which contains both H and K.

For example, let

$$\mathbf{Q} = \{\pm I, \pm i, \pm j, \pm k\}$$

be the group of quaternions. Its subgroups are:

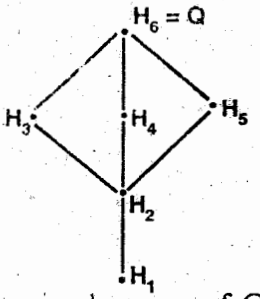
$$H_1 = \{I\}, H_2 = \{\pm I\}, H_3 = \{\pm I, \pm i\},$$

$$H_4 = \{\pm I, \pm j\}, H_5 = \{\pm I, \pm k\}, H_6 = \mathbf{Q}.$$

The lattice of its subgroups is:

$$L = \{H_1, H_2, H_3, H_4, H_5, H_6\}$$

and is shown by the following diagram.



Here, if A and B are subgroups of G and $A \subseteq B$, then A appears below B and a line segment connects the points representing A and B.

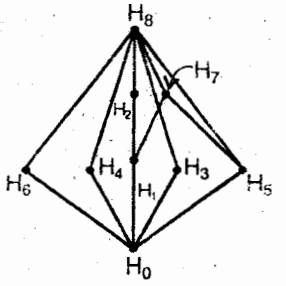
Likewise, as another example, let

$$D_4 = < a, b : a^4 = b^2 = (ab)^2 = 1 >$$

be the dihedral group of order 8. Its subgroups are

$H_0 = \{1\}$, $H_1 = < a^2, a^4 = 1 >$, $H_2 = <: a^4 = 1 >$, $H_3 = < b: b^2 = 1 >$,
$H_4 = < ab;(ab)^2 = 1 >$, $H_5 = < a^2b: (a^2b)^2 = 1 >$, $H_6 = < a^3b: (a^3b)^2 = 1 >$,
$H_7 = < a^2, b: a^4 = b^2 = (a^2b)^2 = 1 >$, $H_8 = < a, b: a^4 = b^2 = (ab)^2 = 1 > = D_4$.

The lattice diagram of the subgroups of D_4 is as follows.



4.4. RELATIONS BETWEEN GROUPS

Various relations exist between groups. The most fundamental of these are the relations of homomorphism and isomorphism of groups. These and a few related concepts are described below.

Let (G, .) and (G′, ×) be groups, A mapping $\varphi : G \to G'$ is called a *homomorphism of G to G′* if, for any pair $a, b \in G$,

$$\varphi (a . b) = \varphi (a) \times \varphi (b)$$

A homomorphism φ of G to G′ is called an epimorphism or an *epic* if φ is surjective and *a monomorphism* or a *monic* if φ is injective.

A homomorphism $\varphi : G \to G'$ is an *isomorphism* if φ is bijective.

Thus a mapping φ from G to G′ is an *isomorphism* if and only if

(i) φ is bijective

(ii) φ satisfies the homomorphism property, *i.e.*,

$\varphi (a . b) = \varphi (a) \times \varphi (b)$ for all $a, b \in G$.

Under isomorphic mappings the properties of groups such as commutativity of elements, finiteness of their orders etc., which are consequences of the algebraic operations defined in them and which are independent of the characteristics of individual elements, are preserved.

The relation of isomorphism between groups is an equivalence relation and therefore partitions the collection of *all* groups into equivalence classes of isomorphic groups. The structural results which are true for a representative of an equivalence class also hold for all the members of that equivalence class.

An *embedding* of a group G into a group G′ (or more generally, a set G′ with an algebraic operation) is simply a monomorphism of G into G′.

It G is embedded in a group G′ then G′ contains a subgroups H′, say, isomorphic to G.

It shall be shown that any group G can be embedded in a group of bijective mappings of a certain set. In general, there can be more than one embeddings of a group in a given group. This simply means that a group can have more than one subgroups isomorphic to a given subgroup.

As an example we have the group S_A of example 4.1.2 (5) which has three subgroups of order 2 namely the subgroups $\{i_A, \psi\}$, $\{i_A, \varphi\psi\}$ and $\{i_A, \varphi^2 \psi\}$. The group $\{\pm 1\}$ under multiplication is isomorphic to each of these subgroups.

For the sake of simplicity, and without any loss of generality, the algebraic operations in the two groups G and G′, having an isomorphism between them, will usually be taken as the same.

4.4.1. Examples:

1. The groups Z of integers and E of even integers, both under addition, are isomorphic under the mapping $\alpha : Z \to E$ given by:

$$\alpha(n) = 2n, n \in Z.$$

Here α is surjective because each even integer $2n$, $n \in Z$ is the image of the integer n under α. Also α is injective because:

$$\alpha(m) = \alpha(n)$$

implies

$$2m = 2n, \text{ that is } m = n.$$

Also

$$\begin{aligned}\alpha(m+n) &= 2(m+n)\\ &= 2m + 2n\\ &= \alpha(m) + \alpha(n).\end{aligned}$$

Hence α is a homomorphism and consequently an isomorphism between Z and E.

2. The groups R^+ of non-zero positive real number under multiplication and R of real numbers under addition are isomorphic under the isomorphic mapping $\varepsilon : R^+ \to R$ given by

$$\varepsilon(x) = \log x, x \text{ in } R^+,$$

since any real number r is the image of some positive real number e^r in $\mathbf{R}^+$ under ε (*i.e.*, $\varepsilon(e^r) = \log e^r = r$) and the equation $\varepsilon(x) = \varepsilon(y)$ implies $\log x = \log y$, yielding $x = y$. So ε is bijective. Moreover

$$\begin{aligned}\varepsilon(xy) &= \log(xy)\\ &= \log x + \log y.\\ &= \varepsilon(x) + \varepsilon(y)\end{aligned}$$

Hence $\varepsilon : R^+ \to R$ is an isomorphism.

3. Let A and B be groups with identities e and e' respectively. The set

$$P = \{(a, b) : a \in A, b \in B\}$$

with the algebraic operation given by:

$$(a, b) \cdot (a', b') = (aa', bb')$$

is a group. The mappings $\pi_A : P \to A$ and $\pi_B : P \to B$ given by:

$$\pi_A (a, b) = a, \qquad \pi_B (a, b) = b$$

are epimorphisms and are called *projection maps* of P to A and B respectively. The mapping $\delta : A \to P$ given by:

$$\delta (a) = (a, e')$$

is an embedding of A in P.

4. The group $A = \{a, b, c, d\}$ and $C_4 = \{\pm 1, \pm i\}$ having the following group tables are isomorphic.

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

An isomorphic mapping $\varphi : A \to C_4$ is given by:

$$\varphi (a) = 1, \varphi (b) = i, \varphi (c) = -1, \varphi (d) = -i.$$

Let φ be a homomorphism of a group G into a set G′ with an algebraic operation. The collection of those elements of G′ which are images of elements of G under φ is called the *homomorphic image of G* under φ and is denoted by φ (G).

4.4.2. Theorem: The homomorphic image φ (G) of a group G is itself a group.

Proof: Let G be a group and φ (G) the homomorphic image of G in a set G′ with an algeraic operation. To show that φ (G) is a group, we verify the axioms for a group.

Firstly to see that φ (G) is closed under the induced operation of G, let $\varphi (g_1), \varphi (g_2) \in \varphi (G)$, $g_1, g_2 \in G$. Then, since φ is a homomorphic,

$$\varphi (g_1) \cdot \varphi (g_2) = \varphi (g_1 \cdot g_2)$$

so that $\varphi (g_1) \cdot \varphi (g_2)$ is the image of $g_1 \cdot g_2 \in G$.

Hence $\varphi (g_1) \cdot \varphi (g_2) \in \varphi (G)$ and $\varphi (G)$ is closed.

Secondly, for the associative law in φ (G), let $\varphi (g_1), \varphi (g_2), \varphi (g_3) \in \varphi (G)$. Then

$(\varphi(g_1).\varphi(g_2)).\varphi(g_3) = \varphi(g_1 . g_2) . \varphi(g_3)$, 'φ is a homomorphism

$= \varphi((g_1 . g_2) . g_3)$

$= \varphi((g_1 . (g_2 . g_3))$, 'associative law holds in G.

$= \varphi(g_1) . \varphi(g_2 g_3)$

$= \varphi(g_1). (\varphi(g_2) . \varphi(g_3))$

Hence the induced operation in φ (G) is associative.

Thirdly if e is the identity in G, φ (e) is the identity in φ (G) because for any φ (g) ∈ φ (G), we have:

$$\varphi(g) . \varphi(e) = \varphi(g.e) = \varphi(g).$$

Lastly for each φ (g) ∈ φ (G), φ (g^{-1}) ∈ φ (G) and

φ (g) . φ (g^{-1}) = φ (gg^{-1}) = φ (e).

Hence φ (g^{-1}) is the inverse of φ (g) in φ (G). Therefore φ (G) is a group.

From the proof of the above theorem we have the following:

4.4.3. Corollary: Let φ : G → G′ be a homomorphism of G into G′, where G and G′ are groups. Then:

(i) The image of the identity of G is the identity element in φ (G).

(ii) The image of the inverse g^{-1} of g ∈ G is the inverse of the image *i e.*, φ (g^{-1}) = [φ (g)]$^{-1}$

Next we prove an important result concerning the embeddings.

4.4.4. Theorem: (Cayley's theorem). Any group G can be embedded in a group of bijective mappings of a certain set.

Proof: Let G be a group. For each g ∈ G, define a mapping φ_g : G → G by

$$\varphi_g(x) = gx$$

for all x ∈ G. Then φ_g is a bijective mapping because

$$\varphi_g(x) = \varphi_g(y) \Rightarrow gx = gy \Rightarrow x = y$$

and any element, say, y ∈ G is the image of $g^{-1} y$ ∈ G. Put

$$\Phi_G = \{\varphi_g : g \in G\}$$

Let φ_g, $\varphi_{g'}$ ∈ Φ_G. Then, for any x ∈ G,

$$(\varphi_g \varphi_{g'})(x) = \varphi_g (g' x) = g (g' x) = (gg') x = \varphi_{gg'}(x).$$

Hence

$$\varphi_g \cdot \varphi_{g'} = \varphi_{gg'} \qquad 4.4.4\,(1)$$

is an element of Φ_G.

It is easy to see that Φ_G is a subgroup of the group of all bijective mappings of the set G, has φ_e, e the identity in G, as the identity element and for each $g \in G$, $\varphi_{g^{-1}}$ as the inverse of $\varphi_g \in \Phi_G$.

We show that G is isomorphic to Φ_G. For this, define a mapping $\psi : G \to \Phi_G$ as follows:

Let $g \in G$. Put,

$$\psi(g) = \varphi_g.$$

Then ψ is a bijective mapping: ψ is surjective because each $\varphi_g \in \Phi_G$ is the image of a $g \in G$ and ψ is injective because

$$\psi(g_1) = \psi(g_2) \Rightarrow \varphi_{g_1} = \varphi_{g_2}$$

$$\Rightarrow \varphi_{g_1} \left(\varphi (g_2^{-1})\right) = \varphi_e$$

$$\Rightarrow \varphi_{g_1} \varphi_{g_2^{-1}} = \varphi_e$$

$$\Rightarrow \varphi_{g_1 g_2^{-1}} = \varphi_e$$

so that $g_1 . g_2^{-1} = e$, yielding $g_1 = g_2$.

Moreover if $g_1, g_2 \in G$, we have

$$\psi(g_1 g_2) = \varphi_{g_1 g_2}, \text{ by definition of } \psi$$

$$= \varphi_{g_1} . \varphi_{g_2}, \text{ by 4.4.4(1)}$$

$$= \psi(g_1) . \psi(g_2)$$

so that ψ is a homomorphism of G to Φ_G.

Hence G is isomorphic to Φ_G. Therefore G is embedded in a group of all bijective mappings of a set namely G.

In the case of finite group of order n the above theorem assumes the following form.

4.4.5. Corollary: Every finite group of order n can be embedded in a group of bijective mappings of a set consisting of n elements.

Cayley's embedding theorem reduces the study of all finite or infinite groups to that of the groups of bijective mappings of certain sets. The structure of these subgroups give us almost all the information that we need for a particular group. However this does not make life for the students of group theory any easier.

In the following theorem we discuss a special type of embedding of the group Z of integers under the addition into the group R' of all non-zero real number under multiplication.

4.4.6. Theorem: Let R' be the group of non-zero real number multiplication and Z the group of integers under addition. For each $r \in R'$, there is one and only one embedding $f_r : Z \to R'$ such that $f_r(1) = r$

Proof:

For each $r \in R'$, define a mapping $f_r : Z \to R'$ by:

$$f_r(n) = r^n \qquad 4.4.6\ (1)$$

for all $n \in Z$. Then $f_r(1) = r$ and

$$f_r(m + n) = r^{m+n} = r^m \cdot r^n = f_r(m) \cdot f_r(n).$$

So f_r is a homomorphism. For f_r to be an embedding we need only verify that f_r is injective. But this is so because if

$$f_r(m) = f_r(n)$$

for some $m, n \in Z$, then

$$r^m = r^n, \text{ that is, } r^{m-n} = 1 = r^0,$$

giving $m - n = 0$. The only point that remains to be proved is the uniqueness of f_r. Suppose that there is another embedding $gr : Z \to R'$ such that

$$g_r(1) = r.$$

Then

$$\begin{aligned} g_r(n) &= g_r(1 + 1 + \ldots + 1), \text{ n-times} \\ &= g_r(1) \cdot g_r(1) \ldots g_r(1) \ (\because g_r \text{ is a homomorphism.}) \\ &= r^n \\ &= f_r(n) \end{aligned}$$

for all $n \in Z$. Hence $g_r = f_r$ as required.

4.5. SYSTEMS OF GENERATORS AND RELATIONS IN A GROUP

Let G be a group and X an arbitrary non-empty subset of G. Such a subset is called a complex in G. The intersection K of all the subgroups of G which contain the set X is a subgroup of G called the *subgroup generated* by X and is denoted by:

$$K = \langle X \rangle$$

(read as 'K is the group generated by X')

Since K contains, together with every element of X, the inverse of each element in X and also, by closure law, the product of any two and therefore of finitely many elements in X and their inverses, an arbitrary element k of K can be written as:

$$k = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \dots x_{\alpha_m}^{\epsilon_m} \qquad 4.5\ (1)$$

where $x_{\alpha_i} \in X$ and $\epsilon_i = \pm 1$, i = 1, 2, ..., m.

The expression on the right hand side of equation 4.5 (1) is called a *word* in

$$x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_m}$$

If the subgroup K coincides with the group G, then X is called a system of *generators* for G and G is said to be *generated by X*. *X* is an *irreducible system of generators for* G if no proper subset of X can generated G.

A group G is *finitely generated* if and only if a generating set X of G is finite. Otherwise it is infinitely generated.

Finitely generated groups form a very important class of groups and have been the subject of study by various group theorists.

Let X be an arbitrary set of generators for a group G. If, for $x_{\alpha_i} \in X$ and $\epsilon_i = \pm 1$, i = 1, 2, ..., m, the equation

$$w(x_{\alpha_i}, x_{\alpha_2}, \dots, x_{\alpha_m}) = x_{\alpha_1}^{\epsilon_1} \cdot x_{\alpha_2}^{\epsilon_2} \dots x_{\alpha_m}^{\epsilon_m} = e \qquad 4.5\ (2)$$

where e is the identity of G, holds, then 4.5 (2) is called a *relation* in G. The word w in $x_{\alpha_1}, ..., x_{\alpha_m}$ is called a *relator*.

It is often convenient to represent a group in terms of generators and relations. If a group G has a set X as a system of generators and the words $w_1, ..., w_k$ as relators then we write

$$G = < X : w_1 = w_2 = ... = w_k = e > \qquad 4.5\ (3)$$

and read as 'G is a group generated by a set X with

$$w_1 = ... = w_k = e$$

as relations.

A collection of equations $w_1 = ... = w_k = e$, which hold in a group G, is called a system of *defining relations* if every relation in G is derivable from these. Equation 4.5 (3) is then called a *presentation of G*.

A group is *finitely presented* if and only if it has a finite system of generators and can be defined by a finite number of defining relations.

Not every group is finitely generated. For example the group of rationals under addition is not finitely generated.

It may be mentioned that the description of concepts like relations and presentations of groups given here is not very rigorous. A full account of these notions can be found in standard books on group theory.

The usefulness of a presentation of a group, that is, its description in terms of generators and relations, lies in the fact that, with their help, various types of calculations in the group become 'easier'. Given a group in terms of generators and relations it is, for example, 'less difficult' to show whether or not the given group reduces to the trivial group. Similarly the nature of generators and relations of two given groups helps us to determine the existence of a homomorphism between the groups.

4.5.1. Theorem: Let a group G have the presentation

$$G = < a, b: a^{-1} b^2 a = b^3, b^{-1} a^2 b = a^3 >.$$

Then G is the identity group.

Proof: From $a^{-1} b^2 a = b^3$ we have:

$$a^{-1} b^8 a = (a^{-1} b^2 a)^4 = b^{12} \qquad 4.5.1(1)$$

so that

$$a^{-2} b^8 a^2 = a^{-1} b^{12} a = (a^{-1} b^2 a)^6 = b^{18}. \qquad 4.5.1(2)$$

Thus, from 4.5.1 (2) and the equation $b^{-1} a^2 b = a^3$, we have

$$a^{-3} b^8 a^3 = b^{-1} a^{-2} b \,.\, b^8 b^{-1} a^2 b = b^{18},$$

using $b^{-1} a^{-2} b = a^{-3}$.

But $a^{-3} b^8 a^3 = a^{-1} (a^{-2} b^8 a^2) a = a^{-1} b^{18} a = (a^{-1} b^2 a)^9 = (b^3)^9 = b^{27}$.

That is,

$$b^{18} = a^{-3} b^8 a^3 = b^2$$

Hence $b^9 = 1$. Consequently 4.5.1 (2) becomes,

$$a^{-2} b^8 a^2 = 1$$

which is the same as $b^8 = 1$. This together with $b^9 = 1$ gives $b = 1$. but then $b^{-1} a^2 b = a^3$ becomes $a^2 = a^3$ which implies $a = 1$.

Hence G = {1}, as required.

Let $w (x_{\alpha_1}, \ldots, x_{\alpha_k})$ be a word in the variables $x_{\alpha_1}, \ldots, x_{\alpha_k}$. If the equation

$$w (g_{\alpha_1}, \ldots g_{\alpha_k}) = e \qquad 4.5.1\,(4)$$

holds for any choice of elements $g_{\alpha_1}, \ldots, g_{\alpha_k} \in G$

replacing $x_{\alpha_1}, \ldots, x_{\alpha_k}$, then $w = e$ is called an *identical relation* or a *law* in G.

A class of groups defined by a set of law is called a *variety*. The subject of *varieties of groups* has become an important and interesting part of the theory of groups. Its main contributors are B.H. Neumann, Hanna Neumann and their collaborators. There are many unsolved problems in this subject. (see Varieties of groups. by Hanna Neumann, Springer Verlag, 1967, for more details).

4.5.2. Examples:

1. The group C_4 of complex numbers 1, –1, i, –i has a presentation:

   $$C_4 = \langle x : x^4 = 1 \rangle$$

   with x as a generator and $x^4 = 1$ as a defining relation. $x^4 = 1$ is also an identical relation in C_4.

2. Consider the collection V_4 of real valued function. $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = 1/x$, $f_4(x) = -1/x$, under the multiplication defined by:

$$(gf)(x) = g(f(x)).$$

V_4 is a group having f_2, f_3 as generators and

$$f_2^2 = f_3^2 = (f_2 f_3)^2 = f_1$$

as defining relations.

Here

$$(f_2 f_3)(x) = f_2(f_3(x)) = f_2(1/x) = -1/x = f_4(x).$$

Put $f_1 = e, f_2 = a, f_3 = b$. Then $f_4 = ab$ and a presentation for V_4 is:

$$V_4 = \langle a, b : a^2 = b^2 = (ab)^2 = e \rangle$$

V_4 is called Klein's four-group.

3. A presentation for the group S_A of all bijective mappings of the set $A = \{x, y, z\}$ is

$$S_A = \langle \varphi, \psi : \varphi^3 = \psi^2 = (\varphi\psi)^2 = i_A \rangle.$$

Here φ and ψ are given by the equations

$$\varphi(x) = y, \varphi(y) = z, \varphi(z) = x,$$

$$\psi(x) = x, \psi(y) = z, \psi(z) = y,$$

while i_A denotes the identity mapping of A.

4. The group D_n having a presentation:

$$D_n = \langle a, b : a^n = b^2 = (ab)^2 = 1 \rangle$$

is called the *dihedral group* of order 2n.

For $n = 2$, D_2 is simply the Klein's four-group.

5. The group Q of quaternions $\pm I, \pm i, \pm j, \pm k$ has a presentation

$$Q = \langle a, b : a^4 = 1, a^2 = b^2 = (ab)^2 \rangle.$$

Here we have taken $a = i$, $b = j$.

Another presentation of the group Q of quaternions is

$$Q = \langle X, Y : X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, i = \sqrt{-1} \rangle$$

which represents Q in the matrix form. One can verify that

$$I, -I, X, -X, Y, -Y, XY, -XY$$

are the only eight elements of Q. Note that

$$X^2 = Y^2 = (XY)^2 = -I$$

is another presentation of Q.

6. Let Ω be a class of groups defined by the law

$$x^{-1} y^{-1} xy = e \qquad \text{(i)}$$

for all $x, y \in A$ in Ω.

Then Ω is called the *variety of abelian groups.*

If we add another law namely

$$x^m = e,$$

we get the variety Ω_m of all abelian groups of exponent m.

(A group G is said to have exponent m if and only if the equation $x^m = e$ is satisfied for all $x \in G$, i.e., $x^m = e$ is a law in G).

7. Consider the group generated by $a_0, a_1, a_2, \ldots$ with defining relations

$$a_o^p = 1, \; a_{n+1}^p = a_n,$$

where p is a prime integer and n = 0, 1, 2, ...

This group has an infinite number of generators and an infinite number of defining relations. It is known as Prüfer's $\overset{\infty}{p}$-group (after its discoverer H. Prüfer) and is denoted by C_{p^∞}.

Thus

$$C_{p^\infty} = < a_o, a_1, a_2, \ldots : a_o^p = 1, a_{n+1}^p = a_n, n = 0, 1, 2, \ldots >.$$

C_{p^∞} is an abelian group and has been used extensively to construct counter examples to various conjectural questions in group theory.

4.6. CYCLIC GROUPS

In the description of generators in 4.4.5, it was mentioned that for any non-empty subset X of a group G, the intersection H of all the subgroups of G that contain X is called the subgroup generated by X.

If X consists of a single element a, say, then H is called a *cyclic subgroup* of G and the element a is called its *generator*. Thus:

A group G is cyclic if and only if it coincides with one of its cyclic subgroups *i.e.*, if and only if it is generated by a single element.

Thus a cyclic group is one all of whose elements are powers of one and the same element.

If G is a cyclic group generated by a then, for any $x \in G$, there exists an integer k such that

$$x = a^k.$$

G is a finite or infinite cyclic group according as the order of a is finite or infinite.

If G is finite cyclic of order n then its elements are:

$$a^0 = e, a^1, a^2, ..., a^{n-1}$$

and a presentation of G is

$$G = \langle a : a^n = e \rangle.$$

Also $a^k = e$ in G if and only if k is divisible by n.

If G is an infinite cyclic group with a as its generator then no two distinct powers of a can be equal.

For suppose that $a^m = a^n$ for some integers m, n. We can suppose that $m > n$. Then $a^{m-n} = e$, the identity element in G. Hence, by the remark mentioned above, a has finite order, a contradiction.

Every cyclic group is abelian:

For if G is a cyclic group generated by a and $x, y, \in G$, there exist integers k, l such that $x = a^k$, $y = a^l$ and

$$xy = a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k = yx.$$

Examples of cyclic groups are the group Z of integers with 1 (or -1) as a generator and the group C_n of all the nth roots of unity. Elements of C_n are of the form

$$e^{2k\pi i/n}, k = 0, 1, 2, ..., n-1.$$

Also the group

$$G = < a : a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} >,$$

under matrix multiplication, is an infinite cyclic group. Here, by induction on n, one can easily deduce that

$$a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

The following theorem gives a complete characterization of the cyclic groups.

4.6.1. Theorem: Any two cyclic groups of the same order are isomorphic.

Proof: We shall establish this result by showing that a finite cyclic group of order n is isomorphic to the group C_n of all nth roots of unity and an infinite cyclic group to the group $\mathbf{Z}$ of integers under addition and use the transitive property of the relation of isomorphism.

Let G be a finite cyclic group of order n and generated by a. we define a mapping $\varphi : G \to C_n$ by:

$$\varphi(a^k) = e^{2k\pi i/n}.$$

Then φ is obviously surjective. It is injective because $\varphi(a^k) = \varphi(a^l)$ implies

$$e^{2k\pi i/n} = e^{2l\pi i/n}.$$

One can safely suppose that $k > l$. Then $e^{2(k-l)\pi i/n} = 1$ so that $k - l = 0$ or $k-l$ is divisible by n. As $k < n$, $l < n$, $k - l < n$, the latter case does not occur. Hence $k - l = 0$ *i.e.*, $k = l$ whence $a^k = a^l$.

Also for $a^k, a^l \in G$,

$$\begin{aligned} \varphi(a^k . a^l) &= \varphi(a^{k+l}) \\ &= e^{2(k+l)\pi i/n} \\ &= e^{2k\pi i/n} e^{2l\pi i/n} \\ &= \varphi(a^k) . \varphi(a^l). \end{aligned}$$

Hence φ is an isomorphism and $G \cong C_n$.

If G is an infinite cyclic group generated by a then we define a mapping $\varphi : G \to \mathbf{Z}$ by:

$$\varphi(a^k) = k, k \in \mathbf{Z}.$$

Then φ is obviously a bijective mapping and, as

$$\begin{aligned}\varphi(a^k \cdot a^l) &= \varphi(a^{k+l}) \\ &= k + l \\ &= \varphi(a^k) + \varphi(a^l),\end{aligned}$$

φ is an isomorphism between G and **Z**. This completes the proof of the theorem.

That the property in a group 'of being cyclic' is preserved under taking subgroups and homomorphic images is shown in the following theorems.

4.6.2. Theorem: Every subgroup of a cyclic group is itself cyclic.

Proof: Suppose that G is a cyclic group with a as its generator and H one of the subgroups. Let k be the least positive integer for which $a^k \in H$. If a^l is an arbitrary element of H, then there exist integers q and r such that

$$l = kq + r, 0 \leq r < k,$$

Hence

$$\begin{aligned}a^l &= a^{kq+r} \\ &= (a^k)^q \cdot a^r.\end{aligned}$$

As a^l and a^k are in H, $a^l \cdot (a^k)^{-q} = a^r \in H$. By the minimality of k, $r = 0$ and $l = kq$ so that $a^l = (a^k)^q$. Hence every element in H is a power of a^k and H is cyclic.

4.6.3. Theorem: A homomorphic image of a cyclic group is itself cyclic.

Proof: Let G be a cyclic group generated by a and φ (G) the homomorphic image of G under φ. Let $\varphi(a) = b \in \varphi$ (G). We show that every element of φ (G) is a power of b.

Let $x \in \varphi$ (G). Then there is an $a^k \in$ G such that $\varphi(a^k) = x$. However,

$$\begin{aligned}x = \varphi(a^k) &= \varphi(a \cdot a \ldots a) \\ &= b \cdot b \ldots b \\ &= b^k\end{aligned}$$

Hence φ (G) is cyclic with b as it generator.

4.6.4. Theorem: Let G be a cyclic group of order n. Then G contains one and only one subgroup of order d if and only if $d \mid n$.

Proof: Suppose that G is generated by a so that $a^n = e$. Suppose that $d > 0$ divides n. Then $n = kd$, for some integer k. So

$$H = < a^k : k = \frac{n}{d} >$$

is a subgroup of order d is G.

To see that H is the unique subgroup of order d in G, let K be another subgroup of order d in G and generated by a^s, $s > 0$. Then

$$(a^s)^d = a^{sd} = e$$

So n divides sd. Thus $sd = rn$ for some non-zero integer r. But $n = kd$. So $sd = rkd$. Therefore $s = rk$. Hence

$$a^s = a^{rk} \in H.$$

Therefore $K \subseteq H$. Since H and K are subgroups of G having the same order, H = K.

Conversely, suppose that a cyclic group G generated by a and of order n has a subgroup H of order d. Then d, being the order of a subgroup of G, divides n, as required.

REMARKS:

1. For each prime p there is only one isomorphic class of cyclic groups. That is there is (upto isomorphism) only one cyclic group of order p.

2. A group of order 1,000,000,007 is cyclic.
   Here the given number is a prime.

3. There are only two group of order 6.

4. There are only two groups of order
   1, 000, 000, 014, 000, 000, 049.
   The two groups are (i) cyclic group of order equal to the given number and
   (ii) the group $A = <a, b: a^k = b^k = 1, ab = ba, k = 1{,}000{,}000{,}007>$. >

A cyclic group can be generated by more than one element. It has already been mentioned that the group **Z** of integers can be generated by '1' as well as '−1'. Can there be other generators for **Z**? The following theorem gives information about the generators of a finite and infinite cyclic group.

4.6.5. Theorem:

Let G be a cyclic group generated by a, $G = \langle a \rangle$.

(i) If G is of finite order n then an element a^k in G is a generator of G if and only if k and n are relatively prime.

(ii) If G has infinite order, then a and a^{-1} are the only generators of G.

Proof:

(i) Suppose that $G = \langle a \rangle$ has finite order n. Then $a^n = e$. Suppose that k and n are relatively prime. Then there exist integers p, q such that

$$pk + qn = 1.$$

Let H be the subgroup of G generated by a^k. We prove that H = G.

For this it is enough to show that $a \in H$. Now

$$a = a^1 = a^{pk+qn} = (a^k)^p . (a^n)^q = (a^k)^p.$$

As $(a^k)^p \in H$, $a \in H$. Thus H = G and a^k is a generator for G.

Conversely, if a^k is a generator for G, then for some integer p,

$$(a^k)^p = a$$

That is,

$$a^{kp-1} = e$$

Hence n divides $kp - 1$, that is, $qn = kp - 1$ whence $kp - qn = 1$. Thus k and n are relatively prime.

(ii) Here

$$a^k \ k > 1, \text{ is a generator of } G \Leftrightarrow (a^k)^p = a \text{ for some integer } p$$
$$\Leftrightarrow a^{kp-1} = e.$$

So either $kp - 1 = 0$ or $kp - 1 \neq 0$. In the second case a has a finite order, which is a diviser of $kp - 1$, a contradiction because a has infinite order. In the first case, $kp = 1$ so that $k = 1 = p$ or $k = -1 = p$. Hence both a and a^{-1} are the generators of G.

4.6.6. Theorem: Let G be a cyclic group generated by a.

1. If the order of a is infinite then there is a one-one correspondence between the set of all subgroups of G and the set of natural numbers.
2. If the order of a is n then there is a one-one correspondence between the subgroups of G and the set of all divisors of n.

Proof: Suppose that G is generated by a. Then, for each subgroup H of G there is a least natural number k such that $a^k \in H$ and H is generated by a^k.

1. If the order of a is infinite then, for each subgroup H of G, we have a natural number k as stated above.

   Conversely, if k is a natural number then the set

   $$\{a^{mk} : m = 0, \pm 1, \pm 2, \ldots\}$$

   is a subgroup of G. Hence, in this case, there is a one-one correspondence between the set of all subgroups of G and the set of natural numbers.

2. If the order of a is n then again, for each subgroup H of G, there is a smallest natural number k such that $a^k \in H$ and generates H. Let q be the order of H. Then, using the fact that $k < n$, $q < n$, $e = a^{qk} = a^n \Rightarrow n = qk$ so that k divides n.

Conversely, if k divides n so that $n = qk$, the elements

$$a^k, a^{2k}, \ldots, a^{(q-1)k}, a^{qk} = a^n = e$$

form a subgroup H of G of order q. Thus, for each divisor k of n, there is a subgroup of G. Hence the theorem.

Let G be a group. Recall that the least positive integer m (if it exists) such that

$$a^m = e$$

for all $a \in G$, is called the *exponent of G* and G is said to have exponent m.

For example the group Q of quaternions has exponent 4 because

$$x^4 = e$$

for all $x \in Q$ and 4 is the least such positive integer.

It is easy to see that every cyclic group of order n, which is also the order of its generator, has exponent n. In terms of this concept, we have the following characterization of a cyclic group.

4.6.7. Theorem: An abelian group C of order n is cyclic if and only if its exponent is n.

Proof: If C is cyclic of order n, then the foregoing remark shows that C has exponent n.

Conversely, suppose that C is an abelian group of order n and its exponent also is n. We show that C is cyclic.

First we show that, for any two elements a and b of order p, q respectively, in C, with $(p, q) = 1$, ab has order pq.

Here, if the order of ab is k, we have

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

so that

$$a^k = b^{-k} = c, \text{ say.}$$

Let m be the order of c. Then m divides the orders of a and b.

So m | (p, q). Since $(p, q) = 1$, $m = 1$. Hence $c = e$ so that

$$a^k = b^k = e$$

But then p|k, q|k. Hence pq|k. Also

$$(ab)^{pq} = (a^p)^q . (b^q)^p = e = (ab)^k$$

Hence $k \mid pq$. Thus $k = pq$.

Next let x be an element of maximal order in C so that

$$x^m = e.$$

We show that, for each $y \in C$, $y^m = e$.

For this, since C is finite, let k be the order of y. Let

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \ldots p_s^{\beta_s}$$

where $\alpha_i \geq 0$, $\beta_j \geq 0$, $1 \leq i \leq j \leq s$. If $y^m \neq e$ then k does not divide m. So, for some i,

$$\alpha_i > \beta_i.$$

Without any loss of generality we can suppose that i = 1 so that $\alpha_1 > \beta_1$. Take

$$x' = x^{p_1^{\beta_1}}, y' = y^{p_2^{\alpha_2}} \ldots p_r^{\alpha_r}$$

Then

$$(x')^{p_2^{\beta_2} \ldots p_s^{\beta_s}} = x^m = e$$

and

$$(y')^{p_1^{\alpha_1}} = y^{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}} = y^k = e$$

Since

$$(p_1^{\alpha_1}, p_2^{\beta_2} \ldots p_s^{\beta_s}) = 1,$$

x' y' has order $p_1^{\alpha_1} p_2^{\beta_2} \ldots p_s^{\beta_s} > m$. This contradicts our choice of x. Hence $y^m = e$, so that m is the exponent of C. But then m = n. Thus x has order n in C which also has order n. Hence C is a cyclic group generated by x.

4.6.8. Theorem: Let $G_1, G_2, \ldots$ be subgroups of a group G. If $G_i \subset G_{i+1}$, $G_i \neq G_{i+1}$ for i = 1, 2, ..., then $\bigcup_{i=1}^{\infty} G_i$ is not a cyclic group.

Proof: Put $K = \bigcup_{i=1}^{\infty} G_i$. First we show that K is a subgroup of G.

If $a, b \in K$, then there exist integers m, n such that $a \in G_m$ and $b \in G_n$. We can suppose that n > m. Then $G_m \subset G_n$ and so $a, b \in G_n$. As G_n is a subgroup, $a, b, \in G_n$ implies ab^{-1} $G_n \subset K$, proving that K is a subgroup of G.

Now suppose that $K = \langle a \rangle$ is a cyclic group generated by a. Then $a \in G_m$ for some integer m. As G_m is a group, every power of a belongs to G_m so that

$$\langle a \rangle = K = \bigcup_{i=1}^{\infty} G_i \subseteq G_m.$$

But $G_m \subseteq K$. Hence $G_m = K$. So

$$G_m \subset G_{m+p} \subset K = G_m, p \geq 1.$$

Hence $G_m = G_{m+p}$ for all $p \geq 1$, a contradiction to the fact that $G_m \neq G_{m+1}$.

Hence $K = \bigcup_{i=1}^{\infty} G_i$ is not cyclic.

4.6.9. Theorem: Let Q be the group of rationals under addition. Then any two generator subgroup of Q is infinite cyclic.

Proof: Let

$$H = <\frac{m_1}{n_1}, \frac{m_2}{n_2}>$$

be a two generator subgroup of Q. If $d = (m_1, m_2)$, the greatest common divisor of m_1, m_2, then there exists integers q_1, q_2 such that

$$m_1 = q_1 d, \; m_2 = q_2 d.$$

Let $a = \frac{d}{n_1 n_2}$. Now

$$\frac{m_1}{n_1} = q_1 \cdot \frac{d}{n_1} = q_1 n_2 \frac{d}{n_1 n_2} = q_1 n_2 a$$

Similarly

$$\frac{m_2}{n_2} = q_2 n_1 a.$$

So both $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are in the cyclic group generated by a. Hence

$$H \subseteq <a>.$$

As the subgroups of a cyclic group are cyclic, H is cyclic. Of course, H is infinite.

4.6.10. Corollary: Any finitely generated subgroup of the group Q of rationals under addition is cyclic.

Proof: Let $H = <\frac{m_1}{n_1}, \frac{m_2}{n_2}, ..., \frac{m_p}{n_p}>$ be a finitely generated subgroup of Q.

Let d be the greatest common divisor of $m_1, m_2, ..., m_p$, and put

$$a = \frac{d}{n_1 n_2 ... n_p}.$$

vThen each $m_i / n_i \in < a >$, $1 \leq i \leq$ ρ. Hence $H \subseteq < a >$. Thus H, as a subgroup of a cyclic group, is cyclic.

Let P be a property of groups like finiteness, cyclicity, abelianness etc.

A group G is said to be *locally* P if every finitely generated subgroup of G has the property P. Thus a group G is said to be *locally finite* if every finitely generated subgroup of G is finite. Similarly a group G is said to be *loeally cyclic* if every finitely generated subgroup of G is cyclic.

The Corollary 4.6.10 shows that the rationals under addition form a locally cyclic group. This is *locally infinite* as well.

An example of a locally finite group is the Prüfer's p^∞-group C_{p^∞} described in example 4.5.2 (7). C_{p^∞} is also locally cyclic (proved!).

4.7. GROUPS AND SYMMETRIES

By a *symmetry* of a geometrical figure we mean an orthogonal affine transformation of the plane (or 3-dimensional) which leaves the figure invariant. In easier connotation, symmetry of a geometric figure is a rigid motion of it which leaves it in a shape or appearance similar to that it was before the movement was made. Many groups arise in the form of groups of symmetries of geometric figures. In general, for any set of points S in a plane, the set of all distance preserving injective mappings of a plane which leave the points of S invariant are called *symmetries* of S under the binary operation as composition of mappings and form a group G_s called the *symmetry group* of S.

Symmetry groups of geometric figures provide us with an excellent source of examples.

For more complicated than plane symmetries are the symmetries of objects in space. Modern day crystallography and crystal physics are mainly concerned with the properties of groups of symmetries of three-dimensional shapes.

Groups of symmetries find their main use in the theory of electron structure and of molecular vibrations. In elementary particle physics such groups have been used to predict the existence of certain elementary particles before they were found experimentally.

One comes across with symmetries and their group everywhere in nature: in quantum mechanics, flower petals, cell division, the work habits

of bees in the hive, snowflakes, music and floral paintings and tiles structures in mosques and other religious and historical buildings.

The groups of symmetries of some geometrical figures are described in the next paragraphs.

4.7.1 Symmetries of a Rectangle:

Let R be a rectangle with vertices denoted by the numerals 1, 2, 3 and 4 as shown in figure 1.1. The rigid motion s of a rectangle with vertices 1, 2, 3, 4 and centre 0 are the rotations about its centre through and angle of 180° and reflections about its horizontal and vertical axes KL, MN respectively.

Consider the following right motions of R:

e: No motion at all. This is equivalent to a rotation of the rectangle about its centre O through an angle of 360°. This motion does not bring any change in the vertices.

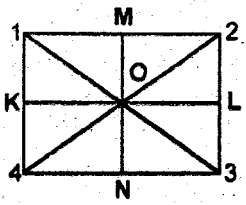


Fig. 1.1

α: The rotation of the rectangle about its centre O through an angle of 180°. The resulting rectangle is shown in figure 1.2.

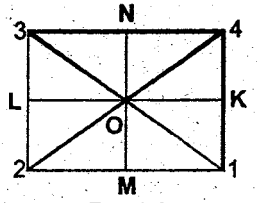


Fig. 1.2

β: The reflexion in the horizontal axis through O. Under this motion resulting rectangle is shown in figure 1.3.

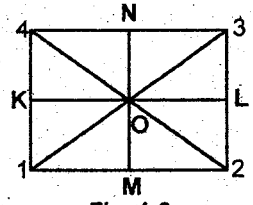


Fig. 1.3

γ: The reflexion in the vertical axis through O. Under this motion the resulting rectangle is shown in figure 1.4.

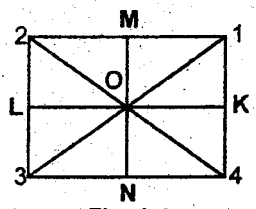


Fig. 1.4

It is easy to see that each rigid motion of the rectangle is one of teh motions e, α, β and γ. Moreover each of the three motions α, β, γ, when repeated, gives us the original figure. Also note that the motions α and β undertaken successively result is the motion γ. So if we denote this 'product' of α and β by $\alpha\beta$, (here we perform α first and then β), then this results in the motion γ. So

$$\alpha\beta = \gamma$$

Likewise $\beta\alpha = \gamma$

One can easily verify that

$$\alpha^2 = \beta^2 = (\alpha\beta)^2 = e$$

The motions e, α, β and $\alpha\beta$ thus form a group called the Klein's Four-group and is the smallest non-cyclic group.

A 'permutation' representation of this group is:

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

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

We shall learn more about permutations in a later chapter.

4.7.2. Symmetries of a Square:

Recall that rigid motion of a geometric object preserves distance between any two of its points. In the case of a square, as shown in figure also, rigid motions are either the rotations, anticlockwise, of the square through the angles 0°, 90°, 180° and 270° or the reflexions of the square in its diagonals and horizontal and vertical axes as described below. Each of these motions is characterized by its effect on the vertices 1, 2, 3 and 4.

Here

$\alpha_1 = e =$ The identity rotation or rotation of the square through an angel of 360o about its centre O.

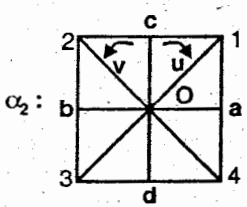


Fig. 2.1

$\alpha_2 = \alpha =$ The rotation of the square through an angle of 90° about its centre O.

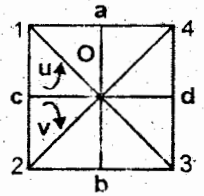


Fig. 2.2

$\alpha_3 = \alpha^2 =$ Rotation of the square through an angle of 180° about O.

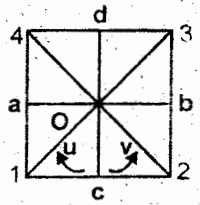


Fig. 2.3

$\alpha_4 = \alpha^3 =$ Rotation of the square through an angle of 270° about O.

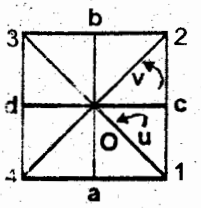


Fig. 2.4

$\alpha^4 = e =$ Rotation of the square though an angle of 360° about O.

(Here we get the original position of the square fig 2.1)

$\alpha^4 = e$

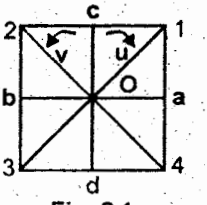


Fig. 2.1

$\alpha_5 = \beta =$ Rotation of the square in its horizontal axis through O.

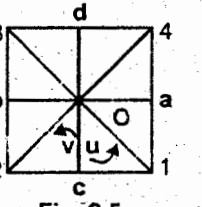


Fig. 2.5

$\alpha_6 = \alpha\beta =$ Reflection of the square in its diagonal v.

This motion is the same as first the rotation α (figure 2.2) and then followed by reflection β in the horizonal axis cd (fig 2.2)

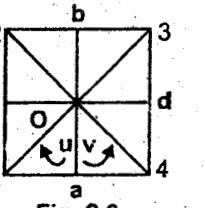


Fig. 2.6

$\alpha_7 = \alpha^2\beta =$ Reflection of the square in its vertical (cd of fig 2.2) axis through O.

This motion is the same as first applying α^2 (fig 2.3)and then reflection in its vertical axis (fig 2.3)

α_7 :

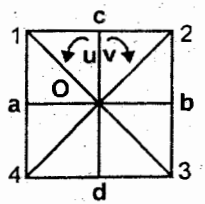


Fig. 2.7

$\alpha_8 = \alpha^3\beta =$ Reflection of the square in its diagonal u.

This motion is the same as first applying α^3 (fig 2.4) and then applying reflection in the diagonal u (fig 2.4)

$\alpha_8 =$

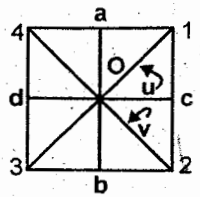


Fig. 2.8

One can easily see that all the rigid motions of square only are

$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7$, and α_8.

We put

$\alpha_1 = e$, $\alpha_2 = \alpha$ and $\alpha_5 = \beta$.

Then one can verify that the elements α_i, $1 \le i \le 8$, can be written as:

$e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta$

when $\alpha\beta$ means first α and then β.

These elements form a group called the *optic group* or *the dihedral group* of order 8.

Its permutation representation is as follows:

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

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

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

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

as can be seen from the figures give above.

Note that, in this group

$$\beta\alpha = \alpha^3\beta$$

as can be seen by actually performing the motions β, α and α^3, β.

4.7.3. Group of Symmetries of an Equilateral Triangle:

Let the vertices of an equilateral triangle be denoted by the numerals 1, 2, 3. The rigid motions of the equilateral consists of rotations of the triangle about its centre through angles of 0°, 120°, 240° and its reflections in its medians.

These rigid motions are shown in the following firgures.

e: The identity motion. This is the rotation of the triangle about its centre O through an angle of 360°.

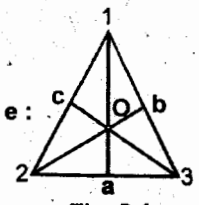


Fig. 3.1

α_1: Rotation of the triangle (original position) through an angle of 120° about O.

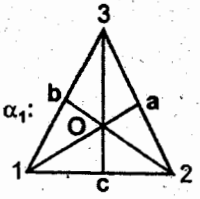


Fig. 3.2

α_2 Rotation of the triangle through an angle of 240° about O.

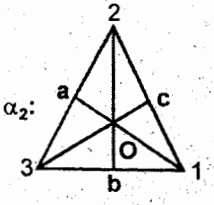


Fig. 3.3

α_3 Reflection in the vertical median *a*.

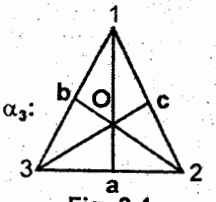


Fig. 3.4

α_4 Reflection in the median b.

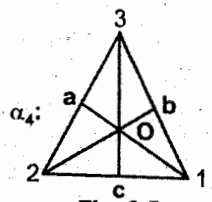


Fig. 3.5

α_5 Reflection in the median c.

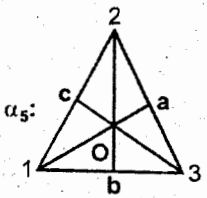


Fig. 3.6

So the group of symmetries of an equilateral triangle consists of the elements:

$$e, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \text{ and } \alpha_5.$$

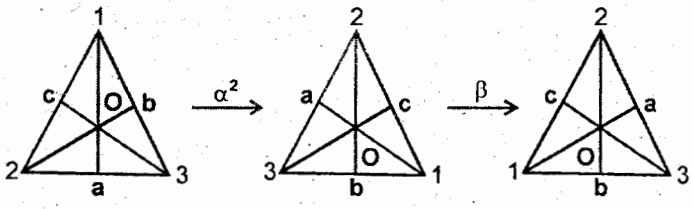
If we write α for α_1 and β for α_3, then one can easily verify that

$$\alpha_2 = \alpha^2, \alpha_3 = \beta, \alpha_4 = \alpha\beta, \alpha_5, = \alpha^2\beta.$$

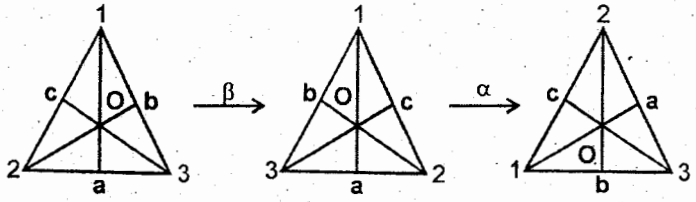
So this group consists of

$$e, \alpha, \alpha^2, \beta, \alpha\beta \text{ and } \alpha^2\beta \text{ with } \alpha^3 = \beta^2 = (\alpha\beta)^2 = e$$

Note that here the effect of $\alpha^2\beta$ and $\beta\,\alpha$ is shown below:



and



So

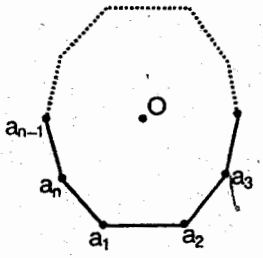
$\beta\alpha = \alpha^2\beta$.

Thus the group G of symmetries of an equilateral triangle is not an abelian group.

G is the smallest finite non-abelian group.

4.7.4. Group of Symmetries of an n-Polygon:

A regular n-gon or n-polygon is a geometrical figure all of whose sides and angles are equal. Each internal angle of an n-gon is $\theta = \pi\ (n - 2k)\ /n = \pi - 2k\pi/n$ radians.



The group of symmetries of an n-gon consists of:

rotations. $r_0 = e, r_1, r_2, ..., r_{n-1}$ about its centre O through an angle of $2k\pi/n$ radians, $k = 0, 1, 2, ..., n-1$, all clockwise or all anti-clockwise.

The 'product' of two rotations r_i and r_j is their successive application and is equivalent to a rotation through an angle of $2\pi(i + j)/n$ radians.

This rotation is the same as the rotation r $(i + j)$, where $(i + j)'$ is the least positive residue of $i + j$ modulo n.

Reflections. Here we must distinguish two cases namely when n is even or odd. In the case when n is even, there are two types of reflections.

Type I: This type consists of reflections in a line joining the mid points of the opposite sides.

Type II: This type consists of reflections in a line joining two opposite vertices.

If n = 6, these reflections are in the bold lines and dotted lines in figure 4.1.

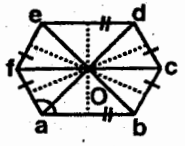


Fig. 4.1

If n is odd then we cannot talk about the opposite sides and opposite vertices. In this case we consider reflections through those lines which join a vertex with the mid point of the opposite side.

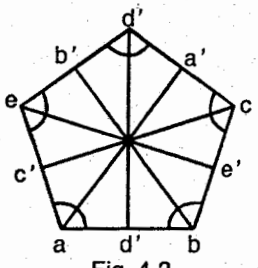


Fig. 4.2

The classes of symmetries described above exhaust all possible situations. The group of symmetries of an n-gon consists of 2n elements, that is, n rotations and n reflections. This group is denoted by D_n and is called the *dihedral group of order* $2n$.

We write $r_1 = \alpha$. Then $r_i = \alpha^i$, $1 \le i \le n-1$ and $r = 0 = e$.

Also if n is even and β denotes the reflection in any line joining the mid points of the opposite sides, the elements of D_n are

$$e, \alpha, \alpha^2, ..., \alpha^{n-1}, \quad \beta, \alpha\beta, \alpha^2\beta, ..., \alpha^{n-1}\beta.$$

with

$$\alpha^n = \beta^2 = (\alpha\beta)^2 = e.$$

If n is odd and β is the reflection in any line joining the mid point of a side to the point opposite to it then the group D_{2n} again consists of

$$e, \alpha, \alpha^2, ... \alpha^{n-1}, \beta, \alpha\beta, ..., \alpha^{n-1}\beta.$$

Thus, when n = 2, we get the dihedral group of order 4 which is simply the Klein's four-group. For n = 3, 4, 5 and 6, we get the groups of symmetries of an equilateral triangle, a square, a pentagon and an hexagon, respectively.

EXERCISES

1. Which of the following sets are groups and why?

   (a) The set $C = \{2^n, n \in \mathbf{Z}\}$ under multiplication.

   (b) The set of non-zero positive irrational numbers under multiplication.

   (c) The set **U** of all complex numbers of unite modulus under complex multiplication.

   (d) The set **Z** of integers under the usual subtraction.

   (e) The set $X = \{0, 1, 2, 3\}$ under the algebraic operation defined by:

   $$x \times y = r, \qquad x, y \in X$$

   where r is the remainder obtained after dividing the usual product xy of x and y by 4.

   (f) The set $A = \{1, 2, 3, 4\}$ under 'multiplication' defined by:

   $$x \times y = r, \qquad x, y \in A$$

where r is the remainder obtained after dividing the usual product of x, y by 5.

(g) The set $A = \left\{\left(\frac{1+2m}{1+2n}\right); m, n \in \mathbf{Z}\right\}$ under ordinary multiplication.

(h) The set G of non-zero real numbers under the binary operation

$$a * b = \frac{ab}{2}, a, b \in G.$$

2. Let G be a group and H = G. For a fixed element a of G, define a binary operation $\times$ in H by:

$$x \times y = x\, a\, y$$

for all $x, y \in H$. Show that H is a group with a^{-1} as its identity and, for each $x \in G$, $a^{-1}\, x^{-1}\, a^{-1}$ as its inverse.

3. Justify the following definition of a group.

An ordered pair (G, .) where G is a non-empty set and '.' an algebraic operation in G, is a group if and only if

(a) '.' is associative

(b) The equations

$$ax = b \quad \text{and} \quad ya = b$$

have unique solutions in G for all $a, b \in G$.

4. Let B^n be a subset of $\boldsymbol{R}^n$ such that, for each $x = (x_1, x_2, ..., x_n)$ in B^n, $x_i = 0$ or 1. Show that $(B_n, +)$ is a group.

(A subset of B^n is called a *code* and the elements of the subset are called *code words*).

5. In a group G, let $a, b, c \in G$. Show that there is a unique $x \in G$ such that $a\, x\, b = c$.

[**Hint:** Here $a\, x\, b = c \Rightarrow x = a^{-1}\, cb^{-1}$ which is in G. Uniqueness?]

6. Let n be a fixed integer and $\mathbf{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$ be all the distinct congruence classes in $\mathbf{Z}$ modulo n. Define an algebraic operation '+' in $\mathbf{Z}_n$ by:

(i) $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a}$, $\overline{b} \in Z_n$

where $\overline{a+b}$ is the class containing $a + b$. Show that the class $\overline{a+b}$ is the same as the class $\overline{r}$, where r is the remainder obtained after dividing $a + b$ by n. Show that $(\mathbf{Z}_n, +)$ is a group.

Define another algebraic operation $\times$ in $\mathbf{Z}_n$ by

(ii) $\overline{a} \times \overline{b} = \overline{a \times b}, \overline{a}, \overline{b} \in \mathbf{Z}_n$.

Show that the class $\overline{a \times b}$ is the same as the class $\overline{r}$, where r is the remainder obtained after dividing the usual product $a \times b$ of a, b by n. Prove that the set $\mathbf{Z}'_n$ of all non-zero congruence classes modulo n under the binary operation $\times$ is a group if and only if n is a prime.

Write down the addition tables for $\mathbf{Z}_4$, $\mathbf{Z}_7$ and the multiplication table for $\mathbf{Z}'_7$.

7. Show that the set F of the six complex valued functions:

$$f_1(z) = z, \quad f_2(z) = \frac{1}{1-z}, \quad f_3(z) = \frac{z-1}{z},$$

$$f_4(z) = \frac{1}{z}, \quad f_5(z) = 1 - z, \quad f_6(z) = \frac{z}{z-1},$$

is a group under the usual multiplication of mappings.

8. Let G be the set of all rotations about origin in a cartesian plane.

An element of G is a rotation $\mathbf{R}_\theta : \mathbf{R}^2 \to \mathbf{R}^2$ such that:

$$\mathbf{R}_\theta(x, y) = (x', y')$$

where $x' = x\cos\theta - y\sin\theta$, $y' = x\sin\theta + y\cos\theta$

Show that G is a group under the usual composition of rotations $\mathbf{R}_\theta$ (as mapping).

9. (a) For any integer n, let $\alpha_n : \mathbf{Z} \to \mathbf{Z}$ be such that

$$\alpha_n(m) = m + n, \; m \in \mathbf{Z}$$

Let $A = \{\alpha_n ; n \in \mathbf{Z}\}$. Show that A is a group under the usual composition of mappings.

(b) For a real number r define a mapping $t_r : \boldsymbol{R} \to \boldsymbol{R}$ by:

$$t_r(x) = x + r, x \in \boldsymbol{R}.$$

Show that T = $\{t_r : r \in \boldsymbol{R}\}$ is a group under the usual composition of mappings. (T is, in fact, the set of all translations on the real line).

(c) For real numbers a, b, define a mapping $\mu_{a,b} : R \to R$ by:

$$\mu_{a,b}(x) = ax + b, x \in R.$$

Prove that the set M = $\{\mu_{a,b} : a, b \in \boldsymbol{R}, a \neq 0\}$ is a group under the ordinary composition of mappings. Is this group abelian? Show that T of (b) above is a subgroup of M.

10. For any real numbers r, s, define a mapping $\delta_{r,s} : \boldsymbol{R}^2 \to \boldsymbol{R}^2$ by:

$$\delta_{r,s}(x, y) = (x + r, y + s), (x, y) \in \boldsymbol{R}^2$$

Let D = $\{\delta_{r,s} ; r, s \in \boldsymbol{R}\}$. Show that D is a group under ordinary composition of a mappings. (D is the set of all distance preserving mappings in plane).

11. Let (X, d) , (Y, d') be metric spaces. A mapping $\varphi : X \to Y$ is said to be an *isometry* if φ is bijective and

$$d'(\varphi(x), \varphi(x')) = d(x, x') \text{ for all } x, x' \in X.$$

Show that the set M of all isometries defined from (X, d) to itself is a group under the usual composition of mappings. (Properties of M for different metric spaces still need investigation).

[To see that φ^{-1} is an isometry note that, for $y = \varphi(x)$, $y' = \varphi(x')$,

$$d'(y, y') = d'(I(y), I(y')) = d'(\varphi(\varphi^{-1}(y)), \varphi(\varphi^{-1}(y')))$$
$$= d(\varphi^{-1}(y), \varphi^{-1}(y'))].$$

12. Show that the groups G and H of exercise 2 are isomorphic under the mapping $\alpha : G \to H$ given by $\alpha(x) = a^{-1}x$ for all $x \in G$ and a, a fixed element of G.

13. Show that the following matrices form a group isomorphic to the group of quaternions.

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, -\mathbf{I} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, -\mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, -\mathbf{j} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, -\mathbf{k} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, i^2 = \sqrt{-1}.$$

14. For any group G prove that the following conditions are equivalent.
    (a) G is abelian.
    (b) $(ab)^{-1} = a^{-1} b^{-1}$ for all $a, b \in G$.
    (c) $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

15. Show that a group in which every element is of order 2 is necessarily abelian.

16. For a finite group G show that there is a finite integer n such that
    $a^n = e$ for all $a \in G$.

17. Verify the following statements.
    (i) The additive group $\boldsymbol{Z}$ of integers is generated by 2, 3.
    (ii) The additive group $\boldsymbol{Q}$ of rational numbers is generated by the set $\{1/p : p \text{ a prime}\}$.

18. Show that the additive group Q of rationals is not finitely generated:
    [Hint : Suppose that $\boldsymbol{Q}$ is finitely generated and $\left\{\frac{m_1}{n_1}, ..., \frac{m_k}{n_k}\right\}$ is a system of generators for Q. Consider now $\frac{1}{2n_1}$. Then
    $$\frac{1}{2n_1} \text{ is not in } < \frac{m_1}{n_1}, ..., \frac{m_k}{n_k} >.]$$

19. If H is a non-empty subset of a group G, verify that the following conditions are equivalent.
    (a) H is a subgroup of G
    (b) $HH^{-1} \subseteq H$
    (c) $H^2 \subseteq H$ and $H^{-1} \subseteq H$.
    (d) $hH = H$ for all $h \in H$.

20. Let G be a group.
    (a) For any two elements a, b of G, show that the elements ab and ba have the same order.

(b) For $a, b \in G$, if $ba = a^r b^s$ for some integers r and s, then the elements $a^{r-2} b^s$, $a^r b^{s-2}$, ab^{-1} and ba^{-1} have the same order.

(c) For $a, b \in G$, let there be an $x \in G$ such that

$$b = xax^{-1}.$$

Show that a and b have the same order.

(d) If $ba = a^k b$ for $a, b \in G$ and some integer k, then

$$b^r a^s = a^{ks^r} b^r.$$

(e) If G is abelian and $a, b \in G$ have orders m and n where m and n are relatively prime, then ab has order mn. If m, n are not relatively prime then ab has order k where k is the least common multiple of m and n.

21. Determine all the subgroups of:

(i) the four-group $\{e, a, b, ab\}$ with $a^2 = b^2 = (ab)^2 = e$.

(ii) the cyclic groups of order 4 and 5.

(iii) the group G consisting of the elements e, a, a^2, b, ab, a^2b with $a^3 = b^2 = (ab)^2 = e$.

(iv) the group Q of all quaternions.

22. Let a, b be elements of a group G and $a^2 = 1$, $a^{-1} b^2 a = b^3$. Prove that $b^5 = 1$.

[Hint: Here

$$(a^{-1} b^2 a)^6 = b^{18}, \text{ that is, } a^{-1} b^{12} a = b^{18}.$$

So, as $a^2 = 1$,

$$b^{12} = a^{-2} b^{12} a^2 = a^{-1} b^{18} a = (a^{-1} b^2 a)^9 = b^{27}.$$

Hence $b^{15} = 1$. Also.

$$(a^{-1} b^2 a)^5 = a^{-1} b^{10} a = b^{15} = 1$$

which yields $b^{10} = 1$.

This, together with $b^{15} = 1$ implies $b^5 = 1$.]

23. Show that the groups $\boldsymbol{Z}$ and $\boldsymbol{R}$ can be embedded in the group A of exercise 9 (a) and the group T of exercise 9 (b) respectively. Can $\boldsymbol{R}$ be embedded in the group M given in exercise 9 (c) ? Justify your answer.

24. Let G be a cyclic group generated by a. Show that an element b of G is a generator of G if and only if there is a bijective homomorphism of G to G mapping a to b.

25. Let $(G, .)$, $(G', \times)$ and $(G'', +)$ be groups. Let

$$\varphi : G \to G', \varphi' : G' \to G''$$

be group homomorphisms. Show that $\varphi' \varphi : G \to G''$ is also a group homomorphism.

26. Let A and B be abelian groups under addition and Hom (A, B) denote the set of all homomorphisms of A to B. Define an algebraic operation $\oplus$ in Hom (A, B) as follows:

For $\varphi . \psi \in$ Hom (A, B) the 'sum' $\varphi \oplus \psi : A \to B$ is given by:

$$(\varphi \oplus \psi)(a) = \varphi(a) + \psi(a), a \in A.$$

Show that Hom (A, B) is a group under $\oplus$ with mapping $\underline{0}$, which sends each $a \in A$ into the zero of B, as the identity and $-\varphi$ given by:

$$(-\varphi)(a) = -\varphi(a), a \in A.$$

as the inverse of φ.

27. Let $\alpha : G \to G'$ be a surjective homomorphism. Define a relation R on G as follows:

For $x, y \in G$, $(x, y) \in R$ if and only if $\alpha(x y^{-1}) = e'$, the identity element in G'.

Show that R is an equivalence relation on G. Determine the factor set G/R.

[Hint: The G/R consists of all

$$aK, a \in G, K = \text{Ker}\, \alpha = \{x \in G : \alpha(x) = e'\}]$$

28. Describe the symmetry group of
    (i) a five pointed star.
    (ii) a non-circular ellipse.
    (iii) a regular tetrahedron.
    (iv) a cube.

29. Find the group of symmetries of an isosceles triangle. (It is of order 2).

30. There are only five regular solids: the tetrahedron, the octahedron, the dodecahedron and the icosahedron. Their groups of symmetries are a lot complicated. Try to find these.

31. Write the group of symmetries of a parallelogram which is regular and which is not rectangular.

Chapter - V

COMPLEXES IN GROUPS

Some results about subgroups of a group were proved in the preceding chapter. This chapter contains a discussion on complexes in groups, coset decomposition of a group, the order of a finite group and the orders of its subgroups. One of the most important theorems of the theory of finite groups namely the Largrange's theorem is proved here. This theorem gives a connection between order of a finite group and the orders of its subgroups. The relation of conjugacy between elements and between subgroups of a group is given in § 5.4. As shall be seen, this relation turns out to be an equivalence relation. The concepts of normaliser and centraliser of a subset and of conjugacy classes are also introduced.

5.1. COMPLEXES AND COSET DECOMPOSITION OF A GROUP

An arbitrary subset X of a group G is a called a *complex* in G. For two complexes X and Y in G we define their product as a complex XY given by:

$$XY = \{xy : x \in X, y \in Y\}$$

The complexes X and Y are said to be *permutable*, *i.e.*, $XY = YX$, if and only of, for any $x \in X$ and $y \in Y$, there exist $x' \in X$, $y' \in Y$ such that

$$xy = y'x'$$

Two arbitrary complexes in a group need not be permutable.

For instance the complexes $X = \{a, b\}$, $Y = \{a^2, ab\}$ of the group

$$< a, b : a^3 = b^2 = (ab)^2 = 1 >$$

are such that $XY \neq YX$.

Here $XY = \{a^3, a^2b, ba^2, bab\}$

$= \{1, a^2b, ab, a^2\}$

and $YX = \{a^3, a^2b, aba, ab^2\}$

$$= \{1, a^2b, b, a\}$$

so that $XY \neq YX$.

However, for any three complexes X, Y, Z of a group G, since $(xy)z = x(yz)$ for any $x \in X$, $y \in Y$, $z \in Z$, we have

$$(XY)Z = X(YZ).$$

Also, for a complex X in G, we define

$$X^{-1} = \{x^{-1} : x \in X\}$$

Then, for complexes X and Y, since $(xy)^{-1} = y^{-1}x^{-1}$ for all $x \in X$, $y \in Y$,

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

We now have the following restatement of theorem 4.2.2.

5.1.1. Theorem: A non-empty complex H of a group G is a subgroup of G if and only if $H H^{-1} \subseteq H$.

Proof: Suppose that H is a subgroup. Then

$$HH^{-1} = \{ab^{-1} : a, b \in H\} \subseteq H,$$

because of the closure law in H.

Conversely, if $HH^{-1} = \{ab^{-1} : a, b \in H\} \subseteq H$ then, trivially, for any $a, b \in H$, $ab^{-1} \in H$. So, by Theorem 4.2.2, H is a subgroup.

If the complexes H, K in a group G are subgroups of G then the product HK of H and K need not be a subgroup of G.

For example the complexes.

$$H = \{1, b\}, \text{ and } K = \{1, ab\}$$

are subgroups, each of order 2, of the group

$$< a, b : a^3 = b^2 = (ab)^2 = 1 >.$$

However

$$HK = \{1, b, ab, bab\} = \{1, b, ab, a^2\}$$

is not a subgroup of G. Here

$$a^2 . a^2 = a \notin HK.$$

The following theorem gives a necessary and sufficient condition for the product HK of the subgroups H and K to be a subgroup.

5.1.2. Theorem: Let, H, K be subgroups of a group G. The product HK of H and K is a subgroup of G if and only if H and K are permutable.

Proof: Let H and K be permutable. Then, for any $h \in H$ and $k \in K$, there exist $h' \in H$, $k' \in K$ such that

$$hk = k'h'.$$

To see that HK is a subgroup, let $x = hk$ and $y = h_1 k_1$ be in HK.

Then $xy^{-1} = hk.(h_1k_1)^{-1}$

$= hk\, k_1^{-1} h_1^{-1}$

$= h\, k_2\, h_1^{-1}$, $\quad kk_1^{-1} = k_2 \in K$ because K is a subgroup

$xy^{-1} = hh'\, k_2'$, $\quad \because HK = KH$

$= h_2'\, k_2'$, $\quad hh' = h'_2 \in H$ because H is a subgroup.

Hence $xy^{-1} \in HK$ and HK is a subgroup.

Conversely, suppose that HK is a subgroup. We show that HK = KH.

Let $hk \in HK$, $h \in H$, $k \in K$. Then $(hk)^{-1} \in HK$ because HK is a subgroup. However

$$(hk)^{-1} = k^{-1} h^{-1} = k'h',\ k', = k^{-1} \in K,\ h' = h^{-1} \in H,$$

is an element of KH. Hence for each $(hk)^{-1} \in HK$, $(hk)^{-1} \in KH$. Thus $HK \subseteq KH$, Also any $kh \in KH$, being the product of two elements ek and he of the subgroup HK, is in HK, so that $KH \subseteq HK$.

Combining the two inclusion relations we have

$$HK = KH$$

as required.

For the subgroup H, K of a group G, let $< H, K >$ (read as 'the group generated by H and K') denote the smallest subgroup of G that contains both H and K as subgroups. This subgroup, of course, contains the set HK but, in general, may be different from HK. In fact $< H, K > = HK$ if and only if H and K are permutable.

If K = H then $H \subseteq HH$ because any $h \in H$ can written as $h.e$. Also any hh' in HH, as a product of two elements h, h' of H, is an element of H, by virtue of H being a subgroup. Hence

$$HH = H$$

for any subgroup H. This fact will often be used in the sequel.

If $K = \{a\}$ for some $a \in G$, then

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

is called a right coset modulo H (or of H) determined by an element a of G and is denoted by Ha. As H contains the identity e, $ea = a \in Ha$.

The element ha of Ha is called a *representative element* of the coset Ha. The right coset of H determined by the identity e of G is H itself.

A right coset Ha is equal to H if and only if $a \in H$.

For if $a \in H$, then $Ha = \{ha: h \in H\}$ is just the collection of elements of H multiplied by an element of H and so must coincide with H, because of closure law.

Conversely, if $Ha = H$ then, for some $h \in H$, there is an $h' \in H$ such that

$$ha = h'.$$

But then $a = h^{-1} h' \in H$.

In the collection $\{Ha: a \in G\}$ of all right cosest of H in G, the set R consisting of the distinct elements a of G is called a *right transversal* of H.

We similarly define a *left transversal.*

The collection of all distinct right cosets of H is called a *right coset decomposition of G modulo H* (or relative to H). One can similarly define a *left coset decomposition of G* modulo H.

Let us define $(Ha)^{-1}$ by:

$$(Ha)^{-1} = \{(ha)^{-1} : h \in H\} = \{a^{-1} h^{-1} : h \in H\}$$

Then $(Ha)^{-1} = a^{-1} H$.

The mapping

$$Ha \to (Ha)^{-1} = a^{-1} H, a \in G,$$

which is a one-one correspondence between the collection of right and left cosets, shows that the right and left cosets of H in a group G are equal in number.

5.1.3. Examples:

(a) Let $G = <\varphi, \psi : \varphi^3 = \psi^2 = (\varphi\,\psi)^2 = 1>$. Then

$$H = <\varphi : \varphi^3 = 1>$$

is a subgroup of G. Its right cosets are H and H ψ. These are the only two distinct right cosets of H in G.

(b) In the dihedral group

$$D_4 = <a, b : a^4 = b^2 = (ab)^2 = 1>$$

of order 8, the left cosets of the subgroup $H = <a^2 : a^4 = 1>$, consisting of $1, a^2$ only, are:

$$1.H = H,\ aH,\ bH,\ abH.$$

Other cosets are equal to some one of these.

Here a left transversal L of H is given by:

$$L = \{1, a, b, ab\}.$$

(c) When the algebraic operation in a group G is termed as addition, then, for any $a \in G$, we write $a + H$ for the left coset of a subgroup H of a group G determined by an element a. Thus for the subgroup **E** of even integers in the group **Z** of integers, the left cosets are:

$$0 + \mathbf{E} = \mathbf{E},\ 1 + \mathbf{E}.$$

In general, for a fixed integer n, the set $\mathbf{Z} = \{0. \pm n, \pm 2n, ...\}$ of all multiples of n in **Z** is a subgroup of **Z**. If we put nZ = H, then the left coset decomposition of **Z** relative to H = n **Z** is

$$0 + H,\ 1 + H,\ ...,\ (n - 1) + H.$$

Here $n + H = \{0, \pm n, \pm 2n, ...,\} = H$.

(d) In the group Q of quaternions $\pm I, \pm i, \pm j, \pm k$, the left coset decomposition of Q relative to the subgroup $H = \{\pm 1, \pm i\}$ is

$$\{H, jH\}$$

Here, for example, the coset $kH = \{\pm k, \pm ki\}$ is equal to $jH = \{\pm j, \pm ji\}$.

5.2. LAGRANGE'S THEOREM

Let H be a subgroup of a group G. By the *index of* H in G, denoted by (G : H) and read as *the index of H in G,* we mean the number of distinct right (or left) cosets of H in G. If the number of right cosets of H in G is finite then H is called a *subgroup of finite index.* Otherwise H is said to have *infinite index* in G.

For instance, the subgroup H of example 5.1.3 (c) above has finite index in **Z**. Here H has only n distinct left (or right) cosets in G.

For a subgroup H in a group G, define a relation '$\equiv$' in G as follows:

For $x, y \in G$, we put

$x \equiv y \bmod H$

if and only if $xy^{-1} \in H$.

This relation is an equivalence relation because:

(a) as $xx^{-1} = e \in H$, $x \equiv x \bmod H$ for all $x \in G$ and '$\equiv$' is reflexive.

(b) if $x \equiv y \bmod H$, $y \equiv z \bmod H$, then $xy^{-1} \in H$, $yz^{-1} \in H$. Since H is a subgroup, $xy^{-1} \cdot yz^{-1} = xz^{-1} \in H$. Hence $x \equiv z \bmod H$ and '$\equiv$' is transitive.

(c) if $x \equiv y \bmod H$, then $xy^{-1} \in H$. Since H is a subgroup, $(xy^{-1})^{-1} = yx^{-1} \in H$. Thus $y \equiv x \bmod H$ and '$\equiv$' is symmetric.

The relation '$\equiv$' defined above is *called congruence relation in G modulo H.* Being an equivalence relation the congruence relation partitions G into equivalence classes. Since $xy^{-1} \in H$ implies $x \in Hy$ and, conversely, two elements $x, y \in G$ are in the same an equivalence class if and only if they are in the same right coset of H. There is, thus, a one-one correspondence between the equivalence classes determined by the congruence relation modulo H and the right cosets of H. But the number of right cosets of H is called the index of H. Thus the number of equivalence classes determined by the congruence modulo H is equal to the index of H in G.

It is easy to see that if C_x denotes an equivalence class determined by an element $x \in G$ under this congruence relation, then

$$C_x = \{y \in G : xy^{-1} \in H\}$$
$$= \{y \in G : xy^{-1} = h \text{ for some } h \in H\}$$
$$= \{y \in G : y = h^{-1}x \text{ for some } h \in H\}$$
$$= Hx$$

If G happens to be a finite group of order, say, n then the number r of equivalence classes determined by the above relation is finite. This 'r' is the index of H in G.

The equation $C_x = Hx$ shows that the number of elements in an equivalence class determined by an element $x \in G$ is equal to the number of elements in the right coset Hx. However this number is the same as the number of elements in the coset He determined by the identity element, because the one-one correspondence $h \to hx$, $h \in H$, between H and Hx.

Thus if H has order m, then each right coset Hx and hence each equivalence class contains exactly m elements. Now there are r equivalence classes each containing m elements. Hence the total number of elements in all the equivalence classes is m.r. Since these classes partition G and G contains n elements we have

$$n = m.\ r.$$

Hence the order m and index r of a subgroup H in a group G are divisors of the order n of G.

We therefore have the following theorem which is one of the basic and most important results in the theory of finite group and is named after the French mathematician Joseph L. Lagrange (1736 - 1813). Lagrange prove only a special case of this theorem. The general idea of a group did not emerge until the middle of nineteenth century. A second special case was proved by Cauchy. The general result was established by Jordan who attributed it to Lagrange and Cauchy.

5.2.1. Theorem: (Lagrange). The order and index of a subgroup of a finite group divide the order of that group.

In view of the significance of the above result, we give another proof of this theorem.

Proof: Let G be a group of order n and H a subgroup of order m in G. Let Ω be the collection of all right cosets of H in G. We first show that Ω is a partition of G.

Each element a of G belongs to a right coset Ha of H. Hence $G \subseteq \cup \Omega$. Also $\cup \Omega$, being the union of certain subsets of G, is contained in G. Hence

$$G = \cup \Omega. \qquad 5.2.1(1)$$

Moreover, if Ha, Hb are distinct right cosets of H, then

$Ha \cap Hb = \phi$.

For if $x \in Ha \cap Hb$, then

$$x = ha = h'b, \qquad h, h' \in H.$$

Hence

$$a = h^{-1} h' b = h'' b, \; h'' = h^{-1} h' \in H$$

so that $a \in Hb$. But then, for any element $y \in Ha$,

$$y = h_1 a = h_1 h'' b = h_2 b \in Hb$$

Hence $Ha \subseteq Hb$. By reasoning similarly, $Hb \subseteq Ha$. Consequently $Ha = Hb$, contradicting our supposition that Ha, Hb are distinct right cosets. Thus $Ha \cap Hb = \phi$. This proves that Ω is a partition of G.

As G has finite order namely n, Ω, which simply consists of the right cosets of H in G, is finite. Let r be the number of cosets in Ω.

Since every coset Ha of H contains exactly m elements, because of the one-one correspondence $h \rightarrow ha$, and there are r distinct right cosets, the number of elements in $\cup \Omega$, and therefore in G also, is r. m. But this must be equal to n by 5.2.1 (1). Hence

$$n = m. r.$$

So both m and r are divisors of the order n of G.

From the second proof of Lagrange's theorem we have:

5.2.1.(i). Corollary:

Two right (or left) cosets of a subgroup H in a group G are either identical or disjoint.

5.2.1.(ii). Corollary:

Every element of G belong to one and only one right (or left) coset of H.

A few other important consequences of the theorem of Lagrange are:

5.2.1.(iii). Corollary:

The order of an element of a finite group divides the order of the group. Also, if |G| denotes the order of G then $x^{|G|} = e$ for all $x \in G$.

Proof: The order of an element $a \in G$ is equal to the order of the cyclic group A generated by a and must therefore be a factor of the order of G, by Lagrange's theorem.

Also, if G has finite order n and $a \in G$ has order m then, as m divides n, n = m q for some integer q. Hence

$$a^n = a^{mq} = (a^m)^q = e^q = e.$$

So, if |G| denotes the order of a finite group G, then $x^{|G|} = e$ for all $x \in G$.

5.2.1.(iv). Corollary:

Every group whose order is a prime number is necessarily cyclic.

Proof: Let C be a group of order p where p is a prime and $a \neq e$ be an element of C. Then the order m of the cyclic group C′ generated by a is a factor of p. As $a \neq e$, m ≠ 1 and so m = p. Thus C′ coincides with C. Therefore C is cyclic.

5.2.1.(v). Corollary: (Fermat's Theorem).

Let a be any integer and p a prime number. Then

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

Proof: The non-zero integers

$$1, 2, ..., p - 1,$$

where p is a prime, form a group G of order p − 1 under the multiplication defined by:

$$a \,.\, b = r,\ 0 < r \leq p - 1,$$

where r is the remainder obtained after dividing the ordinary product $a \,.\, b$ by p. Hence the order of an element r in G divides the order of G so that

$$r^{p-1} \equiv 1 \bmod p.$$

Multiplying the above congruence relation by $r \in G$ we have:

$$r^p \equiv r \bmod p. \qquad 5.2.1 \text{ (i)}$$

Now let $a \in \mathbf{Z}$. If $a \neq np$, $n \in \mathbf{Z}$, then $a = kp + r$, $0 < r \leq p - 1$. So

$$a \equiv r \bmod p. \qquad 5.2.1 \text{ (ii)}$$

As

$$a^p = (r + kp)^p = r^p + xp, x \in Z,$$

we have

$$a^p \equiv r^p \bmod p. \qquad 5.2.1 \text{ (iii)}$$

But then, by using the symmetric and transitive properties of the congruence relation, we have, from equations 5.2.1 (i), 5.2.1 (ii) and 5.2.1 (iii),

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

as required.

For $a = np$, $n \in Z$, the equation $a^p \equiv a \bmod p$ is trivially satisfied.

5.2.1.(vi). Corollary (Eüler):

Let n be a natural number and φ (n) denote the number of integers less than n and prime to n. Then, for any integer a prime to n,

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Proof: The set of all natural numbers less than n and prime to n form a subgroup H of the group G of non-zero residues mod n. The order of this subgroup is naturally equal to φ (n). By Corollary 5.2.1.(iii),

$$a^{\varphi(n)} \equiv 1 \bmod n$$

for all $a \in$ G, as required.

Note: The function φ, which, for a natural number n, determines the number of integers less than n and prime to n, is called the Eüler's ϕ - function.

The theorem given below is the converse of Corollary 5.2.1.(iv).

5.2.1.(vii). Corollary: Let G be a non-cyclic group of order p^2 where p is a prime. Then each $e \neq a \in$ G satisfies the equation $a^p = e$.

Proof: Let $e \neq a \in$ G and m be the order of the cyclic subgroup C generated by a in G. Since G has order p^2, by Lagrange's theorem, m divides p^2. So m = 1, p or p^2. Since $a \neq e$, m ≠ 1. Now suppose that m = p^2. Then a and so also C has order p^2. Since C is a subgroup of G, C = G. Hence G is cyclic, a contradiction. So m ≠ p^2. So m = p. Thus, for each $e \neq a \in$ G,

$$a^p = e.$$

5.2.2. Theorem: Let H, K be subgroups of order m, n respectively of a group G and $(m, n) = 1$. Then the complex

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

has exactly mn elements.

Proof: Here the order r of $H \cap K$ divides the order m of H and order n of K. Since (m, n) = 1, r = 1. Hence $H \cap K = \{e\}$. Also, if, for some h, $h' \in H$, k, $k' \in K$, $hk = h'k'$ then $h^{-1} h' = k\, k'^{-1} \in H \cap K = \{e\}$. Hence $h^{-1} h' = e = k\, k'^{-1}$. That is

$$h = h', k = k'.$$

Thus the elements of HK are all distinct. Counting the possibilities for $h \in H$, $k \in K$. we see that the number of elements in HK is m n.

5.2.3. Theorem: If a group G has composite order then it has proper subgroups.

Proof: Suppose that the order n of a group G is a composite number *i.e.*,

$$n = pq \quad p, q \text{ integers}, p \neq 1, q \neq 1.$$

Then we have the following two cases:

(i) G is cyclic with an element a as its generator. The order of a is n.

Hence $a^p \neq 1$ and the cyclic group generated by a^p is a proper subgroup of G of order q.

(ii) G is not cyclic so that an irreducible system of generators for G contains at least two elements. Then again, the cyclic group generated by any one of these generators is a proper subgroup of G.

Hence, in both cases, G has a proper subgroup.

5.2.3.1. Corollary: If a nontrivial finite group G has only the trivial subgroups then its order is a prime number.

Proof: Here, for any $a \in G$, $a \neq e$, $< a >$ is a cyclic subgroup of G and is equal to G. So $< a >$ has no proper subgroup. Thus the order of a must be a prime by theorem 5.2.3.

For a subgroup H of a group G, let $G = \bigcup_{x \in G} xH$ be a left coset decomposition of G relative to H.

If $x' = xh$, $h \in H$ then the cosets xH and $x'H$ are the same. So we can assume that, in the decomposition of G, no cosets are written in the form H as well as xh H. That is, $xH = x'H \Rightarrow x = x'$.

The collection of all such left coset representatives in the decomposition of G is called a *left transversal* of H and is uniquely determined. We call such a transversal as the *reduced transversal* of H in G.

We now prove the following theorem:

5.2.4. Theorem: Let H and K be subgroups of a group G such that $K \subseteq H$. If

$$G = \bigcup_{x \in G} xH \text{ and } H = \bigcup_{y \in H} yK$$

are the left coset decompositions of G relative to H and of H relative to K then

$$G = \cup xyK \; ; x \in G, y \in H$$

is a left coset decomposition of G relative to K.

Moreover, if K has finite index in G then

$$(G : K) = (G : H)\,(H : K)$$

Proof: For subgroups H and K of G with $K \subseteq H$, let

$$G = \bigcup_{x \in G} xH, \quad H = \bigcup_{y \in H} yK$$

be left coset decomposition of G relative to H and of H relative to K with reduced transversals. By the remarks preceding the theorem, we can assume that the cosets representatives x of H and y of K are not of the form $x = x'h$, $y = y'k$ for $h \in H$ and $k \in K$. Consider now

$$\cup xy\,K \; ; x \in G, y \in H.$$

We show that this union defines a left coset decomposition of G relative to K. Obviously, for $x \in G$, $y \in G$,

$$\cup xy\,K \subseteq G.$$

Also, for any $g \in G$, $g \in x\,H$ for some $x \in G$. So

$$g = xh,\ h \in H.$$

Also $h = yk$, for some $k \in K$. Hence $g = xyk \in xy\,K$. Thus

$$G \subseteq \cup xy\,K\ ;\ x \in G, y \in H,$$

so that

$$G = \cup xy\,K\ ;\ x \in G, y \in H. \qquad 5.2.4\ (1)$$

is a left coset decomposition of G. Here the left cosets $xy\,H$, $x \in G$, $y \in H$ are all distinct. For if $g \in G$, then

$$g = xh,\ h \in H \text{ and } h = yk,\ k \in K$$

so that $g = xy\,k$.

Now, if $g \in xy\,K$ and $x'\,y'\,K$ both, then

$$g = xy\,k = x'\,y'\,k',\ k' \in K.$$

But

$$xy\,k\,H = xH = x'\,y'\,H = x'\,H \Rightarrow x = x'$$

and $$yk\,K = y'\,k'\,K \Rightarrow yk = y'\,k \Rightarrow y = y'$$

because the coset representives are taken as such. Hence

$$xy\,K = x'\,y'\,K.$$

If (G : K) is finite, then it follows, from 5.2.4 (1), that

$$(G : K) = (G : H)\,(H : K)$$

The following formula determines the number of elements in the product AB of two *finite* subgroups A and B of a group G.

5.2.5. Theorem: Let A and B be finite subgroups of a group G. Then

$$|AB| = \frac{|A|\,.\,|B|}{|A \cap B|}\,,\ |X| \text{ denotes the number of elements of X.}$$

Proof: Let $H = A \cap B$. Then H is a subgroup of both A and B. Consider the left coset decompositions

$$A = \bigcup_{i=1}^{m} a_i\,H \qquad 5.2.5\ (1)$$

$$B = \bigcup_{j=1}^{n} b_j H \qquad 5.2.5\ (2)$$

of A and B, with reduced transversals, respectively. Then

$$AB = \bigcup_{i=1}^{m} a_i HB \qquad 5.2.5\ (3)$$

Since $H \subseteq B$, $HB = \{hb : h \in H, b \in B\} = B$. Hence

$$AB = \bigcup_{i=1}^{m} a_i B = \cup a_i b_j H,\ 1 \le i \le m,\ 1 \le j \le n. \qquad 5.2.6\ (4)$$

Now the cosets $a_i H$, i = 1, 2, ..., m are all distinct and disjoint.

For let $x \in a_i B \cap a_j B$. Then

$$x = a_i b = a_j b',\ b, b' \in B$$

so that

$$a_j^{-1} a_i = b' b^{-1} \in A \cap B = H.$$

Thus $a_i \in a_j H$. But then $a_i H = a_j H$, a contradiction. Hence $a_i B \cap a_j B = \phi$.

Counting the number of elements on both sides of 5.2.5 (4) we find that, as

$$m = \frac{|A|}{|A \cap B|}, \qquad \text{by 5.2.5 (1)},$$

$$|AB| = mn = \frac{|A| \cdot |B|}{|A \cap B|}, \qquad \text{by 5.2.5 (2)}$$

as required.

For still another proof see Theorem 5.2.8.

5.2.6. Theorem: (Poincare's Theorem). Let H and K be subgroups of finite index in a group G. Then $H \cap K$ also has finite index in G.

Proof: Let

$$G = \bigcup_{i=1}^{m} x_i H$$

be a finite left coset decomposition of G relative to H. Then, for any subgroup K of G,

$$K = G \cap K = \bigcup_{i=1}^{m} (x_i H \cap K) \qquad 5.2.6(1)$$

where some of the sets on the right hand side of (1) may be empty and may be ignored.

Suppose $x_i H \cap K \neq \phi$. Then there is a $k \in K$ such that $x_i h = k$ for some $h \in H$. So

$$x_i h H = k H$$

That is $x_i H = kH$. Hence

$$x_i H \cap K = k H \cap K = k H \cap k K = k (H \cap K).$$

So every non-empty $x_i H \cap K$ in 5.2.6 (1) is a left coset of $H \cap K$ in K. Therefore

$$(K : H \cap K) \leq (G : H)$$

and

$$(G : K) (K : H \cap K) \leq (G : H) (G : K).$$

But

$$(G : K) (K : H \cap K) = (G : H \cap K).$$

Hence

$$(G : H \cap K) \leq (G : H) (G : K)$$

as required.

5.2.7. Theorem: Let G be a group and H, K be its subgroups of finite index. Then

$$(H : H \cap K) = (G : H)$$

if, and only if,

$G = HK = KH$.

Proof: We know, from Theorem 5.2.6, that, for subgroups H and K, of finite index in G, $H \cap K$ is of finite index in G. Also, from the proof of theorem 5.2.6,

$$(H : H \cap K) \leq (G : H)$$

Now if $(H : H \cap K) = (G : H)$

then none of the intersections $xH \cap K$ in 5.2.6 (1), Theorem 5.2.6, $x \in G$, is empty. Let $k \in x H \cap K$. Then $x H \cap K = k (H \cap K) \subseteq k H$. So $xh = kh'$ for some $h, h' \in H$.

Since $G = \bigcup_{x \in G} xH$, for each $g \in G$, $g = xh$ for some $h \in H$. So $g = xh = kh' \in KH$. Hence $G = KH$.

But then $G = KH = HK$, by Theorem 5.1.2.

Conversely suppose that $G = KH = HK$. Then, for every coset xH of H, $x = kh \in G$ for some $k \in K, h \in H$. So $xH = khH = kH$.

Hence all the cosets of H in G are given by the cosets of H determined by elements of K. So none of the intersections $xH \cap K$ in Theorem 5.2.6 is empty. Thus

$$(H : H \cap K) = (G : H).$$

5.2.8. Theorem: Let G_1 and G_2 be finite subgroups of a group G. Then

$$|G_1 G_2| = |G_1| \cdot |G_2| / |G_1 \cap G_2|$$

where $|G_i|$ denotes the number of elements in G_i.

We need the following lemma in the proof.

5.2.8.1. Lemma: Let A and B be sets and $\alpha : A \to B$ be a surjective mapping. Then α defines an equivalence relation $\sim$ on A given by:

$$a \sim a' \Leftrightarrow \alpha(a) = \alpha(a') \text{ for all } a, a' \in A.$$

The equivalence classes are the subsets

$$\overline{a} = \alpha^{-1}(a) = \{a' \in A : \alpha(a) = \alpha(a')\}, a \in A,$$

of A. The factor set $A / \sim$ and the set B are equivalent under the bijection $\overline{\alpha} : A/\sim \to B$ given by:

$$\overline{\alpha}(\overline{a}) = \alpha(a), a \in A.$$

Proof:

The relation $\sim$ on A given by

$$a \sim a' \Leftrightarrow \alpha(a) = \alpha,(a'), a, a' \in A,$$

is reflexive, symmetric and transitive. For any $a \in A$, the equivalence class $\overline{a}$ consists of all $a' \in A$ such th at $\alpha(a) = \alpha(a')$. Thus

$$\overline{a} = \{a' \in A : \alpha(a) = \alpha(a')\} = \alpha^{-1}(a)$$

The mapping $\overline{\alpha} : A/\sim \to B$ given by

$$\overline{\alpha}(\overline{a}) = b = \alpha(a),\ a \in A,\ b \in B$$

is a bijection. Here, for $a_1, a_2 \in A$,

$$\overline{\alpha}(\overline{a_1}) = \overline{\alpha}(\overline{a_2}) \Leftrightarrow \alpha(a_1) = \alpha(a_2)$$

$$\Leftrightarrow a_2 \in \overline{a_1} \text{ and } a_1 \in \overline{a_2}$$

$$\Leftrightarrow \overline{a_1} = \overline{a_2}$$

Proof of theorem:

Consider the surjective mapping $\varphi : G_1 \times G_2 \to G_1 G_2$ given by:

$$\varphi(g_1, g_2) = g_1 g_2,\ g_1 \in G_1, g_2 \in G_2.$$

Then φ defines an equivalence relation on $G_1 \times G_2$ given by:

$$(g_1, g_2) \sim (g_1', g_2') \Leftrightarrow g_1 g_2 = g_1' g_2'.$$

The factor set $(G_1 \times G_2) / \sim$ is equivalent to $G_1 G_2$. However, an equivalence class containing (g_1, g_2) in the factor set $(G_1 \times G_2) / \sim$ consists of the elements

$$(g_1 k, k^{-1} g_2),\ k \in G_1 \cap G_2.$$

Hence this equivalence class contains exactly $|G_1 \cap G_2|$ elements. Since $G_1 \times G_2$ consists of $|G_1| \times |G_2|$ elements, by the above lemma, $(G_1 \times G_2) / \sim$ consists of

$$\frac{|G_1| \cdot |G_2|}{|G_1 \cap G_2|}$$

elements. But this number is equal to the number of elements in $G_1 G_2$ which is $|G_1 G_2|$. Hence

$$|G_1 G_2| = \frac{|G_1| \cdot |G_2|}{|G_1 \cap G_2|}.$$

5.3. NORMALIZERS AND CENTRALIZERS

Let X be an arbitrary subset of a group G. The set of those elements of G which *permute with* X is called the *normalizer* of X in G and is denoted by $N_G(X)$, read as 'the normalizer of X in G'. Symbolically:

$$N_G(X) = \{a \in G : aX = Xa\}.$$

Since $eX = Xe$, at least the identity element e of G is in $N_G(X)$. So $N_G(X)$ is a non-empty subset of G. If $X = \{a\}$ then we speak of the Normalizer of a in G and denote it by $N_G(a)$. Since $a^k a = aa^k$ for any integer k, $N_G(a)$ contains, together with a, all powers of a.

5.3.1. Example:

Let $G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$, and $H = \{1, b\}$.

Then $aH = \{a, ab\}$, $Ha = \{a, ba\}$.

As $ab = ba^2 \neq ba$, $aH \neq Ha$ so that $a \notin N_G(H)$.

However $bH = \{b, b^2 = 1\} = Hb$. Hence $b \in N_G(H)$.

One can verify that

$$N_G(H) = H.$$

If $H = \{1, a, a^2\}$, then $N_G(H) = G$.

5.3.2. Theorem: Let $H \subseteq K$ be subgroups of a group G. If $Hk = kH$ for all $k \in K$, then $K \subseteq N_G(H)$.

Proof: Suppose that H, K with $H \subseteq K$ are subgroups of a group G and $Hk = kH$ for all $k \in K$. Then, by definition, for each $k \in K$, $k \in N^G(H)$.

5.3.3. Theorem: Let a group G contain elements a and b of order m and n respectively where $(m, n) = 1$ and $ab = ba$. Then G contains an element of order mn.

Proof: Let $H = \langle a : a^m = e \rangle$, $K = \langle b : b^n = e \rangle$. Since $(m, n) = 1$, $H \cap K = \{e\}$ by Lagrange's Theorem.

Now suppose that $ab = ba$ and $c = ab$. Then

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

Also if, for some integer k,

$$c^k = e$$

then $e = c^k = a^k b^k$

so that

$a^k = b^{-k} \in H \cap K = \{e\}$. Hence $a^k = e = b^k$. Thus m and n both divide k. That is $mn \mid k$. So c has order mn.

Let H be a subgroup of G. Since

$$hH = Hh$$

for all $h \in H$, $H \subseteq N_G(H)$. Thus the normalizer of a subgroup H of G contains H.

The following theorem show that the normalizer of a subset, and, in particular, of a subgroup in a group is a subgroup of that group.

5.3.4. Theorem: The normalizer $N_G(X)$ of a subset X of a group G is a subgroup of G.

Proof: Let $a, b \in N_G(X)$.

Then $aX = Xa$ and $bX = Xb$.

Now $bX = Xb$ implies

$$b^{-1} bXb^{-1} = b^{-1} Xbb^{-1} \text{ i.e., } Xb^{-1} = b^{-1} X,$$

so that $b^{-1} \in N_G(X)$. Hence

$$(ab^{-1}) X = a(b^{-1}X) = a(Xb^{-1}) = (aX)b^{-1} = X(ab^{-1}).$$

Therefore $ab^{-1} \in N_G(X)$. So $N_G(X)$ is a subgroup.

Now we come to the definition of the *centralizer.*

The centralizer of a subset X in a group G is the set of those elements of G which are permutable with *every* element of X. It is denoted by $C_G(X)$ (read as 'the centralizer of X in G'). Symbolically

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

The centralizer of a subset like its normalizer is non-empty. If X consists of a single element x then the normalizer of X and centralizer of X are identical. In general, however, the centralizer of X containing more than one element may be different from its normalizer.

5.3.5. Example:

Let G = $\langle a, b: a^4 = b^2 = (ab)^2 = 1\rangle$ be the dihedral group of order 8. Its elements are $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Also

$$(ab)^2 = 1 \Rightarrow ab = (ab)^{-1}$$
$$= b^{-1}a^{-1}$$
$$= ba^3, \text{ from } b^2 = 1, a^4 = 1.$$

Moreover

$$a^2b = a.\ ab = aba^3 = b.\ a^3.\ a^3 = ba^2.$$

Now let $X = \{1, a, a^2, a^3\}$. Then

$$bX = \{b, ba, ba^2, ba^3\} = Xb.$$

So $b \in N_G(X)$. Similarly $ab, a^2b, a^3b \in N_G(X)$. Hence

$$N_G(X) = G$$

But $C_G(X) = X \neq G = N_G(X)$.

However if $X = \{1, a^2\}$, then $C_G(X) = G = N_G(X)$

Like the normalizer of a subset we show that the centralizer of a subset is also a subgroup.

5.3.6. Theorem: The centralizer $C_G(X)$ of a subset X in a group G is a subgroup of G.

Proof: Let $a, b \in C_G(X)$. Then

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

for all $x \in X$. Hence

$$(ab^{-1})\,x = axb^{-1} = x\,(ab^{-1})$$

for all $x \in X$. Thus $ab^{-1} \in C_G(X)$ and it is a subgroup.

The centralizer as well as the normalizer of an element a, of course, contains that element and so also the cyclic subgroup generated by a. In fact, in this case, these basic concepts coincide. That is

$$C_G(a) = N_G(a)$$

However the centralizer of a subgroup need not contain that subgroup.

5.3.7. Example:

Consider the group

$G = < a, b, c : a^3 = b^2 = (ab)^2 = c^2 = (bc)^2 = 1, ac = ca >$. G is a group of order 12 and in it

$H = < a, b : a^3 = b^2 = (ab)^2 = 1 >$

is a subgroup and $bc = cb$. The centralizer of H in G is the subgroup

$K = < c : c^2 = 1 >$

because 1 and c are the only elements which are permutable with every element of H. Obviously $K = C_G(H)$ does not contain H.

For a group G, the centralizer of the whole group G is called the *centre* of G.

Thus the centre of G is the set of those elements of G which commute with *every* element of G. It is denoted by $\zeta(G)$. That is:

$$\zeta(G) = \{a \in G : ag = ga \text{ for all } g \in G\}.$$

If $\zeta(G) = \{e\}$, then G is called a *group without centre* or with *trivial centre.*

The centre of a group G is its subgroup.

It is, in fact, the abelian part of G. The centre of a group G coincides with G if and only if G is abelian.

5.3.8. Examples:

(i) In the group Q of all quaternions $\pm 1, \pm i, \pm j, \pm k$, the quaternions ± 1 form the centre of Q.

(ii) The group $S = < a, b : a^3 = b^2 = (ab)^2 = 1 >$ has trivial centre.

(iii) The centres of the groups $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ of integers, rationals, reals, and of complex numbers, under their usual addition, are the corresponding groups themselves.

(iv) The center of a subgroup of a group G may contain the centre of G as a subgroup

For if $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0, a, b, c, d \in R\right\}$, is the general linear group of degree 2,

$$\xi(G) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in R\}$$

consists of all scalar matrices. The set

$$H = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, ad \neq 0, a, d \in R\right\}$$ is a subgroup of G and is commutative. So then $\xi(G)$ is a (proper) subgroup of $\xi(H) = H$.

5.4. CONJUGACY RELATION IN GROUPS

Let G be a group. *For any* $a \in G$, the element gag^{-1} , $g \in G$ is called *the conjugate* or *transform* of a by g.

Two elements $a, b \in$ G are said to be *conjugate* if and only if there exists an element $g \in$ G such that

$$b = gag^{-1}.$$

Conjugate elements in a group are of the same order.

This follows from the equation $b^m = ga^m g^{-1}$ and $a = (g^{-1})\, b\, (g^{-1})^{-1}$, because then $a^m = e$ if and only if $b^m = e$

For $a, b, \in G$, the element $ab\, a^{-1}b^{-1}$ is called the *commutator of a, b* and is written as $[a, b]$.

Now we have:

5.4.1. Theorem: The relation of conjugacy between elements of a group is an equivalence relation.

Proof: Let us denote the relation of conjugacy between elements of a group by R. Then:

(i) R is reflexive *i.e.*, aRa because the identity element $e \in$ G and

$$eae^{-1} = a.$$

(ii) R is symmetric because if aRb for $a, b \in$ G, then there exists a $g \in$ G such that

$$b = gag^{-1},$$

but then

$$a = (g^{-1})\, b\, (g^{-1})^{-1}$$

so that $b\mathrm{R}a$.

(iii) R is transitive. For this, let $a\mathrm{R}b$ and $b\mathrm{R}c$. Then there exist $g, g' \in G$ such that

$$b = gag^{-1}, \qquad c = g' b g'^{-1}$$

Hence

$$c = g' b g'^{-1} = g' gag^{-1} g'^{-1} = (g' g) a (g' g)^{-1}$$

Thus $a\mathrm{R}c$.

Hence R is an equivalence relation in G.

In any group G, the relation of conjugacy between elements of G, being an equivalence relation, partitions G into equivalence classes. Each equivalence class consists of elements which are conjugate to one-another.

An equivalence class determined by the conjugacy relation between elements in G is called a *class of conjugate elements* or simply a *conjugacy class.*

A conjugacy class consisting of elements conjugate to an element a of G will be denoted by C_a.

In an abelian group, no two distinct elements are conjugate. Hence in this case there are as many conjugacy classes as the number of elements in that group.

In an arbitrary group G, a conjugacy class C_a consists of the element a alone if and only if a is permutable with every element of G, that is, if and only if $a \in \zeta(G)$.

Such elements are called *self-conjugate* (*invariant or central*).

The following theorem gives a relationship between the number of elements in a conjugacy class determined by an element and the index of the normalizer of that element.

5.4.2. Theorem: The number of elements in a conjugacy class C_a of an element a in a group G is equal to the index of its normalizer in G.

Thus $|C_a| = |G : N_a(x)|$.

Proof: Let Ω be the collection of right cosets of the normalizer $N_G(a) = N$ of $a \in G$. We have to show that the number of elements in Ω, being the index of N in G is equal to the number of elements in C_a.

Define a mapping, $\varphi : \Omega \to C_a$ as follows:

With each right coset Ng, $g \in G$, we associate the conjugate $g^{-1} a(g^{-1})^{-1} = g^{-1} ag \in C_a$ under φ *i.e.*, we put

$$\varphi (Ng) = g^{-1} ag. \qquad 5.4.2\ (1)$$

The mapping φ given by (1) is well defined because if $Ng = Ng'$ then $g' g^{-1} \in N$ *i.e.*, $g' = ng$ for some $n \in N$. Hence

$g'^{-1} ag' = (ng)^{-1} a (ng) = g^{-1} (n^{-1} an) g = g^{-1} ag$. That is $\varphi (Ng) = \varphi (Ng')$.

We show that φ is bijective : Firstly, φ is surjective because each $g^{-1} ag \in C_a$ is the image of a coset Ng. Secondly,

$$\varphi (Ng) = \varphi (Ng') \quad \Rightarrow \quad g^{-1} ag = g'^{-1} ag', \text{ that is}$$

$$\Rightarrow \quad g'g^{-1} agg'^{-1} = a.$$

Thus $g'g^{-1} \in N$, *i.e.*, $g' \in Ng$. But $g' \in Ng'$ also. Hence $Ng = Ng'$.

So φ is injective and therefore a bijective mapping. Consequently the sets Ω and C_a have the same number of elements. Therefore the number of element in C_a is equal to the index of the normalizer of a.

5.4.3. Corollary: Let G be a finite group and $a \in G$. Then the number of elements in the conjugacy class of a divides the order of G.

Proof: Since $N_G (a)$ is a subgroup of G, its order and index divide the order of G, by Larange's theorem. However the index of $N_G (a)$ is equal to the number of elements in C_a which therefore divides the order of G.

5.4.4. Corollary: The number of elements in a conjugacy class of an element in a group is finite if and only if the index of the normalizer of that element is finite.

Proof: This corollary follows directly from the above theorem.

It was shown in Theorem 5.4.1. that the relation of conjugacy between elements of a group G is an equivalence relation and partitions G into equivalence classes of conjugate elements. If G is a finite group of order n then the number r of conjugacy classes in G is also finite. Let

$$C_1, C_2, ..., C_r$$

be the conjugacy classes in G each containing

$$m_1, m_2, ..., m_r$$

elements respectively. Then, as $\bigcup_{i=1}^{r} C_i = G$, one has

$$n = m_1 + m_2 + \ldots + m_r \qquad (c)$$

where each m_i divides n, i = 1, 2, ..., r. The equation (c) is called *the class equation* of G and plays a very significant role in the theory of finite groups.

The positive integer r, in (c) above, is called the *class number* of G. The equation (c) can also be written as

$$|G| = \sum_{i=1}^{r} |G : C_G(a_i)|$$

when $C_G(a_i)$ is the centraliser of a_i, $i = 1, 2, \ldots, r$ in G.

Here $C_G(a_i) = N_G(a_i)$ and r is the number of conugacy classes in G.

One of the many uses of the class equation of a group is illustrated in the following theorem concerning finite p-groups *i.e.*, groups all of whose elements have orders powers of p for some fixed prime p. The order of a finite p-group is of the form p^m, for some positive integer m. There are also, of course, infinite p-groups, as we shall see later.

5.4.5. Theorem: The centre of a finite p-group is non-trivial.

Proof: Let P be a p-group of order p^m and

$$p^m = m_1 + \ldots + m_r \qquad 5.4.5\ (1)$$

be its class equation. Then each m_i divides p^m and hence must be of the form p^{α_i} ; $i \geq 1$. As the identity element e of P commutes with every element of P, the conjugacy class C_e consists of e alone. Thus there is at least one m_i, m_1 say, which is equal to 1. Also the conjugacy class of a self-conjugate element consists of only that element. Let there be k such classes. Without any loss of generality we can suppose that these are the first k classes so that, for these classes, $m_1 = m_2 = \ldots = m_k = 1$. Thus

$$p^m = k + p^{\alpha_{k+1}} + \ldots + p^{\alpha_r},$$

that is

$$k = m^p - (p^{\alpha_{k+1}} + \ldots + p^{\alpha_r}). \qquad 5.4.5\ (2)$$

The right hand side of 5.4.5 (2) is divisible by p. So should also be the left hand side. Thus k is a multiple of p. As $k \neq 0$ and is divisible by p, there

are more than one self-conjugate, that is, central elements in P. Hence P has a non-trivial centre.

Similar to the relation of conjugacy between elements of a group we have the *conjugacy relation between subgroups of* a group.

Let G be a group and H a subgroup of G. Then, for each $g \in G$, the set

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

is a *subgroup of G* because, for k_1, k_2 in K, where $k_1 = gh_1g^{-1}$, $k_2 = gh_2g^{-1}$, we have

$$\begin{aligned} k_1k_2^{-1} &= gh_1g^{-1} \cdot (gh_2g^{-1})^{-1} \\ &= gh_1g^{-1} \cdot gh_2^{-1}\, g^{-1} \\ &= gh_1h_2^{-1}\, g^{-1} \end{aligned}$$

Since H is a subgroup, $h_1h_2^{-1} \in H$ so that $k_1k_2^{-1} \in K$.

The subgroup K is called a *subgroup conjugate to H* determined by $g \in G$.

One can easily verify that the relation of conjugacy between subgroups of a group is an equivalence relation in G. This relation partitions G into conjugacy classes of subgroups.

A *conjugacy class of a subgroup* H is the collection of all subgroups of G which are conjugate to H.

Conjugate subgroups are connected by the following theorem.

5.4.6. Theorem: Any two conjugate subgroups of a group are isomorphic.

Proof: Let H and K be conjugate subgroups of a group G. Then, for some $g \in G$,

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

The mapping $\gamma : H \to K$ given by:

$$\gamma(h) = ghg^{-1} \in K,$$

is obviously bijective. That γ is a homomorphism, follows from the equation

$$\gamma(h_1 h_2) = gh_1h_2g^{-1} = gh_1g^{-1}\, gh_2g^{-1}$$
$$= \gamma(h_1) \cdot \gamma(h_2)$$

for all $h_1, h_2 \in$ H. Hence H and K are isomorphic.

5.4.7. Corollary: Two conjugate subgroups of a group have the same order.

One can workout the proof of the theorem given below on lines similar to those given in theorem 5.4.2.

5.4.8. Theorem: The number of conjugate subgroups of a subgroup H in a group G is equal to the index of the normalizer N_G (H).

5.4.9. Remarks:

1. If a finite group G has precisely two conjugacy classes then G has order 2.
2. If a group G contains an element a having exactly two conjugates, then G contains a normal subgroup $N \neq E$.

Groups with a finite number of conjugate classes of elements and of subgroups have been discussed by B.H. Neumann (cf. B.H. Neumann (1955). Math. Z. pp. 76-96).

5.5. DOUBLE COSETS

The concept of double cosets in a group is a generalization of that of cosets. This notion is helpful in proving some very important results in the theory of finite groups.

Let H, K be subgroups of a group G and a an arbitrary element of G. Then the set HaK consisting of elements of the form hak, $h \in$ H, $k \in$ K is called a *double coset* in G modulo (H, K) determined by a.

Just as the left (or right) cosets of a subgroup in a group determine its partition, similarly the collection Ω of double cosets in a group is a partition of that group. This is shown in the following theorem.

5.5.1 Theorem: Let H, K be subgroups of a group G. Then the collection Ω of all the double cosets HaK, $a \in$ G is a partition of G.

Proof: To see that the collection of all double cosets in G modulo (H, K) is a partition, we have to prove that:

(i) G = $\cup\, \Omega$, where $\cup\, \Omega$, is the union of double cosets HaK, $a \in$ G and

(ii) any two distinct double cosets are disjoint.

It is obvious that $\cup\, \Omega$, being the union of certain subsets of G, is contained in G.

Conversely each $a \in$ G is in a double coset namely the double coset HaK because a is expressible as $a = e.\, a.\, e$. Hence G $\subseteq \cup\, \Omega$.

Consequently,

$$G = \cup\, \Omega$$

and we have (i).

For (ii) let HaK, HbK be distinct double cosets in G and suppose that $x \in$ HaK $\cap$ HbK. Then

$$x = hak = h'\, bk',\ h, h' \in H,\ k, k' \in K.$$

But this equation gives

$$a = h^{-1}\, h'\, bk'\, k^{-1}$$
$$= h''\, bk''$$

where $h'' = h^{-1}\, h' \in$ H and $k'' = k'\, k^{-1} \in$ K. Now let y be an arbitrary element of HaK. Then

$$y = h_1\, ak_1 = h_1 h''\, bk''\, k_1,\ h_1 h'' \in H,\ k''\, k_1 \in K$$

is in HaK so that

$$HaK \subseteq Hbk.$$

Likewise

$$HbK \subseteq HaK,$$

Combining the two inequalities given above we have

$$HaK = HbK,$$

contradiction. Hence HaK and HbK are disjoint and we have (ii) Therefore the double cosets of G modulo (H, K) define a partition of G.

All the right cosets of H of the form Hak, $k \in$ K are contained in the double coset HaK. Similarly all the left cosets of K of the form haK, $h \in$ H are contained in HaK. We now investigate the number of elements in a double coset HaK where H and K are finite subgroups of a group. For this, however, we need the following result which is the same as Theorem 5.2.8 but with a different proof

5.5.1. Lemma: Let A, B be finite subgroups of a group G. Then the complex AB contains exactly mn/q elements where m, n and q are respectively the orders of A, B and the intersection Q = A $\cap$ B.

Proof: Since Q is the intersection of the subgroups A and B of a group G, it is a subgroup of both A and B. Also, as A and B are finite groups, the order q of Q and its index r = n/q in B is finite. Let

$$B = \bigcup_{i=1}^{r} Qb_i ; \qquad 5.5.1\ (1)$$

be a right coset decomposition of B. Then only one of the b_i's say $b_1 = e$ and $b_i \notin$ Q for any i > 1 so that the coset Qb_i is not equal to Q. Also

$$AB = \bigcup_{i=1}^{r} AQb_i. \qquad 5.5.1\ (2)$$

Since Q is a subgroup of A the coset Ax is equal to A for all $x \in$ Q. Hence

$$AQ = \{Ax ; x \in Q\} = A.$$

As a consequence we have

$$AB = \bigcup_{i=1}^{r} Ab_i. \qquad 5.5.1\ (3)$$

As $b_i \in$ B and $b_i \notin$ Q, $b_i \notin$ A for i > 1, the cosets Ab_i, i = 1, 2, ...r, are all distinct. Each of these cosets contains exactly m elements and there are r such cosets. Hence the total number of elements in $\bigcup_{i=1}^{r} Ab_i$ is m.r = m.n/q. But this is the number of elements in AB, by 5.5.1 (2).

Hence the lemma.

We are now in a position to prove:

5.5.2. Theorem: Let H, K be finite subgroups of a group G. Then each double coset HaK contains mn/q elements where m, n and q are the orders of the subgroups H, K and Q = H $\cap$ aKa^{-1} respectively.

Proof: Since H, K are finite subgroups of G, the double coset HaK consists of only a finite number of elements of G. Let

$$x_1, x_2, \ldots, x_r$$

be all the elements of HaK.

Then

$$HaK = \bigcup_{i=1}^{r} \{x_i\}$$

and

$$\text{v} \qquad HaKa^{-1} = \bigcup_{i=1}^{r} \{x_i a^{-1}\}$$

where, of course, the elements $x_i a^{-1}$, i = 1, 2, ..., r are all distinct, for otherwise $x_i a^{-1} = x_j a^{-1}$, $i \neq j$ would imply $x_i = x_j$. Put $aKa^{-1} = K'$. Then K', being a subgroup conjugate to K, also has order n. Now, since $HaKa^{-1} = HK'$, the number of elements in HK', by lemma 5.5.1, is mn/q where q is the order of

$$Q = H \cap K' = H \cap aKa^{-1}.$$

Hence the theorem.

5.5.3. Theorem: Let a group G of order n have subgroups H, K of order l and m respectively. Then

$$n = \frac{lm}{q_1} + \frac{lm}{q_2} + \ldots + \frac{lm}{q_r}$$

where q_i is the order of $Q_i = H \cap a_i K a_i^{-1}$ i = 1, 2, ..., r.

Proof: Since the collection Ω of the double cosets HaK, $a \in G$, is a decomposition of G,

$$G = \cup \Omega,$$

where $\cup \Omega$ is the union of all the double cosets Ha_iK in G, i = 1, 2, ..., r.

Now each double coset, say, Ha_iK contains $\frac{lm}{q_i}$ elements, l, m and q_i respectively being the orders of H, K and the intersection $Q_i = H \cap a_i K a_i^{-1}$. As there are r such double cosets, the order n of G satisfies the equation

$$n = \frac{lm}{q_1} + \frac{lm}{q_2} + \ldots + \frac{lm}{q_r}.$$

5.5.4. Theorem: Let HaK be a double coset modulo the subgroups H, K of a group G and Q = H $\cap$ aKa^{-1}. Then there is a one-one correspondence between the left cosets of K that are contained in HaK and the left cosets of the intersection Q of H and aKa^{-1} in H.

Proof: Let Ω be the collection of the left cosets haK of K that are contained in HaK and Ω' the collection of all the left cosets of the intersection Q = H $\cap$ aKa^{-1} in H.

Define a mapping $\psi : \Omega \to \Omega'$ as follows:

With each haK $\in$ Ω we associate the left coset hQ of Q in H, that is, we put

$$\psi(haK) = hQ. \qquad 5.5.4\ (i)$$

Then ψ is well defined, for if $haK = h'aK$, there exist elements $k, k' \in K$ such that

$$hak = h'\,ak'$$

Hence

$$h'^{-1}\,h = ak'\,k^{-1}\,a^{-1}$$

is in H $\cap$ aKa^{-1} = Q so that $h \in h'Q$. As $h \in hQ$ as well, we have $hQ = h'Q$.

Also if

$$\psi(haK) = \psi(h'aK)$$

i.e.,

$$hQ = h'Q$$

then $h'^{-1}\,h \in Q$. Thus there exists a $k \in K$ such that $h'^{-1}h = aka^{-1}$ *i.e.*,

$$ha = h'ak.$$

so that $ha \in h'aK$. But $ha = hae \in haK$. Hence haK and $h'aK$ are not disjoint. Thus,

$$haK = h'aK.$$

Therefore ψ is injective. Since ψ is obviously surjective, it is a one-one correspondence between Ω and Ω'.

Hence the theorem.

The following corollary is now a straight forward consequence of Theorem 5.5.4.

5.5.5. Corollary: If the index of $Q = H \cap aKa^{-1}$ in H is finite, then the number of left cosets of K that are contained in the double coset HaK is also finite and conversely. Moreover these numbers are equal.

A subset H of a group G is called *normal* if $xH = Hx$ for all elements x of G.

While answering a question of I.D. Macdonald in Mathematical Gazette (Volume 62 (1978) p. 29 - 35) about certain subset H of a group G satisfying $xH = HxH$ for all x in G, B.H. Neumann (Math. Gaz. 62(1978)p. 298 - 299) proved the following theorem.

5.5.6. Theorem: Let H be a non-empty subset of a group G such that $xH = HxH$ for all x in G. Then H is normal in G.

Proof: For $x, y \in G$ we write $y^x = xyx^{-1}$ and similarly $H^x = xHx^{-1}$. Now suppose that

$$xH = HxH \qquad 5.5.6\ (1)$$

for all $x \in G$. Multiplying both sides of (1) by x^{-1} on the right, we obtain,

$$H^x = HH^x \qquad 5.5.6\ (2)$$

Since x, and so also x^{-1}, range over the whole of G, we can replace x^{-1} by x in the above equation and obtain

$$H = H^xH. \qquad 5.5.6\ (3)$$

From 5.5.6 (2) we see that an arbitrary element of H^x can be written as zy^x; $y, z \in H$. But

$$zy^x = zxyx^{-1}z^{-1}z = y^{zx}z$$

which is an element of $H^{zx}H$, and Thus by 5.5.6 (3), with zx replaced for x, is an element of H. It follows that H^x is a subset of H. But $H^x \subseteq H$ is equivalent to $H \subseteq x^{-1}Hx$. Again, since x ranges over the whole of G, so does x^{-1} and replacing x^{-1} by x we have, $H \subseteq H^x$.

Thus $H^x = H$ and the theorem follows.

EXERCISES

1. Let G be a finite group and x an arbitrary element of G. Show that there exists an integer n such that $x^n = e$.

   If G is an arbitrary group and there exists an integer n such that $x^n = e$ for some $x \in G$, show that there is an integer m such that $x^{-1} = x^m$.

2. In the group having the presentation

   $$G = < a, b : a^6 = b^2 = (ab)^2 = 1 >,$$

   show that

   $$a^i b^j,\ 0 \le i \le 5,\ 0 \le j \le 1$$

   are all the distinct elements of G. Hence show that the order of G is 12.

3. Show that every group of order ≤ 5 is abelian

4. Find the number of generators of a cyclic group whose order is
   (i) a prime number, (ii) 12.

5. Let A and B be cyclic groups of order n. Show that the set Hom (A, B) of all homomorphisms from A to B is a cyclic group.

6. Show that if $a, b \in G$ are conjugate then $b = ca$ for some commutator c in G.

7. Let A be an additive abelian group of exponent n, that is

   $$na = 0$$

   for all $a \in A$. Let n = pq; where p, q are relatively prime and put

   $$A_p = \{x \in A : px = 0\}$$

   $$A_q = \{y \in A : qy = 0\}.$$

   Show that A_p and A_q are subgroups and have no common element except 0.

8. Let H be a subgroup of a group G. For $a, b \in G$, let $a \equiv b \bmod H$ if and only if $ab^{-1} \in H$. Show that

$$a \equiv b \bmod H \text{ implies } ag \equiv bg \bmod H.$$

for all $g \in G$. Is

$$ga \equiv gb \bmod H$$

for all $g \in G$? Justify.

9. Let a be an element of order n in a group. Show that

$$a^k = a^l$$

if and only if

$$k \equiv l \bmod n.$$

10. **In a group G, let G^n denote the set of nth powers of all the elements of G. Verify that, in each of the following groups, G^2 is a subgroup.**

(i) $G = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$ of order 8 (Dihedral group).

(ii) $G = \langle a, b : a^4 = 1, a^2 = b^2 = (ab)^2 \rangle$ of order 8 (Quaternion group).

(iii) $G = \langle a, b : a^4 = b^2 = 1, ab = ba \rangle$ of order 8 (Abelian).

11. Let H and K be subgroups of a group G. For $g_1, g_2 \in G$ let $Hg_1 = Kg_2$. Show that $H = K$.

[Hint : $Hg_1 = Kg_2$. $\Rightarrow$ for each $h \in H$, there is a $k \in K$ such that $hg_1 = kg_2$. Let $h_1 \in H$. Then $h_1kg_2 = h_1hg_1 = h'g_1 = k'g_2$. So $h_1 = k'k^{-1} \in K$, ...].

12. Let G be a group and $a \in G$. Let $C_G(a)$ be the centraliser of a in G. Then show that, for any $g \in G$,

$$gC_G(a)\, g^{-1} = C_G(gag^{-1}).$$

Also, for any subgroup H and an element g of G

$gN_G(H)g^{-1} = N_G(gHg^{-1})$.

13. Let Q be the group of quaternions $\pm I, \pm i, \pm j, \pm k$ and $H = \{\pm I, \pm i\}$.

a subgroup of Q. Find the subgroups of Q (if any) conjugate to H.

14. Let G, G′ be groups and $\varphi = G \to G'$ be a homomorphism. Show that

(i) if $\varphi(G)$ has n elements then $x^n \in \text{Ker}\,\varphi$ for all $x \in G$.

(ii) if, for a natural number m, $(m, |\varphi(G)|) = 1$, then

$x^m \in \text{Ker}\,\varphi \Rightarrow x \in \text{Ker}\,\varphi$.

(iii) if $a \in G$ has order n and $(n, m) = 1$, $m = |\varphi(G)|$, then $a \in \text{Ker}\,\varphi$

15. **Find all the subgroups of:**

(i) $G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$

conjugate to

$H = \langle b : b^2 = 1 \rangle$

(ii) $G = \langle a, b : a^3 = b^2 = c^2 = (bc)^2 = 1, ab = ca, ac = bca \rangle$

conjugate to

$H = \langle a : a^3 = 1 \rangle$.

16. Find the subgroup lattice of the dihedral group

$D_4 = \{a, b : a^4 = b^2 = (ab)^2 = 1\}$

17. Let H be finite subgroup of order k in a group G. For an element g of G with $gH = Hg$, let m be the least positive integer such that $g^m \in H$. Show that

(a) g has finite order.

(b) m divides the order of g.

(c) the order of $\langle H, g \rangle$ is mk.

[Hint: (c) If n is the order of g, then $g^n = e$ Suppose that m does not divide n. If r denote the greatest common divisor of m, n then there exist integers p, q such that

$r = pm + qn$, $0 < r < m$ so that $g^r = (g^m)^k \in H$, (a contradiction)].

[Hint: (c) Since $gH = Hg$, every element of the group $< H, g >$ is of the form $g^i h$, $h \in H$ for some integer i. As $g^m \in H$, every element of the group is in one and only one of the left cosets.

$eH, gH, ..., g^{m-1}H$

and conversely each of these cosets is a subset of $< H, g >$.

Hence

$$< H, g > = \bigcup_{i=0}^{m-1} g^i H.]$$

18. If H, K are subgroups of a group G such that $H \cap K = \{e\}$ and if

$$hKh^{-1} = K, \; kHk^{-1} = H \text{ for all } h \in H, k \in K,$$

show that H and K commute elementwise.

Chapter - VI

NORMAL SUBGROUPS, FACTOR GROUPS

In group theory we usually have to examine the structure of a group, its subgroups and its relationship with other groups. Among the subgroups of a group there is a special class namely the class of '*normal*' subgroups of a group.

E. Galois was the first famous mathematician who directed his attention to the study of normal subgroups and their important properties. Normal subgroups play a key role in the theory of groups. One of the main and fundamental properties of normal subgroups is that they give rise to quotient groups. Groups which have no proper normal subgroups are known as simple groups. Finite simple groups have now been all classified. All finite simple groups are now known and their determination was completed in 1980's. This classification is one of the greatest achievements in mathematics.

The classification of finite simple groups has two aspects. One is the listing of all such groups and the other is the verification that every finite simple group is included in the list.

Apart from certain infinite families of finite simple groups relating to permutations and matrices there are 26 *sporadic simple groups* including the largest and the one found last of all. This is called the *Monster* (or the *friendly giant*). This is a group of order

$$2^{46} \times 3^{20} \times 5^{9} \times 7^{6} \times 11^{2} \times 13^{3} \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$$

It is estimated that more than 200 mathematicians have contributed to this classification. Not much is known about infinite simple groups although a few classes of infinite simple groups have been found by Ruth Camn, P. Hall etc.

Normal subgroups are closely related to homomorphisms of groups. In fact there is a one-one correspondence between the class of all normal subgroups of a group and the possible homorphisms which this

group can have. A brief account of these concepts is given in the following paragraphs.

6.1. NORMAL SUBGROUPS

Let H be a subgroup of G. H is said to be a *normal (self-conjugate or invariant)* subgroup of G if it coincides with all its conjugate subgroups in G.

Thus H is normal in G if and only if

$$gHg^{-1} = H \text{ for all } g \in G$$

The relation of 'being a normal subgroup' is not a transitive relation. Thus if H is a normal subgroup of a group K and K is a normal subgroup of G then H may not be a normal subgroup of G (see example 6.1.1 (b) below).

Every group G has at least two normal subgroups namely the identity subgroup $E = \{e\}$ and the group G itself. Normal subgroup of G which are different from these two are called *proper* normal subgroups. Groups having no proper normal subgroups are called *simple*.

All the subgroups of an abelian group are normal. However there are non-abelian groups all of whose subgroups are normal. Such groups are called *Hamiltonian* groups.

6.1.1. Examples:

(a) The subgroup $H = < \varphi : \varphi^3 = e >$ is a normal subgroup of the group

$$G = < \varphi, \psi : \varphi^3 = \psi^2 = (\varphi\psi)^2 = e >.$$

(b) Let

$$G = < a, b, c : a^3 = b^2 = c^2 = (bc)^2 = 1, ab = ca, ac = bca >.$$

The subgroup

$$K = < b, c : b^2 = c^2 = (bc)^2 = 1 >$$

is normal in G. Also the subgroup $H = < b : b^2 = 1 >$ is normal in K. However H is not a normal subgroup of G because

$$aHa^{-1} = \{1, aba^{-1} = c\} \neq H.$$

(c) The group Q of quaternions $\pm$ I, $\pm$ i, $\pm$ j, $\pm$ k is such that it is non-abelian but every subgroup of Q is normal in Q. (why?).

(d) The centre of any group is a normal subgroup. For if ζ (G) denotes the centre of G then

$$g\ \zeta\ (G)\ g^{-1} = \{gzg^{-1} = z : z \in \zeta\ (G)\} = \zeta\ (G)$$

for all $g \in G$.

(e) A cyclic group C whose order is a prime number is simple.

In this case C, by Lagrange's theorem, has no proper subgroups and therefore no proper normal subgroups. The class of cyclic groups of prime order is the only class of abelian simple groups.

To check that a subgroup H of a group G is normal in G it is enough to verify that $gHg^{-1} \subseteq H$ for *all* $g \in G$.

For if $gHg^{-1} \subseteq H$ for all $g \in G$ then

$H = g^{-1}gHg^{-1}g \subseteq g^{-1}Hg$ by multiplying left and right by g^{-1} and g respectively)

So.

$$H \subseteq g^{-1} H g$$

for all g $\in$ G. Replacing g^{-1} by g again, we have H $\subseteq gHg^{-1}$. So

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

However a subgroup H of a group G may be such that, for a $g \in G$, $gHg^{-1} \subseteq$ H but H may not be normal in G. The following counter example, in this case, given by I. N. Herstein [27] substantiates this claim.

Example. Let

$$G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0,\ a, b, c, d \in Q\right\}$$

and

$$H = \left\{\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, k \in \mathbf{Z}\right\}.$$

It is possible that, for $a\ g \in G$,

$$gHg^{-1} \subset H$$

but

$$g\,Hg^{-1} \neq H, \text{ for some other } g \in G$$

For example, if

$$g = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Then

$$g\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & 3k \\ 0 & 1 \end{pmatrix} \in H$$

so that

$$< g\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g^{-1} > = g\,Hg^{-1} \subset H$$

But, for $g = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \in G$,

$$g\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g{-}1 = \begin{pmatrix} 1-3k & k \\ -9k & 1+3k \end{pmatrix} \notin H$$

So

$$gHg^{-1} \neq H$$

6.1.2. Theorem: The following statements about a subgroup H of a group G are equivalent.

(a) H is a normal subgroup of G.

(b) The normaliser of H in G is the whole of G i.e. $N_G(H) = G$.

(c) Any left coset gH of H is equal to its right coset Hg for all $g \in G$, i.e. $gH = Hg$ for all $g \in G$.

(d) For each $h \in H$ and any $g \in G$, $ghg^{-1} \in H$; that is, H contains the whole class of conjugates of each of its elements.

Proof: We show that (a) implies (b), (b) implies (c), (c) implies (d) and (d) in turn implies (a).

(a) implies (b). Assume that (a) holds, that is, H is a normal subgroup of G. Then

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

for all $g \in G$. Hence $gH = Hg$ for all $g \in G$ so that every $g \in G$ is in the normaliser $N_G(H)$. Therefore $G \subset N_G(H)$. But $N_G(H) \subseteq G$ and (b) is true.

(b) implies (c). Suppose that (b) holds, that is $N_G(H) = \{g \in G: gH = Hg\} = G$. Then $gH = Hg$ for all $g \in G$. Thus (c) holds.

(c) implies (d). Suppose that (c) holds, that is, $gH = Hg$ for all $g \in G$. Then, given any $h \in H$, there exists an $h' \in H$ such that $gh = h'g$ for all $g \in G$. Hence $ghg^{-1} = h' \in H$. Thus G contains, together with $h \in H$, all its conjugates namely the elements ghg^{-1}, $g \in G$. Therefore (d) is true.

(d) implies (a). Suppose that (d) is true. Then, for each $h \in H$ and any $g \in G$, $ghg^{-1} = h' \in H$.

Hence $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H$ for all $g \in G$. Also for any $h \in H$,

$$h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$$

because $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$.

Thus $H \subseteq gHg^{-1}$. Therefore $gHg^{-1} = H$.

for all $g \in G$. Hence H is a normal subgroup and we have (a).

From the above theorem it follows that each one of the statement (b), (c) and (d) also can be taken as a definition of a normal subgroup.

6.1.3. Thereon: The intersection of any collection of normal subgroups of a group is a normal subgroup.

Proof: Let Ω, be a collection of normal subgroups in a group G and $D = \cap\Omega$ the intersection of the members of Ω. Then D is a subgroup as proved in Theorem 4.2.3. To see that D is normal in G, let $d \in D$. Then $d \in H$ for each $H \in \Omega$. Therefore $gdg^{-1} \in \cap\,\Omega = D$ for all $g \in G$. Hence D is a normal subgroup.

In cases where a group and a subgroup of it are given in terms of generators and relations it is often convenient to make use of the following theorem to show that the given subgroup is normal.

6.1.4. Theorem: A subgroup H of a group G is normal in G if and only if every generator of G transforms each generator of H into an element of H.

Proof: Let H be a normal subgroup of G. Then every element of H and, in particular, a generator of H is transformed into an element of H by each element of G especially a generator of G.

Conversely, let G be a group generated by g_α, $\alpha \in I$, and H a subgroup of G generated by h_β, $\beta \in I'$. Let the generators of G transform each generator of H into an element of H. Then every $g \in G$ and $h \in H$ are of the form.

$$g = g_{\alpha_1}^{\epsilon_1} g_{\alpha_2}^{\epsilon_2} \ldots g_{\alpha_k}^{\epsilon_k} \quad (\epsilon_i = \pm 1, 1 \le i \le k)$$

$$h = h_{\beta_1}^{\delta_1} h_{\beta_2}^{\delta_2} \ldots h_{\beta_l}^{\delta_l} \quad (\delta_j = \pm 1, 1 \le j \le \ell)$$

As

$$x(y_1 y_2)x^{-1} = (xy_1 x^{-1}) \cdot (xy_2 x^{-1}), (xy_1^{-1} x^{-1}) = (xy_1 x^{-1})^{-1} \in H,$$

we have ghg^{-1} as an element of H. Hence H is a normal subgroup.

6.1.5. Theorem: A subgroup of index 2 in a group G is normal.

Proof: Let H be a subgroup of index 2 in G. Then G has the following left and right cost decompositions relative to H.

$$\{H, gH\} = G = \{H, Hg\}, g \in G \setminus H.$$

So $gH = Hg$ for all $g \in G \setminus H$. However if $g \in H$ then obviously

$$gH = Hg.$$

Hence H is normal in G.

6.1.6. Theorem: Let a be an element of order 2 in a group G. Then

$$H = \langle a : a^2 = 1 \rangle$$

is normal in G if and only if $a \in \zeta(G)$.

Proof: Here, for any $g \in G$,

$$H \text{ is normal in } G \Leftrightarrow gH = Hg$$

$$\Leftrightarrow g\{e, a\} = \{e, a\}g$$

$$\Leftrightarrow \{g, ga\} = \{g, ag\}$$

$$\Leftrightarrow ag = ga$$

So $a \in \zeta(G)$.

6.1.7. Theorem: Let A be a normal subgroup and B a subgroup of a group G. Then

$$< A, B > = AB.$$

Proof: Each element of $< A, B >$ is of the form

$$a_1^{\epsilon} b_1 a_2 b_2 \ldots a_k b_k^{\delta}, \qquad 6.1.7\ (1)$$

$a_i \in A$, $b_i \in B$, $\epsilon, \delta = 0$ or 1. Since A is normal in G

$$ga = a'g$$

for $g \in G$ and $a, a' \in A$. In particular

$$ba = a'b$$

for all $b \in B$. Applying repeatedly the above equation to 6.1.7 (1), we have

$$a_1^{\epsilon} b_1 a_2 b_2 \ldots a_k b_k^{\delta} = a_1^{\epsilon} a'_2 \ldots a'_k b_1 b_2 \ldots b_k^{\delta}$$

$$= ab \in AB,$$

$a \in A$, $b \in B$. Hence $< A, B > \subseteq AB$. But, obviously, $AB \subseteq < A, B >$.

Hence

$$< A, B > = AB.$$

6.1.8. Corollary: Let H, K be normal subgroups of a group G. Then HK is a normal subgroup of G.

Proof: By theorem 6.1.7, HK is a subgroup of G. Also, for any $h \in H$, $k \in K$ and $g \in G$,

$$ghkg^{-1} = ghg^{-1}\, gkg^{-1} = h'k' \in HK,$$

where $h' = ghg^{-1} \in H$, $k' = gkg^{-1} \in K$, because both H and K are normal in G. Hence HK is normal in G.

6.1.9. Theorem: Let H be a subgroup of a group G. Then H is a normal subgroup of $N_G(H)$.

Proof: By definition,

$$N_G(H) = \{g \in G : gH = Hg\}$$

and is a subgroup. Since $hH = H = Hh$, $H \subseteq N_G(H)$. Also for each

$x \in N_G(H)$, $xH = Hx$. Hence H is a normal subgroup $N_G(H)$.

6.1.10. Theorem: The centraliser $C_G(H)$ of a normal subgroup H of G is normal in G.

Proof: Here

$$C_G(H) = \{ x \in G : hx = xh \text{ for all } h \in H\}.$$

Since H is normal in G, for each $h \in H$, $g \in G$, there is an $h' \in H$ such that

$$hg = gh' \text{ i.e. } g^{-1} h = h'g^{-1}.$$

So, for each $x \in C_G(H)$ and $g \in G$,

$$h(gxg^{-1}) = (hg)xg^{-1} = gh'xg^{-1} = gxh'g^{-1} = (gxg^{-1})h$$

So $gxg^{-1} \in C_G(H)$. Hence $C_G(H)$ is normal in G.

6.2. QUOTIENT OR FACTOR GROUPS

Let H be a normal subgroup of a group G and consider the collection Q of all left cosets aH of H, $a \in G$. Define a 'multiplication' in Q as follows:

For aH, bH $\in$ Q, we put

$$aH \,.\, bH = abH \qquad 6.2\ (1)$$

We show that this multiplication is well defined. For this we have to prove that equation (1) is independent of the choice of representatives in aH and bH.

Let ah, bh' be arbitrary representatives in aH and bH respectively. Then

$$(ah)H.\ (bh')H = ahbh'H.$$

As H is normal in G, $ahbh' = abh_1h'$ for some $h_1 \in H$. Since $h_1h' \in H$, we have $h_1h'H = H$ so that

$$ahbh'H = abH.$$

Hence 6.2 (1) is independent of the choice of representatives in the cosets.

It is easy to verify that, under the multiplication defined by 6.2 (1), Q is a group with eH = H as the identity and a^{-1}H as the inverse of aH in Q. This group is called the *quotient (or factor)* group of G by H and is denoted by G/H.

6.2.1. Examples:

(a) Consider the additive group $\boldsymbol{Z}$ of integers. For a fixed integer n, the set

$$< n> = \{kn : k \in \boldsymbol{Z}\}$$

is a normal subgroup of $\boldsymbol{Z}$. The cosets

$$\bar{0} = 0 + < N >, \bar{1} = 1 + < n >, \bar{2} = 2 + < n >, ...,$$

$$\overline{n-1} = n - 1 + < n >$$

form a group under the addition defined by:

$$p + < n > + q + < n > = r + < n >,$$

where r is the remainder obtained after dividing the usual sum $p + q$ of p and q by n.

This group is the factor group of $\boldsymbol{Z}$ by $< n>$ and is denoted by $\boldsymbol{Z}_n$.

(b) Let $\boldsymbol{Q}$ be the group of rationals under addition. The additive group $\boldsymbol{Z}$ of intergers is a normal subgroup of $\boldsymbol{Q}$. The factor group $\boldsymbol{Q/Z}$ of $\boldsymbol{Q}$ by $\boldsymbol{Z}$ is called the *group of rationals* modulo 1.

Every element of $\boldsymbol{Q/Z}$ has finite order.

For if

$$a = p/q + \boldsymbol{Z} \in \boldsymbol{Q/Z}, q \neq 0,$$

p, q relatively prime, then

$$qa = q(p/q + \boldsymbol{Z}) = p + \boldsymbol{Z} = \boldsymbol{Z}$$

is the identity element of $\boldsymbol{Q/Z}$. Hence a has finite order q. Thus $\boldsymbol{Q/Z}$ is a periodic abelian group.

This group is, in fact, locally finite.

(c) Let Q be the group of quaternions $\pm I, \pm i, \pm j, \pm k$.

The subset

$$H = \{\pm I, \pm i\}$$

is a normal subgroup of Q. The factor group Q/H consists of

$$H \text{ and } jH \ (= kH)$$

and so is cyclic of order 2. The order of jH is 2 because $j^2 = -I$ and

$$(j\mathrm{H})^2 = j^2\,\mathrm{H} = -I\mathrm{H} = \mathrm{H}$$

It will be appropriate to recall, at this juncture, that a *homomorphism* of a group G to a group G′ is a mapping $\varphi : \mathrm{G} \to \mathrm{G}'$ satisfying the equation $\varphi(ab) = \varphi(a)\,\varphi(b)$. (The algebraic operation in the two groups has been taken as the same just for the sake of convenience).

A surjective homomorphism is called an *epimorphism*. The set of those elements of G which are mapped onto the identity e' of G′ is called the *kernel of* φ and *is denoted by Ker* φ. Thus

$$\mathrm{Ker}\ \varphi = \{k \in \mathrm{G} : \varphi(k) = e'\}.$$

Connected with the above concepts is the following important theorem.

6.2.2. Theorem: (Fundamental theorem of homomorphism).

Let $\varphi : \mathrm{G} \to \mathrm{G}'$ be an epimorphism from G to G′. Then:

(a) the kernel $K = \ker \varphi$ of φ is a normal subgroup of G.

(b) the factor group G/K is isomorphic to G′.

(c) a subgroup H′ of G′ is normal in G′ if and only if its inverse image $\mathrm{H} = \varphi^{-1}(\mathrm{H}')$ is normal in G.

(d) there is one-one correspondence between the subgroups of G′ and those subgroups of G which contain the kernel K.

Proof:

(a) If K is the kernel of φ and $k_1, k_2 \in \mathrm{K}$ then

$\varphi(k_1) = \varphi(k_2) = e'$ and $\varphi(k_2^{-1}) = (\varphi(k_2))^{-1} = e'$

Hence

$$\begin{aligned}\varphi(k_1 k_2^{-1}) &= \varphi(k_1)\,.\,\varphi(k_2^{-1}) \\ &= \varphi(k_1)\,.\,(\varphi(k_2))^{-1} \\ &= e'.e' \\ &= e'.\end{aligned}$$

So $k_1 k_2^{-1} \in K$ and K is a subgroup.

Also for each $k \in K$ and $g \in G$

$$\varphi(gkg^{-1}) = \varphi(g)\,\varphi(k).\,\varphi(g^{-1})$$
$$= \varphi(g).\,e'.\,\varphi(g)^{-1}$$
$$= e'.$$

Thus $gkg^{-1} \in K$ for any $k \in K$ and $g \in G$. Hence K is a normal subgroup.

(b) Define a mapping $\psi : G/K \to G'$ as follows:

For $gK \in G/K$, we put

$$\psi(gK) = \varphi(g).$$

One can verify that ψ is well-defined. Also ψ is surjective because each $g' = \varphi(g)$ is the image of $gK \in G/K$ under ψ.

Moreover if

$$\psi(gK) = \psi(g_1K)$$

then $\varphi(g) = \varphi(g_1)$.

Hence

$$\varphi(g)^{-1}\,\varphi(g_1) = e'$$

i.e. $\varphi(g^{-1} g_1) = e'$.

Thus $g^{-1} g_1 \in K$ i.e. $g_1 \in gK$. But $g_1 \in g_1K$. Hence $gK = g_1K$.

Therefore ψ is injective.

To see that ψ is a homomorphism, let $gK, g_1K \in G/K$. Then

$$\psi(gK\,g_1K) = \psi(gg_1K) = \varphi(gg_1) = \varphi(g)\,.\,\varphi(g_1)$$
$$= \psi(gK)\,.\,\psi(g_1K).$$

Hence ψ is an isomorphism between G/K and G'.

(c) Suppose that H' is a normal subgroup of G' and

$$H = \varphi^{-1}(H') = \{h \in G : \varphi(h) = h' \in H'\}.$$

Then K, being the inverse image of e', is contained in H. To show that H is normal in G, let $h \in H$ and $g \in G$. Consider the element ghg^{-1}. This belongs to H if and only if $\varphi(ghg^{-1}) \in H'$.

But

$$\varphi(ghg^{-1}) = \varphi(g).\ \varphi(h)\ .\ \varphi(g^{-1})$$
$$= \varphi(g)\ .\ \varphi(h)\ .\ \varphi(g)^{-1}$$

which is an element of H′ because H′ is normal in G′. Hence $ghg^{-1} \in H$ and H also is normal.

Conversely, suppose that H is normal in G where $H = \varphi^{-1}(H')$. For $h' \in H'$, $g' \in G'$ consider the element, $g'h'g'^{-1}$. Let g be one of the pre-images in G of $g' \in G'$ and $h \in H$ that of h'. Then

$$g'h'g'^{-1} = \varphi(g)\ \varphi(h)\ \varphi(g)^{-1}$$
$$= \varphi(ghg^{-1}).$$

As H is normal in G, $ghg^{-1} \in H$. Hence $\varphi(ghg^{-1}) \in \varphi(H) = H'$. Therefore H′ is normal in G′.

(d) Let α be a mapping from the collection Ω of all subgroups of G containing K to the collection Ω' of all subgroups of G′ given by:

$$\alpha(H) = H' = \varphi(H)$$

$H \in \Omega$, $H' = \varphi(H) \in \Omega'$. If $H_1, H_2, \in \Omega$ and $\alpha(H_1) = \alpha(H_2) = H'$, (say), then we show that $H_1 = H_2$ to prove that α is injective .

Let $H_1 = \varphi^{-1}(H')$. Then certainly $H_1 \subseteq H$. Next let $h \in H$. Then

$$\varphi(h) = h' = \varphi(h_1),$$

from $\alpha(H) = H' = \varphi(H_1)$, for $h' \in H'$, $h_1 \in H_1$. Hence $h_1^{-1}\, h \in K$ i.e. $h \in h_1\, K \subseteq H_1$. Thus $H \subseteq H_1$. So we have $H = H_1$. Similarly $H = H_2$. Hence α is injective.

Also, each $H' \in \Omega'$ is the image of an $H = \varphi^{-1}(H')$. Hence α is surjective and therefore bijective. Consequently α is a one-one correspondence between the subgroups of G′ and those subgroups of G which contain K.

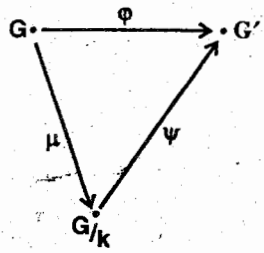
This proves the fundamental theorem completely.

This theorem is also called the *first isomorphism theorem.*

We have seen that the factor group [illegible] by the kernel K under an epimorphic mapping $\varphi : G \to G'$ is isomorphic to G′. Define a mapping $\mu : G \to G/K$, by

$$\mu(g) = gK, g \in G$$

Then μ is an epimorphism of G to G/K and is called the *natural* or *canonical homomorphism* of G onto G/K. Moreover the mapping $\psi : G/K \to G'$ defined by $\psi(gK) = \varphi(g) \in G'$, $g \in G$ is a homomorphism. Since the product of two homomorphism is a homomorphism, we have $\varphi = \psi\mu$. This fact is illustrated by the following diagram:



In such a situation we say that the above *triangle is commutative.* In view of the equality $\varphi = \psi\mu$, we sometimes also say that the mapping φ can be factored by the natural canonical map μ.

Let K be a normal subgroup of a group G. The subgroups of G/K are all of the form H/K for any subgroup H of G such that $K \subseteq H \subseteq G$. Moreover *a subgroup H, containing a normal subgroup K, is normal in G if and only if H/K is normal in G/K.*

For any subgroups H_1 and H_2 of G containing a normal subgroup K, *H_1 and H_2 are conjugate subgroups of G if and only if H_1/K, H_2/K are conjugate subgroups of G/K.*

Since, corresponding to each homomorphism of a group, we have a normal subgroup of that group namely the kernel of that homomorphism and conversely, each normal subgroup of a group determines a homomorphism of that group, *there is a one-one correspondence between the number of normal subgroups of a group and the number of homomorphisms of that group.*

Further it is important to observe the following points:

In the above theorem suppose that $K = \{e\}$. Then φ is injective because if

$$\varphi(g_1) = \varphi(g_2), g_1, g_2 \in G,$$

then

$$\varphi(g_1^{-1} g_2) = e',$$

where e' is the identity of G'. Hence $g_1^{-1} g_2 \in K = \{e\}$, that is, $g_1^{-1} g_2 = e$ so that $g_1 = g_2$. φ is already surjective. Hence φ is an isomorphism between G and G'.

Conversely, if G is isomorphic to G' with φ as an isomorphism between them then $K = \{e\}$, for if a g belonging to G is in K, then

$$\varphi(g) = e' = \varphi(e).$$

As φ is injective, $g = e$. Thus:

An epimorphism from G to G' is an isomorphism if and only if the kernel K of φ consists of the identity element of G alone.

6.2.3. Theorem: (Second isomorphism theorem).

Let H be a normal subgroup and K a subgroup of a group G. Then HK is a subgroup of G, $H \cap K$ is normal in K and $HK/H \cong K/(H \cap K)$.

Proof: The fact that HK is a subgroup of G was proved in Theorem 4.1.5. To see that $H \cap K$ is normal in K, let $x \in H \cap K$ and $k \in K$. Then

$$kxk^{-1} \in K \ (\because K \text{ is a subgroup and } x, k \in K)$$

$$\in H \ (\because x \in H \subseteq G \text{ and H is normal in G}).$$

Hence $kxk^{-1} \in H \cap K$. Thus $H \cap K$ is normal in K. Put $H \cap K = D$. Every element of HK/H is of the form $hkH = kh'H = kH$, $k \in K$, $h, h' \in H$, using the fact that H is normal in G. Define a mapping $\varphi : HK \to K/D$ by:

$$\varphi(hk) = kD. \qquad \text{(i)}$$

Then φ is surjetive because each $kD \in K/D$ is the image of an $hk \in HK$.

Moreover,

$$\begin{aligned} \varphi(hkh'k') &= \varphi(hh''kk') \\ &= kk'D \\ &= kD\,k'D. \end{aligned}$$

Hence φ is a homomorphism. By Theorem 6.2.2,

$$HK/\text{Ker } \varphi \cong K/D.$$

We show that Ker $\varphi = H$. Certainly Ker $\varphi \supseteq H$ by (i).

Conversely, $hk \in$ Ker φ implies

$$\varphi(hk) = D = kD.$$

Hence $k \in D = H \cap K \subseteq H$. Thus $hk \in H$ so that $H \supseteq \text{Ker } \varphi$. Therefore

$$\text{Ker } \varphi = H.$$

Hence

$$KH/H \cong K/(H \cap K).$$

Alternatively: Every element of HK/H is of the form $hkH = kH$

Let $H \cap K = D$. define $\psi : HK/H \to K/D$ by:

$$\psi(kH) = kD.$$

Obviously x is well-defined and surjective. ψ is also injective because if

$$\psi(kH) = \psi(k'H), k, k' \in K,$$

then $kD = k'D$ i.e. $k \in k'D \subseteq k'H$. As $k \in kH$, we have

$$kH = k'H$$

Finally

$$\begin{aligned}\psi(kH.\, k'H) &= x(kk'H)\\ &= kk'D\\ &= kD\,.\,k'D.\\ &= \psi(kH).\,\psi(k'H)\end{aligned}$$

Hence ψ is a bijective homomorphism, and so an isomorphism between HK/H and K/D. Thus

$$HK/H \cong K/D.$$

6.2.4. Theorem: (Third isomorphism theorem) Let, H, K be normal subgroups of G and $H \subseteq K$. Then

$$(G/H) / (K/H) \cong G/K.$$

Proof: The subgroup H, being a normal subgroup of G, is normal in any subgroup of G containing H. In particular H is normal in K. Define a mapping $\varphi : G/H \to G/K$ by:

$$\varphi(gH) = gK, g \in G \qquad \text{(i)}$$

Certainly φ is surjective. The homomorphism property of φ follows from the equations

$$\begin{aligned}\varphi(gH\,.\,g'H) &= \varphi(gg'H)\\ &= gg'K\end{aligned}$$

$$= gK \,.\, g'K.$$

By Theorem 6.2.2.

$$(G/H)/K' \cong G/K,$$

where $K' = \text{Ker}\ \varphi$. We show that

$$K' = K/H.$$

Obviously $K' \supseteq K/H$.

Conversely if $gH \in K'$, then

$$\varphi(gH) = gK, \text{ by definition of } \varphi.$$

$$= K, \text{ by the assumption that } gH \in K'$$

Thus $g \in K$. Hence $gH \in K/H$ and therefore $K' \subseteq K/H$. Combining the two inequalities, we have $K' = K/H$ and consequently

$$(G/H) \,/\, (K/H) \cong G/K.$$

A group G is abelian if and only if G coincides with its centre $\zeta(G)$. The theorem that follows gives another necessary and sufficient condition for a group to be abelian.

6.2.5. Theorem: A group G is abelian if and only if the factor group $G/\zeta(G)$ is cyclic.

Proof: As remarked above if G is abelian then $G = \zeta(G)$, the centre of G. So $G/\zeta(G)$ is the trivial group and hence cyclic. (The trivial or the identity group is assumed to be generated by the empty set).

Conversely, suppose that $G/\zeta(G)$ is a cyclic group and $a\zeta(G)$, $a \in G$, is its generator. We show that G is abelian. For this let $x, y \in G$. Then $x\zeta(G)$, $y\zeta(G)$ belong to $G/\zeta(G)$. So there exist integers m, n such that

$$x\zeta(G) = a^m\,\zeta(G),\ y\zeta(G) = a^n\,\zeta(G).$$

Thus $x = a^m z$, $y = a^n z'$ for some $z, z' \in \zeta(G)$. Using the fact that $\zeta(G)$ is abelian, we have,

$$xy = a^m z \,.\, a^n z' = a^m \,.\, a^n \,.\, z \,.\, z' = a^n \,.\, a^m z' z = a^n z' \,.\, a^m z = yx.$$

Consequently G is abelian.

6.2.6. Theorem: Every group of order p^2, where p is a prime number, is abelian.

Proof: Suppose that G is a group of order p^2, p a prime. By Theorem 5.4.3., G has non-trivial centre $\zeta(G)$. By Largange's theorem, the order of $\zeta(G)$, being a divisor of p^2, must be p or p^2. Suppose that the order of $\zeta(G)$ is p. Then $G/\zeta(G)$ has order p and so must be cyclic, by corollary 5.2.1 (d). By Theorem 6.2.5. given above G is abelian. Thus $G = \zeta(G)$ so that the order of $\zeta(G)$ is not equal to p, contradicting our supposition. Hence the order of $\zeta(G)$ is p^2. But then $\zeta(G)$ considered as a subgroup of G of the same finite order as the order of G, must coincide with G, that is, $G = \zeta(G)$. Hence G is abelian.

If $\zeta(G)$ has order p^2 then $\zeta(G) = G$ and is abelian.

6.3. AUTOMORPHISM GROUP OF A GROUP

Given a group G there are many ways to form new groups. One of these is to form the group of automorphisms of G. A detailed description of this concept is given in this section.

For a group G, a homomorphism α from G into G is called an *endomorphism* of G. In the case where α is bijective, it is said to be an automorphism of G.

Thus a mapping $\alpha : G \to G$ is an *automorphism* if and only if

(i) α is bijective,

(ii) $\alpha(g_1 g_2) = \alpha(g_1)\,\alpha(g_2)$ for all $g_1, g_2 \in G$.

6.3.1. Theorem: The set A(G) of all automorphism of G is a group.

Proof: Let $\alpha, \beta \in A(G)$. Then the product $\beta\alpha$ of the bijective mapping α and β is bijective.

Moreover:

$$(\beta\alpha)(g_1 g_2) = \beta(\alpha(g_1 g_2))$$

$$= \beta(\alpha(g_1)\,\alpha(g_2)), \because \alpha \text{ is an automorphism}$$

$$= \beta(\alpha(g_1)) \cdot \beta(\alpha(g_2)), \because \beta \text{ is an automorphism}$$

$$= (\beta\alpha)(g_1) \cdot (\beta\alpha)(g_2)$$

for all $g_1, g_2 \in G$. Hence $\beta\alpha$ is an automorphism. Thus A(G) is closed under the usual multiplication of mappings. The associative law in A(G) follows form the associativity of mappings of a set. Also, the identity mapping $I : G \to G$ given by

$$I(g) = g \text{ for all } g \in G$$

is bijective and

$$I(g_1 g_2) = g_1 g_2 = I(g_1).\ I(g_2) \text{ for all } g_1, g_2 \in G.$$

Hence $I \in A(G)$ and satisfies the equation

$$\alpha . I = I . \alpha = \alpha$$

for all $\alpha \in A(G)$. Thus I is the identity in A(G).

Next, for each $\alpha \in A(G)$, the inverse mapping $\alpha^{-1} : G \to G$ is bijective. The automorphism property of α^{-1} follows from the equations

$$\begin{aligned}
\alpha^{-1}(g_1 g_2) &= \alpha^{-1}(I(g_1 g_2)) \\
&= \alpha^{-1}(I(g_1), I(g_2)) \\
&= \alpha^{-1}(\alpha\alpha^{-1}(g_1) . \alpha\alpha^{-1}(g_2)) \\
&= \alpha^{-1}(\alpha(\alpha^{-1}(g_1) . \alpha^{-1}(g_2))) \\
&= (\alpha^{-1}\alpha)(\alpha^{-1}(g_1) . \alpha^{-1}(g_2)) \\
&= \alpha^{-1}(g_1)\,\alpha^{-1}(g_2)
\end{aligned}$$

for all $g_1, g_2 \in G$. Thus each $\alpha \in A(G)$ has an inverse α^{-1} in A(G). Therefore A(G) is a group.

6.3.2. Inner Automorphism of a group:

Let a be a fixed element of G and consider the mapping $I_a : G \to G$ given by:

$$I_a(g) = aga^{-1},\ g \in G. \qquad 6.3.2\ (A)$$

Then I_a is surjective because each $g \in G$ is the image of an element $a^{-1}ga$ under I_a. I_a is injective because, for all $g_1, g_2 \in G$,

$$I_a(g_1) = I_a(g_2)$$

implies

$$ag_1a^{-1} = ag_2a^{-1}$$

i.e.

$$g_1 = g_2.$$

Also

$$\begin{aligned} I_a(g_1g_2) &= a(g_1g_2)\,a^{-1} \\ &= (ag_1a^{-1})\,(ag_2a^{-1}) \\ &= I_a(g_1)\,.\,I_a(g_2). \end{aligned}$$

Hence I_a is an automorphism of G.

The mapping I_a, given in (A) above, is called an *inner automorphism* of G.

Also, for $a, b \in G$,

$$\begin{aligned} I_a.\,I_b(g) &= I_a[(bgb^{-1})] \\ &= a(bgb^{-1})\,a^{-1} \\ &= (ab)g\,(ab)^{-1} \\ &= I_{ab}(g) \end{aligned}$$

for all $g \in G$. Hence

$$I_a\,.\,I_b = I_{ab} \qquad 6.3.2\ (B)$$

An automorphism of G which is not an inner automorphism is called an *outer automorphism*.

Every automorphism of an abelian group except the identity automorphism is outer. However it may be mentioned that there exist non-abelian groups all of whose automorphisms are outer.

Similarly there exists groups all of whose automorphism are inner (see example. 6.3.4 (c)).

The structural properties of the group of automorphism of a group vary, sometimes, to a very large degree from those of the group.

For instance the automorphism group of an abelian group may be non-abelian (see example. 6.3.4 (b)). The automorphism group of an infinite group may turn out to be finite.

Similarly some other group-theoretical properties of a group may not be inherited by its group of automorphism.

However the group of automorphism of a finite group is always finite.

A group G is said to be *complete* if:

(a) The center $\xi(G)$ of G is trivial, and (b) Every automorphism of G is inner.

6.3.3. Theorem: Let G be a group. The mapping $\varphi : G \to G$ defined by:

$$\varphi(g) = g^{-1}, g \in G$$

is an automorphism if, and only if G is abelian.

Proof: Suppose that G is abelian. Then, for $g_1, g_2 \in G$

$$\varphi(g_1) = g_1^{-1}, \varphi(g_2) = g_2^{-1}.$$

So

$$\varphi(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$$

$$= g_1^{-1} g_2^{-1} \because G \text{ is abelian}$$

$$= \varphi(g_1) \cdot \varphi(g_2)$$

So φ, being bijective, is an automorphism.

Conversely, if $\varphi = G \to G$ given by

$$\varphi(g) = g^{-1}, g \in G$$

is an automorphism then, for any $g_1, g_2 \in G$,

$$\varphi(g_1 g_2) = (g_1 g_2)^{-1}, \text{ by definition of } \varphi$$

$$= g_2^{-1} g_1^{-1} \qquad 6.3.3 \text{ (i)}$$

Also

$$\varphi(g_1 g_2) = \varphi(g_1)\, \varphi(g_2)$$

$$= g_1^{-1} g_2^{-1} \qquad 6.3.3 \text{ (ii)}$$

From (i) and (ii) we have:

$$g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} \text{ or } (g_1 g_2)^{-1} = (g_2 g_1)^{-1}$$

That is

$$g_1 g_2 = g_2 g_1.$$

Hence G is abelian.

6.3.4. Theorem: Let G be a group which has an element of order > 2. Then G has an automorphism different form the identity automorphism.

Proof: Here if G is abelian and has an element g of order > 2 then $\varphi : G \to G$ defined by

$$\varphi(g) = g^{-1} \neq g,$$

is an automorphism different from the identity automorphism, by Theorem 6.3.2.

If G is non-abelian and contains an element a of order m > 2, then there is a $g \in G$ such that

$$gag^{-1} \neq a$$

so that $I_g : G \to G$ given by $I_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism different from the identity automorphism.

6.3.5. Examples.

(a) The mapping $\alpha : \mathbf{Z} \to \mathbf{Z}$ of the group of integers defined by:

$\alpha(n) = -n, n \in \mathbf{Z}$

is an automorphism. This is the only non-identity automorphism of $\mathbf{Z}$.

Thus A($\mathbf{Z}$) is of order 2.

(b) The mappings $\alpha : \mathbf{V} \to \mathbf{V}$ and $\beta : \mathbf{V} \to \mathbf{V}$ of the four-group $\mathbf{V} = < a, b : a^2 = b^2 = (ab)^2 = 1 >$ given by:

$\alpha(a) = b, \alpha(b) = (ab), \alpha(ab) = a, \alpha(1) = 1$

and

$\beta(a) = b, \beta(b) = a, \beta(ab) = ab, \beta(1) = 1$

are automorphisms and

$$A(V) = < \alpha, \beta : \alpha^3 = \beta^2 = (\alpha\beta)^2 = 1 >.$$

(c) The group of automorphisms of the group

$G = < a, b ; a^3 = b^2 = (ab)^2 = e >$ is isomorphic to G.

The only automorphisms of G are the inner automorphisms

$$I_e, I_a, I_{a^2}, I_b, I_{ab}, I_{a^2b}$$

(This fact will follow from theorem 6.3.6).

An automorphism of a cyclic group C_n is a mapping $\alpha: C_n \to C_n$ which maps the generator of C_n into an element a^m, where (m, n) = 1 The set $\mathbf{Z}'_n$ consisting of the non zero elements m of $\mathbf{Z}'_n$ has an inverse if and only if $(m, n) = 1$, Such elements of $\mathbf{Z}'_n$ are called units of $\mathbf{Z}'_n$.

Thus Aut $(C_n) \cong$ the group of units of $\mathbf{Z}'_n$.

6.3.6. Theorem: The set I(G) of all inner automorphisms of a group G is a normal subgroup of A(G).

Proof: Let $I_a, I_b \in I(G)$. Then

$$I_b(g) = bgb^{-1}, I_b^{-1}(g) = b^{-1}gb$$

and

$$\begin{aligned} I_b \cdot I_{b^{-1}}(g) &= I_b(b^{-1}gb) \\ &= b(b^{-1}gb)b^{-1} \\ &= g \\ &= I_e(g), \end{aligned}$$

for all $g \in G$.

Hence

$$I_b^{-1} = (I_b)^{-1}.$$

Now

$$\begin{aligned} I_a I_b^{-1}(g) &= I_a(b^{-1}gb) \\ &= a(b^{-1}gb)a^{-1} \\ &= (ab^{-1})g(ab^{-1})^{-1} \\ &= I_{ab^{-1}}(g) \end{aligned}$$

for all $g \in G$. Hence $I_a \cdot I_{b^{-1}} = I_{ab^{-1}} \in I(G)$ and I(G) is a subgroup.

Next let $\alpha \in A(G)$. Then, for any $I_a \in I(G)$, we have,

$$\begin{aligned}(\alpha I_a \alpha^{-1})(g) &= \alpha I_a(\alpha^{-1}(g)) \\ &= \alpha(a(\alpha^{-1}(g))a^{-1}) \\ &= \alpha(a).(\alpha.\alpha^{-1}(g)).\alpha(a^{-1}) \\ &= \alpha(a)((\alpha\alpha^{-1})(g))(\alpha(a))^{-1}, \quad \because \alpha \text{ is an automorphism.} \\ &= \alpha(a)\, g\, (\alpha(a))^{-1} \\ &= I_{\alpha(a)}(g)\end{aligned}$$

for all $g \in G$. Hence

$$\alpha I_a \alpha^{-1} = I_{\alpha(a)} \in I(G).$$

Therefore I(G) is a normal subgroup.

The theorem that follows gives a relationship between the group of inner automorphisms of a group and the factor group of that group by its centre.

6.3.7. Theorem: Let G be a group with $\zeta(G)$ as its centre and I(G) the group of its inner automorphisms. Then $G/\zeta(G)$ is isomorphic to I(G).

Proof: Consider the mapping $\varphi: G \to I(G)$ given by

$$\varphi(g) = I_g, \qquad \text{for all } g \in G.$$

Then φ is surjective. Also

$$\begin{aligned}\varphi(g_1 g_2) &= I_{g_1 g_2} \\ &= I_{g_1} \cdot I_{g_2} \qquad \text{by 6.3.2 (B)} \\ &= \varphi(g_1)\,\varphi(g_2)\end{aligned}$$

Hence φ is a homomorphism.

By the fundamental theorem of homomorphism,

$$G/K \cong I(G)$$

where $K = \text{Ker}\,\varphi$. We show that $K = \zeta(G)$.

Let $z \in \zeta(G)$, then

$$\varphi(z) = I_z$$

and

$$I_z(g) = zgz^{-1} = g = I_e(g).$$

So $I_z = I_e$ for all $z \in \zeta(G)$. Hence $z \in K$, that is, $\zeta(G) \subseteq K$.

Conversely, if $k \in K$ then

$$\varphi(k) = I_k, \text{ by definition of } \varphi$$

$$= I_e \text{ by assumption that } k \in K.$$

However $I_k = I_e$ implies

$$I_k(g) = kgk^{-1} = g = I_e(g)$$

for all $g \in G$. Therefore $k \in \zeta(G)$ so that $K \subseteq \zeta(G)$. Hence

$$K = \zeta(G).$$

Therefore

$$G/\zeta(G) \cong I(G).$$

Alternatively: Define a mapping $\psi : G/\zeta(G) \to I(G)$ as follows:

For each $g\,\zeta(G) \in G/\zeta(G)$ we put

$$\psi(g\,\zeta(G)) = I_g.$$

Then ψ is obviously surjective. Also let

$$\psi(g_1\,\zeta(G)) = I_{g_1} = I_{g_2} = \psi(g_2\,\zeta(G))$$

Then, for any $x \in G$,

$$I_{g_1}(x) = I_{g_2}(x)$$

That is,

$$g_1 x g_1^{-1} = g_2 x g_2^{-1}$$

or $$g_2^{-1}(g_1 x g_1^{-1})\, g_2 = x$$

$$(g_2^{-1} g_1)(x)(g_2^{-1} g_1)^{-1} = x$$

for all $x \in G$. Hence $g_2^{-1} g_1 \in \zeta(G)$ i.e. $g_1 \in g_2\zeta(G)$. But $g_1 \in g_1\,\zeta(G)$. Hence $g_1\zeta(G) = g_2\zeta(G)$ which shows that ψ is injective.

Also, for $g_1\,\zeta(G)$, $g_2\,\zeta(G) \in G/\zeta(G)$

$$\psi(g_1\,\zeta(G) \cdot g_2\,\zeta(G)) = \psi(g_1 g_2\,\zeta(G))$$
$$= Ig_1g_2$$
$$= Ig_1 \cdot Ig_2$$
$$= \psi(g_1\,\zeta(G)) \cdot \psi(g_2\,\zeta(G))$$

Hence ψ is an isomorphism. Thus

$$G/\zeta(G) \cong I(G).$$

6.3.8 Example:

Let $Q = \langle a, b: a^4 = 1, a^2 = b^2, bab = a^{-1} \rangle$ be the group of quaternion. Then $I(Q) \cong Q/\xi(Q) \cong C_2 \times C_2$.

It was remarked in example 6.3.4(c) above that all the automorphisms of $G = \langle a, b : a^3 = b^2 = (ab)^2 = e \rangle$ are inner. As the centre of G in trivial, the above theorem justifies that remark.

Also if the only inner automorphism of a group G is the identity mapping, then G is abelian.

This is so because, for each $z \in G$, the mappings I_z and I_e are idential and so, for any $g \in G$,

$$I_z(g) = zgz^{-1} = g = I_e(g).$$

So, $gz = zg$. Hence $z \in \zeta(G)$, for all $z \in G$. Thus G is abelian.

6.4. COMMUTATOR OR DERIVED SUBGROUPS

The term commutator subgroup is due to Dedekind but the fundamental and basic properties of these subgroups were first given by G.A. Miller. Their usefulness was quickly recognized and they have become an important and significant part of the recent literature on group theory. The theory of commutators helps determining the inherent structure of groups.

Let G be a group and $a, b \in G$. Then the element

$$aba^{-1}\,b^{-1}$$

is called the *commutator of a and b* and is denoted by $[a, b]$.

A few of the properties of commutators are given below:

6.4.1. Theorem: The following commutator indentities hold in a group G.

(i) $[b, a] = [a, b]^{-1}$

(ii) $[ab, c] = [b, c]^a [a, c]$

(iii) $[a, bc] = [a, b] [a, c]^b$

(iv) $[a, b^{-1}] = [b, a]^{b^{-1}}$ and

$[a^{-1}, b] = [b, a]^{a^{-1}}$

for all $a, b, c \in G$.

(Here x^a denotes the conjugate axa^{-1} of x).

Proof: (*i*) Since $[b, a] = bab^{-1} a^{-1}$, $[b, a] [a, b] = 1$, so

$$[b, a] = [a, b]^{-1} \qquad 6.4.1\ (1)$$

(ii) For $a, b, c \in G$,

$$[ab, c] = abc(ab)^{-1} c^{-1}$$
$$= abcb^{-1} a^{-1} c^{-1}$$
$$= a(bcb^{-1} c^{-1})a^{-1} aca^{-1} c^{-1}$$
$$= [b, c]^a [a, c] \qquad 6.4.1\ (2)$$

(iii) $[a, bc] = a(bc)\, a^{-1} (bc)^{-1}$

$$= abc\, a^{-1} c^{-1} b^{-1}$$
$$= cba^{-1} b^{-1} baca^{-1} c^{-1} b^{-1}$$
$$= [a, b] [a, c]^b \qquad 6.4.1\ (3)$$

(iv) $[a, b^{-1}] = ab^{-1} a^{-1} b = b^{-1} bab^{-1} a^{-1} b$

$$= [b, a]^{b^{-1}} \qquad 6.4.1\ (4)$$

and similarly

$$[a^{-1}, b] = [b, a]^{a^{-1}} \qquad 6.4.1\ (5)$$

The relations 6.4.1 (1) to 6.4.1 (5) are called *commutator identities*.

Obviously a group G is abelian if and only if. for any two elements $a, b \in G$, $[a, b] = e$. Thus the commutators, in a way, measure the extent to which a group can be farther from being abelian.

For any group G, let G′, denote the subgroup of G generated by all the commutators $[a, b]$, $a, b \in G$. G′ is called the *first derived group or commutator subgroup* of G. G′ is also written as [G, G]. Second, third and, in general, an nth derived group ($n > 1$) of G are similarly defined as $G'' = [G', G']$, $G''' = [G'', G'']$ and $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ respectively.

The theorem that follows gives a relation between a group and its derived group.

6.4.2. Theorem: Let G be a group. Then

(a) the derived group G′ is a normal subgroup of G.

(b) the factor group G/ G′ is abelian.

(c) If K is a normal subgroup of G such that G/K is abelian then $K \supseteq G'$.

Proof: (a) Here we make use of theorem 6.1.4. Since G′ is generated by the commutators $[a, b]$, $a, b \in G$, it is enough to show that $g\,[a, b]\,g^{-1} \in G'$ for all $g \in G$. Now

$$g[a, b]g^{-1} = gab\,a^{-1}\,b^{-1}\,g^{-1}$$
$$= gag^{-1} \cdot gbg^{-1} \cdot ga^{-1}\,g^{-1}\,gb^{-1}\,g^{-1}$$
$$= a^g b^g\,(a^g)^{-1}\,(b^g)^{-1}$$
$$= [a^g, b^g]$$

is an element of G′ for all $g \in G$. Hence G′ is normal ;

Or equivalently, let $q \in G'$, $g \in G$. Then $gqg^{-1}\,q^{-1} \in G'$ so that $gqg^{-1} \in G'q = G'$.

(b) Let $aG', bG' \in G/G'$, then

$$[aG', bG'] = aG'\,bG'\,(aG')^{-1}\,(bG')^{-1}$$
$$= aG'\,bG'\,a^{-1}G'\,b^{-1}\,G'.$$
$$= (aba^{-1}\,b^{-1})G'$$
$$= G'.$$

which is the identity in G/G′. Hence G/G′ is abelian

(c) Let K be a normal subgroup of G such that G/K is abelian. Then for all a, b in G,

$aKbK\,(aK)^{-1}\,(bK)^{-1}\,K = aba^{-1}\,b^{-1}\,K = K.$

Hence $ab\,a^{-1}b^{-1} \in K$. Thus $G' \subseteq K$.

A group G is called *solvable* if and only if the sequence of subgroups.

$$G \supseteq G' \supseteq \ldots \supseteq G^{(k)} \supseteq \ldots. \qquad 6.4.2\ (D)$$

where $G^{(i)}$ is the derived group of $G^{(i-1)}$, terminates at some integer k in the identity subgroup i.e. for some integer k,

$G^{(k)} = \{e\}$.

A group which is not *solvable* is naturally called an *unsolvable* group. Solvable groups play an important role in the theory of equations. In fact, with any polynomial equation of degree n in some *variable* x, one can associate a group in a certain way. An equation of degree n is solvable by *algebraic procedures* like addition, subtraction, multiplication, division and extraction of roots if and only if the corresponding group associated with that equation is solvable. This was proved by E. Galois (1811-1831) who associated, with each polynomial, a certain group (group of permutations of roots of the ploynomial). Galois was killed in a duel at the age of 20.

6.4.3. Examples:

(a) A group is belian if and only if its derived group is the identity subgroup. Hence every abelian group is solvable.

(b) Let $G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$. The derived group G' is the group generated by a. G', being of index 2, is normal in G. G/G', being of order 2, is cyclic and hence abelian.

The second derived group G'' of G which is also the derived group of G' is the identity subgroup.

Hence G is a solvable group.

A group G is said to be *metabelian* if the derived group G' of G is abelian.

The group of example 6.4.3(b) is metabelian. So also are the group of quaternions and the dihedral groups.

6.5. CHARACTERISTIC AND FULLY INVARIANT SUBGROUPS

Let Ω be a set of symbols α, β, γ etc. and G be a group. Ω is said to be a *domain of operators* for G if

1. for each $\alpha \in \Omega$ and $g \in G$, $\alpha(g) \in G$, and
2. for each $\alpha \in \Omega$ and $g_1, g_2 \in G$. $\alpha(g_1 g_2) = \alpha(g_1).\ \alpha(g_2)$.

For example, let E(G) be the set of all endomorphisms of G. Then, for each $\varphi \in E(G)$ and $g \in G$, $\varphi(g) \in G$ and $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all g_1, $g_2 \in G$. Hence E(G) is a domain of operaters for G.

If Ω is a domain of operators for a group G and H is a subgroup G then H is said to be an Ω-admissible subgroup of G if

$$\alpha(H) \subseteq H$$

for all $\alpha \in \Omega$.

It is easy to see that the intersection of any collection of Ω-admissible subgroups of a group is an Ω-admissible subgroup.

A subgroup H of a group G is said to be a *characteristic subgroup* if and only if H is mapped onto itself under every automorphism of G.

Thus $H \subseteq G$ is characteristic in G if, for each automorphism α of G,

$$\alpha(H) = H.$$

Using the language of domain of operator, we may define a characteristic subgroup of a group G as a subgroup of G which is A (G)-admissible, where A(G) is the group of automorphims of G.

A subgroup F of a group G is said to be *fully invariant* if F is mapped into itself under *every endomorphism* of *G*.

Thus $F \subseteq G$ is fully invariant if, for each endomorphism φ of G, $\varphi(F) \subseteq F$ or, if F is E (G)-admissible.

It is easy to see that a subgroup F of G is fully invariant if and only if each generator of F is mapped into an element of G by every endomorphism of G.

6.5.1. Examples:

(a) The commutator subgroup of a group is fully invariant.

For if $G' = [G, G]$ is the commutator subgroup of G then, for any endomorphism φ of G and any generator $[x, y]$ of G',

$$\varphi[x, y] = \varphi(xyx^{-1}y^{-1}) = \varphi(x) \cdot \varphi(y) \cdot \varphi(x)^{-1} \varphi(y)^{-1}$$
$$= [\varphi(x), \varphi(y)]$$

is an element of G'.

(b) The centre of a group G is characteristic.

For let $\zeta(G)$ be the centre of G and α any automorphism of G. We show that, for any $z \in \zeta(G)$, $\alpha(z) \in \zeta(G)$.

Let $x \in G$ Then there is a $y \in G$ such that $x = \alpha(y)$.

Hence

$$\alpha(z) \cdot x = \alpha(z) \cdot \alpha(y) = \alpha(zy) = \alpha(yz) = \alpha(y) \cdot \alpha(z)$$
$$= x \cdot \alpha(z).$$

So $\alpha(z) \in \zeta(G)$. Therefore $\zeta(G)$ is characteristic.

(c) Let A be an abelian group and A_p the set of all those elements of A whose orders are powers of a fixed prime p. Then A_p is a fully invariant subgroup of A.

This follows from the fact that an element whose order is a power of a prime is mapped onto a similar element or the identity under a group homomorphism.

In general, in a group G, if $H = \{x \in G : x^n = 1\}$ is a subgroup then H is fully invariant.

(d) For a group G let $G^n = \langle x^n : x \in G \rangle$, that is, G^n is the group generated by the nth powers of all elements of G. Then G^n is fully invariant (verify!).

(e) Every group G has two characteristic subgroups namely the identity subgroup and the group G. A group which has no characteristic subgroup other than these two is called a *characteristically* simple group. Such groups have been investigated by P. Hall. [26].

(*e*) If a subgroup H is the only subgroup of order m of a group G then H is characteristic. For any automorphism α, α (H) is a subgroup of G of order m and so coincides with H.

6.5.2. Theorem: Every fully invariant subgroup is characteristic.

Proof: Let F be a fully invariant subgroup of G and α any automorphism of G. Since every automorphism of G is an endomorphism, $\alpha(F) \subseteq F$. Since α^{-1} is also an automorphism, $\alpha^{-1}(F) \subseteq F$, that is, for each $a \in F$, $\alpha^{-1}(a) = b \in F$ so that $a = \alpha(b) \in \alpha(F)$. Hence $F \subseteq \alpha(F)$. Consequently $\alpha(F) = F$. So F is characteristic.

5.3. Theorem: Intersection of any class of characteristic subgroups is a characteristic group.

Proof: Let Ω be a class of characteristic subgroups of a group G. Put $H = \cap K$, $K \in \Omega$. For any automorphism α of G and $K \in \Omega$.

$$\alpha(K) = K.$$

Now $\alpha(H) \subseteq \alpha(K) = K$ for all $K \in \Omega$. Hence

$$\alpha(H) \subseteq \cap\, \alpha(K) \subseteq \cap K = H,\ K \in \Omega$$

So $\alpha(H) = H$. Therefore H is characteristic.

6.5.4. Theorem: Every characteristic subgroup is normal.

Proof: Let H be a characteristic subgroup of G. Then $\alpha(H) = H$ for every automorphism α of G. In particular $I_g(H) = gHg^{-1} = H$, for every inner automorphism I_g, $g \in G$. Thus H is normal in G, as required.

6.5.5. Corollary: Every fully invariant subgroup is normal.

Proof: Since every fully invariant subgroup is characteristic and every characteristic subgroup is normal we have the above corollary.

Remark: In example 6.5.1 (a) we showed that the commutator subgroup of a group G is fully invariant. Corollary 6.5.5 shows that every fully invariant subgroup is normal in G. Hence the commutator subgroup is normal. This provides yet another proof for the normality of the commutator subgroup. The first proof was given in Theorem 6.4.1.

We have seen in example 6.1.1 (b) that a normal subgroup H of a normal subgroup K in a group G many not be normal in G. The theorem

that follows gives a condition which ensures the normality of a subgroup of a normal subgroup in the parent group.

6.5.6. Theorem: Let H be a characteristic subgroup of a normal subgroup K of a group G. Then H is normal in G.

Proof: Since K is a normal subgroup of G, K is mapped onto itself under every inner automorphism I_g, $g \in G$. The restriction (also to be denoted by I_g) to K of I_g, $g \in G$, is an automorphism of K. as H is characteristic in K, H is mapped onto itself under I_g. So, for each $g \in G$, $gHg^{-1} = H$. Hence H is normal in G.

EXERCISES

1. Let $\mathbf{C}'$ be the group of non-zero complex numbers under multiplication and $\boldsymbol{R}^+$ the group of non-zero positive real numbers under multiplication. Show that the mapping $\mu : \boldsymbol{C}' \to \boldsymbol{R}^+$ given by:

   $$\mu(z) = |z|$$

   is an homomorphism from $\boldsymbol{C}'$ to $\boldsymbol{R}^+$.

2. Let $\mathbf{R}$ be set of all real numbers and

   $$G = \{(a, b) : a, b \in \boldsymbol{R}, a \neq 0\}.$$

   Define a binary relation in G by:

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

   Show that

   (i) G is a group under this binary operation.

   (ii) $K = \{(1, b) : b \in \boldsymbol{R}\}$ is normal in G.

   (iii) G/K is isomorphic to the group of non-zero real numbers under multiplication.

3. Let $\boldsymbol{C}'$ and $\boldsymbol{R}^+$ be as given in Exercise 1 and $\boldsymbol{U}$ be the group, under multiplication, of all complex numbers of unit modulus. Define a mapping $\nu : \boldsymbol{C}' \to \boldsymbol{U}$ by:

   $$\nu(z) = \frac{z}{|z|}$$

Show that ν is an epimorphism with R^+ as its kernel and hence C'/R^+ is isomorphic to U.

4. Show that if $(R, +)$ is the group of reals, the mapping $f : R \to U$ define by $f(x) = \cos x + i \sin x$, $x \in R$, is a surjective homomorphism with $\text{Ker} f = \{2n\pi : n \in Z\}$.

5. Consider the additive group Z of integers as a subgroup of the group R of all real numbers under addition. If U is the group of all complex numbers of unit modulus under multiplication, then prove that the mapping $\varphi : R \to U$ define by:

$$\varphi(x) = e^{2\pi ix} = \cos 2\pi x + i \sin 2\pi x, x \in R$$

is an epimorphism with Z as its kernel showing thereby that R/Z is isomorphic to U.

6. Let $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0, a, b, c, d \in R\right\}$ be the group under multiplication. Show that $\varphi : G \to (R, .)$ given by:

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc \neq 0$$

is a homomorphism.

7. Let a group G have the following presentation:

$$G = \langle a, b : a^2 = b^2 = 1 \rangle.$$

G is called the *infinite dihedral group*. Show that the cyclic group generated by ab is a normal subgroup of G. Also show that every finite dihedral group is a homomorphic image of G and therefore isomorphic to a factor of G.

8. Describe the cosets of $H = \{(x, y) : x = y, x, y \in R)\}$ in $R \times R$.

9. A group G has the following presentation.

$G = \langle a, b, c : a^3 = b^2 = c^2 = (bc)^2 = 1, b^a = c, c^a = bc \rangle$.

Find all the normal subgroups of G, the normal subgroups of these normal subgroups and so on.

10. Let A be a subgroup of G. For any subgroup B of G, containing A, show that if A is normal in B then $B \subseteq N_G(A)$.

11. Let $C_G(H)$ and $N_G(H)$ respectively be the centraliser and normaliser of a subgroup H in G. Show that $C_G(H)$ is normal in $N_G(H)$.

Also show that every subgroup of the centre $\zeta(G)$ of a group G is normal in G.

12. Let H be a subgroup of a group G. Suppose that all the left cosets of H in G form a group under multiplication defined by:

$$aH.\ bH = abH.$$

Show that H is normal in G.

13. Let K be a normal subgroup of G. Then $\zeta(K)$ is normal in G.

[Hint: K normal in G $\Rightarrow$ for $g \in G$ and $k \in K$, $kg = gk_1$ and

$$g^{-1}k = k_1 g^{-1}, \text{ for } k_1 \in K.$$

So, for $z \in \zeta(K)$, $g \in G$ and $k_1 \in K$

$$k_1 g\, zg^{-1} = gk_2\, zg^{-1} = gzk_2 g^{-1} = gz\, g^{-1}k_1.$$

So $gzg^{-1} \in \zeta(K)$ for all $z \in \zeta(K)$, $g \in G$.]

14. Let G be a group and H be a normal subgroup of G. Show that G/H is cyclic if and only if there is an element a in G with the property that, for every $x \in G$, there is some integer n such that $x\, a^n \in H$.

15. If every element of a normal subgroup H and factor group G/H of a group G has finite order then show that every element of G has finite order.

16. Let a group G have a normal subgroup H of index p, a prime. Show that G has at least one element of order p.

17. *A subgroup H of a group G is called maximal if and only if, for any subgroup K of G such that*

$$H \subseteq K \subseteq G,$$

either K = H or K = G.

Show that a normal subgroup H of G is maximal in G if and only if G/H is simple.

18. Let K be a normal subgroup of G and H a subgroup of G containing K. Then show that H/K is a subgroup of G/K. Also show that H/K is normal in G if and only if H is normal in G.

19. Let $a, b \in G$ and $z = ab$. If $z \in \zeta(G)$, show that $ab = ba$,

[Hint: $z \in \zeta(G) \Leftrightarrow ab\, g = g\, ab \Rightarrow bgb^{-1} = a^{-1} ga$ for all $g \in G$. So, with g replaced by $b^{-1}g$,

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

i.e., $a^{-1}b^{-1} ga = g\, b^{-1}$

or $g\, a\, b = b\, a\, g$. But $g\, a\, b = abg = bag$.

Now use cancellation law].

20. Let G be a group, H a maximal subgroup of G and N a normal subgroup of G distinct from H. Show that

$$G/N \cong H/H \cap N$$

[Hint: Here G = HN.]

21. Let a be an element of order 2 in a group G. Show that $< a >$ is normal in G if and only if $a \in \zeta(G)$.

22. Let H be a subgroup of a group G and

$$K = < ghg^{-1} : g \in G, h \in H >.$$

Show that K is a normal subgroup of G.

23. Let $\varphi : \mathbf{Z} \to \mathbf{Z}_4$, $\mathbf{Z}_4$ under addition, be defined by:

$\varphi(\bar{n}) = 0$ if n is even

$= 2$ if n is odd.

Show that φ is a homomorphism which is neither injective nor surjective.

24. If the index of a normal subgroup H of a group G is a prime number, then prove that G/H is cyclic.

25. Let $\varphi : G \to H$ be a homomorphism of groups. Show, by induction on n, that

$$\varphi(a^n) = (\varphi(a))^n \text{ for all } n \in \boldsymbol{Z}, a \in G.$$

26. Determine the group of automorphisms of:

(a) a cyclic group of order p where p is prime.

(b) a cyclic group of order n.

(c) an infinite cyclic group.

27. Show that the dihedral group of order 8 is isomorphic to its group of automorphisms.

28. Determine all the inner automorphisms of:

(i) The dihedral group of order 8,

(ii) The group Q of all quaternions,

and hence verify Theorem 6.3.4.

29. Give an example of a normal subgroup of a group which is not characteristic.

30. Find the derived group of:

(i) $G = \langle a, b, : a^4 = b^2 = (ab)^2 = 1 \rangle$,

(ii) $G = \langle a, b : a^2 = b^2 = (ab)^2 \rangle$.

and hence verify that the corresponding factor groups are abelian.

31. Show that the derived group of a non-abelian simple group coincides with that group.

32. Let G be a group and α be an automorphism of G. Let

$H = \{g \in G : g^\alpha = g\}$.

Show that H is a subgroup of G.

[H is called the *fixed point subgroup* of G under α.]

33. For any group G, the mapping $\varphi : G \to G$ given by:

$$\varphi(x) = x^2$$

is a homomorphism if and only if G is abelian.

34. Find two non-isomorphic groups whose automorphism groups are of order 2 and hence isomorphic.

35. Let H be a subgroup of a group G which contains the derived group G′ of G. Show that H is normal in G.

36. Show that, for any $a \in G$, $I_a : G \to G$ given by

$$I_a(x) = axa^{-1}, x \in G$$

is the identity automorphism if and only if $a \in \zeta(G)$.

37. Show that the mapping $x \to x^2$, $x \in G$, is an automorphism of G if G is abelian and of odd order.

38. Let A and B be subgroups of a group G and

$$[A, B] = \langle [a, b] : a \in A, b \in B \rangle$$

then prove that:

(i) A, B are permutable element-wise if and only if $[A, B] = \{e\}$.

(ii) $[A, B] = [B, A]$.

(iii) If A, B are normal subgroups of G, then [A, B] is normal in G and is contained in $A \cap B$.

39. Let $\varphi : G \to H$ be an epimorphism with K as its kernel. For any $v \in H$, let

$$K_v = \{g \in G : \varphi(g) = v\}$$

Show that

1. for each $g \in K_v$, $gK = K_v = Kg$

2. For $g_1, g_2 \in G$,

$$\varphi(g_1) = \varphi(g_2) \Leftrightarrow g_1K = g_2K.$$

[Here, for (1) use the equations $\varphi(gk) = \varphi(g) = v$ for all $g \in K_v$, $k \in K$ so that $gK \subseteq K_v$ etc.]

40. Let $(\mathbf{R}, +)$ and $(\mathbf{C}', .)$ be the groups of real and non-zero comples numbers. Let $\varphi : \mathbf{R} \to \mathbf{C}'$ be defined by:

$$\varphi(x) = (\cos x, \sin x), x \in \boldsymbol{R}.$$

Show that φ is a homomorphism which is neither injective nor surjective.

41. Let H be a subgroup of a group G. Let

$$K = \cup Ha,\ a \in N_G(H).$$

Show that K is a subgroup of G in which H is normal.

[Hint: Here $a \in N_G(H) \Leftrightarrow ah = h'a$ for each $h \in H$ and some $h' \in H$. Also for each $k \in K$, $k = h_1 a$ for some $h_1 \in H$.

So $khk^{-1} = h_1 ak^{-1} ak_1^{-1} = h,\ h'h_1 = h_2 \in H$.]

42. Let α be an automorphism of G which fixes only the identity element of G. Show that the mapping $\varphi : G \to G$ given by

$$\varphi(g) = \alpha(g) \cdot g^{-1},\ g \in G$$

is injective. Hence show that, if G is finite then, each element f G is of the form $\alpha(g)\, g^{-1}$.

43. Let H_1, H_2 be normal subgroups of G such that

$$G/H_1 \cong G/H_2.$$

Are H_1 and H_2 necessarily isomorphic?

Conversely if $H_1 \cong H_2$, are G/H_1, G/H_2, also isomorphic?

Chapter - VII

PRODUCTS OF GROUPS

Given two or more groups we can construct new groups in a variety of ways. Two much constructions are the direct product of groups and semi-direct product of groups. These, together with their properties, will be discussed in this chapter.

7.1. DIRECT PRODUCT OF GROUPS

In this section we discuss a group theoretic construction known as the *direct product of groups*. There are two kinds of direct products of groups namely the *internal* and *external direct products*. We first explain the concept of external direct product of groups.

Let A and B be group with identities e and e' respectively. The set

$$P = \{(a, b) : a \in A, b \in B\}$$

under the multiplication defined by:

$$(a, b)\,(a', b') = (aa', bb') \qquad (1)$$

is a group with (e, e') as the identity and (a^{-1}, b^{-1}) as the inverse of $(a, b) \in P$.

P is called the external direct product of the groups A and B and is denoted by $A \times B$.

A and B are called the *direct factors* of $A \times B$.

7.1.1. Theorem: Let $A \times B$ be the direct product of the groups A and B. Then the sets

$$\overline{A} = \{(a, e'); a \in A\}, \qquad \overline{B} = \{(e, b); b \in B\}$$

are normal subgroups of $A \times B$ isomorphic to A and B respectively and $\overline{A} \cap \overline{B} = \{(e, e')\}$.

Proof:

Let $\overline{a} = (a, e')$, $\overline{a}_1 = (a_1, e') \in \overline{A}$. Then:

$$\overline{a}\,\overline{a}_1^{-1} = (a, e')(a_1^{-1}, e') = (aa_1^{-1}, e')$$

belongs to $\overline{A}$. So $\overline{A}$ is a subgroup of $A \times B$.

Also for any $\overline{x} = (a_1, b_1) \in A \times B$

$$\begin{aligned}\overline{x}\,\overline{a}\,\overline{x}^{-1} &= (a_1, b_1)(a, e')(a_1^{-1}, b_1^{-1}) \\ &= (a_1 a a_1^{-1}, e') \\ &= (a', e'),\end{aligned}$$

where $a' = a_1 a a_1^{-1} \in \overline{A}$. So $\overline{x}\,\overline{a}\,\overline{x}^{-1} \in \overline{A}$ for all $\overline{x} \in A \times B$ and $\overline{a} \in A$. Therefore $\overline{A}$ is a normal subgroup.

Next, to establish an isomorphism between A and $\overline{A}$ we define a mapping $\varphi : A \to \overline{A}$ by:

$$\varphi(a) = (a, e'), a \in A$$

Then φ is obviously a bijective mapping. Moreover, for all $a, a' \in A$,

$$\begin{aligned}\varphi(aa') &= (aa', e') \\ &= (a, e')(a', e') \\ &= \varphi(a) \cdot \varphi(a')\end{aligned}$$

Hence φ is an isomorphism between A and $\overline{A}$.

Similarly it can be shown that $\overline{B}$ is a normal subgroup of $A \times B$ isomorphic to B.

Finally, to see that $\overline{A} \cap \overline{B} = \{(e, e')\}$, let $(a, b) \in \overline{A} \cap \overline{B}$. Then $(a, b) \in \overline{A}$ and $(a, b) \in \overline{B}$ which implies $b = e'$ and $a = e$ respectively. Hence $(a, b) = (e, e')$. Thus $\overline{A} \cap \overline{B} = \{(e, e')\}$, the identity subgroup of $A \times B$. Hence the theorem.

By the above theorem, A , $\overline{A}$ and B, $\overline{B}$ are respectively isomorphic and therefore structurally the same. Identifying $\overline{A}$ with A and $\overline{B}$ with B, we can write a for (a, e') and b for (e, b). With this convention, every element of P can be expressed as ab, $a \in A$, $b \in B$ because then

$$(a, b) = (a, e')(e, b) = ab.$$

The multiplication rule in $A \times B$ then becomes

$$ab \,.\, a'b' = aa' \,.\, bb' \qquad (2)$$

Using the above theorem we can now define the direct product as follows:

A group G is called the (internal) *direct product* of its subgroups A and B if and only if

(i) G is generated by A, B,

(ii) A, B are normal subgroups of G,

(iii) $A \cap B = \{e\}$ where e is the identity in G.

In general, a group G is the direct product of its subgroups $H_1, H_2, ..., H_k$ if and only if

1. G is generated by $H_1, H_2, ..., H_k$,
2. every H_i is normal in G,
3. H_i intersects the group generated by all H_j, $j = 1, 2, ..., k$, $j \neq i$, in the identity subgroup.

If G is the direct product of its subgroups $H_1, H_2, ..., H_k$, then each H_i, $i = 1, 2, ..., k$, is called a *direct factor* of G. Also we write G as

$$G = H_1 \times H_2 \times ... \times H_k.$$

7.1.2. Remarks:

1. For any two groups A and B the direct products $A \times B$ and $B \times A$ are isomorphic.
2. The process of forming direct products is associative. That is, for groups A, B and C, the direct products

$$(A \times B) \times C \text{ and } A \times (B \times C)$$

are isomorphic.

7.1.3. Example:

The four group $V = < a, b : a^2 = b^2 = (ab)^2 = 1 >$ is the direct product of its subgroups.

$$A = < a : a^2 = 1 >, B = < b : b^2 = 1 >$$

We now give another characterization of direct product.

7.1.4. Theorem: A group G is the direct product of its subgroups A and B if and only if

(i)′ Each element of A is permutable with every element of B,

(ii)′ every element of G is uniquely expressible as

$$g = ab,$$

$a \in A, b \in B$.

Proof: Suppose that G is the direct product of its subgroups A and B.

Let $a \in A, b \in B$ and consider the commutator $aba^{-1}b^{-1}$. Then

$$aba^{-1}b^{-1} = (aba^{-1})\, b^{-1} \in B \text{ ('B is normal in G)}$$
$$= a\,(ba^{-1}b^{-1}) \in A \text{ ('A is normal in G).}$$

So $aba^{-1}b^{-1} \in A \cap B = \{e\}$. Hence $aba^{-1}b^{-1} = e$. Thus

$$ab = ba$$

for all $a \in A, b \in B$. and (i)′ is satisfied.

Next, as G is generated by its subgroups A and B, each $g \in G$ is of the form

$$g = a_1^{\epsilon} b_1 a_2 b_2 \ldots a_k b_k^{\delta}$$

where ϵ, δ are 0 or 1. Using (i) we have

$$g = a_1^{\epsilon} a_2 \ldots a_k b_1 b_2 \ldots b_k^{\delta}$$
$$= ab$$

$a \in A, b \in B$.

To see that the expression (ii)′ is unique, let

$$g = ab = a'b'$$

$a, a' \in A, b, b' \in B$. Then

$$a'^{-1}a = b'b^{-1} \in A \cap B = \{e\}.$$

Hence $a = a', b' = b$ and the expression (ii)′ is unique.

Conversely, suppose that the subgroups A and B of G satisfy the conditions (i)′ and (ii)′. Then the requirement (i) is a part of (ii)′.

To prove (ii) let $a \in A$ and $g = a_1 b_1 \in G, a_1 \in A, b_1 \in B$. Then

$$gag^{-1} = (a_1b_1)\, a(a_1b_1)^{-1}$$
$$= a_1aa_1^{-1}\, b_1b_1^{-1} \qquad \text{by (i)}'$$
$$= a_1aa_1^{-1}$$

is an element of A. Hence A is normal in G. Similarly B is normal in G. Therefore (ii) is satisfied.

For (iii), let $x \in A \cap B$. Then $x \in A$ and $x \in B$ so that

$$x = a \,.\, e, \quad a \in A$$
$$= e \,.\, b, \quad b \in B$$

has two distinct expressions. One, therefore, must have $a = e$, $b = e$ by (ii)′. Hence $A \cap B = \{e\}$ and (iii) is satisfied.

The above theorem gives an alternative definition of the direct product.

More generally, a group G is the direct product of its subgroups $A_1, A_2, ..., A_k$ if and only if

(i)″ A_i is permutable with each A_j element-wise, $i \neq j$, $i, j = 1, 2, ..., k$. That is $a_i\, a_j = a_j\, a_i$ for all $a_i \in A_i$, $a_j \in A_j$, $i \neq j$.

(ii)″ every element of G has a unique expression as

$$a_1\, a_2 \ldots a_k,\ a_i \in A_i,\ 1 \leq i \leq k.$$

It was shown by example 4.1.2 that the relation of being a normal subgroup is, in general, not transitive. For certain subgroups of a direct product the situation is different as is shown by the following theorem:

7.1.5. Theorem: Every normal subgroup A′ of a direct factor A of a group G is normal in G.

Proof: Since A is a direct factor of G, there exists a subgroup B of G such that

$$G = A \times B.$$

Let $g \in G$. Then $g = ab$, $a \in A$, $b \in B$. So, for each $a' \in A'$,

$$ga'g^{-1} = (ab)a'(ab)^{-1}$$
$$= aba'b^{-1}\, a^{-1}$$
$$= aa'a^{-1},$$

As A′ is normal in A, $gag^{-1} = aa'a^{-1} \in A'$ for all $a' \in A'$, $g \in G$. Hence A′ is normal in G.

7.1.6. Theorem: If $G = A \times B$ and $\zeta(G)$, $\zeta(A)$, $\zeta(B)$ are the centres of G, A and B respectively, then

$$\zeta(G) = \zeta(A) \times \zeta(B).$$

Proof: Since A and B are permutable element-wise, $\zeta(A) \times \zeta(B)$ is permutable with A and B and therefore with G element-wise.

Hence

$$\zeta(A) \times \zeta(B) \subseteq \zeta(G). \qquad 7.1.6\ (1)$$

Conversely if $z \in \zeta(G)$, then for all $g \in G$, $zg = gz$.

In particular, $za = az$ for all $a \in A$ and $zb = bz$ for all $b \in B$. As

$$z = a'b', a \in A, b' \in B$$

we have

$$za = a'b'a = a'ab' \text{ and } az = aa'b'$$

so that $za = az$ implies $a'a = aa'$ for all $a \in A$. thus $a' \in \zeta(A)$. Similarly, $b' \in \zeta(B)$. Therefore $z = a'b' \in \zeta(A) \times \zeta(B)$. Consequently

$$\zeta(G) \subseteq \zeta(A) \times \zeta(B) \qquad 7.1.6\ (2)$$

Combining 7.1.6 (1) and 7.1.6 (2), we obtain

$$\zeta(G) = \zeta(A) \times \zeta(B).$$

7.1.7. Theorem: Let $G = A \times B$. Then $G' = A' \times B'$ where G′, A′, B′ are the commutator subgroups of G, A and B respectively.

Proof: Clearly each generator $[g, g_1]$ of G′ is such that

$$[g, g_1] = [ab, a_1b_1] = [a, a_1][b, b_1] \in A' \times B'.$$

Hence $G' \subseteq A' \times B'$.

Conversely, both A′ , B′ are subgroups of G′. So $A' \times B' \subseteq G'$.

Hence

$$G' = A' \times B'.$$

7.1.8. Theorem: Let $G = B \times A$. Then the factor group G/A is isomorphic to B.

Proof: Elements of G/A are of the form

$$gA = baA = bA,\ b \in B.$$

Define a mapping $\varphi : G/A \to B$ by:

$$\varphi(bA) = b.$$

Then φ is well defined because for $g = ba$, $g' = b'a'$ and $gA = g'A$ implies $bA = b'A$ so that $b'^{-1}b \in A$. But $b'^{-1}b \in B$. As $A \cap B = \{e\}$, $b'^{-1}b = e$ so that $b = b'$. Hence $\varphi(bA) = \varphi(b'A)$. φ is obviously bijective.

Next,

$$\begin{aligned}\varphi(bA \,.\, b'A) &= \varphi(bb'A)\\ &= bb'\\ &= \varphi(bA)\,.\,\varphi(b'A)\end{aligned}$$

Hence φ is an isomorphism between G/A and B, as required.

Let $G = A \times B$ and H be a subgroup of G. Then elements of H are of the form ab, $a \in A$, $b \in B$. Let

$$A_1 = \{a \in A : ab \in H \text{ for some } b \in B\},\ b \neq e$$

$$B_1 = \{b \in B : ab \in H \text{ for some } a \in A\}.\ a \neq e$$

Then, it is easy to see that $H \subseteq A_1 \times B_1$.

In general H is a proper subgroup of $A_1 \times B_1$.

To prove this, let $A = \{a : a^4 = 1 > B = < b : b^4 = 1 >$ and $G = A \times B$. Let $H = < ab : (ab)^4 = 1 >$. Then $H \subseteq G$. But in this case $A_1 = A$, $B_1 = B$ but $H \neq A_1 \times B_1 = G$ because $a \in G$, $a \notin H$.

A group which is expressible as the direct product of its proper subgroups is called *decomposable* (or decomposable into direct product). Thus a group G is *decomposable* into direct product if and only if there are proper subgroups A and B in G such that $G = A \times B$.

A group which is not decomposable is called *indecomposable*.

Among the indecomposable groups are cyclic groups whose order is a prime number and the group

$$G = < a, b : a^3 = b^2 = (ab)^2 = 1 >$$

The following theorem gives a class of decomposable groups.

7.1.6. Theorem: Every cyclic group whose order is a composite number is decomposable:

Proof: Let G be a cyclic group of order n where

$$n = p_1^{\alpha_1} \; p_2^{\alpha_2} \; \ldots \; p_k^{\alpha_k} . \; k \geq 2,$$

and let a be its generator. Put

$$q_i = p_1^{\alpha_1} \; p_2^{\alpha_2} \; \ldots \; p_{i-1}^{\alpha_{i-1}} \; p_{i+1}^{\alpha_{i+1}} \; \ldots \; p_k^{\alpha_k}$$

The group B_i generated by $b_i = a^{q_i}$ is of order $p_i^{\alpha_i}$

B_i intersects the group B'_i generated by all b_j, $j = 1, 2, \ldots, k$, $j \neq i$ in the identity subgroup because the orders of B_i and B_i' are co-prime. The group G' generated by all b_i, $i = 1, 2, \ldots, k$ is a subgroup of G and has the same order as that of G. Hence $G' = G$. However, in G' every B_i is normal because it is a subgroup of an abelian group. Also $B_i \cap B'_i = \{e\}$. Hence G' and therefore G is the direct product of the groups B_i. Of course $B_i \neq \{e\}$. Thus G is decomposable.

7.1.7. Example:

Let $G = < a; a^{60} = 1 >$. We can write 60 as $60 = 2^2 . 3.5$.

Let

$$B_1 = < b_1 = a^{15} : b_1^4 = 1 >,$$

$$B_2 = < b_2 = a^{20} : b_2^3 = 1 >,$$

$$B_3 = < b_3 = a^{12} : b_3^5 = 1 >.$$

Then $G = B_1 \times B_2 \times B_3$.

7.1.8. Theorem: Let C_m and C_n be cyclic groups of order m and n respectively, where m, n are relatively prime. Then $C_m \times C_n$ is a cyclic group of order mn.

Proof: Let $C_m = < a : a^m = 1 >$, $B = < b = b^n = 1$. Let $G = C_m \times C_n$. Then ab is an element of $C_m \times C_n$. Also

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

if and only if m |k, n|k. Since $(m, n) = 1$, $mn|k$. Moreover

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

Hence ab has order mn. Since $C_m \times C_n$ has mn elements,

$$< a, b : a^m = b^n = 1, ab = ba >$$

exhaust all of G. Hence G is cyclic of order mn.

7.2. NORMAL (OR SEMI-DIRECT) PRODUCTS

Closely related with the concept of direct product of groups is the notion of normal products or semi-direct products. This construction has been usefully employed in order to construct counter-examples to answer various questions in group theory.

A group G is called an *extension* of a group A by a group B if G has a normal subgroup A′ isomorphic to A such that G/A′ is isomorphic to B. For example, the group

$$G = < a, b : a^3 = b^2 = (ab)^2 = 1 >$$

is an extension of a cyclic group $A = < a : a^3 = 1 >$ of order 3 by a cyclic group $B = <b : b^2 = 1>$ of order 2. Also, as Theorem 7.1.8 shows, a direct product $A \times B$ is an extension of A by B.

It will be seen that a normal product also is an extension of a group by another group.

Let A and B be groups with identities e and e' respectively. Suppose that each $b \in B$ induces an automorphism α_b in A. Then, for each $a \in A$, the image $\alpha_b(a)$ is denoted by *conjugation* a^b for all $a \in A$ and $\alpha_b(a) = a^b$ is an element of A.

For $b_1, b_2 \in B$,

$$\alpha_{b_1 b_2}(a) = a^{b_1 b_2}$$

$$= (a^{b_2})^{b_1}$$

$$= b_1 a^{b_2} b_1^{-1}$$

$$= \alpha_{b_1}(a^{b_2})$$

$$= \alpha_{b_1}(\alpha_{b_2}(a))$$

$$= (\alpha_{b_1}\alpha_{b_2})(a)$$

for all $a \in A$. Hence

$$\alpha_{b_1 b_2} = \alpha_{b_1}\alpha_{b_2} \text{ and } a^{b_1 b_2} = (a^{b_2})^{b_1}. \qquad 7.2\ (1)$$

Also, as α_b is an automorphism.

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

Thus

$$(a_1 a_2)^b = a_1^b\, a_2^b. \qquad 7.2\ (2)$$

Consider the set G of all ordered pairs (a, b), $a \in A$, $b \in B$. Define an algebraic operation in G as follows:

For $(a_1, b_1), (a_2, b_2) \in G$, we put

$$(a_1, b_1)\,.\,(a_2, b_2) = (a_1 a_2^{b_1}, b_1 b_2). \qquad 7.2\ (3)$$

Since, for each $a \in A$, $b \in B$, $a^b \in A$, the multiplication given by 7.2 (3) is well-defined.

Now

(i) The algebraic operation defined by 7.2 (3) in G is associative.

For this, let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$. Then

$$[[(a_1, b_1)(a_2, b_2)](a_3, b_3)] = (a_1 a_2^{b_1}, b_1 b_2)(a_3, b_3), \quad \text{by 7.2 (3)}$$

$$= ((a_1 a_2^{b_1})\, a_3^{b_1 b_2}, (b_1 b_2) b_3), \quad \text{by 7.2 (3)}$$

$$= (a_1 \cdot (a_2^{b_1}\, a_3^{b_1 b_2}), b_1(b_2 b_3))$$

$$= (a_1 (a_2 a_3^{b_2})^{b_1}, b_1(b_2 b_3)), \quad \text{by 7.2 (1)}$$

$$= (a_1, b_1)(a_2 a_3^{b_2}, b_2 b_3), \quad \text{by 7.2 (3)}$$

$$= (a_1, b_1)\,[(a_2, b_2)(a_3, b_3)], \quad \text{by 7.2 (3).}$$

So the algebraic operation given by 7.2 (3) is associative.

(ii) The element (e, e') is the identity in G. For, let $(a, b) \in$ G. Then

$$(e, e')(a, b) = ((ea^{e'}), e'b), \qquad \text{by 7.2 (3)}$$
$$= (a, b)$$

where $a^{e'} = a$, as obtained from 7.2 (1) by taking $b_2 = b_1^{-1}$.

(iii) For each $(a, b) \in$ G, $((a^{-1})^{b^{-1}}, b^{-1})$ is its inverse. This is so because

$$((a^{-1})^{b^{-1}}, b^{-1})\,(a, b) = ((a^{-1})^{b^{-1}} \cdot a^{b^{-1}}, b^{-1}b), \qquad \text{by 7.2 (3)}$$
$$= ((a^{-1}a)^{b^{-1}}, e'), \qquad \text{by 7.2 (2)}$$
$$= (e, e'),$$

using $e^{b^{-1}} = e$, because the identity element is mapped onto itself under every automorphism.

Hence G is a group.

The group G obtained, in this way, from the groups A and B is called a normal product of A by B. Hence we have:

7.2.1. Theorem: If A and B are groups and e, e' are their respective identities and if each $b \in$ B induces an automorphism a^b in A, $a \in$ A, then the set

$$G = \{(a, b);\ a \in A, b \in B\}$$

is a group under the algebraic operation defined by:

$$(a_1, b_1)\,(a_2, b_2) = (a_1 a_2^{b_1}, b_1 b_2).$$

7.2.2. Theorem: Let G be the normal product of A and B. Then

(i) $A' = (\{(a, e');\ a \in A\}, B' = \{(e, b);\ b \in B\}$ are subgroups of G isomorphic to A and B respectively.

(ii) A′ is a normal subgroup of G.

(iii) the factor group G/A′ is isomorphic to B.

Proof: (i) Let $(a, e'), (a_1, e') \in A'$. Then $\left(\left(a_1^{-1}\right)^{e'}, e'\right) = (a_1^{-1}, e')$ is the inverse of (a_1, e') in A and

$$(a, e')(a_1^{-1}, e') = (aa_1^{-1}, e')$$

is again an element of A′. Hence A′ is a subgroup of G. Similarly B′ is a subgroup of G. To see that A′ is isomorphic to A, define a mapping $\alpha : A' \to A$ by:

$$\alpha(a, e') = a$$

for all $(a, e') \in A'$. Then α is obviously bijective.

Also, for $(a, e'), (a_1, e') \in A'$,

$$\begin{aligned}\alpha((a \cdot e')(a_1, e')) &= \alpha(a_1 a_2^{e'}, e') \\ &= \alpha(a_1 a_2, e') \\ &= a_1 a_2 \\ &= \alpha(a, e')\, \alpha(a_1, e')\end{aligned}$$

Hence α is an isomorphism between A′ and A.

Likewise the mapping $\beta : B' \to B$ defined by:

$$\beta(e, b) = b$$

is an isomorphism between B′ and B.

This proves (i).

For (ii) let $(a_1, e) \in A'$. Then for each $(a, b) \in G$.

$$\begin{aligned}(a, b)(a_1, e')(a, b)^{-1} &= (aa_1^b, b)\,((a^{-1})^{b^{-1}}, b^{-1}) \\ &= (aa_1^b\,((a^{-1})^{b^{-1}})^b, e') \\ &= (aa_1^b\, a^{-1}, e'),\end{aligned}$$

is an element of A′. Hence A′ is normal in G.

Lastly, to establish an isomorphism between G/A′ and B, define a mapping $\mu : G \to B$ by:

$$\mu(a, b) = b$$

for all $(a, b) \in G$. Clearly μ is sujective. Also for $(a, b), (a_1, b_1) \in G$.

$$\begin{aligned}\mu((a, b)(a_1, b_1)) &= \mu(aa_1^b, bb_1) \\ &= bb_1 \\ &= \mu(a, b) \cdot \mu(a_1, b_1).\end{aligned}$$

Hence μ is an epimorphism of G to B. If K is the kernel of μ then, by the fundamental theorem of homomorphism.

$$G/K \cong B.$$

We show that $K = A'$. Clearly $K \supseteq A'$. Conversely, let $(a, b) \in K$. Then

$$\mu(a, b) = b \qquad \text{by definition of } \mu$$
$$= e' \qquad \text{by assumption that } (a, b) \in K.$$

Hence $(a, b) = (a, e') \in A'$ and $K \subseteq A'$. Thus $K = A'$.

Therefore G/A' is isomorphic to B.

This completes the proof of the theorem.

Since A' is isomorphic to A and B' is isomorphic to B, it is often convenient to identify the elements of A' and B' with those of A and B respectively. So we put $(a, e') = a$ and $(e, b) = b$.

Then

$$(a, b) = (a, e')(e, b)$$
$$= (ae^{e'}, b)$$
$$= ab \qquad 7.2\ (4)$$

and the rule of composition in G becomes:

$$ab \,.\, a_1b_1 = aa_1^{b} \,.\, bb_1.$$

Hence every element of G can be expressed as ab, $a \in A$, $b \in B$ so that we can write $G = AB$. Now $A' \cap B' = \{(e, e')\}$ and according to the rule of identification $(e, e') = e = e'$ so that $A \cap B = \{e\}$. The expression 7.2 (4) is then unique; for if

$$ab = a'b'$$

$a' \in A$, $b' \in B$, then

$$a^{-1}a' = b'b^{-1}$$

is an element of $A \cap B = \{e\}$. Therefore $a = a'$, $b = b'$. Also, as before, A is a normal subgroup of G with G/A isomorphic to B. These remarks give us:

7.2.3. Theorem: A group G is a normal product of its subgroup A by a subgroup B if and only if

(a) A is normal in G

(b) $A \cap B = \{e\}$.

(c) G/A is isomorphic to B.

In the definition of a normal product, it was assumed that each element of B induces an automorphism in A. *The mapping φ which associates with each $b \in B$ an automorphism α^b of A given by $\alpha^b(a) = a^b$, $a \in A$, is a homomorphism of B into the automorphism group of A.*

For if $b, b' \in B$, then, by (1), $\alpha_{bb'} = \alpha_b \alpha_{b'}$. So

$$\varphi(bb') = \alpha_{bb'} = \alpha_b \alpha_{b'}.$$

Hence we obtain:

7.2.4. Theorem: If a group G is a normal product of a group A by a group B then there is a homomorphism of B into the automorphism group of A.

The preceding discussion includes the proof of the

7.2.5. Theorem: Let G be a group with a normal subgroup A and a subgroup B of G. Then the following statements about G, A and B are equivalent.

(i) G is a semidirect product of A by B.

(ii) $G = AB$ and $A \cap B = \{e\}$.

(iii) Each element g of G can be uniquely written as $g = ab$.

Notation: If a group G is a normal product of a group A by a group B corresponding to the automorphism φ of B induced by elements of B in A, then we write

$$G = A \ltimes_{\varphi} B.$$

7.2.6. Examples:

1. The dihedral group D_n is a normal product of a cyclic group C_n of order n by a cyclic group C_2 of order 2.

   Here, if $C_n = \langle a : a^n = 1 \rangle$ and $C_2 = (b: b^2 = 1)$, the mapping $\varphi: C_n \to C_n$ defined by:

   $$\varphi(x) = x^{-1}, \text{ for all } x \in C_n,$$

   is an automorphism of C_2 induced by b in C_n. Hence

$$D_n = C_n \ltimes_\varphi C_2.$$

2. Consider the cyclic groups $C_3 = < a : a^3 = 1 >$, $C_4 = < b : b^4 = 1 >$. Then C_4 induces an automorphism in C_3 given by $a \to (a)^b = a^2 = a^{-1}$. So the group having the presentation.

$$G = < a, b : a^3 = b^4 = 1, bab^{-1} = a^{-1} >$$

is the semidirect product of C_3 by C_4. G has order 12 but is not isomorphic to A_4.

If the homomorphim from C_4 to Aut (C_3) is taken as $a \to a^b = a$ then the semidirect product of C_3 by C_4 degenerates into the direct product of C_3 and C_4 and also has order 12.

These are the only semidirect products of C_3 by C_4.

3. Both the symmetric group S_3 and the cyclic group C_6 are semidirect products of C_3 by C_2 and correspond to the automorphis ms $a \to a^{-1}$ and $a \to a$ respectively.

Two homomorphi m φ, φ' from B to Aut (A) are said to be conjugate if there is some $\alpha \in$ Aut(A) such that $\alpha\varphi(b)\alpha^{-1} = \varphi'(b)$

for all $b \in B$.

For the next paragraph, instead of denoting the image of a under a homomorphism $\varphi : B \to$ Aut (A) by a^b, $b \in B$ and the product $((a_1, b_1)(a_2, b_2) = (a_1 a_2^{b1}, b_1 b_2)$, of two elements (a_1, b_1) and (a_2, b_2) let us write these as $\varphi(b)\, a$, $a \in A$ and as

$$((a_1, b_1)(a_2, b_2) = (a_1 \varphi(b_1)\, a_2, b_1 b_2)$$

respectively.

The following theorem relates isomorphic semidirect products of the group A by a group B.

7.2.7. Theorem: For two groups A and B and conjugate homomorphisms φ, φ' from B to Aut (A), the semidirect products of A by B determined by φ and of A by B determined by φ', respectively, are isomorphic.

Proof: Let $(a_1, b_1), (a_2, b_2) \in A \ltimes_{\varphi} B = G$. Define a mapping $\psi: G \to G' = A \ltimes_{\varphi'} B$ by

$$\psi(a, b) = (\alpha(a), (b)), (a, b) \in G.$$

Then

$$\begin{aligned}
\psi((a_1, b_1)(a_2, b_2) &= \psi(a_1\, \varphi(b_1)\, a_2, b_1 b_2)) \\
&= (\alpha(a_1)\, \alpha(\varphi(b_1)\, a_2), b_1 b_2) \\
&= (\alpha(a_1)\, (\alpha\varphi)(b_1)\, a_2), b_1 b_2) \\
&= (\alpha(a_1)\alpha(\varphi(b_1)\, \alpha^{-1}(\alpha(a_2)), b_1 b_2) \\
&= (\alpha(a_1))\alpha(\varphi(b_1)\, \alpha^{-1})(\alpha(a_2)), b_1 b_2) \\
&= (\alpha(a_1)\, \varphi'(b_1)\, \alpha(a_2), b_1 b_2) \\
&= \psi(a_1 \varphi'(b_1)\, a_2, b_1 b_2) \\
&= \psi(a_1, b_1)\, \psi(a_2, b_2).
\end{aligned}$$

Thus ψ is a homomorphism with an inverse mapping ψ^{-1} given by:

$$\psi^{-1}(a, b) = (\alpha^{-1}(a), b)$$

and so is an isomorphism.

A normal product of a group A by a group B is, in general, different from the normal product of B by A. However if every element of B induces the identity automorphism in A, that is, for any $b \in$ B,

$$a^b = a$$

for all $a \in$ A, then the normal product of A by B coincides with their direct product and is the *same* as the direct product of B and A.

Some authors use the words "split extension" to describe the notion of normal products.

Thus if G is a normal product of A by B then we also say that G is a *split extension* of A by B. G is then said to *split over* A.

The group B is called the *complement* of A.

Suppose that a group G contains subgroups A and B such that

$$G = AB \text{ and } A \cap B = \{e\}. \qquad (*)$$

One may, quite naturally, ask as to what kind of group G can be if the normality condition is dropped.

Such a group is called the *general product of A and B*. It is generally an interesting but very difficult problem to characterise one of the groups G, A or B satisfying the equation in (*) when the nature of the other two of these is known.

7.3. HOLOMORPH OF A GROUP

As stated earlier, the concepts of direct products and normal products are used to form new groups from old. In what follows, for any group G, we find a new group as a normal product of two groups.

Let G be a group and A(G) its group of automorphisms. Then the normal product of G by A(G) is called the *holomorph of G*.

Thus the holomorph H(G) of a group G is a group consisting of all ordered pairs

$$(g, \alpha)$$

$g \in$ G, $\alpha \in$ A(G) under the multiplication defined by:

$$(g, \alpha)(g', \alpha') = (gg'^{\alpha}, \alpha\alpha').$$

Here g'^{α} denotes the image of g' in G under the automorphism α.

By the remarks preceding theorem 6.6.3, every element of H(G) can be uniquely expressed as:

$$g\alpha$$

where $g\alpha$ is, in a certain sense, the product of $g \in$ G and α in A(G) with the product rule as:

$$g \cdot \alpha \cdot g' \cdot \alpha' = gg'^{\alpha} \alpha\alpha'$$

7.3.1. Examples:

Let V_4 be the four-group having the presentation:

$$V_4 = < a, b : a^2 = b^2 = (ab)^2 = 1).$$

The group of automorphisms of V_4 is the group

$$G = < \alpha, \beta : \alpha^3 = \beta^2 = (\alpha\beta)^2 = 1 >$$

where α, β are automorphisms of V_4 given by:

$$\alpha(a) = b, \alpha(b) = ab, \alpha(ab) = a, \alpha(1) = 1$$

and

$$\beta(a) = b, \beta(b) = a, \beta(ab) = ab, \beta(1) = 1.$$

Hence the holomorph of V_4 is the group consisting of elements of the form

$$xg$$

$x \in V_4$ and $g \in G$ with the multiplication rule defined as under.

$$xg.x_1g_1 = x\,x_1^g\,gg_1 \text{ where } x_1^g \text{ is the image of } x_1 \in V_4 \text{ under } g \in G.$$

The order of the holomouph of V_4 is 24.

7.4. GENERALIZED DIHEDRAL GROUP

Let A be an abelian group. The generalised dihedral group is a group Gdih (A) which is semidirect product of A by a cyclic group C_2 of order 2.

In the case when A is itself cyclic then Gdih(A) is the ordinary dihedral group, finite or infinite.

The structure of Gdih(A) can be different from the structure of A.

Thus if A is an elementary abelian 2-group, G dih(A) may or may not be an elementary abelian 2-group.

This is evident from example 7.3.1.

EXERCISES

1. Let H_1, H_2 be normal subgroups of G and $H = H_1 \cap H_2$. Show that G/H is isomorphic to a subgroup of $G/H_1 \times G/H_2$.

   [Hint: Consider the mapping $\varphi : G \to G/H_1 \times G_2/H_2$ defined by:

   $$\varphi(g) = (gH_1, gH_2)$$

   which is a homomorphism with H as its kernel.]

2. Show that the group $G = H \times K$ and $G_1 = K \times H$ are isomorphic.

3. Let G_1, G_2 be groups and H_i be normal subgroups of G_i, i = 1, 2. Show that the function $f : G_1 \times G_2 \to G_1/H_1 \times G_2/H_2$ defined by

   $$f(x, y) = (xH_1, yH_2)$$

   is a homomorphism and

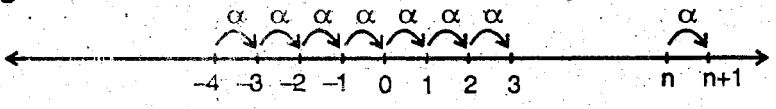
   $(G_1 \times G_2) / (H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2$.

4. Find all the subgroups of

   $$\mathbf{Z}_4 \times \mathbf{Z}_3, \quad \mathbf{Z}_4 \times \mathbf{Z}_6, \quad \mathbf{Z}_2 \times \mathbf{Z}_4.$$

5. Show that, for distinct primes p, q, $\mathbf{Z}_p \times \mathbf{Z}_q$ is cyclic. What can you say about $(\mathbf{Z}_m \times \mathbf{Z}_n)$ for natural numbers m and n such that (m, n) = 1?

6. Let $\mathbf{Z}$ be the set of integral points on the real line as indicated in fig. below



   Let $\alpha : \mathbf{Z} \to \mathbf{Z}$ and $\beta : \mathbf{Z} \to \mathbf{Z}$ be such that

   $$\alpha(n) = (n + 1).$$

while β rotates a point n clockwise about itself through an angle of 180°. Show that α has infinite order while β has order 2. Also show that $\alpha\beta = \beta\alpha$ and the group generated by α, β is $C \times C_2$.

7. Prove that if $G \times H$ is cyclic then both G and H are cyclic. However the converse is not true. Give an example.

8. Let $G = A \times B$ be a finite group. Show that $(ab)^k = 1$, $a \in A$, $b \in B$ if and only if k is a multiple of the orders of a and b.

9. Let $\{A_i: i = 1, 2, ..., n\}$ be a collection of groups and

$$G = \prod_{i=1}^{n} A_i$$

Let $\xi(A_i)$ be the centre of A_i, $i = 1, 2 ....., n$. Show that

$$\xi(G) = \prod_{i=1}^{n} \xi(A_i)$$

10.(*a*) Let Q be a group all of whose subgroups are normal and E_{p^n} be the direct product of n cyclic groups of order p. Let

$$G = Q \times E_{p^n}$$

Show that every subgroup of G in normal.

(*b*) Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of quaternions under multiplication and let $A = \{a: a^4 = 1\}$. Is there a subgroup of Q_8 which is isomorphic to A and is also a direct factor of Q_8?

11. Let $\{A_i : i = 1, 2, ..., k\}$ be groups and B_i be a normal subgroup of A_i, $i = 1, 2, ..., k$. Let

$$G = \prod_{i=1}^{n} A_i \text{ and } G' = \prod_{i=1}^{k} B_i.$$

Show that G' is normal in G.

12. Let A, B be groups and $A \ltimes B$, $A \times B$ be the normal and direct products of A, B respectively.

Show that the identity mapping $i : A \ltimes B \to A \times B$ is a group homomorphism if and only if B is normal in $A \times B$.

13. Show that the infinite dihedral group D_∞ is a normal product of an infinite cyclic group by a cyclic group of order 2.

14. One can define the direct product of two groups, one under addition and the other under multiplications as follows.

Let $G_1 = Z_6$, the group of integers under addition modulo 6 and

$$G_2 = \left\{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha\delta - \beta\gamma \neq 0\right\} \text{ under multiplication.}$$

Then the direct product of G_1 and G_2 consists of elements of the form

$$\left(a, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) : \alpha\delta - \beta\gamma$$

with the algebraic operation in P defined by:

$$\left(a, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)\left(a', \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}\right) = \left(a + a', \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}\right)$$

where $a + a'$ is sum of a, a' modulo 6 and the matrices are multiplied as usual.

(Note: However in such a case there is no harm in denoting the algebraic operation in the groups by the same symbol but keeping their inherent meaning.)

15. Give an example of an infinite group in which every element is of order 1 or 2. Show that this group is the direct product of an infinite number of certain groups.

16. Let H, K be normal subgroups of a group G such that $H \cap K = \{1\}$. Show that the subgroup generated by H and K in G is their direct product.

Chapter - VIII

GROUPS OF PERMUTATIONS

The theory of groups has gradually developed out of the groups of permutations (or symmetric groups) of some degree. It was shown in chapter IV. (Cayley's theorem 4.3.3) that every group is isomorphic to a group of bijective mappings (also called permutations) of a set. So the study of groups is the study of permutation groups of certain sets. In the subsequent paragraphs we briefly describe the nature of permutation groups.

8.1. SYMMETRIC OR PERMUTATION GROUPS

Let A be a finite or infinite set and let S be the collection of all bijective mappings of A. Using the fact that the product of two bijective mappings is bijective we find that S is *closed* under multiplication. Associative law in S follows from the usual associative law for multiplication for mappings. The identity mapping, that is the mapping which leaves every member of A fixed, is the identity element in S. Also the inverse on a bijective mapping is itself bijective and hence is a member of S. *Thus S is a group.* This group is called the *group of permutations or symmetric group* on A. The elements of S are called permutations of A.

A permutation φ in S is said to be *finitary* if and only if it moves only a finite number of elements of A. If A is a finite set then every permutation of A is finitary. If A is infinite then the *collection S' of all finitary permutations of A is a subgroup of S*, because the product of two finitary permutations is finitary and the inverse of finitary permutation is finitary. In fact S' *is a normal subgroup of S.*

The group S of all permutations of an infinite set is called the *unrestricted symmetric group* and the group S' of all finitary permutations is called the *restricted symmetric group.*

When A is a finite set consisting of n elements then the two concepts given above coincide and we have simply the symmetric group S_n.

The number n is called the *degree* of S_n.

Thus the symmetric group of degree n is the collection of all bijective mappings of a set consisting of n elements together with the usual multiplication of mappings as an algebraic operation in S_n.

Here we shall be concerned with permutation groups of finite degree only.

Let $A = \{x_1, x_2, ..., x_n\}$ and $\alpha \in S_n$. Then α is given by the equations.

$$\alpha(x_i) = x_{(i)\alpha} \qquad 8.1\ (1)$$

where i = 1, 2, ..., n and $(i)\alpha$ is one of the integers in {1, 2,..., n}. Equation (1) shows that each $\alpha \in S_n$ is uniquely determined by its action on the integers 1, 2,..., n which occur as suffices of elements in A. Thus, without any loss of generality, we can suppress the x's and consider only the suffices. That is, we take A = {1, 2,..., n] and α a mapping from A to A.

Here we denote the image of $i \in A$ under α by $(i)\ \alpha$. This is a deviation (only for the present chapter) from our earlier practice of writing the mapping to the left of an element of the domain and is hoped to make many a calculation not only more convenient but simpler as well.

With this convention the mapping $\alpha : A \to A$ will now be written as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)\alpha & (2)\alpha & (3)\alpha & \dots & (n)\alpha \end{pmatrix} = \begin{pmatrix} i \\ (i)\alpha \end{pmatrix} \qquad 8.1\ (2)$$

and every element of S_n will be taken in the form as given in equation 8.1(2).

Let $\beta \in S_n$ and

$$\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ (1)\beta & (2)\beta & \dots & (n)\beta \end{pmatrix} \qquad 8.1\ (3)$$

Since (i) $\alpha = j \in A$ and every element of A is uniquely determined by its effect on the elements of A, some (j) β occurs as the image of (i) α under β. We can write $(j)\beta$ as (i) $(\alpha\beta)$. Then β can be written as:

$$\beta = \begin{pmatrix} (1)\alpha & (2)\alpha & (3)\alpha & \dots & (n)\alpha \\ (1)(\alpha\beta) & (2)(\alpha\beta) & (3)(\alpha\beta) & \dots & (n)(\alpha\beta) \end{pmatrix} \qquad 8.1\ (4)$$

Using the representations 8.1 (2) and 8.1 (4), it is easy to write down the product of permutations α and β as

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

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

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ (1)(\alpha\beta) & (2)(\alpha\beta) & \dots & (n)(\alpha\beta) \end{pmatrix} = \begin{pmatrix} (i) \\ (i)(\alpha\beta) \end{pmatrix} \qquad 8.1\ (5)$$

The above remarks give a practical and useful technique for finding the product of two permutations.

Thus, to obtain the product of two permutations α and β given by 8.1 (2) and 8.1 (3) we re-arrange the elements in the upper row of 8.1 (3) so that this row becomes the lower row of 8.1 (2) and write down the corresponding images (i) $(\alpha\beta)$ of each (i)α under β in the second row of 8.1 (3), thereby getting β in the form given by 8.1 (4).

The product of α and β is then obtained simply by taking the upper row of α and the lower row of β in the new form as the upper and lower rows of $\alpha\beta$, as shown above.

The associative law for any triplet of permutations

$$\alpha = \begin{pmatrix} i \\ (i)\alpha \end{pmatrix}, \quad \beta = \begin{pmatrix} i \\ (i)\beta \end{pmatrix}, \quad \gamma = \begin{pmatrix} i \\ (i)\gamma \end{pmatrix}$$

follows from the equation

$$(\alpha\beta)\gamma = \alpha(\beta\gamma)$$

$$(\alpha\beta)\gamma = \left(\begin{pmatrix} i \\ (i)\alpha \end{pmatrix}\begin{pmatrix} i \\ (i)\beta \end{pmatrix}\right)\begin{pmatrix} i \\ (i)\gamma \end{pmatrix}$$

$$= \left(\begin{pmatrix} i \\ (i)\alpha \end{pmatrix}\begin{pmatrix} (i)\alpha \\ (i)(\alpha\beta) \end{pmatrix}\right)\begin{pmatrix} i \\ (i)\gamma \end{pmatrix}$$

$$= \begin{pmatrix} i \\ (i)(\alpha\beta) \end{pmatrix}\begin{pmatrix} i \\ (i)\gamma \end{pmatrix}$$

$$= \begin{pmatrix} i \\ (i)(\alpha\beta)\gamma \end{pmatrix} = \begin{pmatrix} i \\ (i)\alpha(\beta\gamma) \end{pmatrix} = \alpha(\beta\gamma).$$

The identity permutation of A is

$$I=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}=\begin{pmatrix}(1)\alpha & (2)\alpha & \dots & (n)\alpha\\ (1)\alpha & (2)\alpha & \dots & (n)\alpha\end{pmatrix} \qquad 8.1\ (7)$$

The inverse of a permutation α given by (2) is

$$\alpha^{-1}=\begin{pmatrix}(1)\alpha & (2)\alpha & \dots & (n)\alpha\\ 1 & 2 & \dots & n\end{pmatrix} \qquad 8.1\ (8)$$

Thus the collection of all permutations of a set A satisfies the axioms of a group and is therefore a group. This is the group which we have denoted by S_n. Its order is $n!$.

8.1.1. Examples: (i) Let A = {1, 2, 3}. Then the elements of the permutation group S_3 of A are

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

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

Hence $(1)\alpha=2$, $(2)\alpha=3$, $(3)\alpha=1$, $(1)\beta=2$, $(2)\beta=1$, $(3)\beta=3$.

To verify that the product of the permutation α and β is actually

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

we compute it by the method given above.

Thus
$$\alpha\beta=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$
$$=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}2 & 3 & 1\\ 1 & 3 & 2\end{pmatrix}$$
$$=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

Similarly for $\alpha^2\beta$.

(ii) The permutations

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

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

form a group.

It is the so-called *regular representation of Klein's* four-group generated by a and b and has the relations.

$$a^2 = b^2 = (ab)^2 = I$$

This is a subgroup of S_4.

Similarly, if $\mathbf{Z}_3$, is the additive group of residues mod 3, then

$$\alpha_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \alpha_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix},$$

define a regular representation of $\mathbf{Z}_3$. Here $G = \{\alpha_0, \alpha_1, \alpha_2\}$ and $\mathbf{Z}_3$ are isomorphic under the mapping f: $\mathbf{Z}_3 \to G$ given by

$$f(0) = \alpha_0, f(1) = \alpha_1, f(2) = \alpha_2$$

The permutation group S_n is non-abelian for $n \geq 3$. In example 8.1.1 (i) above, one can verify that, for the permutations

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

Also for $n > 3$, S_n contains the symmetric group S_{n-1} of degree $n - 1$ as a subgroup so that, for $n \geq 4$, S_n contains S_3 and so is non-abelian.

8.2. PERMUTABILITY OF PERMUTATIONS

We have seen that two given permutations in S_n may or may not commute. A permutation is said to *act non-trivially* (or, more simply, act) on a set A if it changes at least two elements of A. Otherwise it is said to *act trivially* on A. The following theorem gives a sufficient condition for the permutability of two permutations.

8.2.1. Theorem: Two permutations acting on mutually disjoint sets are permutable.

Proof: Let α and β be permutations of a set A which act on mutually disjoint subsets A_1 and A_2 of A respectively. Then the permutations $\alpha\beta$ and $\beta\alpha$ act only on the subset $X = A_1 \cup A_2$ of A and do not move any element of $A \setminus X$.

Let $x \in X$. Then $x \in A_1$ or $x \in A_2$. If $x \in A_1$ then x is mapped onto $x' \in A_1$ under $\alpha\beta$. But x goes to x' under $\beta\alpha$ as well. Similarly, if $x \in A_2$ the action of $\alpha\beta$ and $\beta\alpha$ on x is the same. Hence $\alpha\beta$ and $\beta\alpha$ have the same effect on any element of X. So $\alpha\beta = \beta\alpha$.

8.2.2. Illustration:

Let $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$.

Then a acts only on {1, 2} while b acts only on {3, 4} and these sets are mutually disjoint. Hence $ab = ba$. This fact can also be verified by direct multiplication. Here

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

Similarly the permutations

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}, d = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix},$$

which act on mutually disjoint sets {1, 2, 3} and {4, 5, 6} alone, are permutable.

8.3. CYCLIC PERMUTATIONS AND ORBITS

Let A be a set and $x_1, x_2, \ldots, x_r \in A$. A permutation φ on A is called a *cyclic permutation* or simply a *cycle* if and only if φ takes x_1 to x_2, x_2 to x_3, and so on, x_r to x_1, while it keeps other members of A fixed. It is denoted by $(x_1, x_2, \ldots, x_r)$. The cycles

$$(x_1, x_2, \ldots, x_r), (x_2, x_3, \ldots, x_r, x_1), \ldots, (x_r, x_1, x_2, \ldots, x_{r-1})$$

are all one and the same permutations. The subset

$$A' = \{x_1, x_2, \ldots, x_r\}$$

of A is called the *φ-orbit* of any of the elements of A'.

For example

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

is a cyclic permutation and the set {1, 2, 3} is the φ-orbit of 1. [1, 2, 3] is the φ-orbit of 2 and 3 as well.

If $\varphi = (x_1, x_2, ..., x_r)$ is a cyclic permutation then the number r is said to be the *length of* that cycle. For example, the permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 8 & 9 & 5 \end{pmatrix}$$

are cycles of length 4 and 5, respectively.

The fact that the cyclic permutations are important in the discussion on permutation groups of finite degree is apparent from the following fundamental theorem for permutations.

8.3.1. Theorem: Every permutation of degree n is decomposable in a *unique* way into a product of cyclic permutations acting on mutually disjoint sets, apart from the order in which these cycles are taken.

Proof: Let α be a permutation of degree n and x_1 be one of the elements on which α acts. Suppose α sends x_1 to x_2, x_2 to x_3 and so on. As n is finite, there is an integer p, $1 \leq p \leq n$ such $(x_p)\ \alpha = x_1$. Thus a part of the effect of α is equal to the cyclic permutation

$$\alpha_1 = (x_1, x_2, ..., x_p).$$

If $p = n$ then $\alpha = \alpha_1$ is a cycle of length n and we are through.

However, if $p < n$ there is some y_1 different from $x_1, x_2, ..., x_p$ on which α acts. Arguing as before, let α take y_1 to y_2, y_2 to y_3 and so on. Again there is some integer q such that $(y_q)\ \alpha = y_1$. The y's so obtained must be different from x's for otherwise α will have two images for one and the same element. Thus the sets

$$\{x_1, x_2, ..., x_p\}\ ,\ \{y_1, y_2, ..., y_q\}$$

are disjoint. Moreover, a part of the effect of α will be the product $\alpha_1\ \alpha_2$ of the cycles α_1 and α_2 where

$$\alpha_2 = (y_1, y_2, ..., y_q).$$

If $p + q = n$ we have α as the product of cyclic permutations. But if $p + q < n$, we continue the process of extracting, each time, a cyclic permutation from α.

As the degree n of α is finite, this process must end after a finite number of such steps so that we finally obtain α as *a* product of cyclic permutations.

Let a decomposition of α be

$$\alpha = (x_1, x_2, ..., x_p)(y_1, y_2, ...y_q) ... (z_1, z_2, ..., z_r) \qquad 8.3.1 \text{ (i)}$$

where $p + q + ... + r = n$ and the cycles act on mutually disjoint sets. Since two cycles acting on mutually disjoint sets are permutable, the expression in (i) is unique apart from the order in which these cycles are taken. Hence the theorem.

8.3.2. Example: Consider the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 5 & 1 & 6 & 7 & 3 & 9 & 10 & 8 \end{pmatrix}$$

Then

$$\alpha = (1\ \ 2\ \ 4)\,(3\ \ 5\ \ 6\ \ 7)\,(8\ \ 9\ \ 10) \qquad 8.3.2 \text{ (ii)}$$

Similarly the permutation

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

has decomposition as

$$\beta = (1\ \ 2)\,(3)\,(4\ \ 5\ \ 6)\,(7)\,(8) \qquad 8.3.2 \text{ (iii)}$$

which we also write as $\beta = (1\ \ 2)\,(4\ \ 5\ \ 6)$, ignoring cycles of length one which are just the identity permutations.

Suppose that a permutation α of degree n is decomposable into disjoint cycles of lengths (including cycles of length 1).

$$s_1, s_2, ..., s_k$$

We may assume that

$$s_1 \le s_2 \le ... \le s_k.$$

It is easy to see that

$$s_1 + s_2 + ... + s_k = n. \qquad 8.3.2 \text{ (1)}$$

The ordered k-tuple $(s_1, s_2, ..., s_k)$ is called the *type* of the permutation α.

For example if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 2 & 5 & 3 & 4 & 8 & 6 & 7 & 10 & 12 & 9 & 11 \end{pmatrix}$$

$$= (1)\ \ (2)\ \ (3\ \ 5\ \ 4)\ \ (6\ \ 8\ \ 7)\ \ (9\ \ 10\ \ 12\ \ 11)$$

then α is of type

$$(1,\ 1,\ 3,\ 3,\ 4).$$

Suppose that in the decomposition of a permutation α of degree n into disjoint cycles there are q_s cycles of length s (s = 1, 2, ...) where we assume $q_i = 0$ if α contains no cycles of length i. Then, since a cycle of length s contains exactly s elements, we have the equation

$$q_1 + 2q_2 + 3q_3 + \ldots = n. \qquad 8.3.2\ (2)$$

Thus the number of disjoint types among the permutations of degree n is equal to the number of non-negative integral solutions of (2).

8.3.3. Theorem: Two permutations α and β in S_n are conjugate if and only if they are of the same type.

Proof: Suppose that $\alpha, \beta \in S_n$ are of the same type. Then

$$\alpha = (x_1, x_2, \ldots, x_p)(y_1, y_2, \ldots, y_q) \ldots (z_1, z_2, \ldots, z_r)$$

$$\beta = (x_1', x_2', \ldots, x_p')(y_1', y_2', \ldots, y_q') \ldots (z_1', z_2', \ldots, z_r')$$

Consider the permutation

$$\gamma = \begin{pmatrix} x_1' x_2' \ldots x_p' & y_1' y_2' \ldots y_q' \ldots z_1' z_2' \ldots z_r' \\ x_1 x_2 \ldots x_p & y_1 y_2 \ldots y_q \ldots z_1 z_2 \ldots z_r \end{pmatrix}$$

Then

$$\gamma\alpha\gamma^{-1} = \beta$$

so that α and β are conjugate. Here, under $\gamma\alpha\gamma^{-1}$,

$$x_i' \to x_i \to x_{i+1} \to x'_{i+1}.$$

Conversely, suppose that α and β are conjugate. Then there is a permutation $\gamma \in S_n$ such that

$$\beta = \gamma\alpha\gamma^{-1}.$$

Suppose that

$$\alpha = \begin{pmatrix} i \\ (i)\alpha \end{pmatrix}$$

$$= (x_1, x_2, \ldots, x_p)(y_1, y_2, \ldots, y_q) \ldots (z_1, z_2, \ldots, z_r)$$

and $\gamma = \begin{pmatrix} i \\ (i)\gamma \end{pmatrix}$

$= (u_1, u_2, ..., u_s)\ (v_1, v_2, ..., v_t) \ldots (w_1, w_2, ..., w_u)$

Then, as γ can also be written like $\gamma = \begin{pmatrix} (i)\gamma^{-1} \\ i \end{pmatrix}$, we have

$$\beta = \begin{pmatrix} (i)\gamma^{-1} \\ i \end{pmatrix} \begin{pmatrix} i \\ (i)\alpha \end{pmatrix} \begin{pmatrix} i \\ (i)\gamma^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} (i)\gamma^{-1} \\ (i)\alpha \end{pmatrix} \begin{pmatrix} i \\ (i)\gamma^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} (i)\gamma^{-1} \\ (i)\alpha \end{pmatrix} \begin{pmatrix} (i)\alpha \\ ((i)\gamma^{-1})\alpha \end{pmatrix}$$

$$= \begin{pmatrix} (i)\gamma^{-1} \\ ((i\gamma^{-1}))\alpha \end{pmatrix} \begin{pmatrix} j \\ (j)\alpha \end{pmatrix}$$

where $j = (i)\gamma^{-1}$. Here we have used the equation that

$$\begin{pmatrix} i \\ (i)\alpha \end{pmatrix} = \begin{pmatrix} (i)\delta \\ ((i)\delta)\alpha \end{pmatrix} \text{ for all } \delta \in S_n.$$

So $\beta = \begin{pmatrix} j \\ (j)\alpha \end{pmatrix}$ with $j = (i)\gamma^{-1}$.

Thus

$\beta = (x_1\gamma^{-1}, x_2\gamma^{-1}, ..., x_p\gamma^{-1})\ (y_1\gamma^{-1}, y_2\gamma^{-1}, ..., y_q\gamma^{-1}) \ldots$
$(z_1\gamma^{-1}, z_2r^{-1}, ..., z_r\gamma^{-1})$

Hence α and β are of the same type.

8.3.4. Example: Suppose that

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 1 & 3 & 7 & 8 & 5 & 6 & 4 & 11 & 9 & 10 \end{pmatrix} = \begin{pmatrix} i \\ (i)\alpha \end{pmatrix}$$

$$= (1\ 2)\ (3)\ (4\ 7\ 6\ 5\ 8)\ (9\ 11\ 10)$$

and $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 2 & 1 & 5 & 8 & 7 & 4 & 6 & 10 & 11 & 9 \end{pmatrix}$

$$= (1\ 3)\ (2)\ (4\ 5\ 8\ 6\ 7)\ (9\ 10\ 11)$$

Then

$$\gamma\alpha\gamma^{-1} = \begin{pmatrix} (\mathrm{i})\,\gamma^{-1} \\ ((\mathrm{i})\,\gamma^{-1})\alpha \end{pmatrix}$$

$$= ((1\gamma^{-1})(2\gamma^{-1})(3\gamma^{-1}))((4\gamma^{-1})(7\gamma^{-1}) \quad (6\gamma^{-1}) \quad (5\gamma^{-1}) \quad (8\gamma^{-1}))\,((9\gamma^{-1}) \quad (11\gamma^{-1}) \quad (10\gamma^{-1})$$

$$= (3 \quad 1)\ (2)\ (7 \quad 6 \quad 8 \quad 4 \quad 5)\ (11 \quad 10 \quad 9)$$

$$= (1 \quad 3)\ (2)\ (4 \quad 5 \quad 7 \quad 6 \quad 8)\ (9 \quad 11 \quad 10)$$

which is of the same type as of α.

Since the number of distinct types among the permutations of degree n is equal to the number of non-negative integral solutions of equation $q_1 + 2q_2 + 3q_3 \ldots = n$ and two permutations of different types cannot be conjugate, *the number of conjugacy classes in S_n is equal to the number of non-negative integral solutions of the above equation* 8.3.2 (2).

8.4. ORDER OF A PERMUTATION

By the order of a permutation α we mean the least positive integer m such that

$$\alpha^m = I,$$

the identity permutation.

8.4.1. Theorem: The order of a cyclic permutation of length m is m.

Proof: Let $\varphi = (x_1, x_2, \ldots, x_m)$ be a cyclic permutation of length m. The element x_1 is mapped onto x_2, x_3, ..., x_m, x_1 respectively under $\varphi, \varphi^2, \ldots, \varphi^{m-1}, \varphi^m$. Similarly x_2 is mapped onto x_2 under φ^m, and so on, x_m is mapped onto x_m under φ^m. Hence $\varphi^m = I$.

Of course m is the least such integer. Hence the result.

Now consider an arbitrary permutation α of degree n. By Theorem 8.3.1, α is expressible as a product of disjoint cyclic permutations $\alpha_1, \alpha_2, \ldots, \alpha_k$ (say) of lengths (and hence also of order) $m_1, m_2, \ldots, m_k$ respectively. These disjoint cycles are permutable with one another. Hence, if m is the least common multiple of m_i, i = 1, 2, ..., k, then $m = m_i q_i$ so that

$$\alpha^m = \alpha_1^m \alpha_2^m \ldots \alpha_k^m$$
$$= I$$

(because $\alpha_i^{m_i} = (\alpha_i^{m_i})^{q_i} = 1$). Obviously m is the least positive integer satisfying $\alpha^m = I$.

We therefore have:

8.4.2. Theorem: The order of a permutation is the least common multiple of the orders of the disjoint cyclic permutations into whose product it is decomposed.

8.5. TRANSPOSITIONS, EVEN AND ODD PERMUTATIONS

A cycle of length 2, that is a cycle of the form $(x\ y)$, is called a *transposition*. Clearly

$$(x\ y)^2 = I$$

so that

$$(x\ y) = (x\ y)^{-1} = (y\ x)$$

8.5.1. Theorem: Every cyclic permutation can be expressed as a product of transpositions.

Proof: Let

$$\varphi = (x_1, x_2, \ldots, x_k)$$

be a cyclic permutation. Consider the permutation

$$(x_1\ x_2)\ (x_1\ x_3) \ldots (x_1\ x_k) \qquad 8.5.1\ (1)$$

which is such that under this permutation

$$x_1 \to x_2,\ x_2 \to x_1 \to x_3, \text{ that is } x_2 \to x_3$$

and so on

$$x_{k-1} \to x_1 \to x_k, \text{ that is } x_{k-1} \to k_k \text{ and } x_k \to x_1.$$

Thus the effect of φ and the permutation in (1) on the set $\{x_1, x_2, \ldots, x_k\}$ is the same. Hence these are equal and so

$$\varphi = (x_1\ x_2)\ (x_1\ x_3) \ldots (x_1\ x_k)$$

8.5.2. Corollary: Every permutation can be expressed uniquely as a product of transpositions.

Proof: Since each permutation, by Theorem 8.3.1, is the product of cyclic permutations and each cyclic permutation is a product of transpositions, so every permutation is expressible as a product of transpositions *taken in that particular order.*

8.5.3. Corollary: A cyclic permutation of length m is a product of (m – 1) transpositions.

Proof: This is obvious. Just count the number of transpositions in expression (1) of Theorem 8.5.1.

With each permutation α one can associate a fixed positive integer m_α as follows.

Let α be expressed as a product of k cycles α_i, each of length m_i, respectively, $i = 1, 2, ..., k$. Every α_i is a product of $(m_i - 1)$ transpositions. Thus α is a product of

$$(m_1 - 1) + (m_2 - 1) + ... + (m_k - 1) = m_\alpha \quad 8.5.3\ (2)$$

transpositions.

Here m_α is a positive integer.

A permutation α is said to be *even or odd* according as m_α is even or odd.

Since each cycle of length m is a product of (m – 1) transpositions, the number m_α, given by 8.5.3 (2), is the number of transpositions in α. Thus a *permutation α is even or odd according as it is a product of an even or an odd number of transpositions.*

In particular, a cycle of length m is even or odd according as m is odd or even respectively.

If $\alpha = I$ then $m_\alpha = 0$. Hence I is an even permutation.

For any permutations α and β the product $\alpha\beta$ contains $m_\alpha + m_\beta - 2k$ transpositions, where k is an integer. Thus if α and β are even permutations then $\alpha\beta$ is an even permutation. Also the inverse of an even permutation is an even permutation. Since the inverse of a cyclic

permutation of length m is a cycle of length m so the integer m_α associated with a permutation α remains unchanged if α^{-1} replaces α.

Let A_n denote the set of all even permutations in S_n. Then, because of the remarks given above, we have:

8.5.4. Theorem: The set A_n of all even permutations in S_n is a subgroup of S_n.

The subgroup A_n of S_n which consists of all even permutations in S_n is called the *alternating group* of degree n.

Since a permutation is either even or odd and a transposition is an odd permutation, so if we multiply elements of A_n by a transposition we get odd permutations in S_n and vice-versa. Hence there is an equal number of even and of odd permutations in S_n. As the order of S_n is n!, the order of A_n is $(1/2)n!$ Thus A_n has index 2 in S_n and hence is normal in S_n.

This yields us Theorem 8.5.5. given below.

The following rules for the product of two permutations are easily verifiable:

(a) The product of two even permutations is even.

(b) The product of an even and an odd permutation is odd.

(c) The product of two odd permutations is even.

We then have another proof of the normality of A_n.

8.5.5. Theorem: The alternating group A_n of degree n is a normal subgroup of S_n and has order $(1/2)n!$

Proof: We shall prove this theorem by showing that A_n has index 2 in S_n.

Define a mapping $f : S_n \to \{1, -1\}$, which is a group under multiplication, as follows:

For each $\alpha \in S_n$, we put

$$f(\alpha) = 1 \text{ if } \alpha \text{ is even}$$
$$= -1 \text{ if } \alpha \text{ is odd.}$$

Then f is surjective. We show that f is a homomorphism.

Let $\alpha, \beta \in S_n$. Then we examine the following possibilities.

(i) α and β both are even.

(ii) α is even and β is odd and vice versa.

(iii) α and β both are odd.

For case (i), $\alpha\beta$ is even. So

$$f(\alpha\beta) = 1 = 1.1 = f(\alpha).f(\beta).$$

In case (ii), $\alpha\beta$ is odd. So

$$f(\alpha\beta) = -1 = 1(-1) = f(\alpha).f(\beta).$$

Fore case (iii), $\alpha\beta$ is even. So

$$f(\alpha\beta) = 1 = -1 . -1 = f(\alpha).f(\beta).$$

Thus f is a homomorphism of S_n onto $\{1, -1\}$ with A_n as its kernel. By the fundamental theorem of homomorphism,

$$S_n / A_n \cong \{1, -1\}.$$

So A_n has index 2. Thus the order of A_n is $(1/2)n!$

Another proof of Theorem 8.5.5, which is, in fact, a detailed explanation of the remarks preceding it, is given below:

It has already been shown that A_n is a subgroup of S_n. To show that A_n is normal in S_n we prove that A_n has index 2 in S_n:

Let $(x_1\ x_2)$ be a transposition in S_n and consider the set

$$S = A_n \cup (x_1\ x_2)A_n \qquad 8.5.5\ (1)$$

where $(x_1\ x_2)\ A_n$ is a left coset of A_n determined by $(x_1\ x_2)$. Obviously

$$S \subseteq S_n. \qquad 8.5.5\ (2)$$

Conversely, let $\alpha \in S_n$. then α is either even or odd. If α is even $\alpha \in A_n$ and hence to S. If α is odd then $(x_1, x_2)\alpha$ is even and therefore in A_n.

Now $\alpha = (x_1\ x_2)((x_1\ x_2)\alpha)$.

Hence $\alpha \in (x_1\ x_2)\ A_n$ and again $\alpha \in S$. So

$$S_n \subseteq S. \qquad 8.5.5\ (3)$$

From 8.5.5 (2) and 8.5.5 (3) we have $S = S_n$. Hence A_n has index 2 in S_n. So A_n is normal in S_n and has order $(1/2)n!$.

8.5.6. Examples:

(i) The alternating group A_3 of S_3 consists of the permutations

I, (1 2 3), (1 3 2).

(ii) S_4 has the following 24 elements

(a) I, (1 2) (3 4), (1 3) (2 4), (1 4) (2 3), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3).

(b) (1 2), (1 3), (1 4), (2 3), (2 4), (3 4),
(1 2 3 4), (1 2 4 3) (1 3 2 4), (1 3 4 2)
(1 4 2 3), (1 4 3 2).

All permutations in (a) are even while those in (b) are all odd. So A_4 consists of the elements listed in (a).

The elements

I, (1 2) (3 4), (1 3) (2 4), (1 4) (2 3)

form a normal subgroup of A_4.

This is the only proper normal subgroup of A_4.

It should be interesting to note that A_4 has no subgroup of order 6, for such a subgroup, being of index 2 in A_4, is normal in A_4. But, as in (a), no subset consisting of any six elements in (a) forms a subgroup. So A_4 has no normal subgroup of order 6.

This example also shows that the converse of the Lagrange's theorem for finite groups does not hold.

Thus *if* the order of a finite group is divisible by some integer k, the group may not necessarily have a subgroup of order k.

8.6. GENERATORS OF THE SYMMETRIC AND ALTERNATING GROUP

Let S_n be the symmetric group on n symbols 1, 2, ..., n. We have seen that every element of S_n can be expressed as a product of transpositions. Hence a subset of these transpositions must be a system of generators for S_n.

The following theorem gives one such set of generators.

8.6.1. Theorem: The symmetric group S_n is generated by the transpositions

$$(12),\ (13),\ ...,\ (1\ n).$$

Proof: It is obvious that all the transpositions

$$(12),\ (13),\ ...,\ (1\ n) \qquad 8.6.1\ (i)$$

are elements of S_n. Since every element of S_n is a product of transpositions, by corollary 7.5.2 of Theorem 7.5.1, and an arbitrary transposition (ab) can be expressed as

$$(a\ b) = (1\ a)\ (1\ b)\ (1\ a),$$

so every element of S_n can be expressed as a product of transpositions from (i). So (i) is a system of generators for S_n.

8.6.2. Corollary: S_n can be generated by the transpositions

$$(1\ \ 2),\ (2\ \ 3),\ ...,\ (n-1,\ n).$$

Proof: Let $H = <(1\ \ 2),\ (2\ \ 3),\ ...,\ (n-1,\ n)>$. Then $H \subseteq S_n$. To see that $S_n \subseteq H$ we have only to check the equations

$$(1\ \ 3) = (1\ \ 2)\ (2\ \ 3)\ (1\ \ 2)$$

$$(1\ \ 4) = (1\ \ 3)\ (3\ \ 4)\ (1\ \ 3)$$

and so on

$$(1\ \ n) = (1,\ n-1)\ (n-1,\ n)\ (1,\ n-1)$$

These equations are easily verifiable by actual computation. Hence $S_n \subseteq H$. Thus

$$S_n = H = <(1\ \ 2), (2\ \ 3), ..., (n-1, n)>.$$

8.6.3. Corollary: S_n is generated by the permutations

$$(1\ \ 2), (1\ \ 2\ \ 3 \ldots n).$$

Proof: Let $H = <(1\ \ 2), (1\ \ 2\ \ 3 \ldots n)>$. Then $H \subseteq S_n$.

Conversely, to show that $S_n \subseteq H$, we prove that the generators of S_n, given in corollary 8.6.2, are expressible as products of generators for H. This follows from the following equations which can be verified by actual computation.

$$(2\ \ 3) = (1\ \ 2\ \ 3 \ldots n)^{-1}\,(1\ \ 2)\,(1\ \ 2\ \ 3 \ldots n)$$

$$(3\ \ 4) = (1\ \ 2\ \ 3 \ldots n)^{-1}\,(2\ \ 3)\,(1\ \ 2\ \ 3 \ldots n)$$

and so on

$$(n-1, n) = (1\ \ 2\ \ 3 \ldots n)^{-1}\,(n-2, n-1)\,(1\ \ 2\ \ 3 \ldots n).$$

Hence $S_n \subseteq H$. So

$$S_n = H = <(1\ \ 2), (1\ \ 2\ \ 3 \ldots n)>.$$

8.6.4. Theorem: For $n \geq 3$, A_n is generated by cycles of length 3.

Proof: When $n = 3$, $A_3 = \{I, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$ so that A_3 is generated by $(1\ \ 2\ \ 3)$, that is, by a 3-cycle.

Suppose that $n \geq 4$. Then every element of A_n, being an even permutation, is the product of an even number of transpositions. We show that the product of any pair of transpositions is either a cycle of length 3 or else is the product of two cycles of length 3.

Now an arbitrary pair of transpositions is either of the form $(a\ b)$, $(b\ c)$ or of $(a\ b)$, $(c\ d)$, a, b, c, d all different. In the first case

$$(a\ b)\,(b\ c) = (a\ b\ c)$$

and in the second case

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

So every element of A_n is a product of cycles of length 3. Hence A_n is generated by cycles of length 3.

The following theorem shows that the number of 3-cycles generating A_n can be reduced.

8.6.5. Theorem: A_n is generated by (n – 2) 3 - cycles

(1 2 3), (1 2 4), ..., (1 2 n).

Proof: Let H = < (1 2 3), (1 2 4), ..., (1 2 n) >. Clearly $H \subseteq A_n$.

Conversely, as A_n is generated by the 3-cycles, to prove that $A_n \subseteq$ H, it is enough to show that each cycle of length 3 is in H.

But an arbitrary 3-cycles can be written as

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

and
$$(a\ \ b) = (1\ \ a)(1\ \ b)(1\ \ a)$$
$$(a\ \ c) = (1\ \ a)(1\ \ c)(1\ \ a).$$

So
$$(a\ \ b\ \ c) = (1\ \ a)(1\ \ b)(1\ \ c)(1\ \ a)$$
$$= (1\ \ a\ \ b)(1\ \ c\ \ a).$$

Hence we show that each of $(1\ \ a\ \ b)$ and $(1\ \ c\ \ a)$ is in H. If a = or $b = 2$ then $(1\ \ a\ \ b) \varepsilon$ H. So we assume that $2 \neq a \neq b$. But

$$(1\ \ a\ \ b) = (1\ \ 2\ \ b)(1\ \ 2\ \ a)(1\ \ 2\ \ b)^{-1}$$

which is in H. Similarly $(1\ \ c\ \ a) \varepsilon$ H. Hence $(a\ \ b\ \ c) \varepsilon$ H so that $A_n \subseteq$ H.

Consequently

$$A_n = H = < (1\ \ 2\ \ 3), (1\ \ 2\ \ 4), ..., (1\ \ 2\ \ n) >.$$

The theorems which follow now are basically concerned with the structure of the alternating group A_n, $n \geq 3$. As defined earlier, a simple group is one which has no proper normal subgroup. It has already been shown that A_n is a normal subgroup of S_n. For n = 1, $S_1 = \{I\}$. For n = 2, S_2 has order 2 and $A_2 = \{I\}$. For n = 3, S_3 has order 6 and A_3 is a cyclic group of order 3. So A_3 is simple. When n = 4. S_4 has 24 elements while A_4 has order 12. A_4 has the unique normal group

$$\{I, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)$$

of order 4 so that A_4 is not simple.

Does A_n have a normal subgroup for any $n \geq 5$?

The answer to this question is in the negative. That is, we will show that, for $n \geq 5$, A_n is simple.

We have already shown that for $n \geq 3$, A_n is generated by cycles of length 3. However, to prove our main theorem, we need another auxiliary result.

Before stating that result we make the following observation.

A permutation

$$\alpha = \begin{pmatrix} i \\ (i)\ \alpha \end{pmatrix},$$

if not already even, can be made an even permutation by interchanging any of the two letters (i) α and (j) α.

For example

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

is an odd permutation. Interchange of any two the symbols, 3, 5, say, gives us the new permutation

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

which is an even permutation.

8.6.6. Lemma: Let $n \geq 5$. If a normal subgroup N of A_n contains a cycle of length 3 then $N = A_n$.

Proof: Suppose that N is a normal subgroup of A_n and contains a cycle $(a\ b\ c)$ of length 3. Let $(a'\ b'\ c')$ be any other cycle of length 3 in A_n. We show that $(a'\ b'\ c')$ is in N and thus conclude that $N = A_n$, using Theorem 8.6.4.

Since $n \geq 5$, there exist symbols d, e different from a, b, c and symbols d', e' different from a', b', c' respectively. Consider now the permutation.

$$\alpha = \begin{pmatrix} \ldots a' \ldots b' \ldots c' \ldots d' \ldots e' \ldots \\ \ldots a \ \ldots b \ \ldots c \ \ \ldots d \ \ \ldots e \ \ldots \end{pmatrix}$$

of degree n which, by interchanging d, e, if required, is supposed to be an even permutation and so in A_n. Then

$$\alpha(a\ \ b\ \ c)\,\alpha^{-1} = (a'\ \ b'\ \ c')$$

is an element of N. Hence $N = A_n$.

8.6.7. Theorem: A_n is simple for all $n \geq 5$.

Proof: Suppose that A_n has a proper normal subgroup H. Then H has an element either of order 2 or order 3 or of order ≥ 4. By discussing these cases separately we show that if H has an element of order 2 or 3 then H has also an element of order ≥ 4.

Case I: Let H have an element γ of order 2. Since γ is an even permutation, it is a product of 2m transpositions, $m \geq 1$. If $m = 1$, then

$$\gamma = (a\ \ b)\,(a'\ \ b').$$

Since $n \geq 5$, there is a symbol c different from a, b, a', b' such that $\alpha = (a\ \ b\ \ c) \in A_n$. Since H is normal in A_n,

$$\gamma' = \alpha\gamma\,\alpha^{-1} = (a\ \ b\ \ c)\,(a\ \ b)\,(a'\ \ b')\,(a\ \ c\ \ b)$$
$$= (a\ \ c)\,(a'\ \ b')$$

is an element of H. But then

$$\gamma'\gamma = (a\ \ c\ \ b)$$

is also in H. By lemma 8.6.6, $H = A_n$. So we can suppose that $m > 1$.

Then

$$\gamma = (a\ \ b)\,(a'\ \ b')\,(a''\ \ b'')\,(a'''\ \ b''')\ldots \qquad 8.6.7\ (1)$$

where dots denote other pairs of transpositions. Since $\alpha = (a'\ \ b)\,(b'\ \ a'') \in A_n$, H also contains the element

$$\gamma' = \alpha\gamma\alpha^{-1} = (a'\ \ a)\,(b\ \ a'')\ (b'\ \ b'')\,(a'''\ \ b''')\ldots \qquad 8.6.7\ (2)$$

where dots in (2) denote the same transpositions as in (1).

Hence

$$\gamma\gamma' = (a\ \ a''\ \ b')\,(b\ \ a'\ \ b'')$$

belongs to H. So H contains an element of order 3.

Next we proceed to show that if H contains an element of order 3 then H also contains an element of order ≥ 4.

Suppose that H has an element γ of order 3. Then either γ is a 3-cycle

$$\gamma = (a \quad b \quad c)$$

in which case, $H = A_n$, by lemma 8.6.6, or γ is a product of 3-cycles:

$$\gamma = (a \quad b \quad c)\,(a' \quad b' \quad c') \ldots$$

where dots denote other cycles of length 3. As H is normal in A_n, for $\alpha = (c \quad a' \quad b')$ in A_n,

$$\gamma' = \alpha\gamma\alpha^{-1} = (c \quad a' \quad c')\,(b' \quad a \quad b) \ldots$$

is in H. Hence H also contains

$$\gamma\gamma' = (a \quad b' \quad c \quad b \quad a') \ldots$$

which has order ≥ 5. So we, in the first instance, could have supposed that H has an element of order ≥ 4.

Case II: Suppose that H has an element of order ≥ 4. Such an element does not have order 2q or 3q, (2, q) = 1, (3, q) = 1, for otherwise qth power of such an element has order 2 or 3 respectively and we are back in case I.

Now if H has an element γ of order > 4, then γ, when expressed as a product of disjoint cycles, must contain a cycle of length > 4 only. Thus

$$\gamma = (a \quad b \quad c \quad d \ldots) \ldots \qquad 8.6.7\ (3)$$

where dots outside the parenthesis denote other cycles. Take $\alpha = (c \quad a \quad b) \in A_n$. Then H also contains

$$\gamma' = \alpha\gamma\alpha^{-1} = (c \quad a \quad b \quad d \ldots) \ldots \qquad 8.6.7\ (4)$$

where dots outside the parenthesis denote the same cycles as in 8.6.7 (3). Thus

$$\gamma^{-1}\gamma' = (a \quad c \quad d)$$

belongs to H. By lemma 8.6.6, $H = A_n$. Thus A_n has no proper normal subgroups. Therefore A_n is simple.

A system of subgroups

$$H_1, H_2, \ldots, H_n, \ldots$$

of a group G is said to form an *ascending sequence of subgroups if*

$$H_n \subseteq H_{n+1},\ n = 1, 2, 3, \ldots$$

We know that, for every integer n, the alternating group A_n of degree n has the alternating group A_{n-1} of degree $n - 1$ as a subgroup. If A_n is the alternating group on $\{1, 2, 3, ..., n\}$ then A_{n-1} can be taken as the alternating group on $\{1, 2, 3, ..., n - 1\}$ fixing n. Thus, if $N = \{1, 2, 3, ...,\}$, the system $\{A_n : n \in N\}$ of alternating groups is an ascending sequence of the *restricted alternating group* A_N. A_N consists of those even permutations on N which act on only finite subsets of N. As seen before, A_n is simple for $n \geq 5$. Is A_N simple? We now answer this question.

Before answering the above question we prove:

8.6.8. Theorem: Let

$$H_1 \subset H_2 \subset ... \subset H_n \subset ...$$

be an ascending sequence of simple subgroups of a group G.

Then

$$H = \bigcup_{n \in N} H_n$$

is a simple subgroup of G.

Proof: First we show that H is a subgroup. Let $\alpha, \beta \in H$. Then there exist indices m, n such that $\alpha \in H_m$, $\beta \in H_n$. Without any loss of generality, we can suppose that $n \geq m$. Then $\alpha, \beta \in H_n$. As H_n is a subgroup, $\alpha\beta^{-1} \in H_n$. Hence $\alpha\beta^{-1} \in H$.

Now we prove the simplicity of H. Suppose that H has a proper normal subgroup K. Then there is an integer n such that $K \cap H_n$ is a proper normal subgroup of H_n. This contradicts the simplicity of H_n. Hence H is simple.

Consider now A_N. Of course A_n is a subgroup of A_N for every $n \in N$. If

$$A^* = \bigcup_{n \in N} A_n,$$

then $A^* \subseteq A_N$. Now let $\alpha \in A_N$. Then α acts on a finite subset $\{x_1, x_2, ..., x_k\}$ of N. Let $m = \max_{i=1}^{k} x_i$

Then $\alpha \in A_m$ and so $\alpha \in A^*$. Hence $A_N \subseteq A^*$. Thus $A_N = A^*$.

From these remarks and the above theorem, we have:

8.6.9. Theorem: The restricted alternating group A_N on $N = \{1, 2, 3, ...\}$ is simple.

Note that A_N is infinite.

8.7. ORBITS, STABILIZER SUBGROUP AND TRANSITIVE GROUPS

A subgroup of the symmetric group S_n, $n > 1$, is called a permutation group. In theorem 4.3.3., it was shown that every group is isomorphic to a group of bijective mappings of a set. Since we have defined a permutation to be a bijective mapping of a set, we can restate the above result as follows.

Every group is isomorphic to a permutation group on a suitable set.

Recall that, in 4.3.3., for each $g \in G$ we had defined a bijective mapping $\varphi_g : G \to G$ by

$$\varphi_g(x) = gx \text{ for all } x \in G. \qquad 8.7\ (1)$$

Using the notation of this chapter we rewrite $\varphi_g : G \to G$ as

$$(x)\ \varphi_g = xg\ ,\ x \in G.$$

so that we can represent φ_g, $g \in G$ as a permutation

$$\varphi_g = \begin{pmatrix} x \\ xg \end{pmatrix}, x \in G, \qquad 8.7\ (2)$$

of G, considered as a set. Then the set of all permutations

$$\Phi_G = \{\varphi_g : g \in G\}$$

is a group with $\varphi_e = \begin{pmatrix} x \\ xe \end{pmatrix}$, e, the identity of G, as the identity element of Φ_G.

The mapping $\alpha : G \to \Phi_G$ given by :

$$\alpha(g) = \varphi_g \qquad 8.7\ (3)$$

is then an isomorphism between G and Φ_G. The homomorphism property of α follows from the equation.

$$\alpha(g_1 g_2) = \varphi_{g_1 g_2} = \begin{pmatrix} x \\ xg_1 g_2 \end{pmatrix}$$

$$= \begin{pmatrix} x \\ xg_1 \end{pmatrix} \begin{pmatrix} xg_1 \\ (xg_1) g_2 \end{pmatrix}$$

$$= \begin{pmatrix} x \\ xg_1 \end{pmatrix} \begin{pmatrix} x \\ xg_2 \end{pmatrix}$$

$$= \varphi_{g_1} \cdot \varphi_{g_2}$$

$$= \alpha(g_1)\, \alpha(g_2)$$

for all $g_1, g_2 \in G$.

Let G be an arbitrary group. A homomorphism α of G into S_n, $n \geq 1$, is called a *permutational representation* of G. The representation is said to be *faithful* if α is a monomorphism, that is, if kernel of α is the identity subgroup of G.

8.7.1. Example: The mapping $\alpha : G \to \Phi_G$ defined by 8.7 (3) above is a permutational representation of G.

It is easy to see that this representation is faithful. So we can regard every group as a permutation group on some suitable set.

8.7.2. Example: Let $G = \langle a : a^n = e \rangle$ be a cyclic group of order n. The mapping $\varphi : G \to S_n$ defined by:

$$\varphi(a) = (1 \quad 2 \quad 3 \ldots n).$$

is a faithful representation of G.

8.7.3. Example: Let $G = \langle a, b : a^2 = b^2 = (ab)^2 = e \rangle$.

Consider the mapping $\varphi : G \to S_4$ defined by:

$$\varphi(e) = I,\ \varphi(a) = (1 \quad 2)\,(3 \quad 4)$$

$$\varphi(b) = (1 \quad 3)\,(2 \quad 4),\ \varphi(ab) = (1 \quad 4)\,(2 \quad 3).$$

Then it is easy to check that φ is a monomorphism of G into S_4 and so is a faithful representation of G.

The use of representation of a group by a permutation group lies in the fact that calculations and computations become 'easier' in permutation groups.

Let G be a permutation group on a set A. Two elements x and y of A are said to be *connected* if there exists an $\alpha \in G$ such that $x\alpha = y$. We then write $x \sim y$, We show that '$\sim$' is an equivalence relation on A.

Let $x \in A$. Then, for the identity permutation I in G, $xI = x$ for all $x \in A$ so that $x \sim x$. Hence '$\sim$' is reflexive.

Next suppose that $x \sim y$. Then there is an $\alpha \in G$ such that $x\alpha = y$. But then $y\alpha^{-1} = x$ so that $y \sim x$. Hence '$\sim$' is symmetric.

Lastly let $x \sim y$ and $y \sim z$. Then there are $\alpha, \beta \in G$ such that

$$x\alpha = y \text{ and } y\beta = z$$

so that $x\alpha\beta = z$. As $\alpha\beta \in G$, '$x \sim z$'.

Thus '$\sim$' is transitive and so is an equivalence relation.

Thus, for any permutation group G on a set A, the relation '$\sim$' defines a partition of A into equivalence classes.

These equivalence classes, which are subsets of A, are called *orbits* of G and A is the union of these orbits.

For each $x \in A$, the set

$$x^G = \{x\alpha : \alpha \in G\}$$

is an orbit called the *orbits of x*.

The number of elements in an orbit is called the *length of the orbit*.

Also, for each $x \in A$, consider the set

$$G_x = \{\alpha \in G : x\alpha = x\}.$$

Then $I \in G_x$ and for $\alpha, \beta \in G$ with $x\alpha = x$, $x\beta = x$, we have $x\alpha\beta^{-1} = x$. So $\alpha\beta^{-1} \in G_x$. Thus G_x is a subgroup of G.

G_x is called the *stabilizer* (or *stability*) *subgroup of x*.

8.7.4. Theorem: If x and y both belong to one and the same orbit of G then G_x and G_y are conjugate, that is,

$$G_x = \gamma G_y \gamma^{-1} \quad \text{for some } \gamma \in G.$$

Proof: For if x and y are in the same orbit of G there is a $\gamma \in G$ such that $x\gamma = y$. Now

$$G_y = \{\beta \in G : y\beta = y\}.$$

Let $\alpha \in G_x$ and consider $\gamma^{-1}\alpha\gamma$. We have,

$$(y)(\gamma^{-1}\alpha\gamma) = x\alpha\gamma = x\gamma = y.$$

So $\gamma^{-1}\alpha\gamma = \beta \in G_y$, that is, $\alpha = \gamma\beta\gamma^{-1} \in \gamma G_y \gamma^{-1}$. Hence

$$G_x \subseteq \gamma G_y \gamma^{-1}.$$

Conversely let $\beta \in G_y$. Then

$$x\gamma\beta\gamma^{-1} = y\beta\gamma^{-1} = y\gamma^{-1} = x.$$

So $\gamma\beta\gamma^{-1} \in G_x$. Thus

$$\gamma G_y \gamma^{-1} \subseteq G_x.$$

Therefore,

$$G_x = \gamma G_y \gamma^{-1}.$$

The natural question about the number of elements in an orbit of G is answered by the following theorem.

8.7.5. Theorem: Let O be an orbit of G. The number of elements in O is equal to the index of the stabilizer subgroup G_x in G of any arbitrary element x of O.

Proof: Let Ω be the collection of all right cosets $G_x\beta$, $\beta \in G$, of the stabilizer subgroup G_x of x in G. Let O be the orbit of x in G. Define a mapping $\varphi : O \to \Omega$ as follows:

Let $y \in O$. Then there is a $\gamma \in G$ such that

$$y = x\gamma.$$

So we put

$$\varphi(y) = G_x\gamma.$$

We show that φ is a bijection between O and Ω.

To see that φ is injective, let, for $y_1, y_2 \in O$, $\varphi(y_1) = \varphi(y_2)$. Then

$$G_x\gamma_1 = G_x\gamma_2$$

where γ_1, γ_2 satisfy the equations $y_1 = x\gamma_1$, $y_2 = x\gamma_2$. That is, $\gamma_1\gamma_2^{-1} \in G_x$, so that

$$x\gamma_1\gamma_2^{-1} = x.$$

So,

$$x\gamma_1 = y_1 = y_2 = x\gamma_2.$$

Hence φ is injective.

Next let $G_x\beta \in \Omega$ for some $\beta \in G$. Consider $y = x\beta$. Then $y \in O$ and $\varphi(y) = G_x\beta$. So φ is surjective. Thus

$$|O| = |x^G| = |G : G_x|.$$

Hence the number of elements in $O = x^G$ is equal to the index of the stabilizer G_x in G.

8.7.6. Corollary: The order of a finite permutation group is divisible by the least common multiple of the number of elements in the orbits of G.

A permutation group on a set A is said to be *transitive* if G has only one orbit namely A, that is, for any two elements x, y of A there is a permutation α such that,

$$y = x\alpha.$$

G is said to be *intransitive* if G has at least two orbits.

G is said to be $\frac{1}{2}$ – *transitive* if all orbits of G have the same number of elements.

If G is a finite permutation group and if G is transitive then the order of G is divisible by its degree, by corollary 8.7.6.

Here degree of permutations in G is equal to the number of elements in the only orbit of G.

8.7.7. Examples:

(i) The symmetric group S_n of degree n, $n \geq 2$ is transitive.

(ii) The alternating group A_n of degree n, $n \geq 2$ is transitive.

(iii) The group G consisting of
I, (1 2) (3 4), (1 3) (2 4), (1 4) (2 3)
is transitive on {1, 2, 3, 4}.

A permutation group G on a set A is said to be *regular* if

$$G_x = E$$

for each $x \in A$. Here E is the identity subgroup of G.

8.7.8. Theorem: A transitive permutation group G on a set A is regular if and only if, for any two symbols x, y of A, there is one and only one element of G which takes x to y.

Proof: Suppose that G is regular on A. Then, for each $x \in A$, $G_x = E$. Let $x, y \in A$. Since G is transitive on A, there is an $\alpha \in G$ such that $y = x\alpha$. Suppose that for some $\beta \in G$ also $y = x\beta$. Then $x = x\alpha\beta^{-1}$ so that $\alpha\beta^{-1} \in G_x = E$. Hence $\alpha = \beta$.

Conversely suppose that for any pair $x, y \in A$, there is one and only one α of G such that $y = x\alpha$. Then G is transitive.

Also let $\gamma \in G_x$ for some $x \in A$. Then $x = x\gamma$. But $x = x$ I as well. So γ = I, by hypothesis. Hence $G_x = E$ for all $x \in A$. Thus G is regular on A.

8.7.9. Corollary: A transitive permutation group is regular if and only if its order is equal to its degree.

Proof: Let a permutation group G be transitive on A. Then G is regular if and only if $G_x = E$ for all $x \in A$. Since G is transitive, G has only one orbit namely A. So, from Corollary 8.7.5, we have

$$|G| = |G_x| \cdot |x^G| = 1 \cdot |x^G| = |A|,$$

as required.

8.7.10. Theorem: Let G be a transitive abelian group. Then G is regular.

Proof: Let G be transitive on A and abelian. Let $x \in A$ be a fixed element. Let $y \in A$. Since G is transitive, there is an $\alpha \in G$ such that $y = x\alpha$. Now

$$G_y = G_{x\alpha} = \alpha^{-1} G_x \alpha, \qquad \text{by Theorem 8.7.4.}$$

$$= G_x$$

because G is abelian. So G_x fixes y. Since G is transitive, G_x fixes every element of A. But then $G_x = E$. Hence G is regular.

A permutation group on a set A is said to be *k-transitive* if, for any pair of k-tuples

$$(x_1, x_2, ..., x_k), (y_1, y_2, ..., y_k)$$

there is an $\alpha \in G$ such that $y_i = x_i \alpha$, $1 \le i \le k$.

If $k \ge 2$, then k-transitive obviously implies $(k-1)$ transitive.

8.7.11. Theorem: S_n is n-transitive. A_n is $(n-2)$ transitive but not $(n-1)$-transitive.

Proof: If S_n is the symmetric group on $A = \{x_1, x_2, ..., x_n\}$, then, for any n-tuples.

$$(x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n)$$

the permutation $\begin{pmatrix} x_i \\ y_i \end{pmatrix}$ is in S_n and changes x_i to y_i. Hence S_n is n-transitive.

Next let

$$(x_1, x_2, ..., x_{n-2}), (y_1, y_2, ..., y_{n-2})$$

be any two $(n-2)$-tuples of distinct elements of A. Then precisely one of the permutations.

$$\begin{pmatrix} x_1 & x_2 & ... & x_{n-2} & x_{n-1} & x_n \\ y_1 & y_2 & ... & y_{n-2} & y_{n-1} & y_n \end{pmatrix} \text{ and } \begin{pmatrix} x_1 & x_2 & ... & x_{n-2} & x_{n-1} & x_n \\ y_1 & y_2 & ... & y_{n-2} & y_n & y_{n-1} \end{pmatrix}$$

is even. Hence A_n is $(n-2)$ transitive is not $(n-1)$ transitive.

Here $x_{n-1}, x_n, y_{n-1}, y_n$ are the remaining elements. So A_n is $(n-2)$ transitive but not $(n-1)$-transitive.

Let G be a permutation group on a set A. A non-empty subset B of A is said to be a *block (or a set of impirimitivity)* for G if, for each $\alpha \in G$, either $B\alpha = \{y\alpha : y \in B\}$ and B are equal or $B\alpha \cap B = \phi$.

All singleton subsets of A and the set A itself are blocks called the *trivial* blocks.

This is so because, for each $x \in A$ and $\alpha \in G$, either $x \neq x\alpha$ or $x = x\alpha$ so that, if $B = \{x\}$, then either $B\alpha = \{y\alpha; y \in B\}$ and B are equal or $B \cap B\alpha = \phi$.

Similarly for A.

A group G is said to be *primitive* if it has no non-trivial blocks. Otherwise G is said to be *imprimitive.*

It is easy to see that the symmetric group S_n, $n \geq 1$, is primitive.

8.7.12. Theorem: Let G be a transitive permutation group of prime degree. Then, G is primitive.

Proof: Suppose that G is imprimitive on A consisting of p elements, p a prime. Let B be a non-trivial block containing m elements. Then, for each $\alpha \in G$, $B\alpha \cap B = \phi$ so that

$$A = \bigcup_{\alpha \in G} B\alpha$$

is a disjoint union. As B and $B\alpha$ consist of the same number of elements, m|p. Since p is a prime, m = 1 so that B is a singleton subset, a contradiction. Hence G is primitive.

8.7.13. Theorem: Let G be a transitive permutation group on a set A. G is primitive on *A* if and if the stabilizer subgroup G_x is a maximal subgroup of G for every $x \in A$.

Proof: Suppose that G is primitive on A. Suppose that for some G_x there is a subgroup H of G such that

$$G_x \subset H \subset G.$$

Put $B = x^H$. Since G_x is a proper subgroup of H there is a $\gamma \in H \setminus G_x$ such that $x \neq x\gamma$ and $x, x\gamma$ both belong to B. So B is not a singleton subset. Also if B = A then H is transitive on A. Hence, by corollary 8.7.6, with $x^H = A = x^G$,

$$|A| = (G : G_x) = (H : G_x)$$

so that H = G, a contradiction. So $B \neq A$.

Next suppose that $B \cap B\alpha \neq \phi$, for some $\alpha \in G$ and let $y \in B \cap B\alpha$. Then

$$y = x\gamma = x\gamma\alpha$$

so that

$$x = x\gamma\alpha\gamma^{-1}.$$

Thus $\gamma\alpha\gamma^{-1} \in G_x \subset H$. Since $\gamma \in H$ we have $\alpha \in H$. Hence H = G, again a contradiction. Hence G_x is maximal.

Conversely, suppose that every G_x, $x \in A$, is maximal in G and further suppose that G is not primitive. Let B be a non-trivial block. Put

$$H = \{\alpha \in G : B\alpha = B\}$$

Then H is a subgroup of G. Let $x \in B$. If $\gamma \in G_x$, that is, $x\gamma = x$ then $x \in B \cap B\gamma$. Since B is a block, $B = B\gamma$. Thus $\gamma \in H$. So

$$G_x \subseteq H \subseteq G.$$

Since G is transitive on A and $B \neq A$, we have $H \neq G$. Now B, being a block, contains at least two elements. Let $y \in B$ and $y \neq x$. Since G is transitive on A, there is a $\gamma \in G$ such that $y = x\gamma$ so that $\gamma \notin G_x$. Now $y \in B \cap B\gamma$ because $x \in B$. So $B = B\gamma$. Hence $\gamma \in H$. Thus $G_x \neq H$. That is G_x is not maximal in G, a contradiction. Hence G is a primitive.

8.7.14. Theorem: Let G be a transitive permutation group on A and H a subgroup of G which also is transitive on A. Then

$$G = G_x H = H G_x, \; x \in A.$$

Proof: Let $y \neq x$ be an element of A. Since G is transitive on A, there is an $\alpha \in G$ such that $y = x\alpha$. Also since H is transitive on A, there is a $\gamma \in H$ such that $y = x\gamma$. Thus $x = x\alpha\gamma^{-1}$ so that $\alpha\gamma^{-1} \in G_x$. That is, $\alpha \in G_x\gamma \subseteq G_x H$. But trivially $G_x H \subseteq G$. Hence $G = G_x H$.

Also since $(G_x H)^{-1} = H^{-1}G_x^{-1} = H G_x H$. we have

$$G = G_x H = H G_x.$$

EXERCISES

1. Show that the order of the symmetric group S_n is n!.

2. Find the product of the permutations:

   (i) $(a_1\ a_2 \ldots a_k)\ (a_1\ b_1\ b_2 \ldots b_l)$ and $(b_1\ b_l a_k\ a_1)$

   (ii) $(1\ 2\ 3\ 4\ 5)\ (2\ 5\ 4\ 3\ 1)$ and $(1\ 5\ 3\ 2\ 4)$

3. Find the order of each of the following permutations:

$$\begin{pmatrix}1&2&3&4&5&6\\2&4&5&1&6&3\end{pmatrix}, \qquad \begin{pmatrix}1&2&3&4&5&6\\4&5&6&1&2&3\end{pmatrix}$$

$$\begin{pmatrix}a&b&c&d&e&f&g&h\\h&a&f&c&d&e&b&g\end{pmatrix}, \qquad \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&4&5&3&1&8&6&7&10&9\end{pmatrix}$$

4. Let $\alpha = (2\ 1\ 5\ 6\ 3)$, $\beta = (1\ 3\ 7\ 6\ 2)$; $\gamma = (2\ 3\ 5)$. Express each of the following as a product of disjoint cycles.

$$\beta\alpha,\ \beta\alpha^{-1},\ \gamma\beta,\ \alpha\beta^{-1}\gamma,\ \beta^3\alpha^2\gamma,\ \alpha^{-1}\gamma^2\alpha.$$

5. Let α be a cyclic permutation of length k. Show that α^2 is a cyclic permutation if and only if k is odd.

6. For any two disjoint cycles α, β, show that

   (i) $(\alpha\beta)^k = \alpha^k \beta^k$ for every natural number k.

   (ii) $\alpha\beta = I$ if and only if $\alpha = I$, $\beta = I$.

   (iii) For $\alpha = (a_1\ a_2 \ldots a_k)$, $\beta = (b_1\ b_2 \ldots b_l)$, find a transposition γ such that $\gamma\beta\alpha$ is a cyclic permutation. Are then $\alpha\beta\gamma$ and $\alpha\gamma\beta$ also cyclic?

7. Write down all elements of order 2, 3 and 4 in the symmetric group of degree 4.

8. Find the commutator of the permutations.

$$x = (a_1\ a_2 \ldots a_{n-2}\ a_{n-1}),\ y = (a_1\ a_2 \ldots a_{n-2}\ a_n).$$

9. Show that the permutations $(1\ 2\ 3\ 4\ 5)$, $(6\ 7\ 8\ 9)$, $(10\ 11\ 12)$ generate a cyclic group of order 60. Find one of its generators.

10. If S is the symmetric group on a set X and Y is a subset of X, then prove that the set of those elements of S which change elements of Y into elements of Y is a subgroup S.

11. Show that the permutations

$$a = (1\ \ 2\ \ 3\ \ 4)\,(5\ \ 6\ \ 7\ \ 8)$$

and

$$b = (1\ \ 6\ \ 3\ \ 8)\,(2\ \ 7\ \ 4\ \ 5)$$

generate an abelian group of order 8.

12 Show that the permutations

I, (1 2), (3 4), (1 2) (3 4), (1 3) (2 4), (1 4) (2 3), (1 4 2 3), (1 3 2 4)

are the only permutations on {1, 2, 3, 4} under which the expression

$$x_1 x_2 + x_3 x_4$$

remains unaltered.

13. Determine the largest permutation group on x_1, x_2, x_3, x_4 under which the expression

$$(x_1 + x_2)(x_3 + x_4)$$

remains unaltered.

14. Find all the subgroups of S_4 which are isomorphic to S_3.

15. Show that the permutations

$$\varphi = (x_1\ \ x_2 \ldots x_{2n})\,(y_1\ \ y_2 \ldots y_{2n})$$

and

$$\psi = (x_1\ y_{2n}\ x_{n+1}\ y_n)\,(x_2\ y_{2n-1}\ x_{n+2}\ y_{n-1})\,(x_3\ y_{2n-2}\ x_{n+3}\ y_{n-2}) \ldots (x_n\ y_{n+1}\ x_{2n}\ y_1)$$

satisfy the relations

$$\varphi^{2n} = \varphi^n\ \psi^2 = \varphi\ \psi\ \varphi\ \psi^{-1} = I.$$

16. Show that the commutator subgroup of S_n is the alternating group A_n.

17. Show that the centre of S_n, $n \geq 3$ is trivial.

[**Hint:** Let $I \neq \alpha \in \varsigma(G)$. Then, for some symbols $x_1 \neq x_2$, $(x_1)\alpha = x_2$. Also there is an $x_3 \neq x_1$ or x_2. Take a $\beta \in S_n$ such that

$$(x_1)\beta = x_1, (x_2)\beta = x_3, (x_3)\beta = x_2.$$

Then $(x_1)\alpha\beta = x_3 \neq x_2 = (x_1)\beta\alpha$. So $\alpha\beta \neq \beta\alpha$. Thus $\varsigma(S_n) = \{I\}$].

Chapter - IX

SYLOW THEOREMS

The theorem of Lagrange about subgroups of a finite group states that the order and index of a subgroup of a finite group is a divisor of the order of the group. The converse of this theorem is not true. That is, if G is a finite group of order n and m is a divisor of n then it is not necessary that G should have a subgroup H of order m. A counter-example is the alternating group A_4 of degree 4 which has no subgroup of order 6.

To prove this, let K be a subgroup of order 6 in A_4. Then, being of index 2, K is normal in A_4. Also then, for each $x \in A_4$, $x^2 \in K$. Now let $x = (123)$. Then $x^2 = (132) \in K$. So $x^3 = I$ implies that $x = x^4 \in K$. So K contain the permutations

$$I, (123), (132).$$

Similarly K contains

$$(124), (142), (134), (143), (234), (243),$$

$$(12)(34) = (132)(243), (13)(24) = (123)(234),$$

$$(14)(23) = (123)(124)$$

But then K is a subgroup of A_4 and has order 12. So $K = A_4$.

Thus A_4 has no subgroup of order 6.

It is thus natural to ask the following question:

For which divisor of the order n of a group G, has G a subgroup of that divisor?

A partial answer to this question was given by A.L. Cauchy who proved that corresponding to each prime divisor of the order of a group there is a subgroup of that order. Cauchy's results were later generalised by L. Sylow, a Norwegian Mathematician. He proved that if G is a group of order n and p^α, $\alpha \geq 1$, is the highest power of a prime p dividing n, then G has a subgroup of order p^α.

Because of the usefulness and fundamental nature of this result, it has rightly called the second most important theorem of classical group theory, preceded only by the theorem of Lagrange. It is one of those results about finite groups which derive deep properties of such groups.

Various generalisations of Sylow's theorems have been given by *reknowned group theorists*. Sylow theorems and their generalisation have engendered an expansion of knowledge of such cosmic proportion that these might well be compared to the Big Bang for group theory. In this chapter, however, we shall not go into the details of these and restrict ourselves to the discussion of Sylow's theorems and a few of their immediate and easy applications.

In this chapter, by a group G we shall always mean a finite group.

9.1. CAUCHY'S THEOREM FOR ABELIAN AND NON-ABELIAN GROUPS

Let p be a prime number. A finite p-group is a group of order p^α, $\alpha \geq 1$. The order of each element of a p-group being a divisor of its order p^α is a power of p. Infinite p-groups are groups in which every element has order a power of *p*. Structural properties of finite p-groups substantially differ from those of infinite p-groups. We shall mention one such property in the last section of this chapter.

Let G be a finite group of order n and p a prime divisor of n. A subgroup H of G is called a p-subgroup if H is a p-group the sense of given above.

We now prove Cauchy's theorem for abelian groups. This will be needed in the proof of Cauchy's theorem for arbitrary finite groups.

9.1.1. Theorem: If A is a finite abelian group and p a prime divisor of the order of A then A contains an element of order p.

Proof: Let A be an abelian group of order n and p a prime divisor of n. For proof we use induction on the order of A. If n = p, then A is a cyclic group of order p and a generator of A will be an element of order p. So we have a basis for induction.

Suppose now that the theorem is true for all abelian groups of order less than n and divisible by p. Consider now the group A. Let $a \neq 1$ be an element of A and H the cyclic group generated by *a*. There are then the following two possibilities.

(i) The order k of H is divisible by p.

(ii) k is not divisible by p.

In case (i) $k = pq$, $q \geq 1$. Since $a^k = (a^q)^p = 1$, a^q is an element of order p in H and hence in A. In case (ii) H is normal in A since A is abelian. So A/H has order less than n but divisible by p. By induction hypothesis, A/H has an element xH, $x \in A$, of order p, that is,

$$(xH)^p = x^pH = H$$

But then $x^p \in H$. As (p, k) = 1, x^p has order k so that $(x^p)^k = (x^k)^p = 1$ and x^k has order p. Hence the theorem.

Next we prove Cauchy's theorem for finite non-abelian groups.

9.1.2. Theorem: If a prime p divides the order of a group G then G contains an element of order p.

Proof: Let G be a group of order n and p a prime divisor of n. Again we prove the theorem by using induction on the order of G. If n = p then G is a cyclic group of order p and hence contains an element of order p. So we have a basis for induction. Thus we suppose that the theorem is true for all groups of order less than n and divisible by p. Now consider the group G of order n. We examine the following two cases:

(i) G contains a proper subgroup H whose index is prime to p.

(ii) Every proper subgroup of G has index divisible by p.

In case (i) the order of the proper subgroup H is divisible by p and H has, by induction hypothesis, an element of order p which is also an element of order p in G.

In case (ii), let the class equation of G be:

$$n = n_1 + n_2 + \ldots + n_k \qquad 9.1.2\ (1)$$

where n_i is the number of elements in a conjugacy class in G. Now each n_i, being the index of the normaliser (a subgroup) of a representative element in the ith conjugacy class, is divisible by p, by (ii), or else is equal to 1. Since the identity element is its own conjugacy class, one of the n_i's say n_1, is 1. The left hand side of 9.1.2 (1) is divisible by p so should also be the right hand ride. But then, since $n_1 = 1$, the number of n_i's which are equal to 1 must be a multiple of p. The corresponding conjugacy classes.

that is, classes for which $n_i = 1$ are such that each consists of a central element. Hence the order of the centre $\varsigma(G)$ of G is a multiple of p. Since $\varsigma(G)$ is abelian, $\varsigma(G)$ contains an element of order p which is also an element of order p in G.

9.2. SYLOW THEOREMS

Let G be group of order n and p a prime divisor of n. *A subgroup H of G is said to be a Sylow p-subgroup of G if H has order p^α where p^α divides n but $p^{\alpha+1}$ does not divided n.*

A Sylow p-subgroup of a group can also be defined as follows:

A subgroup H of a finite group G is a Sylow p-subgroup if and only if the order of H is a power of p and the index of H is prime to p.

The first of the three remarkable theorems of Sylow is concerned with the existence of such subgroups.

9.2.1. Theorems: (Sylow's first theorem). A finite group whose order is divisible by a prime p contains a Sylow p-subgroup.

Proof: Let G be a group of order n and p^α the highest power of the prime p dividing n. We apply induction on the order of G to prove the existence of Sylow p-subgroups.

If n = p then G itself is a p-group and the theorem is true. Suppose now that the theorem is true for all groups of order less than n and divisible by p. Let G be a group of order n where n is divisible by p. There are now the following two possibilities:

(i) There is a subgroup H of G with index prime to p,

(ii) Every subgroup of G has index divisible p.

In Case (i) the order of H is less than that of G and, by induction hypothesis, H has a Sylow p-subgroup. As the index of H in G is prime to p, a Sylow p-subgroup of H is also a Sylow p-subgroup of G.

In case (ii) G has a non-trivial centre $\varsigma(G)$ as shown in the proof of Theorem 9.1.2. The order of $\varsigma(G)$ is a multiple of p. $\varsigma(G)$ contains an element z of order p by Theorem 9.1.1. Let

$$C = \langle z : z^p = 1 \rangle$$

Then C, being a subgroup of the centre, is normal in G. Consider now the factor group G/C. The order of G/C is less than the order of G and is

divisible by $p^{\alpha-1}$ and by no higher power of p. By induction hypothesis, G/C contains a subgroup H/C of order $p^{\alpha-1}$, where H is subgroup of G. The order of H is then $p^{\alpha-1}.\ p = p^{\alpha}$. *So H is a Sylow p-subgroup of G.*

Second theorem of Sylow gives a relationship between Sylow p-subgroups of a group corresponding to the same prime p.

9.2.2. Theorem: (Sylow's second theorem). Any two Sylow p-subgroups of a group are conjugate.

Proof: Let G be a group of order n and H, K be any two Sylow p-subgroups each of order p^{α} in G. Then $n = p^{\alpha}m$ and $(p, m) = 1$. Consider the double coset representation of G modulo (H, K)

$$G = \bigcup_{i=1}^{r} Ha_i K,\ a_i \in G.$$

Then, by Theorem 5.5.3.

$$n = \sum_{i=1}^{r} \frac{p^{\alpha}.p^{\alpha}}{q_i} \qquad 9.2.2\ (1)$$

where q_i is the order of $H \cap a_i K a_i^{-1}$. Upon division of both sides of (1) by p^{α}, we obtain

$$m = \sum_{i=1}^{r} \frac{p^{\alpha}}{q_i} \qquad 9.2.2\ (2)$$

Now q_i, being the order of the intersection of two p-groups, is a power of p. So each term on the right hand side of 9.2.2 (2) is either a multiple of p or else is equal to 1. Since the left hand side of 9.2.2 (2) is not divisible by p, $p^{\alpha}/q_i = 1$ for a least one i, i = 1, 2, ..., r. Without any loss of generality one can suppose that $p^{\alpha}/q_1 = 1$. Then $q_1 = p^{\alpha}$ so that the order
of $H \cap a_1 K a_1^{-1}$ is p^{α}. But $H \cap a_1 K a_1^{-1}$ is subgroup of H of the same order as that of H. So $H = H \cap a_1 K a_1^{-1}$. Hence $H \subseteq a_1 K a_1^{-1}$. As the order of H is equal to that of $a_1 K a_1^{-1}$, we have

$$H = a_1 K a_1^{-1},\ a_1 \in G.$$

Hence H and K are conjugate.

9.2.3. Corollary: A finite group G has a unique Sylow p-subgroup H if and only if H is normal in G.

Proof: For if H is a Sylow p-subgroup and $a \in$ G then $a\,Ha^{-1}$ is also a Sylow p-subgroup of G. By the uniqueness of H,

$$H = aHa^{-1},\ a \in G.$$

Hence H is normal in G.

Conversely if H is normal in G the then $aHa^{-1} = H$ for all $a \in$ G. Since all Sylow p-subgroup of G are of form aHa^{-1}, $a \in$ G, and all these coincide with H, H is the unique Sylow p-subgroup of G.

9.2.4. Corollary: A Sylow p-subgroup of a finite group is the only Sylow p-subgroup of its normaliser.

Proof: For if H is a Sylow p-subgroup of a group G and N is the normaliser of H in G then H is a Sylow p-subgroup of N. As H is normal in N, H is the unique Sylow p-subgroup of N.

9.2.5. Corollary: Let H be the unique Sylow p-subgroup of a group G. Then H is characteristic.

Proof: For each automporhpism α of G, α(H) is a Sylow p-subgroup of G. By the uniqueness of H,

$$\alpha(H) = H.$$

Hence H is characteristic.

9.2.6. Theorem: (Sylow's third theorem).

The number k of Sylow p-subgroups of a finite group is congruent to 1 mod p and is a factor of the order of the group.

Proof: Let H be a Sylow p-subgroups of G. Let n be the order of G. Since any two Sylow p-subgroups of G are conjugate, by Theorem 9.2.2, the number of Sylow p-subgroups of G is equal to the number of subgroups in a cojugacy class of H and this is the same as the index of the normaliser $N_G(H) = N$ of H in G. If the order of H is p^α, that of N be n_1 and its index in G be k, we have to show that $k \equiv 1 \bmod p$.

Consider the double coset decomposition modulo (N, H) of G:

$$G = \bigcup_{i=1}^{r} Na_i H,\ a_i \in G$$

Then
$$n = \sum_{i=1}^{r} \frac{n_1 \cdot p^\alpha}{q_i} \qquad 9.2.6\ (1)$$

where q_i is the order of $N \cap a_i H a_i^{-1}$ and so is a power of p because it is the order of a subgroup of a p-group $a_i H a_i^{-1}$. Hence

$$k = \sum_{i=1}^{r} \frac{p^\alpha}{q_i} \qquad 9.2.6\ (2)$$

where k is the index of N in G.

Each term on the right hand side of 9.2.6 (2) is a multiple of p or else is unity. However one of the terms among the double cosets Na_iH, Na_1H say, is such that for it $a_1 = e$, the identity of G. As $H \subseteq N$,

$$Na_1H = NH = N,$$

and

$$N \cap H = H.$$

So $q_1 = p^\alpha$. The corresponding term in 9.2.6 (2) is then $p^\alpha/q_1 = 1$. Hence 9.2.6 (2) becomes

$$k = 1 + \sum_{i=2}^{r} \frac{p^\alpha}{q_i}. \qquad 9.2.6\ (3)$$

We show that no other term in 9.2.6 (3) is unity. Suppose, on the contrary, that for some $j > 1$, $p^\alpha/q_j = 1$ in 9.2.6 (3), that is, $q_j = p^\alpha$. Then the intersection $N \cap a_j H a_j^{-1}$, being a subgroup of $a_j H a_j^{-1}$ and having order equal to the order of $a_j H a_j^{-1}$ must coincide with $a_j H a_j^{-1}$. Thus

$$a_j H a_j^{-1} = N \cap a_j H a_j^{-1}$$

so that

$$a_j H a_j^{-1} \subseteq N.$$

Since a Sylow p-subgroup H of G is a Sylow p-subgroup of any subgroup containing H, H is a Sylow p-subgroup of N. But H is normal in its normaliser N. So H is the unique Sylow p-subgroup of N. So

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

Thus $a_j \in N$. Consequently,

$$Na_jH = NH = Na_1H,$$

giving j = 1, a contradiction. Hence no other term on the right hand side of 9.2.6 (3), except the first, is unity. So $\sum_{i=2}^{r} p^{\alpha}/q_i$ is a multiple of p. Thus

$$k \equiv 1 + xp$$

for some integer x, that is,

$$k \equiv 1 \bmod p.$$

Since k is the index of a subgroup of G, k is a factor of the order of G. Hence the theorem.

9.2.7. Theorem: If P is a p-subgroup of a finite group G then P is contained in a Sylow p-subgroup of G.

Proof: Let G be a group of order n and P a p-subgroup of G of order p^{μ}. Let H be a Sylow p-subgroup of order p^{α} in G. Then, if $n = mp^{\alpha}$, (m, p) = 1. Consider the double coset decomposition of G modulo (P, H):

$$G = \bigcup_{i=1}^{r} Pa_i H, \; a_i \in G.$$

Then
$$n = \sum_{i=1}^{r} \frac{p^{\mu} \cdot p^{\alpha}}{q_i} \qquad 9.2.7\ (1)$$

where q_i is the order of $P \cap a_i H a_i^{-1}$. Both P and $a_i H a_1^{-1}$ are p-subgroups. Hence $q_i = p^{\mu} i$. Dividing 9.2.7 (1) by p^{α} we get

$$m = \sum_{i=1}^{r} p^{\mu}/p^{\mu_i} \qquad 9.2.7\ (2)$$

Each of the terms on the right hand side of 9.2.7 (2) is a multiple of p or else is unity.

Arguing as before, at least one of the terms on the right hand side of 9.2.7 (2) is unity. Without any loss of generality we can suppose that

$$p^{\mu}/p^{\mu_1} = 1, \text{ that is, } \mu = \mu_1.$$

Then the order of $P \cap a_1 H a_1^{-1}$ is p^{μ}. This intersection, being a subgroup of P of the same order as that of P, coincides with P, so that

$$P = P \cap a_1 H a_1^{-1}.$$

Hence $P \subseteq a_1 H a_1^{-1}$. But $a_1 H a_1^{-1}$ is a Sylow p-subgroup of G. Hence the theorem.

9.3. MISCELLANEOUS THEOREMS

9.3.1. Theorem: Let H be a Sylow p-subgroup of a group G and N a normal subgroup of G. Then $N \cap H$ is a Sylow p-subgroup of N and HN/N is a Sylow p-subgroup of G/N.

Proof: If H is a Sylow p-subgroup of G and N a normal subgroup of G then H is a Sylow p-subgroup of HN so that the index of H in HN is prime to p. Let (G : H) denote the index of H in G. Now $H \cap N$ is a subgroup of a p-group H and so is a p-subgroup of N. Also, from the isomorphism

$$HN/N \cong H/H \cap N,$$

we find that $(HN : H) = (N : N \cap H)$ so that index of $H \cap N$ in N is prime to p. Thus $H \cap N$ is a Sylow p-subgroup of N. Next, $HN/N (\cong H/H \cap N)$ is a p-subgroup of G/N and index of HN/N in G/N is given by:

$$(G/N : HN/N) = (G/N : H/H \cap N)$$
$$= (G : H)/(N : H \cap N)$$

Since (G : H) and $(N : H \cap N)$ are prime to p, (G/N : HN/N) is prime to p. Hence HN/N is a Sylow p-subgroup of G/N.

9.3.2. Theorem: If a subgroup K contains the normaliser of a Sylow p-subgroup of a group G then K is its own normaliser.

Proof: Suppose H is a Sylow p-subgroup of G and $N = N_G(H)$ with $N \subseteq K$, a subgroup of G. We show that $K = N_G(K)$. Clearly $K \subseteq N_G(K)$.

Conversely let $x \in N_G(K)$. Then $H \subseteq K$ implies

$$xHx^{-1} \subseteq x K x^{-1} = K.$$

Thus H and $H' = xHx^{-1}$ are Sylow p-subgroups of K and so are conjugate in K. That is, there is a $y \in K$ such that

$$yH' y^{-1} = H$$

or

$$yx Hx^{-1} y^{-1} = H$$

So $yx \in N$. Hence $x \in y^{-1} N \subseteq K$. Thus $N_G(K) \subseteq K$.

Consequently

$$K = N_G(K),$$

as required.

9.3.3. Corollary: The normaliser of a Sylow p-subgroup of a finite group G is its own normaliser.

Proof: Just take $K = N_G(H) = N$, H a Sylow p-subgroup of G so that $K = N = N_G(K)$.

9.3.4. Theorem: If P is a p-subgroup of G and is contained in exactly one sylow p-subgroup H of G then $N_G(P) \subseteq N_G(H)$.

Proof: If P is a subgroup of G and H is the only Sylow p-subgroup of G containing P, then, for any $x \in N_G(P)$, $x H x^{-1}$ is a Sylow p-subgroup of G. However $x \in N_G(P)$ implies

$$P = x P x^{-1} \subseteq x H x^{-1}.$$

Since P is contained in only one Sylow p-subgroup H, $x H x^{-1} \supseteq P$ must coincide with H. So, for any $x \in N_G(P)$,

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

Hence $x \in N_G(H)$. Therefore $N_G(P) \subseteq N_G(H)$.

9.3.5. Theorem: Let G be a group of order pq, p, q primes and $p > q$. Let $a \in G$ be of order p and $H = \langle a : a^p = 1 \rangle$. Then H is normal in G.

Proof: To show that H is normal, it is enough to show that H is the unique subgroup of G of order p.

Suppose K is another subgroup of order p in G and $H \neq K$. Then $H \cap K = \{e\}$. Otherwise, if $x \in H \cap K$, $x \neq e$, the order of the cyclic subgroup generated by x being a subgroup of both and of order $p \neq 1$ coincides with H and K so that H = K, a contradiction. Also

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

has p^2 elements because, if $hk = h'k'$, then $h'^{-1}h = k'k^{-1} \in H \cap K = \{e\}$. So $h = h'$, $k = k'$. But then G has at least p^2 elements. Since $p > q$, $p^2 > pq$, a contradiction. Hence G has a unique subgroup H of order p. Since, for each $g \in G$, gHg^{-1} also is a subgroup of order p in G,

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

Hence H is normal in G.

9.3.6. Corollary: Let G be a group of order pq, p > q and a be element of order p in G. Then, for each $g \in$ G,

$$gag^{-1} = a^k$$

for some k, $0 < k < p$.

Proof: Here $H = < a : a^p\ 1 >$ is normal in G so that, for each $g \in$ G, $gag^{-1} \in$ H. Now

$$gag^{-1} \neq a^0 = e$$

for otherwise $a = e$. Since $gag^{-1} \in$ H, $gag^{-1} = a^k$, $0 < k < p$.

9.3.7. Corollary: Let G be a group of order pq, p, q distinct primes and p > q. If $p \not\equiv 1 \bmod q$ then G is cyclic.

Proof: By Cauchy's theorem, G contains elements a and b of orders p, q respectively. Let $H = < a : a^p = 1$, $K = < b : b^q = 1>$. Then, by Lagrange's theorem $H \cap K = \{e\}$.

By corollary 9.3.6

$$bab^{-1} = a^k$$

for some integer k, $0 < k < p$. Since $b^q = e$, and, by induction,

$$a = b^q ab^{-q} = a^{k^q}$$

p divides k^{q-1}. That is

$$k^q \equiv 1 \bmod p$$

Also, by Fermat's theorem,

$$k^{p-1} \equiv 1 \bmod p.$$

Since q does not divide p − 1, ($p \not\equiv 1 \bmod q$), and is a prime number,

$$k \equiv 1 \bmod p.$$

So p divides k − 1. But $0 < k < p$. Hence k = 1. So $bab^{-1} = a$ and $ab = ba$. But then $< c = ab >$ contains H and K and has order pq. Hence $G = < c : c^{pq} = 1 >$ is cyclic.

9.3.8. Theorem: If K is a normal subgroup of a finite group G and H a Sylow p-subgroup of K then

$$G = KN$$

where N is the normaliser of H in G.

Proof: Since K is normal in G, KN is a subgroup of G.

Conversely let g be an arbitrary element of G. Then $H \subseteq K$ implies $g\,Hg^{-1} \subseteq K$, because K is normal. So both H and $H' = g\,Hg^{-1} \subseteq K$ are Sylow p-subgroups of K. Hence there exists an $x \in K$, such that

$$x\,H'x^{-1} = H.$$

That is

$$x\,g\,Hg^{-1}\,x^{-1} = H$$

so that $xg \in N_G(H) = N$. This means that $g \in x^{-1}\,N \subseteq KN$. So G is a subgroup of KN. Hence

$$G = KN.$$

Recall that a subgroup M of a group G is said to be maximal if G has no subgroup K such that

$$M \subset K \subset G.$$

Every finite group has a maximal subgroup. A group may have more than one maximal subgroups. An example is the group S_3 which has three maximal subgroups of order 2.

An infinite group, however, may not have a maximal subgroup. For instance Prufer's group C_p^{∞} has no maximal subgroup.

The theorem that follows gives a relationship between the normality of Sylow p-subgroups and of maximal subgroups of a group.

9.3.9. Theorem: Let G be a finite group. If every maximal subgroup of G is normal in G then every Sylow p-subgroup of G is normal in G.

Proof: Suppose that every maximal subgroup of G is normal in G and let H be a Sylow p-subgroup of G. Let $N = N_G(H)$. We show that $N = G$. Clearly $N \subseteq G$.

Conversely let g be an arbitrary element of G. Since G is finite, N is contained in a maximal subgroup M of G and so $N_G(H) \subseteq M$. Hence

$$N_G(M) = M$$

by Theorem 9.3.2. But M is normal in G, by hypothesis. So

$$M = N_G(M) = G.$$

Hence N is not contained in any maximal subgroup of G.

Thus N is itself maximal in G and so is a normal subgroup of G. Therefore $gNg^{-1} = N$. In particular $gHg^{-1} \subseteq N$. As H is normal in N, H and gHg^{-1} both are Sylow p-subgroups of N, $H = gHg^{-1}$. So $g \in N$. Hence $G \subseteq N$. Thus

$$G = N = N_G(H)$$

and H is normal in G.

9.3.10. Theorem: If every Sylow p-subgroup of a finite group G is normal in G then G is the direct product of its Sylow p-subgroups.

Proof: Suppose that every Sylow p-subgroup is normal in G.

Let n be the order of G. Then

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

and G has Sylow p_i-subgroups H_i, $1 \le i \le k$. Obviously G is generated by its Sylow p-subgroups. Moreover the subgroups

$$H_i \text{ and } < H_j : 1 \le i, \ j \le k, j \ne i >$$

have orders

$$p_i^{\alpha_i} \text{ and } n/p_i^{\alpha_i}$$

which are relatively prime to each other. Hence

$$H_i \cap < H_j : 1 \le j \le k, j \ne i > = E.$$

So G is the direct product of its Sylow p-subgroups.

9.3.11. Theorem: If the commutator of each pair a, b in a finite group G commutes with both a and b then G is the direct product of its Sylow p-subgroups.

Proof: First we show that, under the hypothesis, for any positive integer m,

$$[a, b]^m = [a^m, b] = [a, b^m] \qquad 9.3.11\ (1)$$

for a, $b \in$ G. The proof is by induction on m. Equation 9.3.11 (1) is triavially true for m = 1. Suppose that (1) is true for m = k, k > 1, that is,

$$[a, b]^k = [a^k, b] = [a, b^k]$$

and consider $[a, b]^{k+1}$. Then

$$\begin{aligned}
[a, b]^{k+1} &= [a, b]^k [a, b] \\
&= [a^k, b] [a, b] \qquad \text{by} \qquad 9.3.11\ (2) \\
&= a^k ba^{-k} b^{-1} [a, b] \\
&= a^k [a, b] b a^{-k} b^{-1} \qquad \text{(by the hypothesis)} \\
&= a^k aba^{-1} b^{-1} ba^{-k} b^{-1} \\
&= [a^{k+1}, b],
\end{aligned}$$

after combing a^k with a and a^{-1} with a^{-k}, cancelling the b's.

So the result is true for m = k + 1. Hence

$$[a, b]^m = [a^m, b]$$

for all positive integers m. Similarly

$$[a, b]^m = [a, b^m].$$

Hence we have 9.3.11 (1).

Next we see that if a and b have order m and n respectively and d = (m, n) is the greatest common divisor of m and n, we have

$$[a, b]^d = 1. \qquad 9.3.11\ (2)$$

For then we have $a^m = b^n = 1$ so that

$$[a, b]^m = [a^m, b] = 1$$

and

$$[a, b]^n = [a, b^n] = 1.$$

As

$$d = m\lambda + n\mu$$

for some integers λ, μ, we have

$$\begin{aligned}
[a, b]^d &= [a, b]^{m\lambda + n\mu} \\
&= [a, b]^{m\lambda} [a, b]^{n\mu} \\
&= 1.
\end{aligned}$$

Consequently if m and n are relatively prime integers, we have,

$$[a, b] = 1 \text{ that is } ab = ba.$$

Now let n be the order of G,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Let $H_1, H_2, \dots H_k$ be the corresponding Sylow p_i-subgroups, $1 \le i \le k$. Since the orders of H_j, H_i are relatively prime, H_j and H_i are permutable element-wise. Since G is generated by its Sylow p-subgroups, every $g \in G$ can be written as

$$g = h_1 h_2 \dots h_k, h_i \in H_i, 1 \le i \le k$$

So, for any $x_i \in H_i$.

$$g x_i g^{-1} = h_i x_i h_i^{-1}$$

is an element of H_i. Thus H_i is normal in G. By theorem 9.3.10, G is the direct product of its Sylow p-subgroups.

Let π be a non-empty set of prime numbers finite or infinite. Let G be a periodic group, that is, a group in which every element has finite order. G is said to be π-group if the prime divisors of the order of every element of G belong to π. If π consists of a single prime then we have the usual concept of a p-group as defined earlier.

A subgroup H of a group G is said to be a *π-subgroup* if H is a *π-group* in the sense defined above.

A π-subgroup H of a group G is said to be a Sylow π-subgroup of G if H is not contained in a larger π-subgroup of G. When $\pi = \{p\}$, we have the concept of a Sylow p-subgroup.

We state the following theorems. (For proofs see Theory of Groups by A. G. Kurosh Vol. II).

(a) Every group has Sylow π-subgroups.

(b) Every subgroup of a group G that is conjugate to a Sylow π-subgroup H of G is itself a Sylow π-subgroup of G. In particular, a Sylow π-subgroup cannot be conjugate to one of its proper subgroups.

(c) The normaliser of a Sylow π-subgroup is its own normaliser.

A subgroup H of a finite group G is said to be a *Hall subgroup* of G if the order and index of H are relatively prime to each other. Every Sylow p-subgroup of a finite group G is a Hall subgroup of G.

9.3.12 Theorem: If H is a Hall subgroup of G and A a normal subgroup of G then $A \cap H$ is a Hall subgroup of A.

Proof: Since A is normal in G, AH is a subgroup of G. Also

$$AH/A \cong H/(A \cap H)$$

so that $(AH : H) = (A : A \cap H)$. Moreover H is a Hall subgroup of AH. So the order of H and its index in AH are relatively prime. Hence the order of $A \cap H$ and its index in A are relatively prime. Thus $A \cap H$ is a Hall subgroup of A.

One of the many applications of Sylow theorems is to determine whether or nor a group of certain specific order can be simple. We illustrate the use of Sylow theorems in this connection by an example.

9.3.11. Example: A group of order 2540 cannot be simple.

For if G is a group of order

$$2540 = 2^2 . 5 . 127$$

then G has Sylow subgroups of orders 2^2, 5 and 127. The number of Sylow 127-subgroups is $1 + 127k$ and this number divides 2540. But it is easy to check that, for no value of k other than $k = 0$, $1 + 127k$ would divide 2540. Thus there is a unique Sylow 127-subgroup which must be normal in G by Corollary 9.2.3. Hence G cannot be simple.

EXERCISES

1. Show directly that a group of order 93 is cyclic.

2. Let G be a group of order $p^2 q$ where p and q are primes such that
   $q < p$ and $p^2 \not\equiv 1 \bmod q$. Then G is an abelian group.

3. Show that, in a group G, a normal p-subgroup is contained in every Sylow p-subgroup. (**Hint:** If N is a normal p-subgroup in G then N is contained in a Sylow p-subgroup H of G. Any

other Sylow p-subgroup is gHg^{-1}, $g \in G$. Hence $N \subseteq H$ implies $N = gNg^{-1} \subseteq gHg^{-1}$).

4. If N is a normal subgroup of a finite group G and index of N in G is prime to p, then N contains every Sylow p-subgroup of G.

(**Hint:** Index of N is prime to p. So there is a Sylow p-subgroup H of G which is also a Sylow p-subgroup of N. Every other Sylow p-subgroup is conjugate to H. Hence

$$H \subset N \text{ implies } gHg^{-1} \subseteq gNg^{-1} = N.$$

for all $g \in G$.)

5. If a group G is the direct product of its Sylow p-subgroup then every subgroup of G is direct product of the Sylow p-subgroup of that subgroup.

6. If G is a finite group and all its Sylow p-subgroups are abelian normal, then G is abelian.

7. Find all the Sylow 2-subgroups and Sylow 3-subgroups of the alternating group of degree 4.

8. Show that if a group G of order 56 contains eight subgroups of order 7 then every subgroup of G is abelian.

9. Show that there is no simple group of order 204.

10. Can a group of order 616 be simple?

11. Show that a group of order 200 contains a Sylow subgroup which is self-conjugate and hence show that no group of order 200 can be simple.

12. Find the number of elements of order 7 in the simple group of order 168.

(This simple group is the group of automorphisms of the abelian group

$$A = \langle a_i : a_i^2 = [a_i, a_j] = 1, i, j = 1, 2, 3 \rangle.$$

Chapter - X

GROUP ACTIONS

10.1. GROUP ACTION

Let X be a non empty set and G a group. By an *(left) action of* G *on* X we mean a mapping : $G \times X \to X$ which assigns, to each element (g, x) of $G \times X$, $g \in G$, $x \in X$, an element $g.\ x$ of X as its image under '.' satisfying the following conditions.

1. For any $x \in X$ and the identity element e of G,

$$\bullet : (e, x) = e.\ x = x \qquad 10.1(1)$$

2. For any $x \in X$ and $g, g' \in G$,

$$\bullet : (g'g, x) = (g'g).\ x = g'.\ (g.\ x) \qquad 10.1(2)$$

The set X, together with the group action of G on X, is called a *G-space* and G is called a *transformation group on X*.

The right action $\bullet : X \times G \to X$, of G on X is defined as

$$\bullet\ (x, g) = x.\ g \qquad 10.1(*)$$

for all $x \in X$, $g \in G$.

The set of those elements of G for which $g.\ x = x$, for all $x \in X$, is called the *kernel of the action.*

There is a close relationship between the set G/H of cosets of a subgroup H (not necessarily a normal subgroup) of a group G and the action of the group G on a set X. This will be explained later.

10.1. EXAMPLES:

10.1.1. Permutation Group Action: Let $X = \{1, 2, 3, ..., n\}$ and $G = \Sigma_n$ be the group of all permutations on X. Then, for any $x \in X$ and $\sigma \in G$, we define the mapping

$$\bullet : (G, X) \to X$$

by

$$\bullet : (\sigma, x) = \sigma(x). \qquad 10.1\ (*)$$

Let $\sigma_1, \sigma_2 \in G$. Then

$$(\sigma_1 \sigma_2) . x = \sigma_1 . (\sigma_2 . x)$$

and

$$I. x = x \qquad 10.1\ (*)$$

for all $x \in X$, I, being the identity of Σ_X.

So X is a G-set under the action 10.1 (*) of $G = \Sigma_X$.

Likewise every subgroup H of Σ_X also acts on X. This action is the restriction

$\bullet$: $(H \times G) \to X$ of the action of Σ_X on X.

10.1.2. (Group Action on Cosets): Let G be a group and H a subgroup of G. Let

$$X = \{xH : x \in G\}$$

be the set of all left cosets of H in G.

For each $g \in G$, we define an action of G on X by

$$\bullet : (g, xH) = g. (xH) \qquad 10.1.2\ (*)$$
$$= (gx)H$$

$xH \in X, x \in G$. Then, for $g, g' \in G$,

$$(g'g)(xH) = ((g'g)x)H$$
$$= (g'. (gx))H$$
$$= (g' . (g. (xH)))$$
$$= g'. (g. (xH))$$

and

$$e.\,(xH) = (ex)H$$
$$= xH$$

So (*) defines an action of G on X.

The set X, in this case, is called the *coset space* of G by H.

10.1.3. (Group Action as Left Multiplication in a Group-The Regular Group Action.): Let G be a group. Take $X = G$. Define a mapping $\bullet : G \times X \to X$ by

$$\bullet\,(g, x) = g.\,x \qquad 10.1.3\ (*)$$

for all $g \in G$, $x \in G$. Then (*) defines an action of G on $X = G$, called the *left multiplication in G*. Here

$$\bullet\ (e, x) = e.\,x = x$$

and, for $g, g' \in X$,

$$\bullet\ (g'g, x) = (g'g).\,x$$
$$= g'.\,(g.\,x)$$

for all $x \in G$, using the property of the identity element and the associative law in G.

10.1.4. (Group Action by Conjugation): For a group G, again take $X = G$. Define a mapping

$\bullet : (G, X) \to X$ as follows.

For any $g \in G$ and $x \in X = G$, we let

$$\bullet\ (g, x) = g.\,x \qquad 10.1.4\ (*)$$
$$= gxg^{-1}$$

Then, for all $x \in X$ and the identity e of G

$$\bullet\ (e, x) = e.\,x$$
$$= exe^{-1}$$
$$= x$$

and, for $g, g' \in G$,

$$\begin{aligned} \bullet\ (g'g, x) &= (g'g).\ x \\ &= g'gxg^{-1}g'^{-1} \\ &= g'(g.\ x)g'^{-1} \\ &= g'.\ (g.\ x) \end{aligned}$$

Hence $(*)$ defines an action of G on X.

The kernel of this action on G is the center $\zeta(G)$ of G.

10.1.5. (The Inner Automorphism Group Action): Let $I(G)$ denote the set of all inner automorphisms of a group G. Then, for any $I_g \in I(G)$ and $x \in X = G$, the mapping

$$\bullet :\ (I(G), X) \to X$$

defined by

$$\bullet\ (I_g, x) = gxg^{-1}$$

for $I_g \in I(G), x \in X$, defines a group action on $X = G$.

This group action is the same as the one in example 10.1.4.

10.1.6. (Subgroup Conjugation Action): Let G be a group and X be the set of subgroups (or all subsets) of G. Define a mapping

$$\bullet :\ (G, X) \to X$$

as follows. For each $H \in X$ and $g \in G$ we take

$$\begin{aligned} \bullet\ (g, H) &= g.\ H \qquad\qquad 10.1.6\ (*) \\ &= gHg^{-1} \end{aligned}$$

Then, for the identity e of G, we have

$$\begin{aligned} \bullet\ (e, H) &= e.\ H \\ &= eHe^{-1} \\ &= H \end{aligned}$$

and, for $g, g' \in G$,

$$\begin{aligned}(g', g, H) &= (g'\, g).\, H \\ &= g'\, gHg^{-1}\, g'^{-1} \\ &= g'\, (gHg^{-1})\, g'^{-1} \\ &= g'.\, (g.\, H)\end{aligned}$$

Hence X is a G-set under the action of G on X given by (*).

Note that, here also X is an $I(G)$ – set, where $I(G)$ is the set of all inner automorphisms.

10.1.7. (The Automorphism Group Action): Here, for a group G, let $A(G)$ be the group of all automorphisms of G. Define an action

$$\bullet : (A(G), G) \to G$$

of $A(G)$ on $G = X$ as follows.

For each $\alpha \in A(G)$, and $g \in G$, we put

$$\bullet\ (\alpha, g) = \alpha(g). \qquad 9.1.7\ (*)$$

Then (*) defines an action of $A(G)$ on G. Here it is easy to check that, for the identity automorphism I of $A(G)$,

$$\begin{aligned}(I, g) &= I.\, g \\ &= I(g) = g\end{aligned}$$

for all $g \in G$ and, for $\alpha, \beta \in A(G)$,

$$(\alpha\beta).\, g = \alpha.\, (\beta.\, g).$$

The restriction of this action to the subgroup $I(G)$ of $A(G)$, consisting of the inner automorphisms of G is the same as the one given in Example 10.1.6.

10.1.8. (Group Action on Polynomial Rings): Let R be a ring and $X = R[x_1, x_2, x_3, \ldots x_n]$ be the ring polynomials in the variables $x_1, x_2, x_3, \ldots, x_n$. Let Σ_n be the group of all permutations on $\{1, 2, 3, \ldots, n\}$ and $\sigma \in \Sigma_n$. We define an action of Σ_n on X as follows.

For an $f = f(x_1, x_2, x_3, \ldots, x_n) \in X$ we take

$$\sigma f = f(x_{\sigma(x_1)}, x_{\sigma(x_2)}, x_{\sigma(x_3)}, \ldots, x_{\sigma(x_n)}) \qquad 10.1.8(*)$$

Then, for the identity permutation I of Σ_n, and an $f \in X$,

$$I.f = f$$

Also, for $\tau, \sigma \in \Sigma_n$,

$$(\tau\sigma).f = f(x_{(\tau\sigma)(x_1)}, x_{(\tau\sigma)(x_2)}, x_{(\tau\sigma)(x_3)}, \ldots, x_{(\tau\sigma)(x_n)})$$
$$= f(x_{\tau.\sigma(x_1)}, x_{\tau.\sigma(x_2)}, x_{\tau.\sigma(x_3)}, \ldots, x_{\tau.\sigma(x_n)})$$
$$= \tau.(\sigma.f)$$

Hence

$$(\tau\sigma).f = \tau.(\sigma.f).$$

Therefore $(*)$ defines an action of Σ_n on X.

10.1.9. The Symmetry Group Actions on Geometrical Objects: Let V be an n-dimensional vector space over a field F. Then the set *Hom* (V, V) of all linear transformations $T : V \to V$, (*i.e.* T has the property that $T(\alpha x + \beta y) = \alpha Tx + \beta Ty$, for all x, y $\in$ V and $\alpha, \beta \in$ F), is a ring under the usual addition and successive application of mappings as multiplication.

The set of all invertible mappings in *Hom* (**V, V**) is the *general linear group* GL_n (**V**).

There is then a group action of the group $G = GL_n$ (**V**) on the vector space V with the identity mapping I as the identity of the group.

Similarly, the general linear group $GL\ (n, R) = G$ of invertible matrices with entries from a ring R, acts on the ring R.

Like wise we have actions of groups of symmetries of a geometrical figures like an equilateral triangle, a square, an n-polygon and polyhedral.

10.2. A BASIC THEOREM

Let G be a group. Then, for any set X, and Σ_X, as usual, the set of all permutations of X, we have the following important theorem.

10.2.1. Theorem: There is a one-one correspondence between the set of all actions of G on X and the set of all homomorphisms of G into Σ_X.

Proof: Let X be a G-set. Each action of G on X defined by a mapping $\alpha: (G, X) \to X$, is given by

$$\alpha(g, x) = \alpha(g)x = g.\, x \qquad 10.2.1\ (1)$$

$x \in X, g \in G$.

To see that $\alpha(g), g \in G$, is bijective on X we note that $\alpha(g^{-1})$ is the inverse of $\alpha(g)$. Here

$$\begin{aligned}(\alpha(g)\alpha(g^{-1}))x &= \alpha(g).\,(g^{-1}.\, x)\\ &= g.\,(g^{-1}.\, x)\\ &= (g.\, g^{-1}).\, g\\ &= e.\, x : e, \text{ the identity element of } G\\ &= x\end{aligned}$$

Similarly

$$\alpha(g^{-1})\ \alpha(g)x = x, \text{ for all } x \in G.$$

Hence

$$\alpha(g^{-1})\ \alpha(g) = \alpha(g)\alpha(g^{-1}) = I$$

so that

$$\alpha(g^{-1}) = (\alpha(g))^{-1}.$$

Thus $\alpha(g)$ is bijective and so is a permutation on X. Therefore $\alpha(g) \in \Sigma_X$. for all $g \in G$.

Next we show that α defines an action of G on X.

First we observe that if e is the identity element of G then $\alpha(e)$ is the identity mapping on X. Here

$$\alpha(e).\, x = e.\, x = x \qquad 10.2.1\ (i)$$

for all $x \in G$.

Also, for $g, g' \in G$,

$$\begin{aligned} \alpha(g'g)x &= (g'g).\, x \\ &= g'.\, (gx) \\ &= \alpha(g')\,(gx) \\ &= \alpha(g').\, (g.\, x) \\ &= \alpha(g').\, (\alpha(g)\, x) \\ &= (\alpha(g').\, \alpha(g))\, x \end{aligned}$$

for all $x \in X$. Hence (1) defines an action on X.

Moreover

$$\alpha(g'.\, g) = \alpha(g')\,.\,\alpha(g) \qquad 10.2.1\ (ii)$$

for all g, g' in G.

Now define a mapping $\varphi : G \to \Sigma_X$ as follows.

For each g in G we put

$$\varphi(g) = \alpha(g) \qquad 10.2.1\ (iii)$$

Equation 10.2.1 (ii) shows that φ is a homomorphism from G into Σ_X. So each action of G induces a homomorphism of G into Σ_X.

Conversely, suppose that $\sigma : G \to \Sigma_X$ is a homomorphism of G into Σ_X. Then, for each $g \in G$, $\sigma(g)$ is an element of Σ_X. Moreover $\sigma(e)$, e the identity element of G, is the identity permutation of Σ_X. Let

$$\bullet\ (g, x) = \sigma(g)\,.\, x = g.\, x \qquad 10.2.1\ (*)$$

for all $g \in G$, $x \in X$. Then, for the identity e of G,

$$\bullet\ (e, x) = \sigma(e).\, x = x$$

for all $x \in G$. Moreover

$$\begin{aligned} \bullet\ (g'g, x) &= \sigma(g'g).\, x \\ &= (\sigma(g')\sigma(g)).\, x \\ &= \sigma(g')\,(\sigma(g).\, x) \end{aligned}$$

$$= \sigma(g')\,(g.x)$$
$$= g'.(g.x)$$

for all $g', g \in G, x \in X$. So the mapping given by $(*)$ defines an action of G on X. Thus each homomorphism of G into Σ_X gives rise to an action of G on X. Hence there is a one-one correspondence between the set of all actions of G on X and the set of all homomorphism of G into Σ_X.

10.2.1. Remarks:

1. If H is a subgroup of G and X is a G-set then, with σ defining an action of G on X, the restriction of σ to (H, X) defines an action of H on X. So X also is an H-set.

2. A homomorphism φ from G to Σ_X, defined by 10.2.1 (*iii*) in the 10.2.1 Basic Theorem given above, is called a permutation representation of G corresponding to the action α of G on X.

3. An action of a group G on a set X is said to be *faithful* (or G *act on* X *faithfully*) if the homomorphism φ of G into Σ_X is injective.

4. An action of a group G on a set x is faithful if and only if only the identity element of G fixes every element of X.

5. In the discussion of group actions on a set X, we don't just look at the subgroups of Σ_X but also at the homomorphisms of groups into Σ_X.

10.3. ORBITS AND TRANSITIVE ACTIONS

Let X be a G-set. Define a relation '~' on X as follows:

For $x, y \in X$, we say that $x \sim_G y$ (read as 'x is G-equivalent to y') if there is a $g \in G$ such that

$$y = g.x. \qquad 10.3.\ (1)$$

10.3.1. Theorem: The relation $\sim_G$ defined by 10.3. (1) is an equivalence relation on X.

Proof:

1. '$\sim_G$' is reflexive. Here, for each $x \in X$ and the identity element e of x

$$x = e.x$$

2. '$\sim_G$' is symmetric. For if $x \sim_G y$, for $x, y \in G$, then there is a $g \in G$ such that

$$y = g.x.$$

But then, as $g^{-1} \in G$,

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

Hence $y \sim_G x$.

3. '$\sim_G$' is transitive. For if $x \sim_G y$ and $y \sim_G z$ then there are $g_1, g_2 \in G$ such that $y = g_1.x$ and $z = g_2.y$. So

$$\begin{aligned} z &= g_2.y \\ &= g_2.(g_1.x) \\ &= (g_2 g_1).x \\ &= g'.x \end{aligned}$$

for $g' = g_2 g_1 \in G$. Hence $x \sim_G y$ and $y \sim_G z$ imply $x \sim_G z$ and the relation is transitive.

Thus '$\sim_G$' is an equivalence relation.

As is the case for every equivalence relation, the relation '$\sim_G$' partitions X into equivalence classes. These equivalence classes are called the *orbits* or the *transitivity classes* of the action. Let an equivalence class determined by x be denoted by O_x.

That is

$$O_x = \{y \in X : y \sim_G x\}. \qquad 10.3.1(2)$$

Then

$$X = \cup O_x : x \in X. \qquad 10.3.1\ (3)$$

and

$$O_x \cap O_y = \phi \qquad 10.3.1\ (4)$$

for $x \neq y$, $x, y \in G$. So we have an *orbital partition* of X.

The set O_x, $x \in X$ is called an *orbit* of x in X under the action of G or simply a G-orbit. Thus the G-orbits determine a partition of X, called the G – *orbital partition* of X.

The set of all G-orbits is denoted by X/G.

Also, from 10.3.1 (2), and by labeling the orbits as $O_{x_1}, O_{x_2}, \ldots, O_{x_r}$, we have the following simple relation between the cardinalities of X and those of the orbits of the orbital partition of X.

$$|X| = |O_{x_1}| + |O_{x_2}| + \ldots + |O_{x_r}| \qquad 10.3.1\ (5)$$

The formula 10.3.1 (5) has a large number of important applications.

Let us write

$$Gx = \{g.x : g \in G\}. \qquad 10.3.1\ (6)$$

Gx is called the *G-stable subset* of X and contains x because $e \in G$.

If $Gx = X$ for some $x \in X$ then we say that *the action of G on X is transitive or G acts on X trasitively.*

Otherwise we say that the action of G on X is *intransitive.*

Moreover if $Gx = X$ for some $x \in X$, then, for every $y \in X$, $Gy = X$.

We then also call X a *homogeneous G-space.*

The regular action of G of $X = G$ is transitive.

Note that G acts transitively on each orbit.

Also G acts on X transitively if and only if G has only one orbit namely Gx for some $x \in X$.

A subset Y of X is *G-transitive or G-invariant* if $Gy = Y$ for some $y \in Y$.

As a subset of X, Gx also is a G-set under the action induced by the action of G on X. Here, for any $g' \in G$ and $gx \in Gx$,

$$g'.(g.x) = (g'g).x \in Gx.$$

So $G(Gx) = Gx$ for all $x \in X$.

An action of a group G on X is said to be *k-ply transitive* if, for any two k-element subsets

$$\{x_1, x_2, ..., x_k\}, \{y_1, y_2, ..., y_k\}$$

of X there is a $g \in G$ such that $y_i = g.x_i$, $1 \le i \le k$.

For $k = 2$, such an action of G on X is said to be *doubly transitive.*

To describe all G-subsets of a set X, it is enough to describe all its orbits.

10.3.2. Example: Let Σ_n be the group of permutations on $X = \{1, 2, 3, ..., n\}$. Then the action of Σ_n on X is transitive. Here, for any pair of elements $i, j \in X$, there is a permutation namely (ij) of Σ_n which changes i to j.

Similarly the natural action of A_n, $n \ge 3$, on X is transitive. For let $i, j \in X$. As $n \ge 3$ there is a $k \in X$ such that $\sigma = (ijk) \in A_n$. But then σ changes i to j.

We now give another characterization of a transitive action of a group G on X.

10.3.3. Theorem: G acts on X transitively if and only if for any $x, y \in G$, there is a $g \in G$ such that $y = g.\, x$.

Proof: Suppose that G acts on X transitively. Then, for any $x \in X$,

$$G.\, x = X. \qquad 10.3.3\ (*)$$

Assume that $x, y \in X$. Then, 10.3.3 $(*)$ means that for a $y \in G.\, x$ and there is a $g \in G$ such that $y = g.\, x$.

Conversely, suppose that, for any $x, y \in X$, there is a $g \in G$ such that $y = g.\, x$. Then

$$Gx = \{g.\, x : g \in G\} \subseteq X.$$

Also, for any $x_1 \in X$, there is a $g_1 \in G$ such that $g_1 x_1 = x$. So $x_1 = g_1^{-1}.\, x \in Gx$. Hence

$$X = \cup \{x_1 : x_1 \in X\} \subseteq Gx.$$

Thus $Gx = X$ and the action of G on X is transitive.

10.3.4. Theorem: For any subgroup H of G, the action of G on G/H (the coset space of G) is transitive.

Proof: For any $g_1, g_2 \in G$, g_1H, g_2H are arbitrary cosets of H in G. Take $g = g_2 g_1^{-1} \in G$. Then

$$\begin{aligned} g.\, (g_1H) &= (g_2 g_1^{-1}).\, (g_1H) \\ &= g_2.\, (g_1^{-1}\, g_1).\, H \\ &= g_2.\, (e.\, H) \\ &= g_2.\, H \end{aligned}$$

Hence the action of G on G/H is transitive.

OR, for any $gH \in G/H$, $g \in G$,

$$\begin{aligned} G\,(gH) &= \{g'.\, (gH) : g' \in G\} \\ &= \{(g'\, g)\, H : g' \in G\} \\ &= G/H. \end{aligned}$$

10.3.5. Theorem: Every *G-set X* has a unique partition consisting of transitive *G*-sets.

Proof: Suppose that X is a G-set. Then for each $x \in X$,

$$Gx \subseteq X.$$

Hence

$$\cup \{Gx : x \in X\} \subseteq X. \qquad 10.3.5\ (1)$$

Also, for each $x \in X$,

$$x = e.\ x \in Gx \subseteq \cup \{Gx : x \in X\}.$$

So

$$X \subseteq \cup \{Gx : x \in X\} \qquad 10.3.5\ (2)$$

Form 10.3.5 (1), 10.3.5 (2) we have

$$X = \cup \{Gx : x \in X\}. \qquad 10.3.5\ (*)$$

Next we show that the sets in the union are disjoint. For this let $x, y \in X$ and $Gx \cap Gy \neq \phi$.

If $u \in Gx \cap Gy$ then there are $g, g' \in G$ such that $u = gx = g'y$. So $x = (g^{-1} g')y \in Gy$.

Hence

$$Gx \subseteq Gy. \qquad 10.3.5\ (3)$$

Similarly

$$Gy \subseteq Gx. \qquad 10.3.5\ (4)$$

Form 10.3.5 (3) and 10.3.5 (4) we have

$$Gx = Gy.$$

So $\{Gx : x \in X\}$ defines a partition of G.

The equation 10.3.5 $(*)$ implies that

$$|X| = \sum_{x \in X} |Gx|. \qquad 10.3.5\ (5)$$

10.4. STABILIZERS

If X is a G-set and $x \in X$, then the subset

$$G_x = \{g \in G : g.x = x\} \qquad 10.4\ (1)$$

of G is called the *stabilizer of* x in G or the *isotropy group of* x in G.

10.4.1. Remarks:

1. *G_x is a subgroup of G.*

Here, for $g_1, g_2, \in G_x$,

$$\begin{aligned}(g_1 g_2^{-1}).x &= (g_1.(g_2^{-1}.x)\\ &= g_1.x\\ &= x\end{aligned}$$

Hence $g_1 g_2^{-1} \in G$. So G_x is a subgroup of G.

In fact *G_x is a normal subgroup of G* because, for every $g_1 \in G$ and $g \in G_x$,

$$\begin{aligned}(g_1 g g_1^{-1})(x) &= (g_1(g.(g_1^{-1}.x)))\\ &= g_1.(g_1^{-1}x)\\ &= (g_1 g_1^{-1}).x\\ &= e.x = x\end{aligned}$$

because $g_1^{-1}x \in X$ and $g.x = x$ for all $x \in X$. Hence $g_1 g g_1^{-1} \in G_x$.

It is clear that the action of G on X is faithful or regular if and only if $G_x = \{e\}$.

2. If X is a G-set then, for any $x \in X$ and $g \in G$,

$$G_{g.x} = gG_x g^{-1} \qquad 10.4.1\ (2)$$

Here, for any $u \in G_{g.x}$,

$$u \in G_{g.x} \Leftrightarrow u.(g.x) = g.x$$

$$\Leftrightarrow (g^{-1}ug).x = x$$

$$\Leftrightarrow (g^{-1}ug) \in G_x$$

$$\Leftrightarrow u \in gG_xg^{-1}$$

$$\Leftrightarrow G_{g.x} = gG_xg^{-1}$$

Hence (2) holds.

In a similar fashion, one can prove that, if G_S is the stabilizer of $S \subseteq X$, *i.e.*,

$$GS = \{g \in G : g.s = s, s \in S\}$$

then

$$Stab\,(gS) = G_{g.S} = gG_sg^{-1} \qquad 10.4.1\ (3)$$

$$= \bigcap_{x \in S} gG_xg^{-1}$$

We relate examples of stabilizers with examples of group actions.

10.4.2. Examples:

1. Let $X = \{1, 2, 3\}$ and $G = \Sigma_3$. Then

$$G = \{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

where

$$I = (1),\ \sigma = (123),\ \sigma^2 = (132),\ \tau = (12),\ \sigma\tau = (13),\ \sigma^2\tau = (23).$$

Moreover the stabilizers of 1, 2, 3 are

$$G_1 = \{I, (23)\},\ G_2 = \{I, (13)\},\ G_3 = \{I, (12)\}.$$

Note that the orbits of 1, 2, 3 are

$$G1 = \{1, 2, 3\} = X = G2 = G3$$

respectively.

2. Let $G = \{\pm I, \pm i, \pm j, k\}$ be the group of quaternion and $X = G$. Let the action of G on X be the usual left multiplication in G, *i.e.*, for $x \in X = G$ and $g \in G$, we have

$$g.x = gx.$$

Then

$$GI = X = G = Gi = Gj = Gk.$$

So the action of G on $X = G$ is transitive.

Next, for any $x \in X = G$,

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

So the stabilizer of each element of X is $\{I\}$.

3. Let G be any group and $I(G)$ be the group of all inner automorphisms of G. Then $I(G)$, as a group, acts on $X = G$ by

$$I_g.\,(x) = gxg^{-1},\ g \in X = G.$$

for all $x \in X$.

The orbit of $x \in X$ under $I(G)$ is

$$\begin{aligned} I(G)x &= \{I_g.\, x : g \in G\} \\ &= \{gxg^{-1} : g \in G\} \end{aligned}$$

which is the set of elements of G conjugate to x *i.e.*, the conjugacy class containing x.

Also the stabilizer of $x \in X = G$ is

$$\begin{aligned} I(G)_x &= \{g \in G : I_g\,.\, x = gxg^{-1} = x\} \\ &= \{g \in G : gxg^{-1} = x\} \end{aligned}$$

which is the centralizer $C_G(x)$ of x in G.

4. Let H be a subgroup (or a subset) of a group G and $X = \{H: H \subseteq G\}$. Under the action of G on X defined by

$$(g, H) \to g.\, H = gHg^{-1},\ g \in G$$

the orbit of H is

$$\begin{aligned} G.\, H &= \{g.\, H = gHg^{-1} : g \in G\} \qquad 10.4.2\ (1) \\ &= \{gHg^{-1} : g \in G\} \end{aligned}$$

which is the set of all conjugate subgroups (or subsets) of H in G.

Equation 10.4.2 (1) also shows that, for any subgroup H of a group G, *the number of conjugate subgroups of H is equal to the number of elements in the orbit $G.H$ of the subgroup H in the group G.*

The stabilizer of H is

$$G_H = \{g \in G : g.H = H,\} \qquad 10.4.2\ (2)$$
$$= \{g \in G : gHg^{-1} = H\}$$

which is the normaliser $N_G(H)$ of H in G.

The equation $G_H = N_G(H) = \{g \in G : gHg^{-1} = H\}$ also shows that the stabilizer G_H is the smallest subgroup of G in which H is normal.

By the Orbit-Stabilizer Theorem 10.5.2 we have

$$|G| = |GH| \times |G_H| \qquad 10.4.2\ (o\text{-}s\text{-}1)$$

which shows that the number of conjugate subgroups of a subgroup H is equal to the index of its normaliser in G.

This provides yet another proof of Theorem 5.4.8.

The equation 10.4.2 (o-s-1) also shows that there is a natural bijection φ between the collections

$$\{O_x : x \in X\}$$

of all the orbits O_x of $x \in X$ and the set $\{gG_x : g \in G\}$ of all the left cosets of G_x given by

$$\varphi(gG_x) = g.x. \qquad 10.4.2\ (o\text{-}s\text{-}2)$$

10.5. MAPPINGS BETWEEN G-SETS: THE ORBIT STABILIZER THEOREM

Let X and Y be G-sets. We denote the action of G on X and Y by the same symbol namely '.'.

A mapping $\varphi : X \to Y$ is said to be a *G-set homomorphism* if, for each $x \in X$ and any $g \in G$,

$$\varphi(g.x) = g.\varphi(x). \qquad 10.5\ (*)$$

If, in addition, φ is also bijective then φ is said to be a *G-set isomorphism.*

In case of G-isomorphism between X and Y, the two sets are called *isomorphic G-sets.*

We know that the coset space G/H of G over H is a transitive G-set.

We now prove the following:

10.5.1. Theorem: Let G be group. Then every transitive G-set X is G-set isomorphic to a coset space G/G_x of G by G_x, $x \in X$.

Proof: Let X be a transitive G-set. Define a mapping $\varphi : G/G_x \to X$ as follows:

For each $x \in X$ and $gG_x \in G/G_x$, we put

$$\varphi(gG_x) = g.x. \qquad 10.5.1\ (1)$$

Then φ is well defined: For if gG_x, $g'G_x \in G/G_x$, and $gG_x = g'G_x$ then $g^{-1}g' \in G_x$. So $(g^{-1}g').x = x$. That is $g.x = g'.x$. Hence

$$\varphi(gG_x) = g.x = g'.x = \varphi(g'G_x).$$

Next, φ is injective.

Here, for gG_x, $g'G_x \in G/G_x$,

$$\phi(g(G_x) = \phi(g'G_x)$$

implies $g.x = g'.x$. That is, $(g^{-1}g').x = x$. Hence $g^{-1}g' \in G_x$. So $gG_x = g'G_x$. Thus φ is injective.

Lastly, let $y \in X$. Since X is G-transitive and $x \in X$, there is a $g \in G$ such that

$$y = g.x = \varphi(gG_x)$$

So φ is surjective.

Also, for each $g, g^* \in G$,

$$g^*.\ \varphi(gG_x) = g^*.\ g.\ x$$
$$= (g^*\ g).\ x$$
$$= g^*.\ (g.\ x)$$
$$= \varphi\ (g^*.\ (gG_x)).$$

Therefore φ is a G-set isomorphism.

The above Theorem yields the following important result.

10.5.2. Theorem (The Orbit-Stabilizer Theorem): Let X be a G-set. Then the sets G_x and G/G_x and G-set isomorphic as sets.

Specifically, if G is finite then

$$|Gx| = [G : G_x]. \qquad 10.5.2\ (1)$$

That is, (*The order of the orbit of* $x \in X$ = *The index of the stabilizer of* x.) 10.5.2 (2)

Or

$$|G| = |Gx|\ .\ |G_x|. \qquad 10.5.2\ (3)$$

Or

(Order of G) = (Order of the orbit) (Order of the stabilizer) 10.5.2 (4)

(The relation 9.5.2 (3) is also called the *counting formula* for group actions.)

Proof: Since Gx is a transitive G-set, it is G-set isomorphic to G/G_y, for every $y = g.\ x \in G_x$, $x \in X$, by the above theorem.

Specifically, if G is finite then, $Gx \simeq G/G_x$ implies

$$|Gx| = [G : G_x].$$

which is equation 10.5.2 (1).

Similarly for the other forms.

From the relation 10.5.2 (1) above, we have the following obvious corollary.

10.5.3. Corollary: The order or number of elements in an orbit divides the order of the group.

10.5.4. Theorem: Let $\varphi : X \to Y$ be a G-set homomorphism and $x \in X$. Then

$$G_x \subseteq G_{\varphi(x)}.$$

In particular, if φ is a G-set isomorphism then,

$$G_x = G_{\varphi(x)}.$$

Proof: Let $g \in G_x$ so that $g.x = x$. Then

$$\begin{aligned}\varphi(x) &= \varphi(g.x)\\ &= g.\varphi(x).\end{aligned}$$

So g fixes $\varphi(x)$. Hence $g \in G_{\varphi(x)}$. So

$$G_x \subseteq G_{\varphi(x)}.$$

In particular, if φ is a G-set isomorphism then G_x, as a subset of $G_{\varphi(x)}$, and G-set isomorphic to $G_{\varphi(x)}$, is equal to $G_{\varphi(x)}$.

10.6. APPLICATIONS TO GROUP THEORY

In the following paragraphs we describe use of group actions to concepts of groups.

We have already seen that, for a group G and a subgroup H of it, the set G/H, of cosets of H in G, is a G-set, under the action of G given by:

$$\bullet : (g^*, gH) \to g^* . (gH) = (g^*g).H.$$

Also any two cosets $eH = H$ and gH have the same number of elements. Moreover the action of G on the coset space G/H is transitive.

10.6.1. (Action of a subgroup on the group):

The lagrange's theorem: Let G be a finite group and H a subgroup of G. Then the order and index of H divide the order of G.

Proof: For a subgroup H of G we can define an action α of H on G as follows:

Let $h \in H$ and $g \in G$. We put

$$\alpha(h, g) = gh. \qquad 10.6.1\ (1)$$

Then

$$\alpha(e, g) = ge = g$$

and

$$\begin{aligned}\alpha(h_1h_2, g) &= g(h_1h_2)\\ &= (gh_1)\, h_2\\ &= \alpha(h_2, gh_1)\\ &= \alpha(h_2, \alpha(h_1, g)).\end{aligned}$$

So 10.6.1 (i), indeed, defines an action of H on G.

For any $g \in G$, the stabilizer H_g of g is

$$H_g = \{h \in H : gh = g\} = \{e\}.$$

So only the identity element of H fixes every element of G. Hence the action of H on G is faithful.

More over the H –orbit of $g \in G$ is the coset

$$\{gh : h \in H\} = gH$$

of H in G. Let g_1H, g_2H, ..., g_rH be all the distinct left cosets (orbits) of H in G. These r cosets are mutually disjoint because they arise out of an action of H on G. By the Orbit-Stabilizer Theorem,

$$\begin{aligned}|gH| &= [H : H_g]\\ &= |H|\end{aligned}$$

Now let G be of order n and H, a subgroup of G, of order m. Then, from.

$$G = \cup H_i,\ i = 1, 2, ..., r,$$

we have

$$|G| = \Sigma_{i=1}^{r} |Hg_i|$$

or

$$n = |G| = m.\, r. \qquad 10.6.1\ (2)$$

The above equation shows that the order m and index r of a subgroup H of a group G are divisors of the order of G, which is the Lagrange's Theorem.

10.6.2. Corollary: The order of an element of a finite group G divides the order of G.

Proof: Here the order of an element a is the order of the subgroup generated by a and Theorem 10.6.1 applies.

10.6.3. Theorem (The Class Equation):

Let G be a finite group. Then

$$|G| = \sum_{1}^{q} |C_{x_i}| \qquad 10.6.3 \text{ (C-E-1)}$$

Where $|C_{x_i}|$ is number of elements in the conjugacy class C_{x_i} determined by $x_i \in G$ in G and q is the number of such conjugacy classes.

Proof: We have already seen that, for the group G and $X = G$, the function

$$\bullet : (G, X) \to X$$

defined by

$$\bullet\ (g, x) = gxg^{-1}$$

is an action of G on $X = G$. The stabilizer of an $x \in G$ is

$$G_x = \{g \in G : g.\ x = gxg^{-1} = x\} = C_G(x)$$

where $C_G(x)$ is the centralizer of x in G.

The orbit of x in G is

$$Gx = \{g.\ x = gxg^{-1} : g \in G\} \qquad 10.6.3 \text{ (1)}$$
$$= \{gxg^{-1} : g \in G\}$$

which is the conjugacy class C_x of x in G.

So, by the Orbit-Stabilizer Theorem, we have

$$|Gx| = \frac{|G|}{|G_x|} \qquad 10.6.3 \text{ (2)}$$

Or

$$|G_x| = \frac{|G|}{|Gx|} \qquad 10.6.3\ (3)$$

More over, if k is the total number of orbits under the group action given above then

$$|G| = \sum_{i=1}^{k} |Gx_i| = \sum_{i=1}^{k} \frac{|G|}{|G_{x_i}|} = \sum_{i=1}^{k} |C_{x_i}|. \qquad 10.6.3\ (4)$$

Here $Gx = C_x$, the conjugacy class containing x. The number of elements in C_x is equal to the index of the normalizer of x in G.

A conjugacy class consists of only one element if and only if that element is in the centre of G.

If n_1 is the number of conjugacy classes of such elements and $n_2, n_3, \ldots, n_k$ are the number of elements in the respective remaining conjugacy classes then we have an equation

$$|G| = \sum_{i=1}^{k} n_i$$

$$= |\zeta(G)| + \sum_{i=2}^{k} n_i \qquad 10.6.3\ (C\text{-}E\text{-}2)$$

which is equivalent to 10.6.3 (C-E-1).

10.6.4. Theorem: If G is a finite group and H a subgroup of G then the number of subgroups conjugate to H is equal to the index of the normalize of H in G. That is

$$|C_H| = \frac{|G|}{|N_G(H)|} \qquad 10.6.4\ (1)$$

where C_H is the conjugacy class of H and $N_G(H)$ is the normalizer of H in G.

Proof: For a subgroup H of a group G and $X = \{H : H \subseteq G\}$, the function

$$\bullet : (g, H) \to g.H = gHg^{-1}, g \in G \qquad 10.6.4\ (2)$$

defines an action of G on X. The orbit of H is

$$G.H = \{g.H, g \in G\} \qquad 10.6.4\ (3)$$

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

which is the conjugacy class C_H of the subgroup H in G. The stabilizer of H is

$$G_H = \{g \in G : g.H = gHg^{-1} = H\} \qquad 10.6.4\ (4)$$

which is the normalizer $N_G(H)$ of H in G. By the Orbit-Stabilize Theorem

$$|C_H| = |G.H| = \frac{|G|}{|G_H|} \qquad 10.6.4\ (5)$$

Or

$$|C_H| = \frac{|G|}{|N_G(H)|} \qquad 10.6.4\ (6)$$

Thus the number of conjugate subgroups of a subgroup H in G is equal to the index of the normalizer of H in G.

10.6.5. Theorem: Let H, K be subgroups of a group G. Then

$$|HK| = \frac{|HK|}{|H \cap K|} \qquad 10.6.5\ (1)$$

Proof: We first note that, here we have not necessarily taken any of H or K to be a normal subgroup of G. Thus HK may be just a subset of G. However

$$HK = \{hK : h \in H\} \qquad 10.6.5\ (2)$$

and HK is the union of all hK, $h \in H$. As K is a left coset eK of K, the orbit of K in HK is given by $\{hK : h \in H\}$ which are all disjoint and the number of elements in each coset is $|K|$. Hence the number of elements in the H-Orbit of K is

$$|O_K| = |HK|$$

We look at the stabilizer of K in HK which, under the (left)-regular action of H on K, is

$$\{h \in H : h.K = K\}.$$

But $hK = K \Leftrightarrow h \in K$. Also each element of K is in the stabilizer. So the stabilizer of K is

$$H \cap K.$$

Hence, by the Orbit-Stabilizer Theorem, we have

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

which is the relation 10.6.5 (1).

10.6.6. Lemma: For any subsets A, B of a group G and a $g \in G$,

$$g(A \cap B)g^{-1} = (gAg^{-1}) \cap (gBg^{-1}). \qquad 10.6.6\ (*)$$

Proof:

Here

$$gyg^{-1} \in g(A \cap B)g^{-1}, y \in A \cap B$$
$$\Leftrightarrow gyg^{-1} \in gAg^{-1} \cap gBg^{-1}$$
$$\Leftrightarrow g(A \cap B)g^{-1} = gAg^{-1} \cap gBg^{-1}$$

as required.

Let H, K be subgroups of a group G. For any $x \in G$ the set

$$HxK = \{hxk : h \in H, k \in K\}$$

is called a *double coset of G modulo H, K.*

It easy to see that two double cosets HxK and HyK are either identical or disjoint. We now have the following theorem about the number of elements in a double coset HxK.

10.6.6. Corollary: Let H, K be finite subgroups of a group G. Then

$$|HxK| = \frac{|H|\,|xKx^{-1}|}{|H \cap (xKx^{-1})|} \qquad 10.6.6\ (1)$$
$$= \frac{|K||H|}{|K \cap (xHx^{-1})|}$$

Proof: The number of elements in HxK is the product of the number of left coset hxK, $h \in H$ by the number of elements in xK. Also, under the usual action of H on the set of left cosets xK of K, HxK is the H-orbit of the coset xK of K in G. Hence HxK has

$$|HxK| = |HxKx^{-1}| = |HK'|, K' = xKx^{-1}.$$

elements. We now use Theorem 10.6.5, knowing the fact that K and xKx^{-1} have the same order.

So,

$$|HxK| = |HxKx^{-1}|$$
$$= \frac{|H||K'|}{|H \cap K'|}$$
$$= \frac{|H|\,|xKx^{-1}|}{|H \cap (xKx^{-1})|}$$
$$= \frac{|H|\,|K|}{|H \cap (xKx^{-1})|}$$

as required.

Interchanging the role of H and K, considering the left action of K on the set of left cosets of xH in KxH, we have

$$|KxH| = \frac{|K||xHx^{-1}|}{|K \cap (xHx^{-1})|}$$
$$= \frac{|K||H|}{|K \cap (xHx^{-1})|}$$

Using $|HxK| = |KxH|$, we have the required result. This completes the proof of the theorem.

10.6.7. Theorem: (Theorem of Poincare) Let G be a group and H, K be subgroups of G. Then

$$[G : H \cap K] \leq [G : H]\,[G : K]. \qquad 10.6.7\ (1)$$

Proof: The factor set $G/(H \cap K) = \{g(H \cap K) : g \in G\}$. Also the sets G/H and G/K are

$$G/H = \{gH : g \in G\} \text{ and } G/K = \{gK : g \in G\}$$

Consider the set

$$G/H \times G/K = \{(gH, gK) : g \in G.\}$$

and the mapping $\varphi : G/(H \cap K) \to G/H \times G/K$ defined by

$$\varphi(g(H \cap K)) = (gH, gK) : g \in G.$$

Then φ is obviously well-defined. Moreover φ is injective. This follows form

$$\varphi(g(H \cap K)) = \varphi(g'(H \cap K))$$
$$\Rightarrow (gH, gK) = (g'H, g'K)$$
$$\Rightarrow gH = g'H, gK = g'K$$
$$\Rightarrow g^{-1}g' \in H \text{ and } g^{-1}g' \in K$$
$$\Rightarrow g^{-1}g' \in H \cap K$$
$$\Rightarrow g' \in g(H \cap K)$$
$$\Rightarrow g(H \cap K) = g'(H \cap K).$$

Hence

$$|G/(H \cap K)| \leq |G/H \times G/K|$$

But $|G/H| = [G: H]$, $|G/K| = [G: K]$ and $|G/(H \cap K)| = [G: H \cap K]$. Therefore

$$[G : H \cap K] \leq [G : H]\,[G : K]$$

as required.

EXERCISES

1. Let X be a square with vertices A, B, C, D and $G = S_4$, the symmetric group of degree 4. Describe the action of G on X. Is this action on X transitive?

   Indicate the orbits and stabilizers of each element of X under G. Also verify the Orbit-Stabilizer Theorem for each element of X.

   What are the orbits and stabilizers of the mid points of the sides of X and of the mid points of its diagonals?

   Also find the orbits and stabilizers of points x of X which devide the sides of X in the ratio 1 : 3.

2. Let $X = \{1, 2, 3, 4, 5\}$ and $G = \langle(123)(45)\rangle$ be a cyclic subgroup of S_6 with the usual action on X. Find all the orbits of X under this action of G.

3. Let G be a finite group and p be a prime number. Suppose that p^r divides the order of G. Show that G has a proper subgroup of order p^r.

4. Let G be finite group and p be prime dividing the order of G. A subgroup H of G is said to be a Sylow p-subgroup of G if, for some integer k, p^k is the highest power of p dividing the order of G.

   Show, by using the concept of group actions, that G has a Sylow p-subgroup for every such prime and that any two Sylow p-subgroups are conjugate.

Chapter - XI

SERIES IN GROUPS

Various techniques are used to discuss the structure of a group. We have already seen as to how subgroups and normal subgroups of a group give us information about the structure of that group. In the present chapter we discuss the notion of sub-normal subgroups of a group. This notion leads us to the concept of normal series[§] in groups. The usefulness of this concept will become apparent in later chapters on solvable and nilpotent groups.

11.1. ZASSENHAUS' BUTTERFLY LEMMA

In this section we prove an important result due to Zassenhaus. This result will be used in the subsequent discussion.

11.1.1. Theorem: (Zassenhaus' Butterfly Lemma)

Let H, H′, K, K′ be subgroups of a group G with H′ normal in H and K′ normal in K. Then H′(H ∩ K′) and K′(K ∩ H′) are normal subgroups of H′(H ∩ K) and K′(K ∩ H) respectively and the corresponding factor groups are isomorphic. That is

$$H'(H \cap K)/_{H'(H \cap K')} \cong K'(K \cap H)/_{K'(K \cap H')}$$

Proof: Put

$$U = H \cap K$$

$$V = (H \cap K') \,.\, (K \cap H')$$

Since $H' \subseteq H$, $K' \subseteq K$,

$$H \cap K' \subseteq H \cap K = U$$

$$K \cap H' \subseteq H \cap K = U$$

so that $H \cap K'$ and $K \cap H'$ are subgroups of U. Also if $x \in H \cap K'$ and $u \in U$ then:

[§] Some authors call it *subnormal series.*

$uxu^{-1} \in H$ (because x and u are in H and H is a subgroup)

$\in K'$ (because $x \in K'$, $u \in K$ and K' is normal in K).

Hence $uxu^{-1} \in H \cap K'$. So $H \cap K'$ is normal in U.

By symmetry, $K \cap H'$ is normal in U. So the product

$$(H \cap K') \,.\, (K \cap H') = V$$

of two normal subgroups of U is normal in U. Thus we can form the factor group U/V.

Next since H' is normal in H and $H \cap K'$ is a subgroup of H, $H'(H \cap K')$ is a subgroup of H. $H'(H \cap K')$ is also a subgroup of $H'(H \cap K)$ because $H'(H \cap K')$ is contained in $H'(H \cap K)$ and is a subgroup. Define a mapping

$$\varphi : H'(H \cap K) \to U/V$$

by:

$$\varphi(h'u) = Vu,\ h' \in H' \text{ and } u \in H \cap K = U.$$

Then φ is well-defined. For, if $h'u = h_1'u_1$ for $h'u$ and $h_1'u_1$ in $H'(H \cap K)$, then

$$h'^{-1} h_1' = u u_1^{-1},\ uu_1^{-1} \in H \cap K \subseteq K,\ h'h' \in H',$$

belongs to $H' \cap K \subseteq V$. So $u u_1^{-1} \in V$. That is $u \in Vu_1$. But $u \in Vu$. Hence $Vu = Vu_1$. So $\varphi(h'u) = \varphi(h_1' u_1)$.

Also
$$\varphi(h' u \,.\, h_1u_1) = \varphi(h'h_2' u u_1)$$
$$= Vuu_1$$
$$= Vu \,.\, Vu_1$$
$$= \varphi(h'u) \,.\, \varphi(h_1' u_1).$$

So φ is a homomorphism. φ is clearly surjective. By the fundamental theorem of homomorphism

$$H'(H \cap K)/W \cong U/V$$

where W is the kernel of φ. We show that

$$W = H'(H \cap K').$$

Let $w \in W$. Then $w = h'u$ for some $h' \in H'$ and $u \in U$. Hence

$$\varphi(w) = Vu = V.$$

So $u \in V = (H \cap K') . (K \cap H')$. Thus

$$u = a . b_1,\ a \in H \cap K',\ b_1 \in K \cap H' \subseteq H'$$
$$= b . a,\ b \in K \cap H' \subseteq H'.$$

because $K \cap H'$ is normalised by $H \cap K'$. Hence, as $h'b \in H'$ whenever $h', b \in H'$,

$$w = h'u = h'b. a$$

is in $H'(H \cap K')$. So

$$W \subseteq H'(H \cap K'). \qquad 11.1.1\ (1)$$

Conversely, let $h'u \in H'(H \cap K')$, $h' \in H'$, $u \in H \cap K'$. As $H \cap K' \subseteq V$, $u \in V$ so

$$\varphi(h'u) = Vu = V.$$

Hence $h'u \in W$. Thus

$$H'(H \cap K') \subseteq W. \qquad 11.1.1\ (2)$$

So

$$H'(H \cap K)/H'(H \cap K') \cong U/V. \qquad 11.1.1\ (3)$$

Incidently it follows that $H'(H \cap K')$, as the kernel of a homomorphism, is normal in $H'(H \cap K)$.

Since U and V remain unchanged if H and H′ are interchanged by K and K′ respectively we have, by symmetry,

$$K'(K \cap H)/K'(K \cap H') \cong U/V. \qquad 11.1.1\ (4)$$

From (3) and (4) we obtain the required isomorphism.

11.2. NORMAL SERIES

Let G be a group and A a subgroup of G. A finite sequence of subgroups.

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supset G_{i+1} \ldots \supseteq G_k = A \qquad 11.1.1\ (1)$$

is said be a *normal series or a sub invariant series from G to A* if every G_i is a normal subgroup of G_{i-1}.

If A is the identity subgroup E of G then 11.1.1 (1) is called *a normal series of G.*

11.2.1. Example:

(a) Every group G has a normal series namely the series
$G = G_0 \supseteq G_1 = E$.

(b) If H is a normal subgroup of G then a normal series for G is
$G \supseteq H \supseteq E$.

(c) Let $G = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$ be the dihedral group of order 8. Then

$$A = \langle a : a^4 = 1 \rangle$$

is normal in G. So

$$G \supset A \supset E$$

is a normal series for G.

Also, since

$$B = \langle a^2 : a^4 = 1 \rangle$$

is normal in A, another normal series for G is

$$G \supset A \supset B \supset E.$$

Let

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq \ldots \supseteq G_k = E \qquad 11.2.1\ (2)$$

and

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_j \supseteq \ldots \supseteq H_l = E \qquad 11.2.1\ (3)$$

be two normal series for G. The series 11.2.1 (3) is said to be a *refinement* of the series 11.2.1 (2) if every G_i that occurs in 11.2.1 (2) also occurs in 11.2.1 (3).

For example

$$G \supset A \supset B \supset E$$

is a refinement of

$$G \supset A \supset E$$

is example 11.2.1 (c) above.

In particular every normal series of a group G is a refinement of itself.

In the normal series 11.2.1 (2), the factor groups

$$G_{i-1}/G_i \qquad i = 1, 2, ..., k$$

are called *normal factors*[§] of the normal series. The number of such factors in (2) is called the *length* of that series.

The normal series 11.2.1 (2) and 11.2.1 (3) of a group G are said to be *isomorphic* if their lengths are equal and their factors can be put in on-one correspondence such that the corresponding factors are isomorphic.

11.2.2. Example: Let

$$G = < a : a^6 = 1 >.$$

Then

$$H = < a^3 : a^6 = 1 > \text{ and } K = < a^2 : a^6 = 1 >$$

are normal subgroup of G having order 2 and 3 respectively. The series

$$G \supset H \supset E$$

$$G \supset K \supset E$$

are isomorphic normal series for G. Here the factors for these series are

G/H, H/E and G/K and K/E

respectively. G/H is isomorphic to the factor K/E (both are of order 3) and the factor H/E is isomorphic to G/K (both are of order 2).

11.2.3. Theorem: (Schreier's Refinement Theorem).

Any two normal series of a group G have isomorphic refinements.

Proof: Let

$$G = G_0 \supseteq G_1 \supseteq ... \supseteq G_i \supseteq ... \supseteq G_k = E \qquad 11.2.3\ (1)$$

and

$$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_j \supseteq ... \supseteq H_l = E \qquad 11.2.3\ (2)$$

by any two normal series for a group G. Put

$$G_{ij} = G_i (G_{i-1} \cap H_l)$$

$$H_{ij} = H_j (H_{j-1} \cap H_i)$$

for i = 1, 2, ..., k, j = 1, 2, ..., l Since G_i is normalised by $G_{i-1} \cap H_j$ and both are subgroups, G_{ij} is a subgroup of G. Similarly H_{ij} is a subgroup of G. Also

$$G_{i0} = G_i . (G_{i-1} \cap H_0)$$

$$= G_i \cdot (G_{i-1} \cap G)$$

$$= G_i \cdot G_{i-1}$$

$$= G_{i-1} \qquad \text{because } G_i \subseteq G_{i-1}$$

and

$$G_{il} = G_i \cdot (G_{i-1} \cap H_l)$$

$$= G_i \cdot (G_{i-1} \cap E)$$

$$= G_i$$

Similarly

$$H_{0j} = H_{j-1} \text{ and } H_{kj} = H_j.$$

Also, since H_j is a subgroup of H_{j-1}, G_{ij} is a subgroup of $G_{i,j-1}$.

Similarly H_{ij} is a subgroup of $H_{i-1,j}$. We show that G_{ij} and H_{ij} are normal in $G_{i,j-1}$ and $H_{i-1,j}$ respectively.

For this we put

$$G_{i-1} = H,\ G_i = H',\ H_{j-1} = K,\ H_j = K'$$

in Zassenhaus lemma. So

$$H'(H \cap K') = G_i(G_{i-1} \cap H_j)$$

$$= G_{ij}$$

is normal in

$$H'(H \cap K) = G_i(G_{i-1} \cap H_{j-1}) = G_{i,j-1} \qquad 11.2.3\ (3)$$

while

$$K'(K \cap H') = H_j(H_{j-1} \cap G_i)$$

$$= H_{ij}$$

is normal in

$$K'(K \cap H) = H_j(H_{j-1} \cap G_{i-1}) = H_{i-1,j} \qquad 11.2.3\ (4)$$

But then the corresponding factor groups are isomorphic , by Zassenhaus' Lemma. Thus:

$$G_{i,j-1}/G_{ij} \cong H_{i-1,j}/H_{ij} \qquad 11.2.3\ (5)$$

Now between the terms G_{i-1}, G_i and between H_{j-1}, H_j we insert $(l-1)$ additional terms

$$G_{i-1} = G_{i0} \supseteq G_{i1} \supseteq G_{i2} \supseteq \ldots \supseteq G_{ij} \supseteq \ldots \supseteq G_{il} = G_i$$

and $(k-1)$ additional terms

$$H_{j-1} = H_{0j} \supseteq H_{1j} \supseteq \ldots \supseteq H_{ij} \supseteq \ldots \supseteq H_{kj} = H_j$$

and obtain refinements

$$G = G_0 = G_{10} \supseteq G_{11} \supseteq G_{12} \supseteq \ldots \supseteq G_{1l} = G_1 = G_{20} \supseteq G_{21} \supseteq \ldots \supseteq G_{i-1} = G_{i0} \supseteq G_{i1} \supseteq \ldots \supseteq G_{il} = G_i \supseteq \ldots \supseteq G_{kl} = G_k = E \qquad 11.2.3\ (6)$$

and

$$G = H_0 = H_{01} \supseteq H_{11} \supseteq H_{21} \supseteq \ldots \supseteq H_{k1} = H_1 = H_{02} \supseteq H_{12} \supseteq \ldots H_{j-1} = H_{0j} \supseteq H_{1j} \supseteq \ldots H_{kj} = H_j \supseteq \ldots \supseteq H_{kl} = H_l = E \qquad 11.2.3\ (7)$$

of 11.2.3 (1) and 11.2.3 (2). The length of the series in both 11.2.3 (6) and 11.2.3 (7) is

$$k(l-1) + k = kl = l(k-1) + l$$

Thus the terms of refinements 11.2.3 (6) and 11.2.3 (7) of the series 11.2.3 (1) and 11.2.3 (2) can be put in one-one correspondence such that the corresponding factors $G_{i,j-1}/G_{ij}$ and $H_{i-1,j} / H_{ij}$ are isomorphic.

Moreover, if a repetition $G_{i,j-1} = G_{ij}$ occurs in 11.2.3 (6) then, from the isomorphism between $G_{i,j-1}/G_{i,j}$ and $H_{i,j-1}/H_{i,j}$ we have

$$H_{i-1,j}/H_{ij} \cong E$$

so that $H_{i-1,j} = H_{ij}$. Thus repetitions, if any, occur together in 11.2.3 (6) and 11.2.3 (7). After deletion of the corresponding repetitions we have two isomorphic refinements of the series as required.

A subgroup H of G is said to be *sub-normal (subinavariant, accessible or finitely serial)* if H occurs in a normal series, that is, there is a normal series

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = H$$

from G to H.

Among the examples of sub-normal subgroups of a group G are the normal subgroup of G, the normal subgroup of these normal subgroups and so on.

A subnormal subgroup need not be a normal subgroup.

11.2.4. Example: Let

$$A_4 = \langle a, b, c : a^3 = b^2 = c^2 = (bc)^2 = 1, b^a = c, c^a = bc \rangle$$

be the alternating group of degree 4. Then

$$V = \langle b, c : b^2 = c^2 = (bc)^2 = 1 \rangle$$

and

$$U = \langle b : b^2 = 1 \rangle$$

are subnormal subgroups of A_4. Here, of course, U is a subnormal but not a normal subgroup of A_4.

11.2.5. Theorem: The intersection of two subnormal subgroups of a group is a subnormal subgroup.

Proof: Let H, K be subnormal subgroups of a group G. Then there are normal series

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i = H \supseteq \ldots \supseteq G_k = E$$

and

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_j = K \supseteq \ldots \supseteq H_l = E$$

passing through H and K respectively. So

$$G = G_0 = G_1 \supseteq \ldots \supseteq G_i = H = H \cap H_0 \supseteq H \cap H_1 \supseteq \ldots \supseteq H \cap H_j = H \cap K \supseteq \ldots \supseteq H \cap H_l = E$$

is a normal series for $H \cap K$. Hence $H \cap K$ is subnormal.

Let H be a subgroup of G. The *normal closure* H^G of H in G is the smallest normal subgroup of G containing H. Thus

$$H^G = \langle xhx^{-1} : h \in H, x \in G \rangle = \langle x H x^{-1} : x \in G \rangle$$

so that the normal closure H^G of H in G is generated by elements of H and their conjugates in G.

For example the normal closure of

$$U = \langle b : b^2 = 1 \rangle$$

in

$$A^4 = \langle a, b, c : a^3 = b^2 = c^2 = (bc)^2 = 1, b^a = c, c^a = bc \rangle$$

is

$$V = \langle b, c : b^2 = c^2 = (bc)^2 = 1 \rangle.$$

The normal closure H^G of H in G is equal to H if an only if H is normal in G.

Given a subnormal subgroup H of G we describe a method to construct a normal series from G to H as follows:

Let $H_0 = G$, $H_1 = H^G$ the normal closure of H in G and so on $H_i = H^{H_{i-1}}$ be a normal closure of H in H_{i-1}, i = 1, 2, ... Then H_i is normal in H_{i-1}, i = 1, 2, ...

Let m be the length of a normal series from G to H, that is,

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = H$$

We show that

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_m = H \qquad 11.2.3\ (**)$$

is a normal series from G to H such that $H_i \subseteq G_i$. The proof is by induction on i. When i = 0, $H_0 = G_0 = G$. Suppose that

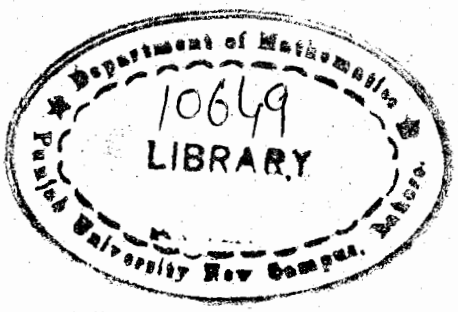
$$H_{i-1} \subseteq G_{i-1}, i \geq 1.$$

Then

$$H_i = H^{H_{i-1}} \subseteq H^{G_{i-1}} = \langle xhx^{-1} : x \in G_{i-1}, h \in H \rangle \subseteq G_i$$

because $H \subseteq G_i$ and G_i is normal in G_{i-1}. Also H_i is normal in H_{i-1}. This shows that 11.2.3 (**) is a normal series from G to H.

Thus, given a subnormal subgroup, we can write down a normal series whose terms are 'known'.



11.3. COMPOSITION SERIES

A normal series

$$G = G_0 \supset G_1 \supset \ldots \supset G_1 \supset \ldots \supset G_k = E$$

is said to be a *composition series* for G if and only if this series is isomorphic to each of is refinements.

Thus a composition series cannot be refined further, that is, every refinement of a composition series is that series itself.

Since, in a composition series, we cannot insert additional terms between any subnormal subgroups G_{i-1}, G_i; every G_i is a maximal normal subgroup of G_{i-1}. Thus we can define a compositions series in the following manner as well.

A normal series

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E$$

is a composition series if and only if each G_i is a maximal normal subgroup of G_{i-1} $i = 1, 2, \ldots k$.

We know that a normal subgroup H of a group G is maximal if and only if G/H is simple. Using this fact we have yet another equivalent definition of a composition series as follows:

A normal series

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E$$

is a composition series for G if and only if each factor G_{i-1}/G_i is simple $i = 1, 2, \ldots, k$.

Every finite group G has a composition series.

For if G is simple then

$$G \supset E$$

is a composition series for G.

If G is not simple, then G has a maximal normal subgroup G_1, say. If G_1 is simple then

$$G \supset G_1 \supseteq E$$

is a composition series for G.

If G_1 is not simple then G_1 has a maximal normal subgroup G_2, say. If G_2 is simple then

$$G \supset G_1 \supset G_2 \supset E$$

is a composition series for G. Continuing in this way, as G is finite, we end up in a composition series

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset \ldots \supset G_k = E$$

An infinite group may not have a composition series.

11.3.1. Examples:

(a) Let

$$G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$$

Then

$$A = \langle a : a^3 = 1 \rangle$$

is a normal subgroup of G and

$$G \supset A \supset E$$

is a composition series for G.

(b) The series

$$A_4 \supset V \supset U \supset E, U = \langle b : b^2 = 1 \rangle$$

and

$$A_4 \supset V \supset W \supset E, W = \langle c : c^2 = 1 \rangle$$

of the alternating group A_4 given in example after Theorem 11.2.5 are two 'distinct' composition series for A_4.

We, however, show that this distinctness is not every significant.

11.3.2. Theorem:

(Jordan-Holder theorem)

Any two composition series of a group G are isomorphic.

Proof:

Let

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E \ldots \qquad 11.3.2\ (1)$$

and

$$G = H_0 \supset H_1 \supset \ldots \supset H_j \supset \ldots \supset H_1 = E \ldots \qquad 11.3.2\ (2)$$

by any two composition series for G. By Schreier's refinement theorem, 11.3.2 (1) and 11.3.2 (2) have isomorphic refinements and both are refinements of each other. So $k = 1$. However a composition series is its own refinement. Thus 11.3.2 (1) and 11.3.2 (2) cannot be refined further so that these series are isomorphic.

The length of a composition series of a group G is called the *composition length* of G and the factors of a composition series are called *composition factors*.

Since a finite group has maximal subgroups, every finite group has a composition series.

Although, as already seen, every group has a normal series, an arbitrary group, in general, may not have a composition series.

11.3.3. Example:

Let

$$G = < a >$$

be the infinite cyclic group. Since G is abelian, every subgroup of G is normal in G. An arbitrary subgroup of G is of the form

$$H_k = < a^k , k \text{ a natural number} >$$

and is itself an infinite cyclic group. Thus we can insert additional terms of the form

$$H_{2^{mk}} = < a^{2^{mk}} : m , k \in Z\}$$

in between H_k and E. So every normal series for G has a proper refinement. Hence G has no composition series.

We now try to answer the question as to which groups have composition series.

A sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \ldots \supset G_i \supset \ldots \qquad 11.3.3\ (1)$$

is called a *descending normal chain* if every G_i is a proper normal subgroup of G_{i-1}, i = 1, 2, 3, ...

A descending normal chain 11.3.3 (1) is said to "break off" if $G_k = E$ for some natural number k.

For an arbitrary group G, a descending normal chain may not break off.

For example, the descending normal chain.

$$G = \langle a \rangle \supset \langle a^2 \rangle \supset \ldots \supset \langle a^{2^n} \rangle \supset \ldots.$$

of an infinite cyclic group G, does not break off.

A sequence of subgroups

$$E = F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots \subset G \qquad 11.3.3\ (2)$$

of a group G is said to be an *ascending normal chain* for G if each F_i is a proper normal subgroup of F_{i+1} and a subnormal subgroup of G.

An ascending normal chain 11.3.3 (2) is said to break off if, for some natural number n, $F_n = G$.

For an arbitrary group G, an ascending normal chain may not break off.

11.3.4. Examples:

Let

$$G = \langle a_0, a_1, a_2, \ldots : a_0^p = 1, a_{n+1}^p = a_n, n = 1, 2, 3, \ldots \rangle$$

be Prüfer's p^∞-group. G is abelian so that very subgroup of G is normal. For a generator a_n of G, let

$$F_n = \langle a_n \rangle$$

Then F_n is a cyclic group of order p^{n+1} and $F_n \subset F_{n+1}$ for each n = 0, 1, 2, 3, ...

The sequence

$$E = F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots$$

is ascending normal chain which does not break off.

This is so because, for each natural number n, F_n is finite while G is an infinite group.

A group G is said to satisfy the *normal chain condition* if all of its ascending and descending normal chains break off.

We are now in a position to give a necessary and sufficient condition for group G to have a composition series.

11.3.5. Theorem: A group G has a composition series if and only if all its ascending and descending normal chains break off.

Proof: Suppose that G has a composition series

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E \qquad 11.3.5\ (1)$$

so that the composition length of G is k. We show that all ascending and descending normal chains of G break off. Let

$$G = H_0 \supset H_1 \supset \ldots \supset H_i \supset \ldots \supset H_n \supset \ldots \qquad 11.3.5\ (2)$$

be a descending normal chain for G. Choose $n \geq k$. Then

$$G = H_0 \supset H_1 \supset \ldots \supset H_i \supset \ldots \supset H_n \supset E \qquad 11.3.5\ (3)$$

is a normal series of length $n + 1 > k$. This contradicts Scheier's theorem because a composition series in 11.3.5 (1), being its own refinement, cannot be isomorphic to 11.3.5 (3). Hence the descending normal chain 11.3.5 (2) must breaks off.

Next, let

$$E = F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots \subset G \qquad 11.3.5\ (4)$$

be an ascending normal chain. Take $n > k$. Since each F_n is subnormal, there is a normal series

$$G = H_0 \supset H_1 \supset \ldots \supset H_{m-1} \supset F_n \supset F_{n-1} \supset \ldots \supset F_1 \supset F_0 = E \quad m \geq 1$$

through F_n and of length > k.

This again contradicts Scheier's theorem. Thus all ascending normal chains of G must break off after at most k steps.

Conversely, suppose that G has both the ascending chain condition and the descending chain condition for subnormal subgroups. Since all the

ascending normal chains break off, G and every other subnormal subgroup of G must have a maximal normal subgroup.

For let a subnormal subgroup H of G have no maximal normal subgroup. Then, since H is subnormal, there is a normal series

$$G = H_0 \supset H_1 \supset \ldots \supset H_m = H$$

from G to H. As H has no maximal normal subgroup, for each normal subgroup K of H there is a normal subgroup U_1 of H such that

$$K \subset U_1 \subset H.$$

So we can form an *infinite ascending normal* chain

$$E \subset K \subset U_1 \subset U_2 \subset \ldots \subset H = H_m \subset \ldots \subset H_0 = G,$$

for H (and also for G), which contradicts the hypothesis that all ascending normal chains for G break off.

Now we construct a composition series for G as follows.

Let $G = H_0$ and H_1 be a maximal normal subgroup of G. If $H_1 = E$, then

$$G = H_0 \supset H_1 = E$$

is a composition series for G. If $H_1 \neq E$ then H_1 has maximal normal subgroup H_2. If $H_2 = E$ then

$$G = H_0 \supset H_1 \supset H_2 = E$$

is a composition series for G. If, however, $H_2 \neq E$ then we continue as before and find maximal normal subgroups H_3, H_4, ... successively. Since G satisfies the descending normal chain condition for subnormal subgroups, this sequence of successive maximal normal subgroups cannot continue indefinitely. So there exists an integer k such that $H_k = E$. Thus

$$G = H \supset H_1 \supset \ldots \supset H_k = E$$

is a composition series for G.

Suppose that G is a group with a composition series. Is it true that every subgroup of G also has a composition series? The following example shows that this is not always possible.

11.3.6. Example: Let A_N be the restricted alternating group on $N = \{1, 2, 3, ...\}$. It was shown in Theorem 8.6.10 that A_N is simple. So A_N has a composition series,

$$A_N \supset E.$$

We take the subgroup H of A_N generated by all permutations of the form

$$a_m = (4m - 3, 4m - 1)(4m - 2, 4m), m = 1, 2; 3, ...$$

Then H is an infinitely generated abelian 2-group. Consider now the ascending normal chain

$$G_1 \subset G_2 \subset ... \subset G_m \subset ...$$

of subgroups of H, where

$$G_m = < a_1, a_2, ..., a_m >.$$

This ascending normal chain does not break off. Hence, by theorem 11.3.5, H has no composition series.

We shall, however, show that the class of all subnormal subgroups of a group with a composition series has this property. Thus:

11.3.7. Theorem: A subnormal subgroup H of a group G with a composition series is itself a group with a composition series.

Proof: Consider the normal series

$$G = G_0 \supset G_1 \supset ... \supset G_i = H \supset G_{i+1} \supset ... \supset G_k = E$$

of G through H. This series can be refined to a composition series of G. The part of the refined series from H to E is then a composition series of H.

11.3.8. Corollary: If G is a group with a composition series and H is a subnormal subgroup then the composition length of H is less than or equal to the composition length of G.

Also the composition factors of H form a part of the composition factors of G.

11.3.9. Corollary: If H is a normal subgroup of a group G with a composition series then G/H is a group with a composition series and its composition length is equal to the difference of the composition lengths of G and of H.

That a subgroup of a group with a composition series may not have a composition series is in contrast to the existence of a normal series for subgroups of a group having a normal series.

11.3.10. Theorem: Every subgroup F of a group G with a normal series itself has a normal series whose factors are isomorphic to subgroups of the factors of the normal series of G.

Proof: Let a normal series for G be

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq \ldots \supseteq G_k = E. \qquad 11.3.10\ (1)$$

Take $F_i = F \cap G_i$. Then $F_{i-1} = F \cap G_{i-1} \supseteq F_i$. Also, since G_i is normal in G_{i-1}, F_i is normal in F_{i-1} so that we have a normal series

$$F = F_0 \supseteq F_1 \supseteq \ldots \supseteq F_i \supseteq \ldots \supseteq F_k = E \qquad 11.3.10\ (2)$$

for F. If we take

$$H = F, H' = E, K = G_{i-1}, K' = G_i$$

in Zassenhaus' lemma then

$$H'(H \cap K) = F \cap G_{i-1}, H'(H \cap K') = F \cap G_i,$$

$$K'(K \cap H) = G_i(F \cap G_{i-1}) \ , \ K'(K \cap H') = G_i$$

and

$$H'(H \cap K)/H'(H' \cap K') = (F \cap G_{i-1})/(F \cap G_i) = F_{i-1}/F_i,$$

$$K'(K \cap H)/K'(K \cap H') = G_i(F \cap G_{i-1})/G_i = G_i F_{i-1}/G_i$$

and $F_{i-1}/F_i \cong G_i F_{i-1}/G_i$.

Since $G_i \subseteq G_{i-1}$ and $F_{i-1} \subseteq G_{i-1}$, $G_i F_{i-1} \subseteq G_{i-1}$. Thus $G_i F_{i-1}/G_i$ is a subgroup of the factor G_{i-1}/G_i. Hence F_{i-1}/F_i is isomorphic to a subgroup of G_{i-1}/G_i, as required.

11.4. CHIEF OR PRINCIPAL SERIES

Another important type of series of subgroups of a group G is the *chief series* (or *principal series*) of the group which we now define.

A sequence

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E$$

is called a *chief series (principal series)* for G if each G_i is a maximal normal subgroup of G contained in G_{i-1}.

Factor groups of a chief series are called *chief* or *principal factors* of G.

Clearly every chief series is a normal series. However a normal series may not be a chief series nor it may have a refinement which is a chief series.

In the group of example of Theorem 11.2.5, V is a maximal normal subgroup of G. No proper subgroup of V is normal in G.

Hence

$$G \supset V \supset E$$

is a normal series for G which is neither a chief series nor can be refined to a chief series for G.

Here E is not a maximal normal subgroup of G contained in V. The subgroup U contains E as a normal subgroup and U is not normal in G.

The following theorem and its proof are analogous to Theorem 11.3.6 for composition series for G.

11.4.1. Theorem: A group G has a chief series if and only if every ascending and descending normal chain of subgroups of G breaks off.

If G has a chief series then every sequence of subgroups

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_k = E$$

such that each G_i is normal in G can be refined to a chief series of G.

This is so because every proper normal subgroup of G is contained in a maximal normal subgroup of G and also contains a maximal normal subgroup of G.

For if G_1 is not maximal, then there is a normal subgroup K_1 of G containing G_1. If K_1 is maximal we are finished. Otherwise there is a normal subgroup K_2 of G containing K_1 and so on. Thus we have an ascending chain

$$G_1 \subset K_1 \subset K_2 \subset \ldots \subset G$$

of normal subgroups of G. This ascending chain breaks off so that the term preceeding G will be a maximal normal subgroup of G containing G_1. Similarly for the other case.

It should be noted that chief factors of a group G need not be simple groups. (See the remarks preceding Theorem 11.4.1).

EXERCISES

1. Write down a chief series for S_4.

2. If all the descending normal chains for a group G break off then show that every normal subgroup of G contains a minimal normal subgroup.

3. If H is a subnormal subgroup of G then, for any automorphism α of G, $\alpha(H)$ also is subnormal in G.

4. Let H be a subnormal subgroup of G and α any automorphism of G. Put $H = G$ and $H_i = H^{H_{i-1}}$, $i \geq 1$. Then

$$G = H_0 \supset H_1 \supset \ldots \supset H_m = H$$

is a normal series from G to H and each H_i is mapped onto itself under α.

5. If G is a finite p-group then G has a chief series such that all chief factors are cyclic groups of order p.
(**Hint:** Use the fact that the centre of a finite p-group is non-trivial).

6. Show that the infinite dihedral group does not have a composition series.

7. A group G is said to be *characteristically simple* if it has no proper characteristic subgroup. Show that the chief factors of a group G are characteristically simple.

8. Show that every cyclic group C_n, $n = p_1 p_2 \ldots p_k$, where p_i are not necessarily distinct, has a composition series with composition factors as cyclic group C of order p_i, $1 \leq i \leq k$.

All other composition series of C_n have composition factors $C_{\sigma(p_i)}$ where σ is a permutation of the set $\{p_1, p_2, ..., p_k\}$.

9. Show that the only composition series for S_n, $n \geq 5$ is

$$S_n \supset A_n \supset E$$

10. Let G be the direct product of simple subgroups

$$H_1, H_2, ..., H_k.$$

Write a composition series for G.

What is the total number of all composition series of G?

Chapter - XII

SOLVABLE GROUPS

In this chapter we discuss a new class of groups called solvable groups. This contains the class of all abelian groups. Solvable groups are closely related to certain problems involving the solutions of an equation of the form

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

by radicals. This relation actually proved to be the basis of Galois Theory. In what follows we shall briefly describe some properties of solvable groups.

12.1. SOLVABLE GROUPS

Let G be a group and A, B be subgroups of G. We denote by [A, B] the group generated by all commutators $[a, b]$, $a \in A$, $b \in B$.

Now we inductively define a series of subgroups of G as follows.

We put

$$G^{(0)} = G \text{ and } G^{(i+1)} = [G^{(i)}, G^{(i)}], i \geq 0.$$

$G^{(i)}$ is called the *ith derived subgroup of* G.

The group G is said to be *solvable* if $G^{(k)} = E$, the identity subgroup, for some integer k. The smallest integer k for which $G^{(k)} = E$ is called the *solvability* length of G.

A solvable group of solvability length 2 is called a *metabelian group*. Thus a metabelien group is one whose derived group is abelian.

12.1.1. Examples:

(i) Every abelian group is solvable of solvability length 1.

For if A is an abelian group then

$$A' = \langle [a_1, a_2] : a_1, a_2 \in A \rangle = E$$

(ii) The group Q of quaternions $\pm I, \pm i, \pm j, \pm k$ is solvable of length 2.

Here the first derived group

$Q' = [Q, Q] = < [x, y] : x, y \in Q >$

$= \{\pm I\}$

which is abelian and so $Q'' = E$. Thus Q is metabelian.

(iii) The symmetric group S_3 which has a presentation

$S_3 = < a, b : a^3 = b^2 = (ab)^2 = 1 >$

is metabelian.

Here the first derived group of S_3 is $H = < a: a^3 = 1 >$ which is abelian.

(iv) The alternating groups A_n, $n \leq 4$ are solvable.

However, for $n \geq 5$, A_n, being a non-abelian simple group, is not solvable.

12.2. THEOREMS ON SOLVABLE GROUPS

For a group G, let $G' = [G, G] = < [g_1, g_2], g_1, g_2 \in G>$.

If A and B are subgroups of a group G then $A \subseteq B$ implies $A' \subseteq B'$. This is so because, for $a_1, a_2 \in A$, $a_1, a_2 \in B$ so that $[a_1, a_2] \in B$.

We now give a new characterisation of solvable groups.

12.2.1. Theorem: A group G is solvable if and only if it has a normal series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ..... \supseteq G_{k-1} \supseteq G_k = E$$

in which G_{i-1}/G_i are abelian for $1 \leq i \leq k$.

Proof: Suppose that G is a solvable group of solvability length k. Then the series.

$$G = G^{(0)} \supset G^{(1)} \supset ..... \supseteq G^{(k-1)} \supseteq G^{(k)} = E$$

is a normal series in G with its factors $G^{(i-1)}/G^{(i)}$ as abelian, by Theorem 6.4.2

Conversely, suppose that G has a normal series

$$G = G_0 \supseteq \ldots\ldots \supseteq G_{k-1} \supseteq G_k = E$$

where the factors G_{i-1}/G_i are abelian. Consider first the factor G/G_1 which is abelian. By Theorem 6.4.2

$$G^{(1)} = G' \subseteq G_1$$

Next, G_1/G_2 is aelian so $G_1' \subseteq G_2$. Hence

$$G^{(2)} \subseteq G_1' \subseteq G_2.$$

Continuing in this way we inductively find that

$$G^{(k)} \subseteq G_k = E \subseteq G^{(k)}$$

Hence $G^{(k)} = E$ and G is solvable, as required.

From now on we shall take the statement of Theorem 12.2.1 as a definition of solvable groups

We now discuss the nature of subgroups and factor groups of a solvable group.

12.2.2. Theorem:

1. Every subgroup and factor group of a solvable group is solvable.
2. For a group G and a normal subgroup N of G, G is solvable if and only if both N and G/N are solvable.

Proof:

1. Let G be a solvable group and H a subgroup of G. Let k be the solvability length of G so that $G^{(k)} = E$. Now

$$H \subseteq G$$

implies

$$H' \subseteq G'$$

and, inductively,

$$E \subseteq H^{(k)} \subseteq G^{(k)} = E$$

so that $H^{(k)} = E$. Hence H is solvable.

Now let N be a normal subgroup of a solvable group G. Consider the factor group G/N. Since G is solvable, G has a normal series

$$G = G_0 \supseteq G_1 \supseteq \ldots\ldots \supseteq G_k = E$$

with abelian factors. Consider now the series

$$G/N = G_0N/N \supseteq G_1N/N \supseteq \ldots\ldots \supseteq G_k\, N/N \cong E. \qquad 12.2.2\ (*)$$

Since G_i is normal in G_{i-1}, G_iN/N is normal in G_{i-1} N/N. Also, since

$$(G_{i-1}\, N/N) / (G_i\, N/N) \cong G_{i-1}/G_i,$$

by Theorem 6.2.4, and G_{i-1}/G_i is abelian, $(G_{i-1}\, N/N) / (G_iN/N)$ is abelian. Hence 12.2.2 (*) is a normal series for G/N with abelian factors. So G/N is solvable.

2. Suppose that G is solvable. Then, by the first part of the theorem, for any normal subgroup N, both N and G/N are solvable.

Conversely suppose that for a normal subgroup N, both N and G/N are solvable. Then both N and G/N have normal series with abelian factors.

Now consider the series

$$N = N_0 \supseteq N_1 \supseteq \ldots\ldots \supseteq N_q = E \qquad 12.2.2\ (i)$$

and

$$G/N = G_0/N \supseteq G_1/N \ldots\ldots G_p/N = \{N\} \cong E \qquad 12.2.2\ (ii)$$

with factors N_{i-1}/N_i and (G_{j-1}/N) as abelian for $1 \le i \le q$ and $1 \le j \le p$.

So

$$G = G \supseteq G_1 \supseteq \ldots\ldots \supseteq G_p = N \supseteq N_1 \supseteq \ldots\ldots \supseteq N_q = E \qquad 12.2.2\ (iii)$$

Since

$$G_{i-1}/G_i \cong (G_{i-1}/N) / (G_i/N),$$

the factors in 12.2.2 (iii) are all abelian so that 12.2.2 (iii) is a normal series with abelian factors. Hence G is solvable.

From the proof of the above theorem, it may be noted that the solvability length of a subgroup or factor group of a solvable group does not exceed the solvability length of the group.

12.2.3. Theorem: The direct product of a finite number of solvable groups is solvable.

Proof: It is sufficient to prove the theorem for the direct product of two groups because an easy induction on the number of factors proves the theorem in that case.

Now let

$$G = A \times B$$

where A and B are solvable. Then A and B have normal series

$$A = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_p = E$$

and

$$B = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_q = E$$

with abelian factors in both cases. Without any loss of generality one can suppose that $q \geq p$. Then

$$G = A \times B \supseteq A_1 \times B_1 \supseteq \ldots \supseteq A_p \times B_p \supseteq E \times B_{p+1} \ldots \supseteq E \times B_q \cong E$$

is normal series with abelian factors. Here $(A_{i-1} \times B_{i-1}) / (A_i \times B_i)$ is isomorphic to $(A_{i-1}/A_i) \times (B_{i-1}/B_i)$ which is abelian. Hence G is solvable.

Or, alternatively, if $G = A \times B$, then $G/A \cong B$. Since both A and G/A are solvable, G is solvable, by Theorem 12.2.2.

Note that the solvability length of the direct product is equal to the maximum of the solvability lengths of the direct factors.

Theorem 12.2.3 is not valid for the direct product of an infinite number of solvable groups.

For example if, for each interger n, $n = 1, 2, \ldots$, H_n is a solvable group of solvability length n, then

$$G = \prod_{n=1}^{\infty} H_n$$

is not a solvable group.

However the direct product of any finite or infinite number of solvable groups whose solvability lengths are bounded by a fixed integer k, is solvable and its solvability length does not exceed k.

12.2.4. Theorem: Every finite p-group is solvable.

Proof: Let G be a p-group of order p^n. We apply induction on n to prove the theorem.

When n = 1, G is a cyclic group of order p, hence abelian and therefore solvable. So suppose that $n \geq 1$ and suppose that all groups of order p^m, $m < n$, are solvable. Let G a group of order p^n. By Theorem 5.4.5, G has non-trivial centre $\zeta(G)$.

$\zeta(G)$, being abelian, is solvable. Also $G/\zeta(G)$ has order p^m, for some $m < n$ and so is solvable, by our induction hypothesis. So, by Theorem 12.2.2, G is solvable.

12.2.5. Theorem: A finite group G is solvable if and only if the factor groups in a composition series from G to E are cyclic of prime order.

Proof: Suppose that G is finite and solvable. Then there is an integer k such that $G^{(k)} = E$. Since G/G' is abelian and G is finite, G has a maximal normal subgroup $G_1 \supseteq G'$ such that G/G_1 is abelian and simple. Then G/G_1 is cyclic of prime order.

As a subgroup of G, G_1 is solvable and so contains a maximal normal subgroup $G_2 \supseteq G_1'$ with G_1/G_2 cyclic of prime order. Since G is finite, this process of finding successive maximal normal subgroups ends after a finite number of steps so that there is an integer r such that $G_r = E$. Then

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r = E$$

is a composition series with G_{i-1}/G_i cyclic of prime order.

Since any two composition series of G are isomorphic, the above statement is true for any composition series.

Conversely, suppose that G has a composition series

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k = E$$

with G_{i-1}/G_i of prime order and hence abelian. Since G/G_1 is abelian, $G_1 \supseteq G'$. Next since G_1/G_2 is abelian,

$$G_2 \supseteq G_1' \supseteq G_2''.$$

Continuing is this way we find that

$$E = G_k \supseteq G^{(k)} \supseteq E$$

So $G^{(k)} = E$. Hence G is solvable.

2.6. Theorem: For $n \geq 5$, S_n is not solvable.

Proof: The alternating group A_n of degree n is a subgroup of S_n. If S_n is solvable then A_n, as a subgroup of S_n, is solvable. But, for $n \geq 5$, A_n is a non-abelian simple group and hence not solvable. Therefore S_n is not *solvable.*

EXERCISES

1. If H, K are solvable subgroups of a group G with H normal in G then HK is a solvable subgroup of G.
   (Hint: Here HK is a subgroup of G and $HK/H \cong K/K \cap H$ is solvable. Now apply Theorem 11.2.2 (2)).

2. Every group of order p^2q, where p, q are primes, is solvable.

3. The infinite dihedral group D_∞ and the finite dihedral groups D_n, $n \geq 2$ are solvable.
   (Hint: Here $D_\infty = \langle a, b : a^2 = b^2 = 1 \rangle$ and
   $D'_\infty = \langle (ab)^2 \rangle$).

4. Show that S_3, A_4 and S_4 are all solvable.

5.* (Philip Hall). Let G be a finite group of order n. Suppose that, for every prime divisor p of n, $n = p^a m$ and $(p, m) = 1$, G has a subgroup of order m. Show that G is solvable.
   (Such a subgroup of order m is called a *sylow p-complement*).

6.** Every finite group of odd order is solvable.
   (This is a very deep result of W. Feit and J.G. Thomson proved in one of their joint papers in 1963. As a consequence of this every non-abelian finite simple group has even order).

Chapter - XIII

NILPOTNET GROUPS

Some properties of finite p-groups were discussed in Chapter 5. One of the characteristic properties of a finite p-group is that its centre is non-trivial. A generalisation of the class of p-groups is the class of nilpotent groups which will be defined in this chapter. As we shall see, the class of nilpotent groups lies between the class of abelian groups and the class of solvable groups.

13.1. NILPOTENT GROUPS

Let G be a group. A *central series* in G is a normal series

$$G = G_o \supset G_1 \supset \ldots \supset G_k = E \qquad 13.1\ (I)$$

such that

(i) G_i is a normal subgroup of G, $1 \leq i \leq k$; and

(ii) G_{i-1}/G_i is a subgroup of the centre of G/G_i, $1 \leq i \leq k$.

Following observations regarding the definition of a central series are worthy of consideration.

(a) Requirement (i) is deducible from (ii) because if G_{i-1}/G_i is a central subgroup of G/G_i, then, for each $g_i \in G_i \subset G_{i-1}$ and $g \in G$,

$$[g\,G_i,\ g_iG_i] = G_i$$

so that $gg_i\,g^{-1}\,g_i^{-1} \in G_i$, that is, $gg_i\,g^{-1} \in g_i\,G_i = G_i$. So G_i is normal in G.

(b) The last but one term namely G_{k-1} is a central subgroup of G. This is so because $G_{k-1} / G_k \equiv G_{k-1}$ is a subgroup of the centre of $G/G_k \equiv G$.

One of the definitions of a nilpotent group is as follows:

A group G is said to be *nilpotent* if G has a central series.

13.1.1. Examples:

1. Every abelian group is nilpotent.

   Here a central series for an abelian group A is

   $$A = A_0 \supset A_1 = E$$

   where A_1 is normal in A and $A_0/A_1 = A/A_1$ with

   $\zeta (A/A_1) = A/A_1 \cong A$.

2. Consider the group

   $$Q = \{ \pm I, \pm i, \pm j, \pm k\}$$

   of quaternions. Take $Q_1 = \{\pm I\}$. Then Q_1 is normal in Q and Q/Q_1, being of order 4, is abelian. Hence $\zeta (Q/Q_1) = Q/Q_1$ so that Q/Q_1 is a subgroup (improper) of Q/Q_1. If we take $Q_2 = E$ then conditions (i) and (ii) are satisfied for the series

   $$Q = Q_0 \supset Q_1 \supset Q_2 E \qquad 13.1.1\ (1)$$

   so that 13.2.1 (I) is a central series for Q. Hence Q is nilpotent.

3. Consider the symmetric group

   $$S_3 = < a, b, = a^3 = b^2 = (ab)^2 = 1 >.$$

   The only non-trivial normal subgroup of S_3 is

   $$H = < a : a^3 = 1 >.$$

   So the only non-trivial normal series for S_3 is

   $$S_3 \supset H \supset E$$

   which is not a central series for S_3 because H/E is not contained in the centre of S_3/E.

   Here centre of S_3/E ($\cong S_3$) is trivial while $H/E \cong H$. So S_3 is not nilpotent.

It may, however, be noted that S_3 is solvable. Thus a solvable group need not be nilpotent.

Later on we shall see that every nilpotent group is solvable.

As before, for subgroups A and B of a group G, we put

$$[A, B] = \langle [a, b] : a \in A, b \in B \rangle.$$

It is easy to verify that $A_1 \subseteq A$, $B_1 \subseteq B$ implies $[A_1, B_1] \subseteq [A, B]$.

We now define the lower central series of G as follows.

Take $\gamma_0(G) = G$ and put $\gamma_i(G) = [\gamma_{i-1}(G), G]$ for $i \geq 1$. Then:

$\gamma_i(G)$ is normal in G.

This is proved by induction on i.

For $i = 0$, $\gamma_0(G) = G$ is trivially a normal subgroup of G. For $i = 1$, $\gamma_1(G) = [G, G]$ which, being the derived group of G, is normal in G.

Suppose that $i \geq 1$ and that $\gamma_{i-1}(G)$ is normal in G. Let z be a generator of $\gamma_i(G)$. Then

$$z = [x, y]$$

for $x \in \gamma_{i-1}(G)$ and $y \in G$. So, for any $g \in G$,

$$z^g = [x^g, y^g].$$

By the induction hypothesis, $\gamma_{i-1}(G)$ is normal in G so $x^g \in \gamma_{i-1}(G)$ while $y^g \in G$. Hence $z^g \in \gamma_i(G)$. So, by Theorem 6.1.4, $\gamma_i(G)$ is normal in G. Thus we have a normal series.

$$G = \gamma_0(G) \supseteq \gamma_1(G) \supseteq \ldots \supseteq \gamma_k(G) \ldots$$

This series is said to be a *lower central series* for G if $\gamma_k(G) = E$ for some integer k.

To see that

$$G = \gamma_0(G) \supset \gamma_1(G) \supset \ldots \supset \gamma_k(G) = E \qquad 13.1.1\ (II)$$

is, in fact, a central series, consider the factor groups $\gamma_{i-1}(G) / \gamma_i(G)$ and $G/\gamma_i(G)$. We show that $\gamma_{i-1}(G) / \gamma_i(G)$ is a central subgroup of $G/\gamma_i(G)$.

For this let $y \in \gamma_{i-1}(G)$ and $g \in G$. Then the commutator

$$[y\,\gamma_i(G), g\,\gamma_i(G)] = [y, g]\,\gamma_i(G)$$
$$= \gamma_i(G)$$

because $[y, g] \in \gamma_i(G)$. Hence $y\,\gamma_i(G)$ commutes with $g\,\gamma_i(G)$, as required.

In view of the above observations, we have yet another definition of a nilpotent group.

A group G is said to be *nilpotent* if and only if it has a lower central series (II).

The integer k is said to be the *(nilpotency) class* of G and G is said to be a *nilpotent group* of class *k*.

The remarks preceding the above paragraph are, in fact, easy consequences of the following.

13.1.2. Lemma: Let

$$G = G_0 \supset G_1 \supset \ldots \supset G_k = E \qquad 13.1.2\ (1)$$

be such that G_i is normal in G, $1 \le i \le k$. Then (1) is a central series for G if and only if

$$[G_{i-1}, G] \subseteq G_i,\ 1 \le i \le k.$$

Proof: The group G_{i-1} / G_i is a central subgroup of G/G_i if and only if for each $y \in G_{i-1}$, $g \in G$;

$$[y\,G_i, gG_i] = G_i,$$

that is, if and only if $[y, g] \in G_i$, which is equivalent to saying that

$$[G_{i-1}, G] \subseteq G_i,\ 1 \le i \le k.$$

13.1.3. Theorem: A group G, with identity 1, is nilpotent of class *k* if and only if

$$[\ldots [[[g_1, g_2], g_3], g_4] \ldots], g_{k+1}] = 1.$$

Proof: By lemma 13.1.2,

$$G = G_0 \supset G_1 \supset \ldots \supset G_k = \{1\}$$

is a central series for G, and so G is a nilpotent group of class k, if and only if,

$$[G_{i-1}, G] \subseteq G_i,\ i = 1, 2, ..., k.$$

Now, for $i = 1, 2, ..., k$,

$$[G_0, G] = [G, G] \subseteq G_1, \Leftrightarrow [g_1, g_2] \in G_1$$

$$[G_1, G] \subseteq G_2 \Leftrightarrow [[g_1, g_2], g_3] \in G_2$$

$$[G_2, G] \subseteq G_3 \Leftrightarrow [[[g_1, g_2], g_3], g_4] \in G_3$$

and so on,

$$[G_{k-1}, G] \subseteq G_k = \{1\} \Leftrightarrow [... [[[g_1, g_2], g_3], g_4] ...], g_{k+1}] \in G_k = \{1\}$$

$$\Leftrightarrow [... [[[g_1, g_2], g_3], g_4] ...], g_{k+1}] = \{1\}$$

for all $g_1, g_2, g_3, ..., g_{k+1} \in G$.

13.1.4. Example:

1. In the dihedral group.

$$D_4 = < a, b: a^4 = b^2 = (ab)^2 = 1 >,$$

every commutator $[g_1, g_2]$, $g_1, g_2 \in D_4$ is either 1 or is a^2. Also $[a^2, g_3] = 1$ for all $g_3 \in D_4$. Hence

$$[[g_1, g_2], g_3] = 1$$

for all $g_1, g_2, g_3 \in D_4$. So D_4 is nilpotent of class 2.

In contrast the symmetric group of degree 3 having the presentation:

$$S_3 = < a, b: a^3 = b^2 = (ab)^2 = 1>$$

is not nilpotent: Here:

each commutator $[g_1, g_2]$, $g_1, g_2 \in G$ is either 1 or a or a^{-1}.

Hence

$$[[g_1, g_2], g_3]$$

is either 1 or a or a^{-1}, for all $g_1, g_2, g_3 \in S_3$. So

$$[[g_1, g_2], g_3] \neq 1$$

for every choice of $g_1, g_2, g_3 \in S_3$. The same is true for

$$[.... [[g_1, g_2], g_3] ...], g_{k+1}] \neq 1$$

for every choice of g_i, $1 \leq i \leq k+1$. Hence S_3 is not nilpotent.

13.1.4: Theorem: Every subgroup and factor group of a nilpotent group is nilpotent.

Proof: Suppose that H is a subgroup of a nilpotent group G. Let

$$G = G_o \supset G_1 \supset ... \supset G_k = E \qquad 13.1.4\ (1)$$

be a central series for G. Put $H_i = H \cap G_i$, $1 \leq i \leq k$. Then $H_o = H$ and $H_k = E$. Also H_i is normal in H because G_i is normal in G. Moreover, as is obvious,

$$[H_{i-1}, H] \subseteq H.$$

Since

$$H_{i-1} \subseteq G_{i-1}, H \subseteq G;$$

$$[H_{i-1}, H] \subseteq [G_{i-1}, G] \subseteq G_i.$$

So

$$[H_{i-1}, H] \subseteq H \cap G_i = H_i.$$

Hence the series

$$H = H_o \supseteq H_1 ... \supseteq H_k = E \qquad 13.1.4\ (2)$$

is a central series for H. Therefore H is nilpotent.

Next, let H be a normal subgroup of G and consider the factor group G/H. Consider the series

$$G/H = G_o/H \supseteq G_1\ H/H \supseteq ... \supseteq G_k\ H/H = \{H\} \cong E \qquad 13.1.4\ (3)$$

Since G_i is normal in G, G_i H/H is normal in G/H. To see that (3) is a central series, it only remains to show that

$$[G_{i-1}\ H/H, G/H] \subseteq G_i\ H/H \qquad 13.1.4\ (4)$$

For this, let $y \in G_{i-1}$, $g \in G$. then $[y, g] \in G_i$ so that $[yH, gH]$ is an arbitrary element of $[G_{i-1}\ H/H, G/H]$. Also

$$[yH, gH] = [y, g]\ H \in G_i\ H/H$$

which establishes (4). Hence (3) is a central series for G/H so that G/H is nilpotent.

In contrast to Theorem 12.2.2(2), if, for a normal subgroup H of a group G, both H and G/H are nilpotent then it is not necessary that G be nilpotent.

A counter example in this case is the symmetric group

$$S_3 = < a, b : a^3 = b^2 = (ab)^2 = 1 >$$

having

$$H = < a : a^3 = 1 >$$

as a normal subgroup. Here both H and G/H are nilpotent. However G is not nilpotent.

We also mention that the symmetric group S_n, $n \geq 3$ is not nilpotent. The reason is that S_n contains an isomorphic copy of S_3 as a subgroup and S_3 is not nilpotent.

13.1.6. Theorem: The direct product of a finite number of nilpotent groups is nilpotent.

Proof: We prove the result for the direct product of only two groups. For a direct product involving a finite number of direct factors, the result follows by an easy induction.

Let:

$$G = H \times K$$

where the central series for H and K are

$$H = H_o \supset H_1 \supset \ldots \supset H_p = E \qquad 13.1.6\ (1)$$

$$K = K_o \supset K_1 \supset \ldots \supset K_q = E. \qquad 13.1.6\ (2)$$

We can insert additional terms in the series to make the length of the series 13.1.6 (1) and 13.1.6 (2) equal. Let k be the common length of the enlarged series.

Then,

$$G = G_o \supseteq G_1 \supseteq \ldots \supseteq G_k = E$$

where

$$G_i = H_i \times K_i,\ 1 \le i \le k,$$

is a central series for G. Here

$$[G_{i-1}, G] = [H_{i-1} \times K_{i-1}, H \times K]$$
$$= [H_{i-1}, H] \times [K_{i-1}, K] \subseteq H_i \times K_i = G_i.$$

One may note that the class of the direct product is the maximum of the classes of the direct factors.

Also note that Theorem 13.1.5 does not hold for the direct product of an infinite number of nilpotent groups.

Here again, for each integer n, the group

$$K_n = D_{2^n} = \langle a, b : a^{2^n} = b^2 = (ab)^2 = 1 \rangle$$

of order 2^{n+1} is a nilpotent group of class percisely n and the direct product

$$G = \prod_{n=1}^{\infty} K_n$$

is not a nilpotent group.

12.1.6. Theorem: Every finite p-group is nilpotent.

Proof: Let P be a finite p-group of order p^n. By theorem 5.4.5, P has a non-trivial centre. Let $\zeta(P)$ be the centre of P. We apply induction on n to prove the theorem.

For n = 0 or 1, P is either the trivial group or cyclic group of order p and hence abelian and so nilpotent. So we suppose that $n \ge 1$ and that all p-group of order p^k, $k < n$ are nilpotent. Now take the group P of order p^n and centre $\zeta(P)$. The order of $\zeta(P)$ is $\ge p$. If the order of $\zeta(P)$ is p^n then $P = \zeta(P)$ is abelian and hence nilpotent. Suppose that the order p^k of $\zeta(P)$ is less than p^n. Then $\zeta(P)$ is nilpotent, by our induction hypothesis, (also form the fact that $\zeta(P)$ is abelian). Also $P/\zeta(P)$ has order p^m, $m < n$ so that $P/\zeta(P)$ is nilpotent. Let

$$P/\zeta(P) = P_0/\zeta(P) \supset P_1/\zeta(P) \supset \ldots \supset P_k/\zeta(P) = \{\zeta(P)\}$$

be a central series of $P/\zeta(P)$. Then, by lemma 13.1.2,

$$[P_{i-1}/\zeta(P), P/\zeta(P)] \subseteq P_i/\zeta(P),\ 1 \le i \le k.$$

That is, for each $y \in P_{i-1}$ and $x \in P$,

$$[y, x]\ \zeta(P) \in P_i / \zeta(P)$$

so that $[y, x] \in P_i$. Hence $[P_{i-1}, P] \subseteq P_i$, $1 \leq i \leq k$. Thus

$$P = P_0 \supset P_1 \supset \ldots \supset P_k = \zeta(P) \supset P_{k+1} = E$$

is a central series for P and P is nilpotent.

If H is a subgroup of G then always $H \subseteq N_G(H)$. The following theorem explains as to when H is properly contained in $N_G(H)$.

13.1.8. Theorem: Let G be a nilpotent group and H a proper subgroup of G. Then H is a proper subgroup of its normaliser $N_G(H)$.

Proof: Since G is nilpotent, $\gamma_k(G) = E$ for some integer k. If

$$G = \gamma_0(G) \supset \gamma_1(G) \supset \ldots\ldots \supset \gamma_k(G) = E,$$

is a central series for G and H a proper subgroup of G then there is an integer $i \neq 0$ such that

$$\gamma_i(G) \subseteq H \text{ but } \gamma_{i-1}(G) \not\subseteq H. \qquad 13.1.8\ (1)$$

From

$$[\gamma_{i-1}(G), G] = \gamma_i(G) \subseteq H$$

we have

$$[\gamma_{i-1}(G), H] \subseteq H.$$

That is, for each $y \in \gamma_{i-1}(G)$,

$$y\, H\, y^{-1} \subseteq H$$

so that $y \in N_G(H)$. Since y is arbitrary, $\gamma_{i-1}(G) \subseteq N_G(H)$. So, from 13.1.8 (1), we see that there is an element x of G such that $x \notin H$ and $x \in N_G(H)$. Hence $N_G(H)$ contains H properly.

13.2. FINITE NILPOTENT GROUPS

In this section we characterise finite nilpotent groups. We shall show that a finite nilpotent group is the direct product of its Sylow p-subgroups. First we prove the following theorem.

13.2.1. Theorem: Let G be a nilpotent group and H a subgroup of prime index in G. Then H is normal in G.

Proof: In a nilpotent group G, the normaliser $N_G(H)$ of H contains H properly, by theorem 13.1.6. Now

$$p = (G : H) = (G : N_G(H)) . (N_G(H) : H)$$

so that either $(G : N_G(H)) = 1$ or $(N_G(H) : H) = 1$ The later equation implies $H = N_G(H)$, a contradiction. Hence $(G : N_G(H)) = 1$ so that

$G = N_G(H)$. Thus H is normal in G.

Now we give a characterisation of finite nilpotent groups.

13.2.2. Theorem: A finite group G is nilpotent if and only if G is the direct product of its Sylow p-subgroups.

Proof: Suppose that G is the direct product of its Sylow p-subgroups. Then, by Theorems 13.1.6 and 13.1.7 applied in succession, G is nilpotent.

Conversely, suppose that G is nilpotent and P a Sylow p-subgroup of G. Let $N = N_G(P)$. Then P is a proper subgroup of N. By Corollary 9.3.3. N is its own normaliser. If N is a proper subgroup of G then N cannot be its own normaliser, a contradiction. Hence

$$N = G = N_G(P)$$

Thus P is normal in G.

Now if $P_1, P_2, ..., P_k$ are the Sylow p_i-subgroups of G of order $p_i^{\alpha_i}$, $1 \le i \le k$ (so that $n = p_1^{\alpha_1} p_2^{\alpha_2} = ... p_k^{\alpha_k}$ = the order of G), then, for any two elements $a \in P_i$ and $b \in P_j$, $i \neq j$,

$$[a, b] \in P_i \cap P_j = E.$$

Hence $ab = ba$. So P_i and P_j commute element wise. Also then

$$P_1 \times P_2 \times ... \times P_k$$

is a subgroup of G having order equal to that of G and so coincides with G. Hence the theorem.

13.3. UPPER CENTRAL SERIES

Given a group G, we define another type of series for G and establish its relationship with the lower central series of G.

We first define a class of subgroup ζ_i (G) of G as follows:

We put

$$\zeta_0 (G) = E$$

and let ζ_i (G) be that subgroup of G for which

$$\zeta_i (G)/ \zeta_{i-1} (G) = \zeta (G/\zeta_{i-1} (G)) \text{ for } i \geq 1.$$

Here ζ (H) denotes the centre of H. We thus have a series

$$E = \zeta_0 (G) \subset \zeta_1 (G) \subset ... \subset \zeta_k (G) \subset ... \subset G \qquad 13.3\ (1)$$

in which ζ_{i-1} (G) is a normal subgroup of ζ_i (G).

The series 13.3 (1) is called the *upper central series for G* if ζ_k (G) = G for some integer k.

13.3.1 Example:

Consider the dihedral group

$$G = D_4 = < a, b = a^4 = b^2 = (ab)^2 = 1 >.$$

Here ζ_0 (G) = E and

$$\zeta_1 (G)/ \zeta_0 (G) = \zeta(G/\zeta_0 (G) \cong \zeta (G) = < a^2 : a^4 = 1 >$$

so that ζ_1 (G) = ζ (G). Now G/ζ (G) is isomorphic to the non-cyclic group of order 4 which is ableian. Hence

$$\zeta(G/\zeta_1 (G)) \cong G/\zeta_1 (G).$$

So

$$\zeta_2 (G) / \zeta_1 (G) = G /\zeta_1 (G).$$

Therefore ζ_2 (G) = G. Thus

$$E = \zeta_0 (G) \subset \zeta_1 (G) \subset \zeta_2 (G) = G$$

is the upper central series for G.

In general, a group may or may not have an upper central series. For instance S_3 has no upper central series.

13.3.2. Theorem: Every term $\zeta_i(G)$ of the upper central series of a group G is a characteristic subgroup of G.

Proof: Let

$$E = \zeta_0(G) \subset \zeta_1(G) \subset \ldots \subset \zeta_k(G) = G$$

be the upper central series of G. We prove the theorem by induction on i. For $i = 0$, $\zeta_0(G) = E$ and for $i = 1$, $\zeta_1(G) = \zeta(G)$ are characteristic subgroups of G.

Now suppose that $\zeta_{i-1}(G)$ is a characteristic subgroup of G for $i \geq 1$ and consider $\zeta_i(G)$. Let α be an automorphism of G. Then $\alpha(\zeta_{i-1}(G)) = \zeta_{i-1}(G)$. Also, for $x \in \zeta_i(G)$,

$$[x\,\zeta_{i-1}(G), y\,\zeta_{i-1}(G)] = \zeta_{i-1}(G), \text{ for all } y \in G,$$

by definition of $\zeta_i(G)$. So, applying α on both sides of the above equation, we have

$$[\alpha(x)\,\zeta_{i-1}(G), \alpha(y)\,\zeta_{i-1}(G)] = \alpha(\zeta_{i-1}(G)) = \zeta_{i-1}(G).$$

As y ranges over the whole of G, $\alpha(y)$ ranges over the whole of G. Hence, replacing $\alpha(y)$ again with y, we have,

$$[\alpha(x)\,\zeta_{i-1}(G), y\,\zeta_{i-1}(G) = \zeta_{i-1}(G) \text{ for all } y \in G.$$

That is $\alpha(x) \in \zeta_i(G)$. Hence $\zeta_i(G)$ is characteristic.

13.3.3. Theorem: Let

$$G = G_0 \supset G_1 \supset \ldots \supset G_k = E$$

be a central series for G. Then $G_i \supseteq \gamma_i(G)$, $i = 0, 1, 2, \ldots, k$ and

$G_{k-i} \subseteq \zeta_i(G)$ for $i = 0, 1, 2, \ldots, k$.

Proof: For $i = 0$, we have $G_0 = G$ and $\gamma_0(G) = G$, Hence $G_0 \supseteq \gamma_0(G)$. So we have a basis for induction. Suppose that $G_i \supseteq \gamma_i(G)$ for $i \geq 0$. We have to show that $G_{i+1} \supseteq \gamma_{i+1}(G)$.

Since G_i/G_{i+1} is contained in the centre of G/G_{i+1}, we have

$$[g_iG_{i+1}, gG_{i+1}] = G_{i+1} \text{ for all } g_i \in G_i \text{ and } g \in G.$$

So

$$[g_i, g] \in G_{i+1} \text{ for all } g_i \in G_i \text{ and } g \in G.$$

Hence

$$[G_i, G] \subseteq G_{i+1}.$$

But then

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \subseteq [G_i, G] \subseteq G_{i+1},$$

by induction hypothesis. Hence, $G_i \supseteq \gamma_i(G)$ for all $i = 0, 1, 2, ..., k$.

Now to prove that $G_{k-i} \subseteq \zeta_i(G)$ for $i = 0, 1, 2, ..., k$, we first observe that for $i = 0$, $G_k = E \subseteq \zeta_k(G)$ so that we have a basis for induction.

Now suppose that

$$G_{k-i} \subseteq \zeta_i(G) \text{ for } i \geq 0.$$

We show that

$$G_{k-i-1} \subseteq \zeta_{i+1}(G). \qquad 13.3.3\ (1)$$

For this, consider the factor group G/G_{k-i}. Since G_{k-i-1}/G_{k-i} is in the centre of G/G_{k-i}, its image, under the homomorphism from G/G_{k-i} to $G/\zeta_i(G)$, is in the centre of $G/\zeta_i(G)$. But the centre of $G/\zeta_i(G)$ is $\zeta_{i+1}(G)/\zeta_i(G)$. Hence, for each $x \in G_{k-i-1}$, xG_{k-i} is mapped onto the element $x\,\zeta_i(G)$ of $\zeta_{i+1}(G)/\zeta_i(G)$. So $x \in \zeta_{i+1}(G)$ and this establishes 13.3.3 (1).

13.3.4. Corollary: If G has a central series

$$G = G_0 \supset G_1 \supset ... \supset G_k = E$$

then $\zeta_k(G) = G$.

(Thus, in a nilpotent group, the upper central series leads to the group itself in a finite number of steps.)

Proof: From

$$G_{k-i} \subseteq \zeta_i(G), \text{ for } i = 0, 1, 2, ..., k,$$

we have, for $k = i$,

$$G = G_0 = G_{k-k} \subseteq \zeta_k(G).$$

But $\zeta_k(G) \subseteq G$. Hence $\zeta_k(G) = G$.

13.3.5. Corollary: In a nilpotent group G, the upper and lower central series have the same length.

13.4. THE FRATTINI SUBGROUP

We recall that a subgroup M of a group G is said to be maximal if M is not properly contained in any other proper subgroup of G.

We now define the Frattini subgroup of group G as follows:

The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all the maximal subgroups of G.

If G has no maximal subgroup then $\Phi(G)$ is taken as G itself.

Since an automorphism of a group maps a maximal subgroup onto a maximal subgroup and hence permutes its maximal subgroups, $\Phi(G)$ is a characteristic subgroup of G. Hence $\Phi(G)$ is a normal subgroup of G.

13.4.1. Example:

Consider the group of Q of quaternions $\pm I, \pm i, \pm j, \pm k$. The maximal subgroups of Q are $\{\pm I, \pm, i\}, \{\pm I, \pm j\}, \{\pm I, \pm k\}$ so that

$$\Phi(Q) = \{\pm I\},$$

is the Frattini subgroup of G.

However, the Frattini subgroup of the alternating group A_4 of degree 4 is trivial.

Here maximal subgroups of A_4 are all of order 3 or 4. So these intersect only in the identity subgroup.

The following theorem gives a characterisation of the Frattini subgroup of a group.

13.4.2. Theorem: The Frattini subgroup of a group G consists of precisely those elements of G which can be omitted from every generating system of generators of G in which they occur.

That is, $a \in \Phi(G)$ if and only if whenever $G = < X, a >$ for a subset X of G then already $G = < X >$.

Proof: Suppose that $a \in \Phi(G)$ and, for an arbitrary subset X of G, $G = \langle X, a \rangle$. Suppose that $G \neq \langle X \rangle$. Then there is a maximal subgroup M of G containing X so that $G = \langle M, a \rangle$. But $\langle M \rangle = M \neq G$ and $a \in \Phi(G) \subseteq M$, a contradiction. Hence $G = \langle X \rangle$.

Conversely suppose that, for an element $a \in G$ and *any* subset X of G,

$$G = \langle X, a \rangle \Rightarrow G = \langle X \rangle.$$

Take X = M, a maximal subgroup of G.

Then we have $\langle M \rangle = M \neq G$ so that

$$\langle M, a \rangle \neq G$$

(for otherwise $G = \langle M \rangle$ by our supposition).

Hence

$$\langle M, a \rangle = M$$

which implies $a \in M$ for an arbitary maximal subgroup M.

Thus $a \in \Phi(G)$, as required.

13.4.2. Corollary: For any subset X of G, $\langle X, \Phi(G) \rangle = G$ implies

$$\langle X \rangle = G.$$

Let G be a group and H a normal subgroup of G. A subgroup K of G is said to be a *partial complement* of H in G if

$$G = HK.$$

13.4.3. Theorem: A normal subgroup H of G is contained in the Frattini subgroup of G if and only if H has no partial complement in G.

Proof: Let H be a normal subgroup of G and contained in $\Phi(G)$. Suppose that H has a partial complement K in G. Then

$$\langle H, K \rangle = HK = G.$$

But $H \subseteq \Phi(G)$ implies

$$G = \langle H, K \rangle = K,$$

a contradiction. Hence H has no partial complement in G.

Conversely, suppose that a normal subgroup H has no partial complement in G. Then, for each subgroup K of G, $HK \neq G$. Choose K to be a maximal subgroup of G. Then $HK \neq G$ implies $H \subseteq K$ for every maximal subgroup K of G. Hence $H \subseteq \Phi(G)$.

13.4.4. Theorem: Let H be a normal subgroup of G contained in $\Phi(G)$. Then

$$\Phi(G/H) = \Phi(G)/H.$$

Proof: Under the natural homomorphism $\mu : G \to G/H$, there is a one-one correspondence between subgroups of G/H and those subgroups of G which contain H. Since $H \subseteq \Phi(G)$, the maximal subgroups of G (containing, of course, H) and of G/H correspond. Hence

$$\Phi(G/H) = \cap (M/H), \text{ M a maximal subgroup of G}$$

$$= (\cap M)/H$$

$$= \Phi(G)/H$$

as required.

In general, we have the following.

13.4.5. Theorem: Let $\alpha : G \to G'$ be a surjective homomorphism. Then $g \in \Phi(G)$ implies $\alpha(g) \in \Phi(G')$.

Proof: Suppose that $g \in \Phi(G)$. Let M′ be an arbitrary maximal subgroup of G′. Then there is a maximal subgroup M of G such that $\alpha(M) = M'$. But then $g \in M$ implies $\alpha(g) \in M'$. As M′ is arbitrary, $\alpha(g) \in \Phi(G')$.

13.4.6. Corollary: For any surjective homomorphism $\alpha : G \to G'$,

$$\alpha(\Phi(G)) = \Phi(\alpha(G)).$$

Next we prove a theorem which charactrises the Frattini subgorup of a finite group.

13.4.7. Theorem: The Frattini subgroups of a finite group G is nilpotent.

Proof: Let Φ (G) be the Frattini subgroup of a finite group G. We show that Φ (G) is the direct product of its Sylow p-subgroups. For this it is enough to show that every Sylow p-subgroup of Φ (G) is normal.

Let P be any Sylow p-subgroup of Φ (G). Since Φ (G), being a characteristic subgroup, is normal in G, for every $g \in G$,

$$g P g^{-1} \subseteq g \Phi (G) g^{-1} = \Phi (G).$$

So $g P g^{-1}$ is a Sylow p-subgroup of Φ (G) and hence conjugate to P in Φ (G). Thus there exists an $x \in \Phi$ (G) such that

$$xPx^{-1} = gPg^{-1}$$

so that $x^{-1} g \in N_G (P)$. That is $g \in xN_G (P) \subseteq \Phi (G) N_G (P)$. Since g is an arbitrary element of G, we have,

$$G \subseteq \Phi (G) N_G (P) \subseteq G.$$

$$G = \Phi (G). N_G (P) = < \Phi (G), N_G (P) >$$

$$= N_G (P)$$

because each element of Φ (G) can be ignored from any generating system of G. Hence P is normal in G and therefore in Φ (G)., Thus Φ (G) is nilpotent, by Theorem 13.2.2.

13.4.8. Theorem: If K is a normal subgroup and H a subgroup of G such that $K \subseteq \Phi (H)$, then $K \subseteq \Phi (G)$.

Proof: Suppose that K is a normal subgroup of G, $K \subseteq \Phi$ (H) but that K is not cntained in Φ (G). Then, by Theorem 13.4.3, K has a partial complement L in G so that G = KL. Since $K \not\subseteq L$, so $K \not\subseteq L \cap H$. So $L \cap H$ is a proper subgroup of H . Now G = KL implies

$$H = H \cap G = H \cap KL.$$

But $x \in H \cap KL$ implies $x \in H$ and $x \in KL$ so that

$$x = k\ell \text{ for some } k \in K \subset H \text{ and } \ell \in L.$$

Hence $\ell = k^{-1}x \in H$. But $\ell \in L$. Hence $\ell \in L \cap H$. Therefore $x \in K (L \cap H)$. So $H \cap KL \subseteq K(L \cap H)$. But clearly $K (L \cap H) \subseteq H \cap KL$. Hence

$$H = H \cap KL = K (L \cap H).$$

So K has a partial complement in H. Thus $K \not\subseteq \Phi$ (H) by 13.4.3, a contradiction. Hence $K \subseteq \Phi$ (G).

The next theorem establishes a relationship between the structure of a group G and its commutator and Frattini subgroups.

13.4.9. Theorem: (Wielandt). A finite group G is nilpotent if and only if $G' \subseteq \Phi(G)$.

Proof: Suppose that G is nilpotent. We show that G' is contained in every maximal subgroup of G. Let M be an arbitrary maximal subgroup of G. Since G is nilpotent, $N_G(M)$ contains M properly so that $N_G(M) = G$. Hence M is normal in G. Since M is also maximal, G/M is of prime order and hence abelian. So $G' \subseteq M$. That is

$$G' \subseteq \cap M.$$
$$\subseteq \Phi(G).$$

Conversely, suppose that $G' \subseteq \Phi(G)$. Let P be a Sylow p-subgroup of G and $N_G(P)$ its normaliser in G. Suppose that $N_G(P)$ is properly contained in G. Then $N_G(P)$ is contained in a maximal subgroup M of G. Since $G' \subseteq \Phi(G) \subset M$, M/G', being a subgroup of an abelian group G/G', is normal in G/G'. But then M is normal in G. However, by Theorem 9.3.2., M is its own normaliser, a contradiction. Hence $N_G(P) = G$. So every Sylow p-subgroup is normal in G. Therefore G is nilpotent, by Theorem 13.2.2.

13.5. SUPERSOLVABLE GROUPS

In this section we discuss a new class of groups which lies in between the classes of finitely generated nilpotent group and solvable groups. The groups of this class will be termed as supersolvable groups. Before we define a supersovable group we need the following concept.

A series

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k = E$$

of subgroup of a group G is said to be an *invariant series* if each G_i is normal in G, $1 \leq i \leq k$.

Such a series is clearly a normal series.

Also it is easy to see that an invariant series is a principal series if and only if each G_i is a maximal normal subgroup of G contained in G_{i-1}, $1 \leq i \leq k$.

A group G is said to be *supersolvable* if it has an invariant series with cyclic factors.

Clearly every supersolvable group is solvable. However, a solvable group need to be supersolvable.

13.5.1. Examples:

1. The alternating group A_4 has no invariant series with cyclic factors. A principal series of A_4 is

   $$A_4 \supset V \supset E$$

   where V is Klein's four-group. Here A_4/V is cyclic but V/E is not cyclic. Hence A_4 is not supersolvable. However it is solvable.

2. Let $C_p\infty$ denote Prufer's p-group. $C_p\infty$ being abelian, is nilpotent. However $C_p\infty$ is not supersolvable.

   This follows from the theorem given below.

13.5.3. Theorem: Every supersolvable group is finitely generated.

Proof: Suppose that G is supersolvable and

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k = E$$

is an invariant series with cyclic factors. Suppose that, under the natural homomorphism of G_{i-1} onto G_{i-1}/G_i, an element a_{i-1} of G_{i-1} is mapped onto a generating element of G_{i-1}/G_i. Then

$$G_{i-1} = < G_i, a_{i-1} >, i = 1, 2, \ldots, k.$$

So the elements $a_0, a_1, a_2, \ldots, a_{k-1}$ generate G.

13.5.4. Theorem: Every subgroup and factor group of a supersolvable is supersovable.

Proof: Let G be a supersolvable group and H a subgroup of G. Since every invariant series is a normal series, by Theorem 10.3.11, H has a normal series whose factors (after deletion of repetitions) are isomorphic to subgroups of the factors of the invariant series for G. These, being subgroups of cyclic groups, are all cyclic. But such a normal series for H is, in fact, an invariant series for H with cyclic factors. Hence H is supersolvable.

Next, let K be a normal subgroup of a supersolvable gorup G. If

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k = E \qquad 13.5.4\ (1)$$

is an invariant series for G, then the natural homomorphism of G onto G/K maps 13.5.4 (1) onto the invariant series.

$$G / K = G_0 / K \supseteq G_1K / K \supseteq \ldots \supseteq G_k\ K/K = K/K \qquad 13.5.4\ (2)$$

of G/K. Each factor $(G_{i-1}K/K)/(G_iK/K)$ of 13.5.4 (2) is isomorphic to a subgroup of the factor (G_{i-1}/G_i) of 13.5.4 (1) and hence is cyclic. So G/K is supersolvable.

Before we prove the next result we note the well known facts that the factor group of a finitely generated and also that every subgroup of a finitely generated nilpotent group is finitely generated. We also assume the following result about finitely generated abelian groups.

Every finitely generated abelian group is the direct product of a finite number of cyclic groups, finite or infinite.

13.5.5. Theorem: Every finitely generated nilpotent group is supersolvable.

Proof: Suppose that G is a finitely generated nilpotent group. Then G has a central series

$$G = G_0 \supset G_1 \supset \ldots \supset G_k = E \qquad 13.2.5\ (1)$$

and the factors G_{i-1}/G_i are abelian and finitely generated. As such each G_{i-1}/G_i is the direct product of cyclic groups. The characteristic property of central series namely that $G_{i-1}/G_i \subseteq \zeta\ (G/G_i)$ enables one to refine the central series 13.2.5 (1) by inserting only a finite number of additional terms so that the factors of the refined series are cyclic and finite in number. So G is supersolvable.

13.5.6. Theorem: A finite group G is supersolvable if and only if it has a principal series whose factors are cyclic of prime order.

Proof: If a group G has a principal series whose factors are cyclic of prime order then such a series is also an invariant series with cyclic factors. Hence G is supersolvable.

Conversely, suppose that G is a finite supersolvable group. Then G has an invariant series.

$$G = G_0 \supset G_1 \supset ,.... \supset G_k = E \qquad 13.5.6\ (1)$$

with each $G_{i-1} / G_i = K_i$, a cyclic group of finite order. Now consider the pair (G_{i-1}, G_i). Let m_i be the order of the cyclic group $K_i = G_{i-1} / G_i$. Let

$$m_i = p_1 p_2 \cdots p_r$$

where p_i's are primes not necessarily all distinct. For each divisor μ_{i_j} of m_i, K_i has a unique subgroup of order μ_{i_j}. Such a subgroup is therefore characteristic. Put

$$\mu_{i_j} = p_{j+1} p_{j+2} \cdots p_r,\ 0 \le j \le r - 1$$

Then K_i has characteristic subgroups

$$K_i = K_{i0} \supset K_{i1} \supset K_{i2} \supset \cdots \supset K_{ir-1} \supset K_{ir} = E$$

of orders

$$m_i = m_{i0}\ ,\ m_{i1} = m_{i0}/p_1,\ ...,\ m_{i_r} = m_{i_{r-1}}/p_r$$

respectively. Each K_{ij}, being a subgroup of G_{i-1} / G_i, is of the form H_q / G_i, $0 \le q \le r$. Also, since H_q / G_i is a characteristic subgroup of a normal subgroup G_{i-1} / G_i of G/G_i, H_q / G_i is normal in G/G_i, $0 \le q \le r$. So H_q is normal in G. Inserting now additional terms of the form H_q / G_i, $0 \le q \le r$, between any two (G_{i-1}, G_i), $1 \le i \le k$, we have a finite refinement of the series 13.5.6 (1) and the factors of the new series are cyclic of prime order. But such a refinement then becomes a principal series whose factors are cyclic of prime order.

A slight additional argument yields the following.

13.5.7. Theorem: Let G be a supersolvable group. Then G has an invariant series whose factors are cyclic of infinite or prime order.

EXERCISES

1. Prove that if a finite group G has a unique subgroup of order m for each divisor m of the order n of G then G is cyclic.

2. A normal subgroup M of a group G is said to be *minimal* if it does not properly contain any other normal subgroup of G. If M is a minimal normal subgroup and K a nilpotent normal subgroup of a group G then show that

$$M \subseteq C_G(K).$$

3. A group G is said to satisfy the *normaliser condition* for subgroups if every proper subgroup H of G is a proper subgroup of its normaliser $N_G(H)$. Likewise a group G is said to satisfy the *maximal condition* for subgroups if every collection of subgroups of G contain a maximal subgroup namely a subgroup which is not properly contained in any other subgroup of the collection.

   Show that a group G which satisfies both the maximal condition and normaliser condition on subgroups is nilpotent.

4. If H is a maximal nilpotent subgroup of a group G and $N = N_G(H)$, then N is its own normaliser.

5. Let G be a group. The *Fitting subgroup (or nil radical)* of G is the set R(G) consisting of those elements of G which lie in some normal nilpotent subgroup of G. Show that the Fitting subgroup is a characteristic subgroup of G.

6. Show that every subgroup of a finitely generated nilpotent group is nilpotent.

7. Let H and K be normal subgroups of a group G such that

$$K \subseteq H \subseteq \Phi(G)$$

   and H / K is nilpotent. Show that H is nilpotent.

8. Let $G = A \times B$ be finitely generated. Show that

$$\Phi(G) = \Phi(A) \times \Phi(B)$$

9. Prove that the commutator subgroup G' of a finite group G is nilpotent if and only if the second derived group of G is contained in Φ (G).

10. Let G be an infinite cyclic group. Show that Φ (G) = E. Also show that there exists a normal subgroup N of G such that $\Phi (G/N) \neq E$.

Chapter - XIV

FREE GROUPS AND FREE PRODUCTS OF GROUPS

In this chapter we discuss, in a sense, the most general class of groups namely the free groups. It will be shown that every group is a homomorphic image of a suitable free group. We shall also define the notions of free products of groups and of the generalized free products of groups.

14.1. FREE GROUPS: BASIC THEORY

Let B be a collection of symbol x_α, $\alpha \in \Omega$. Let B^{-1} be the set of symbols x_α^{-1} which correspond to x_α in a one-one correspondence $x_\alpha \to x_\alpha^{-1}$. Put $X = B \cup B^{-1}$. By a 'word' in X we mean an expression of the form

$$w = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k}, \quad \epsilon_i = \pm 1, \alpha_i \in \Omega, 1 \le i \le k. \qquad 14.1(1)$$

The *word* w in 14.1 (1) is said to be *freely reduced* if the symbols x_α^{ϵ} and $x_\alpha^{-\epsilon}$, $\epsilon = \pm 1$, $\alpha \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, called *associates*, do not occur consecutively.

For example, the words.

$$x_1 x_2 x_2^{-1} x_1 x_2 \text{ and } x_2^{-1} x_2 x_1 x_2 x_1^{-1} x_1 x_1^{-1}$$

are not freely reduced while the words

$$x_1 x_2 x_1^{-1} x_2 x_1 x_2 \text{ and } x_1 x_2^{-1} x_1 x_3 x_1 x_2$$

are freely reduced.

Among the words in X we also include the *empty word* which contains no symbol. The empty word is denoted by the symbol '*e*'.

Any word in X can be brought into the form of a freely reduced word or the empty word by successive use of *cancellation* of associates. Thus, for example, in the word

$$x_1 x_2 x_2^{-1} x_1 x_3 x_3^{-1} x_2 x_1$$

cancellation of associates yields the word $x_1 x_1 x_2 x_1$ which is freely reduced.

Freely reduced words are uniquely determined

Let F be the set of all freely reduced words on X. For any two elements

$$w = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k}, \epsilon_i = \pm 1, \alpha_i \in \Omega, 1 \le i \le k, \quad 14.1(2)$$

$$w' = x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \ldots x_{\beta_m}^{\delta_m}, \delta_j = \pm 1, \beta_j \in \Omega, 1 \le j \le m, \quad 14.1(3)$$

of F, we define the product ww' of w and w' by juxtaposition, that is, by writing ww′ as:

$$ww' = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k} . x_{\beta_1}^{\delta_1} \ldots x_{\beta_m}^{\delta_m}$$

and bring the right hand expression in the reduced form by successive cancellation of the associates if any[§].

Also if

$$w'' = x_{\gamma_1}^{\eta_1} x_{\gamma_2}^{\eta_2} \ldots x_{\gamma_r}^{\eta_r}, \eta_i = \pm 1, \gamma_i \in \Omega, 1 \le i \le r, \quad 14.1(4)$$

is another element of F, then, by discussing various possibilities of cancellation of associates, the associative law

$$(ww')w'' = w(w'w'')$$

holds in F.

The empty word, denoted by e, serves as the identity element in F.

Also, for each freely reduced word w, as given in 14.1 (2),

$$w^{-1} = x_{\alpha_k}^{-\epsilon_k} x_{\alpha_{k-1}}^{-\epsilon_{k-1}} \ldots x_{\alpha_1}^{-\epsilon_1} \quad 14.1(5)$$

[§] Two freely reduced words w and w′ as given in 14.1 (2), 14.1 (3) are *equal* if and only if their corresponding components are equal.

is freely reduced and satisfies the equation

$$ww^{-1} = w^{-1}w = e.$$

So each element of F has an inverse in F. This shows that F is a group under the product of words defined above.

F is known as a *free group* on the set B and the elements of B are called a *free system* of generators for F.

The set B is also said to be a *free basis* of F.

The number of elements in B is called the *free rank* of F.

Thus if B consists of n elements then F is called a *free group of rank n* and is denoted by F_n.

In fact the relation 'Two words w and w′ are equivalent if and only if the two have the same freely reduced form' obviously is an equivalence relation.

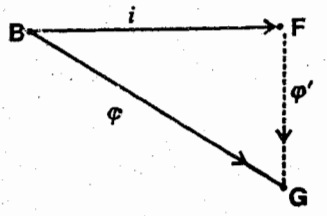
A free group of rank one is simply the infinite cyclic group and is the only example of an abelian free group.

All free groups of rank greater or equal to 2 are non-abelian because in such groups the words $x_1 x_2$ and $x_2 x_1$ always represent distinct elements.

We can also define a free group as follows:

Let B be a set and F a group containing B. Then F is said to be a free group on B if, for any group G and mapping $\varphi : B \to G$, there is a unique homomorphism $\varphi' : F \to G$ which coincides with φ on B.

If we denote the identity mapping of B into F by i, then F is free if and only if, for every group G and a mapping $\varphi : B \to G$, there is a unique homomorphism $\varphi' : F \to G$ such that the following diagram is commutative.



That is

$$\varphi' i = \varphi$$

A freely reduced word

$$w = x_{\alpha_1}^{\epsilon_1} . x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k}$$

as given in 14.1 (2), is said to be *cyclically reduced* if $x_{\alpha_k}^{\epsilon_k} \neq x_{\alpha_1}^{-\epsilon_1}$ that is, $\alpha_k \neq \alpha_1$ or $\epsilon_k \neq -\epsilon_1$.

$$x_1 x_2 x_3^{-1} \quad \text{and} \quad x_1^{-1} x_2 x_3 x_2$$

are cyclically reduced while

$$x_1 x_2 x_1^{-1}, x_2^{-1} x_3^{-1} x_4 x_1 x_3 x_2$$

are not cyclically reduced.

14.1.1. Theorem: In a free group F with a free basis B, every element different from e is of infinite order.

Proof: Let

$$w = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k}, \epsilon_i = \pm 1, x_{\alpha_i} \in B, 1 \leq i \leq k,$$

be a non-trivial element in F. Suppose that w is cyclically reduced. That is, $\alpha_k \neq \alpha_1$ or $\epsilon_k \neq -\epsilon_1$. Then

$$w^n = x_{\alpha_1}^{\epsilon_1} \ldots x_{\alpha_k}^{\epsilon_k} . x_{\alpha_1}^{\epsilon_1} \ldots x_{\alpha_k}^{\epsilon_k} \ldots x_{\alpha_k}^{\epsilon_k}$$

that is, w combined with w n-times, cannot reduce to the empty word. Hence $w^n \neq e$ for any integer n so that w is of infinite order.

If, however, w is not cyclically reduced, then

$$w = x_{\alpha_1}^{\epsilon_1} \ldots x_{\alpha_m}^{\epsilon_m} . x_{\gamma_1}^{\eta_1} x_{\gamma_2}^{\eta_2} \ldots x_{\gamma_r}^{\eta_r} - x_{\alpha_m}^{-\epsilon_m} \ldots x_{\alpha_1}^{\epsilon_1}$$

where $\gamma_r \neq \gamma_1$ or $\eta_r \neq -\eta_1$. Put

$$w_1 = x_{\alpha_1}^{\epsilon_1} \ldots x_{\alpha_m}^{\epsilon_m}, \quad w_2 = x_{\gamma_1}^{\eta_1} \ldots x_{\gamma_r}^{\eta_r}$$

Then w_2 is cyclically reduced and

$$w = w_1 w_2 w_1^{-1}$$

So, for any integer n,

$$w^n = w_1 w_2^n w_1^{-1}$$

Since $w_2^n \neq e$ for any integer n, $w^n \neq e$. Thus w is of infinite order.

In view of the above theorem we see that *every fee group is torsion free*, that is, each non-identity element of a free group has infinite order.

A group G is said to be *locally in ïnite* if every finitely generated subgroup of G is infinite.

The above theorem shows that *every free group is locally infinite.*

14.1.2. Theorem: Every group is isomorphic to a factor group of a free group of suitable rank.

Proof: Let G be an arbitrary group and S a system of generators for G. Such a system of generators always exists. (For example one can take S = G.) Then each $g \in G$ is of the form

$$g = g_{\alpha_1}^{\epsilon_1} g_{\alpha_2}^{\epsilon_2} \ldots g_{\alpha_k}^{\epsilon_k}, \epsilon_i = \pm 1, g_{\alpha_i} \in S, 1 \leq i \leq k.$$

Let X be a set of symbols and of cardinality (the number of elements) of X be equal to that of S. Let F be the free group on X. Define a mapping $\varphi : F \to G$ as follows:

For

$$w = x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k},$$

in F, we put

$$\varphi(w) = g_{\alpha_1}^{\epsilon_1} g_{\alpha_2}^{\epsilon_2} \ldots g_{\alpha_k}^{\epsilon_k}$$

Then it is easy to check that φ is a homomorphism of F onto G.

By the fundamental theorem of homomorphism of groups, F has a normal subgroup R, say, such that

$$F/R \cong G,$$

as required.

The normal subgroup R of F, determined by Theorem 14.1.2, is such that if

$$x_{\alpha_1}^{\epsilon_1} x_{\alpha_2}^{\epsilon_2} \ldots x_{\alpha_k}^{\epsilon_k}$$

is in R, then the corresponding image

$$g_{\alpha_1}^{\epsilon_1} g_{\alpha_2}^{\epsilon_2} \ldots g_{\alpha_k}^{\epsilon_k} = e$$

Because of this, every relation in G corresponds to some element of R. Let R* be an irreducible system of generators for R. Then the relations in G, corresponding to the elements in R*, are called the *defining relations* of G.

If $\{w_\alpha : \alpha \in \Lambda\}$ are elements of R*, then we write

$$G = < S : w_\alpha(s_{\alpha_1}, s_{\alpha_2}, ..., s_{\alpha_r}) = 1, \alpha \in \Lambda, s_{\alpha_i} \in S, 1 \leq i \leq r > \quad 14.1.2\ (*)$$

and call 14.1.2 (*) a *presentation* of G.

Thus it follows that every group has a presentation in terms of generators and relations.

14.1.2 (*i*) Examples:

1. Let $X = \{a_1, a_2, ..., a_n\}$ and $R = ([a_i, a_j] : a_i, a_j \in X)$.

   Here $[a_i, a_j]$ is the usual commutator $a_i\ a_j\ a_i^{-1}\ a_j^{-1}$ of a_i, a_j. Then $F/_R$ is called the *free abelian group* of rank n.

2. A presentation of the infinite dihedral group is

   $$D_\infty = < a, b: a^2 = b^2 = 1 >$$

   and each finite dihedral group of order $2n$ has a presentation as:

   $$D_n = < a , b = a^n = b^2 = (ab)^2 = 1$$

   Or: $D_n = < a, b : a^2 = b^2 = (ab)^n = 1$

3. The group A_4, having a presentation

   $$A_4 = < a, b : a^3 = b^3 = (ab)^2 = 1 >$$

is the alternating group A_4 of degree 4. A_4 is isomorphic to a factor group F/R of F by R. Here R is the normal closure of

$$< a^3, b^3, ab\ ab >$$

in the free group of rank 2 with $\{a, b\}$ as its basis.

A free group has no defining relations. This fact leads to another definition of a free group.

A group F on a non-empty set X is free if and only if the set of relations in F is void.

14.1.3. Von Dyck's Theorem: Let G_1 and G_2 be groups having the same system of generators. Suppose that all the relations of G_1 occur among the relations of G_2. Then G_2 is isomorphic to a factor group of G_1.

Proof: Let F be a free group of suitable rank such that

$$G_1 \cong F/R_1 \text{ and } G_2 \cong F/R_2,$$

where R_1 and R_2 are determined by the defining relations of G_1 and G_2 respectively.

Since every defining relation of G_1 occurs among the defining relations of G_2, R_1 is a normal subgroup of $R_2 \subseteq F$. The factor group R_2/R_1 is a normal subgroup of F/R_1. The normal subgroups of F/R_1 and those of G_1 correspond. Let N be the normal subgroup of G_1 which corresponds to R_2/R_1.

Then

$$G_1/N \cong (F/R_1) / (R_2/R_1) \cong F/R_2 \cong G_2,$$

as required.

14.1.4. Illustrations:

1. Let

$$G = \langle a, b : a^2 = b^2 = 1 \rangle,$$

$$D_n = \langle a, b : a^2 = b^2 = (ab)^n = 1 \rangle.$$

Then D_n is a homomorphic image of G. This is so because D_n has an additional relation $(ab)^n = 1$.

Here G is the infinite dihedral group while D_n is the dihedral group of order 2n.

2. Let F be a free group with basis $B = \{a_1, a_2, a_3, ..., a_n\}$. Then the set of relations in F is empty.

Now let

$$A_n = \langle a_1, a_2, a_3, ..., a_n : [a_i, a_j] = e, 1 \le i, j \le n \rangle.$$

Let R be the normal closure of

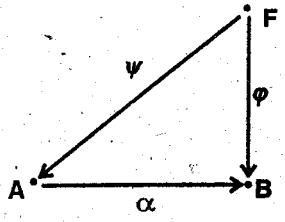
$$\langle [a_i, a_j], 1 \le i, j \le n \rangle$$

in F. Then $F/R \cong A_n$.

The group A_n is called the *free abelian group of rank n.*

14.1.5. Theorem: (Projective property of free groups)

Let A and B be any groups and $\alpha : A \to B$ be an epimorphism. Let F be a free group and $\varphi : F \to B$ be a homomorphism. Then there is a unique homomorphism $\psi : F \to A$ such that the following diagram is commutative.



That is $\alpha \psi = \varphi$.

Proof: Let $X = \{x_i : i \in I\}$ be a basis of F. Then

$$\varphi(x_i) = b_i \in B, i \in I.$$

Since α is onto B, there is an $a_i \in A$ such that

$$\alpha(a_i) = b_i.$$

Define a mapping $\gamma : X \to A$ by:

$$\gamma(x_i) = a_i, i \in I.$$

By the fact that F is free, γ has a unique extension to a homomorphism $\psi : F \to A$ such that

$$\psi(x_i) = \gamma(x_i), i \in I.$$

Then

$$(\alpha\psi)(x_i) = \alpha(a_i) = b_i = \varphi(x_i)$$

for all $x_i \in X$, $i \in I$. Since α, φ and ψ, are homomorphisms, for each $f \in F$, f is a word in elements of X. So

$$(\alpha\psi)(f) = \varphi(f), f \in F.$$

Hence $\alpha \psi = \phi$, as required.

14.2. FREE PRODUCT OF GROUPS

In this section we shall define the ordinary free product of groups. This construction is more general than that of free groups, in the sense that a free group is the free product of infinite cyclic groups whereas a free product of groups is not necessarily a free group.

Let $\{G_\alpha : \alpha \in 1\}$ be a family of subgroups of a group G. The group G is said to be the *ordinary free product* of G_α, $\alpha \in$ I, if

(i) the subgroups G_α generate G, that is, every element $g \neq e$ of G is expressible as product of a finite number of elements from G_α's *i..e.*

$$g = g_1 g_2 \cdots g_k, \qquad g_i \in G_{\alpha_i}, g_i \neq e, i = 1, 2, ..., k; \quad 14.2(*)$$

$$\text{and } \alpha_i \neq \alpha_{i+1}, i = 1, 2, ..., k-1.$$

(ii) the expression (*) for g is unique for every $g \neq e$ in G.

If G is the free product of G_α, $\alpha \in$ I, then we write

$$G = \overset{*}{\prod_{\alpha \in I}} G_\alpha$$

If the indexing set I is finite then we use the notation

$$G = G_1 * G_2 * ... * G_n.$$

The subgroups G_α of G, $\alpha \in$ I, are called the *free factors* of G while the expression (*) is called the *normal form* of an element g of G.

The uniquely determined integer k in the expression 14.2 (*) is called the *length of g*.

Thus, in a free product, no two elements having different lengths can be equal.

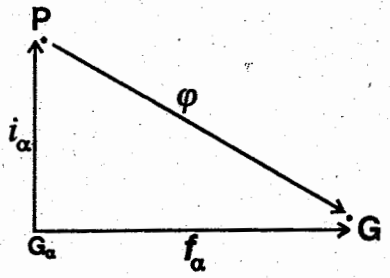
Also, an element g_α of G_α in G is considered to have length 0 or 1 according as g_α is or is not the identity element of G_α

We can define the free product of groups in another way as follows:

Let $\{G_\alpha : \alpha \in I\}$ be a family of groups. The free product of G_α, $\alpha \in I$, is a group P such that:

(1) P contains an isomorphic copy of each G_α that is, for each $\alpha \in I$, there is a monomophism $i_\alpha : G_\alpha \to P$;

(2) For every group G and every family of homomorphisms $f_\alpha : G_\alpha \to G$, there is a unique homomorphism $\varphi : P \to G$ which extends each f_α such that the diagram



is commutative. That is $\varphi i_\alpha = f_\alpha$ for all $\alpha \in I$.

Still another definition of a free product is as follows:

Let $\{G_\alpha : \alpha \in I\}$ be a family of groups such that each G_α has a presentation

$$G_\alpha = \langle X_\alpha : R_\alpha \rangle,$$

where X_α is a system of generators and R_α is the set of all defining relations of G_α for all $\alpha \in I$. Put

$$X = \bigcup_{\alpha \in I} X_\alpha \qquad R = \bigcup_{\alpha \in I} R_\alpha$$

Then the group

$$G = \langle X : R \rangle,$$

with X as its system of generators and R as the set of its defining relations, is called the free product of the groups G_α, $\alpha \in I$.

14.2.1. Examples:

(i) The infinite dihedral group

$$D_\infty = \langle a, b : a^2 = b^2 = 1 \rangle$$

is the free product of cyclic groups

$$A = \langle a : a^2 = 1 \rangle, B = \langle b : b^2 = 1 \rangle$$

(ii) Let $C^* = C \cup \{\infty\}$ be the extended complex plane. Consider the mappings $\alpha : C^* \to C^*$, $\beta = C^* \to C^*$, defined by:

$$\alpha(z) = \frac{1}{-z+1}, \beta(z) = -\frac{1}{z}, z \in C^*$$

Then $\alpha^3 = \beta^2 = I$ where I denotes the identity mapping of C^*, and

$$G = \langle \alpha, \beta : \alpha^3 = \beta^2 = I \rangle$$

is the free product of $A = \langle \alpha : \alpha^3 = I \rangle$, $B = \langle \beta : \beta^2 = I \rangle$.

Here G is the group of all unimodular linear fractional mappings namely the transformations $\varphi : C^* \to C^*$ given by:

$$\varphi(z) = \frac{az+b}{cz+d}, z \in C^*, ad - bc = 1, a, b, c, d \text{ integers.}$$

(cf. Combinatorial Group Theory by Magnus, Karrass and Solitar)

14.2.2. Theorem: If a group G is the free product of the groups G_α, $\alpha \in I$, then $G_\alpha \cap \langle G_\beta : \beta \in I, \beta \neq \alpha \rangle = E$.

Proof: Suppose that $g \in G_\alpha \cap \langle G_\beta : \beta \in I, \beta \neq \alpha \rangle$. Then

$$g = g_\alpha$$

$$= g_{\beta_1} g_{\beta_2} \cdots g_{\beta_k}, \qquad g_{\beta_i} \in G_{\beta_i}, \beta_i \neq \alpha, 1 \leq i \leq k,$$

has two expressions for $g \in G$. Also no $g_{\beta_i} = g_\alpha$ for $\beta_i \neq \alpha, 1 \leq i \leq k$. So, by the uniqueness of the expressions for elements of G, $g = e$. Hence

$$G_\alpha \cap \langle G_\beta : \beta \in I, \beta \neq \alpha \rangle = E.$$

14.2.3. Theorem: Let $G = A * B$ and C be a subgroup of A, D a subgroup of B. Then the subgroup H of G generated by C and D is the free product of C and D.

Proof: Since H is generated by C and D, each $h \in H$ is of the form $h_1 h_2 \ldots h_k$, $h_i \in C$ or D. But then h is also an element of G so that the representation

$$h = h_1 h_2 \ldots h_k$$

of h in G is unique in G and so also is in H. Also $C \cap D \subseteq A \cap B = E$. Hence

$$H = C * D.$$

14.2.4. Theorem: If an element g of $G = A * B$ is of finite order then g is conjugate to an element of finite order in A or in B.

Proof: Suppose that g is an element of finite order in A * B. Then, in the normal form,

$$g = g_1 g_2 \cdots g_k , \qquad g_i \in A \text{ or } B. \qquad 14.2.4\ (*)$$

We use induction on the length k of g. If k = 0 or 1 then $g = e$ or $g = g_1$ is element of A or B so that the assertion holds.

Suppose that, for all x of length less than k, if x has finite order then x is conjugate to some element of A or of B. Let g in G as in (*) have length k and have finite order. If, in the normal form 14.2.4 (*) of g, g_1 and g_k are not in the same free factor then, for any integer m,

$$g^m = g_1 g_2 \cdots g_k\, g_1 g_2 \cdots g_k \cdots g_1 g_2 \cdots g_k$$

has length > k so that $g^m \neq e$ for any integer m. If g_1, g_k are in the same factor then

$$g_1^{-1}\, g g_1 = g_2\, g_3 \cdots (g_k\, g_1)$$
$$= x$$

has length less than k. If g is of finite order then so is $g_1^{-1}\, g g_1$. So by our induction hypothesis, some conjugate g' of $g_1^{-1}\, g g_1$ and so also of x is in a free factor. But then g' and g are also conjugate and are in the same free factor.

Hence the theorem.

As an immediate consequence of the above theorem, we have the following:

14.2.5. Corollary: The free product of torsion free groups is torsion free.

14.2.6. Theorem: Suppose that $g \in A * B$ and both a and $g\, a\, g^{-1}$ belong to A, $a \neq 1$. Then $g \in A$. In particular, if $g \notin A$, then

$$g\, A\, g^{-1} \cap A = E.$$

Proof: Suppose that

$$g = g_1 g_2 \cdots g_k, \qquad 14.2.6\ (1)$$

$g_i \in A$ or B but not to both, $1 \le i \le k$, is the normal from of $g \in A * B$. We apply induction on the length k of g to prove our assertion.

Suppose that k = 0 or 1. Then $g = e$ or $g = g_1$ is in A or B. If $g_1 = g \in A$, we have nothing to prove. If $g_1 \in B$, with a and $g_1 a g_1^{-1} = a'$ in A, then the length of a' is 1 whereas the length of $g_1 a g_1^{-1}$ is 3. Hence $g_1 \in A$. That is, $g = g_1 \in A$.

Now suppose that k > 1 and that, for all elements x of length < k, both a and xax^{-1} in A imply $x \in A$. Let g, as in 14.2.6 (1), be an element of A * B of length k and, for $a \in A$, both a and $gag^{-1} \in A$. Suppose that $g_k \notin A$. Then

$$g a g^{-1} = g_1 g_2 \cdots g_k a g_k^{-1} g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}$$

has length > k and so is not in A, a contradiction to our supposition that $gag^{-1} \in A$. Thus $g_k \in A$ and $1 \neq g_k a g_k^{-1} \in A$. Now, by our induction hypothesis,

$$gag^{-1} = g_1 g_2 \cdots g_{k-1} (g_k a g_k^{-1}) (g_{k-1}^{-1}) \cdots g_2^{-1} g_1^{-1}$$

in A implies $g_1 g_2 \cdots g_{k-1}$ in A. But then

$$g = (g_1 g_2 \cdots g_{k-1}) g_k$$

is in A, as required.

Next suppose that $g \notin A$. Then for any $a \in A$, $gag^{-1} \notin A$, for otherwise $g \in A$, by the remarks given above.

Hence

$$g A g^{-1} \cap A = E.$$

14.2.7. Corollary: The centre of a free product is trivial.

Proof: Let $e \neq g \in A * B$. If $g \in A$ then $g \notin B$, and, by the above theorem, $gBg^{-1} \cap B = E$. So $gb \neq bg$ for any $b \in B$. Hence $g \notin \zeta (A * B)$. Similarly for $g \in B$.

However, if g is neither in A nor in B then also similar conditions like $gAg^{-1} \cap A = E$, $gBg^{-1} \cap B = E$ are satisfied. Hence $g \notin \zeta (A * B)$. Thus the centre of A * B is trivial.

Next we mention, without proof, the most important result about subgroups of a free product.

14.2.8. Theorem (Kurosch Subgroup Theorem):

Let

$$G = \overset{*}{\prod_{\alpha \in I}} G_\alpha$$

be the free product of its subgroups G_α, $\alpha \in I$. Then a subgroup H of G is itself a free product

$$H = F^* \overset{*}{\prod_{x \in G}} (x G_\alpha x^{-1} \cap H)$$

where F is a free group and $\overset{*}{\prod_{x \in G}} (x G_\alpha x^{-1} \cap H)$ is the free product of $x G_\alpha x^{-1} \cap H$, $\alpha \in I$.

(For proof see Theory of Groups by Kurosch Vol. II).

A direct application of the above theorem yields the following result:

14.2.9. Theorem: Let G be the free product of periodic groups A_α, $\alpha \in I$, and H a subgroup of G. Then H is free if and only if it is torsion free.

Proof: Since every free group is torsion free, the condition is necessary.

To prove the sufficiency of the condition, suppose that H is a torsion free subgroup of

$$G = \overset{*}{\prod_{\alpha \in I}} A_\alpha$$

By Kurosch's subgroup theorem,

$$H = F * \overset{*}{\prod_{x \in G}} (x A_\alpha x^{-1} \cap H).$$

where F is a free group and

$$\overset{*}{\prod_{x \in G}} (x A_\alpha x^{-1} \cap H)$$

is the free product of $x A_\alpha x^{-1} \cap H$, $\alpha \in I$. Since H is torsion free,

$$\overset{*}{\prod_{\alpha \in G}} (x A_\alpha x^{-1} \cap H) = E$$

Hence H = F is free.

The situation is different if the condition that the free factors be periodic is removed. In such a case, a torsion free subgroup of a free product need not be free, by corollary 14.2.5, each free factor, although a torsion free subgroup, need not be a free group.

EXERCISES

1. What kind of free groups are commutative and why?

2. If F is a free group of rank n and H is a subgroup of F generated by squares of all elements of F, prove that H is normal in F. Also find the order of F/H. Is F/H abelian?

3. Show that the operation of forming free products of groups is commutative and associative, that is, for groups A, B, C

$$A * B \cong B * A, (A * B) * C \cong A * (B * C)$$

4. Write down two automorphisms of order 2 and 3 of a free group of rank 3.

5. If $G = A * B$ and $N = B^G$, the normal closure of B in G, *i.e.*, the smallest normal subgroup of G containing B, then prove that $G/N \cong A$.

6. Find the rank of the commutator subgroup of the free product of two cyclic groups, one of order 2 and the other of order 3. Can you generalize this to the case of free product of two cyclic groups of order m and n respectively?

7. Using Kurosch's subgroup theorem for free products, prove that every finite subgroup of the free product of finite groups is isomorphic to a subgroup of some free factor.

8. For any two groups A and B, show that A * B is a free group if an only if A and B are free groups.

9. Let A * B be the free product of A and B and [A, B] be the normal subgroup generated by all commutators of the form $[a, b] = aba^{-1}b^{-1}$, $a \in A, b \in B$.

   Show that (A * B) / [A, B] is isomorphic to the direct product $A \times B$ of A and B.

Chapter - XV

SOME OTHER GROUP CONTRUCTIONS

In this chapter we discuss some other constructions of groups. These are the generalized free products of groups, the permutational products of groups and generalized direct products of groups. These are relatively new topics and there are still many unsolved problems concerning the nature and properties of these products.

15.1. GENERALIZED FREE PRODUCTS OF GROUPS

The concept of generalized free product of groups is a generalization of that of the free product of groups. Main contribution to this topic was made by Hanna Neumann, B.H. Neumann and their students. To describe this concept we first define the notion of an amalgam of groups.

An *amalgam* A of (for convenience only) two groups A and B with prescribed subgroups H and K respectively, is a quintuplet (A, B, H, K, φ) where φ is an isomorphism between H and K.

Usually the isomorphism φ is taken as the identity mapping so that H = K is regarded as a subgroup of both A and B. In such a case the amalgam A of A and B with a common subgroup H is an *incomplete group* whose elements are those of A and of B with elements of H as thought of identified in the two groups. The product of two elements of A is defined if and only if they both belong to A or both belong to B, and its value is as in that group. A and B are called the constituents of A and H is called the *amalgamated subgroup*. A is written as

$$A = am (A, B : H)$$

and read as '*the amalgam of A and B with the subgroup H amalgamated.*'

15.1.1. Example:

Let

$$A = < a : a^4 = 1 >$$

$$B = < b : b^6 = 1 >.$$

Suppose that the isomorphic subgroups

$$H_1 = < a^2 : a^4 = 1 >$$

$$H_2 = < b^3 : b^6 = 1 >,$$

both of order 2, are identified so that

$$H = < a^2 : a^4 = 1, a^2 = b^3 >$$

Then the multiplication table for A = am (A, B : H) is

×	1	a	a^2	a^3	b	b^2	b^3	b^4	b^5
1	1	a	a^2	a^3	b	b^2	b^3	b^4	b^5
a	a	$a^2 = b^3$	a^3	1	*	*	a^3	*	*
a^2	$a^2 = b^3$	a^3	1	a	b^4	b^5	1	b	b^2
a^3	a^3	1	a	$a^2 = b^3$	x	*	a	*	*
b	b	*	b^4	*	b^2	b^3	b^4	b^5	1
b^2	b^2	*	b^5	*	b^3	b^4	b^5	1	b
b^3	b^3	a^3	1	a	b^4	b^5	1	b	b^2
b^4	b^4	*	b	*	b^5	1	b	b^2	b^3
b^5	b^5	*	b^2	*	1	b	b^2	b^3	b^4

Recall that a monomorphism of a group A into a group G is said to be an embedding of A in G. If A is embedded in G then G contains a subgroup A′ isomorphic to A.

For the sake of convenience we usually identify A′ with its preimage A and regard A itself as a subgroup of G.

Let A = am (A, B: H). We say that a group G embeds the amalgam A if G contains subgroups A′ and B′ isomorphic to A and B respectively such that $A' \cap B' = H'$ is isomorphic to H.

Again if $\mathbf{A} = \text{am}(A, B : H)$ is embedded in a group G then we identify the subgroups A', B' and H' with A, B and H respectively and regard A, B and H as subgroups of G.

15.1.2. Example:

Let

$$A = \langle a, b : a^2 = b^3 = (ab)^2 = 1 \rangle$$

$$B = \langle c, b : c^2 = b^3 = (cb)^2 = 1 \rangle$$

$$H = \langle b : b^3 = 1 \rangle$$

so that $\mathbf{A} = \text{am}(A, B : H)$. Consider the group G having the presentation:

$$G = \langle a, b, c : a^2 = b^3 = c^2 = (ab)^2 = (cb)^2 = [a, c] = 1 \rangle$$

The group G contains A and B as subgroups and

$$A \cap B = H$$

in G. Hence the amalgam A is embedded in G.

In general there can be many groups which embed a certain amalgam.

For example

$$G_1 = \langle a, b, c : a^2 = b^3 = c^2 = (ab)^2 = (cb)^2 = (ac)^3 = 1 \rangle$$

is another embedding. G is of order 12, whereas G_1 has order 18.

(G_1 is isomorphic to an extension of S_3 by a cyclic group of order 3.)

Among the groups embedding an amalgam there is a 'largest group'. This group is such that every other group which embeds the given amalgam is a homomorphic image of that group. Such a group is known as the *generalized free product of the groups which occur as constituents of an amalgam.*

For the amalgam A described above

$$G^* = \langle a, b, c : a^2 = c^2 = b^3 = (ab)^2 = (bc)^2 = 1 \rangle$$

is such a group, that is, G^* is the generalized free product of A and B amalgamating H.

We now define this concept.

Let $\{G_\alpha : \alpha \in I\}$ be a family of groups and G the free product of G_α, $\alpha \in I$. Suppose that each of the free factors G_α contains a subgroup $H_{\alpha\beta}$ isomorphic to a subgroup $H_{\beta\alpha}$ of G_β.

Let G* be the group obtainable from the free product G by introducing all relations $h_{\alpha\beta} = h_{\beta\alpha}$, $\alpha \neq \beta$, that is, identifying pairs of elements of $H_{\alpha\beta}$ and $H_{\beta\alpha}$ which correspond under some fixed isomorphism between these two subgroups of G_α and G_β respectively. This makes G* a homomorphic image of G in a natural way.

If, in G*, the images of subgroups G_α of G still are isomorphic to G_α for each α and their intersections, in pairs, are precisely (the images of) the subgroups $H_{\alpha\beta} = H_{\beta\alpha}$, then G* is called 'the generalized free product of G_α with amalgamated $H_{\alpha\beta}$'.

We shall write G* as

$$G^* = \langle \Pi^* G_\alpha : H_{\alpha\beta} = H_{\beta\alpha}, \alpha, \beta \in I, \alpha \neq \beta \rangle.$$

Clearly the existence of the generalised free product of an amalgam A implies the embeddability of A in a group namely their generalized free product.

Let A be an amalgam of the groups G_α with amalgamated $H_{\alpha\beta}$, α, $\beta \in I$. Let H_α be the group generated by all $H_{\alpha\beta}$, $\alpha, \beta \in 1$, α fixed., The amalgam A′ formed by the groups H_α with $H_{\alpha\beta}$ amalgamated, is called the '*reduced amalgam*' of the groups G_α, $\alpha \in I$.

A necessary and sufficient condition for the embeddability of the amalgam A is that the reduced amalgam A′ is embeddable (cf. Hanna Heumann [49, 50]).

Apart from this no necessary and sufficient condition for the embeddability of an amalgam is known, not even in the case of an amalgam of three groups.

An amalgam of more than two groups may or may not be embeddable. This is equivalent to saying that the generalized free product of an amalgam of more than two groups need not exist.

15.1.3. Example:

Let

$$A = \langle a, b, c, d : a^2 = b^2 = (ab)^2 = c^2 = d^2 = (cd)^2 = 1$$
$$c^a = d, d^a = c, c^b = d, d^b = c \rangle$$
$$B = \langle a, b, f : a^2 = b^2 = (ab)^2 = f^3 = 1, a^f = ab, b^f = a \rangle,$$
$$C = \langle c, d, f : c^2 = d^2 = (cd)^2 = f^3 = 1, c^f = cd, d^f = c \rangle.$$

Here $g^x = xgx^{-1}$ denotes the conjugate of g by x.

If we write

$$K = \langle a, b : a^2 = b^2 = (ab)^2 = 1 \rangle,$$
$$L = \langle c, d : c^2 = d^2 = (cd)^2 = 1 \rangle,$$
$$M = \langle f : f^3 = 1 \rangle.$$

then A, B and C are split extensions of L by K, K by M and L by M respectively. The amalgam in question is that of A, B and C with their corresponding intersections as

$$A \cap B = K, B \cap C = M, C \cap A = L$$

Take

$$F = \langle a, b, c, d, f : R_1 \cup R_2 \cup R_3 \rangle$$

where R_1, R_2, R_3 are the sets of relations of A, B and C respectively. If the amalgam is embeddable then this group, being the group freely generated by it, must embed it. But in F we have,

$c^a = d$, that is, $acad = 1$.

Therefore,

$$1 = (acad)^f = a^f c^f a^f d^f = ab.cd.ab.c \qquad 15.1.3 \text{ (i)}$$

Since

$$ab.cd.ab = (cd)^{ab} = cd,$$

we have, from 15.1.3 (i)

$$1 = cd.c = d.$$

From $d^f = c$, with $d = 1$, we have $c = 1$, so that, in F, the group C collapses. Consequently F does not embed the amalgam. That is, the generalized free product of this particular amalgam does not exist.

In contrast, an amalgam A = am (A, B : H) of two groups is always embeddable and one such embedding is the generalized free product of A and B amalgamating H. That is, the generalized free products of two groups always exists.

This result is due to Schreier. We omit its proof.

The generalized free product of the groups A and B amalgamating H shall be denoted by:

$$G = (A * B : H)$$

If $G = (A * B : H)$, then the subgroup A' and B' generated by A and B in G are isomorphic to A and B respectively, with $A' \cap B' = H'$ isomorphic to H.

In general the subgroups A', B' and H' will be identified with the groups A, B and H respectively.

Let $A = am (A, B : H)$. A subset $S \subseteq A$ is called a *transversal* of H in A if every element of A is uniquely expressible as

$$a = sh, s \in S, h \in H.$$

A transversal S of H in A is also called a *coset representative of A modulo H.*

For example if

$$A = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$$

and

$$H = \langle b : b^2 = 1 \rangle$$

then

$$S = \{1, a, a^2\}$$

is a transversal of H in A.

In general there can be more than one transversal of H in A. For instance, in group A, $S' = \{b, a, a^2\}$ is another transversal of H.

Let S and T be transversals of H in A and B respectively and G be the free product of A and B amalgamating H. It can be shown (cf: Magnus, Karrass & Solitar [39] or B.H. Neumann [46], [47, [48]) that for an arbitrary choice of the transversals S and T of H in A and B respectively, each $g \in G$ can be uniquely expressed as

$$g = g_1 g_2 \cdots g_k h,\ g_i \in S \text{ or } T \text{ and } h \in H. \qquad 15.1.3\ (1)$$

As before the integer k is then uniquely determined and is called the length of g.

The expression in 15.1.3 (1) is called the *normal form* of g.

The length of an element of A or of B is taken as one.

Two elements having different lengths are always distinct.

As in the case of free products of groups we have the following theorem about elements of finite order in the generalized free product of groups amalgamating a single group. We restrict ourselves to the case involving only two groups

15.1.4. Theorem: Let G = (A * B :H). If g is an element of finite order in G then g is in a conjugate of A or B.

Proof: Let $g \in G$ and be not in a conjugate of A or B. Let

$$g = g_1 g_2 \cdots g_k h$$

be the normal form of g. Then $k \geq 2$ because otherwise g is in A or B. Suppose that g_1, g_k belong to different constituents. Then

$$g^m = g_1 g_2 \cdots g_k h\, g_1 g_2 \cdots g_k h \cdots g_1 g_2 \cdots g_k h$$
$$= g_1 g_2 \cdots (g_k h)\, g_1 g_2 \cdots (g_k h)\, g_1 g_2 \cdots (g_k h)$$

has length $mk > 1$. Thus $g^m \neq e$.

Now Suppose that g_1 and g_k are in the same constituent. Then $k > 2$ for otherwise $g \in$ A or B. Suppose that every element of finite order and of length $< k$ is in a conjugate of A or B. Let

$$g = g_1 g_2 \cdots g_k h,\ k > 2$$

be of finite order. Then

$$g_1^{-1} g g_1 = g_2 \cdots g_k h g_1^{-1}$$
$$= g_2 \cdots g_k' h',\quad g_k h g_1^{-1} = g_k' h'$$

is also of finite order and has length $< k$. So, by induction hypothesis $g_1^{-1} g g_1$ is in a conjugate of A or B. That is, for some $a \in$ A or $b \in$ B, there is an $x \in G$ such that

$$g_1^{-1} g g_1 = xax^{-1} \quad \text{or} \quad g_1^{-1} g g_1 = xbx^{-1}.$$

That is,

$$g = (g_1x)\, a\, (g_1x)^{-1} \quad \text{or} \quad g = (g_1x)\, b\, (g_1x)^{-1}.$$

So g is in a conjugate of A or B, as required.

15.1.5. Corollary: The generalized free product G = (A * B : H) of torsion free groups is torsion Free.

Proof: By the above theorem, an element of finite order in G must be in a conjugate of A or B. But A and B are torsion free and so contain no element of finite order. Hence G has no element of finite order.

The centre of a free group is trivial. The centre of a free product is also trivial as has been shown in Corollary 14.2.7.

However the centre of the generalized free product is not always trivial.

For example,

$$G = \langle a, b : a^4 = b^6 = 1, a^2 = b^3 \rangle$$

is the generalised free product of

$$A = \langle a : a^4 = 1 \rangle,$$

$$B = \langle b : b^6 = 1 \rangle,$$

amalgamating the subgroup

$$H = \langle a^2 = b^3 : a^4 = 1 \rangle.$$

Here the centre of G is H.

The generalized free product of two or more non-trivial groups amalgamating a single sub-group is always infinite.

For instance, if G = (A * B : H) then, for non trivial $a \in A \setminus H$, $b \in B \setminus H$, ab is of infinite order.

However the situation is different for the generalized free product of more than two groups with more than one subgroup amalgamated. That is, the generalized free product of 3 or more groups may by finite.

To substantiate this statement we first make the following observations.

Let K, L, M be groups and A, B, C be the groups generated by K, L ; K, M and L, M respectively. The intersections $K \cap L$, $L \cap M$ and $M \cap K$ play an important role in the discussion of embeddability criteria. A necessary condition for the embeddability of the amalgam of A, B, C is that $K \cap L$, $L \cap M$ and $M \cap K$ are all isomorphic [cf. H. Neumann, [50]. We identify these intersections under the given isomorphism.

In our case we take these intersections to be the identity subgroup.

15.1.6. Theorem: Let $A = < K , L >$, $B = < K , M >$, $C = < L , M >$ with M normal in both B and C. The generalized free product of A, B, C exists if, and only if, there is a homomorphism of A onto the group generated by the automorphisms induced by K and L in M.

Proof: Let K' , L' be the groups generated by the automorphisms induced by K and L in M respectively. Then there exist homomorphisms $\varphi_1 : K \to K'$, $\varphi_2 : L \to L'$. There is an extension homomorphism φ from A to $A' = < K' , L' >$ such that φ coincides with φ_1 on K and with φ_2 on L.

We form the extension G of M by A determined by the homomorphism φ, that is, the group of pairs (a, m), $a \in A$, $m \in M$, where,

$$(a_1, m_1)(a_2, m_2) = (a_1 a_2, m^{\varphi_1(a)} m_2)$$

$a_1, a_2 \in A$, $m_1, m_2 \in M$. We show that this group embeds the amalgam.

Since $\varphi/_K = \varphi_1$, $\varphi/_L = \varphi_2$, in G the subgroups B_1, C_1 consisting of the pairs (k, m), $k \in K$, $m \in M$ and (l, m), $l \in L$, $m \in M$ are isomorphic to B and C respectively and intersect precisely in the group of pairs $(1, m)$, $m \in M$, isomorphic to M. That these groups have the right intersections also with the group A_1 consisting of the pairs $(a, 1)$, $a \in A$, isomorphic to A, is obvious. Thus G embeds the amalgam of A, B, C.

Conversely suppose that the generalized free product F of A, B and C exists. Since M is normalised by K and L, and F is generated by K, L and M, therefore M is normal in F. Moreover $F/M \cong < K, L > = A$ so that F is an extension of M by A. Hence there is a homomorphism of A into the group generated by the automorphisms induced by K and L in M. The proof of the theorem is now complete.

15.1.7. Corollary: The generalized free product of the groups described in Theorem 15.1.6 is finite provided that the groups A, B, C are finite.

Proof: Here the generalized free product is an extension of a finite group M by a finite group A and so is finite.

Whether or not every embeddable amalgam of three or more finite groups is embeddable in a finite group is an open question (cf: B. H. Neumann and Hann Neumann [51]).

Both B. H. Neumann and Hanna Neumann (in a personal latter to the author) conjecture that there exists an embeddable amalgam of three finite groups which is not embeddable in a finite group.

As a particular case of an amalgam of three finite groups, consider the dihedral groups,

$$A = \langle a, b : a^2 = b^2 = (ab)^l = 1 \rangle$$

$$B = \langle b, c : b^2 = c^2 = (bc)^m = 1 \rangle$$

$$C = \langle c, a : c^2 = a^2 = (ca)^n = 1 \rangle.$$

It is known that the generalized free product F of am (A, B, C) exists (cf: Majeed [42]). F has a presentation

$$F = \langle a, b, c : a^2 = b^2 = c^2 = (ab)^l = (bc)^m = (ca)^n = 1 \rangle \quad (*)$$

and is the group of reflections in the sides of a spherical triangle with angles π/l, π/m, π/n; F is known to be finite if $1/l + 1/m + 1/n > 1$ and infinite otherwise.

Put $bc = g$, $ca = h$. Then another presentation of G is

$$F = \langle g, h, c : g^m = h^n = (gh)^l = c^2 = (gc)^2 = (ch)^2 = 1 \rangle.$$

It is easy to see that F is a split extension of

$$P = P(m, n, l) = \langle g, h : g^m = h^n = (gh)^l = 1 \rangle$$

by a cyclic group of order 2.

P belongs to the well-known family of groups called the *polyhedral groups* or the *generalized triangle groups*.

It is not known whether or not, for arbitrary l, m, n, the amalgam am (A, B, C) described above is embeddable in a finite group.

Some questions related to the range and nature of finite embeddings of an amalgam of three finite groups can be found in Majeed [42].

15.2. PERMUTATIONAL PRODUCTS OF GROUPS

The concept of *permutational products* of groups was first introduced by B.H. Neumann [47]. This group theoretic construction is based on a method given by him in his famous essay [46], for the embeddibility of an amalgam, with a single group amalgamated, in a permutation group. Use of this construction was made to answer various questions about embedding theory of group amalgams. We now give a brief description of this construction.

Let A = am (A, B : H) be an amalgam of the groups A and B with the subgroup H amalgamated. We choose transversals S of H in A and T of H in B. Form the set theoretic product

$$K = S \times T \times H.$$

The elements of K are ordered triplets (s, t, h), $s \in S$, $t \in T$ and $h \in H$. For each $a \in A$, we define a mapping $\rho(a) : K \to K$ by:

$$(s', t, h)^{\rho(a)} = (s', t, h')$$

where $s' \in S$, $h' \in H$ are determined by the equation

$$sha = s'h'$$

Similarly, for $b \in B$, we define a mapping $\rho(b) : K \to K$ by

$$(s, t, h)^{\rho(b)} = (s, t', h')$$

where

$$thb = t' h', t' \in T, h' \in H.$$

It is easy to verify that, for $a = b \in H$, no ambiguity arises in the definition of ρ. Moreover the mapping $\rho : A \to \rho(A)$ with $a \to \rho(a)$ for all $a \in A$, is a homomorphism.

For if a, a' are two elements of A, then

$$(s, t, h)^{\rho(a)\rho(a')} = (s', t, h')^{\rho(a')} = (s'', t, h'')$$

where

$$sha = s'h', s'h'a' = s'' h''$$

so that

$$shaa' = s'' h''$$

which means that

$$(s, t, h)^{\rho(aa')} = (s'', t, h'').$$

establishing $\rho(a)$. $\rho(a') = \rho(aa')$. The proof for $\rho(b)\rho(b') = \rho(bb')$ is similar. It, therefore, follows that

$$\rho(A) = \{\rho(a) : a \in A\}$$

$$\rho(B) = \{\rho(b) : b \in B\}$$

are groups. Moreover, the homomorphism $a \to \rho(a)$, $a \in A$ turns out to be an isomorphism, for if $\rho(a) = i_k$, the identity mapping of K, then

$$(s, t, h)^{\rho(a)} = (s, t, h)$$

for all $(s, t, h) \in K$, means that $sha. = sh$ for all $s \in S$, $h \in H$. Therefore $a = e$.

The above remarks show that the mappings $\rho(a)$, $\rho(b)$; $a \in A$, $b \in B$ are in fact permutations of K. Furthermore the intersection of $\rho(A)$ and $\rho(B)$ is $\rho(H)$. For if $\rho(a) \in \rho(B)$ for some $a \in A$, then $\rho(a)$ leaves the first and second component of each triplet (s, t, h) fixed and so

$$(s, t, h)^{\rho(a)} = (s, t, ha).$$

Therefore $ha \in H$, that is, $a \in H$.

The permutation group P of K generated by $\rho(A)$ and $\rho(B)$ contains isomorphic copies of A and B with $\rho(A) \cap \rho(B) = \rho(H)$ isomorphic to H. Therefore P embeds the amalgam A.

The group P is called a *permutational product* of A = am (A, B:H).

We use here the indefinite article because P depends not only on A but also on the choice of transversals S, T of H is A and B respectively.

Thus we shall denote, by P (A : S, T), the permutational product of A corresponding to the transversals S, T of H in A and B respectively.

As mentioned above the isomorphism type of permutational product depends upon the choice of transversals. It was shown by B. H. Neumann [47] that if the amalgamated subgroup is central (i.e. a subgroup of the centre) in one of the constituents then the isomorphism type of the permutational product is independent of the change of transversals in the

other constituent. The following theorem shows that this is also true if the amalgamated subgroup possesses, in one of the constituents, a transversal which it centralizes. The proof follows the line of argument given by B.H.Neumann.

15.2.1. Theorem: Let A = am (A; B : H) and S be a transversal of H in A which is centralised by H. Then the isomorphism type of the permutational product P(A; S, T′) is independent of the choice of transversals T in B.

Proof: Let T and T′ be two distinct transversals of H in B. Let P(A; S,T) and P′(A; S, T′) be permutational product corresponding to the transversals S, T and S, T′ of H, S in A and T, T′ in B. We define a one-one mapping φ from K = S × T × H to K′ = S × T′ × H as follows:

For $(s, t, h) \in K$, we put

$$(s, t, h)^{\varphi} = (s, t', h')$$

where $(s, t', h') \in K'$ and $th = t'h'$. Let $a \in A$. Then, since φ^{-1} exists,

$$\begin{aligned}(s, t', h')^{\varphi^{-1}\rho(a)\varphi} &= (s, t, h)^{\rho(a)\varphi} \\ &= (s_1, t, h_1)\varphi \\ &= (s_1, t', h_2h_1)\end{aligned}$$

where

$$sha = s_1h_1,\ th = t'h',\ th_1 = t'h'_1 = t'h_2h_1 \text{ that is, } t = t'h_2. \qquad 15.2.1\ (1)$$

Also, for $\rho'(a) : K' \to K'$

$$(s, t', h')^{\rho'(a)} = (s_2, t', h'_2)$$

where

$$sh'a = s_2h'_2 \qquad 15.2.1\ (2)$$

Now form $th = t'h'$ we have $t' = th\ h'^{-1}$. Putting it in $t = t'h_2$, we get $t = thh'^{-1}h_2$ so that $hh'^{-1}h_2 = e$. That is $h' = h_2h$. Therefore

$$\begin{aligned}sh'a = sh_2ha &= h_2\ sha, \because \text{H centralizes S} \\ &= h_2s_1h_1, \qquad \text{by 15.2.1 (1)} \\ &= s_1h_2h_1 \\ &= s_2'h_2', \qquad \text{by 15.2.1 (2)}\end{aligned}$$

Therefore $s_1 = s_2'$, $h_2h_1 = h_2'$ and $\varphi^{-1}\rho(a)\ \varphi = \rho'(a)$ for all $a \in A$. For $b \in B$, we have,

$$(s, t', h')^{\varphi^{-1}\rho(b)\varphi} = (s, t, h)^{\rho(b)\varphi}$$
$$= (s, t_1, h_1)^{\varphi}$$
$$= (s, t', h_1')$$

where

$$t'h' = th,\ thb = t_1h_1 = t_1'h_1' \qquad 15.2.1\ (3)$$

and

$$(s, t', h')^{\rho'(b)} = (s, t_2', h_2')$$

with

$$t'h'b = t_2'h_2' \qquad 15.3.1\ (4)$$

Since $th = t'h'$, we have,

$$thb = t'h'b = t_1'h_1'$$
$$= t_2'h_2'$$

by (3) and (4) respectively. Hence

$t_1' = t_2'$ and $h_1' = h_2'$ so that $\varphi^{-1}\ \rho(b)\varphi = \rho'(b)$ for all $b \in B$. Thus $\varphi^{-1}\ P\varphi = P'$. P and P′ are isomorphic, as required.

15.2.2. Corollary: If H is a direct factor in A then the isomorphism type of the permutational product is independent of the change of transversals in B.

Proof: This is immediate. Choose a complementary direct factor as a transversal.

15.2.3. Corollary: If H is central in both A and B, then the iosmorphism type of the permutational product is uniquely determined.

Proof: Obvious.

Keeping in view the effect of change of transversals when H is not central in both the constituents and the above corollary, one may, quite naturally, ask whether, in all other cases excepting the one mentioned above, that is, of H being central in both the constituents, permutational

product of A and B depends upon the choice of transversals of the amalgamated subgroup. That this is not the case is shown by the following example constructed by B.H. Neumann [46], in a different context.

15.2.4. Example:

Let

$$H = \langle h_0, h_1, h_2, \ldots : h_1^2 = [h_i, h_j] = 1, i, j, = 0, 1, 2, \ldots \rangle,$$

be the restricted direct product of (countably) infinite copies of cyclic group of order 2. Take

$$A = \langle a, H ; a^2 = h_i^2 = [h_i, h_j] = 1, h_{2i}^{a} = h_{2i+1}, h_{2i+1}^{a} = h_{2i} \ (i, j = 0, 1, 2, \ldots) \rangle$$

$$B = \langle b, H : b^2 = h_i^2 = [h_i, h_j] = 1, h_0^{b} = h_0, h_{2i+1}^{b} = h_{2i+1}, h_{2i+2}^{b} = h_{2i+2},$$

$$(i, j = 0, 1, 2, \ldots) \rangle$$

Let P be a permutational product of A and B amalgamating H. Then, in P, the element *ab* is of infinite order because, for any non-zero positive integer n,

$$h_0^{(ab)^n} = h_0^{(ab)(ab)^{n-1}} = h_1^{b(ab)^{n-1}} = h_2^{(ab)^{n-1}} = \ldots = h_{2n} \neq h_0.$$

If F is the free product of A and B amalgamating H then, by definition of the free product, there is a homomorphism of F onto P. To show that F and P are isomorphic it is enough to prove that it is impossible to add an additional relation in F different form those already implied by the relations of A and B, without making any of the groups collapse.

In F, every element can be expressed uniquely as

$$r = ha^{\epsilon_1} bab \ldots ab^{\epsilon_2}$$

$\epsilon_i = 0$ or 1, i = 1, 2, and $h \in H$. Hence a relation $r = 1$ gives

$$h = a^{\epsilon_1} b \, abad \ldots ab^{\epsilon_2}$$

If the right hand side is equal to 1 then this is a relation in H; hence we assume it to be different from 1. Then ϵ_1, ϵ_2 cannot be simultaneously 1 or 0. For the right hand side in such a situation becomes $(ab)^m$ or $(ba)^{m+1}$ for some integer m according as $\epsilon_1 = \epsilon_2 = 1$ or $\epsilon_1 = \epsilon_2 = 0$ and both *ab* and *ba* are elements of infinite order in P whereas h is of order 2. Thus

either $\in_1$ or $\in_2$ is zero. Without any loss of generality we can suppose that $\in_2 = 0$. Then $\in_1 = 1$ and

$$h = ab\ ab\ ...\ aba \qquad 15.2.4\ (*)$$

The number of factors ab preceding the last a on the right hand side of 15.2.4 (*) is either even or odd so that

$$h = gag^{-1} \quad \text{or} \quad gbg^{-1}$$

where $g = (ab)^k$ or $(ab)_a^k$ according as the number of factors ab in (*) is even or odd. Here $g \in < a, b >$. Since H is normal in A and B, H is normal in F so that either $a = g^{-1} hg \in H$ or $b = g^{-1} hg \in H$. but this is impossible because it leads to the collapse of the amalgam of A and B. Thus no proper homomorphic image of F embeds the amalgam of A and B. Since a permutaional product P of A and B amalgamating H also embeds this amalgam, P and F are isomorphic. Thus there is unique *permutaional product* of A and B amalgamating H.

Remarks: Both A and B, being extensions of a solvable group by a solvable group, are solvable. Also F is a split extension of H, a solvable group, by the infinite dihedral group, again a solvable group. So F is solvable. Thus the *generalised free product of two solvable groups can be solvable.*

Can the generalized free product of two solvable groups different from those given in example in 15.2.4 be solvable?

This problem is still unsolved.

15.3. GENERALIZED DIRECT PRODUCTS OF GROUPS

The concept of generalized direct product was first introduced by B.H. Neumann and Hanna Neuamnn who proved an existence theorem for such products [(46)]. Different existence theorems of such products for given amalgams of groups have been discussed in the literature [62]. We now briefly describe this type of product.

A group G is said to be the *generalized direct product* of its subgroups $G_1, G_2, ..., G_n$ amalgamating a subgroup H if

(i) G is generated by $G_1, G_2, ..., G_n$;

(ii) G_i, G_j are elementwise permutable for all i, j, $i \neq j$, i, j, = 1, 2, ..., n;

(iii) $G_i \cap < G_j : j \neq i > = H$, i, j = 1, 2, ..., n.

G is then denoted by:

$$G = (G_1 \times G_2 \times ... \times G_n)_H. \qquad 15.3\ (*)$$

The subgroups G_i, $i = 1, 2, ..., n$, are called the *generalized direct factors* of G.

It may be noted that the subgroup H must be contained in the centre of G_i, $i = 1, 2, ..., n$ and her a also of G.

If $H = \{e\}$ then we have G as the usual direct product of G_i: $i = 1, 2, ..., n$.

Moreover the factor group G/H can be written as

$$G/H = G_1/H \times G_2/H \times .... \times G_n/H,$$

the direct product of the direct factors G_i/H , $i = 1, 2, ..., n$.

If G cannot the written as in 15.3 (*) then G is said to be indecomposable as the generalized direct product of its subgroups.

15.3.1. Examples:

(1) Let

$$A = < a : a^4 = 1 >, B = < b : b^4 = 1 >$$

and

$$H = < a^2 = b^2 >.$$

Then

$$G = < a, b, : a^4 = b^4 = [a, b] = 1, a^2 = b^2 >$$

is the generalized direct product of A and B amalgamating H.

If

$$D_4 = < a, b : a^4 = b^2 = (ab)^2 = 1 >,$$

$$D_4^* = < c, d : c^4 = d^2 = (cd)^2 = 1 > \cong D_4$$

and

$$H = < a^2 = c^2 >,$$

and

$$H = < a^2 = c^2 >,$$

then

$$G_1 = < a, b, c, d : a^4 = b^2 = (ab)^2 = c^4 = d^2 = (cd)^2 = [a, c] = [a, d] = [b, c] = [b, d] = 1, a^2 = c^2 >$$

is the generalized direct product of D_4 and D_4 amalgamating H.

Take

$$Q = < a, b : a^4 = 1, a^2 = b^2, ab = ba^{-1} >$$

$$D_4 = < c, d : c^4 = d^2 = (cd)^2 = 1 >$$

and

$$H = < a^2 = c^2 >.$$

Then

$$G_2 = < a, b, c, d : a^4 = c^4 = d^2 = (cd)^2 = [a, c] = [a, d] = [b, c] = [b, d] = 1, ab = ba^{-1}, a^2 = b^2 = c^2 > = (Q \times D_4)_H$$

is the generalised direct product of Q and D_4 amalgamating H.

One can similarly have

$$G_3 = (Q \times Q)_H.$$

where Q is the quaternion group of order 8 and H the centre of Q.

The group G_1, G_2 and G_3 all have order 32.

The following problem has been discussed by C.Y. Tang [62]. *"Given a group G, do there exist subgroups A and B in G with $A \cap B = H$ such that G is the a generalized direct of A and B amalgamating H? Also, are the subgroups A and B uniquely determined?"*

It is worth mentioning that the generalized direct products

$$(D_4 \times D_4)_H \text{ and } (Q \times Q)_H$$

when H is the central subgroup of D_4 and Q, are isomorphic. However $(D_4 \times Q)_H$ is not isomorphic to $(D_4 \times D_4)_H$ (or $(Q \times Q)_H$).

15.4. CARTESIAN PRODUCTS OF GROUPS

In chapter 6 we defined the direct product of a finite number of groups. Here we generalize the notion to one involving an infinite number of factors. In this situation we obtain two types of products one of which will be called the *'Cartesian product.'*

Let $\{G_\alpha : \alpha \in \Omega\}$ be a family of groups indexed by a set Ω.

Consider the set C of all functions

$$f : \Omega \to \bigcup_{\alpha \in \Omega} G_\alpha$$

such that $f(\alpha) \in G_\alpha$ for all $\alpha \in \Omega$.

We define the group operations in C as follows:

For $f, g \in C$, we put

$$(fg)(\alpha) = f(\alpha) \cdot g(\alpha) \qquad 15.4\ (1)$$

and

$$f^{-1}(\alpha) = (f(\alpha))^{-1}, \qquad 15.4\ (2)$$

for all $\alpha \in \Omega$. It is easy to verify that, under the multiplication and inversion defined by 15.4 (1) and 15.4 (2), C is a group.

The unit element in C is the mapping $e : \Omega \to \bigcup_{\alpha \in \Omega} G_\alpha$ such that $e(\alpha) = 1$, the identity of G_α for all $\alpha \in \Omega$.

C is called the *Cartesian product* of G_α, $\alpha \in \Omega$.

For any $f \in C$, we define the *support* $\sigma(f)$ *of* f by:

$$\sigma(f) = \{\alpha \in \Omega : f(\alpha) \neq 1\}.$$

(Only the unit element of C has empty support).

Take a fixed $\alpha \in \Omega$ and let H_α be the set of those functions f in C for which

$$\sigma(f) \subseteq \{\alpha\}.$$

For any $f, g \in H_\alpha : f \neq g$,

$$\sigma(fg^{-1}) \subseteq \{\alpha\}$$

so that $fg^{-1} \in H_\alpha$. Hence H_α is a subgroup of C and is, in fact, isomorphic to G_α under the mapping $f \to a_f$ where $f(\alpha) = a_f \in G_\alpha$.

H_α is called the *component* or *coordinate subgroup* of C.

It is often convenient to identify H_α with G_α. Then the subgroup of C generated by all the component subgroups G_α, $\alpha \in \Omega$, consists of all functions with finite support. This group is known as the (*restricted*) *direct product* of the family $\{G_\alpha : \alpha \in \Omega\}$ while C itself is called the *unrestricted direct product* or the Cartesian product.

The direct and Cartesian products coincide if the index set is finite. If Ω and each G_α, $\alpha \in \Omega$ are countable then the (restricted) direct product of G_α is countable. However, this is not true in the case of Cartesian product of an infinite family of groups G_α.

Thus the Cartesian product of non-trivial G_α, $\alpha \in \Omega$, with Ω infinite, has order the cardinal of the continuum even if the order of each G_α is no larger than 2.

We also have a special case of the above construction. In this case all the G_α are isomorphic to a single group G and the corresponding Cartesian product is denoted by G^Ω and is called the Ω-th *Cartesian power* of G. Thus G^Ω consists of all functions $f : \Omega \to G$ with multiplication and inversion defined by:

$$(fg)(\alpha) = f(\alpha) \cdot g(\alpha), f^{-1}(\alpha) = (f(\alpha))^{-1}.$$

For any $\alpha \in \Omega$, the component group

$$H_\alpha = \{f \in G^\Omega, \sigma(f) \subseteq \{\alpha\}\}$$

is isomorphic to G. The subgroups H_α, $\alpha \in \Omega$ generate the *direct power* $G^{(\Omega)}$ of G and consists of all functions from Ω to G having finite support.

Both G^Ω and $G^{(\Omega)}$ are different unless Ω is finite or G is the trivial group.

It is known that the center of a direct product is the direct product of the centers of the factors. It is an unsolved problem whether the center of the Cartesian product is the Cartesian product of the centers of the constituents of the Cartesian product.

15.5. WREATH PRODUCT OF GROUPS

In this section we discuss another important group construction called wreath product of groups. This concept has proved to be a principal tool in the solution of many interesting problems in Group Theory. We shall see that a wreath product of two groups A and B is a semi-direct product of the group A^B by the group B.

For arbitrary non-trivial groups A and B we denote by A^B the $|B|$-th Cartesian power of A. A^B consists of all functions f: $B \to A$ with multiplication and inversion defined by:

$$(fg)(b) = f(b)\, g(b) \ , \ f^{-1}(b) = (f(b))^{-1}$$

for all $f, g \in A^B$ and $b \in B$.

As seen in the previous section A^B is a group.

Let a be an arbitrary but fixed element of A. For any $b \in B$, consider the function $\alpha_b : B \to A$ defined by

$$\alpha_b(b) = a \text{ and } \alpha_b(x) = 1 \qquad 15.5(1)$$

for all $x \in B$, $x \neq b$. If b is now fixed and a is allowed to vary over A, then the set A_b of all functions α_b, α'_b, α''_b, ... defined by equations like in 15.5(1) is a subgroup of A^B. Here, for α_b and α'_b in A_b and defined by

$$\alpha'(b)\,(b) = a', \ \alpha'_b(x) = 1$$

for all $x \in B$, $x \neq b$, $a' \in A$, we have,

$$(\alpha'_b \alpha^{-1}_b(b)) = \alpha'_b\,(b).\ \alpha^{-1}_b\,(b)$$

$$= a'\, a^{-1}$$

while

$$(\alpha'_b \alpha^{-1}{}_b)(x) = \alpha'_b(x)\ .\ \alpha^{-1}{}_b(x) = 1, x \neq b,$$

for all $x \in B$. Hence $\alpha'_b \alpha^{-1}{}_b \in A_b$.

The subgroup A_b is called the *coordinate or component subgroup* of A^B. Clearly A_b is isomorphic to A under the mapping defined by

$$\alpha_b \to a, \ \alpha'_b \to a', \ldots .$$

Also, for a fixed $a \in A$, the set A* of all functions $\alpha_a^* : B \to A$ defined by

$$\alpha_a^*(b) = a \qquad 15.5\ (2)$$

for all $b \in B$, is a subgroup of A^B. Here, for $\alpha_1^*, \alpha_2^* \in A^*$ with

$$\alpha_1^*(b) = a_1,\ \alpha_2^*(b) = a_2$$

for all $b \in B$, we have,

$$(\alpha_1^* \alpha_2^{*-1})(b) = \alpha_1^*(b).\ \alpha_2^{*-1}(b)$$
$$= a_1 a_2^{-1} \in A.$$

Hence $\alpha_1^* \alpha_2^{*-1} \in A^*$. (We have written α_1^*, α_2^* for $\alpha_{a_1}^*, \alpha_{a_2}^*$).

The subgroup A* also is isomorphic to A, the mapping $\alpha_a^* \to a$ being an isomorphism.

A* is called the *diagonal subgroup* of A^B.

Next we turn B into a group of automorphisms of A^B as follows. For each $b \in B$ and any $f \in A^B$ we define the *action* of b on f by:

$$f^b(y) = f(yb^{-1}), \text{ for all } y \in B. \qquad 15.5(3)$$

It is easily verifiable that $\varphi_b : A^B \to A^B$ given by $\varphi_b(f) = f^b$, defines an automorphism of A^B. The set

$$\Phi_B = \{\varphi_b : b \in B\}$$

is a group of automorphisms of A^B and is isomorphic to B under the isomorphism given by $\varphi_b \to b$.

Thus we have the following equations:

$$(fg)^b = f^b g^b \qquad 15.5(4)$$
$$(f)^{(b_1 b_2)} = f^{b1}\ .\ f^{b2} \qquad 15.5(5)$$

for all $f, g \in A^B$ and $b, b_1, b_2 \in B$.

For example, 15.5 (4) follows from

$$(fg)^b(y) = (fg)(yb^{-1})$$

$$= f(yb^{-1}) \cdot g(yb^{-1})$$
$$= f^b(y) \cdot g^b(y)$$
$$= (f^b \cdot g^b)(y)$$

for all $y \in B$ while 15.5 (5) is verified as follows:

$$f^{b_1 b_2}(y) = f(y(b_1 b_2)^{-1})$$
$$= f((yb_2^{-1})b_1^{-1})$$
$$= f^{b_1}(yb_2^{-1})$$
$$= (f^{b_1})(f^{b_2}(y))$$
$$= (f^{b_1} f^{b_2})(y)$$

for all $y \in B$.

Because of the isomorphism between Φ_B and B we identify, for each $b \in B$, the corresponding elements φ_b and b in Φ_B and B respectively. So B itself can be regarded as a group of automorphisms of A^B.

Consider now the set P of all formal products of the form:

$$f \cdot b,$$

$f \in A^B$, $b \in B$, with multiplication defined by:

$$f \cdot b \cdot f' \cdot b' = ff'^b \cdot bb' \qquad 15.5(6)$$

In terms of this multiplication the action of elements of B on elements of A^B becomes the transformation

$$f^b = bfb^{-1}.$$

P is a group under the multiplication defined by 15.5 (6), the inverse of each f^b being $(f^{b^{-1}})^{-1} \cdot b^{-1}$

The group P is called the standard *understricted (or complete) wreath product* of A by B and is denoted by

$$A \text{ Wr } B.$$

AWr B is thus the semi-direct product of A^B by B, as defined in 7.6.1.

The subgroup A^B of AWr B is called the *base group*.

The direct power $A^{(B)}$ is easily seen to admit the action of B defined by 15.5 (3). We can, therefore, also form the semi-direct product Q of $A^{(B)}$ by B. Q is called the *standard restricted wreath product* of A by B, and is denoted by

$$A \text{ wr } B.$$

If B is finite then both the unrestricted and restricted wreath products coincide.

15.5.1. Example:

Let

$$A = \langle a : a^2 = 1 \rangle, B = \langle b : b^2 = 1 \rangle.$$

Then $A^B \cong V_4$ and A wr B = D_4, the dihedral group of order 8.

Next we consider a generalization of the standard wreath product of the *non-standard* wreath product as follows:

We take B as a permutation group on an arbitrary set Y and then the semi-direct product of A^Y and B, in the unrestricted case, and of $A^{(Y)}$ and B in the restricted case.

The corresponding wreath products are called the *non-standard unrestricted and non-standard restricted wreath products respectively.*

Suppose now that A also is a permutation group on a set X while B is a permutation group on a set Y. Then the wreath product, which is the semi-direct product of A^Y (or $A^{(Y)}$) by B under the action of B on A^Y (or $A^{(Y)}$) defined by 15.5 (3) has a natural permutation representation on the product set $X \times Y$ as follows:

For any $(x, y) \in X \times Y$ and $f^b \in$ A Wr B (or A wr B), we write

$$(x, y)f^b = (x^{f(y)}, y^b) \qquad 15.5\ (7)$$

where $x^{f(y)}$ and y^b denote the images of x and y under $f(y)$ and b respectively.

It is then easy to verify that this *permutational wreath multiplication* is associative. Indeed, if C is a third permutation group on a set Z, than

$$A \text{ Wr } (B \text{ Wr } C) = (A \text{ Wr } B) \text{ Wr } C$$

and, as permutation groups of

$$X \times (Y \times Z), (X \times Y) \times Z,$$

they are not only isomorphic but even identical. The same is true for restricted wreath product.

Standard wreath multiplication, however, is not associative.

For example, take A, B and C all of order 2. Then A wr B and B wr C both have order 8 while

A wr (B wr C) and (A wr B) wr C

have orders $2^8 \cdot 2^3 = 2^{11}$ and $8^2 \times 2 = 2^7$ respectively and hence are not isomorphic.

One of the many uses of the wreath product was given by B.H. Neumann and Hanna Neumann in 1959 to prove the following important embedding theorem:

Every countable group can be embedded in a two generator group.

In fact if G is a countable group and is embedded in a two generator group Q generated by a and b then we can impose conditions on the generators of Q.

It has been proved by Frank Levin in 1968 that the orders of a and b can be taken as 2 and 3 respectively.

EXERCISES

1. Find the permutational product of A = am (A, B : H) where

   $A = < a, b : a^4 = b^2 = (ab)^2 = 1 >$

   $B = < a, c : a^4 = c^2 = (ac)^2 = 1 >$

   $H = < a : a^4 = 1 >$

   $S = \{1, b\}, T = \{1, c\}$

   Also find its order.

2. If $A = <a, b : a^4 = b^2 = (ab)^2 = 1 >$, $B = < c, d : c^4 = d^2 = (cd)^2 = 1>$ and $H = < a^2 = c^2 >$. Find all the permutational products of am (A, B : H).

3. Show that every permutational product of a finite amalgam am(A, B : H) is finite. Hence show that every finite amalgam of two groups is embeddable in a finite group.

4. Let **A** = am(A, B : H). If H is central in both the constituents A and B, then show that there is a unique permutational product P (**A** ; S, T) which is the generalized direct product of A and B amalgamating H.

5. Let G be the generalized free product of two groups A and B amalgamating H. Let N be a normal subgroup of G such that

$$A \cap N = \{1\}, B \cap N = \{1\}$$

Show that N is a free group and G/N embeds am(A, B : H).

(Hint : Use theorem 15.0 on the structure of subgroups of a generalized free products in [49].

6.*** (Unsolved Problems). Can the Frattini subgroup of a generalized free product be larger than the amalgamated subgroup? Do such groups necessarily have maximal subgroups. [cf. Higman, Neumann & Neumann, J. London Math. Soc. 29, 94-88 (1954)].

7.*** (Unsolved Problem). Can the generalized free product of two solvable group be simple when the amalgamated subgroup is not central in either?

Chapter - XVI

LINEAR GROUPS

Linear groups are important from the point of view of their application in physics and other sciences. They are easy to deal with in the sense that many of their properties can be discussed by ordinary computation. They have been found useful in giving counter examples to answer various group theoretical conjectures. In the present chapter we give a brief description of linear groups and discuss some of the elementary but salient features of this beautiful branch of group theory.

16.1. THE GENERAL LINEAR GROUP

Let V be a vector space of dimension n over a field F. The set $\text{Hom}_F(V, V)$ of all linear transformations of V is a linear associative algebra. $\text{Hom}_F(V, V)$ has both the vector space and ring structures. The identity mapping I of V is the multiplicative identity of $\text{Hom}_F(V, V)$.

An element φ of $\text{Hom}_F(V, V)$ is said to be invertible if there is a mapping ψ in $\text{Hom}_F(V, V)$ such that

$$\varphi\psi = \psi\varphi = I.$$

The set of all invertible elements of $\text{Hom}_F(V, V)$ forms a group.

If V has dimension n then this group is denoted by $GL_n(V)$ and *is called the general linear group of degree (or dimension) n.*

Closely related with $\text{Hom}_F(V, V)$ is the set $M_n(F)$ of all $n \times n$ matrices with entries from F. Both $\text{Hom}_F(V, V)$ and $M_n(F)$ are isomorphic as linear associative algebras. In $M_n(F)$, those matrices which have non-zero determinant (such matrices are also called *non-singular* or *invertible*) form a group under multiplication. This group is denoted by GL(n, F) and is isomorphic to $GL_n(V)$. GL(n, F) also is called the *general linear group of dimension* n.

In general, if R is a ring with identity and M_n (R) is the ring of all $n \times n$ matrices with entries from R then the units of M_n (R), that is, those matrices which are invertible, form a group GL (n, R) which also is called the *general linear group of dimension n over R.*

Among the subgroups of GL(n, F) there are some which are very important and need special consideration. One of these is the *special linear group* SL(n, F) of dimension n. It consists of those matrices in GL(n, F) which have determinant 1, the multiplicative identity of F.

Since, for any $P \in GL(n, F)$ and $Q \in SL(n, F)$,

$$\begin{aligned} \det (PQP^{-1}) &= \det P \det Q (\det P)^{-1} \\ &= \det Q \\ &= 1 \end{aligned}$$

so $PQP^{-1} \in SL(n, F)$. Hence SL(n, F) is a normal subgroup of GL(n, F).

Another subgroup of GL(n, F) is the group TL(n, F) of all $n \times n$ (upper) triangular matrices $A = (a_{ij})$, $a_{ij} = 0$ for all $i > j$. Such matrices can be written as

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

In TL(n, F), those matrices whose determinant is 1, the multiplicative identity of F, form a subgroup STL(n, F). This group is known as the *special (upper) triangular group* and is normal in TL (n, F).

A *diagonal matrix* in GL(n, F) is a matrix of the form

$$A = (\delta_{ij}\, a_{ij}),\ 0 \neq a_{ij} \in F.$$

Here δ_{ij} is the Kronecker delta, that is, $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ii} = 1$.

The diagonal matrices in GL(n, F) form a subgroup, called the *diagonal subgroup* of GL(n, F). It is denoted by Diag (n, F). Among the diagonal matrices there are matrices of the form $A = (a\, \delta_{ij}) = a\, I$, $0 \neq a \in F$, and I is the $n \times n$ identity matrix. Such matrices are known as *scalar matrices*. The scalar matrices also form a subgroup of GL(n, F); This subgroup is abelian and constitutes the centre of GL(n, F).

The algebraic operation in all these subgroups is matrix multiplication.

The factor group of SL(n, F) by its centre $\{\pm I\}$ is called the *projective special linear* group and is denoted by PSL(n, F). Except for a few cases, PSL(n, F) is a simple group.

A matrix $A \in GL(n, F)$ is said to be *monomial* if A has exactly one non-zero entry from F in each row and each column.

It is clear that all such matrices from a group Mon (n, F) under the usual multiplication of matrices. Since every diagonal matrix is monomial, so Diag (n, F) is a subgroup of Mon (n, F) and is, in fact, a normal subgroup of Mon (n, F).

A monomial matrix in which every non-zero entry is $1 \in F$, is called a *permutation matrix.* Permutation matrices in M_n (n, F) form a group Perm (n, F) which is a subgroup of Mon (n, F).

In fact, every monomial matrix is uniquely expressible as a product of a diagonal matrix and a permutation matrix.

Hence

$$\text{Mon } (n, F) = \text{Diag } (n, F).\ \text{Per } (n, F)$$

Moreover

$$\text{Diag } (n, F) \cap \text{Perm } (n, F) = \{I\}.$$

For a vector space V of dimension n over a field F and a fixed basis $v_1, v_2, \ldots, v_n$ of V, the mapping $\varphi: V \to V$ given by

$$\varphi(v) = \varphi\left(\sum_{i=1}^{n} a_i v_i\right) = \sum_{i=1}^{n} a_i v_{\sigma(i)}$$

where $\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$ is a permutation, $\varphi(v_i) = v_{\sigma(i)}$, i =1, 2, ..., n, is a linear transformation of V.

Restricted to $\{v_1, v_2, \ldots, v_n\}$, φ is just the permutation $\sigma = \begin{pmatrix} i \\ \sigma(i) \end{pmatrix}$ of $v_1, v_2, \ldots, v_n$.

The matrix φ_σ associated with φ is simply the permutation matrix with 1 at the $[i, \sigma(i)]$th place and zeroes elsewhere, i = 1, 2, ..., n.

Therefore, corresponding to each such matrix, there is a permutation $\begin{pmatrix} i \\ \sigma(i) \end{pmatrix}$ of the basis $v_1, v_2, \ldots, v_n$ and conversely.

There is thus a one-one correspondence between Perm (n, F) and the group S_n of all permutations of degree n.

This correspondence is, in fact, an isomorphism between these groups.

Note that, here, we have written the image of i under σ as $\sigma(i)$ instead of $(i)\sigma$ as mentioned in chapter 8.

16.2. REPRESENTATIONS OF GROUPS

Finite groups are easy to handle if these are expressed as groups of matrices. Representation Theory of groups is an important technique to express finite groups as such. Representing groups as groups of matrices helps us in making applications of finite groups to crystallography, physics and to geometry. In this section we discuss this theory and some of its properties.

A subgroup of GL_n (V) is called a *linear group* of dimension n over F. A subgroup of GL (n, F) is called a *matrix group* of dimension (or degree) n over F.

Because of the isomorphism between GL_n (V) and GL (n, F) we shall call a matrix group also a linear group.

Let G be an abstract group. A homomorphism ρ of G into GL(n, F) is said to be a matrix *representation* of G of degree n over F.

Thus a mapping P : G $\rightarrow$ GL(n, F) is said to a matrix representation of G if

$$\rho(g_1g_2) = \rho(g_1)\,\rho(g_2), \text{ for all } g_1, g_2 \in G.$$

With each $g \in$ G, ρ associates an n $\times$ n matrix $\rho(g) = (g_{ij})$, say, $g_{ij} \in$ F.

Let G* be the subgroup of GL (n, F) generated by all $\rho(g)$, $g \in$ G. Then ρ : G $\rightarrow$ G* is an epimorphism.

The representation ρ is said to be *faithful* if Ker $\rho = \{e\}$, e the identity of G.

Here

$$\text{Ker } \rho = \{g \in G : \rho(g) = I, \text{ the identity matrix}\}.$$

Likewise, a homomorphism v : G $\rightarrow$ GL_n (V) is called a *linear* representation of G.

V is called the *representative space and the dimension of V is called the dimension of the representation.*

Thus a mapping $\rho : G \to GL(n, F)$ is said to a (matrix) representation of G if

$$\rho(g_1 g_2) = \rho(g_1)\,\rho(g_2). \text{ for all } g_1, g_2 \in G.$$

In the general case we also consider representations of G over an arbitrary ring R. These are homomorphisms of G into the group GL (n, R) of all n × n invertible matrices over R. We then have the following special cases:

1. If R = F is a field of characteristic zero, then the representations over R are called *ordinary representations.*
2. If $R = F_p$ is a field of characteristic $p \neq 0$, and if p divides the order of the group then the theory of representations over F_p is called *modular representation theory* (or Braüer theory). This theory leads to the application of finite group theory to crystallography and to geometry.
3. Representations over integral domains are called *integral representations.*

Although some basic definition and other concepts of the above mentioned types of representations are similar, in detail these are quite different.

16.2.1 Example:

(i) Let

$$G = \langle a, b : a^2 = b^2 = 1 \rangle$$

be the infinite dihedral group. The mapping

$$a \xrightarrow{\rho} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, b \xrightarrow{\rho} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

of generators of G into the generators x, y of

$$G^* = \langle x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, y = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \rangle$$

can be extended to a homomorphism, also denoted by ρ, of G onto G* so that ρ is a 2-dimensional representation of G.

ρ is, of course, faithful.

(ii) Consider the symmetric group G of degree 3 given as

$$G = \langle a, b : a^3 = b^2 = (ab)^2 = 1,$$

and the group of matrices

$$G_1^* = \langle x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, y = \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, w^3 = 1 \rangle.$$

Then the mapping

$$a \xrightarrow{\rho} \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, b \xrightarrow{\rho} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

can be extended to a homomorphism, also denoted by ρ, of G onto G_1^*.

In this case also ρ is faithful.

(iii) Let G be a free group of rank 2 with free generators a and b. Then the mapping

$$a \xrightarrow{\rho} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, b \xrightarrow{\rho} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

can be extended to a homomorphism, again denoted by ρ, of G onto

$$G_2^* = \langle x = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \rangle.$$

It is well known that G_2^* is a free group of rank 2 (cf. [(15a)]). So G_2^* and G are isomorphic and ρ is a faithful representation. Also the mapping

$$a \xrightarrow{\rho'} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, b \xrightarrow{\rho'} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

of the generators of G into

$$G_3^* = \langle x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \rangle$$

can be extended to a homomorphism of G onto G_3^*.

(Both G and G_3^* are two generator groups and G is free).

But the representation ρ', in this case, is not faithful, because G_3^* is not free of rank 2. In fact, G_3^* is the unimodular group and

$$(xy)^3 = -I = (yx)^3.$$

So G_3^* is not isomorphic to G. This representation is not faithful.

Two representations ρ and ρ' of a group G into GL (n, F) are said to be *equivalent* if there exists a matrix P in GL (n, F) such that

$$\rho'(x) = P\,\rho(x)\,P^{-1}$$

for all $x \in G$.

It is easy to verify that the *relation of equivalence among the representations of a group G is an equivalence relation.*

For a vector space V of dimension n over a field F, let G be a subgroup of $GL_n(V)$. A subspace W of V is said to be *G-invariant* (or invariant under G) if

$$g(W) \subseteq W$$

for all $g \in G$. Clearly the null space $\{0\}$ and the vector space V itself are G-invariant.

A two dimensional representation of the group $(R, +)$, reals under addition, is given by:

$$\rho : r \longrightarrow \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, r \in R,$$

and the subspace generated by $(1, 0)^T$ is invariant under ρ.

A group $G \subseteq GL_n(V)$ (equivalently, a representation ρ of G) is said to be *irreducible* if the only subspaces of V which are G-invariant are the null space $\{0\}$ and the space V.

Otherwise G is said to be *reducible.*

Thus G (or the representation ρ of G) is irreducible if and only if V has no non-trivial G-invariant subspace.

G is said to be *completely reducible* if there are G-invariant subspaces $W_1, W_2, \ldots, W_m$, $1 \leq m \leq n$, such that V is the direct sum of $W_1, W_2, \ldots, W_m$.

From this definition if follows that every irreducible group is completely reducible.

Here take m = 1.

A group $G \subseteq GL_n(V)$ is said to be *decomposable* if there exist non-trivial G-invariant subspaces U and W such that

$$V = U \oplus W$$

Let ρ be a representation of a group G into $GL_n(V)$. Let W be a G-invariant subspaces of V. Then each $g \in G$ induces linear

transformations g_1, to be denoted by $g/_W$, and $\overline{g}$ on W and the quotient space V/W respectively. These are defined as follows;

For any $w \in W$, $gw \in W$ and $\overline{g}(v + W) = gv + W \in V/W$.

If dimensions of W and V/W are m and k respectively then $k + m = n$.

The mappings

$$\varphi : G \to GL_m(W),\ \psi : G \to GL_k(V/W)$$

given by

$$\varphi(g) = g/_W \text{ and } \psi(g) = \overline{g}$$

respectively are homomorphisms of G. So, both φ and ψ is are also representations of G.

The representation ψ is called the *factor representation* of ρ on the quotient space V/W.

G is said to be *indecomposable* if no such pair of non-trivial G-invariant subspaces of V exists.

The same definitions apply to the subgroups of GL (n, F).

A (linear or matrix) representation ρ of a group G is said to reducible, irreducible, decomposable, indecomposable or completely reducible if and only if ρ (G) is reducible, irreducible, decomposable, indecomposable or completely reducible as a subgroup of GL_n (V) or GL (n, F).

A representation $\rho : G \longrightarrow GL_n(V)$ is said to be a trivial representation if

$\rho(G) = I$, the identity mapping of V,

16.3. GROUP ALGEBRAS AND REPRESENTATION MODULES

By a *linear associative algebra* over a field F we mean a non-empty set A such that

(i) A is a vector space over F

(ii) A is a ring

(iii) for all $a, b \in A$ and $\lambda \in F$,

$$(\lambda a)b = a(\lambda b) = \lambda(ab).$$

For example the set **C** of complex numbers is a linear associative algebra over the field **R** of real numbers.

Similarly the set Q of all quarternions

$$a_0 I + a_1 i + a_2 j + a_3 k$$

$a_i \in \mathbf{R}$, $i = 0, 1, 2, 3$, is a linear associative algebra over **R** under the usual addition and multiplication of quarterions.

A subset S of a linear associative algebra A over F is said to be a *subalgebra* of A if:

1. for $s_1, s_2 \in S$, $s_1 - s_2 \in S$ and $s_1 s_2 \in S$

2. for $s \in S$ and $f \in F$, $fs \in S$.

The *centre* Z(A) of an algebra A is defined by

$$Z(A) = \{z \in A : za = az, \forall a \in A\}$$

Z(A) is a subalgebra of A.

We now briefly describe the concept of a *group algebra.*

Let G be any group and F a field. Consider the set FG of all formal expressions of the form.

$$\alpha = \sum_{x \in G} a_x x, \; a_x \in F$$

with the provision that only a finite number of a_x, $x \in G$, are different from $0 \in F$.

For two formal expressions $\alpha = \sum_{x \in G} a_x x$, $\beta = \sum_{x \in G} b_x x$, we say that

$$\alpha = \sum_{x \in G} a_x x = \sum_{x \in G} b_x x = \beta$$

if and only if $a_x = b_x$ for all $x \in G$.

We define addition, scalar multiplication and multiplication in FG by:

$$\sum_{x \in G} a_x x + \sum_{x \in G} b_x x = \sum_{x \in G} (a_x + b_x) x \qquad 16.3(1)$$

$$\lambda \sum_{x \in G} a_x x = \sum_{x \in G} (\lambda a_x) x \qquad 16.3(2)$$

$$\sum_{x \in G} a_x x \,.\, \sum_{y \in G} b_y y = \sum_{x \in G} \sum_{y \in G} a_x b_y (xy) \qquad 16.3(3)$$

for all $a_x, b_y, \lambda \in F$.

The equation in 16.3 (3), after writing u for xy, becomes

$$\begin{aligned} \sum_{x \in G} a_x x \,.\, \sum_{y \in G} b_y y &= \sum_{y \in G} \sum_{x \in G} a_x b_y xy \\ &= \sum_{u \in G} \left(\sum_{y \in G} a_{uy^{-1}} b_y \right) u \\ &= \sum_{u \in G} c_u u \qquad 16.3\ (4) \end{aligned}$$

where

$$c_u = \sum_{y \in G} a_{uy^{-1}} b_y.$$

In the multiplication of α and β defined by 16.3 (3), the product $\alpha\beta$ is called the *convolution* of α and β.

Under the addition, scalar multiplication and multiplication defined by 16.3(1) – 16.3(4), FG has both the ring and vector space structures.

In fact, FG is a linear associative algebra over F and is called *group algebra of G over F.*

Here the subset

$$G^* = \{1 \,.\, x : x \in G\}$$

is a basis of FG.

G* is isomorphic to G as a group so that we can identity G* and G.

For any finite group G of order n, let FG be the group algebra of G over F. Then, as stated above, Z(FG) is a subalgebra of FG. If we take the elements of G as

$$e = g_1, g_2, \ldots, g_n$$

then, as these form a basis of FG, for each $z \in Z(FG)$,

$$z = \sum_{i=1}^{n} a_i g_i, \; a_i \in F \qquad 16.3\ (5)$$

Also, for each $g \in G$

$$\sum_{i=1}^{n} a_i g_i = z = gzg^{-1} = \sum_{i=1}^{n} a_i g g_i g^{-1}$$

$$= \sum_{i=1}^{n} a_i' g_i', \quad g_i' = g g_i g^{-1}. \qquad 16.3\ (6)$$

So $a_i = a_i'$ in case g_i and g_i' are conjugate elements.

Hence, if two elements of G are conjugate then they have the same coefficients in 16.3 (1).

Summing up the coefficients of conjugate elements in 16.3 (5), equation 16.3 (5) can be written as

$$z = c_1 C^1 + c_2 C^2 + \ldots + c_k C^k \qquad 16.3(7)$$

where C^j is the sum of elements conjugate to one another and k is the number of conjugacy classes.

Clearly, for each $g \in$ G,

$$g C^j g^{-1} = C^j$$

because the terms in the sum $g C^j g^{-1}$ are simply a rearrangement of the terms of C^j. So, from 16.3(7) we have

$$z = g z g^{-1} = \sum_{i=1}^{k} c_i C^j$$

Equation 16.3 (7) shows that the sums $C^1, C^2, \ldots, C^k$ of elements of conjugacy classes of G form a basis of the subalgebra Z(FG).

This proves the following theorem.

16.3.1. Theorem: Let G be a group of order n. Then a basis of the centre Z(FG) of the group algebra FG of G over F is the set

$$\{C^1, C^2, \ldots, C^k\}$$

where k is the number of conjugacy classes and each C^i is the sum of conjugate elements of an element g_i of G, $1 \le i \le k$.

Let A be an algebra over a field F and $a \in$ A and fixed. Define a mapping $a_L : A \to A$ by:

$$a_L(x) = ax, x \in A.$$

Then

$$a_L(x + y) = a_L(x) + a_L(y) \text{ and } a_L(rx) = r a_L(x),$$

for all $x, y \in A$, $r \in F$.

Thus

$$A_L = \{a_L : a \in A\}$$

is a set of F-homomorphisms of the vector space A.

Each element of A_L is called the *left regular representation* of A.

Similarly the mapping $a_R : A \longrightarrow A$ defined by:

$$a_R(x) = xa^{-1}, x \in A,$$

is an F-homomorphism,

Each element of the set

$$A_R = \{a_R : a \in A\}$$

is called a *right regular representation.*

Let A_1, A_2 be linear associative algebras over F, A mapping $\varphi : A_1 \to A_2$ is said to be an *algebra homomorphism* if

(1) $\varphi(\lambda_1 a_1 + \lambda_2 a_2) = \lambda_1 \varphi(a_1) + \lambda_2 \varphi(a_2)$

(2) $\varphi(a_1 a_2) = \varphi(a_1) \cdot \varphi(a_2)$

for all $a_1, a_2 \in A_1, \lambda_1, \lambda_2 \in F$.

For any group G and a field F, a *representation of degree n* of the group algebra FG over F is a non-zero homomorphism ρ from FG into $\mathrm{Hom}_F(V, V)$ for some n-dimensional vector space V over F.

A representation ρ of FG is said to be *faithful* if ρ is injective.

If we replace $\mathrm{Hom}_F(V, V)$ with the ring $M_n(F)$ of all $n \times n$ matrices over F, then we speak of ρ as a *matrix representation.*

Let R be a ring with identity 1. A non-empty set M is said to be a *(left)* R-module or a *module over R* if

(1) M is an additive abelian group,

(2) For each $m \in M$, $r \in R$ $r \cdot m \in M$ and

(i) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$,

(ii) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$,

(iii) $(r_1 r_2) \cdot m = r_1 \cdot (r_2 m)$,

(iv) $1 \cdot m = m$

for all $m, m_1, m_2 \in M$, $r, r_1, r_2 \in R$ and 1, the identity of R.

From the above definition, one can immediately see that every vector space V(F) over a field F is a module over F and we denote this module also as V(F).

If R is a ring with identity then R can be regarded as a module over itself.

Similarly, the group algebra FG is a module over F.

A subset N of an R-module M is said to be a *submodule* of M if

(i) for any $n_1, n_2 \in N$, $n_1 - n_2 \in N$

(ii) for any $r \in R$ and $n \in N$, $r \,.\, n \in N$.

We now prove a theorem which shows that the study of representations of a group G is equivalent to the study of representations of the group algebra FG over F.

16.3.2. Theorem: There is a one-one correspondence between the representations of a group G and the representations of the group algebra FG over F.

Proof: Let ρ be a representation of G of degree n, that is, a homomorphism of G into $GL_n(V)$ where V is an n-dimensional vector space over F. We extend ρ to a mapping

$$\rho' : FG \to \mathrm{Hom}_F(V, V) \supseteq GL_n(V)$$

by putting

$$\rho'\left(\sum_{x \in G} a_x x\right) = \sum_{x \in G} a_x \rho(x).$$

Then it is easy to verify that ρ' is a homomorphism of the group algebra FG into $\mathrm{Hom}_F(V, V)$.

So, for every representation ρ of G, there is a representation ρ' of the group algebra FG over F of G.

Conversely, suppose that ρ' is a representation of FG of degree n over F, that is, ρ' is non-zero homomorphism of FG into $\mathrm{Hom}_F(V, V)$, where V is an n-dimensional vector space. Restrict ρ' to the subset

$$\{1 \,.\, x : x \in G\}$$

of FG. This restriction ρ, say, of ρ' is then a representation of G of degree n.

Thus to each representation of G there is a representation of an FG-module V and conversely, for each representation of a non-trivial FG-module V, there is a representation of G.

16.3.3. Theorem: The study of representations of FG (or G) of degree n is equivalent to the study of *non-zero FG-modules.*

Proof: Suppose that ρ is a representation of FG (or G) of degree n and V is the underlying vector space. For any $v \in$ V and $g \in$ FG, define the action of g on V by:

$$g \,.\, v = \rho(g) \,.\, (v) \qquad 16.3.3\ (1)$$

Then it is easy to see that the equations

$$g \,.\, (v_1 + v_2) = g \,.\, v_1 + g \,.\, v_2$$
$$(g_1 + g_2) \,.\, v = g_1 \,.\, v + g_2 \,.\, v$$
$$(g_1\, g_2) \,.\, v = g_1 \,.\, (g_2 \,.\, v)$$

follow from the equations

$$\begin{aligned} g \,.\, (v_1 + v_2) &= \rho(g)\,(v_1 + v_2) \\ &= \rho(g)\,(v_1) + \rho(g) \,.\, (v_2), \\ (g_1 + g_2) \,.\, (v) &= \rho(g_1 + g_2) \,.\, v \\ &= (\rho(g_1) + \rho(g_2)) \,.\, v \\ &= \rho(g_1) \,.\, v + \rho(g_2) \,.\, v \end{aligned}$$

and

$$\begin{aligned} (g_1\, g_2) \,.\, v &= \rho(g_1\, g_2) \,.\, v \\ &= (\rho(g_1) \,.\, \rho(g_2)) \,.\, v \\ &= \rho(g_1) \,.\, (\rho(g_2) \,.\, v) \end{aligned}$$

for all $v_1, v_2, v \in$ V, $g_1, g_2, \in$ FG.

Thus V is an FG-module determined by the representation ρ.

Conversely, let V be a non-zero FG-module. For a fixed $g \in$ FG, consider the mapping $\rho_g : V \to V$ defined

$$\rho_g(v) = g \,.\, v$$

for all $v \in V$. Then $\rho_g \in \mathrm{Hom}_{FG}(V, V)$ because:

$$\begin{aligned} \rho_g(v_1 + v_2) &= g \,.\, (v_1 + v_2) \\ &= g \,.\, v_1 + g \,.\, v_2 \\ &= \rho_g(v_1) + \rho_g(v_2) \\ \rho_g(av) &= g \,.\, av \\ &= a\, g \,.\, v \\ &= a\, \rho_g(v). \end{aligned}$$

So $\rho_g \in \mathrm{Hom}_{FG}(V, V)$.

Next define a mapping $\rho : FG \to \mathrm{Hom}_{FG}(V, V)$ by:

$$\rho(g) = \rho_g$$

for all $g \in FG$. It is easy to verify that

$$\rho(g_1 + g_2) = \rho_{g_1} + \rho_{g_2}$$

$$\rho(ag) = a\,\rho_g$$

and

$$\rho(g_1\, g_2) = \rho_{g_1} \cdot \rho_{g_2}$$

for all g_1, g_2, g FG, $a \in$ F. Thus ρ is a representation of FG and is, of course, uniquely determined.

If ρ is a representation of FG of degree n and V is the underlying vector space of dimension n then V is an FG-module under the action defined by equation 16.3.3 (1).

V is called a *representation module* of ρ while ρ is a *representation* of FG *afforded by* V.

Here for each $x \in FG$: $\rho(x)$ is an element of $GL_n(V)$.

A representation ρ (or the representation module V) of G is said to be *irreducible* if the only FG-submodules of V are $\{0\}$ and V itself.

Every trivial representation is irreducible.

Also, every one dimensional represntation is irreducible,

Otherwise ρ (or V) is said to be *reducible*. The representation ρ (or the representation module V) is said to be *completely reducible* if V is the direct sun of its irreducible FG-submodules, that is, if there are FG-submodules $V_1, V_2, \ldots, V_m$ of V such that

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_m,\ m \geq 1.$$

It, therefore, follows that every irreducible representation (or representation module) is completely reducible.

A representation ρ (or the representation module V) of FG is said to be *indecomposable* if V is not expressible as the direct sum of two proper FG-submodules of V.

Otherwise ρ (or V) is said to be *decomposable*.

If the representation module is FG itself or isomorphic to it, then the representation ρ or the representation module is said to be a *regular representation*:

Two representations ρ and ρ' of FG of degree m and n respectively are said to be *equivalent* if and only if their representation modules are isomorphic.

In such a case $m = n$.

We now determine a condition for the equivalence of the representations. We shall show that this definition of equivalence of representations is similar to the one described earlier.

16.3.4. Let V and V′ be the representation modules of the equivalent representation ρ and ρ' respectively. Then V and V′ have the same dimensions because they are isomorphic.

Let

$$\{v_1, v_2, ..., v_n\}, \{v'_1, v'_2, ..., v'_n\}$$

be bases of V and V′ respectively and α an FG-isomorphism between V and V′. Suppose that

$$\alpha(v_i) = \sum_{j=1}^{n} a_{ji} v_j', \; i = 1, 2, ..., n; \; a_{ji} \in F \qquad 16.3.4\ (1)$$

Also

$$\rho(x)(v_i) = x \,.\, v_i = \sum_{j=1}^{n} \xi_{ji} v_j \qquad 16.3.4\ (2)$$

and

$$\rho'(x)(v_i') = x.\, v'_i = \sum_{j=1}^{n} \eta_{ji} v'_j, \; \eta_{ji} \in F, \qquad 16.3.4\ (3)$$

for $x \in$ FG, i = 1, 2, ..., n. Then, for all $x \in$ FG,

$$\alpha\rho(x)(v_i) = \alpha(x \,.\, v_i)$$

$$= x \,.\, (\alpha(v_i)) \;, \alpha \text{ is an FG-homomorphism.}$$

$$= x \,.\, \sum_{j=1}^{n} a_{ji} v_j'$$

$$= \sum_{j=1}^{n} a_{ji} (x \,.\, v_j')$$

$$= \sum_{k=1}^{n} \sum_{j=1}^{n} \eta_{kj} a_{ji} v'_k$$

$$= \sum_{j=1}^{n} a_{ji} \sum_{k=1}^{n} \eta_{kj} v'_k$$

$$= \sum_{j=1}^{n} a_{ji} (x. v_j'), \quad \text{by} \qquad 16.3.4\ (3)$$

$$= \sum_{j=1}^{n} a_{ji} \rho'(x)(v_j'), \quad \text{by} \qquad 16.3.4\ (3)$$

$$= \rho'(x), \sum_{j=1}^{n} a_{ji} v'_j$$

$$= \rho'(x) \cdot \alpha(v_i) \qquad 16.3.4\ (4)$$

for all i = 1, 2, ..., n.

Since 16.3.4 (4) holds for all v_i, i = 1, 2, ..., n, it holds for all $v \in V$. Thus

$$\alpha \rho(x) = \rho'(x) \alpha$$

That is

$$\rho'(x) = \alpha \rho(x) \alpha^{-1} \qquad 16.3.4\ (5)$$

for all $x \in FG$.

Equation 16.3.4 (5) is the required condition for two representations of FG to be equivalent.

Thus the representations ρ and ρ' of FG-modules V and V′ are equivalent if dim V = dim V′ and, for some FG-isomorphism α between V and V′, equation 16.3.4 (5) holds.

16.4. MASCHKE'S THEOREM

Let F be a field. The least positive integer m such that $ma = 0$ for all $0 \neq a \in F$, is called the *characteristic* of F. If the relation $ma = 0$ holds only for m = 0 then F is said to have *characteristic zero.*

Now we prove an improved form of an important result due to H. Maschke (1898).

16.4.1. Theorem:

(Theorem of complete reducibility)

Let G be a subgroup of GL_n (V) where V is a vector space over F and of dimension n. Let H be a subgroup of finite index h in G. Suppose that

(i) characteristic of F is either 0 or else is prime to h.

(ii) H is completely reducible.

The G is completely reducible.

Proof: Since H is completely reducible, V has H-invariant subspaces U and W such that

$$V = U \oplus W$$

The projection mapping $\pi : V \to U$ defined by:

$$\pi(v) = \pi(u + w) = u$$

for all $v = u + w \in V$, $u \in U$, $w \in W$, is a linear transformation of V.
Let

$$G = \bigcup_{i=1}^{h} y_i H,\ y_i \in G,$$

be a left coset decomposition of G. Define a function $\alpha : V \to V$ by:

$$\alpha(v) = \left(\frac{1}{h} \sum_{i=1}^{h} y_i \pi y_i^{-1}\right)(v), \text{ for all } v \in V, \qquad 16.4.1\ (1)$$

which makes sense because $\frac{1}{h} \in F$ because of 16.4.1 (1). Since $G \subseteq \mathrm{Hom}_F(V, V)$, $y_i, \pi \in \mathrm{Hom}_F(V, V)$ so $\alpha \in \mathrm{Hom}_F(V, V)$. Also, U is an H-space. If x and y are in the same left coset of H in G, that is, $y^{-1}x \in H$, then

$$\begin{aligned}(x \pi x^{-1})(V) &= x \pi(V) = x(U)\\ &\quad (U \text{ is H-invariant and } y^{-1}x \in H \text{ so that } (y^{-1}x)(U) = U)\\ &= (y \pi y^{-1})(V).\\ &= y(U)\end{aligned}$$

So $\alpha(v)$, $v \in V$, is independent of the choice of coset representatives of H in G.
We show that $\alpha(V)$ is a G-space of V with W as the complementary space.

For any $x \in G$, the elements $xy_1, xy_2, \ldots, xy_h$ form a set of left coset representatives of H in G. So

$$\begin{aligned}\alpha(V) &= \left(\frac{1}{h} \sum_{i=1}^{h} (xy_i) \pi (xy_i)^{-1}\right)(V)\\ &= \left(\frac{1}{h} \sum_{i=1}^{h} xy_i \pi y_i^{-1} x^{-1}\right)(V)\\ &= \left(x.\left(\frac{1}{h} \sum_{i=1}^{h} y_i \pi y_i^{-1}\right)x^{-1}\right)(V)\\ &= x\,.\,\alpha(V), \qquad (\because x^{-1}(V) = V \text{ since V is G-invariant})\end{aligned}$$

for all $x \in G$. So $\alpha(V)$ is a G-invariant subspace of V. Also $y(W) = W$ for all $y \in G$ and $\pi(W) = \{0\}$. So we have, from the definition of α,

$$\alpha(W) = \{0\}.$$

Thus

$$(I - \alpha)(w) = w - \alpha(w) = w \qquad 16.4.1\ (2)$$

for all $w \in W$. However the definition of π shows that

$$(I - \pi)(V) = V - \pi(V) = V - U = W.$$

Hence

$$\begin{aligned} y_i (I - \pi) y_i^{-1}(V) &= (I - y_i \pi y_i^{-1})(V) \\ &= V - (y_i \pi y_i^{-1}) V \\ &= V - (y_i \pi)(V) = V - U = W. \end{aligned} \qquad 16.4.1\ (3)$$

So

$$\begin{aligned} (I - \alpha)(v) &= \left(I - \frac{1}{h}\sum_{i=1}^{h} y_i \pi y_i^{-1}\right)(v) \\ &= \left(\frac{1}{h}\sum_{i=1}^{h} y_i (I - \pi) y_i^{-1}\right)(v) \end{aligned}$$

is an element of W. So

$$(I - \alpha)(V) = W. \qquad 16.4.1\ (4)$$

But then

$$\begin{aligned} V &= \alpha(V) + (I - \alpha) V \\ &= \alpha(V) + W. \end{aligned} \qquad 16.4.1\ (5)$$

To see that the sum in 16.4.1 (5) is direct, let, for some $v \in V$, $\alpha(v) \in W$. That is, $\alpha(v) \in \alpha(V) \cap W$. Then, using the equation

$$\alpha(I - \alpha) = (I - \alpha)\alpha$$

we have

$$\begin{aligned} \alpha(v) &= (I - \alpha)\alpha(v), \quad \text{by 16.4.1 (4), (see 16.4.1 (2) also)} \\ &= \alpha(I - \alpha)(v). \end{aligned}$$

So

$$\alpha(v) \in \alpha(I - \alpha)(V) = \alpha(W) = \{0\}.$$

Thus

$$W \cap \alpha(V) = \{0\}$$

so that

$$V = \alpha(V) \oplus W.$$

Hence G is completely reducible.

A trivial representation ρ of G is irreducible if and only if it is one dimensional.

When H is the trivial subgroup with its index in G finite, then G is a finite group and we have the original formulation of Maschke's theorem. Thus we have:

16.4.2. Corollary: Let G be a finite subgroup of $GL_n(V)$ of order g. Suppose that the characteristic of F is either 0 or else is prime to g. Then G is completely reducible.

(**Remark:** If G is a finite group and ρ is a completely reducible matrix representation of G into GL (n, F), then, for each $g \in G$,

$$\rho(g) = \begin{pmatrix} A(g) & \mathbf{0} \\ \mathbf{0} & B(g) \end{pmatrix}$$

where A (g), B (g) are square matrices of dimension k and m respectively and n = k + m).

Proof (Mashke's Theorem): Let G be a finite subgroup of GLn(V). Then G is isomorphic to a subgroup $\rho(G) = G_1$ of GL(n, F). The complete reducibility of G_1 implies that of G.

If G_1 is irreducible then it is completely reducible by definition and we have nothing to prove. So suppose that G_1 is reducible so that each matrix in G_1 is of the form

$$\rho(x) = \begin{pmatrix} A(x) & C(x) \\ \mathbf{0} & B(x) \end{pmatrix}, x \in G,$$

where A (x), B (x) are $k \times k$ and $m \times m$ matrices with $k + m = n$, while C (x) is a $k \times m$ matrix and $\mathbf{0}$ is the $m \times k$ zero matrix over F. We shall determine a non-singular matrix P over F such that

$$P\,\rho(x)\,P^{-1} = \begin{pmatrix} A(x) & \mathbf{0} \\ \mathbf{0} & B(x) \end{pmatrix} = \rho'(x) \qquad 16.4.2\ (1)$$

for all $x \in G$. Choose

$$P = \begin{pmatrix} I_k & D \\ \mathbf{0} & I_m \end{pmatrix}$$

where D is to be determined so as to satisfy condition

$$P\rho(x) = \rho'(x)\,P,$$

that is,

$$A(x)\,D = C(x) + D\,.\,B(x). \qquad 16.4.2\ (2)$$

Now, for $x, y \in G$,

$$\rho(x)\,\rho(y) = \begin{pmatrix} A(x) & C(x) \\ \mathbf{0} & B(x) \end{pmatrix}\begin{pmatrix} A(y) & C(y) \\ \mathbf{0} & B(y) \end{pmatrix}$$

$$= \begin{pmatrix} A(xy) & C(xy) \\ \mathbf{0} & B(xy) \end{pmatrix}$$
$$= \rho(xy)$$

gives

$$A(x)\,A(y) = A(xy) \qquad 16.4.2\ (3)$$
$$B(x)\,B(y) = B(xy) \qquad 16.4.2\ (4)$$

and

$$A(x)\,C(y) + C(x)\,B(y) = C(xy). \qquad 16.4.2\ (5)$$

Incidentally the relations 16.4.2 (3) and 16.4.2 (4) show that $x \to A(x)$, $x \to B(x)$ are both representations of G.

Multiply equation 16.4.2 (5) by $A(x^{-1}) = (A(x))^{-1}$ and sum over all $x \in G$, we obtain

$$g\,.\,C(y) + \left(\sum_{x\in G} A(x^{-1})\,C(x)\,(B(y)\right) = \sum_{x\in G} A(x^{-1})\,C(xy)$$

That is

$$C(y) + \left(\frac{1}{g}\sum_{x\in G} A(x^{-1})\,C(x)\,B(y)\right) = \frac{1}{g}\sum_{x\in G} A(x^{-1})C(xy) \qquad 16.4.2\ (6)$$

Put $z = xy$ in the expression on the right hand side of 16.4.2 (6) and note that, as x ranges over G, z also ranges over G and the right hand side expression is:

$$\frac{1}{g}\sum_{x\in G} A(x^{-1})\,C(xy) = \frac{1}{g}\sum_{z\in G} A(yz^{-1})\,C(z)$$
$$= A(y)\,\frac{1}{g}\sum_{z\in G} A(z^{-1})\,C(z)$$

Now take

$$D = \frac{1}{g}\sum_{z\in G} A(z^{-1})\,C(z) \qquad 16.4.2\ (7)$$

Then, for x replaced with z, 16.4.2 (6) becomes

$$C(y) + D\,.\,B(y) = A(y)\,.\,D$$

which is 16.4.2 (2) and holds for all $y \in G$. Thus, if D is chosen as in 16.4.2 (7) then equation 16.4.2 (2) always holds.

Consequently

$$P\,\rho(x)\,P^{-1} = \begin{pmatrix} A(x) & \mathbf{0} \\ \mathbf{0} & B(x) \end{pmatrix}, x \in G.$$

So G is completely reducible.

Masckes's theorem deals with the decomposition of a reducible representation of a finite group into irreducible sub representations. For any finite group G and a representation $\rho : G \longrightarrow GL_n(V)$ of G, V, a vector space over a field of characteristic 0, every G-invariant subspace U of V has an invariant direct complement W so that ρ is completely reducible. Specifically if the characteristic p of the field F does not divide the order of G then every finite dimensioned representation is completely reducible.

A representation ρ of a group G over a field F may or may not be reducible over a subfield of F.

Next we prove another important result called Schur's lemma first proved by Isai Schur in 1905. Maschke's theorem and Schur's lemma are regarded as the two main pillars of the whole representation theory.

The version given here is in terms of representation modules.

16.4.3. Theorems: (Schur's lemma)

For any group G suppose that U and V are irreducible FG-modules over F. Then an FG-homomorphism

$$\varphi : U \to V$$

is either the zero map or is an isomorphism.

Proof: It is enough to prove that if $\varphi \neq 0$, then φ is a bijection. For this we have to show that Ker $\varphi = \{0\}$ and Im $\varphi = V$. Now Ker φ is always a submodule of U. Since U is an irreducible FG-module, Ker $\varphi = \{0\}$ or Ker $\varphi = U$. But Ker $\varphi = U$ implies φ is the zero map, that is φ maps every element of U onto the additive identity of V, a contradiction.
Hence Ker $\varphi = \{0\}$ so that φ is injective.

Next consider the set Im φ which is an FG-submodule of V. Since V is irreducible, either Im $\varphi = \{0\}$ or Im $\varphi = V$. But Im $\varphi = \{0\}$ implies φ is the zero map and Ker $\varphi = U$, a contradiction. Hence Im $\varphi = V$. Thus φ is surjective. Therefore φ is an isomorphism.

The original matrix version of Schur's lemma is as follows.

16.4.4. Theorem: (Schur's lemma).

Let ρ, ρ' be two irreducible representations of degree n of a group G over F. Suppose that there is an $n \times n$ matrix P over F such that

$$P\,\rho(x) = \rho'(x)\,P$$

for all $x \in G$. Then either P is the zero matrix or P is invertible so that ρ and ρ' are equivalent.

A field F is *algebraically closed* if every polynomial equation

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0,\ a_i \in F$$

has all its roots in F.

For example the field **C** of complex numbers is algebraically closed while the fields **R** or **Q** of real or rational numbers respectively are not. Here the equation $x^2 + 1 = 0$ has no root in **R** or **Q**.

For algebraically closed fields, e.g, **C** matrix version of Schur's lemma is an follows.

16.4.5. Corollary: Suppose that ρ is an irreducible representation of a group G over F where F is algebraically closed. Then the only matrices which commute with each $\rho(x)$, $x \in G$ are the scalar matrices.

Proof: Clearly every scalar matrix commutes with all $\rho(x)$, $x \in G$.

Conversely, suppose that S is a non-zero matrix such that

$$S\rho(x) = \rho(x)\, S$$

for all $x \in G$. Then for any $\lambda \in F$.

$$(S - \lambda I)\, \rho(x) = \rho(x)\, (S - \lambda I)$$

for all $x \in G$. By Schur's lemma, $S - \lambda I = \mathbf{0}$, the zero matrix or $S - \lambda I$ is invertible. Suppose that $S - \lambda I$ is invertible, then $S - \lambda I \neq \mathbf{0}$ for any $\lambda \in F$.

Consider the characteristic equation

$$\det (S - \lambda I) = 0 \qquad 16.4.5\ (1)$$

of $S - \lambda I$. Since F is algebraically closed, equation (1) has a solution λ_0, say, in F. Thus

$$S - \lambda_0 I = \mathbf{0}$$

for at least one $\lambda_0 \in F$, a contradiction. Hence $S - \lambda I$ is not invertible. But then $S - \lambda I = 0$ for some $\lambda \in F$. Thus S is a scalar matrix.

16.4.6 Corollary: Let $V \neq \{0\}$ be a completely reducible FG-module. Then V is irreducible if and only if $\mathrm{Hom}_{FG}(V, V)$ is a division ring.

Proof: Suppose that V is a non-zero irreducible FG-module and $\alpha \in \mathrm{Hom}_{FG}(V, V)$. By Schur's lemma, either $\alpha = 0$ or α is invertible. Hence $\mathrm{Hom}_{FG}(V, V)$ is a division ring.

Conversely suppose that V is a non-zero completely reducible FG-module and Hom_{FG} (V, V) is a division ring. Suppose that V is not irreducible. Then

$$V = V_1 \oplus V_2$$

for some non-zero proper submodules of V. Define $\pi: V \to V$ by

$$\pi(v) = \pi(v_1 + v_2) = v_1$$

Then $\pi \in \text{Hom}_{FG}(V, V)$ is non-zero but is not a bijection (here $\text{Ker } \pi \neq \{0\}$). Hence π is not invertible, a contradiction to the fact that Hom_{FG} (V, V) is a division ring. Hence V is irreducible.

16.4.7 Corollary: If V is a non-zero irreducible FG module and F is algebraically closed, then Hom_{FG} (V, V) is a field.

Proof: First note that, by definition, every irreducible FG-module is completely reducible. In such a case we have already shown that $\text{Hom}_{FG}(V, V)$ is a division ring. Let $0 \neq \alpha \in \text{Hom}_{FG}$ (V, V) and A be the matrix corresponding to α under the natural isomorphism between Hom_{FG} (V, V) and the set M_n of $n \times n$ matrices. Then $A - \lambda I$ is not invertible so that, by Schur's lemma,

$$A - \lambda I = \mathbf{0}$$

for some eigen value $\lambda \in F$, because F is algebraically closed, Hence A is a scalar matrix and so α is a scalar linear transformation in $\text{Hom}_{FG}(V, V)$. Since α^{-1} is also a scalar linear transformation and any two scalar transformations are permutable, $\text{Hom}_{FG}(V, V)$ is a field.

16.5. GROUP CHARACTERS

In this section we discuss another important concept which has been extensively used in obtaining information about finite groups. This concept is closely related to the theory of representations of groups. The very first proof of the solvability of groups of order $p^\alpha q^\beta$, p, q distinct primes, and α, β positive integers, was given by Burnside (1904) using character theory. This theorem has now been proved by J. G. Thompson without using group representation theory.

Similarly, a large part of the intricate calculations, in the proof the Feit-Thompson Theorem about the solvability of groups of odd order [20], involve character values.

Many of the important theorems about the structure of finite groups use characters of modular representations.

Let G be a group and ρ a matrix representation of G of degree n. Then, for each $x \in G$, $\rho(x)$ is a matrix. We define a *character of G afforded by* ρ as a function $\chi^\rho : G \to G$ given by:

$$\chi^\rho(x) = \text{tr } \rho(x),$$

for all $x \in G$.

Here tr ρ (x) is the trace *i.e.*, the sum of diagonal elements of the matrix $\rho(x)$.

χ^ρ is then also called the *character of* ρ.

The *degree of a character* is the degree of the representation which affords it.

The kernel of a character χ^ρ is the set

$$\text{Ker } \chi^\rho = \{g \in G : \chi^\rho(g) = \chi^\rho(e)\}$$

where $\chi^\rho(e)$ is the value of χ^ρ at the identity element e of G.

Thus

$$\chi^\rho(e) = \text{tr}[\rho(e)] = \text{tr}(I_n) = n = \text{degree of } \rho,$$

I_n the multiplication identity of GL (n, F)

We also have $\chi^\rho(x^{-1}) = \overline{\chi^\rho(x)}$

Here $\bar{z}$ denotes the complex conjugate of z.

A function $f : G \to F$ is said to be a *class function* if, for any $x \in G$ and all $a \in G$,

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

It is easy to verify that the set *Cl* (G, F) of all class functions from G to F is a vector space over F under the usual addition and scalar multiplication of mappings.

Here we take F to be the field of complex numbers, unless stated otherwise.

16.5.1 Theorem: Characters are class functions. That is, for each character x^{ρ},

$$\chi^{\rho}(x) = \chi^{\rho}(a\,x\,a^{-1}),\ a \in G,$$

Proof: Suppose that χ^{ρ} is the character of a group G afforded by a representation ρ of G degree n. Then, for any x and $a \in G$,

$$\text{tr}\,(\rho(a)\,\rho(x)\,\rho(a^{-1})) = \text{tr}\,(\rho(axa^{-1})).$$

Let $\det(\lambda I - \rho(x))$ be the characteristic polynomial of $\rho(x)$. Then trace of $\rho(x)$ is the coefficient of λ^{n-1} in $\det(\lambda I - \rho(x))$. However since

$$\det(\lambda I - \rho(axa^{-1})) = \det(\rho(a)(\lambda I - \rho(x))\,\rho(a^{-1}))$$

$$= \det(\lambda I - \rho(x)),$$

the coefficient of λ^{n-1} in both is the same.

Hence

$$\text{tr}\,\rho(axa^{-1}) = \text{tr}\,\rho(x).$$

Thus

$$\chi^{\rho}(x) = \text{tr}\,\rho(x) = \text{tr}\,\rho(a\,x\,a^{-1}) = \chi^{\rho}(a\,x\,a^{-1})$$

for all $a, x \in G$. Hence χ^{ρ} is a class function. That is, a character has the same value for elements of the same conjugacy class.

16.5.2 Corollary: Equivalent representations have the same character.

Proof: Suppose that ρ and ρ' are equivalent representations of G of degree n and χ^{ρ}, $\chi^{\rho'}$ are the characters of G afforded by ρ and ρ' respectively. Then there is an $n \times n$ invertible matrix P such that

$$\rho'(x) = P\rho(x)P^{-1}$$

so that

$$\chi^{\rho'}(x) = \text{tr}\,\rho'(x) = \text{tr}\,(P\,\rho(x)P^{-1}) = \text{tr}\,\rho(x) = \chi^{\rho}(x)$$

for all $x \in G$.

16.5.3. Corollary: The number of irreducible characters (representations) of G is equal to the number of conjugacy classes of G)

Proof: Left as an exercise

A character χ^{ρ} of G afforded by an irreducible representation ρ is called an *irreducible character.*

The character χ^{ρ} is called a *linear character* if the representation ρ has degree 1.

For two class function f_1, f_2 we define an inner product in $Cl\ (G, F)$ by:

$$< f_1, f_2 >= \frac{1}{|G|} f_1\ (x).\ \overline{f_2(x)}\ , x \in G. \qquad 16.5.3\ (*)$$

Here F is the field of complex numbers and $\overline{f(x)}$, $x \in G$, denotes the conjugate of $f(x)$ in F.

So we have the following orthogonality relations.

$$< \chi_i\ , \chi_j > = \delta_{ij}, \qquad 16.5.3\ (**)$$

where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. Thus the set of all irreducible characters form an orhtonormal basis of $Cl\ (G, F)$. Moreover the equations 16.5.3 (*) and 16.5.3 (* *) help us in finding the order of the group G.

For $x, y \in G$, let $\chi_i\ (x)$, $\chi_j\ (y)$ denote the values of irreducible characters χ_i and χ_j at x and y respectively. Then

$$\sum_{i,\ j} \chi_i\ (x)\ .\ \chi_j\ (y) = |C_G(x)|, \text{ if } x \text{ and } y \text{ are conjugate in } G$$

$$= 0, \text{ otherwise}$$

Here the summation is taken over all the irreducible characters of G

Also $C_G(x)$ is the cenralizer of x in G and the sum is over all the irreducible characters χ_i of G.

Note that the above relation also determines the number of elements in the conjugacy classes of elements of the group.

16.5.4. Theorem: Every character afforded by a reducible representation of a group G can be expressed as the sum of irreducible characters.

Proof: Suppose that ρ is a reducible representation of G of degree n. Then there is a matrix $P \in GL\ (n, F)$ such that

$$P\ \rho\ (x)P^{-1} = \begin{pmatrix} \rho_1(x) & * \\ \boldsymbol{0} & \rho_2(x) \end{pmatrix} \qquad 16.5.4\ (1)$$

for all $x \in G$. Here $\rho_1(x)$, $\rho_2(x)$ are square matrices of degree k and m such that $k + m = n$, $\boldsymbol{0}$ is the rectangular $m \times k$ zero matrix and * denotes a rectangular $k \times m$ matrix. ρ_1, ρ_2 are the *constituents of* ρ.

Thus

$$\chi^{\rho}(x) = \text{tr}\ \rho(x) = \text{tr}\ (P\rho(x)P^{-1})$$

$$= \text{tr}\ \rho_1(x) + \text{tr}\ \rho_2(x)$$

$$= \chi^{\rho_1}(x) + \chi^{\rho_2}(x) \qquad 16.5.4\ (2)$$

Thus the character of a reducible representation is the sum of the characters of its constituents.

We continue this process of expressing a reducible constituent in the form given in 16.5.4 (1) and, after a finite number of steps, arrive at irreducible representations ρ_1, ρ_2, ..., ρ_s and a corresponding decomposition of χ^{ρ} as the sum of irreducible characters χ^{ρ_1}, χ^{ρ_2}, ..., χ^{ρ_s}.

So every character χ^{ρ} of a group G can be expressed as the sum of irreducible characters.

16.5.5 Corollary: The character of a reducible representation is the sum of characters of the irreducible representation ρ_1, ρ_2, ..., ρ_s.

Proof: The trace of $\rho(\chi)$ is sum of the traces of $\rho_1(\chi)$, $\rho_2(\chi)$, ..., $\rho_s(\chi)$.

Note: Let χ^{ρ} be a character of G corresponding to the representation ρ and let H be a subgroup of G. Then the restriction of χ^{ρ} to H is a character of H.

16.6. CHARACTER TABLES

Let G be a finite group. We like to know about all the characters of G. This information is usually displayed in the form of a table, called the (Frobenius) *character table* of G. The table contains a listing of values of irreducible characters of all the elements of G. Since the characters are class functions we need only write down the values of irreducible characters of representative elements in the conjugacy classes of the group.

The character table is always a square table and the first row of a character table consists of ones and correspond to the trivial representation sending each element of G to the $n \times n$ matrix with the first entry as 1 and zeroes elsewhere.

The first column of the table is labeled according to representatives of conjugacy classes of the group. The entries of the first column represent the values of the irreducible characters at the identity element of the group. These are just the degrees of the irreducible characters.

Before we define the character table of a group G we mention, without proof, the following results. (cf. Ledermann's book [34]).

16.6.1 Theorem A: Let G be a finite group of order g. Suppose that F is a field of characteristic 0 or a prime p where p does not divide g. Let n_1,

$n_2, ..., n_s$ denote the degrees of the distinct irreducible representations of G over F.

Then

$$g = n_1^2 + n_2^2 + ... + n_s^2,$$

Every group G has the trivial irreducible representation given by $\rho(x) = 1$, the identity of the field F, for all $x \in G$. Hence, if n_1 denotes the degree of this representation, we always have $n_1 = 1$.

16.6.2 Theorem B: If F is an algebraically closed field of characteristic 0 or p where p does not divide the order of a finite group G, then the number of distinct irreducible representations (characters) of G over F is equal to the number of distinct conjugacy classes.

Theorems A and B can be applied to show that all representations of a finite abelian group K are of degree 1. For if k is the order of K and $n_1, n_2, ...n_s$ denote the degrees of s irreducible representations then

$$k = n_1^2 + n_2^2 + ... + n_s^2$$

Since each element of K determines its own conjugacy class consisting of only that element itself, there are k distinct conjugacy classes so that s = k. But then, as each n_i is a non-zero positive integer,

$$n_i = 1, \text{ for } i = 1, 2, ..., k.$$

We now define the character table of a group G as follows:

Suppose that a finite group G has k distinct irreducible characters $\chi^{(1)}, \chi^{(2)}, ..., \chi^{(k)}$. Let $C_1, C_2, ..., C_k$ be all the k conjugacy classes, equal to the number of irreducible representations or characters, of G and h_i the number of elements in the conjugacy class C_i, i = 1, 2, ..., k. Then the k × k matrix table,

	h_1	h_2	h_3	. . .	h_k
$\chi^{(1)}$	$\chi_1^1 = 1$	$\chi_2^1 = 1$	$\chi_3^1 = 1$	. . .	$\chi_k^1 = 1$
$\chi^{(2)}$	$\chi_1^2 = n_2$	χ_2^2	χ_3^2	. . .	χ_k^2
$\chi^{(3)}$	$\chi_1^3 = n_3$	χ_2^3	χ_3^3	. . .	χ_k^3
.	.	.	.	. .	.
.	.	.	.	. .	.
				.	
.	.	.	.	. .	.
$\chi^{(k)}$	$\chi_1^k = n_k$	χ_2^k	χ_3^k	. . .	χ_k^k

where $\chi_j^i = \chi_j^i(x)$, the value of $\chi^{(i)}$ at the element x in C_j, is called the *character table* of G.

Here the entries in the first column of the matrix (χ_j^i) indicate the degrees of the irreducible characters and the values of the characters at the identity element e in C_1.

Thus the character table of a group G is a matrix whose rows correspond to the different characters while its columns contain values of all irreducible characters for the particular respective conjugacy classes.

A brief outline of a method of computing the character table of a finite group G is given below:

1. Write down all the conjugacy classes
$$C_1, C_2, ..., C_k$$
of G and also determine the number h_i of elements in each conjugacy class C_i, i = 1, 2, ..., k.

2. For each class C_i, write down the formal sums of all the elements in C_i. That is, form S_i where
$$S_i = \sum_{x \in C_i} x, \; i = 1, 2, ..., k.$$

3. Express the products $S_i S_j$ as a linear combination of the class sums $S_1, S_2, ..., S_k$ and determine the corresponding coefficients in
$$S_i S_j = \sum_{m=1}^{k} s_{ijm} S_m, \; i, j = 1, 2, ..., k.$$

4. Find the k matrices
$$A_i = (s_{ijm}), \; i = 1, 2, ..., k.$$
Thus $A_i = (s_{ijm})$, j, m = 1, 2, ..., k and so no.

5. Determine the degrees $n_1, n_2, ..., n_k$ of the distinct irreducible representations of G. These are obtained by the formula
$$n_1^2 + n_2^2 + ... + n_k^2 = g$$
where g is the order of G.

6. Find the characteristic roots of A_j, $j = 1, 2, ..., k$. If the characteristic roots of A_j are
$$w_j^1, w_j^2, ..., w_j^k$$
then the corresponding character values are given by:
$$w_j^i = h_j \chi_j^i / n_i \qquad (*)$$

The choice of roots must be made in such a say that the orthogonality relations

$$\sum_{t=1}^{g} \chi_i^t \chi_j^t = \frac{g}{h_i} \delta_{ij} \qquad \text{and}$$

$$\frac{1}{g} \sum_{x \in G}^{r} \chi^i(x) \chi^j(x) = \delta_{ij},$$

where $\delta_{ij} = 1$ if C_i consists of the inverses of the elements of C_j and zero otherwise, are satisfied when h_j and n_i are as given above.

7. The matrix $X = (\chi_j^i)$, where χ_j^i are obtained from (*) gives the required character table.

The case of cyclic groups is particularly simple. Here all the irreducible representation are of degree 1. So all the characters of such a group are of degree 1. (Recall that such characters *i.e.*, characters of degree 1, are called *linear*).

Thus if C is a cyclic group of order g and

$$w^{(r)} = e^{2\pi i r/g}$$

is a gth root of unity, $r = 0, 1, 2, ..., g - 1$, then the character table of C is the matrix (χ_s^r) where

$$\chi_s^r = \chi^{(r)}(w^s) = w^{rs} = e^{2\pi i rs/g},\ r, s = 0, 1, 2, 3, ..., g-1.$$

The fact that χ^r is infact a linear character of G is clear from the equation

$$\chi^{(r)}(w^s) \cdot \chi^{(r)}(w^t) = w^{rs} \cdot w^{rt} = w^{r(s+t)} = \chi^r(w^{s+t})$$

$r, s = 0, 1, 2, ..., g-1.$

Here we denote the trivial character by $\chi^{(0)}$

Information about the structure of the group is more easily available from the character table. For example, the order g of the group G is:

$$g = n_1^2 + n_2^2 + ... + n_k^2 = \text{sum of the entries of the first column}$$

If the value $\chi(e) = 1$ for all characters χ of G then G is an abelian group and conversely if G is abelian their $\chi(e) = 1$ for all characters χ.

16.6.3 Illustrations

1. Let $G = \langle a : a^3 = 1 \rangle$. Then there are three conjugacy classes and consequently three irreducible representations, all of degree 1. The

corresponding characters are all linear. So the character table of C is determined by the matrix $(x_s^r) = (e^{2\pi i rs/3})$ r, s = 0, 1, 2.

	C_0	C_1	C_2
$\chi^{(0)}$	1	1	1
$\chi^{(1)}$	1	w	w^2
$\chi^{(2)}$	1	w^2	w

2. Consider the group

$$G = < a, b : a^3 = b^2 = (ab)^2 = 1 >$$

which is the symmetric group of degree 3. The conjugacy classes of G are

$$C_1 = \{1\}, C_2 = \{a, a^3\}, C_3 = \{b, ab, a^2b\}.$$

If h_i denotes the number of elements in the conjugacy class C_i, then

$$h_1 = 1, h_2 = 2, h_3 = 3.$$

Also there are three (equal to the number of conjugacy, classes) irreducible representations of G. Let n_1, n_2, n_3 be the degrees of these representations. Then, as remarked earlier, $n_1 = 1$ and

$$1 + n_2^2 + n_3^2 = 6$$

so that $n_2 = 1$, $n_3 = 2$.

The formal sums of all elements in the conjugacy classes are

$$S_1 = \sum_{x \in C_1} x = 1, S_2 = a + a^2, S_3 = b + ab + a^2b$$

The expressions $S_i S_j$, as the linear combinations of S_1, S_2, S_3, are

$$S_1 S_1 = 1 = S_1, S_1 S_2 = S_2, S_1 S_3 = S_3.$$

Thus

$$\begin{aligned} S_1S_1 &= 1.S_1 + 0.S_2 + 0.S_3 \\ S_1S_2 &= 0.S_1 + 1.S_2 + 0.S_3 \\ S_1S_3 &= 0.S_1 + 0.S_2 + 1.S_3 \end{aligned} \qquad 16.6.3\ (1)$$

so that $A_1 = I_3$

Next

$$\begin{aligned} S_2S_1 &= S_2 = 0S_1 + 1S_2 + 0S_3 \\ S_2S_2 &= (a + a^2)(a + a^2) \\ &= 2 + a + a^2 \\ &= 2S_1 + S_2 \end{aligned}$$

$$= 2S_1 + S_2 + 0S_3$$

$$S_2S_3 = (a + a^2)\,(b + ab + a^2b)$$

$$= 2b + 2ab + 2a^2b$$

$$= 2S_3$$

$$= 0.S_1 + 0.S_2 + 2.S_3 \qquad 16.6.3\ (2)$$

Lastly

$$S_3S_1 = S_3$$

$$= 0.S_1 + 0.S_2 + 1.S_3,$$

$$S_3S_2 = 2S_3,$$

$$= 0.S_1 + 0.S_2 + 2.S_3$$

$$S_3S_3 = (b + ab\ a^2b)\,(b + ab + a^2b)$$

$$= 3 + 3(a + a^2)$$

$$= 3S_1 + 3S_2$$

$$= 3.S_1 + 3.S_2 + 0.S_3 \qquad 16.6.3\ (3)$$

Thus, from the equations in 16.6.3 (1) and in 16.6.3 (2), we have

$$A_1 = I_3,\ A_2 = \begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},\ A_3 = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 3 \\ 1 & 2 & 0 \end{pmatrix}$$

Here we have taken the columns of A_1, A_2 and A_3 as the coefficients as the S_1, S_2 and S_3 in the systems 16.6.3 (1), 16.6.3 (2) and 16.6.3 (3).

The characteristic roots of A_1, A_2, A_3 are

$$(w^1{}_1, w^2{}_1, w^3{}_1) = (1, 1, 1)$$

$$(w^1{}_2, w^2{}_2, w^3{}_2) = (2, 2, 1)$$

$$(w^1{}_3, w^2{}_3, w^3{}_3) = (3, -3, 0)$$

So, as the order n of G is 6, using the equation $w_j^i = h_j\,\chi_j^i / n_i$, we have

$$1 = w^1{}_1 = h_1 \frac{\chi_1{}^1}{n_1}, \text{ that is } \chi^1{}_1 = 1$$

$$1 = w^2{}_1 = h_1 \frac{\chi^2{}_1}{n_2}, \text{ that is } \chi^2{}_1 = 1$$

$$1 = w^3{}_1 = h_1 \frac{\chi^3{}_1}{n_3}, \text{ that is } \chi^3{}_1 = 2$$

Similarly $\chi^1{}_2 = 1,\ \chi^2{}_2 = 1,\ \chi^3{}_2 = -1$

$$\chi^1{}_3 = 1, \chi^2{}_3 = -1, \chi^3{}_3 = 0$$

So the character table of G is

	C_1	C_2	C_3
$\chi^{(1)}$	1	1	1
$\chi^{(2)}$	1	1	−1
$\chi^{(3)}$	2	−1	0

It may be remarked that two non-isomorphic groups may have the same character table. For example, the dihedral group D_4 and the quaternion group, both of order 8, are non-isomorphic but both have the same character table.

16.7. LIFTED CHARACTERS

Suppose that G is a group of order g and N is a normal subgroup of G.

Let $\rho_0 : G/N \to GL(n, F)$ be a representation of G/N. Then

$$\rho_0(xN) \cdot \rho_0(yN) = \rho_0(xyN)$$

for all $x, y \in G$ and

$$\rho_0(N) = I_n.$$

Let χ_0 be the character of ρ_0, that is,

$$\chi_0(xN) = \text{tr } \rho_0(xN), x \in G.$$

Define a mapping $\rho : G \to GL(n, F)$ by:

$$\rho(x) = \rho_0(xN), \text{ for all } x \in G.$$

Then ρ is a representation because,

$$\begin{aligned}\rho(xy) = \rho_0(xyN) &= \rho_0(xN) \cdot yN) \\ &= \rho_0(xN)\, \rho_0(yN) \\ &= \rho(x)\, \rho(y)\end{aligned}$$

Also

$$\chi_\rho(x) = \chi_0(xN),$$

for $x \in G$, defines the character of ρ.

Since the matrices $\rho(x)$ and $\rho_0(xN)$ are the same, ρ is reducible or not according as ρ_0 is reducible or not.

The representation ρ is called a representation of G *lifted* from the representation ρ_0 of G/N while the character χ_ρ is called the *lifted character* of ρ.

If $\rho : G \to GL(n, F)$ is a representation of G with identity e and $K = \text{Ker}\ \rho$, then, for any $x \in K$, $\rho(x) = I_n$. Hence

$$\chi_\rho(x) = n = \chi_\rho(e)$$

for all $x \in K$.

Conversely, suppose that, for a finite group G and a representation ρ of G into GL(n, F),

$$\chi_\rho(x) = \chi_\rho(e) \qquad 16.7.1\ (1)$$

for some $x \in G$. Since G is finite, $\rho(x)$ is an element of finite order in GL(n, F). The cyclic group $<\rho(x)>$ generated by $\rho(x)$ is a finite abelian group of matrices and so is completely reducible. Each irreducible component of ρ restricted to the cyclic-group generated by x is of degree 1. So $\rho(x)$ is diagonalisable in the form

$$\text{diag}\ (w_1, w_2, ..., w_n)$$

where $w_1, w_2, ..., w_n$ are the nth roots of unity. Thus

$$\chi_\rho(x) = w_1 + w_2 + ... + w_n = n,$$

from 16.7.1 (1). But

$$n = |w_1 + w_2 + ... + w_n| \leq |w_1| + |w_2| + ... + |w_n| = n$$

and the equality holds only if $w_1 = w_2 = ... = w_n = 1$. But then $\rho(x)$ is equivalent to the identity matrix and therefor $\rho(x) = I_n$. That is $x \in \ker \rho$.

We therefore, have:

16.7.1 Theorem: Suppose that G is a finite group and ρ is a representation of G of degree n with character χ_ρ. Then

$$\chi_\rho(x) = \chi_\rho(e)$$

if and only if $x \in \ker \rho$.

Recall that the character of a one-dimensional representation is called a linear character and that all characters of an abelian group are linear. If χ is a character of an abelian group A then, since $\chi(a)$, $a \in A$, is a field element,

$$\chi(ab) = \chi(a)\,\chi(b)$$
$$= \chi(b)\,\chi(a)$$

for all $a, b \in A$.

If G is an arbitrary finite group then the number of linear characters of G are given by following theorem:

16.7.2 Theorem: Let G be a group and G′ its commutator subgroup. Then there is a one-one correspondence between the linear characters of G and of the quotient group G/G′.

The corresponding characters have the same value.

Moreover, the number of such characters is the index of G′ in G.

Proof: The characters of G/G′ are all linear because G/G′ is abelian. Let χ_0 be a linear character of G/G′. Define a mapping $\chi : G \to F$ by

$$\chi(x) = \chi_0(xG'), x \in G \qquad 16.7.2\ (1)$$

It is easily seen that χ is a character of G. Since χ_0 is linear, χ is also linear on G.

Conversely, suppose that χ is a linear character on G. Consider the mapping $\chi_0 : G/G' \to F$, defined by:

$$\chi_0(xG') = \chi(x), x \in G. \qquad 16.7.2\ (1')$$

We first show that χ_0 is well-defined. Let $x' \in xG'$. Then $x' = xq$ for some $q \in G'$ and

$$\begin{aligned}\chi(x') = \chi_0(x'G') &= \chi_0(xG') \\ &= \chi(xq) \\ &= \chi(x)\,\chi(q).\end{aligned}$$

But, for any commutator $[g_1, g_2] \in G'$,

$$\begin{aligned}\chi([g_1, g_2]) &= \chi(g_1\, g_2\, g_1^{-1}\, g_2^{-1}) \\ &= \chi(g_1)\,\chi(g_2)\,\chi(g_1)^{-1}\,\chi(g_2)^{-1} \\ &= 1\end{aligned}$$

because linear characters commute. Hence $\chi(q) = 1$ and

$$\chi_0(x'G') = \chi(x') = \chi_0(xG') = \chi(x)$$

so that χ_0 is well-defined.

Since χ is linear on G, χ_0 is a linear character of G/G′.

Thus to every linear character of G there corresponds a linear character of G/G′.

Hence there is a one-one correspondence between the linear characters of G and those of G/G′ and equation 16.7.2 (1) or 16.7.2 (1′) shows that the corresponding linear characters have the same value.

Next, since G/G′ is abelian, all its characters are linear and their number equals the order of G/G′, that is, the index of G′ in G. Hence the theorem.

In this last paragraph we mention some of the applications of characters.

1. The character table of a finite group G indicates the presence of normal subgroups of G. Thus, if χ_ρ is the character of G afforded by a representation ρ and

$$\chi_\rho(x) = \chi_\rho(e)$$

for some $x \in G$ then, as shown earlier in Theorem 16.7.1, $x \in \ker \rho$ and all such elements form a normal subgroup.

2. The character table helps one to detect whether or not a certain finite group is simple or not.

This is seen from the fact that the character table of simple groups are such that, for every non-linear irreducible character $\chi^{(i)}$,

$$\chi^{(i)}(g) \neq \chi^{(i)}(e)$$

for any non-trivial $g \in G$.

For if G is simple then G has no proper normal subgroup so that

$$\chi^{(i)}(g) \neq \chi^{(i)}(e)$$

(otherwise $e \neq g \in \ker \rho$ for some representation ρ and $\ker \rho$ would be a proper normal subgroup).

Conversely if, for every non-linear irreducible character $\chi^{(i)}$,

$$\chi^{(i)}(g) = \chi^{(i)}(e)$$

for any $g \in G$ and N is a proper normal subgroup of G then consider an irreducible representation ρ_0 of G/N of degree n.

Define a mapping $\rho : G \to GL(n, F)$ by

$$\rho(x) = \rho_0(xN), x \in G.$$

Then ρ is a representation of G. Since both G and G/N are represented by the same matrices, ρ is irreducible. Also ker ρ contains N. However, for every $x \in \ker \rho$, $x \neq e$, $\chi(x) = \chi(e)$, a contradiction. Here G has no normal subgroups.

3. Theory of characters has been used to prove some important results about finite groups. For example, Burnside's theorem about the solvability of a group of order $p^\alpha q^\beta$, p, q distinct primes, was proved by using characters. The problem of giving a group theoretic proof remained open for more than sixty years. Such a proof was given by J.G. Thompson in 1970.

EXERCISES

1. Let $(R, +)$ be the additive group of real numbers. Show that the mapping $\rho : R \to GL(2, R)$ defined by:

$$\rho(r) = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}, \quad r \in R,$$

is a faithful representation of R.

2. Show that the mapping $\rho : C_4 \to GL(2, R)$, where $C_4 = < x : x^4 = 1 >$, defined by

$$\rho(x) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

is a faithful irreducible representation of C_4. Show that ρ is irreducible.

[Hint:: An irreducible representation of C_4 must be one dimensional. The only one-dimensional faithful representation of C_4 is $\rho' : C_4 \to GL(1, \mathbf{C})$, $\mathbf{C}$, the complex field, given by $x \to i$, $i^4 = 1$, and no such representation exits over R.]

3. Show that the matrices

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and } b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate the dihedral group of order 8. Write down all its elements.

4. Let $D_4 = < a, b : a^4 = b^2 = (ab)^2 = 1 >$ be the dihedral group of order 8. Show that the mapping $\rho : D_4 \to GL(\mathbf{V})$, where $\mathbf{V}$ is a two dimensional vector space, given by

$$\rho(a) = T_a, \rho(b) = T_b,$$

where $T_a, T_b : \mathbf{V} \to \mathbf{V}$, are defined by

$$T_a(x, y) = (-y, x), T_b(x, y) = (y, x),$$

is a faithful representation of D_4.

[Hint. Here the matrices of the linear transformations T_a, T_b are

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

of order 4 and 2 respectively.

5. The representation $\rho : \mathbf{R} \to GL(2, \mathbf{R})$ of $\mathbf{R}$ given by

$$\rho(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, x \in \mathbf{R}$$

is two dimensional. Is this a reducible representation? Explain.

6. Let S_3 be the symmetric group of degree 3. Show that the subspace space

$$U = \{\mathbf{u} = (z_1, z_2, z_3) : \mathbf{u} \in \mathbf{C}^3, z_1 + z_2 + z_3 = 0\}$$

is an S_3 – invariant subspace of $\mathbf{C}^3$ and is a two dimensional irreducible representation space of S_3.

7. Write all the irreducible representations of degree 1 and 2 of the dihedral group

$$D_4 < a, b : a^4 = b^2 = (ab)^2 = 1$$

of order 8.

[Hint: The only irreducible representations of D_4 of degree 1 and of degree 2 are the following ones.

(*i*) The trivial representation $\rho : x \to 1, x \in D_4$. and

(*ii*) The two dimensional rep[illegible] $\rho : D_4 \to GL(2, \mathbf{R})$ defined by

$$\rho(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \rho(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

8. Consider the symmetric group

$$S_3 = <a, b : a^2 = b^2 = (ab)^3 = 1>$$

of degree 3. Take a mapping $\rho : S_3 \to GL(2, C)$ mapping a and b to

$$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

respectively. Show that ρ is a faithful representation of S_3 by proving that $\rho(a), \rho(b)$ generate a group isomorphic to S_3.

9. If TL(n, F) and STL(n, F) denote the (upper) triangular and special (upper) triangular groups of degree n over G respectively, show that the commutator subgroup of TL(n, F) is a subgroup of STL(n, F) while STL(n, F) is nilpotent of class n – 1.

10. Show that the commutator subgroup of GL(n, F) is SL(n, F).

11. Let G be an irreducible subgroup of GL(n, F) and A an abelian normal subgroup of G. Show that A is conjugate to a diagonal subgroup of GL(n, F).

12. Show that the symmetric group S_n of degree n has exactly two linear characters.
(Hint : Here the Commutator subgroup of S_n is A_n which has index 2 in S_n).

13. Prove Burnside's theorem : A group of order $p^\alpha q^\beta$, p and q distinct primes, is solvable.

14. Show that the numbers $h_i \chi_j^i / n_i$, i, j = 1, 2, ..., k are algebraic integers. (A root of any polynomial equation of) degree n with integer coefficients is called an *algebraic integer*.
Here, for any $x \in C_j$, $<\rho(x)>$ is completely reducible and so $\rho(x)$ is diagonisable. Thus $\chi_\rho(x) = \text{tr } \rho(x)$, as the sum of diagonal entries which are algebraic integers, is an algebraic integer].

15. Show that the non-isomorphic groups D_4 and Q have the same character table. Here D_4 is the dihedral group of order 8 and Q is the group of quaternions of order 8.

INDEX

abelian group, 65
accessible, 299
addition, 48
adjacency matrix, 24
algebra homomorphism, 398
algebraic integer, 426
algebraic operation, 47
algebraically closed field, 409
alternating group, 222
amalgam, 361
amalgamated subgroup, 361
anti-symmetric relation, 19
ascending normal chain, 305
ascending sequence of subgroups, 230
associates, 345
associative algebraic operation, 51
associative law, 9
automorphism, 165
base group, 383
bijective mapping, 32
binary operation, 47
binary relation, 47
block, 238
canonical homomorphism, 161
cardinal number, 32
cartesian n-space, 13
cartesian power, 13, 380
cartesian product, 12
cartesian product of groups, 379
Caley's Theorem, 80
Cauchy Theorem, 246
Cauchy Theorem (non-abelian case), 247
algebraic operation table, 55
centralizer of an element, 132
central series, 321
centralizer of a subset, 131
centre of a group, 133
centre of a group algebra, 394
chain, 25
character of a group, 411
character of a representation, 411
character table, 414, 416
characteristic of a field, 403
characteristically simple group, 178, 311
characteristic mapping, 44
chief factor, 310
chief series, 309
class of conjugate elements, 135
class equation, 137
class function, 411
closed under algebraic operation, 47
code, 106
code words, 106
commutative group, 65
commutative algebraic operation, 47
commutative diagram, 34
commutative law, 9
commutator of elements, 173
commutator subgroup, 175
comparable sets, 25

complete wreath product, 290
completely reducible group, 393
completely reducible representation, 393, 401
complex in a group, 113
complement of a binary relation, 18
complement of a group, 203
complement of a set, 6
component of a Cartesian product, 385
components (ordered pair), 12
composition length, 304
composition series, 302
congruence relation, 118
conjugacy class, 138, 397
conjugate subgroup, 138
conjugate element, 138
conjugate of a permutation, 217
conjugation, 158, 195
connected elements, 234
constant mapping, 29
constituents of an amalgam, 363
constituents of a representation, 413
convolution, 396
coordinate or component subgroup, 380, 381
coordinates or components, 12
coset representative of a subgroup, 366
coset space, 265
counting formula, 282
cycle, 214
cyclic group, 88
cyclic permutation, 214
cyclic subgroup, 88
cyclically reduced word, 348
decomposable group, 193, 393
decomposable representation, 401
defining relation, 84, 350
degree of a character, 411
degree of symmetric group, 210
derived group, 175, 330
descending normal chain, 305
diagonal of a cartesian power, 12
diagonal subgroup of GL(n, F), 388
dihedral group, 86, 101
dihedral group of order 2n, 105
dimension of a representation, 391
direct factor of a group, 187, 189
direct factor of direct product, 187
direct power, 380
direct product of groups, 187
direct product of subgroups, 189
disjoint sets, 6
distributive law, 9
divisible group, 54
domain, 17
domain of operators, 177
double coset, 139
doubly transitive, 274
element of a set, 1
embedding, 77
empty relation, 17
empty set, 3
empty word, 345
endomorphism, 165

epic, 77
epimorphism, 77, 158
equal mappings, 28
equal sets, 3
equal words, 346
equivalence class, 20
equivalence relation, 20, 272, 393
equivalent set, 32
equinumerous, 32
equipotent, 32
equivalent representations, 392, 402
even permutation, 221
exponent of a group, 87, 93
extension of a group, 195
extension of a mapping, 33
factor group, 156
factor representation, 394
factor set, 20
faithful representation, 233, 390, 398
fatihful group action, 271
Format's theorem, 121
fiber over an element, 36
finite cyclic group, 88
finite group, 65
finite p-group, 137, 246
finite set, 32
finitely generated group, 83
finitely presented group, 84
finitely serial subgroup, 299
finitary permutation, 209
first derived group, 175
first isomorphism theorem, 160
Fitting subgroup, 342
fixed point subgroup, 184
Frattini subgroup, 334
free basis, 347
free factors, 353
free group, 347
free product of groups, 353
free rank, 347
free system of generators, 347
freely reduced word, 345
full relation, 17
fully invariant, 177
function, 27
fundamental theorem of homomorphism, 158
FG-modules, 399
G-set, 272
G-stable subset, 273
G-invariant, 393
G-set homomorphism, 281
G-transitive, 274
Group action
  -on sets, 363
  -on polynomials, 267
  -on cosets, 264
  -on geometrical objects, 268
  -as left multiplication, 263
  -as conjugation by elements, 265
  -as subgroup conjugation, 266
  -by automorphisms, 267
  -by inner automorphism, 266
group of quaternians, 70
general linear group, 382, 387
general linear group over a ring, 382
general product of group, 203

generalized direct product, 376
generalized direct factors, 377
generalized free product, 363
generators, 88
greatest element of a set, 26
group (under addition), 65
group (under multiplication), 65
group algebra, 395, 396
group axioms, 64
group of mobiüs transformations, 70
groups of permutation, 209
group with trivial centre, 133
groupoid, 52
half transitive groups, 236
Hall subgroup, 260
Hamiltonian groups, 150
Hasse diagram, 25
holomorph of a group, 203
homomorphic image, 79
homomorphism, 77
idempotent element, 65
idempotent laws, 8
identical relation, 85
identity, 53
identity element, 53
identity mapping, 28
identity relation, 18, 28
identity subgroup, 72
image, 27
improper subset, 4
inclusion mapping, 34
inclusion relation, 3
inclusion symbol, 3
indecomposable group, 193, 394
indecomposable representation, 394, 401
index of a subgroup, 118
indexing family, 5
indexing set, 6
induced algebraic operation, 49
infinite cyclic group, 88
infinite dihedral group, 181
infinite group, 65
infinite p-group, 305
infinite set, 32
injective mapping, 31
inner automorphism, 166
integral representation, 391
intersection of sets, 5
intersection of subgroups, 73
intransitive group action, 273
intransitive permutation group, 236
invariant element, 135
invariant series, 338
invariant subgroup, 150
inverse image set, 35
inverse of a binary relation, 18
inverse of a mapping, 35
inverse of an element, 53, 63
involution, 75
irreducible character, 412
irreducible group, 393
irreducible representation, 393
irreducible system of generators, 83
isomorphic G-sets, 281
isomorphic normal series, 297

isomorphism, 57, 77
isotropy group, 277
Jordan-holder theorem, 303
k-transitive, 238
kernel of a group action, 263
kernel of a homomorphism, 158
k-ply transitive, 273
Klein's four group, 86, 99
Kurosch subgroup theorem, 358
Lagrange's theorem, 119
lattice, 75
law is a group, 85
least element, 26
left coset decomposition, 116
left inverse, 53
left inverse of a mapping, 37
left regular representation, 398
left unit, 53
length of a cycle, 215
length of an element, 353
length of an orbit, 234
length of series, 297
lifted character, 420, 421
linear associative algebra, 394
linear character, 412
linear group, 390
linear relation, 25
Linear representation, 390
locally cyclic group, 97
locally finite group, 97
locally infinite group, 97, 349
loop, 55
lower central series, 323
Mashke's Theorem, 403, 406, 408
mapping, 27
mathematical induction, 26
matrix group of dimension n, 390
matrix representation of a group, 390, 398
maximal condition, 342
maximal subgroup, 182
membership, relation 3
metabelian group, 176, 313
minimal normal subgroup, 342
module over a ring, 398
modular representation theory, 391
module, 398
monic, 677
monoid, 53
monomial matrix, 389
monomorphism, 77
Monster, 149
n-ary algebraic operation, 47
natural homomorphism, 161
nil radical, 342
nilpotency class, 324
nilpotent group, 322, 324
nilpotent group of class k, 324
non-trivial action of permutation, 213
non-restricted wreath product, 291
non-standard unrestricted wreath-product, 383
normal chain condition, 306
normal closure, 300
normal factors, 297
normal form of an element, 353, 367
normal product of groups, 197

normal series, 295
normal subgroup, 150
normaliser condition, 342
normaliser of a subset, 130
normaliser of an element, 131
nth term of a sequence, 30
null set, 3
nullery relation, 17
neutral element, 53
odd permutation, 220, 221
projective space, 22
one-one correspondence, 32
one-one mapping, 31
onto mapping, 30
optic group, 101
orbits, 234, 273
orbit-stabilizer theorem, 282
order of permutation, 219
order relation, 24
ordered pair, 11, 27
ordinal number, 32
ordinary free product, 353
ordinary representation, 391
ordinary subtraction, 49
outer automorphism, 167
overlapping, 6
p-subgroup, 246
partial complement of a subgroup, 335
partial order, 24
partially ordered set, 25
partition of a set, 6, 20
periodic group, 66, 259
permutable complexes, 113
permutation group action, 264
permutation matrix, 389
permutational product of an amalgam, 372
permutational representation, 233
permutational wreath multiplication, 380
phi orbit, 214
pi group, 259
pi subgroup, 259
pigeonhole principle, 32
Poincare's theorem, 126
polyhedral group, 370
power set, 4, 26
presentation, 84,350
primitive permutation groups, 239
principal factor, 310
principal series, 309
principle of finite induction, 26
product of relations, 18
product of mappings, 33
projection mappings, 29, 79
projective special linear group, 389
proper subgroup, 72
proper subset, 4
Prufer's p-group, 87, 305
quasi group, 55
quaternary relation, 18, 47
quaternions, 70
quotient of a group, 156
quotient set, 20
R-modular (left), 398
R-relative, 17
relator, 84
range, 17

reduced amalgam, 364
reducible group, 393
reducible representation, 393, 401
refinement, 296
reflections, 98
reflexive relation, 18
regular group action, 265
regular permutation group, 237
regular reducible representation, 401
regular representation, 213
relation, 17
relator, 84
representation module, 401
representation of a group algebra, 398, 401
representation space, 391
representative element, 20, 116
restricted alternating group, 231
restricted direct product, 380
prestricted symmetric group, 209
restriction of a mapping, 33
right coset, 116
right coset decomposition, 116
right inverse, 53
right inverse of a mapping, 37
right regular representation, 398
right transversal, 116
right unit, 53
rotations, 98
Russell's paradox, 15
Ω-admissible subgroup, 177
standard wreath multiplication, 384
scalar matrix, 388
Schreir's refinement theorem, 297
Schur's lemma, 408
second isomorphism theorem, 162
self-conjugate element, 135
self-conjugate subgroup, 150
semi-direct product, 197
semi-group, 57
sequence, 30
sequence of real numbers, 30
set, 1
set of imprimitivity, 238
simple groups, 150
singleton set, 8
solution set, 2
solvability length, 313
solvable group, 176, 313
special linear group, 388
special triangular group, 388
split extension, 203
sporadic simple group, 149
stabilizer subgroup, 234, 277
stability subgroup, 234
standard restricted wreath product, 384
standard unrestricted wreath product, 383
subalgebra, 395
subgroup, 71
subgroup generated by a complex, 83
subgroup of finite index, 118
subgroup of infinite index, 118
subinvariant series, 295
subinvariant subgroup, 299

submodule, 399
subnormal subgroup, 299
subnormal factors, 297
subnormal series, 295
subnormal subgroup, 299
subset, 3
sum, 48
super set, 3
super solvable group, 238
surjective mapping, 30
Sylow p-subgroups, 248
Sylow π-subgroup, 259
Sylow's 1st theorem, 248
Sylow's 2nd theorem, 249
symmetric difference, 7
symmetric group, 97, 209
symmetric relation, 19
symmetry, 97
system of defining relations, 84
system of generators, 83
system of generators of S_n, 225
ternary relation, 18
ternary operation, 47
third isomorphism theorem, 163
torsion free group, 66
totally ordered set, 25
transform of an element, 134
transformation group, 263
transitive action, 273
transitivity classes, 273
transitive permutation group, 236
transitive relation, 19
transposition, 220
transversal, 366
trivial action of permutation, 213
trivial block, 238
trivial subgroup, 72
type of a permutation, 216
types of binary relations, 18
types of mappings, 30
unary, 47
union of sets, 5
unit element, 53
unit subgroup, 72
unrestricted direct product, 380
unrestricted symmetric group, 209
unrestricted wreath product, 383
upper central series, 331
usual addition of vectors, 48
Venn diagram, 7
vacous, 3
variety, 85
variety of abelain groups, 87
variety of groups, 85
-of exponent n, 87, 93
vector product, 50
von Dyck's theorem, 351
well-ordering principle, 26
well ordered set, 26
Wielandt's theorem, 351
word, 83, 345
wreath product, 381
Zassanhaus butterfly lemma, 293

BIBLIOGRAPHY

1. Alperin, J.L. and Rowen, B. Bel:
Groups and Representations, Graduate Texts in Math. Springer-Verlag, N.Y. Inc. (1995).

2. Bass, H.: *Finitely generated subgroups of GL_2 (**C**).* in "The Smith Conjecture", Wiley, New York, 127-136 (1984).

3. Baumslag, Gilbert; Shalen, P.B.:
Amalgamated Products and Finitely Presented Groups. Comment. Math. Helv. **65**, 243-254 (1990).

4. Baumslag, Gilbert; Morgan, J.W.:
Shalen, P.B.: *Generalized Triangle Groups*. Math. Proc. Cambridge Philos. Soc. **102**(1), 25-31 (1987).

5. Benyash-Krivets, V.V.:
On Decomposing Some Groups into Free Products with Amalgamations, Dokl. Akad. Nauk. Belarus, **41:6** 1-4. (1997).

6. Benyash-Krivets, V.V.:
Decomposing One Relator Products of Cyclic Groups into Free Products with Amalgamations, Sbornik: Mathematics, **189:8** 1125-1137 (1998).

7. Benyash-Krivets, V.V.:
Decomposing Some Finitely Generated Groups into Free Products with Amalgamations, (Thesis).

8. Benyash-Krivets, V.V., and Chernousov, V.I.:
Representation Varieties of the Fundamental Groups of Compact Non-orientable Surfaces. Sorbornik: Mathematics, **188:7** 1997-1039 (1997).

9. Burrow, M.: Representation Theory of Finite Groups. Academic Press, (1965).

10. Burnside, W.: The Theory of Groups of Finite Order (2nd Ed.) Dover Publications Inc. New York, (1955).

11. Collins, M.J.: *Representations and Characters of Finite Groups*. Cambridge University Press, (1990).

12. Coxeter, H.S.M., and Moser, W.O.J.: *Generators and Relations for Discrete Groups*. Ergeb. Math. Grenzgebiette. Springer-Verlag, Berlin-Heidelberg-New York, (1972).

13. Culler, M., and Shalen, P.: *Varieties of Group Representations and Splittings of 3 Manifolds*. Ann. of Math. **117**, 109-147 (1983).

14. Curtis, C.W. and Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Interscience, New York, (1962).

15. Dicks, W., Dunwoody, M.J.: *Groups Acting on Graphs*. Cambridge University Press, (1989).

16. Dixon, J.D.: Structure of Linear Groups: Von Nostrand Reinhold Co. New York, (1971).

17. Dixon, J.D.: Problems in Group Theory. Dover Publications Inc. New York, (1973).

18. Dornhoff, L.: Group Representation Theory, Vol. 1. Marccel Dekker, New York, (1971).

19. Dunwoody, M.J. and Sageev, M.: *Splitting of Certain Fuchsian Groups*. Proc. Amer. Math. Soc. **125;7** 1953-1954 (1997).

20. Feit, W., and Thomson, GJ.:
Solvability of Groups of Odd Order. Pacific J. Math. *13*, 775-1029, (1963).

21. Feit, Walter.: *The Representations of Finite Groups*. North Holland Publishing Company, (1982).

22. Fine, Benjamin; Levin, Frank, and Rosenberger, Gerhard.:
Free Groups and Decompositions of One Relator Products of Cyclics I. The Tits Alternative. Arch. Math. (Bassel), **50(2)**:97 -109 (1998).

23. Fine, Benjamin; Levin, Frank, and Rosenberger, Gerhar:
Free Groups and Decompositions of One Relator Products of Cyclics. Part II. Normal Torsion Free Subgroups and FPA Decompositions. J. of Indian Math. Soc. **49**. 237-247 (1985).

24. Fulton, W; Harris Joe:
Representation Theory, A First Course, Springer, (N.Y) (1991).

25. Hall, M. Jr.: The Theory of Groups. The Macmillan Co. New York, (1959).

26. Hall, P.: A Contribution to the Theory of Groups of Prime Power Order. Proc. London Math. Soc. *36*, 29-95, (1953).

27. Herstein, I.N.: Topics in Algebra 2nd Ed. Wiley, N.Y, (1975).

28. Horowitz, Robert D.:
Characters of Free Groups Represented in the Two Dimensional Special Linear Group,. Comm. Pure Appl. Math., **25**. 635-649 (1972).

29. Howie, James: *Free Subgroups in Groups of Small Deficiency.* J. Group Theory. **1(1)**: 95-112 (1998).

30. Issacs, I.M.: *Character Theory of Finite Groups.* Academic Press, (1976). Reprinted by Dover, (1994).

31. Jacobson, Nathan; W.H. Freeman: *Algebra II* (1989).

32. Johnson, D.L.: *Presentations of Groups.* London Math. Soc. Graduate Student Texts 15. Cambridge University Press, 1990.

33. Jacobson, Nathan: *Algebra I.* W.H. Freeman, (1985).

34. James, Gordon: Liebeck, Martin. : *Representations and Characters of Finite Groups* (1993).

35. Lang, Serge: *Algebra*, Addison-Wesley, (1993).

36. Leadermann, W.: Introduction to Group Characters. Cambridge University Press, Cambridge, (1977).

37. Levin, F. : Factor Groups of the Modular Group. J. London Math. Soc. *43*, 195-203, (1968).

38. Lubotzky, A., and Magid A.: *Varieties of Representations of Finitely Generated Groups.* Memoirs AMS. **58**, 1-116 (1985).

39. Lyndon, R.C., Schupp, P. E.: *Combinatorial Group Theory.* Springer-Verlag, Berlin-Heidelberg-New York, (1977).

40. MacDonald, I.D.: The Theory of Groups. Oxford University Press, New York, (1968).

41. Magnus, W. Karrass A. and Solitar, D. : Combinatorial Group Theory. Interscience J. Willey & Sons, New York, (1966).

42. Magnus, W.: *The Uses of 2 by 2 Matrices in Combinational Group Theory.* Result der Math. **4**: **2**, 171-192 (1981).

43. Majeed, A.: Existence Theorems for Generalised Free Products of Groups I. Bull, Instit. Polite. Din I.A.S.I (S.N.) Tom XIV(XVIII), 23-26, (1968).

44. Majeed, A.: On the embeddable finite amalgams of groups. Glasgow Math. J. *13* 142-143, (1972).

45. Majeed A.: On the range of finite embeddings of a finite amalgam. Glasgow Math. J. *13*, 41-46 (1972).

46. Majeed, A.: Some Properties of Permutational Products of Groups. P.U.J. Math. *2*, 63-89, (1969).

47. Mumford, D.: *Geometric Invariant Theory*. Springer-Verlag, Berlin-Heidelberg-New York, (1967).

48. Neuman, B.H.: An Essay on Free Products of Groups with Amalgamations. Phil. Trans. Royal Soc. of London. *246*, 503-554 (1954).

49. Neuman, B.H.: Permutational Products of Groups. J. Austral. Math. Soc. *1*, (299-310), (1961).

50. Neuman, B.H.: Group Constructions. Distinguished Lecturer Series Notes: University of Waterloo, Canada, (1968).

51. Neuman, H.: Generalised Free Products with Amalgamated Subgroups (I). Amer. J. Math. 70, 590-625 (1948).

52. Neuman, H.: Generalised Free Products with Amalgamated Subgroup II. Amer. J. Math. *71*, 491-540 (1949).

53. Neuman, B.H., Hanna Neumann.: Embedding Theorems for Groups. J. London Math. Soc. *34*, 465-479 (1959).

54. Neuman, B.H., Hanna Neumann.: A Remark on Generalised Free Products J. London Math. Soc. *25*, 202-204 (1950).

55. Robinson, Donald. J.S.: *A Course in the Thoery of Groups*. Springer Verlag. (1982). (Reprinted in 1994).

56. Rose, John, S.: *A Course on Group Theory*. Cambridge University Press. (1978). (Reprinted by Dover, (1994)).

57. Rosenberger, Gerhard: *On Free Subgroups of Generalized Triangle Groups*. Algebra i Logica., **28** (2). 227-240, 245 (1989).

58. Rotman, J.J.; *The Thoery of Groups, An Introduction*, 2nd. Ed. Allyn and Bacon, (1973).

59. Rotman, J.J.: *An Introduction to the Theory of Groups*, Springer Verlag, (1995).

60. Schenkman, E.: *Group Theory*, D. Van Nostrand Company, Inc. (1965).

61. Scot, W.R.: *Group Theory*, Prentice-Hall, (1964).

62. Serre, Jean-Pierre: *Linear Representations of Finite Groups;* Springer Verlag, (1977).

63. Sukuki, Michio: *Group Theory I*, Springer-Verlag, (1982).

64. Tang, C.Y.: On Uniqueness of Generalised Direct Decompositions. Pacific J. Math. *23*, 177-182 (1967).

65. Triana, C: *Trace Polynomial for Two Generated Subgroups of* $SL_2(C)$. Proc. Amer. Math. Soc. **79**, 369-372 (1980).

66. Zassenhaus, H.: Theory of Groups. (2nd Ed.) Chelsea, New York, (1958).