

Volume-I

GROUP THEORY

Course Introduction **3**

BLOCK 1 **5**

Introduction to Groups

BLOCK 2 **143**

Normal Subgroups and Group Homomorphisms

Unitised Course Outline

Volume I Group Theory

Block 1 Introduction to Groups

Unit 1: Some Preliminaries

Unit 2: Groups

Unit 3: Subgroups

Unit 4: Cyclic Groups

Block 2 Normal Subgroups and Group Homomorphisms

Unit 5: Lagrange's Theorem

Unit 6: Normal Subgroups

Unit 7: Quotient Groups

Unit 8: Group Homomorphisms

Unit 9: Permutation Groups

Volume II Ring Theory

Block 3 Introduction to Rings

Unit 10: Rings

Unit 11: Subrings

Unit 12: Ideals

Unit 13: Ring Homomorphisms

Block 4 Integral Domains

Unit 14: Integral Domains and Fields

Unit 15: Polynomials Rings

Unit 16: Roots and Factors of Polynomials

January, 2021

© Indira Gandhi National Open University

ISBN-8]-

All right reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the Indira Gandhi National Open University.

Further information on the Indira Gandhi National Open University courses, may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 and IGNOU website www.ignou.ac.in.

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi by Prof. Sujatha Varma, School of Sciences.

COURSE INTRODUCTION

Algebra is a word that you are familiar with. You may also know that it is derived from the Arabic word 'Al-jabr'. Classically, algebra was concerned with obtaining solutions of equations. Then came 'modern algebra', a term used to describe detailed investigations within classical algebra. In Block 1 of the course, Calculus, you have studied some of the concepts of modern algebra – sets and operations on them, functions, a binary operation on a set, an algebraic way of studying plane geometry, properties of complex numbers, what a polynomial over \mathbb{R} is, and solutions of some polynomial equations. In this course, we shall build on this learning, and take you much further.

In this course, we will focus on 'abstract algebra', a generalisation of modern algebra. In **abstract algebra** we study algebraic systems that are defined by axioms alone. These axioms normally evolve from concrete situations. In this course, **comprising four blocks**, you will study three basic algebraic systems, namely, groups, rings and fields.

In Block 1, you will study what a group is, and several examples and properties of this algebraic system. You will study different kinds of groups, with so many differences, and so many similarities! Here you will also study what a subgroup is. The set of integers forms a particular kind of group called a cyclic group. Such a group has many special properties. This is why we will give it special attention in this block.

In Block 2, the focus is on a particular type of group, called a quotient group. Such a group necessitates a particular kind of subgroup, as you will see. You will study such subgroups in some detail too. The real importance of a quotient group shows up in a type of function from one group to another that satisfies the property of 'preserving' the operation of the domain group. The importance of such functions, and their relationship with quotient groups, will be thoroughly discussed in this block too. Finally, you will study sets of bijections from a set to itself, as a detailed case study of the different aspects and properties of groups that you studied in Blocks 1 and 2.

In Block 3, we move the focus to another, but related, algebraic system. This is called a ring. In this block, you will study what a ring is, along with many of its properties. Here you will also study about subrings, and special subrings that allow us to define quotient rings. Finally, in this block, you will study about a special kind of function from one ring to another. As you go through this block, you will see how similar concepts related to rings are to those you studied about groups in the first two blocks.

In Block 4, the focus is on rings that satisfy certain special properties. In particular, you will study another important algebraic system, which is a ring, and yet more than a ring. This is the concept of a field. You will see that the set of real numbers forms a field, as does the set of complex numbers. We go on, in this block, to discuss the properties of the set of polynomials over \mathbb{R} , over \mathbb{C} , or over any field.

You may wonder why you should study this course. As you study the blocks, you will realise that your way of thinking is changing. You will see how the methods of abstract algebra allow us to deal with several similar algebraic systems by just dealing with one representative system. This helps us to think at a macro level about systems, be precise and concise and to understand the structure of several groups or rings more quickly.

There are several practical applications of what you will study in this course. Let us start with some applications of group theory. This theory is used by physicists and chemists in crystallography, spectroscopy, general relativity, solid state physics and the modern theory of elementary particles. In fact, using group theory, scientists predicted

the existence of the Omega minus particles, which were actually identified in 1964, much after the prediction.

Now let us look at some applications of rings and fields. Polynomial rings and matrix rings are used in quantum mechanics. Field theory is being used to construct efficient error detecting and correcting codes in the area of data communications. Of course, finite fields are very useful in statistics too.

Now, a few words about the way you should study the material! **We have presented this course with the assumption that you have already studied the courses 'Calculus' and 'Real Analysis.** Do not simply read the material in these blocks. You must actually **interact** with every line, idea, example and question in it. As you know, whenever we introduce concepts, we give you a lot of concrete examples to help you understand it. We also include a host of exercises to help you strengthen your understanding of the concepts and processes concerned. You must solve every exercise as you come to it, to benefit from it.

Now, a word about the layout of a block. In each block, you will first find a block introduction, followed by a list of symbols that are used in the block. And then come the units of the block. Every unit starts with an introduction, where we also list the precise learning objectives of the unit. Each unit has been divided into sections. Since the material in the different units is heavily interlinked, we will be doing a lot of cross-referencing. For this purpose we will be using **the notation Sec. x.y. to mean Section y of Unit x.** As in your earlier mathematics courses, you will find the examples, exercises and important equations numbered sequentially throughout a unit. Further, the exercises in each unit are interspersed within the text. They are meant to help you check your progress. The solutions, or solution outlines, or answers to the exercises in a unit are given at the end of the unit. **After you finish studying a unit, please go back to the objectives of the unit** (given in the introduction of the unit), **and see if you are confident that you have achieved them.**

As part of the tutorial component, at the end of every block you will find several miscellaneous exercises for you to do. These are based on all the units you would have studied upto that point. Further, we will send you an assignment. It is meant to be a teaching aid, apart from an assessment aid. Your academic counsellor, at the study centre, will assess this, **and return it to you** with suitable detailed remarks.

You may also like to view our **video programme**, "Groups of Symmetries", available in the IGNOU Youtube archives. In it we have tried to concretise the idea of a symmetry of an object, which you will deal with throughout the first two blocks of this course.

Now a word **about the cover.** The painting in it is by a well-known artist. It depicts you, and your peers, moving through the beautiful forest that is Algebra, looking for the beautiful algebraic concepts and processes.

If you feel like reading more than what this course contains, **you may like to consult the following books:**

- i) A First Course in Abstract Algebra, by J. B. Fraleigh, Pearson.
- ii) Contemporary Abstract Algebra, by J. A. Gallian, Narosa.
- iii) Abstract Algebra, by Hodge, Schlicker and Sundstrom, CRC Press.

For any query related to this course you can contact us at directorsos@ignou.ac.in.

Wishing you a happy learning experience!

The Course Team

Block

1**INTRODUCTION TO GROUPS**

Block Introduction	7
Notations and Symbols	8
UNIT 1	9
Some Preliminaries	
UNIT 2	53
Groups	
UNIT 3	93
Subgroups	
UNIT 4	113
Cyclic Groups	
Miscellaneous Examples and Exercises	139

Course Design Committee*

Prof. Rashmi Bhardwaj
G.G.S. Indraprastha University, Delhi

Dr. Sunita Gupta
University of Delhi

Prof. Amber Habib
Shiv Nadar University
Gautam Buddha Nagar

Prof. S. A. Katre
University of Pune

Prof. V. Krishna Kumar
NISER, Bhubaneswar

Dr. Amit Kulshreshtha
IISER, Mohali

Prof. Aparna Mehra
I.I.T., Delhi

Prof. Rahul Roy
Indian Statistical Institute, Delhi

Prof. Meena Sahai
University of Lucknow

Dr. Sachi Srivastava
University of Delhi

Prof. Jugal Verma
I.I.T., Mumbai

Faculty members School of Sciences, IGNOU

Prof. M. S. Nathawat (Director)

Dr. Deepika

Mr. Pawan Kumar

Prof. Poornima Mital

Prof. Parvin Sinclair

Prof. Sujatha Varma

Dr. S. Venkataraman

* The Committee met in August, 2016. The course design is based on the recommendations of the Programme Expert Committee and the UGC-CBCS template.

Block Preparation Team

Prof. Parvin Sinclair (*Editor and Writer*)
School of Sciences
IGNOU

Course Coordinator: Prof. Parvin Sinclair

Acknowledgement:

- i) To **Prof. Meena Sahai** (Retd.), University of Lucknow, and **Dr. Pooja Yadav**, Kamla Nehru College, University of Delhi, for their detailed comments.
- ii) To **Sh. K. Vishwanathan**, Graphic Unit, EMPC, IGNOU, for the cover artwork and design.
- iii) To Sh. S. S. Chauhan, for the line diagrams, and the CRC, of this block.
- iv) Some material of the earlier IGNOU undergraduate course, Abstract Algebra (MTE-06), has been used in this block.

BLOCK INTRODUCTION

A group is an algebraic system consisting of a set, along with one binary operation defined on it. Groups have been studied by mathematicians for over two hundred years. Throughout the nineteenth century, group theory was a study of permutations and substitutions. It slowly evolved into its present abstract form.

Group theory, in its present form, helps in analysing basic mathematical structures. Mathematicians working in a variety of branches of mathematics borrow methods and tools from group theory to make progress in their own field. Not only mathematicians, but chemists and physicists also use group theory to analyse the structures of molecules and crystals, or to study the “solid circuits” of sophisticated electronics. It was a group of algebraic transformations, devised by a Dutch physicist, Lorentz, which Einstein used for analysing Special Relativity. It is the basics of this interesting and useful theory that we want to introduce you to in this block, and in Block 2.

In this block, we will build on your earlier understanding of algebraic objects. Recall that in Block 1 of your first semester course you have studied about sets, functions, complex numbers and polynomials over \mathbb{R} . Further, in Block 1 of your third semester course, you have studied different methods of proof. Now you should do a quick revision of those units before going further.

This block comprises four units. In Unit 1, we will summarise some of the basic ideas concerning properties of divisibility of integers. Then we will introduce you to partitions, and discuss their connect with equivalence relations. Finally, we will introduce you to two new algebraic objects, matrices and permutations. We will also discuss a few basic properties of these objects.

You will begin the study of group theory in Unit 2. In this unit you will see what a group is, and you will study some basic properties of this algebraic system. You will also discover that a lot of familiar sets, like the sets of integers and rational numbers, are groups with respect to addition. Here, we will also introduce you to some groups that you will come across off and on, throughout the course, like the group of integers modulo n , permutation groups, dihedral groups, matrix groups, the group formed by the n th roots of unity, and a group formed by combining two or more groups in an interesting way.

In Unit 3, you will study subsets of groups that are groups in their own right. They are, appropriately, called subgroups. Here you will study properties of subgroups, including the way subgroups behave when set operations are applied on them.

In Unit 4, the last unit of this block, we will focus on a particular kind of group. This is called a cyclic group, for reasons that will become clear to you when you study about them. The set of integers is a typical cyclic group, as you will see. While studying these groups the concept of an order of an element of the underlying set of a group comes into play. You will study this concept in this unit too. Further, you will study a generalisation of the idea of a cyclic subgroup also in this unit.

In the next block, you will go a little deeper into group theory, and you will need everything that you learn in this block. So go through this block carefully. Try every exercise as you come to it, and go further only after solving it.

NOTATIONS AND SYMBOLS (used in Block 1)

Please **review the notations and symbols** given in Block 1 of the courses, Calculus and Real Analysis.

$a \mid b$ ($a \nmid b$)	a divides b (a does not divide b)
(a, b)	the greatest common divisor of a and b
$[a, b]$	the least common multiple of a and b
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$M_{m \times n}(S)$ ($M_n(S)$)	the set of all $m \times n$ matrices ($n \times n$ matrices) over a set S
$\mathbf{0}$ ($\mathbf{0}_{m \times n}$)	the zero matrix of appropriate order (of order $m \times n$)
I_n	the identity matrix of order $n \times n$
$(G, *)$	the group G w.r.t. the operation $*$
$o(G)$	the order of a group G
S_n	the symmetry group on n symbols
D_{2n}	the dihedral group of order $2n$
S^1	the unit circle
Q_8	the group of quaternions
K_4	the Klein 4-group
Z_n	the group of integers modulo n
U_n	the group of n th roots of unity
$(x_1 x_2 \dots x_r)$	a cycle of length r
A^t	the transpose of the matrix A
$\det(A)$, $ A $	the determinant of a square matrix A
S^*	$S \setminus \{0\}$, where S is a set containing 0
$GL_n(\mathbb{R})$	the general linear group of degree n over \mathbb{R}
$SL_n(\mathbb{R})$	the special linear group of degree n over \mathbb{R}
$\wp(S)$	the set of subsets of a set S
$A \Delta B$	$(A \setminus B) \cup (B \setminus A)$
$G_1 \times G_2$	the external direct product of the groups G_1 and G_2
\leq	is a subgroup of
$\leq, <$	is a proper subgroup of
$\not\leq$	is not a subgroup of
$Z(G)$	the centre of the group G
$\langle x \rangle$	the cyclic group generated by an element x
$\langle S \rangle$	the group generated by the set S
$o(x)$	the order of an element x
w.r.t	with respect to
s.t	such that
iff	if and only if

UNIT 1

SOME PRELIMINARIES

Structure	Page Nos.
1.1 Introduction Objectives	9
1.2 Divisibility in \mathbb{Z}	10
1.3 Partitions and Equivalence Relations	20
1.4 Introducing Matrices	24
1.5 Introducing Permutations	38
1.6 Summary	43
1.7 Solutions / Answers	44

1.1 INTRODUCTION

In this unit, the aim is to help you become familiar with some mathematical concepts that you will use off and on in this course. We shall help you recall some aspects of integers that you have studied earlier. We shall also introduce you to the ideas of 'matrix' and 'permutation'.

In this unit, and in the rest of this course, we will often refer to what you have studied about functions and binary operations in Block 1 of the first semester course, Calculus. We will also often refer to Units 1 and 2 of the third semester course 'Real Analysis', directly and indirectly. So please keep these materials handy while you are studying this course.

This unit really begins with Sec.1.2. Here we will discuss various concepts and algorithms related to the divisibility of integers. In particular, you will be studying the Euclidean algorithm for finding the greatest common divisor of two non-zero integers.

You have studied what an equivalence relation is in Calculus. In Sec.1.3, we will take that understanding further, and relate it to the concept of a partition of a set.

In Sec.1.4, we will discuss a concept that you may be familiar with from your studies in school. This is the concept of a matrix over a non-empty set. We will actually focus on matrices over \mathbb{C} , or a subset of \mathbb{C} . Here you will also study some operations on the set of matrices over \mathbb{C} (or a subset of \mathbb{C}).

Finally, in Sec.1.5, we will introduce you to the concept of a permutation of the elements of a set. In particular, we shall discuss the symmetries of a regular planar figure.

We have given below the precise learning expectations around which this unit has been created. If you study the unit carefully, and try your best to solve every exercise as you come to it, you will be able to meet these expectations. Take your own time for doing this, but do it yourself.

Objectives

After studying this unit, you should be able to:

- state, prove and apply the division algorithm for \mathbb{Z} ;
- prove, and use, the theorem that the g.c.d of $a, b \in \mathbb{Z}, a \neq 0$, is of the form $ma + nb$, for some $m, n \in \mathbb{Z}$;
- prove, and apply, the Fundamental Theorem of Arithmetic;
- apply the Euclidean algorithm to find the g.c.d. of any two non-zero integers;
- prove, and apply, the statement that any partition of a non-empty set S defines an equivalence relation on S , and its converse;
- define, and give examples of, matrices over a set and operations on them;
- define, and give examples of, permutations of a set and their composition.

1.2 DIVISIBILITY IN \mathbb{Z}

You have studied, and worked with, integers through most of your schooling, and later. In this section we shall focus on one of the fundamental ideas that you would be quite familiar with, namely, the divisibility of integers. For example, what are the divisors of 30? Why do we say 5 divides 30, and 7 doesn't, in \mathbb{Z} ? Again, does 0 divide every integer? Think about the answers to these questions, while considering the following definition.

Definition: Let $a, b \in \mathbb{Z}, a \neq 0$. We say that **a divides b** if there exists an integer c such that $b = ac$. We write this as $a \mid b$, and read it as ' **a is a divisor (or factor) of b** ', or that ' **b is divisible by a** ', or that ' **b is a multiple of a** '.

If a does not divide b , we write this as $a \nmid b$.

For example, $5 \mid 30$ since there is an integer, 6, such that $30 = 5 \times 6$.

Again, $7 \nmid 30$ since there is no integer x s.t. $30 = 7x$.

Here, you must consider the following important comment about divisors.

Remark 1: For $a, b \in \mathbb{Z}, a \neq 0$, if $a \mid b$, then $\exists c \in \mathbb{Z}$ s.t. $ac = b$. This c is **unique**. This is because if $ac = b$ and $ad = b$ for $c, d \in \mathbb{Z}$, then $ac = ad$. Since $a \neq 0$, this gives us $c = d$. (Actually, you will study more about this in Block 3.)

This leads us to our next comment.

Remark 2: Coming to 0, note that $0 \cdot z = 0 \forall z \in \mathbb{Z}$, so it seems that $0|0$. However, as $0 \cdot 1 = 0(-1)$, for example, and $1 \neq -1$, by Remark 1 we face a contradiction. Hence, division by 0 is considered meaningless, and $\frac{0}{0}$ is undefined, as you may already know.

We give some properties of divisibility of integers in the following exercise. You would already be familiar with some of them. Here is your chance to prove them.

E1) Let a, b, c be non-zero integers. Prove that

- i) $a|0, \pm 1|a, \pm a|a$.
- ii) $a|b \Rightarrow ac|bc$.
- iii) $a|b$ and $b|c \Rightarrow a|c$.
- iv) $a|b$ and $b|a \Leftrightarrow a = \pm b$.
- v) $c|a$ and $c|b \Rightarrow c|(ax + by) \forall x, y \in \mathbb{Z}$.

Before going further, we will remind you of some equivalent statements which you have studied in Unit 2 of the course 'Real Analysis', in some detail. For this, you need to recall the following definition.

Definition: Let S be a non-empty subset of \mathbb{Z} . An element $a \in S$ is called a **least element** (or a **minimum element**) of S if $a \leq b \forall b \in S$.

For example, \mathbb{N} has a least element, namely, 1. But \mathbb{Z} has no least element. In fact, many subsets of \mathbb{Z} , like $2\mathbb{Z}, \{-1, -2, -3, \dots\}$, etc., don't have least elements.

Now we state an axiom of the integers that we will often use, explicitly and implicitly, namely, the well-ordering principle. It tells us of some sets that have a least element.

Well-ordering Principle: Every non-empty subset of \mathbb{N} has a least element.

In fact, this principle is equivalent to '**Every non-empty subset of $\mathbb{N} \cup \{0\}$ has a least element**'.

As you may recall from 'Real Analysis', this principle is actually equivalent to the **principle of mathematical induction**, which you have studied in detail in Block 1 of that course. Let us state the principle here.

Theorem 1 (Principle of Mathematical Induction): Let $S \subseteq \mathbb{N}$ such that

- i) $1 \in S$, and
- ii) whenever $k \in S$, then $k+1 \in S$.

Then $S = \mathbb{N}$. ■

This theorem is further equivalent to the following result.

Theorem 2 (Extended Principle of Induction): Let $S \subseteq \mathbb{N}$ such that

We will sometimes use **PMI** as an abbreviation of the 'Principle of Mathematical Induction'.

- i) $n_0 \in S$, and
- ii) whenever $k \in S$, $k + 1 \in S$.

Then $S = \{n \in \mathbb{N} \mid n \geq n_0\}$. ■

The fourth equivalent statement that you have studied in 'Real Analysis' is:

Theorem 3 (The Strong Form of the Principle of Induction): Let $S \subseteq \mathbb{N}$ such that

- i) $n_0 \in S$, and
- ii) whenever $m \in S \forall n_0 \leq m < k$, then $k \in S$.

Then $S = \{n \in \mathbb{N} \mid n \geq n_0\}$. ■

We will not prove the equivalence of the well-ordering principle with Theorems 1, 2 and 3 in this course, since the proof is slightly technical. However, we shall rewrite Theorems 2 and 3 in the equivalent forms that we will normally use.

Theorem 2' (Extended Principle of Mathematical Induction, PMI): Let $P(n)$ be a predicate about a positive integer n such that

- i) $P(n_0)$ is a true statement for some $n_0 \in \mathbb{N}$, and
- ii) whenever $P(k)$ is true for some $k \in \mathbb{N}$, $k \geq n_0$, then $P(k+1)$ is true.

Then, $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq n_0$. ■

Theorem 3' (The Strong Form of the PMI): Let $P(n)$ be a predicate about a positive integer n such that

- i) $P(n_0)$ is a true statement for some $n_0 \in \mathbb{N}$, and
- ii) whenever $P(m)$ is true for all positive integers m s.t. $n_0 \leq m < k$, then $P(k)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq n_0$. ■

The equivalent statements given above are very useful for proving several results in Analysis, as you have seen. You will see the same in the case of algebra. We will now use it to prove the division algorithm for \mathbb{Z} . You have used this algorithm countless times. For instance, if you were asked to find the number of weeks in 365 days, you would say 52. Why? Possibly because $365 = (7 \times 52) + 1$.

Of course, you could also have noted that $365 = (7 \times 50) + 65$, but then 65 is greater than 7, so there are some more weeks in the remaining 65 days. The algorithm tells us how to come to a unique remainder which has no more 'weeks left in it'.

Theorem 4 (Division Algorithm): Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \leq r < b$.

Proof: We will first prove that q and r exist. Then we will show that they are unique. To prove their existence, we will consider three different situations: $a = 0$, $a > 0$, $a < 0$.

Recall from Unit 2, 'Real Analysis', that 'a predicate' is a sentence $P(n)$, where $P(n)$ may be true for some values of $n \in \mathbb{N}$, and false for some values of n .

In Block 4 you will study a version of this algorithm for polynomials.

Case 1 ($a = 0$): Take $q = 0, r = 0$. Then $a = qb + r$.

Case 2 ($a > 0$): We shall use Theorem 2' in this case.

For $n \in \mathbb{N}$, let $P(n)$ be the predicate that $n = qb + r$ for some $q, r \in \mathbb{Z}, 0 \leq r < b$. We want to see if $P(n)$ is true $\forall n \in \mathbb{N}$.

So let us see if $P(1)$ is true.

If $b = 1$, we can take $q = 1, r = 0$, and thus, $1 = 1 \cdot 1 + 0$.

If $b > 1$, then take $q = 0, r = 1$, i.e., $1 = 0 \cdot b + 1$.

So, in every case of $b \geq 1$, $P(1)$ is true.

Now suppose $P(k-1)$ is true for some $k \in \mathbb{N}, k \geq 2$, i.e.,

$(k-1) = q_1 b + r_1$ for some $q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < b$.

$\Rightarrow k = q_1 b + (r_1 + 1)$, where $r_1 \leq b-1$, i.e., $r_1 + 1 \leq b$.

Therefore, $k = \begin{cases} q_1 b + (r_1 + 1), & \text{if } (r_1 + 1) < b \\ (q_1 + 1)b + 0, & \text{if } r_1 + 1 = b. \end{cases}$

This shows that $P(k)$ is true.

Hence, by Theorem 2', $P(n)$ is true, for any $n \in \mathbb{N}$. That is, for $a > 0$, $a = qb + r$, for some $q, r \in \mathbb{Z}, 0 \leq r < b$.

Case 3 ($a < 0$): Here $(-a) > 0$. Therefore, by Case 2, we can write

$(-a) = q'b + r'$, for some $q', r' \in \mathbb{Z}, 0 \leq r' < b$

$\Rightarrow a = \begin{cases} (-q')b, & \text{if } r' = 0 \\ (-q' - 1)b + (b - r'), & \text{if } 0 < r' < b. \end{cases}$

Thus, $a = qb + r$, for some $q, r \in \mathbb{Z}$, where $0 \leq r < b$.

So you have seen that $\forall a \in \mathbb{Z}, \exists q, r \in \mathbb{Z}$ s.t. $a = qb + r$.

Now let us prove the uniqueness of q and r . Suppose $q', r' \in \mathbb{Z}$ such that $a = qb + r$ and $a = q'b + r'$, where $0 \leq r < b$, and $0 \leq r' < b$.

Then $r - r' = b(q' - q)$. Thus, $b \mid (r - r')$. But $|r - r'| < b$. Thus, the only possibility is $r - r' = 0$, i.e., $r = r'$, and then $q = q'$.

So we have proved the uniqueness of q and r . ■

As we had noted earlier, you would have used the algorithm above quite a bit in your earlier work with integers. For example, to divide 62 by 6, you would write $62 = (6 \times 10) + 2$.

Also, if you were dividing (-25) by 3, you would get $(-25) = (-9)3 + 2$, where $q = -9, r = 2$. Here note that r has to be positive. Therefore, taking $(-25) = (-8)3 - 1$ would not be the outcome of the division algorithm.

This example leads us to an important remark here.

Remark 3: The division algorithm has been proved only for a positive divisor b . What happens if $b \leq 0$? As seen in Remark 2, $b \neq 0$.

If $b < 0$, consider a and $-b (> 0)$.

Then $a = q(-b) + r, 0 \leq r < -b$.

$$= (-q)b + r, 0 \leq r < |b|, \text{ since } |b| = -b.$$

Thus, in its most general form, **the division algorithm says that given**
 $a, b \in \mathbb{Z}$, $b \neq 0$, \exists **unique** $q, r \in \mathbb{Z}$ **s.t.** $a = qb + r$, $0 \leq r < |b|$.

Also consider the following comment regarding terminology.

Remark 4: In the expression $a = qb + r$, where $0 \leq r < b$, q is called the **quotient** and r is called the **remainder** obtained when a is divided by b .

You will find the division algorithm used often while studying certain groups. Try solving some related exercises to get used to applying it.

E2) Apply the division algorithm on the pairs $75, 30$ and $-75, -30$.

E3) Prove that if $a \in \mathbb{Z}$ s.t. $3 \nmid a$, then the remainder on dividing a^2 by 3 is 1.

E4) Let $a, b \in \mathbb{Z}$ such that $3 \mid (a^2 + b^2)$. Show that $3 \mid a$ **and** $3 \mid b$.
(Hint: Use E3.)

Let us now return to discussing divisors and multiples. Consider the following definitions.

Recall that
 $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Definitions: Let $a, b \in \mathbb{Z}^*$.

- i) An integer c is called a **common divisor** of a and b if $c \mid a$ and $c \mid b$.
- ii) An integer m is called a **common multiple** of a and b if $a \mid m$ and $b \mid m$.

For example, 2 is a common divisor of 2 and 4, and 4, as well as 8, are common multiples of 2 and 4. Also, from E1(i), you know that 1 and -1 are common divisors of a and b , for any $a, b \in \mathbb{Z}$. Thus, a pair of integers does have more than one common divisor and common multiple. This leads us to the following definitions.

Definition: An integer d is called a **greatest common divisor (g.c.d)**, in short) of two non-zero integers a and b if

- i) $d \mid a$ and $d \mid b$, and
- ii) whenever $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$, then $c \mid d$.

Note that if d and d' are two g.c.ds of a and b , then (ii) of the definition above says that $d \mid d'$ and $d' \mid d$. Thus, $d = \pm d'$ (see E1).

But then only one of them is positive.

This **unique positive g.c.d. is denoted by** (a, b) .

In the same vein, consider the following definition.

Definition: An integer ℓ is called a **least common multiple (l.c.m)**, in short) of $a, b \in \mathbb{Z}^*$ if

- i) $a \mid \ell$ and $b \mid \ell$, and
- ii) whenever $m \in \mathbb{Z}$ s.t. $a \mid m$ and $b \mid m$, then $\ell \mid m$.

As in the case of the g.c.d, you can show that there is a **unique positive l.c.m.** of a and b , denoted by $[a, b]$.

For instance, $(3, 5) = 1$ and $(-8, 20) = 4$. Also $[3, 5] = 15$ and $[-8, 20] = 40$.

Consider a related remark here.

Remark 5: Some mathematicians also define the g.c.d of $a, b \in \mathbb{Z}$, where only one of them needs to be non-zero. If $b \neq 0$, then $(0, b) = |b|$, as $|b|$ is the greatest positive divisor of both 0 and b . However, we shall continue to discuss the g.c.d. of two non-zero integers. If you choose, you can verify that all the results about (a, b) that we prove here will also work if only one of the integers a, b is non-zero.

Does (a, b) exist for any pair of non-zero integers a and b ? It does, as the following theorem tells us.

Theorem 5: Any two non-zero integers a and b have a greatest common divisor. Further, $(a, b) = ma + nb$, for some $m, n \in \mathbb{Z}$.

Proof: Let $S = \{xa + yb \mid x, y \in \mathbb{Z}, (xa + yb) > 0\}$.

Since $a^2 + b^2 > 0$, $a^2 + b^2 \in S$, i.e., $S \neq \emptyset$. Hence, by the well-ordering principle, S has a least element, say $d = ma + nb$ for some $m, n \in \mathbb{Z}$. You will see that $d = (a, b)$.

As $d \in S$, $d > 0$. So, by the division algorithm we can write

$a = qd + r$, for some $q, r \in \mathbb{Z}$, $0 \leq r < d$.

Thus, $r = a - qd = a - q(ma + nb) = (1 - qm)a + (-qn)b$ (1)

Now, if $r \neq 0$, then (1) shows that $r \in S$, which contradicts the minimality of d in S .

Thus, $r = 0$, i.e., $a = qd$, i.e., $d \mid a$.

You can similarly show that $d \mid b$.

Thus, d is a common divisor of a and b .

Now, let c be an integer such that $c \mid a$ and $c \mid b$.

Then $a = a_1c$, $b = b_1c$ for some $a_1, b_1 \in \mathbb{Z}$.

But then $d = ma + nb = ma_1c + nb_1c = (ma_1 + nb_1)c$.

Thus, $c \mid d$.

So we have shown that d is a g.c.d of a and b . Since $d > 0$, it is the unique positive g.c.d, (a, b) . ■

As an example of what Theorem 5 tells us, consider -7 and 9 . You know that they have no common factor apart from 1 and -1 . So $(-7, 9) = 1$. Also, by hit and trial, you can see that $1 = (-4)(-7) + (-3)9$.

Pairs of integers like -7 and 9 , whose g.c.d is 1, have a special name.

Definition: If two non-zero integers a and b are such that $(a, b) = 1$, then they are called **relatively prime** (or **coprime**) to each other.

By this definition, and using Theorem 5, we can say that **a and b are coprime to each other iff there exist $m, n \in \mathbb{Z}$ such that $1 = ma + nb$.**

Coprime integers have a very useful property that we shall now state and prove.

Theorem 6: If $a, b \in \mathbb{Z}^*$ such that $(a, b) = 1$, and if $c \in \mathbb{Z}$ s.t. $b \mid ac$, then $b \mid c$.

Proof: As you know from Theorem 5, $\exists m, n \in \mathbb{Z}$ such that $1 = ma + nb$. Then $c = c \cdot 1 = c(ma + nb) = mac + nbc$.

Now, $b \mid ac$ and $b \mid bc$. $\therefore b \mid (mac + nbc)$, by E1(v).

Thus, $b \mid c$. ■

Before going further, consider the following remark about the l.c.m.

Remark 6: Given $a, b \in \mathbb{Z}^*$, $[a, b]$ always exists. In fact, $[a, b] = \frac{ab}{(a, b)}$,

which we shall not prove here. Beyond this, we shall not discuss the l.c.m. any further.

Theorem 6 is the basis for proving the Fundamental Theorem of Arithmetic, as you will soon see. For now, let us recall some related definitions.

Definitions: A natural number $p (\neq 1)$ is called a **prime** if its only divisors are 1 and p . If a natural number $n (\neq 1)$ is not a prime, then it is called a **composite number**.

Thus, 5, 17, 101 are primes, and 4 and 100 are composite numbers. Of course, as you know, 1 is neither a prime nor a composite number.

Try solving the following exercises now.

E5) Find $m, n \in \mathbb{Z}$ s.t. $(a, b) = ma + nb$, where

- i) $a = 7, b = 21$;
- ii) $a = -5, b = -271$;
- iii) $a = -c, b = c$ for $c \in \mathbb{Z}^*$.

E6) Find the relationship, if any, between (a, b) , $(-a, b)$, $(-a, -b)$ for $a, b \in \mathbb{Z}^*$.

E7) If p is a prime and $p \mid ab$, then show that $p \mid a$ or $p \mid b$. (This is an **alternative definition** for a prime number.)

E8) Prove the strong form of **Euclid's Lemma**: If p is a prime and $a_1, a_2, \dots, a_n \in \mathbb{Z}$ such that $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some $i = 1, \dots, n$. (**Hint:** Use PMI.)

E9) Prove that in Theorem 4, $(a, b) = (b, r)$.

Now consider the number 50. As you know, we can write $50 = 2 \times 5 \times 5$, as a product of primes. In fact, we can always express any natural number as a product of primes. This is what the **unique prime factorisation theorem**, also called the Fundamental Theorem of Arithmetic, tells us. As we have mentioned earlier, we shall now prove it using Theorem 6.

Theorem 7 (Fundamental Theorem of Arithmetic): Every integer $n > 1$ can be written as $n = p_1 p_2 \dots p_m$, where p_1, \dots, p_m are prime numbers. Further, this representation is unique, except for the order in which the prime factors occur.

Proof: There are two parts to the representation in the theorem – existence, and uniqueness. We will first prove the existence of such a factorisation, using the principle of mathematical induction.

Let $P(n)$ be the predicate that $n + 1$ is a product of one or more primes, for $n \in \mathbb{N}$.

$P(1)$ is true, because 2 is a prime number itself.

Now let us assume that $P(m)$ is true for all positive integers $m < k$. We want to show that $P(k)$ is true.

If $k + 1$ is a prime, $P(k)$ is true.

If $k + 1$ is not a prime, then we can write $k + 1 = m_1 m_2$, where $1 < m_1 < k + 1$ and $1 < m_2 < k + 1$. But then $P(m_1 - 1)$ and $P(m_2 - 1)$ are both true. Thus,

$m_1 = p_1 p_2 \dots p_r$, $m_2 = q_1 q_2 \dots q_s$, where $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ are primes, not necessarily distinct.

Thus, $k + 1 = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$, i.e., $P(k)$ is true.

Hence, by Theorem 3', $P(n)$ is true for every $n \in \mathbb{N}$.

Now let us show that the factorisation is unique.

Let $n = p_1 p_2 \dots p_t = q_1 q_2 \dots q_s$, where $p_1, p_2, \dots, p_t, q_1, q_2, \dots, q_s$ are primes.

We will use induction on t .

If $t = 1$, then $p_1 = q_1 q_2 \dots q_s$. But p_1 is a prime. Thus, its only factors are 1 and itself. Thus, $s = 1$ and $p_1 = q_1$.

Now suppose $t > 1$, and the uniqueness holds for a product of $t - 1$ primes.

Now $p_1 | q_1 q_2 \dots q_s$, and hence, by E8, $p_1 | q_i$ for some $i = 1, \dots, s$. By re-ordering q_1, \dots, q_s if necessary, we can assume that $p_1 | q_1$.

But both p_1 and q_1 are primes. Therefore, $p_1 = q_1$.

But then $p_2 \dots p_t = q_2 \dots q_s$.

So, by induction, $t - 1 = s - 1$ and p_2, \dots, p_t are the same as q_2, \dots, q_s , **in some order**.

Hence, we have proved the uniqueness of the factorisation. ■

The theorem above is fundamental, as it tells us that any positive integer is built up from prime numbers. Thus, prime numbers are the elements that 'combine' to make all the natural numbers, and hence, all the non-zero integers.

The primes that occur in the factorisation of a number may be repeated, just as 5 is repeated in the factorisation $50 = 2 \times 5 \times 5$. By collecting the same primes together, we get the following corollary to Theorem 7.

A corollary to a theorem is a result that is a consequence of the theorem.

Corollary 1: Any natural number n can be uniquely written as $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$, where for $i = 1, 2, \dots, r$, each $m_i \in \mathbb{N}$ and each p_i is a prime with $1 < p_1 < p_2 < \dots < p_r$. ■

As an application of Theorem 7, we give the following important theorem, due to the ancient Greek mathematician, Euclid, mentioned earlier.

Theorem 8: There are infinitely many primes.

Proof: We shall prove this by contradiction. So, let us assume that the set P of prime numbers is finite, say $P = \{p_1, p_2, \dots, p_n\}$. Consider the natural number

$$m = (p_1 p_2 \dots p_n) + 1.$$

Now, suppose some $p_i | m$. Then $p_i | (m - p_1 p_2 \dots p_n)$, i.e., $p_i | 1$, a contradiction.

Therefore, $p_i \nmid m \forall i = 1, \dots, n$.

But, since $m > 1$, Theorem 7 says that m must have a prime factor. So we reach a contradiction.

Therefore, our assumption that the set of primes is finite must be wrong. Hence, there must be infinitely many primes. ■

Try solving the following exercises now.

E10) Prove that if p is a prime number and $a \in \mathbb{Z}$ such that

i) $p \nmid a$, then $(p, a) = 1$;

ii) $p | a^2$, then $p | a$.

E11) Prove that \sqrt{p} is irrational for any prime p .

(Hint: Suppose \sqrt{p} is rational. Then $\sqrt{p} = \frac{a}{b}$, where $a, b \in \mathbb{Z}^*$ and we can assume that $(a, b) = 1$. Now use the properties of prime numbers that we have just discussed.)

E12) Prove that for all $n, m \in \mathbb{N}$, if $n^{1/m} \notin \mathbb{Z}$, then $n^{1/m} \notin \mathbb{Q}$.

E13) Prove Corollary 1.

E14) Use the Fundamental Theorem of Arithmetic to prove that if $y \in \mathbb{N}$, then there is an odd natural number x such that $y = 2^r x$, for some non-negative integer r .

You have seen that every integer is uniquely written as a product of prime powers. So, as you know from your earlier studies, you can use this representation to find the g.c.d of any two integers.

For instance, for finding the g.c.d of 175 and -2205 , we write both in the form given in Corollary 1.

$$\text{So } 175 = 5^2 \cdot 7, \quad -2205 = -(3^2 \cdot 5 \cdot 7).$$

Then you can obtain their g.c.d as the product of the maximum power of each prime dividing both the integers – in this case it is $5^1 \cdot 7^1 = 35$.

As you can see, this requires us to be able to factorise both the integers as a product of primes. This is not easy when the numbers get very large. An algorithm was developed to make matters easier, by the ancient Greeks. It appears to have been first given by the ancient Greek mathematician Euclid, in his 'Elements', comprising 13 books, written around 300 B.C. Hence this algorithm is named after Euclid. It is based on successive applications of the division algorithm.

To help you see how the Euclidean algorithm works, consider an example.

Example 1: Find $(-246, 135)$. Also find $m, n \in \mathbb{Z}$ s.t.
 $m(-246) + n(135) = (-246, 135)$.

Solution: From E6, you know that $(-246, 135) = (246, 135)$.

By the division algorithm for 246 and 135, we get

$$246 = 135 \cdot 1 + 111. \quad \dots(2)$$

Now apply the division algorithm to 135 and the remainder in (2), i.e., 111, to get

$$135 = 111 \cdot 1 + 24. \quad \dots(3)$$

Now apply the division algorithm to 111 and 24, to get

$$111 = 24 \cdot 4 + 15. \quad \dots(4)$$

$$\text{Next, } 24 = 15 \cdot 1 + 9. \quad \dots(5)$$

$$\text{Next, } 15 = 9 \cdot 1 + 6. \quad \dots(6)$$

$$\text{Next, } 9 = 6 \cdot 1 + 3. \quad \dots(7)$$

$$\text{Next, } 6 = 3 \cdot 2 + 0. \quad \dots(8)$$

Once the remainder is zero, we stop.

Now, from E9, you know that

$$(246, 135) = (135, 111) = (111, 24) = (24, 15) = (15, 9) = (9, 6) = (6, 3) = (3, 0) = 3.$$

Thus, $(-246, 135) = 3$.

Note that each step of the Euclidean algorithm reduces the problem of finding the g.c.d of two integers to one of finding the g.c.d of two integers smaller in magnitude.

Also, in the context of Theorem 5, note that (7) gives
 $3 = 9 - 6 = 9 - (15 - 9)$, using (6).

$$= 2 \cdot 9 - 15$$

$$= 2(24 - 15) - 15 = 2 \cdot 24 - 3 \cdot 15, \text{ using (5).}$$

$$= 2 \cdot 24 - 3(111 - 4 \cdot 24) = 14 \cdot 24 - 3 \cdot 111, \text{ using (4).}$$

$$= 14(135 - 111) - 3 \cdot 111 = 14 \cdot 135 - 17 \cdot 111, \text{ using (3).}$$

$$= 14 \cdot 135 - 17(246 - 135) = (31 \cdot 135) - (17 \cdot 246), \text{ using (2).}$$

$$\text{Thus, } 3 = (-17) \cdot 246 + 31 \cdot 135$$

$$= 17 \cdot (-246) + 31 \cdot 135.$$

Thus, in the context of Theorem 5, $m = 17, n = 31$.

In the example above, you can see how the algorithm facilitates us to find $m, n \in \mathbb{Z}$ s.t. $ma + nb = (a, b)$. Otherwise, we simply have to use a hit-and-trial method to find these integers, as we did in the earlier examples.

Let us formally write down the Euclidean algorithm now.

Euclidean Algorithm: For any two positive integers a and $b, \exists q_0, q_1, \dots, q_{n+1}$ and r_0, r_1, \dots, r_n s.t.



Fig.1: Euclid

$$a = bq_0 + r_0, \quad 0 < r_0 < b.$$

$$b = r_0q_1 + r_1, \quad 0 < r_1 < r_0.$$

$$r_0 = r_1q_2 + r_2, \quad 0 < r_2 < r_1.$$

$$\vdots \quad \quad \quad \vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1}.$$

$$r_{n-1} = r_nq_{n+1} + 0.$$

$$\text{Then } (a, b) = r_n.$$

Proof: As you have shown in E9, $(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-1}, r_n) = r_n$. ■

The algorithm above is the basis for solving different kinds of algebraic equations. It is used for securing internet communication and in coding theory.

Why don't you apply the algorithm yourself now?

E15) Apply the Euclidean algorithm to find (a, b) for

i) $a = 54321, b = 12345$, and

ii) $a = -61880, b = -880$.

Also find $m, n \in \mathbb{Z}$ s.t. $(a, b) = ma + nb$, in each case.

We shall curtail our discussion on divisibility in \mathbb{Z} for now. However, we shall now consider one way of gathering the elements of \mathbb{Z} as mutually disjoint subsets, based on the divisibility of pairs of integers.

1.3 PARTITIONS AND EQUIVALENCE RELATIONS

In Block 1 of Calculus, you studied relations, and, in particular, equivalence relations. Let us recall the definitions concerned.

Definitions: Let S be a non-empty set.

- i) A **relation** on S is a subset R of $S \times S$. We also denote the relation R by \sim , defined by ' $a \sim b$ iff $(a, b) \in R$ '.
Here we sometimes write $a \sim b$ as **aRb**.
- ii) A relation R on S is called **reflexive** if $(a, a) \in R \quad \forall a \in S$, i.e.,
 $a \sim a \quad \forall a \in S$.
- iii) A relation R on S is called **symmetric** if $(a, b) \in R \Rightarrow (b, a) \in R$, i.e.,
 $a \sim b \Rightarrow b \sim a$ for $a, b \in S$.
- iv) A relation R on S is called **transitive** if
 $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$, i.e.,
 $a \sim b, b \sim c \Rightarrow a \sim c$ for $a, b, c \in S$.
- v) A relation R on S is called an **equivalence relation** if it is reflexive, symmetric and transitive.

Let us consider an example.

Example 2: Consider the relation \sim on \mathbb{C} , given by ' $a \sim b$ iff $|a| = |b|$ '. Here $R = \{(a, b) \in \mathbb{C} \times \mathbb{C} \mid |a| = |b|\}$. Check whether or not R is an equivalence relation on \mathbb{C} .

Solution: Since $|a| = |a| \forall a \in \mathbb{C}$, \sim is reflexive.

For $a, b \in \mathbb{C}$, if $|a| = |b|$, then $|b| = |a|$. Hence, \sim is symmetric.

For $a, b, c \in \mathbb{C}$, if $|a| = |b|$ and $|b| = |c|$, then $|a| = |c|$. Hence, \sim is transitive.

Thus, \sim is an equivalence relation on \mathbb{C} , i.e., R is an equivalence relation on \mathbb{C} .

In Example 2, for a fixed $z \in \mathbb{C}$, look at the subset of \mathbb{C} ,

$[z] = \{\alpha \in \mathbb{C} \mid |\alpha| = |z|\}$. So, $[z]$ is the infinite set consisting of all the points lying on the circle shown in Fig.2. From Fig.2, you can see that if $|z| \neq |z_1|$, then $[z] \cap [z_1] = \emptyset$; and if $|z| = |z_1|$, then $[z] = [z_1]$.

Also, $\mathbb{C} = \bigcup_{z \in \mathbb{C}} [z]$. In this union, all those elements with the same modulus collapse into one subset. And each such subset is disjoint from the others.

The set $[z]$ is a particular case of what we shall now define.

Definition: Given an equivalence relation R on a set S ,

$[a] = \{b \in S \mid (a, b) \in R\}$ is called the **equivalence class** of $a \in S$.

Note that $[a]$ is a subset of S . Further, $b \in [a]$ iff $[a] = [b]$, since R is an equivalence relation.

Thus, for $a, b \in S$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Also, for any $z \in S$, $z \in [z]$.

So we can write S as a union of disjoint equivalence classes.

Let us consider some more examples of equivalence relations and the corresponding classes.

Example 3: Consider the relation $R = \{(a, a + 5m) \mid a, m \in \mathbb{Z}\}$. In other words, $(a, b) \in R$ iff $5 \mid (a - b)$. Show that R is an equivalence relation, and find two distinct elements in the equivalence class of 1.

Solution: Since $5 \mid (a - a)$, $(a, a) \in R \forall a \in \mathbb{Z}$. Hence, R is reflexive.

Next, $(a, b) \in R \Rightarrow 5 \mid (a - b)$

$$\Rightarrow \exists c \in \mathbb{Z} \text{ s.t. } (a - b) = 5c$$

$$\Rightarrow (b - a) = 5(-c)$$

$$\Rightarrow 5 \mid (b - a)$$

$$\Rightarrow (b, a) \in R.$$

Hence, R is symmetric.

Finally, let (a, b) and (b, c) be in R . Then $\exists m, n \in \mathbb{Z}$ s.t. $(a - b) = 5m$ and $(b - c) = 5n$. Thus, $(a - c) = (a - b) + (b - c) = 5(m + n)$, i.e., $5 \mid (a - c)$.

Hence, $(a, c) \in R$, so that R is transitive.

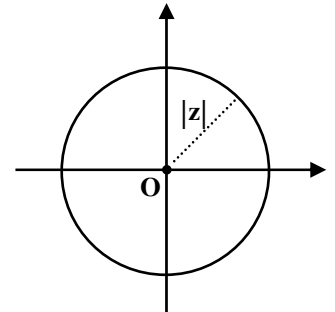


Fig.2: The circle with centre $O(0, 0)$ and radius $|z|$, where $z \in \mathbb{C}$.

Thus, R is an equivalence relation.

$$\begin{aligned} [1] &= \{a \in \mathbb{Z} \mid (a, 1) \in R\} = \{a \in \mathbb{Z} \mid (a-1) = 5m \text{ for some } m \in \mathbb{Z}\} \\ &= \{5m+1 \mid m \in \mathbb{Z}\}. \end{aligned}$$

Hence, to get two distinct elements in $[1]$, we consider two distinct values of $m \in \mathbb{Z}$, say $m = 0, 1$. Then we get two distinct elements 1, 6 in $[1]$.

Let us generalise Example 3 now.

Example 4: Let $n \in \mathbb{N}$. Define R to be the relation on \mathbb{Z} given by ' aRb iff $n \mid (a-b)$ '. Show that R is an equivalence relation on \mathbb{Z} . How many distinct equivalence classes of R is \mathbb{Z} a union of, and why?

Solution: You can show that R is an equivalence relation along the lines given in Example 3.

To find the equivalence classes, let us use the division algorithm. Given any $a \in \mathbb{Z}$, $\exists q$ and r in \mathbb{Z} s.t.

$$a = nq + r, \quad 0 \leq r < n. \quad \dots(9)$$

Now, for each $i = 0, 1, \dots, n-1$, $[i] = \{mn+i \mid m \in \mathbb{Z}\}$, as in Example 3.

Also, from (9), $[a] = [r]$ for some $r, 0 \leq r < n$. Hence, $[0], [1], \dots, [n-1]$ are all the classes.

Further, if $[i] = [j]$ for some j s.t. $0 \leq j < n$, then for some $m, m' \in \mathbb{Z}$,

$$mn+i = m'n+j \Rightarrow n(m-m') = j-i \Rightarrow n \mid (j-i).$$

But $|i-j| < n$.

Thus, $n \mid (j-i)$ is only possible if $j-i = 0$, i.e., $i = j$. And then, $m = m'$.

Hence, $[0], [1], \dots, [n-1]$ are n distinct classes, and these are all the classes.

Hence, $\mathbb{Z} = [0] \cup [1] \cup \dots \cup [n-1]$, a union of n disjoint equivalence classes.

The equivalence relation in Example 4 is called '**congruence modulo n** '.

We write $a \equiv b \pmod{n}$ (read as ' **a is congruent to b modulo n** ') if

$[a] = [b]$ in Example 4, i.e., if $n \mid (a-b)$.

Here the set of all the equivalence classes is denoted by \mathbb{Z}_n .

Thus, $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$.

The examples above lead us to the following definition.

Definition: A **partition** of a non-empty set S is a collection of disjoint non-empty subsets $S_i, i \in I$, of S s.t. $S = \bigcup_{i \in I} S_i$, where I is an indexing set.

The subsets S_i are called the **cells** of the partition.

Thus, if S is partitioned into the cells S_i , then each element of S lies in one and only one cell.

There can be infinitely many cells in a partition, or finitely many cells. For instance, in Example 4, \mathbb{Z} is partitioned into n classes. Here the cells are $[0], [1], \dots, [n-1]$. But in Example 2, \mathbb{C} is partitioned into infinitely many cells, each cell being an infinite set.

Note that \mathbb{Z}_n is a set of sets, since $[i]$ is a set for each $i \in \mathbb{N} \cup \{0\}$.

Let us now prove a result relating partitions with equivalence relations.

Theorem 9: A partition of a non-empty set S defines an equivalence relation on S . Conversely, an equivalence relation on S defines a partition on S .

Proof: Firstly, let $\{S_i | i \in I\}$ be the set of cells of a partition of S , where I is an indexing set.

For $a, b \in S$, define a relation R on S by 'aRb iff a and b lie in the same cell of the partition'.

Thus, aRa , since a lies in the same cell as itself. So R is reflexive.

Next, if aRb , then a and b lie in a cell. Hence, b and a lie in one cell. Thus, bRa , i.e., R is symmetric.

Finally, if aRb and bRc , then a and b lie in one cell, say S_i , and b and c lie in one cell, S_j . Since b lies in $S_i \cap S_j$, $S_i \cap S_j \neq \emptyset$. Thus, $i = j$. Thus, both a and c lie in S_i . Hence, aRc , i.e., R is transitive.

Hence, R is an equivalence relation.

For the converse, consider an equivalence relation R on S . Suppose

$[a] \cap [b] \neq \emptyset$ for some $a, b \in S$.

Let $x \in [a] \cap [b]$. Then xRa and xRb , so that aRx and xRb . Hence aRb , i.e., $[a] = [b]$.

Thus, all the equivalence classes are disjoint or identical.

Also, for any $a \in S$, $a \in [a]$.

Hence, the equivalence classes form a partition of S . ■

For example, the equivalence relation in Example 2 partitions \mathbb{C} into infinitely many cells, which are concentric circles in \mathbb{R}^2 with their centres at $(0, 0)$, as you saw in Fig.2.

Now you can look at some other relations to see if they give partitions of the sets concerned or not.

E16) Check whether the following relations are equivalence relations on \mathbb{Z}^* or not.

i) nRm iff $nm > 0$,

ii) nRm iff n and m have the same number of digits in the base ten notation.

For those R that are equivalence relations, obtain the corresponding partitions of \mathbb{Z}^* .

E17) Show that 'ARB iff $A \Rightarrow B$ ' is a reflexive and transitive relation on the set of all true mathematical statements, but is not symmetric.

E18) Find all the cells of the partitions of \mathbb{Z} , corresponding to 'congruence modulo 8' and 'congruence modulo 1'.

Let us now look at another algebraic object, which is of much interest in algebra. We will often use these objects as examples in this course.

1.4 INTRODUCING MATRICES

In your previous studies in mathematics, you have studied ways of looking for common solutions of several linear equations like:

$$\left. \begin{array}{l} 2x + 3y = 5 \\ 3x + 2y = -5 \end{array} \right\} \dots(I)$$

These two equations, taken together, can also be represented by arranging the coefficients of the variables x and y , and the constant term, in rows and columns, as below:

	coefficient of x	coefficient of y	constant term
	↓	↓	↓
1st eqn	2	3	5
2nd eqn	3	2	-5

In this way we get a rectangular array with its entries being numbers, as below.

$$\begin{bmatrix} 2 & 3 & 5 \\ 3 & 2 & -5 \end{bmatrix}$$

You will later see why we can rewrite the linear system (I) as below, using this array.

$$\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \\ -5 \end{bmatrix}.$$

As you will see in the 5th semester course, such arrangements are very helpful in finding solutions of certain linear systems. These are systems in which the number of variables are very large, and the coefficients involved are not easy to calculate by hand.

The set of such rectangular arrays have considerable importance in algebra. Therefore, we are introducing them to you. You will be studying some of their basic properties in this section. Later you will study more about them.

Historically, these arrays gained algebraic importance in the 19th century, in England. The mathematicians, James Sylvester and Arthur Cayley, first applied them to study systems of linear equations.



Fig.3: J. J. Sylvester
(1814-1897)

So, let us begin with defining these objects.

Definitions: Let S be a non-empty set.

- i) A rectangular array of mn elements from S , arranged in m horizontal rows and n vertical columns, **enclosed in square brackets**, is called an **$m \times n$ matrix**, or a **matrix of order $m \times n$, over S** .
- ii) An $n \times n$ matrix over S is called a **square matrix of order n over S** .
- iii) A $1 \times n$ matrix over S is called a **row vector** over S ; and an $n \times 1$ matrix over S is called a **column vector** over S .

The set of all $m \times n$ matrices over a set S is denoted by $M_{m \times n}(S)$, and the set of all $n \times n$ matrices over S is denoted by $M_n(S)$.

For example, $\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}$ is a square matrix of order 2 over \mathbb{Z} .

'Matrices' is the plural of 'matrix'.

$\begin{bmatrix} x \\ y \end{bmatrix}$ and $\begin{bmatrix} 5 \\ -5 \end{bmatrix}$ are in $M_{2 \times 1}(\mathbb{R})$, assuming that $x, y \in \mathbb{R}$. These are also

examples of column vectors over \mathbb{R} .

The $m \times n$ matrix $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$ is denoted by $[a_{ij}]_{m \times n}$, or simply $[a_{ij}]$,

if m and n don't need to be stressed.

Here a_{ij} is the element in the i th row and the j th column, i.e., a_{ij} is the (i, j) th element of the matrix.

If $A = [a_{ij}]$ is a square matrix of order n , the elements $a_{11}, a_{22}, \dots, a_{nn}$ are called the **diagonal elements** of A , and the **diagonal of A** is the ordered set $\{a_{11}, a_{22}, \dots, a_{nn}\}$, i.e., the elements are in the given order.

For example, the diagonal of $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is $\{1, 4\}$, not $\{4, 1\}$. Here $a_{12} = 3$,

and $a_{21} = 2$.

You will often work with $M_{m \times n}(\mathbb{C})$, the set of all $m \times n$ matrices whose entries are complex numbers.

Note that $M_{m \times n}(\mathbb{Z}) \subseteq M_{m \times n}(\mathbb{Q}) \subseteq M_{m \times n}(\mathbb{R}) \subseteq M_{m \times n}(\mathbb{C})$, since $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Let us now look at a real life (simplified!) situation in which a matrix can arise.

Example 5: There are 5 male and 3 female members on the History faculty of a certain college, 4 female and 3 male members on the Mathematics faculty and 7 females on the Computer Science faculty of the college. Present this information as a matrix.

Solution: One way of presenting the information given is as the following 3×2 matrix

	Male	Female
History	$\begin{bmatrix} 5 & 3 \end{bmatrix}$	
Mathematics	$\begin{bmatrix} 3 & 4 \end{bmatrix}$	
Computer Science	$\begin{bmatrix} 0 & 7 \end{bmatrix}$	

Another possibility is the following 2×3 matrix.

	History	Mathematics	Computer Science
Female	$\begin{bmatrix} 3 & 4 & 7 \end{bmatrix}$		
Male	$\begin{bmatrix} 5 & 3 & 0 \end{bmatrix}$		

Either of these representations immediately tells us how many faculty members there are in the disciplines given, and how many of them are female/male.

There are several real-life problems that mathematics helps to solve using matrices. You will study some in the 5th semester course. For now, you can get used to matrices by solving the following exercises.

E19) Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \\ 0 & 0 & 7 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 5 & 3 & 2 \\ 5 & 4 & 1 & 5 \\ 0 & 3 & 2 & 0 \end{bmatrix}$. Give the

- i) (2, 3)th elements of A and B,
- ii) third row of A,
- iii) diagonals of the square matrices among A and B,
- iv) first column of B,
- v) fourth row of B.

E20) Give an element of $M_{4 \times 2}(\mathbb{Q}) \setminus M_{4 \times 2}(\mathbb{Z})$.

E21) Give a matrix over \mathbb{C} whose diagonal is $\{e, i, \pi, -1\}$, and whose (i, j) th element is 1 for $i > j$ and 0 for $i < j$, where $i, j = 1, 2, 3, 4$.

Now, let us see when two matrices are the same. Why don't you write down two different 2×2 matrices over \mathbb{R} ? Did the (i, j) th entry of one matrix differ from the (i, j) th entry of the other for some i and j ? If not, then these matrices are not different. They are equal. For example, the two 1×1 matrices $[2]$ and $[2]$ are equal. But $[2] \neq [-2]$, according to the following definition.

Definition: Two matrices are called **equal** if

- i) they have the same order, that is, they have the same number of rows as well as the same number of columns, and
- ii) their elements, at all the corresponding positions, are the same.

The following example will clarify what we mean by equal matrices.

Example 6: If $\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} x & y \\ z & 3 \end{bmatrix}$, then what are the values of x, y and z ?

Solution: Firstly, note that both matrices are of the same order, namely, 2×2 . Now, for these matrices to be equal the (i, j) th elements of both must be equal $\forall i, j$. Therefore, we must have $x = 1, y = 0, z = 2$.

Try solving some exercises now.

E22) Can a matrix over \mathbb{R} be equal to a matrix over \mathbb{N} ? Why, or why not?

E23) Are $[3 \ 4]$ and $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ equal? Why?

E24) Is $\begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} = [-1 \ 0 \ 1]$? Why?

Let us now consider some operations on matrices over \mathbb{C} .

Transpose

First, consider a matrix, say $A = \begin{bmatrix} 2 & 5 & -1 \\ 0 & 0.5 & \sqrt{2} \end{bmatrix} \in \mathbb{M}_{2 \times 3}(\mathbb{R})$.

Now look at $B = \begin{bmatrix} 2 & 0 \\ 5 & 0.5 \\ -1 & \sqrt{2} \end{bmatrix} \in \mathbb{M}_{3 \times 2}(\mathbb{R})$.

Do you see any connection between A and B ? Consider the 1st row of A and the 1st column of B . Aren't they the same? Similarly, the 2nd row of A is the 2nd column of B . In fact, B is the transpose of A , as the following definition will tell you.

Definition: Let S be a non-empty set. The **transpose** of a matrix $A = [a_{ij}] \in \mathbb{M}_{m \times n}(S)$ is the $n \times m$ matrix whose rows are the columns of A in the same sequence, and is denoted by A^t . Thus, $A^t = [a_{ji}] \in \mathbb{M}_{n \times m}(S)$.

For example, if $A = \begin{bmatrix} 3 & 2 & 0 & 0 \\ \pi & 3+i & 0 & 0 \end{bmatrix}$, then $A^t = \begin{bmatrix} 3 & \pi \\ 2 & 3+i \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$. Note that

$A^t \neq \begin{bmatrix} \pi & 3 \\ 3+i & 2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$ here because the sequence of rows of A has to be

maintained in writing the columns of A^t .

Also, note that $(A^t)^t = \begin{bmatrix} 3 & 2 & 0 & 0 \\ \pi & 3+i & 0 & 0 \end{bmatrix} = A$.

From the definition, you can see that, as in the example above, $(A^t)^t = A$, for any matrix A .

Now, consider the following comment about 'transpose'.

Remark 7: Note that $f : \mathbb{M}_{m \times n}(\mathbb{C}) \rightarrow \mathbb{M}_{n \times m}(\mathbb{C}) : f(A) = A^t$ is a well-defined function. This is because if $A = B$, then the i th row of A is the i th row of $B \forall i = 1, \dots, m$. Hence, the i th column of A^t is the i th column of $B^t \forall i = 1, \dots, m$. Hence, $A^t = B^t$.

Let us now consider a binary operation on the set of $m \times n$ matrices over \mathbb{C} .

Addition of Matrices

Let us consider $\begin{bmatrix} 2 & 1 & -1 \\ \pi & i & 0.7 \end{bmatrix}$ and $\begin{bmatrix} 2 & 5 & 0.5 \\ 0 & -1 & \sqrt{2} \end{bmatrix}$ in $\mathbb{M}_{2 \times 3}(\mathbb{C})$. Is there a

natural way of adding or subtracting them? What if we add the elements in

the corresponding places of both? So

$$\begin{bmatrix} 2 & 1 & -1 \\ \pi & i & 0.7 \end{bmatrix} + \begin{bmatrix} 2 & 5 & 0.5 \\ 0 & -1 & \sqrt{2} \end{bmatrix} = \begin{bmatrix} 2+2 & 1+5 & -1+0.5 \\ \pi+0 & i-1 & 0.7+\sqrt{2} \end{bmatrix} \\ = \begin{bmatrix} 4 & 6 & -0.5 \\ \pi & i-1 & 0.7+\sqrt{2} \end{bmatrix}.$$

In fact, this is the way matrix addition and subtraction are defined in general, as you will now see.

This definition holds true for matrices over any set S on which addition and subtraction are binary operations.

Definition: For $A = [a_{ij}]$ and $B = [b_{ij}]$ in $M_{m \times n}(\mathbb{C})$, $A + B$ is defined to be the matrix $[a_{ij} + b_{ij}] \in M_{m \times n}(\mathbb{C})$, and $A - B$ is defined to be the matrix $[a_{ij} - b_{ij}] \in M_{m \times n}(\mathbb{C})$.

Note that addition and subtraction, as defined, are binary operations on $M_{m \times n}(\mathbb{C})$.

Consider an important comment here.

Remark 8: In the given definition, note that **only two matrices of the same order can be added or subtracted**. For example, $\begin{bmatrix} 2 \\ 1 \end{bmatrix} + [3 \ 5]$ is not defined

since $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ is a 2×1 matrix and $[3 \ 5]$ is a 1×2 matrix.

Let us look at some detailed illustrations of the operations you have studied so far.

Example 7: Find $A + B$, $B + A$, $A - B$, $B - A$, where

$$A = \begin{bmatrix} -i & 1.5 \\ 0.2 & i \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} \sqrt{2} & \sqrt{3} \\ -\sqrt{2} & -\sqrt{3} \\ \pi & 4 \end{bmatrix} \in M_{3 \times 2}(\mathbb{C}).$$

Also decide whether $A + B = B + A$ and $A - B = B - A$ or not.

Solution: By the definition,

$$A + B = \begin{bmatrix} -i + \sqrt{2} & 1.5 + \sqrt{3} \\ 0.2 - \sqrt{2} & i - \sqrt{3} \\ -1 + \pi & 4 \end{bmatrix}, B + A = \begin{bmatrix} \sqrt{2} - i & \sqrt{3} + 1.5 \\ -\sqrt{2} + 0.2 & -\sqrt{3} + i \\ \pi - 1 & 4 \end{bmatrix}, \\ A - B = \begin{bmatrix} -i - \sqrt{2} & 1.5 - \sqrt{3} \\ 0.2 + \sqrt{2} & i + \sqrt{3} \\ -1 - \pi & -4 \end{bmatrix}, B - A = \begin{bmatrix} \sqrt{2} + i & \sqrt{3} - 1.5 \\ -\sqrt{2} - 0.2 & -\sqrt{3} - i \\ \pi + 1 & 4 \end{bmatrix}.$$

Note that all the corresponding entries of $A + B$ and $B + A$ are the same. Hence, $A + B = B + A$.

Since the (1, 1)th entries of $A - B$ and $B - A$ are not the same, $A - B \neq B - A$.

Example 8: Let $A = \begin{bmatrix} 2 & 1 & 5 \\ -3 & i & 5i \end{bmatrix}$ and $B = \begin{bmatrix} -2 & 1 & 7 \\ 0 & 9 & -8 \end{bmatrix} \in \mathbb{M}_{2 \times 3}(\mathbb{C})$. Find

A^t , B^t , $A+B$ and $(A+B)^t$. Is $(A+B)^t = A^t + B^t$? Why?

Solution: Firstly, $A+B$ is defined, since A and B have the same order.

$$\text{Here } A+B = \begin{bmatrix} 0 & 2 & 12 \\ -3 & 9+i & -8+5i \end{bmatrix}.$$

$$\text{Now } A^t = \begin{bmatrix} 2 & -3 \\ 1 & i \\ 5 & 5i \end{bmatrix}, B^t = \begin{bmatrix} -2 & 0 \\ 1 & 9 \\ 7 & -8 \end{bmatrix}, (A+B)^t = \begin{bmatrix} 0 & -3 \\ 2 & 9+i \\ 12 & -8+5i \end{bmatrix}.$$

$$\text{Also, } A^t + B^t = \begin{bmatrix} 0 & -3 \\ 2 & 9+i \\ 12 & -8+5i \end{bmatrix}.$$

Looking at the corresponding entries of $(A+B)^t$ and $A^t + B^t$, you can see that $(A+B)^t = A^t + B^t$.

Example 9: If $A \in \mathbb{M}_{2 \times 3}(\mathbb{R})$, is $A+A^t$ defined? Under what conditions on m and n is $A-A^t$ defined for an $m \times n$ matrix A over \mathbb{R} ?

Solution: Since A is a 2×3 matrix, A^t is a 3×2 matrix. Hence A and A^t have different orders. Hence, $A+A^t$ is not defined.

Next, since A is an $m \times n$ matrix and A^t is an $n \times m$ matrix, $A-A^t$ is only defined when $m=n$, i.e., if A is a square matrix.

What you have seen in the examples above is true for any two matrices. Let us state the result formally.

Theorem 10: Let $A, B \in \mathbb{M}_{m \times n}(\mathbb{C})$. Then

- i) $A+B = B+A$,
- ii) $(A+B)^t = A^t + B^t$.

Proof: We shall prove (ii) here, and leave (i) for you as an exercise (see E27).

- ii) Let $A = [a_{ij}]$ and $B = [b_{ij}]$. Then $A+B = [a_{ij} + b_{ij}]$.

Therefore, $(A+B)^t = [c_{ij}]$, where

$$\begin{aligned} c_{ij} &= \text{the } (i, j)\text{th element of } (A+B)^t \\ &= \text{the } (j, i)\text{th element of } A+B \\ &= a_{ji} + b_{ji} \\ &= \text{sum of the } (j, i)\text{th elements of } A \text{ and of } B \\ &= \text{sum of the } (i, j)\text{th elements of } A^t \text{ and of } B^t \\ &= (i, j)\text{th element of } A^t + B^t. \end{aligned}$$

Thus, $(A+B)^t = A^t + B^t$. ■

Why don't you solve some exercises now?

E25) Find the sum of

i) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ in $M_2(\mathbb{Z})$,

ii) $[a_{ij}]_{m \times n} + [-a_{ij}]_{m \times n}$ in $M_{m \times n}(\mathbb{C})$,

iii) $[a_{ij}]_{m \times n} + \mathbf{0}$ in $M_{m \times n}(\mathbb{C})$, where $\mathbf{0}$ is the $m \times n$ matrix whose every entry is 0.

E26) Verify Theorem 10(ii) for A, B in Example 7.

E27) Let $A, B, C \in M_{m \times n}(S)$, where $S \subseteq \mathbb{C}$, $S \neq \emptyset$ and '+' is a binary operation on S . Check whether or not

i) $A + B = B + A$,

ii) $A + (B + C) = (A + B) + C$.

E28) Prove that

i) $(A^t)^t = A$, for any $A \in M_{m \times n}(\mathbb{C})$.

ii) $(A + A^t)^t = A + A^t$ and $(A - A^t)^t = -(A - A^t)$, for every $A \in M_n(\mathbb{C})$.

As you know from Block 1, Calculus, E27(i) says that addition of matrices is a **commutative** operation, and (ii) says that addition of matrices is an **associative** operation on S . In Unit 2, you will be using these properties.

Let us now define **two different kinds of multiplication on matrices** – scalar multiplication and matrix multiplication.

Scalar Multiplication

Consider the matrix $A = \begin{bmatrix} 2 & 5 & 2 \\ 3 & 5 & 7 \end{bmatrix}$. Now $2A$ is the same as

$$A + A = \begin{bmatrix} 4 & 10 & 4 \\ 6 & 10 & 14 \end{bmatrix}. \text{ In this way, } nA, \text{ for any } n \in \mathbb{N}, \text{ is the same as adding}$$

A to itself n times. So it makes sense to say that

$$nA = \begin{bmatrix} 2n & 5n & 7n \\ 3n & 5n & 2n \end{bmatrix}, \text{ where } n \in \mathbb{N}.$$

Generalising this process, we have the following definition.

Definition: For any $\alpha \in \mathbb{C}$ and $A = [a_{ij}] \in M_{m \times n}(\mathbb{C})$, the product of α and A is defined to be the **scalar product**, $\alpha A = [\alpha a_{ij}]$.

Note that if $A = [a_{ij}]$, $-\mathbf{A} = (-1)A = [(-1)a_{ij}]$
 $= [-a_{ij}]$.

As an example of scalar multiplication, consider the scalar product of

$$2 + 3i \in \mathbb{C} \text{ and } \begin{bmatrix} i & 5 \\ 0 & -i \end{bmatrix} \in M_2(\mathbb{C}).$$

This definition holds true if \mathbb{C} is replaced by \mathbb{Z} , \mathbb{Q} or \mathbb{R} .

$$(2+3i) \begin{bmatrix} i & 5 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} (2+3i)i & (2+3i)5 \\ (2+3i)0 & (2+3i)(-i) \end{bmatrix}$$

$$= \begin{bmatrix} -3+2i & 10+15i \\ 0 & 3-2i \end{bmatrix}, \text{ since } i^2 = -1.$$

Consider the following comment now, regarding this kind of multiplication.

Remark 9: The multiplication defined above is called ‘scalar’ multiplication because the elements of the set to which the entries of the matrix belong, in this case \mathbb{C} , are called scalars. Here the multiplication is a function

$\bullet : \mathbb{C} \times M_{m \times n}(\mathbb{C}) \rightarrow M_{m \times n}(\mathbb{C})$. Thus, scalar multiplication is **not** a binary operation on $M_{m \times n}(\mathbb{C})$.

Let us now consider some examples. Side by side you will study some elementary properties that relate the operations on matrices that you have studied so far.

Example 10: Let $A = \begin{bmatrix} 2 & 1 \\ 7 & -1 \\ -0.5 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0.3 & -1/3 \\ 1 & 5 \\ -5 & 8 \end{bmatrix} \in M_{3 \times 2}(\mathbb{Q})$.

Find $5A$, $5B$, $5(A+B)$, $5(A-B)$ and $5A^t$.

Is $5(A-B) = 5A - 5B$? Is $(5A)^t = 5A^t$? Give reasons for your answers.

Solution: $A^t = \begin{bmatrix} 2 & 7 & -0.5 \\ 1 & -1 & 0 \end{bmatrix}$.

$$5A = \begin{bmatrix} 5 \times 2 & 5 \times 1 \\ 5 \times 7 & 5 \times (-1) \\ 5 \times (-0.5) & 5 \times 0 \end{bmatrix} = \begin{bmatrix} 10 & 5 \\ 35 & -5 \\ -2.5 & 0 \end{bmatrix}. \text{ Similarly, } 5B = \begin{bmatrix} 1.5 & -5/3 \\ 5 & 25 \\ -25 & 40 \end{bmatrix}.$$

$$\text{Also, } A+B = \begin{bmatrix} 2.3 & 2/3 \\ 8 & 4 \\ -5.5 & 8 \end{bmatrix} \text{ and } A-B = \begin{bmatrix} 1.7 & 4/3 \\ 6 & -6 \\ 4.5 & -8 \end{bmatrix}.$$

$$\text{So, } 5(A+B) = \begin{bmatrix} 11.5 & 10/3 \\ 40 & 20 \\ -27.5 & 40 \end{bmatrix}, 5(A-B) = \begin{bmatrix} 8.5 & 20/3 \\ 30 & -30 \\ 22.5 & -40 \end{bmatrix},$$

$$5A - 5B = \begin{bmatrix} 8.5 & 20/3 \\ 30 & -30 \\ 22.5 & -40 \end{bmatrix}, (5A)^t = \begin{bmatrix} 10 & 35 & -2.5 \\ 5 & -5 & 0 \end{bmatrix},$$

$$5A^t = \begin{bmatrix} 5 \times 2 & 5 \times 7 & 5 \times (-0.5) \\ 5 \times 1 & 5 \times (-1) & 5 \times 0 \end{bmatrix} = \begin{bmatrix} 10 & 35 & -2.5 \\ 5 & -5 & 0 \end{bmatrix}.$$

Looking at corresponding entries in the matrices, we find

$$5(A-B) = 5A - 5B \text{ and } (5A)^t = 5A^t.$$

What you see in the example above is not just true for these A , B and $\alpha = 5$. It is true in all cases, as the following theorem tells us.

Theorem 11: Let $A, B \in \mathbb{M}_{m \times n}(\mathbb{C})$ and $\alpha, \beta \in \mathbb{C}$. Then

- i) $\alpha(A + B) = \alpha A + \alpha B$,
- ii) $\alpha(A - B) = \alpha A - \alpha B$,
- iii) $(\alpha A)^t = \alpha A^t$.
- iv) $(\alpha\beta)A = \alpha(\beta A)$.

Proof: We shall prove (i), and ask you to complete the proof of this theorem (see E29).

i) Let $A = [a_{ij}]$, $B = [b_{ij}]$. Then

$$\begin{aligned}\alpha(A + B) &= \alpha[a_{ij} + b_{ij}] = [\alpha(a_{ij} + b_{ij})] = [\alpha a_{ij} + \alpha b_{ij}] \\ &= [\alpha a_{ij}] + [\alpha b_{ij}] = \alpha[a_{ij}] + \alpha[b_{ij}] \\ &= \alpha A + \alpha B.\end{aligned}$$

Hence, (i) is proved. ■

Solve the following exercises now.

E29) Prove Theorem 11(ii), (iii) and (iv).

E30) If $(0.5)C = \sqrt{2}A - \sqrt{3}B$, where $A = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$ and

$$B = \begin{bmatrix} \cos(\pi/3) & \sin(\pi/3) \\ -\sin(\pi/3) & \cos(\pi/3) \end{bmatrix}, \text{ find } C.$$

E31) Let \sim be defined on $\mathbb{M}_{m \times n}(\mathbb{C})$ by ' $A \sim B$ iff $A - B = 5C$ for some $C \in \mathbb{M}_{m \times n}(\mathbb{Z})$ '. Check whether or not \sim is an equivalence relation on $\mathbb{M}_{m \times n}(\mathbb{C})$. If it is, find $[0]$. Otherwise define an equivalence relation on $\mathbb{M}_{m \times n}(\mathbb{R})$.

Now let us look at how to multiply two matrices.

Matrix Multiplication

Consider $A = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 5 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & -1 \end{bmatrix}$ in $\mathbb{M}_{2 \times 3}(\mathbb{C})$. A natural way to

multiply them seems to be elementwise, as in addition. However, you will be surprised to know that the way matrix multiplication is usually defined, these matrices **cannot** be multiplied. You would definitely wonder why.

The way matrix multiplication is defined is linked with the fact that each matrix is a function, as you will study in the fifth semester course 'Linear Algebra'. In this scenario, multiplying two matrices corresponds to the composition of these two functions. Therefore, the usual matrix multiplication is not defined elementwise, but as you will soon see. This way of multiplying matrices appears to have been formulated by French mathematician Jacques Philippe Marie Binet (1786-1856) in 1812.

So let us see how two matrices are multiplied.

Consider $A = [-1 \ 3 \ 5]$ and $B = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}$.

$$\text{Then } AB = [-1 \quad 3 \quad 5] \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix} = (-1)(0) + (3)(2) + (5)(1) = 11.$$

So we can multiply a row vector with a column vector, **both having the same number of entries**, in this way. We use this multiplication to find the product of two matrices that satisfy a constraint, as you will see.

$$\text{Consider } A = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 5 & 2 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & -\pi \\ 0 & i \\ 2 & 7 \end{bmatrix}. \text{ So } A \text{ is a } 2 \times 3 \text{ matrix and } B \text{ is}$$

a 3×2 matrix. Their matrix product AB will be a 2×2 matrix. Let's see how we get it.

The **(1, 1)th** element of AB is the product of the **1st row** of A and the **1st column** of B ; the **(1, 2)th** element is the product of the **1st row** of A and the **2nd column** of B ; the **(2, 1)th** element is the product of the **2nd row** of A and the **1st column** of B ; and the **(2, 2)th** element is the product of the **2nd row** of A and the **2nd column** of B . So

$$A = \begin{bmatrix} [2 \ 5 \ 7] \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} & [2 \ 5 \ 7] \begin{bmatrix} -\pi \\ i \\ 7 \end{bmatrix} \\ [3 \ 5 \ 2] \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} & [3 \ 5 \ 2] \begin{bmatrix} -\pi \\ i \\ 7 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} 2(1) + 5(0) + 7(2) & 2(-\pi) + 5(i) + 7(7) \\ 3(1) + 5(0) + 2(2) & 3(-\pi) + 5(i) + 2(7) \end{bmatrix} = \begin{bmatrix} 16 & 49 - 2\pi + 5i \\ 7 & 14 - 3\pi + 5i \end{bmatrix}.$$

Note that AB is defined only if the number of elements in each row of A equals the number of elements in each column of B . This means that **the number of columns of A must equal the number of rows of B** .

Then, the number of rows in $AB =$ number of rows in A , and the number of columns in $AB =$ number of columns in B .

More generally, consider the following definition.

Definition: If $A = [a_{ij}] \in \mathbb{M}_{m \times n}(\mathbb{C})$ and $B = [b_{jk}] \in \mathbb{M}_{n \times s}(\mathbb{C})$, then the operation of **matrix multiplication** is defined to be

$\cdot : \mathbb{M}_{m \times n}(\mathbb{C}) \times \mathbb{M}_{n \times s}(\mathbb{C}) \rightarrow \mathbb{M}_{m \times s}(\mathbb{C}) : \cdot(A, B) = AB = [c_{ik}]$, where

$$c_{ik} = [a_{i1} \ a_{i2} \ \dots \ a_{in}] \cdot \begin{bmatrix} b_{1k} \\ b_{2k} \\ \vdots \\ b_{nk} \end{bmatrix} = \sum_{j=1}^n a_{ij} b_{jk}.$$

There are a couple of important observations that you should note again.

Remark 10: i) Two matrices A and B **cannot** be multiplied **unless** the number of columns in A equals the number of rows in B .

- ii) Note that by this definition any two $m \times n$ matrices ($m \neq n$) **cannot** be multiplied. Thus, **matrix multiplication is not a binary operation** on $M_{m \times n}(\mathbb{C})$, **unless** $m = n$.

Let us consider some examples in detail.

Example 11: Is the product of $A = \begin{bmatrix} 3 & 2 \\ -1 & 1 \\ -7/5 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 3 \\ 0 & 5 \end{bmatrix}$ defined? If

yes, find it. Also find BA , if it exists.

Solution: Since A is a 3×2 matrix and B is a 2×2 matrix, AB is defined, and is a 3×2 matrix. However, BA does not exist, since the number of columns in $B = 2 \neq 3$, the number of rows in A .

$$\begin{aligned}
 AB &= \begin{bmatrix} [3 \ 2] \begin{bmatrix} -1 \\ 0 \end{bmatrix} & [3 \ 2] \begin{bmatrix} 3 \\ 5 \end{bmatrix} \\ [-1 \ 1] \begin{bmatrix} -1 \\ 0 \end{bmatrix} & [-1 \ 1] \begin{bmatrix} 3 \\ 5 \end{bmatrix} \\ [-7/5 \ 0] \begin{bmatrix} -1 \\ 0 \end{bmatrix} & [-7/5 \ 0] \begin{bmatrix} 3 \\ 5 \end{bmatrix} \end{bmatrix} \\
 &= \begin{bmatrix} 3(-1) + 2(0) & 3(3) + 2(5) \\ (-1)(-1) + 1(0) & (-1)(3) + 1(5) \\ \left(-\frac{7}{5}\right)(-1) + 0(0) & \left(-\frac{7}{5}\right)(3) + 0(5) \end{bmatrix} \\
 &= \begin{bmatrix} -3 & 19 \\ 1 & 2 \\ \frac{7}{5} & -\frac{21}{5} \end{bmatrix}
 \end{aligned}$$

Example 12: If A and B are an $m \times n$ matrix and an $n \times s$ matrix, respectively, over \mathbb{C} , under what conditions on m , n and s will both AB and BA be defined? And then, is $AB = BA$? Why, or why not?

Solution: AB will always be defined since the number of columns in A equals the number of rows in B . Also AB is an $m \times s$ matrix.

BA will only be defined if $s = m$. And, in this case, AB and BA will be $m \times m$ and $n \times n$ matrices, respectively.

Hence, for $AB = BA$, it would mean that first both have to be of the same order, i.e., $m = n$.

However, even with $m = n$, they may not be equal.

For instance, if $A = \begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 1(1) + (-1)(1) & 1(0) + (-1)(0) \\ 2(1) + 0(1) & 2(0) + 0(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix} \text{ and}$$

$$BA = \begin{bmatrix} 1(1) + 0(2) & 1(-1) + 0(0) \\ 1(1) + 0(2) & 1(-1) + 0(0) \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}.$$

Hence, $AB \neq BA$.

Thus, in general, $AB \neq BA$ for $A, B \in \mathbb{M}_n(\mathbb{C})$.

Let us now consider some properties of matrix multiplication, through some examples.

Example 13: Let $A = \begin{bmatrix} 2 & -1 & 0 \\ 3 & 1 & -2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & -4 & 0 \\ 0 & 2 & 0 \\ 0 & 4 & 1 \end{bmatrix}$. Are AB and $B^t A^t$

defined? If so, find a relationship, if any, between $(AB)^t$ and $B^t A^t$. Otherwise check if $AB = BA^t$ or not.

Solution: You should verify that both AB and $B^t A^t$ are defined. Also

$$AB = \begin{bmatrix} 2(1) + (-1)(0) + 0(0) & 2(-4) + (-1)(2) + 0(4) & 2(0) + (-1)(0) + 0(1) \\ 3(1) + 1(0) + (-2)(0) & 3(-4) + 1(2) + (-2)(4) & 3(0) + 1(0) + (-2)(1) \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -10 & 0 \\ 3 & -18 & -2 \end{bmatrix}$$

$$\text{Hence, } (AB)^t = \begin{bmatrix} 2 & 3 \\ -10 & -18 \\ 0 & -2 \end{bmatrix}.$$

$$\text{Next, } B^t = \begin{bmatrix} 1 & 0 & 0 \\ -4 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } A^t = \begin{bmatrix} 2 & 3 \\ -1 & 1 \\ 0 & -2 \end{bmatrix}.$$

$$\text{Check that } B^t A^t = \begin{bmatrix} 2 & 3 \\ -10 & -18 \\ 0 & -2 \end{bmatrix}.$$

Thus, $(AB)^t = B^t A^t$.

Example 14: Let $A = \begin{bmatrix} 4 \\ 2 \\ -2 \end{bmatrix}$, $B = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}$ and $C = \begin{bmatrix} -1 & 2 \end{bmatrix}$. Are $AC + BC$ and

$(A + B)C$ defined? If yes, find them and the relationship between them. If either of them is not defined, explain why.

Solution: Here A , B and $A + B$ are 3×1 matrices, and C is a 1×2 matrix. Hence AC , BC and $(A + B)C$ are defined, and are 3×2 matrices.

$$\text{Now } AC = \begin{bmatrix} 4(-1) & 4(2) \\ 2(-1) & 2(2) \\ (-2)(-1) & (-2)(2) \end{bmatrix} = \begin{bmatrix} -4 & 8 \\ -2 & 4 \\ 2 & -4 \end{bmatrix}, \quad BC = \begin{bmatrix} -2 & 4 \\ -3 & 6 \\ -1 & 2 \end{bmatrix}.$$

$$A + B = \begin{bmatrix} 4+2 \\ 2+3 \\ (-2)+1 \end{bmatrix} = \begin{bmatrix} 6 \\ 5 \\ -1 \end{bmatrix}, \quad \text{so that } (A+B)C = \begin{bmatrix} -6 & 12 \\ -5 & 10 \\ 1 & -2 \end{bmatrix}.$$

$$\text{Also } AC + BC = \begin{bmatrix} -4 & 8 \\ -2 & 4 \\ 2 & -4 \end{bmatrix} + \begin{bmatrix} -2 & 4 \\ -3 & 6 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} -6 & 12 \\ -5 & 10 \\ 1 & -2 \end{bmatrix}.$$

Thus, $AC + BC = (A + B)C$.

$$\text{Example 15: Let } A = \begin{bmatrix} i & 7 & -1 \\ 0.25 & \pi & 0 \end{bmatrix}, \quad B = \begin{bmatrix} -2 \\ i \\ 1+3i \end{bmatrix} \text{ and } C = [-1 \ 0 \ 0 \ 1].$$

Show that $(AB)C$ and $A(BC)$ are defined, and are equal.

Solution: Here, note that AB is a 2×1 matrix, $BC \in \mathbb{M}_{3 \times 4}(\mathbb{C})$, and hence $(AB)C \in \mathbb{M}_{2 \times 4}(\mathbb{C})$ and $A(BC) \in \mathbb{M}_{2 \times 4}(\mathbb{C})$. Thus, $(AB)C$ and $A(BC)$ are both defined and have the same order. Now,

$$AB = \begin{bmatrix} -2i + 7i - (1+3i) \\ -0.5 + \pi i \end{bmatrix} = \begin{bmatrix} -1 + 2i \\ -0.5 + \pi i \end{bmatrix} \text{ and } BC = \begin{bmatrix} 2 & 0 & 0 & -2 \\ -i & 0 & 0 & i \\ -(1+3i) & 0 & 0 & 1+3i \end{bmatrix}.$$

$$\text{Therefore, } (AB)C = \begin{bmatrix} 1-2i & 0 & 0 & -1+2i \\ 0.5-\pi i & 0 & 0 & -0.5+\pi i \end{bmatrix} \text{ and}$$

$$A(BC) = \begin{bmatrix} 1-2i & 0 & 0 & -1+2i \\ 0.5-\pi i & 0 & 0 & -0.5+\pi i \end{bmatrix}.$$

Thus, $(AB)C = A(BC)$.

Example 16: For A and B in Example 13, show that $(\alpha A)B = \alpha(AB) = A(\alpha B) \forall \alpha \in \mathbb{C}$.

$$\text{Solution: Here } \alpha A = \begin{bmatrix} 2\alpha & -\alpha & 0 \\ 3\alpha & \alpha & -2\alpha \end{bmatrix}, \quad \alpha B = \begin{bmatrix} \alpha & -4\alpha & 0 \\ 0 & 2\alpha & 0 \\ 0 & 4\alpha & \alpha \end{bmatrix},$$

$$\alpha(AB) = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}.$$

$$\text{Also, } (\alpha A)B = \begin{bmatrix} 2\alpha & -\alpha & 0 \\ 3\alpha & \alpha & -2\alpha \end{bmatrix} \begin{bmatrix} 1 & -4 & 0 \\ 0 & 2 & 0 \\ 0 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}.$$

$$\text{Similarly, } A(\alpha B) = \begin{bmatrix} 2 & -1 & 0 \\ 3 & 1 & -2 \end{bmatrix} \begin{bmatrix} \alpha & -4\alpha & 0 \\ 0 & 2\alpha & 0 \\ 0 & 4\alpha & \alpha \end{bmatrix} = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}.$$

Thus, $(\alpha A)B = \alpha(AB) = A(\alpha B)$.

Example 17: Show that if $A = \begin{bmatrix} 3 & i \\ 1+\sqrt{2} & 0 \end{bmatrix}$ and $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $AI = IA = A$.

Solution: You can check that $AI = A$ and $IA = A$.

The Examples 13-17 are actually particular cases of properties that are more generally true, which we will now state. However, we will not prove them, only because the proofs can get quite messy. You will be using these properties frequently in the other units of this course.

P1 (Associative Law): If A, B, C are $m \times n, n \times p$ and $p \times q$ matrices, respectively, over \mathbb{C} , then $(AB)C = A(BC)$.

P2 (Distributive Law): If A is an $m \times n$ matrix and B, C are $n \times p$ matrices over \mathbb{C} , then $A(B+C) = AB+AC$.

P3 (Multiplicative Identity): Let I_n be the $n \times n$ matrix

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, \text{ i.e., } I_n = [a_{ij}], \text{ where } a_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Then $AI_n = A$ and $I_n A = A$, for every $m \times n$ matrix A over \mathbb{C} .

P4 If $\alpha \in \mathbb{C}$, and A, B are $m \times n$ and $n \times p$ matrices over \mathbb{C} , respectively, then $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

P5 If A, B are $m \times n, n \times p$ matrices over \mathbb{C} , respectively, then $(AB)^t = B^t A^t$.

Though the properties P1-P5 have been given for matrices over \mathbb{C} , they are valid for matrices over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{Z}_n, n \in \mathbb{N}$.

Why don't you use these properties to solve the following exercises now?

E32) Find AB, AC and BC , if they are defined, where

$$A = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix}, B = A^t \text{ and } C = \begin{bmatrix} 3 & \sqrt{3} \\ 1 & i \\ i & 1 \end{bmatrix}.$$

E33) Show that $(A+B)^2 = A^2 + AB + BA + B^2$, for any two $n \times n$ matrices A and B .

E34) The inventory of two textbook titles at each of three bookshops in a city

is given by $A = \begin{bmatrix} 9 & 12 \\ 15 & 4 \\ 7 & 0 \end{bmatrix}$. Here, the rows of A pertain to the different

shops and the columns of A denote the number of each textbook title available in the shop. The wholesale costs (in ₹) of the books are given by $C = [700 \quad 1200]^t$. Find AC , and interpret it in the given context.

E35) Consider the system of linear equations,

$$7x + 3y + 4z - 5 = 0$$

$$2x + 3y = 6$$

$$z - 4y = 19$$

Write it in the form $AX = B$, where A is a 3×3 matrix and X and B are 3×1 matrices.

(Hint: Take $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$.)

Just as you have defined matrices over \mathbb{C} , we can define them over any set.

For instance, $\begin{bmatrix} \bar{2} & \bar{3} & \bar{0} \\ \bar{1} & \bar{0} & \bar{4} \end{bmatrix} \in \mathbb{M}_{2 \times 3}(\mathbb{Z}_6)$, where all its entries are from \mathbb{Z}_6 .

Similarly, $\begin{bmatrix} -3 & 7 & 5 \\ 2 & 1 & -6 \end{bmatrix} \in \mathbb{M}_{2 \times 3}(\mathbb{Z})$. However, if we want to add matrices in

$\mathbb{M}_{m \times n}(S)$, where S is a set, according to the definition we can only do so if $+$ is a binary operation on S . Similarly, if we want to multiply matrices in $\mathbb{M}_m(S)$, then $+$ and \cdot should be binary operations on S .

So, for example, if $A, B \in \mathbb{M}_2(\mathbb{Z}_n)$, then $A + B$ and $A \cdot B$ are defined, where the elements are added and multiplied in \mathbb{Z}_n .

Thus, **all the definitions in this section are true for matrices over a non-empty set S , where $+$ and \cdot are binary operations on S** . All theorems will also be true for matrices over S , provided S satisfies certain conditions that you will study in Unit 2.

We shall end our introductory discussion on matrices here. Let us now consider another type of algebraic object, crucial for studying groups.

1.5 INTRODUCING PERMUTATIONS

Let us begin this discussion with looking at the word 'symmetry'. You must have heard this word many times in the context of beauty in nature, or in design. Here we shall consider symmetries of some two-dimensional objects in a plane.

Consider a flat object, say an equilateral triangle made of plastic, lying on a table. If you rotate it about its centroid, or flip it, or push it to another part of the table, does its shape or size change? No, they are not affected. This is why these actions on the triangle are examples of rigid body motions, a term we now define.

A **centroid** of a triangle is the intersection of its three medians.

Definition: A **rigid body motion** of an object X is an action on X that does not change its shape or size.

Thus, a rigid body motion of an object in a plane is a bijective function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that the distance between $f(x)$ and $f(y)$ is the same as the distance between x and $y \forall x, y \in \mathbb{R}^2$.

Now, let us go back to the equilateral triangle on the table. Draw its outline on the table. If you push the triangle 5cm along the table, its position will have clearly changed from its original position. Similarly, try rotating the triangle about its centroid through 90° on the table. Again, you will see that its position will not exactly cover the outline drawn on the table. It will change. But try rotating it about its centroid through 120° . What do you find? Has its position changed? No, it hasn't. This action is an example of what we now define.

Definition: A **symmetry** of an object in the plane is a rigid body motion that does not change the position of the object in the plane.

Thus, a symmetry of an object X in a plane is a bijection f from \mathbb{R}^2 to \mathbb{R}^2 such that $f(X) = X$. So, a symmetry cannot be any rigid body motion that displaces the object. For example, a translation will not be a symmetry.

A symmetry of the planar object can only be one of the following:

- i) **Reflection:** Taking the mirror image of all points of the object X about a line of symmetry (e.g., an angle bisector of the equilateral triangle).
- ii) **Rotation:** Rotating the object X in the plane through a certain angle in the anti-clockwise direction, about a centre point in the plane, such that the position of X is not changed after the rotation (e.g., rotating the equilateral triangle through 120° about its centroid).

Let us look at some examples in detail.

Example 18: Obtain D_6 , the set of symmetries of an equilateral triangle.

Solution: Consider the triangle with vertices 1, 2, 3 (as in Fig.4). Let r_i denote the reflection about the bisector of the angle at the vertex i . See Fig.5 as an example.

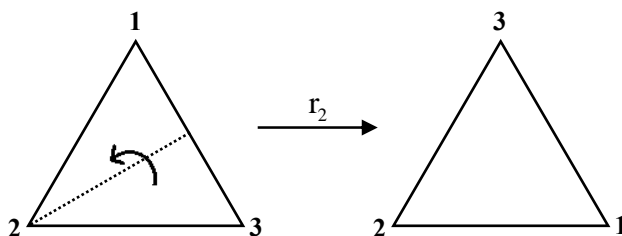


Fig.5: The reflection in the angle bisector of Vertex 2.

So, we can say r_2 is a function from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ that takes 1 to 3, 2 to 2 and 3 to 1.

Let R_{120} denote the rotation of the triangle about its centroid through 120° in the anti-clockwise direction (see Fig.6).

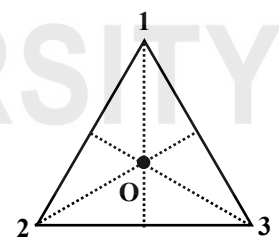


Fig.4: An equilateral triangle.

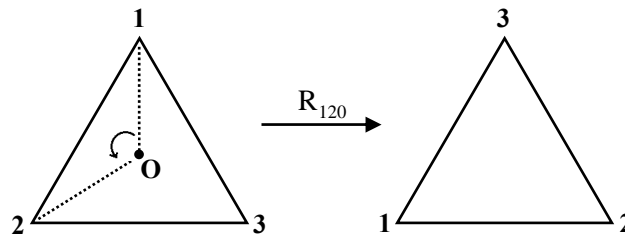


Fig.6: An anti-clockwise rotation through 120° about O, its centroid.

So R_{120} is the function from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ that takes 1 to 2, 2 to 3 and 3 to 1.

Let us represent these bijective functions from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ in the following two-row format:

$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ r_2(1) & r_2(2) & r_2(3) \end{pmatrix}, \text{ i.e., } r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \text{ and } R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

The identity function is also a symmetry, leaving the triangle 'unmoved', given by $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

Then you should verify that all the possible symmetries of the equilateral triangle are $I, r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$

$$R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, R_{240} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Thus, $D_6 = \{I, r_1, r_2, r_3, R_{120}, R_{240}\}$.

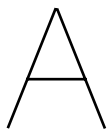
Now, see what happens if we apply r_1 twice to the triangle.

Then $r_1^2(1) = r_1 \circ r_1(1) = r_1(1) = 1, r_1^2(2) = r_1(3) = 2$ and $r_1^2(3) = r_1(2) = 3$.

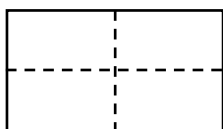
Thus, $r_1^2 = I$.

Similarly, you should check that $r_2^2 = I, r_3^2 = I, R_{120}^2 = R_{240}, R_{120}^3 = I,$

$$r_1 \circ R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_2, \text{ and so on.}$$



(i)



(ii)

Fig.7

Example 19: Give an example of an object that has

(i) no non-trivial rotation symmetry, (ii) exactly two reflection symmetries.

Solution: i) Consider the letter A (see Fig.7(i)). There is no point about which the rotation of this through any angle between 0° and 360° will give you the letter in the same position.

ii) Consider a rectangle with unequal sides (as in Fig.7(ii)). You should verify that the only reflection symmetries it has are about the lines joining the mid-points of opposite sides.

Try solving some exercises now.

E36) Write all the symmetries, in the two-row format, of

i) a square, ii) an isosceles triangle.

In Unit 2 you will see that D_6 is the **dihedral group** of order 6.

E37) Find all the symmetries of the letters N and B.

Generalising from what you have just studied, a **symmetry of a regular polygon** with n vertices is a bijective function from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$. The set of all these symmetries is denoted by D_{2n} . You will study more about these in later units.

So far you have studied a certain kind of bijective function. Let us move to a more general setting.

Definitions: Let X be a non-empty set.

- i) A bijection from X to X is called a **permutation of X** . We denote the set of all permutations of X by $S(X)$.
- ii) If $X = \{1, 2, \dots, n\}$, then $S(X)$ is denoted by S_n , and each element of S_n is called a **permutation on n symbols**.

Thus, a symmetry of an object is a permutation. But there are many more. For

example, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ in S_4 , that is, the function

$f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}: f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1$. However, this is not in the set you found in E36(i).

Suppose we want to construct an element f in S_n . How do we do this? We can start by choosing $f(1)$. Now, $f(1)$ can be any one of the n symbols $1, 2, \dots, n$. Having chosen $f(1)$, we can choose $f(2)$ from the set $\{1, 2, \dots, n\} \setminus \{f(1)\}$, since f is injective. Thus, $f(2)$ can be chosen in $(n-1)$ ways. Inductively, after choosing $f(i)$, we can choose $f(i+1)$ in $(n-i)$ ways. Thus, f can be chosen in $(1 \times 2 \times \dots \times n) = n!$ ways, i.e., S_n **contains $n!$ elements**.

As in the case of a symmetry, we can represent $f \in S_n$ in a 2-line format by

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

For example, take $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ in S_4 . The elements in the top row can

be placed in any order as long as the corresponding elements in the bottom row are changed in the same way.

Thus, $\begin{pmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ also represents the same function f above. However,

$\begin{pmatrix} 3 & 1 & 2 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ is not the same as f because, for example, this function takes 3 to 2, while $f(3) = 3$.

Now, let us look at the symmetry r_3 of Example 18. You saw that $r_3(3) = 3$, that is, r_3 fixes 3, according to the following definition.

Definition: A permutation f of a set X is said to **fix** $x \in X$ if $f(x) = x$, and **move** x if $f(x) \neq x$.

Thus, in Example 18, r_1 fixes 1, r_2 fixes 2 and r_3 fixes 3. Note that R_{120} does not fix any element and I fixes every element.

Now, in Example 18, you saw that one of the symmetries was

$$R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ i.e., } R_{120} \text{ takes } 1 \text{ to } 2, 2 \text{ to } 3, 3 \text{ to } 1. \text{ Thus, } R_{120} \text{ is an}$$

example of a permutation we shall now define.

Definition: A permutation $f \in S_n$ is called a **cycle of length r** (or an **r -cycle**), $r \in \mathbb{N}$, if there are x_1, \dots, x_r in $X = \{1, 2, \dots, n\}$ such that $f(x_i) = x_{i+1}$ for $1 \leq i \leq r-1$, $f(x_r) = x_1$, and f fixes t for $t \neq x_1, \dots, x_r$. In this case, f is written as $(x_1 \ x_2 \ \dots \ x_r)$.

For example, by $f = (2 \ 4 \ 5 \ 10) \in S_{10}$, we mean f is a permutation of $\{1, 2, \dots, 10\}$ such that $f(2) = 4$, $f(4) = 5$, $f(5) = 10$, $f(10) = 2$ and $f(j) = j$ for $j \in \{1, 2, \dots, 10\} \setminus \{2, 4, 5, 10\}$.

Thus, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$ is a cycle of length 4.

Isn't $(2 \ 4 \ 5 \ 10)$ a more elegant and short way of representing f , compared to the 2-line format?

As another example, consider $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$. This is the cycle

$(1 \ 2 \ 5 \ 3 \ 4)$ in S_5 , of length 5.

Note that, in the notation of a cycle, we don't mention the elements that are left fixed by the permutation.

Now, what is a cycle of length 1? Consider $(2) \in S_7$.

This maps 2 to 2, and 1, 3, 4, 5, 6, 7 are fixed. So, all the 7 symbols of $\{1, 2, \dots, 7\}$ are fixed by (2) . Thus, $(2) = I$. In the same way any 1-cycle is the identity function.

In this context, consider the following observation.

Remark 11: The reason a cycle gets its name is because of the way each element moves to the next, and the last element moves to the first element in the cycle. See Fig.8 for a visual interpretation.

Try solving some exercises now.

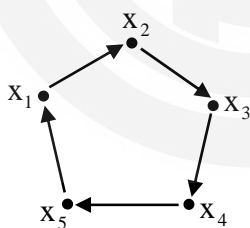


Fig.8: A visual representation of the cycle $(x_1 \ x_2 \ \dots \ x_5)$.

E38) Which of the symmetries in Example 18 are cycles? Is $D_6 = S_3$? Give reasons for your answers.

E39) Give a 3-cycle in S_7 , and its two-line representation.

Now, from the course 'Calculus', recall how we calculate the composition of two permutations, that is, the composition of two bijections. Consider the following example in S_5 .

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

$$\begin{aligned}
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha\beta(1) & \alpha\beta(2) & \alpha\beta(3) & \alpha\beta(4) & \alpha\beta(5) \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(5) & \alpha(3) & \alpha(4) & \alpha(1) & \alpha(2) \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2\ 4), \text{ since } 1, 3 \text{ and } 5 \text{ are left fixed here.}
 \end{aligned}$$

So $\alpha \circ \beta$ is a cycle of length 2.

Consider the following comment in this context.

Remark 12: Note that if α and β are bijections of X , then $\alpha \circ \beta$ is also a bijection of X , as you know from the course, 'Calculus'.

Do this exercise now.

E40) Write $\alpha = (1\ 3\ 2)$ and $\beta = (2\ 4\ 1)$ in S_4 in the 2-line format. Also check if $\alpha \circ \beta$ is a cycle. Further, is $\alpha^2 = \alpha \circ \alpha$ a cycle? Is β^2 a cycle? Is $\alpha \circ \beta = \beta \circ \alpha$? Give reasons for your answers.

With this we come to the end of this introduction to permutations. You will study these objects in Unit 2 also, and, in great detail, in Unit 9.

Let us now see what we have discussed in this unit.

1.6 SUMMARY

In this unit, you have studied the concepts and processes given pointwise below.

1. For $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $b|a$ iff $\exists c \in \mathbb{Z}$ s.t. $a = bc$.
2. The proof, and applications of, the **Division Algorithm**: Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \leq r < b$.
3. i) The g.c.d of any two elements $a, b \in \mathbb{Z}^*$ is $(a, b) = ma + nb$ for some $m, n \in \mathbb{Z}$. (In fact, $(a, 0)$ is also defined for $a \neq 0$, and $(a, 0) = a$.)
 ii) The l.c.m of any two elements $a, b \in \mathbb{Z}^*$ is $[a, b] = \frac{ab}{(a, b)}$.
4. The Euclidean algorithm for finding (a, b) , $a, b \in \mathbb{Z}^*$.
5. The proof, and the applications of, the **Fundamental Theorem of Arithmetic**: Every integer $n > 1$ can be written as $n = p_1 p_2 \dots p_n$, where p_1, \dots, p_n are prime numbers. Further, this representation is unique, except for the order in which the prime factors occur.
6. A partition of a non-empty set S defines an equivalence relation on S . Conversely, an equivalence relation on S defines a partition on S .

7. Examples, and basic terminology, pertaining to matrices.
8. Operations of the transpose of a matrix, addition and subtraction of two matrices in $M_{m \times n}(\mathbb{C})$, scalar multiplication in $M_{m \times n}(\mathbb{C})$, multiplication of an $m \times n$ matrix and an $n \times r$ matrix.
9. The definition, and examples, of a symmetry of an object in a plane.
10. The definition, and examples, of a permutation of any set X .
11. $|S_n| = n!$.
12. The definition, and examples, of a cycle of length r , $r \in \mathbb{N}$.

We shall now give the solutions to the exercises in the unit. Only look at them, once you have solved the exercises on your own. These have been given so that you can check them against your solutions to see how far you are on the right track. In particular, our solutions may help you **present the argument concerned in a mathematically well-reasoned way**. In some cases we have presented only the answer, or very brief solutions.

1.7 SOLUTIONS / ANSWERS

- E1) i) Since $a \cdot 0 = 0$, $a|0$.
 Since $1 \cdot a = a$ and $(-1)(-a) = a$, $(\pm 1)|a$ and $(\pm a)|a$.
- ii) $a|b \Rightarrow b = ad$, for some $d \in \mathbb{Z}$.
 $\Rightarrow bc = (ad)c = (ac)d$
 $\Rightarrow ac|bc$.
- iii) $b = ad$, $c = be$, for some $d, e \in \mathbb{Z}$,
 $\therefore c = ade$. $\therefore a|c$.
- iv) $a|b \Rightarrow b = ad$, for some $d \in \mathbb{Z}$
 $b|a \Rightarrow a = be$, for some $e \in \mathbb{Z}$.
 $\therefore a = ade \Rightarrow de = 1$, since $a \neq 0$.
 $\therefore e = \pm 1$.
 $\therefore a = \pm b$.
- Conversely, if $a = \pm b$, then from (i), $a|b$ and $b|a$.
- v) $c|a$ and $c|b \Rightarrow a = cd$, $b = ce$ for some $d, e \in \mathbb{Z}$.
 \therefore for any $x, y \in \mathbb{Z}$, $ax + by = c(dx + ey)$, and $dx + ey \in \mathbb{Z}$.
 $\therefore c|(ax + by)$.

E2) $75 = (2 \times 30) + 15$, $(-75) = [3 \times (-30)] + 15$.

E3) Let $a = 3q + r$, $0 < r < 3$. So $r = 1$ or 2 .

If $r = 1$, then $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$.

If $r = 2$, then $a^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3q' + 1$, where $q' = 3q^2 + 4q + 1$.

Thus, in both cases the remainder on dividing a^2 by 3 is 1.

E4) Let $a^2 + b^2 = 3c$, for some $c \in \mathbb{Z}$ (10)

Now, suppose $3|a$. Then $3|a^2$, say $a^2 = 3m$, for some $m \in \mathbb{Z}$.

So, by (10), $b^2 = 3(c - m)$, that is $3|b^2$.

So, by E3, $3|b$.

Similarly, if $3|b$, then $3|a$.

Now suppose $3 \nmid a$ and $3 \nmid b$. Then by E3,

$a^2 = 3q + 1$, and $b^2 = 3q' + 1$, for some $q, q' \in \mathbb{Z}$.

So $a^2 + b^2 = 3(q + q') + 2$, i.e., $3 \nmid (a^2 + b^2)$, a contradiction.

Hence, $3|a$ or $3|b$. But, if 3 divides either of them, you have already seen that 3 divides the other.

Hence, $3|(a^2 + b^2) \Rightarrow 3|a$ and $3|b$.

E5) i) Here $(a, b) = 7 = 1 \cdot 7 + 0 \cdot 21$. Thus, $m = 1$ and $n = 0$.

ii) Since 5 is a prime, and $5 \nmid 271$, $(-5, -271) = 1$.

Also $(-271) = (-5)54 - 1$. So $1 = 54(-5) + (-271)(-1)$.

So $m = 54$, $n = -1$ here.

iii) Here $(a, b) = (-c, c) = |c|$.

If $c > 0$, $(a, b) = c = 0(-c) + 1 \cdot c$.

If $c < 0$, $(a, b) = -c = 1(-c) + 0 \cdot c$.

E6) Let $d = (a, b)$.

Now, let $h = (-a, b)$ and $k = (-a, -b)$.

Since $d|a$, $d|(-a)$. So $d|h$.

Also $h|(-a) \Rightarrow h|a$. So $h|d$. Thus, $h = \pm d$.

But $h > 0$, $d > 0$. So $h = d$.

Similarly, show that $k = h$.

Thus, $d = h = k$.

E7) Suppose $p \nmid a$. Then $(p, a) = 1$. \therefore by Theorem 6, $p|b$.

E8) Let $P(n)$ be the predicate that

$p|a_1 a_2 \dots a_n \Rightarrow p|a_i$ for some $i = 1, 2, \dots, n$.

Verify that $P(1)$ is true.

Suppose $P(m-1)$ is true for some $m \geq 2$.

Now, let $p|a_1 a_2 \dots a_m$. Then $p|(a_1 \dots a_{m-1})a_m$.

By E7, $p|(a_1 a_2 \dots a_{m-1})$ or $p|a_m$.

If $p|a_1 a_2 \dots a_{m-1}$, then $p|a_i$ for some $i = 1, \dots, m-1$ (since $P(m-1)$ is true).

$\therefore p|a_i$ for some $i = 1, \dots, m$.

$\therefore P(m)$ is true.

$\therefore P(n)$ is true $\forall n \in \mathbb{N}$.

E9) You have $b > 0$, $q, r \in \mathbb{Z}$ s.t. $a = bq + r$.

Now, let $(a, b) = d$. Then $d|a$ and $d|b$. $\therefore d|(a - bq)$, i.e., $d|r$.

Also, if $c|b$ and $c|r$, then $c|(bq+r)$, i.e., $c|a$. So $c|d$.

Hence, $d = (b, r)$.

E10) i) Let $(p, a) = d$. Then $d|p$. So $d=1$ or $d=p$.

Since $d|a$ and $p \nmid a$, $d \neq p$. $\therefore d=1$.

ii) Now, if $a = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$, then $a^2 = p_1^{2m_1} p_2^{2m_2} \dots p_r^{2m_r}$.

So $p|a^2 \Rightarrow p = p_i$ for some $i=1, \dots, r$. So $p|a$.

E11) Suppose, to the contrary, $\sqrt{p} \in \mathbb{Q}$.

Then $\sqrt{p} = \frac{a}{b}$, where $a, b \neq 0$ and $(a, b) = 1$.

Then $\frac{a^2}{b^2} = p \Leftrightarrow a^2 = pb^2 \Rightarrow p|a^2$.

So, by E10(ii), $p|a$, say $pc = a$, for some $c \in \mathbb{Z}$.

Then $p^2 c^2 = a^2 = pb^2$.

So $pc^2 = b^2$. Hence, $p|b$.

So $p|(a, b)$, i.e., $p|1$, a contradiction.

Hence, $\sqrt{p} \notin \mathbb{Q}$.

E12) We shall prove the contrapositive (see Sec.1.3, Unit 1, Real Analysis) of the given statement, i.e, if $n^{1/m} \in \mathbb{Q}$, then $n^{1/m} \in \mathbb{Z}$ for $n, m \in \mathbb{N}$.

So, let $n^{1/m} = \frac{a}{b}$, where $(a, b) = 1$ and $b \neq 1$.

Then $n = \frac{a^m}{b^m}$, i.e., $b^m n = a^m$.

Let p be a prime s.t. $p|b^m$. Then, as in E10(ii), $p|b$.

Also $p|b^m \Rightarrow p|a^m \Rightarrow p|a$.

So $p|(a, b) = 1$, a contradiction.

Thus, $b=1$.

Hence, $n^{1/m} \in \mathbb{Z}$.

E13) By Theorem 7, $n = p_1 p_2 \dots p_t$, $t \geq 1$, where the p_i s may not all be distinct.

Now, by re-ordering the p_i s if necessary, let p_1 be the least of all the p_i s.

Let $p_1 = p_{i_1+1} = p_{i_1+2} = \dots = p_{i_1+m_1-1}$.

Since $p_i p_j = p_j p_i \forall i, j$, we can gather these m_1 p_i s together and write them as $p_1^{m_1}$.

Now look at $\frac{n}{p_1^{m_1}} = m$. Again choose the least among all the p_i s that m

is factored as. Put this as p_2 . Note that $1 < p_1 < p_2$. Now gather all the

m_2 p_i s which are equal to p_2 to get $m = p_2^{m_2} p_j p_{j+1} \dots p_s$.

So $n = p_1^{m_1} p_2^{m_2} p_j p_{j+1} \dots p_s$, where $t = m_1 + m_2 + (s - j + 1)$.

Continuing in this way, we get

$n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$, $1 < p_1 < \dots < p_r$, $m_1 + m_2 + \dots + m_r = t$.

$$E14) y = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}, r \geq 1, m_i \in \mathbb{N}, 1 < p_1 < p_2 < \dots < p_r.$$

If y is even, then $2 \mid y$. So $p_1 = 2$. Call $m_1 = r$.

Then $y = 2^r x$, where $x = p_2^{m_2} \dots p_r^{m_r}$ is odd since $2 \nmid x$.

If y is not even, then $y = 2^r y$, where $r = 0$.

Hence the result.

$$E15) i) \quad 54321 = 4(12345) + 4941 \quad \dots(11)$$

$$12345 = 2(4941) + 2463 \quad \dots(12)$$

$$4941 = 2(2463) + 15 \quad \dots(13)$$

$$2463 = 164(15) + 3 \quad \dots(14)$$

$$15 = 5(3) + 0.$$

$$\therefore (54321, 12345) = 3.$$

Next, $3 = 2463 - 164(15)$, from (14).

$$= 2463 - 164[4941 - 2(2463)], \text{ from (13).}$$

$$= 329(2463) - 164(4941)$$

$$= 329[12345 - 2(4941)] - 164(4941), \text{ from (12).}$$

$$= (329 \cdot 12345) - (822 \cdot 4941)$$

$$= (329 \cdot 12345) + (-822)[54321 - 4(12345)]$$

$$= (3617 \cdot 12345) + [(-822) \cdot 54321].$$

Thus, $m = -822$, $n = 3617$.

$$ii) \quad \text{First, } (-61880, -880) = (61880, 880).$$

$$\text{Now, } 61880 = 70(880) + 280 \quad \dots(15)$$

$$880 = 3(280) + 40 \quad \dots(16)$$

$$280 = 7(40) + 0$$

$$\therefore (61880, 880) = 40$$

Next, $40 = 880 - 3(280)$, from (16).

$$= 880 - 3[61880 - 70(880)], \text{ from (15).}$$

$$= [(-3) \cdot 61880] + (211 \cdot 880)$$

Hence, $m = -3$, $n = 211$.

E16) i) You should verify that R is reflexive and symmetric.

R is also transitive because if nRm and mRp , then

$$nm > 0, mp > 0 \Rightarrow (nm)(mp) > 0 \Rightarrow (np)m^2 > 0$$

$$\Rightarrow np > 0, \text{ since } m^2 > 0.$$

$$\Rightarrow nRp.$$

Here $[n] = \{m \in \mathbb{Z} \mid nm > 0\}$.

If $n < 0$, then $[n]$ is the set of negative integers. So $[n] = [-1]$.

Also any $n \in \mathbb{Z}^*$ is in $[1]$ or $[-1]$.

Hence, $\mathbb{Z}^* = [1] \cup [-1]$.

ii) You should show that R is an equivalence relation.

Also, here $\mathbb{Z}^* = [1] \cup [10] \cup [100] \cup \dots$, an infinite union.

This is because there are integers with m digits, for each $m \in \mathbb{N}$.

And any such integer is equivalent to 10^{m-1} .

E17) From Unit 1 of the course 'Real Analysis', you know that ' $p \Rightarrow q$ ' denotes that 'if p is true, then q is true'.
Clearly, if A is true, then A is true. So $A \Rightarrow A$.
Thus, ' \Rightarrow ' is reflexive.
Next, if $A \Rightarrow B$ and $B \Rightarrow C$, then B is true whenever A is true, and C is true whenever B is true. Hence, C is true, whenever A is true, i.e., $A \Rightarrow C$.
Thus, ' \Rightarrow ' is transitive.

Now consider

$A: a = b$, where $a, b \in \mathbb{C}$,

$B: |a| = |b|$, where $a, b \in \mathbb{C}$.

Then $A \Rightarrow B$, but $B \not\Rightarrow A$ (for example, $|\omega| = |1|$, where ω is a complex cube root of unity, but $\omega \neq 1$).

Thus, ' \Rightarrow ' is not symmetric.

E18) As in Example 4, you can find them to be $[0], [1], \dots, [7]$, corresponding to $\equiv (\text{mod } 8)$.

Now if $a \equiv b (\text{mod } 1)$, then $1|(a - b)$. Hence, $a = b + n$ for some $n \in \mathbb{Z}$.

Thus, $[a] = \{a + n | n \in \mathbb{Z}\}$.

Hence, $\mathbb{Z} = [0]$, since $[0] = \{n | n \in \mathbb{Z}\}$.

Thus, there is only one cell in this case.

E19) i) They are the elements in the 2th row and the 3th column.
Thus, they are 0 and 1, respectively.

ii) $[0 \ 0 \ 7]$.

iii) Only A is a square matrix. Its diagonal is $\{1, 5, 7\}$.

iv)
$$\begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix}$$

v) It does not exist, since B has only 3 rows.

E20) There are infinitely many such elements. Note that it is a 4×2 matrix with entries from \mathbb{Q} , of which **at least one entry** should not be in \mathbb{Z} .

For example, $A = \begin{bmatrix} 1 & 2 \\ -3 & -4 \\ 0.25 & 0 \\ 0 & 0 \end{bmatrix}$. This is not in $M_{4 \times 2}(\mathbb{Z})$, since $0.25 \notin \mathbb{Z}$.

However, all the entries of A are in \mathbb{Q} .

E21) Since the diagonal has 4 elements, the matrix has to be a 4×4 matrix.

From the given properties, we see that the matrix is
$$\begin{bmatrix} e & 0 & 0 & 0 \\ 1 & i & 0 & 0 \\ 1 & 1 & \pi & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$
.

E22) Since $\mathbb{N} \subseteq \mathbb{R}$, every matrix over \mathbb{N} is a matrix over \mathbb{R} . Hence, if

$A \in M_n(\mathbb{R})$, with $a_{ij} \in \mathbb{N} \forall i, j = 1, \dots, n$, then $A = [a_{ij}] \in M_n(\mathbb{N})$.

E23) Since $[3 \ 4]$ is of order 1×2 and $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ is of order 2×1 , they have different orders. Hence, they are not equal.

E24) No, since they have different orders.

E25) i)
$$\begin{bmatrix} 1+(-1) & 0+0 \\ 0+0 & 1+(-1) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

ii) $[0]_{m \times n} = \mathbf{0}$, the $m \times n$ matrix with all entries 0.

iii) $[a_{ij} + 0]_{m \times n} = [a_{ij}]_{m \times n}$.

E26)
$$A^t = \begin{bmatrix} -i & 0.2 & -1 \\ 1.5 & i & 0 \end{bmatrix}, B^t = \begin{bmatrix} \sqrt{2} & -\sqrt{2} & \pi \\ \sqrt{3} & -\sqrt{3} & 4 \end{bmatrix},$$

$$(A+B)^t = \begin{bmatrix} -i + \sqrt{2} & 0.2 - \sqrt{2} & -1 + \pi \\ 1.5 + \sqrt{3} & i - \sqrt{3} & 4 \end{bmatrix}.$$

Now $A^t + B^t = \begin{bmatrix} -i + \sqrt{2} & 0.2 - \sqrt{2} & -1 + \pi \\ 1.5 + \sqrt{3} & i - \sqrt{3} & 4 \end{bmatrix} = (A+B)^t$, as each entry in the corresponding position is the same.

E27) Let $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}]$.

i)
$$A + B = [a_{ij} + b_{ij}] = [b_{ij} + a_{ij}], \text{ since } + \text{ is commutative in } S.$$

$$= B + A.$$

ii)
$$A + (B + C) = [a_{ij} + (b_{ij} + c_{ij})] = [(a_{ij} + b_{ij}) + c_{ij}], \text{ since } + \text{ is associative in } S.$$

$$= (A + B) + C.$$

E28) i) Let $A = [a_{ij}]$, $(A^t)^t = [c_{ij}]$.

Firstly, note that if A is of order $m \times n$, then A^t is of order $n \times m$.

Hence, $(A^t)^t$ is of order $m \times n$.

Next, for $i = 1, \dots, m$; $j = 1, \dots, n$,

$$\begin{aligned} c_{ij} &= (i, j)\text{th entry of } (A^t)^t \\ &= (j, i)\text{th entry of } A^t \\ &= (i, j)\text{th entry of } A. \\ &= a_{ij}. \end{aligned}$$

Hence, $(A^t)^t = A$.

ii)
$$\begin{aligned} (A + A^t)^t &= A^t + (A^t)^t, \text{ by Theorem 10(ii).} \\ &= A^t + A, \text{ by (i) above.} \\ &= A + A^t, \text{ by E27(i).} \end{aligned}$$

Similarly, you should show that $(A - A^t)^t = -(A - A^t)$.

E29) ii) Let $A = [a_{ij}]$, $B = [b_{ij}]$.
 Then $A - B = [a_{ij} - b_{ij}]$.
 So $\alpha(A - B) = \alpha[a_{ij} - b_{ij}] = [\alpha(a_{ij} - b_{ij})] = [\alpha a_{ij} - \alpha b_{ij}]$
 $= [\alpha a_{ij}] - [\alpha b_{ij}]$
 $= \alpha[a_{ij}] - \alpha[b_{ij}]$
 $= \alpha A - \alpha B$.

iii) Let $A = [a_{ij}]_{m \times n}$. Then $\alpha A = [\alpha a_{ij}]_{m \times n}$.

The (i, j) th entry of $(\alpha A)^t$
 $=$ the (j, i) th entry of αA
 $= \alpha a_{ji}$
 $= \alpha$ (the (i, j) th entry of A^t).

This is true for every $i = 1, \dots, m$ and $j = 1, \dots, n$.

Hence, $(\alpha A)^t = \alpha A^t$.

iv) Let $A = [a_{ij}]$. Then $(\alpha\beta)A = (\alpha\beta)[a_{ij}] = [(\alpha\beta)a_{ij}] = [\alpha(\beta a_{ij})]$
 $= \alpha[\beta a_{ij}] = \alpha(\beta A)$.

E30) $\sqrt{2}A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\sqrt{3}B = \sqrt{3} \begin{bmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{bmatrix} = \begin{bmatrix} \sqrt{3}/2 & 3/2 \\ -3/2 & \sqrt{3}/2 \end{bmatrix}$.

So $\sqrt{2}A - \sqrt{3}B = \begin{bmatrix} \frac{2-\sqrt{3}}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{2-\sqrt{3}}{2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2-\sqrt{3} & -1 \\ 1 & 2-\sqrt{3} \end{bmatrix}$.

Thus, $C = \begin{bmatrix} 2-\sqrt{3} & -1 \\ 1 & 2-\sqrt{3} \end{bmatrix}$.

E31) You should show why \sim is reflexive, symmetric and transitive. Note that the entries of C are from \mathbb{Z} .

Then $[\mathbf{0}] = \{A \in M_{m \times n}(\mathbb{C}) \mid A - \mathbf{0} = 5C \text{ for some } C \in M_{m \times n}(\mathbb{Z})\}$
 $= \{5C \mid C \in M_{m \times n}(\mathbb{Z})\}$.

E32) Since A is a 2×3 matrix, and B and C are 3×2 matrices, AB and AC are defined, but BC is not defined.

Here $AB = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix} \begin{bmatrix} 9 & -3 \\ 5 & 0 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 122 & -35 \\ -35 & 13 \end{bmatrix}$, and

$AC = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix} \begin{bmatrix} 3 & \sqrt{3} \\ 1 & i \\ i & 1 \end{bmatrix} = \begin{bmatrix} 32-4i & -4+9\sqrt{3}+5i \\ -9+2i & 2-3\sqrt{3} \end{bmatrix}$

E33) Since $A, B \in M_n(\mathbb{C})$, $A + B \in M_n(\mathbb{C})$. Hence, $(A + B)^2$ is defined. Now

$(A + B)^2 = (A + B)(A + B) = A(A + B) + B(A + B)$, using P2.
 $= A \cdot A + AB + BA + B \cdot B$, using P2.
 $= A^2 + AB + BA + B^2$.

E34) Here $C = \begin{bmatrix} 700 \\ 1200 \end{bmatrix}$. Hence, $AC = [20,700 \ 15,300 \ 4,900]^t$, which represents the money invested by each shop for both the unsold titles.

E35) Let us rewrite the given equations as

$$7x + 3y + 4z = 5$$

$$2 + 3y + 0 \cdot z = 6$$

$$0 \cdot x - 4y + z = 19$$

Now if you look at the linear system (I) at the beginning of Sec.1.4, you will see how to write this in the required form.

$$\text{Take } A = \begin{bmatrix} 7 & 3 & 4 \\ 2 & 3 & 0 \\ 0 & -4 & 1 \end{bmatrix}, X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, B = \begin{bmatrix} 5 \\ 6 \\ 19 \end{bmatrix}.$$

Then check that the equations are given by the equivalent matrix equation $AX = B$.

E36) i) As we have done with an equilateral triangle, take a square. Draw its outline on a table. Number its vertices in the anti-clockwise direction, as in Fig.9. Now see how many lines of symmetry it has – for example, the line joining opposite vertices, or a line joining the mid-points of opposite sides, is a line of symmetry. Check if there can be any more. Again, rotate this square about its centre (which is the intersection of its diagonals) through 90° in the anti-clockwise direction. You will get a symmetry. What are the other rotational symmetries? In the following chart we give all the symmetries.

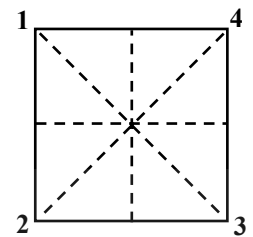


Fig.9: A square, and its 4 lines of reflection symmetry.

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

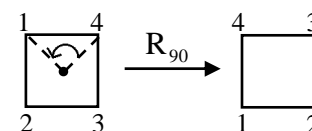
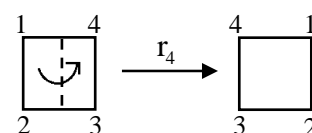
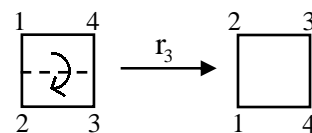
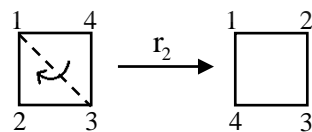
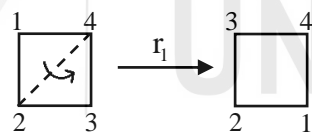
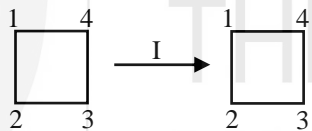
$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

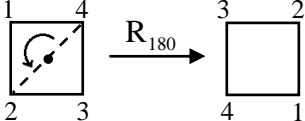
$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

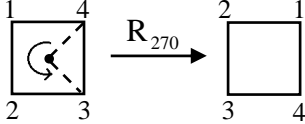
$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$



$$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$


$$R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$


You can take the composition of any of these, and find that it will be one of these only. For example, $r_1 \circ r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = R_{180}$.

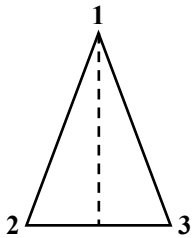


Fig.10: An isosceles triangle.

- ii) An isosceles triangle has only one line of symmetry (see Fig.10), and no non-trivial rotation. Thus, this set has only two elements, I and $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

E37) Verify that N has no reflection symmetry. It has two rotation symmetries, $R_0 = I$ and R_{180} .



Fig.11

B has the trivial rotation symmetry, I, and a reflection symmetry about the horizontal line shown in Fig.11. Thus, B, N and an isosceles triangle have the same number of symmetries.

E38) Every element of D_6 , apart from I, is a cycle.
 $r_1 = (2\ 3)$, $r_2 = (1\ 3)$, $r_3 = (1\ 2)$ are 2-cycles.
 $R_{120} = (1\ 2\ 3)$, $R_{240} = (1\ 3\ 2)$ are 3-cycles.

Also note that S_3 consists of 6 permutations of $\{1, 2, 3\}$. All these are in D_6 . Hence, $S_3 = D_6$.

E39) You can pick any, for example, $(1\ 3\ 5)$.

$$(1\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}$$

E40) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$
 $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)$, a 3-cycle.

You should check that $\alpha^2 = (1\ 2\ 3)$ and $\beta^2 = (1\ 4\ 2)$.

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

Since $\alpha \circ \beta(1) = 1$ and $\beta \circ \alpha(1) = 3$, $\alpha \circ \beta \neq \beta \circ \alpha$.

UNIT 2

GROUPS |

Structure

Page Nos.

2.1	Introduction	53
	Objectives	
2.2	What is a Group?	54
2.3	Elementary Properties of Groups	63
2.4	Some Important Groups	70
	Integers Modulo n	
	Symmetric Groups	
	Dihedral Groups	
	Matrix Groups	
	Roots of Unity	
	Direct Product	
2.5	Summary	84
2.6	Solutions / Answers	84

2.1 INTRODUCTION

In the courses you have studied so far, you have worked with many sets, as well as with binary operations on some sets. In this unit, you will study sets with binary operations defined on them that follow certain rules. These rules place an algebraic structure on the sets concerned. We call such an algebraic system a group.

The theory of groups is one of the oldest branches of abstract algebra. It has many applications in mathematics and in the other sciences. Group theory has helped in developing physics, chemistry and computer science, and, of course, mathematics! Its own roots go back to the work of the eighteenth century mathematicians Lagrange, Ruffini and Galois. With this unit, you will begin the study of this theory.

In Sec.2.2, you will study the definition of a group, and some examples of groups. Here you will also see the wide variety of groups – finite, infinite, commutative, non-commutative. In this section, you will also study about the tables of the binary operations involved in finite groups.

In Sec.2.3, we will discuss details of some basic properties that the elements of any group satisfy.

Finally, in Sec.2.4, you will be introduced to six types of well known, and often used, groups.

In future units we will be developing group theory further. Study this unit well, so that your foundation for the rest of the course is strong. Doing so, will help you achieve the learning expectations of studying this unit, which we are now going to list.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, groups;
- define, and give examples of, abelian and non-abelian groups;
- explain the difference between a finite and an infinite group;
- prove, and use, some basic properties of all groups;
- describe, and use, elementary group properties of the group of integers modulo n , symmetric groups, dihedral groups, groups of matrices over a group, the group of the n th roots of unity (for $n \in \mathbb{N}$) and the direct product of any two groups.

2.2 WHAT IS A GROUP?

In Calculus, you studied about sets and about binary operations. In this section, you will study a certain type of algebraic system consisting of a set with a binary operation. To understand what this system is, consider \mathbb{Z} , and the binary operation '+' on it. You have often used the following properties of integers:

- i) $(a + b) + c = a + (b + c) \quad \forall a, b, c \in \mathbb{Z}$,
- ii) $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$,
- iii) Given $a \in \mathbb{Z}$, we have $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0$.

It is these three properties that make $(\mathbb{Z}, +)$ a group, as you will now see.

Definition: Let G be a non-empty set and $*$ be a binary operation on G . The pair $(G, *)$ is called a **group** if

- G1) $*$ is **associative**, i.e., $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$.
- G2) G contains an element e such that $a * e = a = e * a \quad \forall a \in G$. (Here e is called an **identity element of G for $*$** .)
- G3) for every element a in G , there is an element b in G such that $a * b = e = b * a$. (Here b is called an **inverse of a in G with respect to $*$** .)

You have seen that $(\mathbb{Z}, +)$ is a group. Let us look at another example.

Example 1: Show that $(\mathbb{R}, +)$ is a group, but (\mathbb{R}, \cdot) is not.

Solution: You know that $+$ is an associative binary operation on \mathbb{R} . An identity element with respect to $+$ is 0 , and an inverse of $r \in \mathbb{R}$ w.r.t. $+$ is $(-r)$. Thus, $(\mathbb{R}, +)$ satisfies G1, G2 and G3. Therefore, it is a group.

Now, you know that multiplication in \mathbb{R} is an associative binary operation and $1 \in \mathbb{R}$ is a multiplicative identity. But does every element in \mathbb{R} have a multiplicative inverse? For instance, does 0 have an inverse with respect to \cdot ? No, since there is no real number r such that $r \cdot 0 = 1$. Hence, (\mathbb{R}, \cdot) does not satisfy G3.

Therefore, (\mathbb{R}, \cdot) is not a group.

Consider the following related observation.

Remark 1: $(G, *)$ is called a **semigroup** if $*$ satisfies the property G1. Thus, **every group is a semigroup**. Thus, (\mathbb{R}, \cdot) is a semigroup, since it satisfies G1. So, this is an example of a **semigroup that is not a group**.

Doing the following exercise will give you some more examples of groups.

E1) Check whether or not $(\mathbb{Q}, +)$, (\mathbb{R}^*, \cdot) and $(\mathbb{C}, -)$ are groups.

Recall that $S^* = S \setminus \{0\}$,
for any set S containing 0.

E2) Is the set of 2-cycles in S_3 a group w.r.t. the composition of functions?
Why, or why not?

You have seen that to show that $(G, *)$ is a group, you need to show that G satisfies G1, G2 and G3. For G2, you have to show that there is an $e \in G$ s.t. $a * e = a$ **and** $e * a = a$. Similarly, for G3 you need to show that given $a \in G \exists b \in G$ s.t. $a * b = e$ **and** $b * a = e$. However, as you will now see, it is sufficient to show that $*$ satisfies the following axioms.

- G1') $*$ is associative (which is the same as G1),
- G2') $\exists e \in G$ such that $a * e = a \forall a \in G$,
- G3') Given $a \in G, \exists b \in G$ such that $a * b = e$.

What we are saying is that the two sets of axioms G1, G2, G3 and G1', G2', G3' are equivalent. That is, to show that $(G, *)$ is a group, we only need to prove that $a * e = a$ and that an inverse b of any $a \in G$ only needs to satisfy $a * b = e$. We **do not need** to show **both** $a * e = a$ **and** $e * a = a$, or $a * b = e$ **and** $b * a = e$.

In fact, G1, G2 and G3 (taken together) are also equivalent to the following axioms:

- G1'') $*$ is associative,
- G2'') $\exists e \in G$ such that $e * a = a \forall a \in G$,
- G3'') Given $a \in G, \exists b \in G$ such that $b * a = e$.

Of course, as you can see, if $(G, *)$ satisfies G1, G2 and G3, then it certainly satisfies G1', G2' and G3'. Theorem 1, below, tells us that if $(G, *)$ satisfies G1', G2', G3', then it satisfies G1, G2 and G3. Once Theorem 1 is proved, you have the equivalence of G1, G2, G3 and G1', G2', G3'.

(A theorem on the same lines holds for showing the equivalence of G1, G2, G3 and G1'', G2'', G3''.)

Theorem 1: Let $(G, *)$ satisfy $G1'$, $G2'$ and $G3'$. Then $e * a = a \forall a \in G$. Also, given $a \in G$, if $\exists b \in G$ such that $a * b = e$, then $b * a = e$. Thus, $(G, *)$ satisfies $G1, G2$ and $G3$.

To prove this theorem, let us first prove the following result that we will need.

A **lemma** is a proved statement that is needed to prove a theorem.

Lemma 1: Let $(G, *)$ satisfy $G1'$, $G2'$ and $G3'$. If $\exists a \in G$ such that $a * a = a$, then $a = e$.

Proof: By $G3'$, we know that $\exists b \in G$ such that $a * b = e$.

Now $(a * a) * b = a * b = e$.

Also, $a * (a * b) = a * e = a$.

Therefore, by $G1'$, $a = e$. ■

Now we will use this lemma to prove Theorem 1.

Proof of Theorem 1: $G1$ holds since $G1$ and $G1'$ are the same axiom.

We will next prove that $G3$ is true. For this, let $a \in G$. By $G3'$, $\exists b \in G$ such that $a * b = e$. Now,

$(b * a) * (b * a) = (b * (a * b)) * a$, by $G1$.

$= (b * e) * a = b * a$, by $G2'$.

Therefore, by Lemma 1, $b * a = e$. Therefore, $G3$ is true.

Now, we will show that $G2$ holds. So, let $a \in G$.

Then, by $G2'$, $a * e = a$.

Since $G3$ holds, $\exists b \in G$ such that $a * b = b * a = e$.

Then $e * a = (a * b) * a = a * (b * a) = a * e = a$.

That is, $G2$ also holds.

Thus, $(G, *)$ satisfies $G1, G2$ and $G3$. ■

So, you have seen that the 3 sets of axioms $G1, G2, G3; G1', G2', G3'; G1'', G2'', G3''$ are equivalent. Consider the following important remarks in this context.

Remark 2: i) Have you noticed the order in which the axioms $G1, G2$ and $G3$, or $G1', G2', G3'$, are given? The order of $G2$ and $G3$ is important because $G3$ makes no sense unless $G2$ is stated first. The same goes for $G2'$ and $G3'$, or $G2''$ and $G3''$.

ii) Note that if $(S, *)$ satisfies $G1', G2'$ and $G3''$, or $G1', G2''$ and $G3'$, it **need not be a group**.

For instance, consider $* : \{a, b\} \times \{a, b\} \rightarrow \{a, b\}$, defined by

$x * y = x \forall x, y \in S = \{a, b\}$.

Then $*$ is a well-defined binary operation on S . You can check that it satisfies $G1'$.

Also, $a * a = a$, $b * a = b$. So, we can take a to be an identity, e . Thus, $G2'$ is also satisfied.

Next, $a * a = a$, $a * b = a$. So $G3''$ is satisfied.

However, the definition of a group, requires $b * a = a$ also, which is not true.

Hence, $(S, *)$ is not a group.

So, for the equivalence of axioms, we must have all 3 **of the same set of axioms** being satisfied.

Now, you know that $(G, *)$ has an identity because of $G2$ (or $G2'$). For instance, $(\mathbb{Z}, +)$ has an identity 0. Can $(\mathbb{Z}, +)$ have another additive identity? This is what the next result is about.

Theorem 2: Let $(G, *)$ be a group. Then G has a **unique** identity w.r.t. $*$, and each element in G has a **unique** inverse w.r.t. $*$.

Proof: Suppose e and e' are two identities of G w.r.t. $*$.

Then, since e is an identity,

$$e * e' = e'. \quad \dots(1)$$

Since e' is an identity,

$$e * e' = e. \quad \dots(2)$$

(1) and (2) tell us that $e = e'$.

Thus, G has a unique identity e w.r.t. $*$.

Now, let $a \in G$, and let $b, c \in G$ be inverses of a w.r.t. $*$. So,

$$a * b = e = b * a, \quad a * c = e = c * a.$$

$$\text{Then } b = b * e = b * (a * c)$$

$$= (b * a) * c = e * c$$

$$= c.$$

Hence, a has a unique inverse w.r.t. $*$. ■

Because of Theorem 2, we can say **the** identity of G , instead of *an* identity of G , and **the** inverse of each $a \in G$.

Let us now consider an example of the use of Theorem 1.

Example 2: Check whether or not $(M_3(\mathbb{R}), +)$ is a group.

Solution: Firstly, note that $M_3(\mathbb{R})$ is **closed** w.r.t. $+$, i.e., $+$ is a binary operation on $M_3(\mathbb{R})$, since $A + B \in M_3(\mathbb{R}) \quad \forall A, B \in M_3(\mathbb{R})$.

Secondly, from Sec.1.4, Unit 1, you know that $+$ is associative, so that $G1'$ is true.

Thirdly, for any $A \in M_3(\mathbb{R})$, $A + \mathbf{0} = A$, where $\mathbf{0}$ is the 3×3 matrix with all its entries being 0. Thus, $G2'$ holds.

Finally, given $A = [a_{ij}] \in M_3(\mathbb{R})$, $\exists B = [-a_{ij}] \in M_3(\mathbb{R})$ such that $A + B = \mathbf{0}$.

So, $G3'$ holds too.

Hence, by Theorem 1, $(M_3(\mathbb{R}), +)$ is a group.

On the same lines as in Example 2, you can show that $(M_n(\mathbb{R}), +)$ is a **group** $\forall n \in \mathbb{N}$.

Why don't you try solving some exercises now?

E3) Check whether or not each of the following is a group:

i) $(M_{2 \times 3}(\mathbb{C}), +)$, ii) $(M_3(\mathbb{C}), \cdot)$, iii) (\mathbb{Q}^*, \cdot) , iv) (\mathbb{Z}^*, \cdot) .

E4) Let \mathbb{R}^+ and \mathbb{R}^- denote the set of positive real numbers and the set of negative real numbers, respectively. Check whether or not (\mathbb{R}^+, \div) and (\mathbb{R}^-, \cdot) are groups.



Fig. 1: Arthur Cayley

So far you have seen examples of groups G in which the set G is infinite. So, are the underlying sets of all groups infinite? This is not so. We shall discuss some examples of groups with the underlying sets being finite. For this, you need to know what an operation table is.

Operation Table

Let S be a finite set and $*$ be a binary operation on S . We can represent the binary operation by a square table, called **an operation table**, or a **Cayley table**. The Cayley table is named after the famous British mathematician Arthur Cayley (1821-1895). They were first given in a research article by Cayley in 1854.

To write this table, we first list the elements of S vertically as well as horizontally, **in the same order**. Then we write $a * b$ in the table at the intersection of **the row** headed by **a** and **the column** headed by **b**. For example, if $S = \{-1, 0, 1\}$ and the binary operation is multiplication, denoted by \cdot , then the operation \cdot can be represented by Table 1.

Table 1

\cdot	-1	0	1
-1	$(-1) \cdot (-1)$ = 1	$(-1) \cdot 0$ = 0	$(-1) \cdot 1$ = -1
0	$0 \cdot (-1)$ = 0	$0 \cdot 0$ = 0	$0 \cdot 1$ = 0
1	$1 \cdot (-1)$ = -1	$1 \cdot 0$ = 0	$1 \cdot 1$ = 1

Conversely, if we are given a table, we can define a binary operation on S . For example, we can define the operation $*$ on $S = \{1, 2, 3\}$ by Table 2.

Table 2

*	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

From Table 2, you can see that all the entries are from S . Hence $*$ is a binary operation on S .

Further, the table tells us that, $1 * 2 = 2$ and $2 * 3 = 2$.

Also, $2 * 1 = 3$ and $1 * 2 = 2$. $\therefore 2 * 1 \neq 1 * 2$, that is, $*$ is not commutative in this example.

Again, $(2 * 1) * 3 = 3 * 3 = 1$ and $2 * (1 * 3) = 2 * 3 = 2$.

$\therefore (2 * 1) * 3 \neq 2 * (1 * 3)$. Therefore, $*$ is not associative in this case.

See how much information a mere table can give!

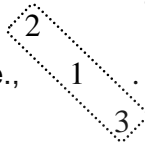
In Table 2 you have seen that $*$ is a binary operation which is not commutative. Actually, by looking at an operation table, you can immediately decide if $*$ is commutative or not. Let's see how. Consider the table below, for a binary operation $*'$ on $\{1, 2, 3\}$.

Table 3

$*'$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

If you look at the entries of Table 3, you will see that they are symmetric about the diagonal starting from the upper left entry of the table and ending at the

bottom right entry of the table, i.e.,



This symmetry shows that $2 *' 1 = 1 *' 2$, $2 *' 3 = 3 *' 2$, etc.

So, if this symmetry is not there in an operation table, the operation will not be commutative. For example, this symmetry is missing in Table 2.

Why don't you try solving a small exercise now?

E5) Complete the following table for the operation $*$ on $S = \{0, 1, 2, 3\}$ so that $*$ is closed on S and $*$ is commutative on S .

$*$	0	1	2	3
0	0	1	2	3
1		2	3	
2			0	1
3		0		2

Let us now consider some finite sets, and see if operations can be defined on them so that they form groups. Look at the following example.

Example 3: Consider the set $G = \{a_1, a_2, a_3, a_4\}$ on which an operation \cdot is defined by the Cayley table given below:

Table 4

\cdot	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_3	a_2	a_1

The group in Example 3 is called the Klein 4-group, named after the mathematician, Felix Klein.

Check whether or not (G, \cdot) is a group.

Solution: By looking at the entries in Table 4, we get the following information:

- i) All the entries are in G . Hence, \cdot is a binary operation on G .
- ii) $(a_1 \cdot a_2) \cdot a_3 = a_2 \cdot a_3 = a_4$, and
 $a_1 \cdot (a_2 \cdot a_3) = a_1 \cdot a_4 = a_4$.
 Thus, $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$.
 Similarly, **you should check that**
 $(a_i \cdot a_j) \cdot a_k = a_i \cdot (a_j \cdot a_k) \forall i, j, k = 1, 2, 3, 4$.
 Thus, \cdot is associative.
- iii) Since $a_1 \cdot a_i = a_i \forall i = 1, 2, 3, 4$, a_1 is the identity w.r.t. \cdot .
- iv) Since $a_1 \cdot a_1 = a_1$, $a_2 \cdot a_2 = a_1$, $a_3 \cdot a_3 = a_1$, $a_4 \cdot a_4 = a_1$, every element of G has an inverse w.r.t. \cdot . In fact, each element is its own inverse in this case.

Hence, (G, \cdot) is a group.

In the table of Example 3, note that no element is repeated in a row or in a column. The following comment is related to this.

Remark 3: The Cayley table of the operation of a group $(G, *)$ cannot have the same element repeated in a row or a column. This is because for $a, b, c \in G$, $a * b = a * c$ (in the row corresponding to a) iff $b = c$, as you will see in Theorem 3 later.

Similarly, $a * b = c * b$ (in the column corresponding to b) iff $a = c$.

Now consider another example where G is finite.

Example 4: Let $G = \{\pm 1, \pm i\}$, $i = \sqrt{-1}$. Check whether or not G is a group w.r.t. multiplication.

Solution: The Cayley table for multiplication in G is:

Table 5

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

This table shows us that \cdot is a binary operation on G .

Since \cdot is associative in \mathbb{C} , and $G \subseteq \mathbb{C}$, \cdot is associative in G .

The table also shows us that $a \cdot 1 = a \forall a \in G$. Therefore, 1 is the identity element w.r.t. \cdot .

Finally, since 1 is in each row, the table shows us that (G, \cdot) satisfies $G3'$.

Therefore, (G, \cdot) is a group.

In Example 4, note that
 $G = \{1, x, x^2, x^3\}$,
 where $x = i$.

From Examples 3 and 4 you can see how we can use Theorem 1 to decrease the amount of checking we have to do to prove that an algebraic system is a group.

Consider a remark about these two examples now.

Remark 4: Note that the groups in both, Example 3 and Example 4, have 4 elements. But if you replace a_1, a_2, a_3, a_4 of Example 3, by $1, -1, i, -i$, in any order, in Table 4, you will find the Cayley tables will not be the same. From Table 4, you find that $a^2 = e \forall a \in G$ in Example 3. Table 5 shows that $i^2 \neq 1$ in Example 4. So the Cayley tables are essentially different. This shows that the algebraic structures of the two groups are different.

Now, as you have seen, the underlying set of a group can be finite or infinite. In this context, we have the following definitions.

Definitions: Let $(G, *)$ be a group.

- i) If G is a finite set consisting of n elements, then $(G, *)$ is called a **finite group of order n** . Here we write $o(G) = n$, where $o(G)$ denotes 'the order of G '.
- ii) If G is an infinite set, then $(G, *)$ is called an **infinite group**.
- iii) If $*$ is commutative on G , i.e., $a * b = b * a \forall a, b \in G$, then $(G, *)$ is called a **commutative group**, or an **abelian group**.
- iv) If $(G, *)$ is not an abelian group, it is called a **non-abelian group**, or a **non-commutative group**.

Thus, the group in Example 4 is a finite abelian group of order 4. The groups in Examples 1 and 2 are infinite abelian groups.

Now let us look at an example of a non-abelian group.

Example 5: Let G be the set of all 2×2 real matrices with non-zero

determinant, that is, $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$.

Show that (G, \cdot) is a non-abelian group, where \cdot is matrix multiplication.

Solution: First, we will show that \cdot is a binary operation. From Sec.1.4, Unit 1, you know that if $A, B \in G$, $A \cdot B$ is a 2×2 matrix.

Also, you can check that

$$\det(A \cdot B) = (\det A) \cdot (\det B) \neq 0, \text{ since } \det A \neq 0, \det B \neq 0.$$

Hence, $A \cdot B \in G \forall A, B \in G$.

From Unit 1, you also know that matrix multiplication is associative and

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity. Note that $\det(I) = 1$, and hence $I \in G$.

Now, for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G , the matrix $B = \begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$ is such that



Fig. 2: Abelian groups are named after the gifted young Norwegian mathematician Niels Henrik Abel (1802-1829).

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

$ad - bc$ is called the **determinant** of A , and is written as **$\det A$** , or **$|A|$** .

$$\det(AB) = (\det A)(\det B)$$

$$\det B = \frac{1}{ad - bc} \neq 0, \text{ and } AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \text{ Thus, } B = A^{-1}.$$

Thus, (G, \cdot) is a group.

Next, let us see why G is non-abelian. Since, for example,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix},$$

we see that (G, \cdot) is not commutative.

The infinite non-abelian group in Example 5 is usually denoted by $GL_2(\mathbb{R})$, and is called the **general linear group of degree 2 over \mathbb{R}** . We will be using this group off and on for examples throughout the course.

Now let us consider an example related to functions.

Example 6: Consider the set \mathcal{F} , of all functions from \mathbb{R} to \mathbb{R} . Check whether or not \mathcal{F} is a group with respect to pointwise addition, i.e., for $f_1, f_2 \in \mathcal{F}$, $(f_1 + f_2): \mathbb{R} \rightarrow \mathbb{R}: (f_1 + f_2)(x) = f_1(x) + f_2(x) \forall x \in \mathbb{R}$.

Solution: Firstly, $I \in \mathcal{F}$, where $I: \mathbb{R} \rightarrow \mathbb{R}: I(x) = x$. Hence, $\mathcal{F} \neq \emptyset$.

Next, for $f_1, f_2 \in \mathcal{F}$, $f_1 + f_2$ is also a function from \mathbb{R} to \mathbb{R} . Hence, $+$ is a binary operation on \mathcal{F} .

Thirdly, for $f_1, f_2, f_3 \in \mathcal{F}$ and $r \in \mathbb{R}$,

$$\begin{aligned} [(f_1 + f_2) + f_3](r) &= (f_1 + f_2)(r) + f_3(r) \\ &= (f_1(r) + f_2(r)) + f_3(r) = f_1(r) + (f_2(r) + f_3(r)) \\ &= [f_1 + (f_2 + f_3)](r). \end{aligned}$$

Hence, $+$ is associative in \mathcal{F} .

Fourthly, $\mathbf{0}$ is the additive identity of \mathcal{F} , where $\mathbf{0}: \mathbb{R} \rightarrow \mathbb{R}: \mathbf{0}(x) = 0$.

Finally, given $f \in \mathcal{F}$, $\exists -f \in \mathcal{F}$, where $(-f): \mathbb{R} \rightarrow \mathbb{R}: (-f)(x) = -f(x)$. Then $f + (-f) = \mathbf{0}$.

Hence, $(\mathcal{F}, +)$ satisfies all the axioms for being a group.

Note that \mathcal{F} is an abelian group, since $f_1 + f_2 = f_2 + f_1 \forall f_1, f_2 \in \mathcal{F}$.

And now, another example of an abelian group.

Example 7: Consider the set T , of all translations of \mathbb{R}^2 , that is,

$$T = \{f_{a,b}: \mathbb{R}^2 \rightarrow \mathbb{R}^2 \mid f_{a,b}(x, y) = (x + a, y + b), \text{ for some } a, b \in \mathbb{R}\}.$$

Note that each element $f_{a,b}$ in T is represented by a point (a, b) in \mathbb{R}^2 .

Show that T is an abelian group w.r.t. the composition of functions.

Solution: Let us first see if \circ is a binary operation on T .

For $a, b, c, d \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned} f_{a,b} \circ f_{c,d}(x, y) &= f_{a,b}(x + c, y + d) = (x + c + a, y + d + b) \\ &= (x + a + c, y + b + d), \text{ since } + \text{ is commutative in } \mathbb{R}. \\ &= f_{a+c, b+d}(x, y). \end{aligned}$$

$$\therefore f_{a,b} \circ f_{c,d} = f_{a+c, b+d} \in T. \quad \dots(3)$$

Since $a + c \in \mathbb{R}$ and $b + d \in \mathbb{R}$, $f_{a,b} \circ f_{c,d} \in T$.

Thus, \circ is a binary operation on T .

Next, $f_{a,b} \circ f_{0,0} = f_{a,b} \in T$, using (3).

Therefore, $f_{0,0}$ is the identity element w.r.t. \circ .

Also, $f_{a,b} \circ f_{-a,-b} = f_{0,0}$, for $f_{a,b} \in T$, using (3).

Therefore, $f_{-a,-b}$ is the inverse of $f_{a,b} \in T$ w.r.t. \circ .

Thus, (T, \circ) satisfies $G1'$, $G2'$ and $G3'$, and hence is a group.

Note that $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} \forall f_{a,b}, f_{c,d} \in T$. Therefore, (T, \circ) is abelian.

Try the following exercises now.

E6) Which of the following statements are true? Give reasons for your answers.

- i) (\mathbb{C}^*, \cdot) is an abelian group.
- ii) (\mathbb{R}^*, \cdot) is a finite group.
- iii) $(\mathbb{Z}_o, +)$ is a group, where \mathbb{Z}_o is the set of odd integers.
- iv) (\mathbb{Q}, \cdot) is a semigroup.
- v) $(\mathbb{Q}^+, *)$ is a group, where \mathbb{Q}^+ is the set of positive rationals, and $*$ is defined on $\mathbb{Q}^+ \times \mathbb{Q}^+$ by $a * b = 2ab$.

E7) Show that $(G, *)$ is a non-abelian group, where

$G = \{(a, b) \mid a, b \in \mathbb{R}, a \neq 0\}$ and $*$ is defined on $G \times G$ by

$$(a, b) * (c, d) = (ac, bc + d).$$

E8) Give an example of the table of a binary operation $*$ on a finite set G which shows that $(G, *)$ cannot be a group. Justify your example.

We will now look at some basic properties that elements of any group satisfy.

2.3 ELEMENTARY PROPERTIES OF GROUPS

In this section we shall discuss some elementary properties that group elements satisfy. But first, note some conventions we will be following.

Remark 5: Henceforth, for convenience, we will **denote a group** $(G, *)$ **by** G only, if there is no confusion about the operation concerned.

We will also denote $a * b$ **by** \mathbf{ab} , for $a, b \in G$, and say that we are **multiplying** a **and** b .

And finally, we will **denote the group identity by e** , and the **inverse of $a \in G$ by a^{-1}** .

Now let us consider some simple properties of a group. You know that whenever $ba = ca$ or $ab = ac$ for a, b, c in \mathbb{R}^* , we can conclude that $b = c$, i.e., we can **cancel** a . This fact is true for any group, as you will now see.

Theorem 3: For a, b, c in a group G ,

- i) $ab = ac \Rightarrow b = c$. (This is known as the **left cancellation law**.)
- ii) $ba = ca \Rightarrow b = c$. (This is known as the **right cancellation law**.)

Proof: We will prove (i) and leave you to prove (ii) (see E9).

- i) Let $ab = ac$.
Now, by G3, $\exists d \in G$ s.t. $da = e$(4)
Multiplying both sides of (4) on the left by d , we get $d(ab) = d(ac)$
 $\Rightarrow (da)b = (da)c$, using G1.
 $\Rightarrow eb = ec$
 $\Rightarrow b = c$.

Remember that by multiplying, we mean we are performing the operation $*$, w.r.t. which G is a group. ■

Before going further, go back to Remark 3 for a moment. You should see why Theorem 3 shows what is noted there.

Now, let's go further. Consider any element n of \mathbb{Z} . You know that $-(-n) = n$. You also know that $-(m+n) = (-m) + (-n)$ for $m, n \in \mathbb{Z}$.

Similarly, for $2 \in \mathbb{Q}$ you know that $(2^{-1})^{-1} = 2$.

More generally, consider the following properties of the inverse of an element of any group.

Theorem 4: Let G be a group. Then

- i) $(a^{-1})^{-1} = a$ for every $a \in G$,
- ii) $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$.

Proof: i) For $a \in G$, $a^{-1} \in G$. Let $(a^{-1})^{-1} = b$. By the definition of inverse,

$$b(a^{-1}) = e = (a^{-1})b. \quad \dots(5)$$

But, by definition,

$$a a^{-1} = a^{-1}a = e. \quad \dots(6)$$

Since the inverse of an element is unique (Theorem 2), we see from (5) and (6) that $b = a$, that is, $(a^{-1})^{-1} = a$.

- ii) For $a, b \in G$, $ab \in G$. Therefore, $(ab)^{-1} \in G$, such that $(ab)(ab)^{-1} = e$(7)

$$\begin{aligned} \text{However, } (ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1}, \text{ by associativity.} \\ &= (a(bb^{-1})a^{-1}), \text{ by associativity.} \\ &= (ae)a^{-1}, \text{ since } bb^{-1} = e. \\ &= aa^{-1}, \text{ since } ae = a. \\ &= e, \text{ since } aa^{-1} = e. \end{aligned}$$

Thus, $(ab)(b^{-1}a^{-1}) = e$(8)

Thus, by (7) and (8), and by the uniqueness of the inverse, we get
 $(ab)^{-1} = b^{-1}a^{-1}$. ■

Note that, for a group G , $(ab)^{-1} = a^{-1}b^{-1} \forall a, b \in G$ **only if** G is abelian. For instance, consider the following example.

Example 8: Show that $A^{-1}B^{-1} \neq (AB)^{-1}$ for some $A, B \in GL_2(\mathbb{R})$ (see Example 5).

Solution: Consider $A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$.

Then $AB = \begin{bmatrix} 1 & 2 \\ -1 & 0 \end{bmatrix}$.

Also $A^{-1} = \begin{bmatrix} 1/2 & -1/2 \\ 0 & 1 \end{bmatrix}$, $B^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$. So $A^{-1}B^{-1} = \begin{bmatrix} -1/2 & -1 \\ 1 & 1 \end{bmatrix}$.

Thus, $(AB)(A^{-1}B^{-1}) = \begin{bmatrix} 3/2 & 1 \\ 1/2 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Thus, $A^{-1}B^{-1} \neq (AB)^{-1}$.

Try doing some exercises now.

E9) Prove (ii) of Theorem 3.

E10) Let $G = \{a_1, a_2, a_3\}$ be a commutative group with respect to $*$.

Complete the Cayley table below.

*	a_1	a_2	a_3
a_1			
a_2		a_3	a_1
a_3			

E11) If in a group G , there exists an element g such that $gx = g$ for all $x \in G$, then show that $G = \{e\}$.

E12) For a, b, c in a group G , $ab = bc \Rightarrow a = c$. Is this true or false? Give reasons for your answer.

E13) Let a_1, a_2, \dots, a_n be in a group G . Find $(a_1a_2 \dots a_n)^{-1}$.

E14) Let $x^2 = x$ for each x in a group G . Show that G is abelian. Is the converse true? Why, or why not?

E15) Let $x^2 = e$ for each x in a group G . Show that G is abelian. Is the converse true?

Let us now prove another property of groups.

Theorem 5: For elements a, b in a group G , the equations $ax = b$ and $ya = b$ have unique solutions in G .

Proof: You will first see why $ax = b$ has a solution in G , and then you will see why the solution is unique.

For $a, b \in G$, consider $a^{-1}b \in G$.

Then $a(a^{-1}b) = (aa^{-1})b = eb = b$.

Thus, $a^{-1}b$ satisfies the equation $ax = b$, i.e., $ax = b$ has a solution in G .

Next, to see uniqueness, suppose x_1, x_2 are two solutions of $ax = b$ in G .

Then $ax_1 = b = ax_2$. By the left cancellation law, we get $x_1 = x_2$.

Thus, $a^{-1}b$ is the unique solution in G .

Similarly, using the right cancellation law, you should prove that ba^{-1} is the unique solution of $ya = b$ in G . ■

Let us look at what Theorem 5 tells us in some particular cases.

Example 9: Consider $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in $GL_2(\mathbb{R})$. Find X and Y s.t.

$AX = B$ and $YA = B$.

Solution: From Theorem 5, you know that $X = A^{-1}B$. Now,

$A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$ (see Example 5).

$\therefore A^{-1}B = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & -2 \\ -1 & 3 \end{bmatrix} = X$.

Verify that $AX = B$ for this X .

Similarly, you should find $Y = BA^{-1}$.

In the next example, we consider an unusual group.

Example 10: Let S be a non-empty set. Consider $\wp(S)$, the set of all subsets of S , with the binary operation of **symmetric difference** Δ , given by

$A \Delta B = (A \setminus B) \cup (B \setminus A) \quad \forall A, B \in \wp(S)$.

Check whether or not $(\wp(S), \Delta)$ and $(\wp(S), \cap)$ are groups. If they are, are they abelian groups?

Further, is there a unique solution for the equations $Y \Delta A = B$ and

$Y \cap A = B \quad \forall A, B \in \wp(S)$? Why, or why not?

Solution: Let us first consider $(\wp(S), \Delta)$. Δ is an associative binary operation on $\wp(S)$. You can check this by using the properties of the set operations that you studied in Block 1 of the course, Calculus, namely,

$A \setminus B = A \cap B^c, (A \cap B)^c = A^c \cup B^c, (A \cup B)^c = A^c \cap B^c \quad \forall A, B \in \wp(S)$,

and that \cup and \cap are commutative and associative.

You would be familiar with $\wp(S)$, from Unit 2 of Calculus.

Δ is also commutative since

$$\begin{aligned} A \Delta B &= (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) \\ &= B \Delta A \quad \forall A, B \in \wp(S). \end{aligned}$$

Here, \emptyset is the identity element w.r.t. Δ since $A \Delta \emptyset = A \quad \forall A \in \wp(S)$.

Further, any element is its own inverse, since $A \Delta A = \emptyset \quad \forall A \in \wp(S)$.

Thus, $(\wp(S), \Delta)$ is an abelian group.

Let us now consider $(\wp(S), \cap)$. As you know, \cap is an associative binary operation on $\wp(S)$. Also, $A \cap S = A \quad \forall A \in \wp(S)$, so that S is the identity w.r.t. \cap . However, given a proper subset A of S , there is no $B \in \wp(S)$ s.t. $A \cap B = S$.

Thus, $(\wp(S), \cap)$ is not a group.

Note that $Y \cap A = S$ does not have a solution for $A \in \wp(S)$, $A \neq S$.

For A, B in $(\wp(S), \Delta)$ we want to solve $Y \Delta A = B$. But we know that A is its own inverse. So, by Theorem 5, $Y = B \Delta A^{-1} = B \Delta A$ is the unique solution. What we have also proved here is that $(B \Delta A) \Delta A = B$ for any A, B in $\wp(S)$.

Try solving the following exercises now.

E16) Is $(\mathbb{Z}, -)$ a group? Can you obtain a unique solution for $a - x = b$, $\forall a, b \in \mathbb{Z}$? What conclusion do you draw from this about the converse of Theorem 5?

E17) If G is a semigroup, but not a group, will $ax = b$ have a solution for all $a, b \in G$? Why, or why not?

And now let us discuss the repeated operation of an element of a group on itself. For example, consider $n \in (\mathbb{Z}, +)$. Then $n + n = 2n$, $(n + n) + n = 3n, \dots$. Similarly, consider repeated addition on the inverse of n , that is, on $-n$. $(-n) + (-n) = 2(-n)$, $[(-n) + (-n)] + (-n) = 3(-n), \dots$. In this context, consider the following definition.

Definition: Let G be a group. For $a \in G$, we define $a^n \quad \forall n \in \mathbb{Z}$ as follows:

- i) $a^0 = e$.
- ii) $a^n = a^{n-1} \cdot a$, if $n > 0$.
- iii) $a^n = (a^{-1})^{(-n)}$, if $n < 0$.

Here n is called the **exponent** (or **index**) of the **integral power** a^n of a .

Thus, by definition, $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a^2 \cdot a$, and so on; and $a^{-2} = (a^{-1})^2$, $a^{-3} = (a^{-1})^3$, and so on.

Remark 6: When the binary operation is addition, a^n becomes na . For example, for any $a \in \mathbb{Z}$, the definition above says

- i) $na = 0$, if $n = 0$;
- ii) $na = a + a + \dots + a$ (n times), if $n > 0$;
- iii) $na = (-a) + (-a) + \dots + (-a)$ ($-n$ times), if $n < 0$.

Let us now prove some laws of **indices** (the plural of 'index') for group elements.

Theorem 6: Let G be a group. For $a \in G$ and $m, n \in \mathbb{Z}$,

- i) $(a^n)^{-1} = a^{-n} = (a^{-1})^n$,
- ii) $a^m \cdot a^n = a^{m+n}$,
- iii) $(a^m)^n = a^{mn}$.

Proof: We will prove (i) and (ii), and leave the proof of (iii) to you (see E18).

- i) If $n = 0$, $(a^n)^{-1} = (a^0)^{-1} = e^{-1} = e$; $a^{-n} = a^0 = e$; and $(a^{-1})^n = (a^{-1})^0 = e$. So, in this case (i) is true.

Now suppose $n > 0$. Since $aa^{-1} = e$, we see that

$$\begin{aligned} e &= e^n = (aa^{-1})^n \\ &= (aa^{-1})(aa^{-1}) \dots (aa^{-1}) \text{ (n times)} \\ &= a^n (a^{-1})^n, \text{ since } a \text{ and } a^{-1} \text{ commute.} \\ \therefore (a^n)^{-1} &= (a^{-1})^n. \end{aligned}$$

Also, $(a^{-1})^n = a^{-n}$, by (iii) of the definition, since $(-n) < 0$.

$$\therefore (a^n)^{-1} = (a^{-1})^n = a^{-n} \text{ when } n > 0.$$

If $n < 0$, then $(-n) > 0$ and

$$\begin{aligned} (a^n)^{-1} &= [a^{(-n)}]^{-1} \\ &= [(a^{-n})^{-1}]^{-1}, \text{ by the case } n > 0 \\ &= a^{-n}, \text{ since } (x^{-1})^{-1} = x \ \forall x \in G. \end{aligned}$$

Also, $(a^{-1})^n = (a^{-1})^{-(n)}$

$$\begin{aligned} &= [(a^{-1})^{-1}]^{-n}, \text{ by the case } n > 0. \\ &= a^{-n}, \text{ since } (a^{-1})^{-1} = a. \end{aligned}$$

So, in this case too,

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

- ii) First, suppose $m = 0$. Then $m + n = n$. Hence,
 $a^{m+n} = a^n = a^0 \cdot a^n$, since $a^0 = e$.
 $= a^m \cdot a^n$.

Similarly, if $n = 0$, then $a^{m+n} = a^m \cdot a^n$.

Now suppose $m \neq 0$ and $n \neq 0$. Let us consider 4 situations.

Case 1 ($m > 0$ and $n > 0$): Let us prove the result in this case by induction on n .

Let $P(n)$ be the predicate that $a^m \cdot a^n = a^{m+n}$, where m is given.

If $n = 1$, then $a^m \cdot a = a^{m+1}$, by definition.

Thus, $P(1)$ is a true statement.

Now assume that $P(k)$ is true, i.e., $a^m \cdot a^k = a^{m+k}$ for some $k \geq 1$.

Then $a^m \cdot a^{k+1} = a^m(a^k \cdot a) = (a^m \cdot a^k)a = a^{m+k} \cdot a$, since $P(k)$ is true.
 $= a^{m+(k+1)}$.

Thus, $P(k+1)$ is true.

Hence, by the principle of induction, (i) holds for all $m > 0$ and $n > 0$.

Case 2 ($m < 0$ and $n < 0$): Here $(-m) > 0$ and $(-n) > 0$. Thus, by

Case 1, $a^{-n} \cdot a^{-m} = a^{-(n+m)} = a^{-(m+n)}$.

Taking inverses of both the sides, and using (i), we get

$$a^{m+n} = [a^{-(m+n)}]^{-1} = (a^{-n} \cdot a^{-m})^{-1} = (a^{-m})^{-1} \cdot (a^{-n})^{-1} = a^m \cdot a^n.$$

Case 3 ($m > 0$, $n < 0$ such that $m + n \geq 0$): Here $(-n) > 0$. So, by

Case 1, $a^{m+n} \cdot a^{-n} = a^m$.

Multiplying both sides on the right by $a^n = (a^{-n})^{-1}$, by (i), we get

$$a^{m+n} = a^m \cdot a^n.$$

Case 4 ($m > 0$, $n < 0$ such that $m + n < 0$): By Case 2, $a^{-m} \cdot a^{m+n} = a^n$.

Multiplying both sides on the left by $a^m = (a^{-m})^{-1}$, we get $a^{m+n} = a^m \cdot a^n$.

You should prove the cases when $m < 0$ and $n > 0$ on the same lines as done in Cases 3 and 4.

Hence, $a^{m+n} = a^m \cdot a^n$ for all $a \in G$ and $m, n \in \mathbb{Z}$.

The proof of Theorem 6 will be complete once you solve E18. ■

You will be applying Theorem 6 very often, through and through the course.

Let us consider what it says in a particular case.

Example 11: Let $A \in \wp(S)$, where $S \neq \emptyset$. Find $A^n \forall n \in \mathbb{Z}$.

Solution: Here the operation is Δ . Also, you know that $A^2 = A \Delta A = \emptyset$.

So $A^{-1} = A$.

Now, if $n = 2m$, $m \in \mathbb{Z}$, then $A^n = (A^2)^m = \emptyset^m = \emptyset$.

If $n = 2m + 1$, $m \in \mathbb{Z}$, then $A^n = A^{2m} \Delta A = \emptyset \Delta A = A$.

Thus, $A^n = \emptyset$ or A , depending on whether n is even or odd.

Solve the following exercises now.

E18) Prove (iii) of Theorem 6.

(Hint: Prove, by induction on n , for the case $n > 0$. Then prove for $n < 0$.)

E19) Let G be an abelian group. Prove that

i) $ab^m = b^ma \forall m \in \mathbb{Z}$ and $\forall a, b \in G$;

$$\text{ii) } (ab)^m = a^m b^m \quad \forall m \in \mathbb{Z}.$$

We will now discuss some groups in detail. You will be working with these groups off and on throughout this course.

2.4 SOME IMPORTANT GROUPS

In this section, we shall introduce you to six types of groups one-by-one. Study these carefully as we will use them as examples (and counterexamples!) very often throughout this course.

These types are:

the group of integers modulo n , symmetric groups, dihedral groups, matrix groups, the groups formed by the n th roots of unity ($n \in \mathbb{Z}$) and the direct product of groups.

2.4.1 Integers Modulo n

Consider the set of integers, \mathbb{Z} , and $n \in \mathbb{N}$. In Unit 1 you studied that the relation of 'congruence modulo n ' (i.e., the relation R , given by aRb iff n divides $a - b$) is an equivalence relation. Thus, from Unit 1 you know that this gives a partition of \mathbb{Z} into disjoint equivalence classes, called **congruence classes modulo n** . We denote the equivalence class containing r by \bar{r} , or $[r]$.

Thus, $\bar{r} = \{m \in \mathbb{Z} \mid m \equiv r \pmod{n}\}$.

So an integer m belongs to \bar{r} for some r , $0 \leq r < n$, iff $m \equiv r \pmod{n}$, i.e., iff $n \mid (m - r)$, i.e., iff $m - r = kn$, for some $k \in \mathbb{Z}$.

$$\therefore \bar{r} = \{r + kn \mid k \in \mathbb{Z}\}.$$

You have also seen in Unit 1, that all the congruence classes modulo n of \mathbb{Z} are $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Further, $\mathbb{Z} = \bigcup_{i=0}^{n-1} \bar{i}$ (a disjoint union).

Let $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

We define the operation $+$ on \mathbb{Z}_n by $\bar{a} + \bar{b} = \overline{a + b}$.

Is this operation well-defined? To answer this, we have to see whether $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$ in \mathbb{Z}_n implies $\overline{a + c} = \overline{b + d}$.

Now, $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Hence, there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $c - d = k_2 n$. But then

$$(a + c) - (b + d) = (a - b) + (c - d) = (k_1 + k_2)n.$$

$$\therefore \overline{a + c} = \overline{b + d}.$$

Thus, $+$ is a well-defined binary operation on \mathbb{Z}_n .

Note that $\overline{a + c} = \bar{r}$ for some $r = 0, \dots, n - 1$, since $a + c \in \mathbb{Z} = \bigcup_{i=0}^{n-1} \bar{i}$.

For example, in \mathbb{Z}_4 , $\bar{2} + \bar{3} = \bar{5} = \bar{1}$, since $2 + 3 = 5$ and $5 \equiv 1 \pmod{4}$.

Also in \mathbb{Z}_{11} , $\bar{7} - \bar{10} = \overline{-3} = \bar{8}$, since $\bar{8} + \bar{3} = \overline{11} = \bar{0}$.

To improve your understanding of addition in \mathbb{Z}_n , do the following exercise.

Note that \bar{i} is a subset of \mathbb{Z} , not an element of \mathbb{Z} , $\forall i \in \mathbb{Z}$.

E20) Fill up the following operation table for $+$ on \mathbb{Z}_5 .

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Now, let us show that $(\mathbb{Z}_n, +)$ is a commutative group, for $n \in \mathbb{N}$.

- $\bar{a} + (\bar{b} + \bar{c}) = \overline{\bar{a} + (\bar{b} + \bar{c})} = \overline{\bar{a} + \bar{b} + \bar{c}} = \overline{(\bar{a} + \bar{b}) + \bar{c}} = (\bar{a} + \bar{b}) + \bar{c} = \overline{(\bar{a} + \bar{b}) + \bar{c}} = (\bar{a} + \bar{b}) + \bar{c} = \overline{(\bar{a} + \bar{b}) + \bar{c}} = (\bar{a} + \bar{b}) + \bar{c}$
 $= (\bar{a} + \bar{b}) + \bar{c} \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, i.e., addition is associative in \mathbb{Z}_n .
- $\bar{a} + \bar{0} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}_n$, i.e., $\bar{0}$ is the identity for addition.
- For $\bar{a} \in \mathbb{Z}_n, \exists \bar{n} - \bar{a} \in \mathbb{Z}_n$ such that $\bar{a} + \bar{n} - \bar{a} = \bar{n} = \bar{0}$.
 Thus, every element \bar{a} in \mathbb{Z}_n has an inverse with respect to addition.
- $\bar{a} + \bar{b} = \overline{\bar{a} + \bar{b}} = \overline{\bar{b} + \bar{a}} = \bar{b} + \bar{a} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_n$, i.e., addition is commutative in \mathbb{Z}_n .

The properties (i) to (iv) above show that $(\mathbb{Z}_n, +)$ is an abelian group of order n .

Can we define multiplication also on \mathbb{Z}_n in a similar way? Let's see.

Let us **define multiplication on \mathbb{Z}_n** by $\bar{a} \cdot \bar{b} = \overline{ab}$.

You should prove that this is a well-defined binary operation on \mathbb{Z}_n .

Also, $(\bar{a} \bar{b})\bar{c} = \overline{(\bar{a} \bar{b})\bar{c}} = \overline{\bar{a}(\bar{b} \bar{c})} = \bar{a}(\bar{b} \bar{c}) = \overline{\bar{a} \bar{b} \bar{c}} = \bar{a} \bar{b} \bar{c} = \overline{\bar{a} \bar{b} \bar{c}} = \bar{a} \bar{b} \bar{c}$
 $= \bar{a} \bar{b} \bar{c} \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, and $\bar{a} \bar{b} = \overline{\bar{a} \bar{b}} = \overline{\bar{b} \bar{a}} = \bar{b} \bar{a} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_n$.

Thus, multiplication in \mathbb{Z}_n is an associative and commutative binary operation.

You should verify that \mathbb{Z}_n also has a multiplicative identity, namely, $\bar{1}$.

But (\mathbb{Z}_n, \cdot) is not a group. Why? For the same reason that (\mathbb{Z}, \cdot) is not a group. Not every element of \mathbb{Z}_n has a multiplicative inverse. For example, $\bar{0}$ does not have a multiplicative inverse since $\bar{0} \cdot \bar{r} = \bar{0} \quad \forall \bar{r} \in \mathbb{Z}_n$.

But, suppose we consider the non-zero elements of \mathbb{Z}_n , that is, (\mathbb{Z}_n^*, \cdot) . Is this a group? Well, $\mathbb{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is not a group because \cdot is not even a binary operation on \mathbb{Z}_4^* , since $\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbb{Z}_4^*$. However, (\mathbb{Z}_p^*, \cdot) is an abelian group for any prime p , as you will now show for $p = 5$.

E21) Show that (\mathbb{Z}_5^*, \cdot) is an abelian group.

(Hint: Draw the Cayley table.)

E22) i) What is the multiplicative inverse of each element of \mathbb{Z}_{11}^* ?

ii) What is the multiplicative inverse of any element of \mathbb{Z}_p^* , where p is a prime?

(Hint: Note that for $\bar{r} \in \mathbb{Z}_p^*$, the g.c.d $(r, p) = 1$.)

iii) Show that (\mathbb{Z}_p^*, \cdot) an abelian group, where p is a prime.

Let us now discuss the symmetric group.

2.4.2 Symmetric Groups

We will now look at a group whose elements are permutations of a set, a concept you have been introduced to in Sec.1.5, Unit 1. In Unit 9 you will study this group in more detail.

Let us begin with an example.

Example 12: Let B be the set of all bijections from \mathbb{R} to \mathbb{R} . Show that B is a group w.r.t. the composition of functions.

Solution: $B \neq \emptyset$, since $I: \mathbb{R} \rightarrow \mathbb{R}: I(x) = x$ is in B .

Next, from Calculus you know that if f and g are in B , then so is $f \circ g$. Thus, \circ is closed in B .

You also know that $(f \circ g) \circ h = f \circ (g \circ h) \forall f, g, h \in B$. Thus, \circ is associative over B .

Since $f \circ I = f \forall f \in B$, I is the identity w.r.t. \circ .

Also, given $f \in B$, f is a bijection from \mathbb{R} to \mathbb{R} . Hence, as you know, there is $g \in B$ s.t. $f \circ g = I$.

Hence, (B, \circ) is a group.

In the example above, B is the set of permutations of \mathbb{R} . More generally, if X is a non-empty set, $S(X)$ is the set of all permutations of X .

From your Calculus course, you know that if α and β are 1-to-1 functions from X to X , then so is $\alpha \circ \beta$.

Thus, the composition of functions is a binary operation on the set $S(X)$.

This binary operation is associative in general, as you know from the course, Calculus; hence, \circ is associative in $S(X)$.

I_X , the identity map, is the identity in $S(X)$ because

$$f \circ I_X = I_X \circ f = f \forall f \in S(X).$$

You also know that if $f: X \rightarrow X$ is bijective, then $\exists g: X \rightarrow X$ s.t. $f \circ g = g \circ f = I_X$. So g is also bijective, and we denote g by f^{-1} . So if $f \in S(X)$, $f^{-1} \in S(X)$.

Let us put together what we have just said about $(S(X), \circ)$.

- i) \circ is a binary operation on $S(X)$,
- ii) \circ is associative,
- iii) I_X is the identity element,
- iv) $f^{-1} \in S(X)$ is the inverse of f , for any $f \in S(X)$.

Thus, $(S(X), \circ)$ is a group. It is called the **permutation group on X** .

Now, from Unit 1, you also know that if the set X is finite, say $X = \{1, 2, 3, \dots, n\}$, then we denote $S(X)$ by S_n .

Definition: The group (S_n, \circ) is called the **symmetric group on n symbols**, where $n \in \mathbb{N}$.

From Unit 1, you know that $\mathbf{o(S_n) = n!}$.

Now, consider $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \in S_4$. What will f^{-1} look like in the two-line

format? Since $f \circ f^{-1} = f^{-1} \circ f = I$, we know that $f^{-1}f(i) = i \forall i = 1, \dots, 4$.

So $1 = f^{-1}f(1) = f^{-1}(3)$, $2 = f^{-1}(1)$, $3 = f^{-1}(4)$ and $4 = f^{-1}(2)$. Thus,

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \text{ i.e., } f^{-1} \text{ is got by interchanging the top}$$

and bottom rows of f ! This is true in general – **the 2-row representation of f^{-1} in S_n is obtained by interchanging the rows of the 2-row**

representation of $f \in S_n$. This is because each $f \in S_n$ is a bijection.

So, for instance, if $f = (1\ 2\ 3)$, what is f^{-1} ?

Remember, the 3-cycle $(1\ 2\ 3)$ is the function given by $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. So

$$f^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = (2\ 1\ 3), \text{ again a 3-cycle!}$$

Doing the following exercises will give you some practice in computing the product and inverse of elements in S_n .

E23) If f is the cycle $(1\ 3)$ in S_5 , write f^{-1} in the 2-row format. Also check if f^{-1} is a cycle or not.

E24) In Sec.1.5, Unit 1, you have obtained all 6 elements of S_3 . Write down the Cayley table for (S_3, \circ) . Hence obtain the inverse of each element of S_3 .

E25) Write the inverses of $(1\ 2)$ and $(2\ 4\ 5)$ in S_5 . Also, show that

$$[(1\ 2) \circ (2\ 4\ 5)]^{-1} \neq (1\ 2)^{-1} \circ (2\ 4\ 5)^{-1}. \text{ (This again shows that in Theorem 4, we can't write } (ab)^{-1} = a^{-1}b^{-1}.)$$

As we said at the beginning of this sub-section, we shall discuss (S_n, \circ) in detail in Unit 9. For now let us discuss certain groups related to these groups.

2.4.3 Dihedral Groups

In Sec.1.5, Unit 1, you studied the set of symmetries of some regular polygons. As you know, each symmetry of a regular polygon of n sides is a permutation on n symbols. You have also seen, in E38 of Unit 1, that (S_3, \circ) is the same as the group of symmetries of a regular 3-gon, that is, an equilateral triangle. However, S_4 is not D_8 , the set of symmetries of a square. This is because, for instance, D_8 has 8 elements, while S_4 has $4!(=24)$ elements.

In fact, S_n is not the set of symmetries of a regular n -gon for $n \neq 3$. But the set of symmetries of a regular n -gon is a subset of S_n , and is a group w.r.t. \circ . To see this, let us look at the set in E36 of Unit 1 again, in detail.

Example 13: Show that the set S , of symmetries of a square forms a group w.r.t. \circ .

Solution: Consider Fig.3.

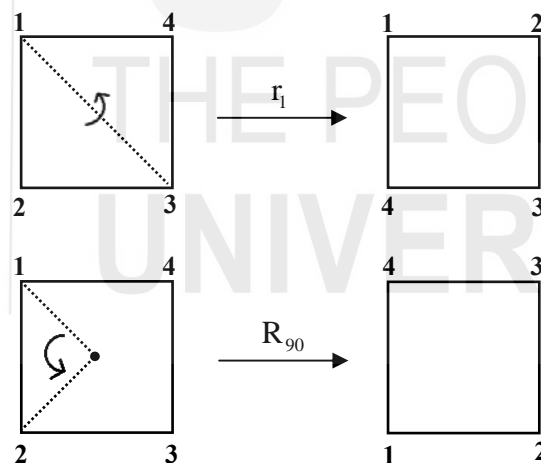


Fig.3: r_1 is the reflection about the diagonal through the vertices 1 and 3; R_{90} is the rotation about the centre of the square, through 90° , in the anti-clockwise direction.

Let us write down all the symmetries of the square in the 2-row format, with reference to the numbering of the vertices in Fig.3. These are:

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Now, to make the operation table, consider $r_2 \circ r_3$, say.

$$r_2 \circ r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ r_2 r_3(1) & r_2 r_3(2) & r_2 r_3(3) & r_2 r_3(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ r_2(2) & r_2(1) & r_2(4) & r_2(3) \end{pmatrix} \\ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = R_{90}.$$

Similarly, you should carry out the other compositions, and check that the table is:

\circ	I	r_1	r_2	r_3	r_4	R_{90}	R_{180}	R_{270}
I	I	r_1	r_2	r_3	r_4	R_{90}	R_{180}	R_{270}
r_1	r_1	I	R_{180}	R_{270}	R_{90}	r_4	r_2	r_3
r_2	r_2	R_{180}	I	R_{90}	R_{270}	r_3	r_1	r_4
r_3	r_3	R_{90}	R_{270}	I	R_{180}	r_1	r_4	r_2
r_4	r_4	R_{270}	R_{90}	R_{180}	I	r_2	r_3	r_1
R_{90}	R_{90}	r_3	r_4	r_2	r_1	R_{180}	R_{270}	I
R_{180}	R_{180}	r_2	r_1	r_4	r_3	R_{270}	I	R_{90}
R_{270}	R_{270}	r_4	r_3	r_1	r_2	I	R_{90}	R_{180}

Now, by looking at the table, you can see that

- \circ is a binary operation on S .
- $\exists I \in S$ s.t. $x \circ I = x \quad \forall x \in S$.
- For each $x \in S$, $\exists y \in S$ s.t. $x \circ y = I$.

Also, since composition of functions is associative in general, it is associative here too.

Hence, (S, \circ) is a group.

Also, note that $R_{180} = R_{90}^2$, $R_{270} = R_{90}^3$. Further, if r denotes r_1 , then

$r_2 = rR_{90}^2$, $r_3 = rR_{90}^3$, $r_4 = rR_{90}$ and $rR_{90} = R_{90}^3 r$, where we are using multiplication to denote the composition of functions, as per Remark 5.

Similar relationships will hold if we take $r = r_2$ instead of r_1 , or $r = r_3$, or $r = r_4$.

Hence, we can write $S = \{I, R_{90}, R_{90}^2, R_{90}^3, r, rR_{90}, rR_{90}^2, rR_{90}^3\}$, where

$$r^2 = I = R_{90}^4 \quad \text{and} \quad rR_{90} = R_{90}^3 r.$$

The group in the example above is a particular case of what we shall now define.

Definition: The group of symmetries of a regular n -gon is called the **dihedral group of order $2n$** , for $n \geq 3$. It is denoted by D_{2n} . (Some authors also denote this by D_n .)

From Example 13 above, and Example 18, of Unit 1, you may have understood why $|D_{2n}| = 2n$. Let us look at the reason, first using an example of $n = 5$.

The term 'dihedral' comes from the Greek words 'di', meaning 'two', and 'hedron', meaning 'surface'.

Let us name the vertices of the regular pentagon 1, 2, ..., 5, where 2 is adjacent to 1, 3 to 2, ..., 5 to 4, and 1 to 5, moving along the edges of the pentagon in the anti-clockwise direction.

Each symmetry will send a vertex to a vertex. So 1 can be sent to any one of 5 vertices. For example in Fig.4, we show the symmetry obtained on rotating it about its centre through $\left(\frac{360}{5}\right)^\circ$ in the anti-clockwise direction. Here we send 1 to 2.

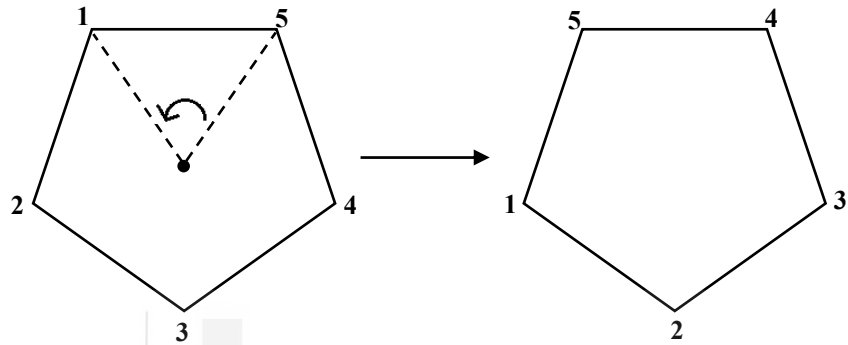


Fig.4: The rotation symmetry of a regular pentagon through $\left(\frac{360}{5}\right)^\circ = 72^\circ$.

Once the image of 1 is fixed, 2 has to go to an adjacent vertex. So there are only 2 choices for 2. Once the image of 2 is also fixed, then the images of the vertices 3, 4, 5 are determined. Thus, there can be $5 \times 2 = 10$ symmetries of a regular pentagon.

In the same way, there are **at most $2n$ symmetries of a regular n -gon.**

Also, generalising from what you have seen in Example 13, if the n -gon rotates about its centre through $\left(\frac{360}{n}\right)^\circ$ in the anti-clockwise direction, we get a symmetry. In fact, we have n distinct rotational symmetries – through 0° (which is the same as not moving at all), through $\left(\frac{360}{n}\right)^\circ$, through $2\left(\frac{360}{n}\right)^\circ$, through $3\left(\frac{360}{n}\right)^\circ$, and so on, up to $(n-1)\left(\frac{360}{n}\right)^\circ$.

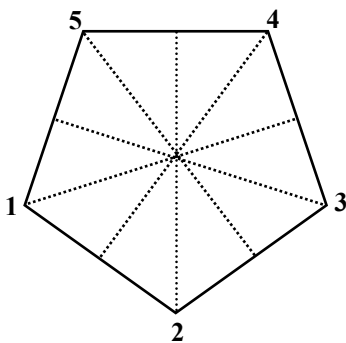


Fig.5: The 5 lines of symmetry corresponding to the 5 reflection symmetries of a regular pentagon.

Don't forget! The polygon also has n distinct reflection symmetries. To see how, consider Example 13 to see what happens when n is even. There are $\frac{n}{2}$ symmetries about the lines joining the mid-points of opposite edges, and there are $\frac{n}{2}$ symmetries about the lines joining opposite vertices.

To understand why there are n reflection symmetries when n is odd, consider the case of the pentagon in Fig.5. The n reflection symmetries are about the lines joining each vertex to the mid-point of the edge opposite it.

Thus, a regular n -gon has n rotational symmetries and n reflection symmetries for all $n \geq 3$. Hence, $o(D_{2n}) = 2n$.

If we denote the rotational symmetry through $\left(\frac{360}{n}\right)^\circ$ of the regular n -gon by

R , then the rotation through $2\left(\frac{360}{n}\right)^\circ$ is got by applying R twice, that is, it is

R^2 . Similarly, the other rotational symmetries are R^3, R^4, \dots, R^{n-1} , and we have I , the rotational symmetry through 0° , when the n -gon does not move at all.

Next, consider any reflection symmetry of the n -gon, say the one about the line through its vertex 1, and call it r . Then taking the mirror image of the mirror image of the n -gon about this line will give us the original position of the n -gon. Thus, $r^2 = I$. This is true for any of the reflection symmetries.

Finally, just as in Example 13, we have

$D_{2n} = \{I, R, R^2, \dots, R^{n-1}, r, rR, rR^2, \dots, rR^{n-1}\}$, where $r^2 = I, R^n = I$ and $rR = R^{n-1}r$.

Try solving some exercises now.

E26) Give an element of S_4 that is not an element of D_8 .

E27) Create the Cayley table for (D_{10}, \circ) .

E28) Is D_{2n} an abelian group $\forall n \geq 3$? Give reasons for your answer.

We will now discuss another important category of groups. You have been introduced to this in Unit 1, and in some earlier examples of this unit.

2.4.4 Matrix Groups

In Sec.1.4, Unit 1, you studied about matrices and some operations on them. In Example 2 and Example 5, you have seen how some sets of matrices form a group w.r.t. matrix addition or multiplication. Now, go through those portions again before going further. We will build on what you have studied there for taking the discussion in this sub-section further.

Let us begin with an example.

Example 14: Show that $(M_{m \times n}(\mathbb{C}), +)$ is an abelian group.

Solution: In Unit 1, you have seen that $+$, given by

$[a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} = [a_{ij} + b_{ij}]_{m \times n}$, where $a_{ij}, b_{ij} \in \mathbb{C}$ for $i = 1, \dots, m, j = 1, \dots, n$,

is a well-defined binary operation on $M_{m \times n}(\mathbb{C})$.

You have also seen that $+$ is associative and commutative.

Next, for any $A \in M_{m \times n}(\mathbb{C})$, $A + \mathbf{0} = A$, where $\mathbf{0}$ is the $m \times n$ matrix with all its entries being 0.

Finally, given $A = [a_{ij}] \in M_{m \times n}(\mathbb{C})$, there is $(-A) = [-a_{ij}] \in M_{m \times n}(\mathbb{C})$ such that $A + (-A) = \mathbf{0}$.

Hence, $(M_{m \times n}(\mathbb{C}), +)$ is an abelian group.

Example 15: Show that $(M_n(\mathbb{C}), \cdot)$ is a semigroup, but not a group, where $n \geq 2$. Is $(M_n(\mathbb{C})^*, \cdot)$ a group?

Solution: From Unit 1, you know that \cdot is a well-defined associative binary operation on $M_n(\mathbb{C})$. Thus, $(M_n(\mathbb{C}), \cdot)$ is a semigroup.

In E3 you have noted why $(M_3(\mathbb{C}), \cdot)$ is not a group. In the same way you can see that $(M_n(\mathbb{C}), \cdot)$ is not a group for any $n \in \mathbb{N}$.

In fact, for each $n \geq 2$, there are infinitely many matrices in $M_n(\mathbb{C})$ that have no multiplicative inverse. For example, for $n = 2$, consider

$$A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \neq \mathbf{0} \text{ and } B = \begin{bmatrix} b_{11} & b_{12} \\ b_{13} & b_{14} \end{bmatrix} \in M_2(\mathbb{C})^*.$$

$$\text{Then } AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{13} & b_{14} \end{bmatrix} = \begin{bmatrix} ab_{11} & ab_{12} \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2,$$

since the (2, 2)th entry of AB is 0 and that of I_2 is 1.

Thus, $(M_2(\mathbb{C})^*, \cdot)$ is not a group.

Similarly, you can show that $(M_n(\mathbb{C})^*, \cdot)$ is not a group for any $n \geq 2$.

Example 16: Show that $M_{3 \times 2}(\mathbb{Z}_8)$ is a finite abelian group w.r.t. matrix addition. What is the order of this group?

$$\text{Solution: } M_{3 \times 2}(\mathbb{Z}_8) = \left\{ \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \\ \bar{e} & \bar{f} \end{bmatrix} \mid \bar{a}, \bar{b}, \dots, \bar{f} \in \mathbb{Z}_8 \right\}.$$

As in Example 14, you should check that addition is a well-defined associative binary operation, using what you have studied in Sec.2.4.1.

$$\text{Here } \mathbf{0} = \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} \text{ and the additive inverse of } \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \\ \bar{e} & \bar{f} \end{bmatrix} \text{ is } \begin{bmatrix} \overline{8-a} & \overline{8-b} \\ \overline{8-c} & \overline{8-d} \\ \overline{8-e} & \overline{8-f} \end{bmatrix}.$$

Hence, $(M_{3 \times 2}(\mathbb{Z}_8), +)$ is a group.

But, why is it finite? Each matrix here has 6 entries. Each entry is one of the elements of \mathbb{Z}_8 , i.e., $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$. So each entry has 8 possibilities.

Note that two different entries of a matrix can be the same element of \mathbb{Z}_8 .

Thus, the total number of elements in $M_{3 \times 2}(\mathbb{Z}_8)$ is 8^6 .

Thus, this group is finite, of order 8^6 .

Finally, you should show that this group is abelian, using the fact that $(\mathbb{Z}_8, +)$ is abelian.

Why don't you solve some exercises now?

E29) Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ be in $M_2(\mathbb{C})$, where $i = \sqrt{-1}$. Show that $A^4 = I$, $B^4 = I$, $AB = -BA$. Also draw up the Cayley table for multiplication in $Q_8 = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$. Hence show that (Q_8, \cdot) is a group. Is it abelian? What is $o(Q_8)$? (This group is called the **group of quaternions**.)

E30) If multiplication in $M_{m \times n}(\mathbb{C})^*$ is defined by $[a_{ij}] \cdot [b_{ij}] = [a_{ij} \cdot b_{ij}]$, check whether or not $(M_{m \times n}(\mathbb{C})^*, \cdot)$ is a group.

In this sub-section you have studied several sets of matrices which form groups. These are examples of **matrix groups**. You will study more about them in the course 'Linear Algebra'. For now, we shall stop our discussion on groups of matrices for now, and introduce you to another group. The underlying set of this group is a subset of \mathbb{C}^* .

2.4.5 Roots of Unity

In Block 1 of the course Calculus, you studied about how to find the 3rd, 4th, 5th... roots of any complex number. In particular, you know that 1 has n distinct n th roots in $\mathbb{C} \forall n \in \mathbb{N}$. You also know that these lie along the circumference of a circle in the plane, with centre at the origin and radius 1 unit.

Next, you know that 1 is the identity of \mathbb{C} w.r.t. multiplication. We call this identity **unity** for reasons that you will study in Block 3.

Thus, **the n th roots of unity are the n th roots of 1.**

Let us now see an example of how the set of n th roots of unity forms a group.

Example 17: Show that the set U_4 , of all the 4th roots of unity, forms a group w.r.t. multiplication.

Solution: From Block 1 of the course, Calculus, you know that the polar form of 1 is $(\cos 0 + i \sin 0) = \cos(0 + 2k\pi) + i \sin(0 + 2k\pi) \forall k \in \mathbb{Z}$.

Hence, the polar form of the 4th roots of unity is

$$[\cos(0 + 2k\pi) + i \sin(0 + 2k\pi)]^{1/4} = \cos \frac{k\pi}{2} + i \sin \frac{k\pi}{2} \text{ for } k = 0, 1, 2, 3.$$

Thus, $U_4 = \{1, i, -1, -i\}$.

So (U_4, \cdot) is the group discussed in Example 4.

In the example above, did you notice that $U_4 = \{i, i^2, i^3, i^4\}$, since $i = \sqrt{-1}$? We will refer again to this in Unit 4.

Let us now generalise what you have seen in Example 17. For this purpose, let us briefly recall what the n th roots of unity are. From Block 1 of Calculus,

you know that the polar form of a non-zero complex number $z \in \mathbb{C}$ is $z = r(\cos \theta + i \sin \theta)$, where $r = |z|$ and θ is an argument of z .

Moreover, if θ_1 is an argument of z_1 , and θ_2 that of z_2 , then $\theta_1 + \theta_2$ is an argument of $z_1 z_2$. Using these facts, let us now find the n th roots of 1, where $n \in \mathbb{N}$.

If $z = r(\cos \theta + i \sin \theta)$ is an n th root of 1, then $z^n = 1$.

Thus, by De Moivre's theorem,

$1 = z^n = r^n (\cos n\theta + i \sin n\theta)$, that is,

$$\cos(0 + 2k\pi) + i \sin(0 + 2k\pi) = r^n (\cos n\theta + i \sin n\theta) \text{ for } k \in \mathbb{Z}. \quad \dots(9)$$

Equating the modulus of both the sides of (9), we get $r^n = 1$, i.e., $r = 1$, since the modulus is a real number.

On comparing the arguments of both sides of (9), we see that $0 + 2\pi k$ ($k \in \mathbb{Z}$) and $n\theta$ are arguments of the same complex number. Thus, $n\theta$ can take any one of the values $2\pi k$, $k \in \mathbb{Z}$. Does this mean that as k ranges over \mathbb{Z} , and θ ranges over $\frac{2\pi k}{n}$, we get distinct n th roots of 1? Let us find out.

Now, $\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = \cos \frac{2\pi m}{n} + i \sin \frac{2\pi m}{n}$ if and only if

$$\frac{2\pi k}{n} - \frac{2\pi m}{n} = 2\pi t \text{ for some } t \in \mathbb{Z}.$$

This will happen iff $k = m + nt$, i.e., $k \equiv m \pmod{n}$. Thus,

corresponding to each \bar{r} in \mathbb{Z}_n , we get an n th root of unity,

$$z = \cos \frac{2\pi r}{n} + i \sin \frac{2\pi r}{n}, \quad 0 \leq r < n; \text{ and these are all the } n\text{th roots of unity.}$$

For example, if $n = 6$, we get the six 6th roots of 1 as z_0, z_1, z_2, z_3, z_4 and z_5 ,

where $z_j = \cos \frac{2\pi j}{6} + i \sin \frac{2\pi j}{6}$, $j = 0, 1, 2, 3, 4, 5$. In Fig.6 you can see that all these lie on the unit circle (i.e., the circle of radius one with centre $(0, 0)$).

They form the vertices of a regular hexagon.

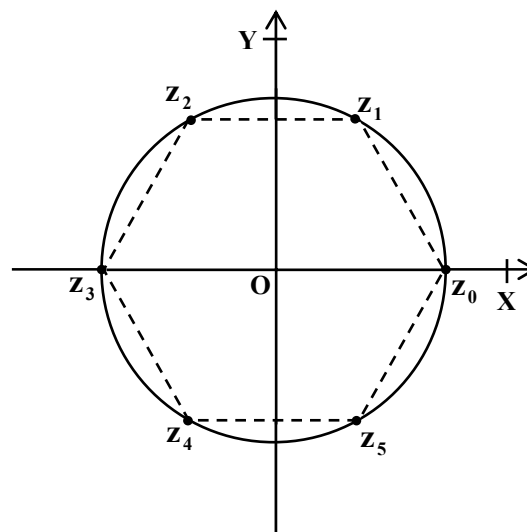


Fig.6: The 6th roots of unity, z_0, \dots, z_5 .

Now, let $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Then all the n th roots of 1 are

ζ is the Greek letter 'zeta'.

$1, \zeta, \zeta^2, \dots, \zeta^{n-1}$, since $\zeta^j = \cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n}$ for $0 \leq j \leq n-1$ (using De Moivre's theorem). We denote the set of the n th roots of unity by U_n .

Thus, $U_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$. Note that $U_n \subseteq \mathbb{C}$.

By solving the following exercises, you will prove an interesting property relating all the n th roots of 1. This property is often used when working with the n th roots of unity.

E31) If $n > 1$ and $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, then show that

$$1 + \zeta + \zeta^2 + \zeta^3 + \dots + \zeta^{n-1} = 0.$$

E32) Show that $U_3 = \{1, \omega, -(1 + \omega)\}$, where $\omega = \frac{-1 + i\sqrt{3}}{2}$.

Now we are in a position to generalise Example 17.

Example 18: Show that U_n is a finite abelian group w.r.t. multiplication.

Solution: As you have seen above, the n th roots of unity are given by

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \text{ for } k = 0, 1, \dots, n-1.$$

Hence, U_n has n elements in it.

$$\begin{aligned} \text{Now, } z_r z_m &= \left(\cos \frac{2r\pi}{n} + i \sin \frac{2r\pi}{n} \right) \left(\cos \frac{2m\pi}{n} + i \sin \frac{2m\pi}{n} \right) \\ &= \cos \frac{2(r+m)\pi}{n} + i \sin \frac{2(r+m)\pi}{n} \\ &= \cos \frac{2j\pi}{n} + i \sin \frac{2j\pi}{n}, \text{ where } (r+m) \equiv j \pmod{n}, \text{ for some } j \text{ s.t.} \end{aligned}$$

$0 \leq j \leq n-1$, using the division algorithm.

Hence, multiplication is a binary operation on U_n .

Since multiplication is associative over \mathbb{C} , and $U_n \subseteq \mathbb{C}$, multiplication is associative over U_n .

The multiplicative identity is $1 = \cos 0 + i \sin 0$.

The multiplicative inverse of z_r is z_{n-r} , since $z_r z_{n-r} = \cos \frac{2n\pi}{n} + i \sin \frac{2n\pi}{n} = 1$.

Finally, since multiplication in \mathbb{C} is commutative, the same holds true for multiplication in U_n .

Thus, (U_n, \cdot) is a finite abelian group. Note that $\mathbf{o}(U_n) = \mathbf{n}$.

Try solving a related exercise now.

E33) Draw the Cayley table for multiplication for the set U_6 . Hence decide if (U_6, \cdot) is the same as (D_6, \circ) .

So far you have considered several different types of groups. Now we shall consider a group made up of two or more groups.

2.4.6 Direct Products

In this sub-section we will discuss a very important method of constructing new groups by using given groups as building blocks. For example, in your previous courses you have come across the set $\mathbb{R} \times \mathbb{R}$, i.e., \mathbb{R}^2 . This is the Cartesian product of \mathbb{R} with itself, as you know.

You also know that for $(x, y), (a, b) \in \mathbb{R} \times \mathbb{R}$,

$$(x, y) \cdot (a, b) = (xa, yb), \text{ and } (x, y) + (a, b) = (x + a, y + b).$$

In fact, $(\mathbb{R} \times \mathbb{R}, +)$ is a group, with identity $(0, 0)$, and the inverse of (a, b) is $(-a, -b)$. On the same lines, given any two groups, we can construct a group using their respective binary operations. Let's see how.

Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. Consider the Cartesian product, G , of G_1 and G_2 (which you studied in Block 1 of the course 'Calculus'). So $G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$.

Can we define a binary operation on G by using the operations on G_1 and G_2 ? Let us try the obvious method, namely, componentwise.

That is, we define the operation $*$ on G by

$$(a, b) * (c, d) = (a *_1 c, b *_2 d) \quad \forall a, c \in G_1, b, d \in G_2.$$

*** is well-defined:** Let $(a, b) = (a', b'), (c, d) = (c', d')$ in G .

Then $a = a', b = b', c = c', d = d'$. Therefore,

$$\begin{aligned} (a, b) * (c, d) &= (a *_1 c, b *_2 d) \\ &= (a' *_1 c', b' *_2 d') \\ &= (a', b') * (c', d'). \end{aligned}$$

Thus, $*$ is well-defined.

*** is closed on G :** For $(a, b), (c, d) \in G$, $(a, b) * (c, d) \in G$, since $a *_1 c \in G_1$ and $b *_2 d \in G_2$. Thus, $*$ is a binary operation on G .

To prove that $(G, *)$ is a group, you need to solve the following exercise.

E34) Show that the binary operation $*$ on $G = G_1 \times G_2$ is associative. Find the identity element, and the inverse of any element (x, y) in G , w.r.t. $*$.

So, you have shown that $G = G_1 \times G_2$ is a group with respect to $*$. We call G the **external direct product** of $(G_1, *_1)$ and $(G_2, *_2)$. (In the next block, you shall study about the 'internal direct product'.)

For example, $(\mathbb{R}^2, +)$ is the external direct product of $(\mathbb{R}, +)$ with itself.

Another example is the direct product $(\mathbb{Z}, +) \times (\mathbb{R}^*, \cdot)$, on which the operation is given by $(m, x) * (n, y) = (m + n, xy)$.

We can also define the external direct product of 3, 4 or more groups on the same lines, as follows.

Definition: Let $(G_1, *_1), (G_2, *_2), \dots, (G_n, *_n)$ be n groups. Their **external direct product** is the group $(G, *)$, where $G = G_1 \times G_2 \times \dots \times G_n$ and $(x_1, x_2, \dots, x_n) * (y_1, y_2, \dots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \dots, x_n *_n y_n) \forall x_i, y_i \in G_i, i = 1, \dots, n$.

Thus, \mathbb{R}^n is the external direct product of n copies of \mathbb{R} and \mathbb{C}^n is the external direct product of n copies of \mathbb{C} , for $n \in \mathbb{N}$.

We would like to make a remark about notation and terminology now.

Remark 7: Henceforth, we will usually assume that all the operations $*, *_1, \dots, *_n$ are multiplication, unless mentioned otherwise, in line with Remark 5. Thus, the operation on $G = G_1 \times G_2 \times \dots \times G_n$ will be given by $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n) \forall a_i, b_i \in G_i$. Further, instead of saying that G is the 'external direct product', **we shall just say 'direct product'**.

Now try solving the following exercises.

E35) Show that $G_1 \times G_2$ is abelian iff both the groups G_1 and G_2 are abelian.

E36) If $G_1 \times G_2$ is infinite, must G_1 and G_2 be infinite? If $G_1 \times G_2$ is finite, must G_1 and G_2 be finite? Give reasons for your answers.

E37) Draw the Cayley table for $(U_3 \times S_3, *)$. What is $o(U_3 \times S_3)$?

With this we come to the end of this introduction to groups. The discussion on various aspects of groups will, of course, continue throughout this course. For now let us consider a brief overview of what you have studied in this unit.

2.5 SUMMARY

In this unit, you have studied the following points.

1. The axioms that define a group, and some examples of this algebraic object.
2. In a group $(G, *)$, the identity w.r.t. $*$ and the inverse of every element w.r.t. $*$ are unique.
3. The right and left cancellation laws hold in a group.
4. The definition, and examples, of abelian and non-abelian groups, of finite and infinite groups, and the order of a finite group.

5. $(ab)^{-1} = b^{-1}a^{-1}$ for a, b in a group G .
6. The laws of indices for elements of a group.
7. An introduction to the group of integers modulo n ($n \in \mathbb{N}$), the symmetric groups, the dihedral groups, matrix groups, the group of the n th roots of unity, for $n \in \mathbb{N}$, and the direct product of groups.

2.6 SOLUTIONS / ANSWERS

- E1) First check that $+$ is a binary operation on \mathbb{Q} . Then, as in Example 1, show that $(\mathbb{Q}, +)$ satisfies G1, G2, G3.

In Example 1, you have seen that (\mathbb{R}, \cdot) satisfies G1 and G2. Hence, (\mathbb{R}^*, \cdot) also satisfies G1 and G2.

Now, for any $r \in \mathbb{R}^*$, $\frac{1}{r} \in \mathbb{R}^*$ s.t. $r \cdot \left(\frac{1}{r}\right) = 1 = \left(\frac{1}{r}\right) \cdot r$.

Hence, (\mathbb{R}^*, \cdot) satisfies G3 also.

Thus, (\mathbb{R}^*, \cdot) is a group.

Similarly, check that subtraction is a binary operation on \mathbb{C} . Then check whether it is associative. For example, is $(2 - 3) - 4 = 2 - (3 - 4)$?

Since G1 is not satisfied, $(\mathbb{C}, -)$ is not a group.

- E2) From Unit 1, you know that the set of 2-cycles in S_3 is $S = \{(1\ 2), (1\ 3), (2\ 3)\}$. Note that $(1\ 2) = (2\ 1)$, and so on. So the question is whether (S, \circ) is a group.

Now, $(1\ 2) \circ (1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3\ 2) \notin S$.

So \circ is not a binary operation on S .

Hence, (S, \circ) is not a group.

- E3) i) From Sec.1.4, Unit 1, you know that $+$ is closed on $M_{2 \times 3}(\mathbb{C})$.

You also know that $+$ is associative over $M_{2 \times 3}(\mathbb{C})$.

Now, you should check that $\mathbf{0} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is the identity w.r.t. $+$.

Also, for $A = [a_{ij}] \in M_{2 \times 3}(\mathbb{C})$, $-A = [-a_{ij}] \in M_{2 \times 3}(\mathbb{C})$ s.t.

$$A + (-A) = \mathbf{0}.$$

Thus, $(M_{2 \times 3}(\mathbb{C}), +)$ is a group.

- ii) From Sec.1.4, Unit 1, you know that \cdot is an associative binary operation on $M_3(\mathbb{C})$.

Also $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is the identity w.r.t. \cdot .

However, not every element has an inverse.

e.g., for $\mathbf{0} \in M_3(\mathbb{C})$, there is no $A \in M_3(\mathbb{C})$ s.t. $\mathbf{0} \cdot A = I$, since

$$\mathbf{0} \cdot \mathbf{A} = \mathbf{0} \quad \forall \mathbf{A} \in \mathbb{M}_3(\mathbb{C}).$$

Thus, $(\mathbb{M}_3(\mathbb{C}), \cdot)$ is not a group.

iii) You should show that (\mathbb{Q}^*, \cdot) is a group, on the same lines as for (\mathbb{R}^*, \cdot) in E1.

iv) Does 2 have an inverse w.r.t. \cdot in \mathbb{Z}^* ? No.
Hence, (\mathbb{Z}^*, \cdot) is not a group.

E4) For $a, b \in \mathbb{R}^+$, $\frac{a}{b} \in \mathbb{R}^+$. Hence, \div is a binary operation on \mathbb{R}^+ . However, show that it does not satisfy G1. Hence, (\mathbb{R}^+, \div) is not a group.

Show that \cdot is not a binary operation on \mathbb{R}^- . Hence, (\mathbb{R}^-, \cdot) is not a group.

E5) '* is closed on S' tells us that all entries of the table have to be from S.
'* is commutative on S' tells us that the table's entries have to be symmetric about the diagonal.

Thus, since the first row is (0 1 2 3), the first column has to be the

same, $\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix}$, and so on. Hence, the table is as below.

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

E6) i) Show that (\mathbb{C}^*, \cdot) is a group, along the lines of E3(iii).
Then explain why it is abelian.

ii) Since \mathbb{R}^* is not finite, this is false.

iii) This is false since $+$ is not a binary operation on \mathbb{Z}_0 .

iv) Explain why this is true, as in Example 1.

v) Check that $*$ is closed on \mathbb{Q}^+ , it is associative, its identity is

$$\frac{1}{2} \in \mathbb{Q}^+ \text{ and the inverse of } a \text{ is } \frac{1}{4a} \in \mathbb{Q}^+.$$

E7) First check that $*$ is a binary operation on G.

Next, for $(a, b), (c, d), (e, f) \in G$,

$$\begin{aligned} ((a, b) * (c, d)) * (e, f) &= (ac, bc + d) * (e, f) = (ace, (bc + d)e + f) \\ &= (ace, bce + (de + f)) \\ &= (a, b) * ((c, d) * (e, f)). \end{aligned}$$

Thus, $*$ satisfies $G1'$.

$$(a, b) * (1, 0) = (a, b) \quad \forall (a, b) \in G.$$

Thus, $G2'$ holds.

$$\text{For } (a, b) \in G, (a, b) * (a^{-1}, -a^{-1}b) = (1, 0).$$

Therefore, $G3'$ holds.

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

E8) Consider the table below:

*	1	2	3
1	2	3	1
2	3	1	2
3	1	3	2

Here $G = \{1, 2, 3\}$. From the operation table of $*$, you can see that all the entries in the table are from G . Hence, $*$ is a binary operation on G . However, there is no element in G that is the identity w.r.t. $*$. Thus, $G2'$ is not satisfied by $(G, *)$. Hence, $(G, *)$ is not a group.

E9) As in the proof of (i), $ad = e$.
Then $ba = ca \Rightarrow bad = cad \Rightarrow b = c$.

E10) Since G is a group, it has an identity e w.r.t. $*$. By the given entries, you know that $a_2 * a_2 \neq a_2$ and $a_2 * a_3 \neq a_2$. Hence, $a_2 \neq e$, $a_3 \neq e$.
Therefore, $a_1 = e$.

Next, by Remark 3, each element occurs once and only once in each row and column of the table.

Finally, since $(G, *)$ is commutative, the table is symmetric with respect to the diagonal from $a_1 * a_1$ to $a_3 * a_3$.

Using the points above, you can see that the table is

*	a_1	a_2	a_3
a_1	a_1	a_2	a_3
a_2	a_2	a_3	a_1
a_3	a_3	a_1	a_2

E11) Take any element of G , say a . Then, by the given condition,
 $ga = g = ge$. By the left cancellation law, this gives $a = e$.
Since a was an arbitrary element of G , this shows that $G = \{e\}$.

E12) Consider $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ in $GL_2(\mathbb{R})$. Now $AB = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$.

Also $C = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}$ is such that $BC = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$.

So $AB = BC$, but $A \neq C$ as, for example, their $(1, 1)$ th elements differ.

$$\begin{aligned}
\text{E13)} \quad & (a_1 a_2 \dots a_n)(a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}) \\
& = a_1 a_2 \dots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \dots a_1^{-1} \\
& = a_1 a_2 \dots a_{n-1} (e) a_{n-1}^{-1} \dots a_1^{-1} \\
& = a_1 a_2 \dots (a_{n-1} a_{n-1}^{-1}) \dots a_1^{-1} \\
& \vdots \\
& = e.
\end{aligned}$$

$$\text{Hence, } (a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}.$$

E14) Let $x, y \in G$.

$$\text{Then } xy = (xy)^2 = xyxy.$$

$$\text{Thus, } x^2 y^2 = xyxy, \text{ since } x^2 = x, y^2 = y.$$

$$\Rightarrow xy = yx, \text{ cancelling } x \text{ from the left and } y \text{ from the right.}$$

Hence, G is abelian.

To see whether the converse is true, consider $(\mathbb{Z}, +)$. This is abelian, but $x + x \neq x$ for any non-zero $x \in \mathbb{Z}$. Hence, the converse is not true.

E15) For $x \in G$, $x^2 = e \Rightarrow x = x^{-1}$, multiplying both sides by x^{-1} .

Now, for $x \in G, y \in G, xy \in G$.

$$\text{So } xy = (xy)^{-1} = y^{-1} x^{-1} = yx.$$

Thus, G is abelian.

You could use $(\mathbb{Z}, +)$ to show why the converse is false.

E16) Since subtraction is not associative, $(\mathbb{Z}, -)$ is not a group. However, $a - x = b$ has a unique solution $a - b$ in \mathbb{Z} . Hence, the converse of Theorem 5 is not true.

E17) No, for example, take (\mathbb{Z}^*, \cdot) . It is a semigroup but not a group. Also $2x = 3$ has no solution in \mathbb{Z}^* .

E18) When $n = 0$, $(a^m)^0 = e = a^{m \cdot 0}$. So the statement is true.

Now, let $n > 0$. We will apply induction on n .

For $n = 1$, the statement is true, since $(a^m)^1 = a^{m \cdot 1} = a^m$.

Now, assume that it is true for $k - 1$, that is, $(a^m)^{(k-1)} = a^{m(k-1)}$, for some $k \geq 2$.

$$\begin{aligned}
\text{Then, } (a^m)^k &= (a^m)^{(k-1+1)} = (a^m)^{(k-1)} \cdot a^m, \text{ by (ii) of Theorem 6.} \\
&= a^{m(k-1)} \cdot a^m, \text{ since it is true for } (k-1). \\
&= a^{m(k-1+1)}, \text{ by (ii) of Theorem 6.} \\
&= a^{mk}.
\end{aligned}$$

So, (iii) is true for k . Hence, it is true $\forall n > 0$ and $\forall m \in \mathbb{Z}$.

Now, let $n < 0$. Then $(-n) > 0$.

$$\begin{aligned}
\therefore (a^m)^n &= [(a^m)^{-n}]^{-1}, \text{ by (i) of Theorem 6.} \\
&= [a^{m(-n)}]^{-1}, \text{ by the case } n > 0.
\end{aligned}$$

$$= [a^{-mn}]^{-1}$$

$$= a^{mn}, \text{ by (i) of Theorem 6.}$$

Thus, $\forall m, n \in \mathbb{Z}$, (iii) holds.

E19) i) Since $b \in G$, $b^m \in G$. So $ab^m = b^m a$, as G is abelian.

ii) If $m = 0$, $(ab)^m = e$, $a^m = e$, $b^m = e$. Hence, $(ab)^m = a^m b^m$.

If $m > 0$, use induction on m to prove it.

If $m < 0$, then $(ab)^{-m} = a^{-m} \cdot b^{-m}$, since $(-m) > 0$.

$$\Rightarrow a^m (ab)^{-m} = b^{-m}$$

$$\Rightarrow a^m = b^{-m} (ab)^m$$

$$\Rightarrow b^m a^m = (ab)^m$$

$$\Rightarrow a^m b^m = (ab)^m, \text{ since } G \text{ is abelian.}$$

E20) Note that $+$ is a binary operation over \mathbb{Z}_5 .

Hence, the table must have entries from \mathbb{Z}_5 only. Thus, it is as below:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Did you notice that the entries are symmetric about the diagonal from $\bar{0} + \bar{0}$ to $\bar{4} + \bar{4}$? What does this tell you about the operation?

E21) From the discussion before the exercises, you know that \cdot is an abelian associative binary operation on \mathbb{Z}_5^* , with identity $\bar{1}$. Thus, the table is as below:

\cdot	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

The Cayley table above shows that for each $\bar{r} \in \mathbb{Z}_5^*$, $\exists \bar{s} \in \mathbb{Z}_5^*$ s.t.

$\bar{r} \cdot \bar{s} = \bar{1}$. Hence, (\mathbb{Z}_5^*, \cdot) is an abelian group.

E22) i) You can form the Cayley table of multiplication over \mathbb{Z}_{11}^* and obtain the inverses as follows.

$$\bar{1}^{-1} = \bar{1}, \bar{2}^{-1} = \bar{6}, \bar{6}^{-1} = \bar{2}, \bar{3}^{-1} = \bar{4}, \bar{4}^{-1} = \bar{3}, \bar{5}^{-1} = \bar{9}, \bar{9}^{-1} = \bar{5}, \bar{7}^{-1} = \bar{8},$$

$$\bar{8}^{-1} = \bar{7}, \bar{10}^{-1} = \bar{10}.$$

ii) For $\bar{r} \in \mathbb{Z}_p^*$, $(r, p) = 1 \Rightarrow rs + pt = 1$ for some $s, t \in \mathbb{Z}$.

$$\Rightarrow \bar{r} \bar{s} \equiv \bar{1} \pmod{p} \Rightarrow \bar{r}^{-1} = \bar{s}.$$

Since $s \in \mathbb{Z} = \bigcup_{i=0}^{p-1} \bar{i}$, $\exists \bar{m} \in \mathbb{Z}_p$ s.t. $\bar{s} = \bar{m}$, $0 \leq m \leq (p-1)$.

However, since $\bar{r}\bar{s} = \bar{1}$, $\bar{s} \neq \bar{0}$ in \mathbb{Z}_p . Hence, $\bar{m} \neq \bar{0}$, i.e., $0 < m \leq (p-1)$.

For example, $\bar{1}^{-1} = \bar{1}$ since $1 \cdot 1 + p \cdot 0 = 1$. (Here $t = 0$.)

Again $\overline{(p-1)}^{-1} = \overline{p-1}$, since $(p-1)^2 \equiv 1 \pmod{p}$. (Note that $(p-1)(p-1) + p(2-p) = 1$.)

- iii) **Multiplication is closed on \mathbb{Z}_p^* :** For $\bar{r}, \bar{s} \in \mathbb{Z}_p^*$, $p \nmid r$ and $p \nmid s$.
Since p is a prime, $p \nmid rs$. Thus, $\overline{rs} = \bar{r}\bar{s} \in \mathbb{Z}_p^*$.

Multiplication is associative and commutative over \mathbb{Z}_p^* , since it is so over \mathbb{Z}_p .

$\bar{1}$ is the multiplicative identity, as discussed earlier.

Every element has an inverse w.r.t. multiplication, as shown in (ii) above.

Thus, (\mathbb{Z}_p^*, \cdot) is an abelian group.

$$\text{E23) } f = (1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

$$\text{So } f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = f.$$

Thus, f^{-1} is a cycle also.

$$\text{E24) } S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

The Cayley table is

\circ	I	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
I	I	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	I	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	I	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	I	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	I
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	I	(1 2 3)

From the table, we see that $I^{-1} = I$, $(1\ 2)^{-1} = (1\ 2)$, $(1\ 3)^{-1} = (1\ 3)$,
 $(2\ 3)^{-1} = (2\ 3)$, $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$, $(1\ 3\ 2)^{-1} = (1\ 2\ 3)$.

$$\text{E25) Check that } (1\ 2)^{-1} = (1\ 2) \text{ and } (2\ 4\ 5)^{-1} = (2\ 5\ 4).$$

Now $(1\ 2) \circ (2\ 4\ 5) = (2\ 4\ 5\ 1)$.

You should check that $[(1\ 2) \circ (2\ 4\ 5)]^{-1} = (1\ 5\ 4\ 2)$.

Also $(1\ 2)^{-1} \circ (2\ 4\ 5)^{-1} = (1\ 2) \circ (2\ 5\ 4) = (2\ 5\ 4\ 1) \neq (1\ 5\ 4\ 2)$, since, for example, $(2\ 5\ 4\ 1)$ maps 2 to 5 and $(1\ 5\ 4\ 2)$ maps 2 to 1.

E26) Consider $(1\ 2\ 3) \in S_4$. This does not lie in D_8 since if you move the vertices 1, 2 and 3 of the square, then you have to move vertex 4 also. But $(1\ 2\ 3)$ leaves 4 fixed and moves the other 3 elements.

E27) $D_{10} = \{I, r, R, R^2, R^3, R^4, rR, rR^2, rR^3, rR^4\}$, where $r^2 = I$, $R^5 = I$ and $rR = R^4r$.

\circ	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
I	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
r	r	I	rR	rR^2	rR^3	rR^4	R	R^2	R^3	R^4
R	R	rR^4	R^2	R^3	R^4	I	r	rR	rR^2	rR^3
R^2	R^2	rR^3	R^3	R^4	I	R	rR^4	r	rR	rR^2
R^3	R^3	rR^2	R^4	I	R	R^2	rR^3	rR^4	r	rR
R^4	R^4	rR	I	R	R^2	R^3	rR^2	rR^3	rR^4	r
rR	rR	R^4	rR^2	rR^3	rR^4	r	I	R	R^2	R^3
rR^2	rR^2	R^3	rR^3	rR^4	r	rR	R^4	I	R	R^2
rR^3	rR^3	R^2	rR^4	r	rR	rR^2	R^3	R^4	I	R
rR^4	rR^4	R	r	rR	rR^2	rR^3	R^2	R^3	R^4	I

E28) No. For example, from the operation table in Example 13, you can see that $r_1 \circ R_{90} \neq R_{90} \circ r_1$ in D_8 , since $r_4 \neq r_3$.

In general, $rR = R^{n-1}r \neq Rr$ unless $n = 2$.

E29) Since $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.

Similarly, check that $B^2 = A^2$, $B^4 = I$ and $BA = -AB = A^3B$, since $-A = (-I)A = A^2 \cdot A = A^3$.

Thus, the table for (Q_8, \cdot) is as below:

\cdot	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	A^2	A	I	A^3
AB	AB	B	A^3B	A^2B	A^3	A^2	A	I
A^2B	A^2B	AB	B	A^3B	I	A^3	A^2	A
A^3B	A^3B	A^2B	AB	B	A	I	A^3	A^2

Since $BA \neq AB$, Q_8 is not abelian.

Also, Q_8 has 8 elements. Hence, $o(Q_8) = 8$.

E30) Elementwise multiplication is a well-defined operation on $M_{m \times n}(\mathbb{C})^*$.

However, it is not closed on $M_{m \times n}(\mathbb{C})^*$, because, for example,

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{C})^*, \text{ but}$$

$$A \cdot B = \begin{bmatrix} 1 \cdot 0 & 0 \cdot 1 \\ 0 \cdot 0 & 0 \cdot 0 \end{bmatrix} = \mathbf{0} \notin \mathbb{M}_2(\mathbb{C})^*.$$

Hence, $(\mathbb{M}_{m \times n}(\mathbb{C})^*, \cdot)$ is not a group.

E31) Note that $0 = 1 - \zeta^n = (1 - \zeta)(1 + \zeta + \zeta^2 + \dots + \zeta^{n-1})$ in \mathbb{C} .

$$\text{Also } \zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \neq 1 \text{ since } n > 1.$$

$$\text{Hence, } 1 + \zeta + \zeta^2 + \dots + \zeta^{n-1} = 0.$$

E32) The cube roots of unity are $1, \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}, \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}$,

$$\text{i.e., } 1, \omega, \omega^2, \text{ where } \omega = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1}{2} + i \frac{\sqrt{3}}{2} = \frac{-1 + i\sqrt{3}}{2}.$$

$$\text{By E31, } 1 + \omega + \omega^2 = 0. \therefore \omega^2 = -(1 + \omega) = \frac{-1 - i\sqrt{3}}{2}.$$

E33) $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, where $\zeta = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6} = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}$.

So the table for (U_6, \cdot) is as below:

\cdot	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
1	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
ζ	ζ	ζ^2	ζ^3	ζ^4	ζ^5	1
ζ^2	ζ^2	ζ^3	ζ^4	ζ^5	1	ζ
ζ^3	ζ^3	ζ^4	ζ^5	1	ζ	ζ^2
ζ^4	ζ^4	ζ^5	1	ζ	ζ^2	ζ^3
ζ^5	ζ^5	1	ζ	ζ^2	ζ^3	ζ^4

Now, you know that $D_6 = S_3$. In E24 you have given the Cayley table of this group. If you compare the tables, you can see that the one above corresponds to a commutative operation, while the one in E24 does not.

Hence, (U_6, \cdot) and (D_6, \circ) are different in structure.

E34) * **is associative:** Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.

Use the fact that $*_1$ and $*_2$ are associative to prove that

$$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3)), \text{ i.e., } * \text{ is associative.}$$

The identity element w.r.t. *: The identity w.r.t. * is (e_1, e_2) , where

e_1 and e_2 are the identities in G_1 and G_2 , respectively. This is because

$$(a, b) * (e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b) \quad \forall (a, b) \in G.$$

The inverse w.r.t. *: You should check that the inverse of $(x, y) \in G$ is

$$(x^{-1}, y^{-1}), \text{ where } x *_1 x^{-1} = e_1, y *_2 y^{-1} = e_2.$$

E35) First let us assume $G_1 \times G_2$ is abelian.

Now, for any $a, c \in G_1, b, d \in G_2$,

$$(a, b)(c, d) = (c, d)(a, b), \text{ i.e., } (ac, bd) = (ca, db).$$

Thus, $ac = ca$ and $bd = db$.
Hence, G_1 and G_2 are abelian.

You should prove the converse. For this, you can move in the reverse direction along the path of the argument above.

E36) Consider $(\{0\}, +)$ and $(\mathbb{Z}, +)$. Then $\{0\} \times \mathbb{Z} = \{(0, m) \mid m \in \mathbb{Z}\}$ is infinite, but $\{0\}$ is finite. Hence, $G_1 \times G_2$ being infinite does not require both G_1 and G_2 to be infinite.

If either of G_1 or G_2 is infinite, then $G_1 \times G_2$ is infinite.

Hence, $G_1 \times G_2$ being finite requires both to be finite.

E37) $U_3 \times S_3 = \{(x, y) \mid x \in U_3, y \in S_3\}$.

Now $U_3 = \{1, \omega, \omega^2\}$ (see E32).

Also S_3 is as in E24.

So $|U_3 \times S_3| = 3 \times 6 = 18$, i.e., $o(U_3 \times S_3) = 18$.

We will start you off on the table. You should complete it.

\cdot	$(1, I)$	$(\omega, (1\ 2))$...
$(1, I)$	$(1, I)$	$(\omega, (1\ 2))$...
$(\omega, (1\ 2))$	$(\omega, (1\ 2))$	(ω^2, I)	...
\vdots	\vdots	\vdots	...

UNIT 3

SUBGROUPS

Structure	Page Nos.
3.1 Introduction Objectives	93
3.2 What is a Subgroup?	94
3.3 Subgroup Tests	96
3.4 Set Operations on Subgroups	103
3.5 Summary	107
3.6 Solutions / Answers	108

3.1 INTRODUCTION

You have studied the algebraic structures of integers, rational numbers, real numbers, and finally, complex numbers. You would have noticed that, not only is $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, but the operations of addition in each of these sets coincide. Similarly, the multiplication in these sets coincide. Further, all these subsets are groups with respect to the same addition. In this unit, the focus is on such subsets of groups.

In Sec.3.2, you will see that subsets of a group $(G, *)$, that are groups with respect to $*$ (in their own right!), are appropriately named subgroups of G . In this section, you will also study several examples of subgroups of different kinds.

In Sec.3.3, you will study conditions on a subset of a group that will ensure that it is a subgroup of the group. You will also get several opportunities to apply these conditions.

Finally, in Sec.3.4, you will be looking at answers to questions like: Is the union of two subgroups a subgroup? Is the intersection of two subgroups a subgroup? Here we will also define the product of two subgroups of a group, and discuss whether or not it is a subgroup also.

Do study this unit carefully because it consists of basic concepts which will be used again and again in the rest of the course. Make sure that you assess yourself regarding having achieved the following expected learning outcomes of this unit. One way of doing so, as we have said in the courses of other semesters too, is to do every exercise on your own, as you come to it.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a subgroup of a group;
- check if the conditions for a subset of a given group to be a subgroup are satisfied or not;
- prove, and apply, results regarding the intersection, union and product of subgroups.

3.2 WHAT IS A SUBGROUP?

As you know, $\mathbb{Z} \subseteq \mathbb{R}$. Also $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$ are groups w.r.t. the operation $+$ defined in the same way. This tells us that $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, as you will now see.

Definition: Let $(G, *)$ be a group. A non-empty subset H of G is called a **subgroup** of G if

- $a * b \in H \forall a, b \in H$, i.e., $*$ is a binary operation on H , and
- $(H, *)$ is a group.

If $(H, *)$ is a subgroup of $(G, *)$, we denote this fact, in symbols, by $(\mathbf{H}, *) \leq (\mathbf{G}, *)$.

For example, $(\mathbb{Z}, +)$ is a subgroup of all 3 groups, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$.

Consider a couple of comments about this concept now.

Remark 1: Re (ii) of the definition above, the associativity of $*$ already holds, since it holds for G , and $H \subseteq G$. So what (ii) really requires is that H must satisfy $G2'$ and $G3'$ (or $G2$ and $G3$) of Unit 2.

Remark 2: In the definition of a subgroup, note that it is important that both H and G are groups w.r.t. **the same operation**. For example, $\mathbb{Q}^* \subseteq \mathbb{Q}$, and (\mathbb{Q}^*, \cdot) is a group. So, is $\mathbb{Q}^* \leq \mathbb{Q}$? No, because \mathbb{Q} is a group w.r.t. addition and \mathbb{Q}^* is not a group w.r.t. $+$. (Why?)

Now, from the definition, you can verify that $(\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. In the same way, you can see why $(\mathbf{G}, *) \leq (\mathbf{G}, *)$ **for any group G** . This leads us to the following definition.

Definition: Let $(G, *)$ be a group and $(H, *) \leq (G, *)$ such that $H \subsetneq G$. Then H is called a **proper subgroup** of G . We denote this by $\mathbf{H} < \mathbf{G}$, or $\mathbf{H} \subsetneq \mathbf{G}$.

We would like to make an important remark about notation here.

Remark 3: If $(H, *)$ is a subgroup of $(G, *)$, **we shall just say that H is a subgroup of G** , provided there is no confusion about the binary operations concerned. We will also denote this fact by $\mathbf{H} \leq \mathbf{G}$.

If H is not a subgroup of G , we will denote it by $\mathbf{H} \not\leq \mathbf{G}$.

Let us consider some examples in detail.

Example 1: Check whether or not \mathbb{Z}_O and \mathbb{Z}_E are subgroups of $(\mathbb{Z}, +)$, where $\mathbb{Z}_O = \{2n+1 \mid n \in \mathbb{Z}\}$ and $\mathbb{Z}_E = \{2n \mid n \in \mathbb{Z}\}$, i.e., \mathbb{Z}_O and \mathbb{Z}_E are the sets of odd integers and even integers, respectively.

Solution: First, we note that \mathbb{Z}_O and \mathbb{Z}_E are non-empty proper subsets of \mathbb{Z} . Now, consider $+$ on \mathbb{Z}_O . In E6, Unit 2, you have seen that $+$ is not a binary operation on \mathbb{Z}_O . Hence, $\mathbb{Z}_O \not\leq \mathbb{Z}$.

Now, regarding \mathbb{Z}_E , for any $n, m \in \mathbb{Z}$, $2n + 2m = 2(n + m)$.

Hence, $+$ is a binary operation on \mathbb{Z}_E .

Since $+$ is associative over \mathbb{Z} , it is associative over \mathbb{Z}_E .

Further, $0 \in \mathbb{Z}_E$ is the identity w.r.t. $+$.

Next, for $a \in \mathbb{Z}_E$, $a = 2n$ for some $n \in \mathbb{Z}$. Hence, $-a = 2(-n) \in \mathbb{Z}_E$.

Thus, by the definition, \mathbb{Z}_E is a group w.r.t. the same operation that makes \mathbb{Z} a group. Hence, $\mathbb{Z}_E \leq \mathbb{Z}$.

Example 2: Show that $M_3(\mathbb{Q})$ is a proper subgroup of $M_3(\mathbb{C})$ (see Sec.2.4.4, Unit 2).

Solution: Firstly, $M_3(\mathbb{Q}) \neq \emptyset$ and $M_3(\mathbb{Q}) \subsetneq M_3(\mathbb{C})$. (Why?)

Next, you know, from Unit 2, that $M_3(\mathbb{Q})$ is a group w.r.t. the same operation of $+$ which makes $M_3(\mathbb{C})$ a group.

Hence, it is a proper subgroup of $M_3(\mathbb{C})$.

Example 3: Show that $n\mathbb{Z} \leq \mathbb{Z} \forall n \in \mathbb{Z}$.

Solution: Note that $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\} \subseteq \mathbb{Z}$.

Now, for any $x, y \in n\mathbb{Z}$, $x = nm$, $y = nr$ for some $m, r \in \mathbb{Z}$.

So, $x + y = nm + nr = n(m + r) \in n\mathbb{Z}$, since $m + r \in \mathbb{Z}$.

Thus, $+$ is closed on $n\mathbb{Z}$.

Next, $+$ is associative in $n\mathbb{Z}$, since it is associative in \mathbb{Z} .

Also, $0 \in n\mathbb{Z}$ is the additive identity, as it is the identity for \mathbb{Z} .

Finally, the additive inverse of $nm \in n\mathbb{Z}$ is $-nm = n(-m) \in n\mathbb{Z}$.

Thus, $(n\mathbb{Z}, +)$ is a group.

Hence, $n\mathbb{Z} \leq \mathbb{Z}$.

Try solving some exercises now.

E1) For each of the following, check whether or not $H \leq G$, where the operation is $+$.

i) $H = \mathbb{R}$, $G = \mathbb{C}$;

- ii) $H = \{I_3, -I_3, \mathbf{0}\}$, where $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, and $G = M_3(\mathbb{Z})$;
- iii) $H = \{5n \mid n \in \mathbb{Z}\}$, $G = \mathbb{Z}$;
- iv) $H = \mathbb{Z}_n$, $G = \mathbb{Z}$ (see Sec.2.4.1, Unit 2);
- v) $H = M_{m \times n}(\mathbb{R})$, $G = M_{m \times n}(\mathbb{C})$ (see Sec.2.4.4, Unit 2).

E2) Make the Cayley tables for $\bar{2}\mathbb{Z}_8$ and \mathbb{Z}_8 . Hence decide if $\bar{2}\mathbb{Z}_8 \leq \mathbb{Z}_8$ or not. What is the relationship between the two Cayley tables?

E3) Prove that a subgroup of an abelian group is abelian.

Here is an important remark about finite subgroups and the corresponding Cayley tables.

Remark 4: While working on E2, you would have realised that if G is finite, and $H \leq G$, then the Cayley table for $(H, *)$ will be a sub-table of the Cayley table for $(G, *)$.

With this, let us end our introductory discussion on subgroups. We now move on to look at some conditions on a subset of a group, that decide whether it is a subgroup or not. These conditions will make it easier for us to give examples, and non-examples, of subgroups.

3.3 SUBGROUP TESTS

While doing E1, you would have checked four conditions in each case – whether $*$ is binary on H , and $G1', G2', G3'$ of Unit 2. Is there a shorter way to decide on whether a subset is a subgroup or not? It turns out that there is. Here is a result which appears to cut down our work a bit.

Theorem 1: A non-empty subset H of a group $(G, *)$ is a subgroup of G if and only if

- i) $*$ is a binary operation on H ;
- ii) $e \in H$, where e is the identity w.r.t. $*$ in G ;
- iii) $\forall h \in H$, the inverse of h in H is the same as the inverse of h in G .

Proof: First let us prove that if $H \leq G$, then these 3 conditions hold.

Now, if $H \leq G$, then the condition (i) is true, by definition of a subgroup.

Regarding (ii), if $(H, *)$ is a subgroup of $(G, *)$, can the identity element in $(H, *)$ be different from the identity element in $(G, *)$? In all the examples you have studied so far, they are the same. But is this only a coincidence? Let us see.

If h is the identity of $(H, *)$, then for any $a \in H$, $h * a = a$.

However, $a \in H \subseteq G$. Thus, $e * a = a$, where e is the identity in G w.r.t. $*$.

Therefore, $h * a = e * a$ in G .

By right cancellation in $(G, *)$, we get $h = e$.

Thus, whenever $(H, *)$ is a subgroup of $(G, *)$, $e \in H$.

Regarding (iii), let $h \in H$. Can its inverse in $(H, *)$ be different from its inverse in $(G, *)$? Let's see.

Let x be the inverse in H , and y be the inverse in G , of $h \in H$.

Since $y = h^{-1}$ in G , $hy = e$ in G .

Also $hx = e$, by (ii).

Hence, $hx = hy$, i.e., $x = y = h^{-1}$. Hence, $h^{-1} \in H$, and (iii) holds.

Now, let us prove the converse, i.e., if (i), (ii) and (iii) hold, then $H \leq G$.

Firstly, by (i), $*$ is a binary operation on H .

Secondly, since $*$ is associative on G , and the operation is the same on H ,

it remains associative on H . Thus, H satisfies $G1'$ (of Sec.2.2, Unit 2).

(ii) and (iii) say that $(H, *)$ satisfies $G2'$ and $G3'$ (of Sec.2.2, Unit 2).

Thus, $(H, *)$ is a group.

Since $H \subseteq G$, $(H, *) \leq (G, *)$. ■

The three conditions in the test above, can be actually abbreviated further to only one condition. Consider the criterion given in the following result.

Theorem 2 (The Subgroup Test): Let H be a **non-empty** subset of a group G . Then the following are equivalent:

- i) H is a subgroup of G .
- ii) Whenever $a, b \in H$, $ab^{-1} \in H$.

Note that in the case of addition the condition in Theorem 2(ii) becomes $a - b \in H \forall a, b \in H$.

Proof: To prove that the statements (i) and (ii) are equivalent, we need to prove that (i) \Rightarrow (ii) and (ii) \Rightarrow (i).

(i) \Rightarrow (ii): Let us assume that $H \leq G$. Then, for any $a, b \in H$, $a, b^{-1} \in H$, by Theorem 1(iii).

Hence, $ab^{-1} \in H$, by Theorem 1(i).

(ii) \Rightarrow (i): Since $H \neq \emptyset$, $\exists a \in H$. But then, $aa^{-1} = e \in H$, by (ii).

Again, for any $a \in H$, since $e \in H$, we get $ea^{-1} = a^{-1} \in H$, by (ii).

Finally, if $a, b \in H$, then $a, b^{-1} \in H$. Thus, $a(b^{-1})^{-1} = ab \in H$, i.e., H is closed w.r.t. the binary operation of G .

Therefore, by Theorem 1, H is a subgroup of G . ■

The **necessary and sufficient criterion** in Theorem 2 makes it easy for us to give examples of subgroups now. Let us re-look the situation in Example 1 to see how Theorem 2 is helpful.

Example 4: Check whether or not the set of even integers, \mathbb{Z}_E , is a subgroup of \mathbb{Z} .

Note that $\mathbb{Z}_E = 2\mathbb{Z}$.

Solution: Firstly, $\mathbb{Z}_E \neq \emptyset$.

Next, for $a, b \in \mathbb{Z}_E$, $a = 2n$ and $b = 2m$ for some $n, m \in \mathbb{Z}$. Thus

$$a + (-b) = 2n - 2m = 2(n - m) \in \mathbb{Z}_E.$$

Hence by Theorem 2, $\mathbb{Z}_E \leq \mathbb{Z}$.

Through Examples 1 and 4 you can see how the subgroup test simplifies life for us! Let us look at a few more examples.

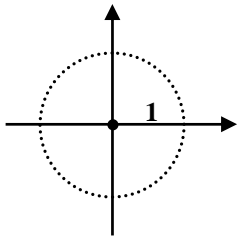


Fig.1: The dotted circle is the unit circle, S^1 .

Example 5: Consider the group (\mathbb{C}^*, \cdot) . Show that $S = \{z \in \mathbb{C} \mid |z|=1\}$ is a subgroup of \mathbb{C}^* . (S is called the **unit circle** in the plane, and is usually denoted by S^1 .)

Solution: Firstly, $S \neq \emptyset$, since $1 \in S$.

Also, for any $z_1, z_2 \in S$, $|z_1 z_2^{-1}| = |z_1| |z_2^{-1}| = |z_1| \frac{1}{|z_2|} = 1$.

Hence, $z_1 z_2^{-1} \in S$.

Therefore, by Theorem 2, $S \leq \mathbb{C}^*$.

Example 6: Show that C , the set of continuous functions from \mathbb{R} to \mathbb{R} , is a subgroup of the group \mathcal{F} of all functions from \mathbb{R} to \mathbb{R} w.r.t. pointwise addition (see Example 6, Unit 2).

Solution: From Calculus, you know that $I: \mathbb{R} \rightarrow \mathbb{R} : I(x) = x$ is a continuous function. Hence, $I \in C$. Thus, $C \neq \emptyset$.

Next, if f is continuous over \mathbb{R} , then you know from Calculus that $(-f)$ is continuous over \mathbb{R} .

Finally, if $f, g \in C$, then $f - g$ is also continuous over \mathbb{R} . Hence, $f - g \in C$. Thus, by Theorem 2, $C \leq \mathcal{F}$.

Example 7: Consider $G = M_{2 \times 3}(\mathbb{C})$, the group of all 2×3 matrices over \mathbb{C} .

Show that $S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{C} \right\}$ is a subgroup of $(G, +)$.

Solution: Since $\mathbf{0} \in S$, $S \neq \emptyset$.

Also, for $\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in S$,

$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} - \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \in S$, since $a-d, b-e, c-f \in \mathbb{C}$.

Therefore, by Theorem 2, $S \leq G$.

Example 8: Consider $GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid \det(A) \neq 0\}$, given in Example 5, Unit 2.

i) Show that $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\}$ is a subgroup of $(GL_2(\mathbb{R}), \cdot)$.

ii) Consider $H = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 2\}$. Is $H \leq GL_2(\mathbb{R})$? Why?

Solution: i) The 2×2 identity matrix is in $SL_2(\mathbb{R})$, since $\det \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) = 1$.

$SL_2(\mathbb{R})$ is called the **special linear group of degree 2 over \mathbb{R}** .

Therefore, $SL_2(\mathbb{R}) \neq \emptyset$.

Now, for $A, B \in SL_2(\mathbb{R})$,

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\frac{1}{\det(B)} = 1, \text{ since } \det(A) = 1 \text{ and}$$

$$\det(B) = 1.$$

$$\therefore AB^{-1} \in SL_2(\mathbb{R}).$$

$$\therefore SL_2(\mathbb{R}) \leq GL_2(\mathbb{R}).$$

ii) Since the determinant of $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ is 2, $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in H$. $\therefore H \neq \emptyset$.

$$\text{However, for any } A \in H, A^{-1} \notin H \text{ since } \det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{2}.$$

Hence $H \not\leq GL_2(\mathbb{R})$.

Now, in E3 you have shown that every subgroup of an abelian group is abelian. The question is: Is every subgroup of a non-abelian group non-abelian? This is not so. Consider the following example.

Example 9: Let $D = \left\{ A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R}^* \right\}$. Show that $D \leq GL_2(\mathbb{R})$ and D

is abelian. Recall, from Unit 2, that $GL_2(\mathbb{R})$ is non-abelian.

Solution: Since $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in D, D \neq \emptyset$.

Also, $AI = A \forall A \in D$. Hence, I is the identity w.r.t. multiplication.

Next, for $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ in D ,

$$AB = \begin{bmatrix} a\alpha & 0 \\ 0 & b\beta \end{bmatrix} \in D, \text{ since } a, b, \alpha, \beta \in \mathbb{R}^*.$$

Also if $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, A^{-1} = \begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$, since $AA^{-1} = \begin{bmatrix} aa^{-1} & 0 \\ 0 & bb^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, the

identity. Thus, $A^{-1} \in D$.

Thus, by Theorem 1, $D \leq GL_2(\mathbb{R})$.

Next, for any $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ in D ,

$$AB = \begin{bmatrix} a\alpha & 0 \\ 0 & b\beta \end{bmatrix} = \begin{bmatrix} \alpha a & 0 \\ 0 & \beta b \end{bmatrix} = BA.$$

Thus, D is an abelian group.

Now consider the direct product of two groups, that you studied in Sec.2.4.6, Unit 2. Can you think of what its subgroups could be? An obvious one is given below.

Example 10: Consider $G_1 \times G_2$, the direct product of the groups G_1 and G_2 . Show that $G_1 \times \{e_2\} \leq G_1 \times G_2$, where e_2 is the identity of G_2 .

Solution: Firstly, $G_1 \times \{e_2\} = \{(a, e_2) \mid a \in G_1\}$. Since $G_1 \neq \emptyset$, $G_1 \times \{e_2\} \neq \emptyset$. Next, let $(a, e_2), (b, e_2) \in G_1 \times \{e_2\}$. Then $(b, e_2)^{-1} = (b^{-1}, e_2) \in G_1 \times \{e_2\}$, since $(b, e_2)(b^{-1}, e_2) = (bb^{-1}, e_2) = (e_1, e_2)$, where e_1 is the identity of G_1 . So $(a, e_2)(b, e_2)^{-1} = (a, e_2)(b^{-1}, e_2) = (ab^{-1}, e_2) \in G_1 \times \{e_2\}$, since $ab^{-1} \in G_1$. Hence, by Theorem 2, $G_1 \times \{e_2\} \leq G_1 \times G_2$.

Now consider a couple of slightly different examples.

Example 11: Let X be a set and Y be a non-empty subset of X . In Example 10 of Unit 2, you studied that $(\wp(X), \Delta)$ is a group. Show that $\wp(Y) \leq \wp(X)$.

Solution: Since $Y \neq \emptyset$, $\wp(Y) \neq \emptyset$.

Now, for any $A \in \wp(Y)$, $A \subseteq Y \subseteq X$. So $A \in \wp(X)$. Thus, $\wp(Y) \subseteq \wp(X)$.

Also, for any $A \in \wp(X)$, $A^{-1} = A$, since $A \Delta A = \emptyset$.

So, for $A, B \in \wp(Y)$, $AB^{-1} = A \Delta B \subseteq Y$. Thus, $AB^{-1} \in \wp(Y)$.

Hence, by Theorem 2, $\wp(Y) \leq \wp(X)$.

Example 12: Check whether or not $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ is a subgroup of \mathbb{R} .

Solution: Firstly, show why $\mathbb{Z}[\sqrt{3}] \neq \emptyset$ and $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R}$.

Next, for $\alpha = a + b\sqrt{3}$ and $\beta = c + d\sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$,

$$\alpha - \beta = (a - c) + (b - d)\sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

Hence, $\mathbb{Z}[\sqrt{3}] \leq \mathbb{R}$.

Try solving the following exercises now.

-
- E4) Show that, for any group G , $\{e\}$ and G are subgroups of G . ($\{e\}$ is called the **trivial subgroup** of G .)
- E5) If G is a finite group and $H \leq G$, what are the maximum and minimum values that $o(H)$ can have?
- E6) Let G_1 and G_2 be two groups. Let $H \leq G_1$, $K \leq G_2$. Show that $H \times K \leq G_1 \times G_2$.
- E7) Show that $(U_n, \cdot) \leq (\mathbb{C}^*, \cdot)$, where U_n is the group of the n th roots of unity.
- E8) Show that the infinite group \mathbb{C}^* has a finite subgroup of order n , for every $n \in \mathbb{N}$.

E9) Give an example, with justification, of

- i) a proper non-trivial subgroup of $M_{3 \times 2}(\mathbb{Z})$,
- ii) a proper subset of $M_{3 \times 2}(\mathbb{C})$ which is not a subgroup,
- iii) a subgroup of \mathbb{R} which is not a subgroup of \mathbb{Q} .

E10) i) Let G be a group, H be a subgroup of G and K be a subgroup of H . Must K be a subgroup of G ? Give reasons for your answer.

E10(i) says that the relation 'is a subgroup of' is transitive.

- ii) Let G be a group and $H \leq G$. If $K \leq G$ s.t. $H \subseteq K$, is $H \leq K$? Why, or why not?

E11) Show that the subset of \mathcal{F} (of Example 6), consisting of functions that are differentiable over \mathbb{R} , is a subgroup of \mathcal{F} .

E12) Check whether or not $\mathbb{Z}[\sqrt{6}] \leq \mathbb{R}$.

Let us now discuss an important subgroup of any group. You will use this subgroup off and on throughout the course. So, let us define the underlying set of this subgroup.

Definition: The **centre of a group** G , denoted by $Z(G)$, is the set of those elements of G that commute with every element of G . Thus,

$$Z(G) = \{g \in G \mid xg = gx \ \forall x \in G\}.$$

The letter Z , which denotes the centre, comes from the German word for centre, 'zentrum'.

For example, if G is abelian, then $Z(G) = G$, since each $g \in G$ commutes with every $x \in G$.

We will now look at why $Z(G) \leq G$ for every group G .

Theorem 3: The centre of a group G is a subgroup of G .

Proof: Since $e \cdot g = g = g \cdot e \ \forall g \in G$, $e \in Z(G)$. Hence, $Z(G) \neq \emptyset$.

Next, $a \in Z(G)$

$$\Rightarrow ax = xa \ \forall x \in G$$

$$\Rightarrow a^{-1}ax = a^{-1}xa \ \forall x \in G$$

$$\Rightarrow x = a^{-1}xa \ \forall x \in G, \text{ since } a^{-1}ax = ex = x.$$

$$\Rightarrow xa^{-1} = a^{-1}x \ \forall x \in G, \text{ multiplying both sides on the right by } a^{-1}.$$

$$\Rightarrow a^{-1} \in Z(G).$$

Also, for any $a, b \in Z(G)$ and for any $x \in G$,

$$(ab)x = a(bx) = a(xb), \text{ since } b \in Z(G).$$

$$= (ax)b = (xa)b, \text{ since } a \in Z(G).$$

$$= x(ab).$$

$$\therefore ab \in Z(G).$$

Thus, by Theorem 1, $Z(G)$ is a subgroup of G . ■

Note that to prove Theorem 3, we needed to prove each condition of Theorem 1. Using Theorem 2 in this case would not help in cutting down the process.

Let us consider some examples about the centre of a group.

Example 13: Check whether or not $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in Z(G)$, where $G = GL_2(\mathbb{R})$.

Solution: For any $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix}$, and

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}.$$

Hence, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ commutes with A only if $b = 0 = c$, i.e., only if A is a diagonal

matrix. So $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ does not commute with every A in G .

Thus, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \notin Z(G)$.

Example 14: Find $Z(Q_8)$ (see E29, Unit 2).

Solution: Consider the Cayley table that you drew up while solving E29, Unit 2. If any element x of Q_8 is in $Z(Q_8)$, it must commute with every element of Q_8 . So, the column headed by x should have elements in exactly the same order as the row headed by x in the Cayley table. This only happens if $x = I$ and $x = A^2 (= -I)$.

Hence, $Z(Q_8) = \{I, -I\}$.

Solving the following exercises will give you some practice in obtaining the centre of a group.

E13) i) Find $Z(S_3)$ and $Z(D_8)$.

(Hint: Write the operation tables for S_3 and D_8 .)

ii) By looking at the Cayley table of a finite group $(G, *)$, how can you decide which element of G is in $Z(G)$?

E14) Is $Z(G)$ an abelian group? Why, or why not?

E15) Prove that $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$, where G_1 and G_2 are groups.

So far you have applied a couple of criteria for checking whether a subset is a subgroup or not. When G is a finite group we have a simpler criterion than the one given in Theorem 2 to decide whether a subset of G is a subgroup or not. In fact, it says that if G is finite, then only (i) of Theorem 1 suffices to decide whether a subset of G is a subgroup or not.

Theorem 4 (Subgroup Test for Finite Groups): Let $(G, *)$ be a finite group. A non-empty subset H of G is a subgroup of G if and only if H is closed w.r.t. $*$.

Proof: If $H \leq G$, then H is closed w.r.t. $*$, by definition.

Let us prove the converse.

Since $H \neq \emptyset$, $\exists a \in H$. Then $A = \{a, a^2, \dots, a^n, \dots\} \subseteq H$.

Since G is finite, so is H . Hence, A must be finite.

Hence, $a^m = a^n$ for some $m, n \in \mathbb{N}$, $m \neq n$(1)

Suppose $m > n$. Then $a^{m-n} = a^m \cdot a^{-n} = a^n \cdot a^{-n} = e$.

Thus, $e \in H$.

Again, (1) tells us that $a^{m-n-1} = a^{m-n} \cdot a^{-1} = e \cdot a^{-1} = a^{-1}$.

Thus, $a^{-1} \in H$.

Thus, by Theorem 1, $H \leq G$.

On exactly the same lines, you can show that $H \leq G$ if $n > m$ in (1). ■

Let us consider an application of Theorem 4 to see how simple it makes life for us!

Example 15: Check whether or not $S = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}\}$ and $T = \{\bar{0}, \bar{6}, \bar{12}\}$ are subgroups of \mathbb{Z}_{20} .

Solution: You can check that the sum of any two elements of S is in S .

Hence, by Theorem 4, $S \leq \mathbb{Z}_{20}$.

Next, $\bar{6} + \bar{12} = \bar{18} \notin T$. Hence, $T \not\leq \mathbb{Z}_{20}$.

Why don't you apply Theorem 4 in some cases now?

E16) Consider the Cayley table of D_8 in Example 13 of Unit 2. Hence decide whether $\{I, R_{90}, R_{90}^2, R_{90}^3\}$ is a subgroup of D_8 or not.

E17) Check if $H = \{I, (1\ 2)\}$ and $K = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ are subgroups of S_3 or not (see Sec.2.4.2, Unit 2).

E18) Give an example to show that the criterion in Theorem 4 does not work for infinite groups.

E19) Let ζ be a 10th root of unity. Check whether or not $\{1, \zeta^2, \zeta^4, \zeta^8\}$ is a subgroup of U_{10} .

Let us now discuss some operations on subgroups.

3.4 SET OPERATIONS ON SUBGROUPS

We will now discuss the behaviour of subgroups under the set operations of intersection, union and product. Let us, first, consider the intersection of any two subgroups of a group.

Consider any $m, n \in \mathbb{Z}$. Then $m\mathbb{Z} \leq \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$. It turns out that $m\mathbb{Z} \cap n\mathbb{Z} \leq \mathbb{Z}$ also, as you will now see.

Theorem 5: If H and K are two subgroups of a group G , then $H \cap K$ is also a subgroup of G .

Proof: Since $e \in H$ and $e \in K$, where e is the identity of G , $e \in H \cap K$.

Thus, $H \cap K \neq \emptyset$.

Now, let $a, b \in H \cap K$.

Since $a, b \in H$, and $H \leq G$, $ab^{-1} \in H$.

Similarly, since $a, b \in K$, and $K \leq G$, $ab^{-1} \in K$.

Thus, $ab^{-1} \in H \cap K$.

Hence, by Theorem 2, $H \cap K$ is a subgroup of G . ■

The whole argument of Theorem 5 remains valid if we take a family of subgroups instead of just two subgroups. Hence, we have the following result.

Theorem 6: If $\{H_i\}_{i \in I}$ is a family of subgroups of a group G , where I is an indexing set, then $\bigcap_{i \in I} H_i$ is also a subgroup of G . ■

Now, do you think the union of two (or more) subgroups is again a subgroup? Consider the two subgroups $2\mathbb{Z}$ and $3\mathbb{Z}$ of \mathbb{Z} . Let $S = 2\mathbb{Z} \cup 3\mathbb{Z}$. Now, $3 \in 3\mathbb{Z} \subseteq S$, $2 \in 2\mathbb{Z} \subseteq S$, but $1 = 3 - 2$ is neither in $2\mathbb{Z}$ nor in $3\mathbb{Z}$. (Why?) Hence, $1 \notin S$. Thus, S is not a subgroup of $(\mathbb{Z}, +)$.

Thus, if A and B are subgroups of G , $A \cup B$ **need not be a subgroup of G** . But, if $A \subseteq B$ (or $B \subseteq A$), then $A \cup B = B$ (or $A \cup B = A$, respectively) is a subgroup of G . E21 says that this is the only situation in which $A \cup B$ is a subgroup of G . You need to prove it, as well as solve the other exercises given below.

E20) Take $G = M_{2 \times 3}(\mathbb{C})$, and let S be the subgroup in Example 7. Let

$$T = \left\{ \begin{bmatrix} a & b & c \\ 0 & 0 & 0 \end{bmatrix} \mid a, b, c \in \mathbb{C} \right\}. \text{ Show that } T \leq G, \text{ and find } S \cap T.$$

Also give two distinct non-trivial elements of this subgroup of G , with justification.

E21) Let A and B be two subgroups of a group G . Prove that $A \cup B$ is a subgroup of G iff $A \subseteq B$ or $B \subseteq A$.

(Hint: Suppose $A \not\subseteq B$ and $B \not\subseteq A$. Take $a \in A \setminus B$ and $b \in B \setminus A$.

Then show that $ab \notin A \cup B$. Hence, $A \cup B \not\leq G$. Note that proving this amounts to proving that $A \cup B \leq G \Rightarrow A \subseteq B$ or $B \subseteq A$.)

E22) You know that if G is a group and $A \leq G$, $B \leq G$, then $A \cap B \leq G$. Is

$A^c = G \setminus A$ also a subgroup of G ? Is $A \Delta B = (A \setminus B) \cup (B \setminus A)$ a subgroup of G , for any group G ? Give reasons for your answers.

Let us now see what we mean by the product of two subsets of a group G .

Definition: Let G be a group and A, B be non-empty subsets of G .

The **product of A and B** is the set $AB = \{ab \mid a \in A, b \in B\}$.

Note that the order of the elements in AB is important. The elements in AB are of the form xy , where $x \in A$ and $y \in B$. Of course, if G is abelian then $xy = yx$. But if G is not abelian yx may not be in AB .

Now, if $H \leq G$, $K \leq G$, is $HK \leq G$? Let us consider some examples that may help us answer this question.

Example 16: Show that $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z} \leq \mathbb{Z}$, but $HK \not\leq S_3$, where $H = \{I, (1\ 2)\}$ and $K = \{I, (1\ 3)\}$.

Solution: $(2\mathbb{Z})(3\mathbb{Z}) = \{(2m)(3n) \mid m, n \in \mathbb{Z}\}$
 $= \{6mn \mid m, n \in \mathbb{Z}\} \subseteq 6\mathbb{Z}$ (2)

Also, if $r \in 6\mathbb{Z}$, then $r = 6s$ for some $s \in \mathbb{Z}$.

So, $r = (2 \cdot 1)(3s) \in (2\mathbb{Z})(3\mathbb{Z})$.

Thus, $6\mathbb{Z} \subseteq (2\mathbb{Z})(3\mathbb{Z})$ (3)

From (2) and (3), we find $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z}$.

Thus, in this case the product of the two subgroups $2\mathbb{Z}$ and $3\mathbb{Z}$ of \mathbb{Z} is a subgroup $6\mathbb{Z}$ of \mathbb{Z} .

Now, consider $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, and its subgroups

$H = \{I, (1\ 2)\}$ and $K = \{I, (1\ 3)\}$.

$HK = \{I \circ I, I \circ (1\ 3), (1\ 2) \circ I, (1\ 2) \circ (1\ 3)\}$
 $= \{I, (1\ 3), (1\ 2), (1\ 3\ 2)\}$.

Now, $(1\ 3), (1\ 2) \in HK$, but $(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \notin HK$.

Hence, HK is not a subgroup of S_3 .

So, the product of two subgroups need not be a subgroup. Now the question is – when will the product of two subgroups be a subgroup? The following theorem answers this question.

Theorem 7: Let H and K be subgroups of a group G . Then HK is a subgroup of G if and only if $HK = KH$.

Proof: Firstly, assume that $HK \leq G$. We will show that $HK = KH$.

Let $hk \in HK$. Then $(hk)^{-1} \in HK$, since $HK \leq G$.

i.e., $k^{-1}h^{-1} \in HK$.

Therefore, $k^{-1}h^{-1} = h_1k_1$ for some $h_1 \in H, k_1 \in K$. But then

$hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$.

Thus, $HK \subseteq KH$ (4)

Now, let $kh \in KH$. Then $(kh)^{-1} = h^{-1}k^{-1} \in HK$. But $HK \leq G$.

Therefore, $((kh)^{-1})^{-1} \in HK$, that is, $kh \in HK$.

Thus, $KH \subseteq HK$ (5)

Putting (4) and (5) together, we see that $HK = KH$.

Conversely, assume that $HK = KH$. We will prove that $HK \leq G$.

Since $e = e^2 \in HK$, $HK \neq \emptyset$.

Now, let $a, b \in HK$. Then $a = hk$ and $b = h_1k_1$ for some $h, h_1 \in H$ and $k, k_1 \in K$.

Then $ab^{-1} = (hk)(k_1^{-1}h_1^{-1}) = h[(kk_1^{-1})h_1^{-1}]$ (6)

Now, $(kk_1^{-1})h_1^{-1} \in KH = HK$. Therefore, $\exists h_2k_2 \in HK$ such that

$(kk_1^{-1})h_1^{-1} = h_2k_2$ (7)

Then, from (6) and (7), $ab^{-1} = h(h_2k_2) = (hh_2)k_2 \in HK$, since $hh_2 \in H$.
Thus, by Theorem 2, $HK \leq G$. ■

Warning: In Theorem 7, note that $HK = KH$ **does not mean** that $hk = kh \forall h \in H$ and $k \in K$.

The following result is a nice corollary to Theorem 7.

Corollary 1: If H and K are subgroups of an **abelian group** G , then HK is a subgroup of G . ■

We give you a chance to prove this (see E23), while solving the following exercises.

E23) Prove Corollary 1.

E24) If $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{C} \right\}$ and $T = \left\{ \begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} \mid a_1, a_2, a_3 \in \mathbb{C} \right\}$, show that

S and T are subgroups of $M_2(\mathbb{C})$. Also check whether $S \cap T$, $S \cup T$ and ST are subgroups of $M_2(\mathbb{C})$ or not.

E25) Prove that a subset H of a group $(G, *)$ is a subgroup iff $HH^{-1} = H$.

You have just seen that if H and K are subgroups of a group G , then $HK \leq G$ only under some conditions.

Now assume G is finite and $HK \leq G$. Is $o(HK) = o(H)o(K)$?

Take, for example, $G = \mathbb{Z}_{30}$, $H = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}, \bar{24}\}$, $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \dots, \bar{28}\}$.

Then $o(H) = 5$, $o(K) = 15$. So $o(H)o(K) = 75 > o(G)$.

Is this possible, since $HK \subseteq G$? No. So, $o(HK)$ need not be $o(H)o(K)$.

So, can we write $o(HK)$ in terms of $o(H)$ and $o(K)$? The answer is in the following theorem.

Theorem 8: Let G be a finite group, and $H \leq G$, $K \leq G$ such that $HK \leq G$.

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

Proof: Firstly, $o(HK) \leq o(H)o(K)$, since $HK = \{hk \mid h \in H, k \in K\}$.

But, to obtain $o(HK)$, we need to know if $hk \in HK$ is repeated, and if so, how many times. So, we want to know under what conditions $hk = h'k'$, where $h, h' \in H$ and $k, k' \in K$, $h \neq h'$, $k \neq k'$.

Now, $hk = h'k' \Rightarrow h^{-1}h = k'k^{-1} = x$, say.

Since $x = h^{-1}h \in H$ and $x = k'k^{-1} \in K$, $x \in H \cap K$.

Also, $h' = hx^{-1}$, $k' = xk$.

So $hk = (hx^{-1})(xk)$, where $x \in H \cap K$.

Further, for any $y \in H \cap K$, $hk = (hy^{-1})(yk)$, with $hy^{-1} \in H$, $yk \in K$.

Thus, each $hk \in HK$ is repeated exactly $o(H \cap K)$ times in HK .

$$\text{Hence, } o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$



If we go back to the example before the theorem, namely, $G = \mathbb{Z}_{30}$, then, $H = \overline{6}\mathbb{Z}_{30}$, $K = \overline{2}\mathbb{Z}_{30}$ and $H \cap K = H$, since $H \subseteq K$. So, by Theorem 8,

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = \frac{o(H)o(K)}{o(H)} = o(K) = 15.$$

Consider another example, one related to S_n .

Example 17: Let $H = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ and $K = \{I, (1\ 2)\}$. Check whether or not $HK \leq S_3$. If it is, find $o(HK)$. If $HK \not\leq S_3$, then find $o(H \cap K)$.

Solution: You should verify that $HK = KH$. Hence, $HK \leq S_3$.

Now $o(H) = 3$, $o(K) = 2$. Also, $o(H \cap K) = 1$, since I is the only common element.

$$\text{Thus, } o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = 6 = o(S_3).$$

Note that $HK \leq S_3$ and both have the same order.

Hence, $HK = S_3$ in this case.

Try solving some exercises now.

E26) Consider D_{10} . Check whether $HK \leq D_{10}$ or not, where $H = Z(D_{10})$ and

$$K = \{1, x, x^2, x^3, x^4 \mid x = R_{72}\}.$$

If it is a subgroup, find $o(HK)$.

If $HK \not\leq D_{10}$, find $o(H \cap K)$.

E27) Check whether or not $AB \leq S_4$, where $A = \{I, (1\ 4)\}$ and $B = \{I, (1\ 2)\}$.

If it is, find $o(AB)$. If $AB \not\leq S_4$, find $C \leq S_4$ s.t. $AC \leq S_4$.

With this we end our discussion on operations on subgroups, and we end this unit. Of course, you will be studying more about subgroups in the other units of this block and the next one. Now let us do a quick point-by-point overview of what you have studied in this unit.

3.5 SUMMARY

In this unit, you have studied the following points.

1. The definition, and examples, of a subgroup of a group.
2. A non-empty subset H of a group $(G, *)$ is a subgroup of G iff
 - i) $*$ is a binary operation on H ;
 - ii) $e \in H$, where e is the identity w.r.t. $*$ in G ;
 - iii) $\forall h \in H$, the inverse of h in H is the same as the inverse of h in G .

3. A non-empty subset H , of $(G, *)$, is a subgroup of $(G, *)$ iff $a * b^{-1} \in H \forall a, b \in H$.
4. The definition, and examples, of the centre of a group G , $Z(G)$. Further, $Z(G)$ is an abelian subgroup of G .
5. Let $(G, *)$ be a finite group. A non-empty subset H of G is a subgroup of G iff H is closed w.r.t. $*$.
6. If H and K are subgroups of a group G , then
 - i) $H \cap K \leq G$;
 - ii) $H \cup K \leq G$ iff $H \subseteq K$ or $K \subseteq H$;
 - iii) $HK = \{hk | h \in H, k \in K\} \leq G$ iff $HK = KH$.
7. If G is a finite group, H and K are subgroups of G such that $HK \leq G$, then
$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

3.6 SOLUTIONS / ANSWERS

- E1) i) As you know, $(\mathbb{R}, +)$ is a group and $\mathbb{R} \subseteq \mathbb{C}$. Hence $(\mathbb{R}, +) \leq (\mathbb{C}, +)$.
- ii) $G = (M_3(\mathbb{Z}), +)$. Since $I_3 \in H$, $I_3 + I_3 = 2I_3$ should be in H if $H \leq G$. But $2I_3 \notin H$. Hence, $+$ is not a binary operation on H . So $H \not\leq G$.
- iii) Here $H = 5\mathbb{Z}$. Show that $H \leq G$, as in Example 3.
- iv) Since the elements of H are subsets of \mathbb{Z} , and not elements of \mathbb{Z} , $H \not\leq G$. Hence, there is no question of H being a subgroup of G .
- v) Argue as in (i) above.

E2) $\bar{2}\mathbb{Z}_8 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

Table for $\bar{2}\mathbb{Z}_8$

+	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Table for \mathbb{Z}_8

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

Use the table of $\bar{2}\mathbb{Z}_8$ to see why it is a group.

Note that the table of $\bar{2}\mathbb{Z}_8$ is the subtable of the table for \mathbb{Z}_8 ,

corresponding to the elements $\bar{0}, \bar{2}, \bar{4}, \bar{6}$. You can see this by taking only the elements in the bigger table that correspond to the rows headed by $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ and the columns headed by $\bar{0}, \bar{2}, \bar{4}, \bar{6}$.

Hence, $\bar{2}\mathbb{Z}_8 \leq \mathbb{Z}_8$.

E3) Let $H \leq G$, where G is abelian. Let $a, b \in H$. Then $a, b \in G$.

So $ab = ba$. Hence, H is abelian.

E4) Since $G \subseteq G$ and G is a group w.r.t. the same operation as G , $G \leq G$.

Since $\{e\} \subseteq G$ and the only element in $\{e\}$ is e , $e \cdot e^{-1} = e \in \{e\}$.

Hence, $\{e\} \leq G$.

E5) Let $o(G) = n$. Since $G \leq G$, the maximum value of $o(H)$ is when

$H = G$, i.e., n . So $o(H) \in \mathbb{N}$ s.t. $o(H) \leq n$.

Also $\{e\} \leq G$, and $o(\{e\}) = 1$. So 1 is the minimum value $o(H)$ can take.

E6) Since H, K are subgroups of G , they are non-empty.

Hence, $H \times K \neq \emptyset$.

Also, for $(h, k) \in H \times K$, $(h, k)^{-1} = (h^{-1}, k^{-1})$.

So, for $(a, b), (c, d) \in H \times K$,

$(a, b)(c, d)^{-1} = (a, b)(c^{-1}, d^{-1}) = (ac^{-1}, bd^{-1}) \in H \times K$, since

$a, c \in H \Rightarrow ac^{-1} \in H$ and $b, d \in K \Rightarrow bd^{-1} \in K$.

Thus, $H \times K \leq G_1 \times G_2$.

E7) In Sec.2.4.5, you have seen that $U_n \subseteq \mathbb{C}^*$ and (U_n, \cdot) is a group. Hence,

$(U_n, \cdot) \leq (\mathbb{C}^*, \cdot)$.

E8) From E7, $U_n \leq \mathbb{C}^* \forall n \in \mathbb{N}$. Also $o(U_n) = n$. Hence the result.

E9) i) Consider $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$. Then you should check that

$S \neq \emptyset$ and $S \leq (M_{3 \times 2}(\mathbb{Z}), +)$.

Since $\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \in M_{3 \times 2}(\mathbb{Z}) \setminus S$, S is a proper subgroup.

Also, since $S \neq \{\mathbf{0}\}$, S is a non-trivial subgroup.

This is only one such example. Look for others too.

ii) Consider $S = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$. Then $S \subsetneq M_{3 \times 2}(\mathbb{C})$.

Since $\mathbf{0} \notin S$, $S \not\leq M_{3 \times 2}(\mathbb{C})$.

There can be many other examples.

- E10) i) Since $K \leq H$, $K \neq \emptyset$ and $ab^{-1} \in K \forall a, b \in K$. Therefore, by Theorem 2, $K \leq G$.
- ii) Since H and K are groups w.r.t. the same operation as that of G , and $H \subseteq K$, $H \leq K$.
- E11) From Calculus, you know that I is differentiable over \mathbb{R} . Argue as in Example 6 to prove that this subset is a subgroup of G .
- E12) $\emptyset \neq \mathbb{Z}[\sqrt{6}] \subseteq \mathbb{R}$, as in Example 12.
 Let $\alpha = a + b\sqrt{6}$ and $\beta = c + d\sqrt{6}$ be in $\mathbb{Z}[\sqrt{6}]$.
 Then $\alpha - \beta = (a - c) + (b - d)\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$.
 $\therefore \mathbb{Z}[\sqrt{6}] \leq \mathbb{R}$.
- E13) i) Look at the Cayley table in your solution of E24, Unit 2. You will find that the only element in S_3 which heads the row with the same entries **in the same order** as the column it heads is I .
 Hence, $Z(S_3) = \{I\}$.
- Look at the table in Example 13, Unit 2. Which elements head the row and the column having the same entries in exactly the same order? I does, but r_1 doesn't since, for example, $r_1 \circ r_3 \neq r_3 \circ r_1$.
 Similarly, r_2, r_3, r_4 and R_{90} don't.
 But R_{180} does, i.e., $R_{180} \circ \sigma = \sigma \circ R_{180} \forall \sigma \in D_8$.
 Again R_{270} does not have the same entries in the row and column headed by it since, for example, R_{270} does not commute with r_1 .
 So $Z(D_8) = \{I, R_{180}\}$.
- ii) From Example 13 and (i) above, you may have got an idea.
 Now $x \in Z(G)$ iff $xg = gx \forall g \in G$, i.e., iff the entries in the row corresponding to x are in exactly the same order as the entries in the column corresponding to x .

E14) Let $x, y \in Z(G)$.

$xy = yx$, since $x \in Z(G)$ and $y \in G$. Thus, $Z(G)$ is abelian.

E15) First, note that both $Z(G_1 \times G_2)$ and $Z(G_1) \times Z(G_2)$ are subgroups of $G_1 \times G_2$ (using the definition of $Z(G)$ and E6).

Next, $(x, y) \in Z(G_1 \times G_2)$

$$\Leftrightarrow (x, y)(a, b) = (a, b)(x, y) \forall (a, b) \in G_1 \times G_2$$

$$\Leftrightarrow (xa, yb) = (ax, by) \forall a \in G_1, b \in G_2$$

$$\Leftrightarrow xa = ax \forall a \in G_1 \text{ and } yb = by \forall b \in G_2$$

$$\Leftrightarrow x \in Z(G_1) \text{ and } y \in Z(G_2)$$

$$\Leftrightarrow (x, y) \in Z(G_1) \times Z(G_2)$$

$$\therefore Z(G_1 \times G_2) = Z(G_1) \times Z(G_2).$$

Note that at each step of the proof **we have used the two-way implication** \Leftrightarrow . This is why we could conclude the equality of the two groups by this argument.

E16) Take the sub-table of the table containing only the elements in the rows and columns corresponding to $I, R_{90}, R_{180} (= R_{90}^2), R_{270} (= R_{90}^3)$. Use these relations, and you will get the table below:

\circ	I	R_{90}	R_{90}^2	R_{90}^3
I	I	R_{90}	R_{90}^2	R_{90}^3
R_{90}	R_{90}	R_{90}^2	R_{90}^3	I
R_{90}^2	R_{90}^2	R_{90}^3	I	R_{90}
R_{90}^3	R_{90}^3	I	R_{90}	R_{90}^2

This table shows that the given set is closed w.r.t. \circ .

Hence, by Theorem 4, $\{I, R_{90}, R_{90}^2, R_{90}^3\} \leq D_8$.

E17) As in E16, consider the Cayley table of S_3 you used in E13(i). Take the sub-tables concerned. Then explain why $H \leq S_3, K \leq S_3$.

E18) Consider $\mathbb{N} \subseteq (\mathbb{Z}, +)$.

\mathbb{N} is closed w.r.t. $+$. However, $(\mathbb{N}, +) \not\leq (\mathbb{Z}, +)$, since $0 \notin \mathbb{N}$.

(There are other reasons you can also give to show why $\mathbb{N} \not\leq \mathbb{Z}$. Why don't you write them down too?)

E19) Since $\zeta^2 \cdot \zeta^4 = \zeta^6 \notin \{1, \zeta^2, \zeta^4, \zeta^8\}$, this is not closed w.r.t. multiplication. Hence, it is not a subgroup of U_{10} .

E20) You should verify that $T \neq \emptyset$ and $T \leq (G, +)$.

Explain why $S \cap T = \left\{ \begin{bmatrix} 0 & \alpha & \beta \\ 0 & 0 & 0 \end{bmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$.

Then, for example, by putting $\alpha = 1, \beta = 0$ and $\alpha = 0, \beta = 1$, you will get two non-zero elements of $S \cap T$. Explain why they are distinct.

E21) You know that if $A \subseteq B$ or $B \subseteq A$, then $A \cup B$ is A or B , and hence, is a subgroup of G .

Conversely, let us assume that $A \not\subseteq B$ and $B \not\subseteq A$, and conclude that $A \cup B \not\leq G$.

Since $A \not\subseteq B, \exists a \in A$ such that $a \notin B$.

Since $B \not\subseteq A, \exists b \in B$ such that $b \notin A$.

Now, if $ab \in A$, then $ab = c$, for some $c \in A$.

Then $b = a^{-1}c \in A$, a contradiction. $\therefore ab \notin A$.

Similarly, $ab \notin B$.

$\therefore ab \notin A \cup B$.

But $a \in A \cup B$ and $b \in A \cup B$. So, $A \cup B \not\leq G$.

E22) For example, consider $S \leq \mathbb{Z}_{20}$ given in Example 15. Then $\bar{3}$ and $\bar{2}$ are in S^c , but $\bar{3} + \bar{2} = \bar{5} \notin S^c$. Hence, $S^c \not\leq \mathbb{Z}_{20}$.

Since $A \setminus B \not\subseteq B \setminus A$ and $B \setminus A \not\subseteq A \setminus B$, by definition, $A \Delta B \not\leq G$, by E21.

E23) For any $hk \in HK, hk = kh \in KH$. So $HK \subseteq KH$. Similarly, $KH \subseteq HK$. Hence, $HK = KH$. Hence, $HK \leq G$.

E24) As in Example 9, show that $S \leq \mathbb{M}_2(\mathbb{C})$.

Similarly, apply Theorem 2, to show that $T \leq \mathbb{M}_2(\mathbb{C})$. Remember, the operation concerned is addition.

By Theorem 5, $S \cap T \leq G$.

Note that $S \subseteq T$. Hence, $S \cup T = T \leq G$.

Now, for $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in S$ and $\begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} \in T$, $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} = \begin{bmatrix} aa_1 & aa_2 \\ 0 & ba_3 \end{bmatrix}$.

So $ST = \left\{ \begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix} \mid a, a_1, a_2, \alpha \in \mathbb{C} \right\}$.

Also, check that $TS = \left\{ \begin{bmatrix} \beta & bb_1 \\ 0 & bb_2 \end{bmatrix} \mid \beta, b, b_1, b_2 \in \mathbb{C} \right\}$.

Now any element of ST lies in TS because $\begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix} = \begin{bmatrix} \beta & aa_2 \\ 0 & a(a^{-1}\alpha) \end{bmatrix}$,

if $a \neq 0$.

If $a = 0$, then $\begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix}$, trivially lies in TS .

Thus, $ST \subseteq TS$. Similarly, show that $TS \subseteq ST$.

Hence, $ST = TS$, and $ST \leq \mathbb{M}_2(\mathbb{C})$.

E25) Note that $HH^{-1} = \{ab^{-1} \mid a, b \in H\}$.

If $H \leq G$, then $ab^{-1} \in H \forall a, b \in H$. Hence, $HH^{-1} \subseteq H$.

Also, for any $h \in H$, $h = he^{-1} \in HH^{-1}$. Hence, $H \subseteq HH^{-1}$.

Thus, $HH^{-1} = H$.

Conversely, if $HH^{-1} = H$, then $ab^{-1} \in H \forall a, b \in H$.

Hence, $H \leq G$.

E26) Since $zy = yz \forall z \in Z(D_{10})$ and $y \in D_{10}$, $zx = xz$. Hence,

$$zx^i = x^i z \forall i = 2, 3, 4.$$

Hence, $HK = KH$.

Thus, $HK \leq D_{10}$.

Now, $H = \{I\}$. (Check this by writing the Cayley table for D_{10} .)

$$\text{So } o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = \frac{1 \times 5}{1} = 5.$$

E27) $AB = \{I, (1\ 4), (1\ 2), (1\ 2\ 4)\}$.

But, $(1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin AB$. $\therefore AB \not\leq S_4$.

Now consider $C = A$.

Then $AC = A^2 = \{I, (1\ 4)\} \leq S_4$.

UNIT 4

CYCLIC GROUPS

Structure

Page Nos.

4.1	Introduction	113
	Objectives	
4.2	Order of an Element	114
4.3	Properties of a Cyclic Group	120
4.4	Set of Generators	130
4.5	Summary	132
4.6	Solutions / Answers	133

4.1 INTRODUCTION

So far you have studied many examples of groups and subgroups. While studying this unit, you will find that some of those are examples of a kind of group that this unit is about, i.e., a cyclic group. For example, you will find that \mathbb{Z}_n and \mathbb{Z} are cyclic groups. In fact, as you will discover in Unit 8, these are essentially the only cyclic groups. These groups are important for several reasons, one of them being that all abelian groups are built up from these cyclic groups.

In Unit 2, you studied about the order of a finite group. In Sec.4.2, we will use this concept to introduce you to the idea of the order of an element of a group. Then you will study several examples and important properties of the order of an element. In this section, we shall also define a cyclic group, and take you through many examples of such a group.

In Sec.4.3, you will study many interesting properties of cyclic groups, finite and infinite. You will also see why every cyclic group is abelian. Further, in this section, you will see why any subgroup of \mathbb{Z} is of the form $m\mathbb{Z}$, for some $m \in \mathbb{Z}$. Also, you will study how to obtain all the subgroups of a group like \mathbb{Z}_n or U_n , $n \in \mathbb{N}$.

Finally, in Sec.4.4, we will extend the idea of one generator of a cyclic group to that of a generating set. You will see that many different sets, with different cardinalities, can generate the same group.

Let us now list the specific learning objectives around which this unit is built.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, the order of an element of a group;
- prove, and use, the relationship between the order of an element of a group and the order of its integral powers;
- explain what a cyclic group is, and give examples of such a group;
- prove, and apply, the statement that every subgroup of a cyclic group is cyclic;
- obtain all the subgroups of a finite cyclic group;
- define, and give examples of, a generating set of a group.

4.2 ORDER OF AN ELEMENT

In Unit 2, you studied about finite and infinite groups. You also know what the order of a finite group is. For instance, $o(D_{2n}) = 2n$ and $o(S_n) = n!$ for $n \in \mathbb{N}$. Here we shall look at what the order of an element of a group is. As you will see, this is the order of a group that is 'built up' by this element.

Recall, from Unit 3, that $m\mathbb{Z} = \{0, \pm m, \pm 2m, \dots\}$ is a subgroup of \mathbb{Z} , for $m \in \mathbb{Z}$. Now, if $H \leq \mathbb{Z}$ s.t. $m \in H$, what do you expect the relationship to be between $m\mathbb{Z}$ and H ? Does it surprise you to know that $m\mathbb{Z} \subseteq H$? You know that if $m \in H$, then $-m \in H$. Hence, $2m, 3m, \dots$ and $-2m, -3m, \dots$ are also in H . Thus, $m\mathbb{Z} \subseteq H$.

Hence, $m\mathbb{Z}$ is contained in every subgroup of \mathbb{Z} containing m . Thus, $m\mathbb{Z}$ is the smallest subgroup of \mathbb{Z} containing m .

What you have noted above is not true for \mathbb{Z} alone. It is true for any group, as we will now prove.

Theorem 1: Let G be a group and $a \in G$. Then $A = \{a^0, a^1, a^{-1}, a^2, a^{-2}, \dots\} = \{a^n \mid n \in \mathbb{Z}\}$ is the smallest subgroup of G containing a .

Proof: First, let us show that $A \leq G$.

Since the operation in G is associative in G , it is associative in A .

Since $a^0 = e$, $e \in A$.

For each $a^n \in A$, $\exists a^{-n} \in A$ s.t. $a^n a^{-n} = e$.

Hence, by the subgroup criteria in Unit 3, $A \leq G$.

Next, let H be any subgroup of G containing a .

Since $a \in H$ and H is a group, $a^n \in H \forall n \in \mathbb{N}$.

Similarly, since $a^{-1} \in H$ and H is a group, $a^{-n} \in H \forall n \in \mathbb{N}$.

Also $e \in H$, since $H \leq G$, i.e., $a^0 \in H$.

Hence, $A \subseteq H$.

Thus, A is contained in every subgroup of G containing a .

Hence, A is the smallest subgroup of G containing a . ■

Theorem 1 leads us to the following definitions.

Definitions: Let G be a group, and $a \in G$.

- i) The smallest subgroup of G containing a is called the **cyclic subgroup of G generated by a** , and is denoted by $\langle a \rangle$.
- ii) If $G = \langle a \rangle$ for some $a \in G$, then G is called a **cyclic group**.
- iii) a is called a **generator** of the group $\langle a \rangle$.
- iv) The **order of the element a** is defined to be the order of the group $\langle a \rangle$, if $\langle a \rangle$ is finite.
If $\langle a \rangle$ is infinite, then the **order of a is infinite**.
In either case, the order of a is denoted by $o(a)$.

For example, the cyclic subgroup of \mathbb{Z} generated by $0 \in \mathbb{Z}$ is $\{0\}$, since $n \cdot 0 = 0 \forall n \in \mathbb{Z}$.

Thus, $o(0) = o(\{0\}) = 1$.

Similarly, for any group G , $o(e) = o(\{e\}) = 1$.

Also, note that in \mathbb{Z} , $\langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \{n \mid n \in \mathbb{Z}\} = \mathbb{Z}$.

Thus, $\mathbb{Z} = \langle 1 \rangle$, that is, \mathbb{Z} is a **cyclic group**. This also shows that $1 \in \mathbb{Z}$ has **infinite order**.

Similarly, for $2 \in \mathbb{Z}$, $\langle 2 \rangle = \{2n \mid n \in \mathbb{Z}\}$, so that 2 has infinite order. In fact, **any non-zero integer has infinite order**.

Let us now look at some more examples of finding the orders of group elements.

Example 1: Find the order of

- i) $\bar{3}$ in \mathbb{Z}_5 , and
- ii) $\bar{3}$ in \mathbb{Z}_6 .

Solution: In either case $\langle \bar{3} \rangle = \{0, \pm \bar{3}, \pm 2 \cdot \bar{3}, \pm 3 \cdot \bar{3}, \dots\}$.

- i) Here $2 \cdot \bar{3} = \bar{6} = \bar{1}$ in \mathbb{Z}_5 and $-\bar{3} = \bar{5} - \bar{3} = \bar{2}$ in \mathbb{Z}_5 , as you know from Sec.2.4, Unit 2.

Similarly, $(-2)\bar{3} = -\bar{6} = \bar{4}$, and so on.

You can check that $\langle \bar{3} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}_5$.

Thus, $\bar{3}$ generates \mathbb{Z}_5 . So the order of $\bar{3}$ is $o(\bar{3}) = o(\mathbb{Z}_5) = 5$.

Also note that \mathbb{Z}_5 is a cyclic group.

- ii) Here $-\bar{3} = \bar{6}$, $2 \cdot \bar{3} = \bar{6}$, $(-2)\bar{3} = -\bar{6} = \bar{3}$, $3 \cdot \bar{3} = \bar{0}$, $-3 \cdot \bar{3} = \bar{0}$, $4 \cdot \bar{3} = \bar{3}$, $-4 \cdot \bar{3} = -\bar{3} = \bar{6}$, and so on.

As you find all the element of $\langle \bar{3} \rangle$, you will see that the elements $\pm n \cdot \bar{3}$ keep returning to being one of $\{\bar{0}, \bar{3}, \bar{6}\}$.

Thus, here $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}\}$.

Hence, $o(\bar{3}) = 3$.

Now, consider $\bar{3}$ in (i) of Example 1. If you compute $\bar{3}, 2 \cdot \bar{3}, \dots$, you will see

that $o(\bar{3}) = 5$ is the least positive integer n such that $n \cdot \bar{3} = \bar{0}$. This is true in general, as you will now see.

Theorem 2: Let G be a group and $g \in G$.

- $o(g) = 1$ iff $g = e$.
- i) If $o(g)$ is finite, then $o(g)$ is the least positive integer n such that $g^n = e$. (Note that if $g \in (G, +)$, then $o(g)$ is the least positive integer n such that $ng = e$.)
 - ii) If $o(g)$ is finite, and $s \in \mathbb{Z}$ s.t. $g^s = e$, then $o(g) \mid s$.
 - iii) If $o(g)$ is infinite, then $g^m \neq g^n$ if $m \neq n$, where $m, n \in \mathbb{Z}$.

Proof: Note that $o(g) = o(\langle g \rangle)$, where $\langle g \rangle = \{e, g^{\pm 1}, g^{\pm 2}, \dots\}$.

- i) Here $g \in G$ has finite order. So, the set $\{e, g, g^2, \dots\}$ is finite. Therefore, all the powers of g can't be distinct. Therefore, $g^r = g^s$ for some $r > s$. Then $g^{r-s} = e$, and $r - s \in \mathbb{N}$.

Thus, the set $T = \{t \in \mathbb{N} \mid g^t = e\}$ is non-empty. So, by the well-ordering principle (see Sec.1.2, Unit 1), T has a least element, say n .

Then $g^n = e$(1)

Let $A = \{e, g, g^2, \dots, g^{n-1}\}$.

Then $A \subseteq \langle g \rangle$(2)

Also, for any $m \in \mathbb{Z}^*$, by the division algorithm $m = qn + r$, for some $q, r \in \mathbb{Z}$, $0 \leq r < n$.

Then $g^m = (g^n)^q \cdot g^r = g^r$ for some r , $0 \leq r < n$, by (1).

Hence, $g^m \in A$.

Therefore, $\langle g \rangle \subseteq A$(3)

By (2) and (3), $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$.

Therefore, $o(g) = o(\langle g \rangle) = n$, the least positive integer s.t. $g^n = e$.

- ii) Let $o(g) = n$ and $g^s = e$ for some $s \in \mathbb{Z}$. By the division algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $s = qn + r$, $0 \leq r < n$.

Then $g^s = e \Rightarrow g^{qn} \cdot g^r = e \Rightarrow g^r = e$.

But n is the least positive integer s.t. $g^n = e$.

Therefore, the only possibility for r is $r = 0$.

Then $s = qn$, i.e., $n \mid s$.

- iii) Now assume $g \in G$ is of infinite order. Let $m, n \in \mathbb{Z}$ s.t. $m \neq n$.

Suppose $g^m = g^n$. Then $g^{m-n} = e$. Then, as in (i) above, this shows that $\langle g \rangle$ is a finite group, a contradiction to the hypothesis that g is of infinite order.

Hence, if $m \neq n$, then $g^m \neq g^n$. ■

So, let us see how Theorem 2 makes life easier for us.

Example 2: Find the order of $\bar{3}$ in \mathbb{Z}_9 .

Solution: In Example 1(ii) you had to calculate $n \cdot \bar{3}$ for several values of $n \in \mathbb{Z}$ before you could find a pattern. But now you can see that

$$1 \cdot \bar{3} = \bar{3}, 2 \cdot \bar{3} = \bar{6}, 3 \cdot \bar{3} = \bar{9} = \bar{0}.$$

Hence, using Theorem 2, $o(\bar{3}) = 3$ in \mathbb{Z}_9 .

Example 3: Find the orders of $(1\ 2)$ and $(1\ 2\ 3)$ in S_5 .

Solution: Recall that $(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq I$.

Next $(1\ 2)^2 = (1\ 2) \circ (1\ 2) = I$.

$\therefore o((1\ 2)) = 2$.

You should similarly show that $o((1\ 2\ 3)) = 3$.

Consider the following observation connected to the example above.

Remark 1: In Unit 9, you will see that the order of any cycle of length n is $n \ \forall n \in \mathbb{N}$.

Try doing a set of exercises now.

E1) Find the orders of

i) R_{90} and R_{180} in D_8 ,

ii) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ in Q_8 ,

iii) $\bar{1}$ in \mathbb{Z}_{10} ,

iv) $\bar{1}$ in \mathbb{Z}_n , for any $n \in \mathbb{N}$,

v) $(-5) \in \mathbb{Z}$,

vi) $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \in M_2(\mathbb{Z})$.

E2) Show that if $H \leq G$, $H \neq \{e\}$, then $H \neq \langle e \rangle$.

E3) Show that $\langle a \rangle = \langle a^{-1} \rangle$ for any a in a group G .

E3 tells us that a cyclic subgroup does not have a unique generator.

E4) Show that if G is a group and $a \in G$, then $\langle a \rangle = \bigcap \{H \mid H \leq G \text{ and } a \in H\}$.

E5) Prove that $\mathbb{Z}_n = \langle \bar{1} \rangle \ \forall n \in \mathbb{N}$.

E6) Find $o(A)$ for $A \in M_{2 \times 3}(\mathbb{R})$, $A \neq \mathbf{0}$.

E7) Find $o(A)$, where $A = \begin{bmatrix} 0 & r \\ 1 & 0 \end{bmatrix} \in GL_2(\mathbb{R})$.

E8) Let S be a non-empty set. Find the order of $A \in \wp(S)$ (see Example 10, Unit 2).

Let us now look at some properties of the order of an element. As an example of the first property, consider any $\bar{x} \in \mathbb{Z}_5$. Now, $n \cdot \bar{x} = n(\bar{m} + \bar{x} - \bar{m})$, for any

$\bar{m} \in \mathbb{Z}_5$. Hence, if $r = o(\bar{x})$, then $r = o(\bar{m} + \bar{x} - \bar{m})$ too. In fact, this is true not just for \mathbb{Z}_5 , but for any group, as you will now see.

gag^{-1} is called the
conjugate of a by g .

Theorem 3: Let G be a group. The order of $a \in G$ is the same as the order of gag^{-1} for any $g \in G$.

Proof: First, note that $ga^n g^{-1} = (gag^{-1})^n \forall g \in G$ and $n \in \mathbb{Z}$. (Why?)

Now, there are two cases – $o(a)$ is finite, or $o(a)$ is infinite.

Case 1: Let $o(a)$ be finite, say m . Then m is the least positive integer s.t.

$$a^m = e.$$

So $ga^m g^{-1} = gg^{-1} = e$. Hence, $(gag^{-1})^m = e$.

Hence, $o(gag^{-1})$ is also finite, say $o(gag^{-1}) = r$.

Then, by Theorem 2(ii),

$$r \mid m. \quad \dots(4)$$

Similarly, since $(gag^{-1})^r = e$, $ga^r g^{-1} = e$, i.e., $a^r = e$.

$$\text{Hence, } m \mid r. \quad \dots(5)$$

By (4) and (5), $r = \pm m$. But both r and m are positive.

Hence, $r = m$.

Thus, $o(gag^{-1}) = o(a)$, for any $g \in G$.

Case 2: Let $o(a)$ be infinite. Then $a^n \neq e$ for any $n \in \mathbb{N}$.

Hence, $(gag^{-1})^n \neq e$ for any $n \in \mathbb{N}$.

Thus, $o(gag^{-1})$ is also infinite, the same as $o(a)$. ■

Let us look at an immediate application of Theorem 3. You know that $(1 \ 2 \dots n) \in S_n$. By Remark 1, $n = o((1 \ 2 \dots n))$. Hence, by Theorem 3,

$o(\sigma(1 \ 2 \dots n)\sigma^{-1}) = n$ for any $\sigma \in S_m$, $m \geq n$. You will be using this result in Unit 9 many times.

Now, let us look at another property. You have earlier seen that $\mathbb{Z} = \langle 1 \rangle$, so that $o(1)$ is infinite. In fact, $o(n)$ is infinite $\forall n \in \mathbb{Z}^*$.

This may lead you to wonder if, for any group G and $g \in G$, $o(g) = o(g^r)$ for $r \in \mathbb{Z}$. However, in \mathbb{Z}_{12} , $o(\bar{1}) = 12$. But $o(\bar{4}) \neq 12$. In fact, $o(\bar{4}) = 3$, as you can verify. So, the question arises – is there a relationship between $o(g^r)$ and $o(g)$, when $o(g)$ is finite? Let's see.

Theorem 4: Let G be a group, and $g \in G$.

- i) If g is of infinite order, then g^m is also of infinite order for every $m \in \mathbb{Z}^*$.
- ii) If $o(g) = n$, then $o(g^m) = \frac{n}{(n, m)} \forall m = 1, \dots, n-1$. (Recall that (n, m) is the g.c.d of n and m .)

Proof: i) An element is of infinite order iff all its powers are distinct. We know that all the powers of g are distinct. We have to show that all the powers of g^m are distinct, where $m \in \mathbb{Z}^*$.

If possible, let $(g^m)^t = (g^m)^w$ for some $t, w \in \mathbb{Z}$. Then $g^{mt} = g^{mw}$.

But then, by Theorem 2, $mt = mw$, since g is of infinite order. Hence,
 $t = w$.

This shows that the powers of g^m are all distinct, and hence, g^m is of infinite order.

- ii) Since $o(g) = n$, $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$. Now $\langle g^m \rangle$ is a subgroup of $\langle g \rangle$, and so it must be of finite order.

Thus, g^m is of finite order.

Let $o(g^m) = t$. We will show that $t = \frac{n}{(n, m)}$.

Now, $g^{mt} = (g^m)^t = e$.

So $n \mid mt$, by Theorem 2(ii). ...(6)

Let $d = (n, m)$. We can then write $n = n_1d$, $m = m_1d$, where $(m_1, n_1) = 1$.

Then $n_1 = \frac{n}{d} = \frac{n}{(n, m)}$.

By (6), $n \mid tm_1d \Rightarrow n_1d \mid tm_1d \Rightarrow n_1 \mid tm_1$.

But $(n_1, m_1) = 1$.

Therefore, $n_1 \mid t$, as you have learnt in Unit 1. ...(7)

Also, $(g^m)^{n_1} = g^{m_1dn_1} = g^{m_1n} = (g^n)^{m_1} = e^{m_1} = e$.

Thus, by the definition of $o(g^m)$ and Theorem 2, we have

$t \mid n_1$(8)

(7) and (8) show that $t = n_1 = \frac{n}{(n, m)}$,

i.e., $o(g^m) = \frac{n}{(n, m)}$. ■

Using Theorem 4 we know, for example, that $o(\bar{4})$ in \mathbb{Z}_{72} is

$$\frac{72}{(72, 4)} = \frac{72}{4} = 18, \text{ since } o(\bar{1}) = 72 \text{ in } \mathbb{Z}_{72}. \text{ Let us consider another example.}$$

Example 4: Consider $D_{20} = \{1, R, \dots, R^9, r, rR, \dots, rR^9\}$, with

$o(r) = 2$, $o(R) = 10$ and $rR = R^{-1}r$. Find $o(R^2)$ and $o(R^3)$.

Solution: Since $o(R) = 10$, by Theorem 4 $o(R^2) = \frac{10}{(10, 2)} = \frac{10}{2} = 5$ and

$$o(R^3) = \frac{10}{(10, 3)} = \frac{10}{1} = 10.$$

Now consider a corollary of Theorem 4.

Corollary 1: If $G = \langle g \rangle$ is finite, of order n , then

i) $o(g^m) = o(g^{(n, m)})$, for $m \in \mathbb{N}$.

ii) $G = \langle g^m \rangle$ iff $(m, n) = 1$. ■

We leave the proof of Corollary 1 to you (see E9).

In the context of Corollary 1(ii), consider the following remark. In this remark we stress the point made because of a common error learners make.

Remark 2: In the context of Corollary 1, you can have $\langle g \rangle = \langle g^m \rangle$ for some $m \in \mathbb{Z}$, but $g \neq g^m$. For example, in \mathbb{Z}_{30} , $o(\bar{1}) = 30$. Also, by Theorem

$$4(\text{ii}), o(\bar{7}) = \frac{30}{(30, 7)} = 30.$$

So $\langle \bar{1} \rangle = \langle \bar{7} \rangle$, but $\bar{1} \neq \bar{7}$.

Similarly, $o(\bar{2}) = \frac{30}{(30, 2)} = 15$ and $o(\bar{4}) = 15$, but $\bar{2} \neq \bar{4}$.

The next few exercises will give you some practice in using Theorem 4.

E9) Prove Corollary 1.

E10) Find the orders of $\bar{2}$, $\bar{4}$ and $\bar{5} \in \mathbb{Z}_{18}$.

E11) If G is a finite cyclic group, then show that $o(x)$ divides $o(G) \forall x \in G$. In particular, show that $x^{o(G)} = e \forall x \in G$.

E12) Let $U_{10} = \langle \zeta \rangle$. Find $o \langle \zeta^3 \rangle$.

E13) Let G be a group, and $x \in G$ be of order 15. Find the orders of x^2 , x^6 and x^{10} .

E14) Let G be a group and let $x \in G$ be of order n . Prove that $\langle x^m \rangle = \langle x^{n-m} \rangle$, where $0 < m \leq n$. Hence prove that $(n, m) = (n, n - m)$.

E15) Find the elements of $\langle \bar{25} \rangle$ in \mathbb{Z}_{30} , and of $\langle \zeta^7 \rangle$ in U_{10} , where ζ is a generator of U_{10} .

The properties you have studied in this section, lead us very naturally to consider properties of cyclic groups. This is what we will discuss in the next section.

4.3 PROPERTIES OF A CYCLIC GROUP

In Sec.4.2, you studied the definition of a cyclic group. Here we shall look at examples of such groups, and some of their properties.

In the previous section, you have seen that $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_5 = \langle \bar{3} \rangle$ and $\mathbb{Z}_{18} = \langle \bar{5} \rangle$. So these are examples of cyclic groups, as you know. Let us consider some more examples.

Example 5: Show that U_n is a cyclic group $\forall n \in \mathbb{N}$.

Solution: In Sec.2.4.5, Unit 2, you have seen that if $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$,

then $U_n = \{\zeta, \zeta^2, \dots, \zeta^n (= 1)\}$.

Thus, $U_n = \langle \zeta \rangle$, where $o(\zeta) = n$.

Notice that the examples of cyclic groups that you have studied so far are all abelian. Can we find non-abelian cyclic groups? This is answered by the following theorem.

Theorem 5: A cyclic group is abelian.

Proof: Let $G = \langle a \rangle$ be a cyclic group, and let $x, y \in G$. Then $x = a^n$, $y = a^m$ for some $m, n \in \mathbb{Z}$. So

$$\begin{aligned} xy &= a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n \\ &= yx, \text{ using Theorem 6, Unit 2.} \end{aligned}$$

Hence, G is a commutative group. ■

Because of Theorem 5, you now know that every **cyclic subgroup of a group is abelian**, regardless of whether the group is abelian or not. For example, you know that S_3 is not abelian. But $\langle (1\ 2) \rangle$ and $\langle (1\ 3\ 2) \rangle$ are abelian subgroups of S_3 .

Now, the question is – are all abelian groups cyclic? The answer is in the following examples.

Example 6: Consider the set $K_4 = \{e, a, b, ab\}$, and the binary operation \cdot on K_4 given by the table below.

\cdot	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Show that K_4 is abelian, but not cyclic. (This group is the **Klein 4-group**, which you have already worked with in Example 3, Unit 2.)

Solution: From the table, you can see that the entries are symmetric about the diagonal containing all entries as e . Hence, K_4 is abelian.

If K_4 were cyclic, it would have to be generated by one of e, a, b or ab . Now, $\langle e \rangle = \{e\} \neq K_4$.

Also, from the table, you can see that $\langle a \rangle = \{e, a\} \neq K_4$.

Similarly, $\langle b \rangle = \{e, b\} \neq K_4$, and $\langle ab \rangle = \{e, ab\} \neq K_4$.

Therefore, K_4 can't be generated by e, a, b or ab .

Thus, K_4 is not cyclic.

Example 7: Show that \mathbb{Q} is not a cyclic group.

There are abelian groups which are not cyclic.



Fig.1: Felix Klein (1849-1925) defined the Klein 4-group in a research paper in 1884.

Solution: We shall prove this by contradiction. So, let us suppose that \mathbb{Q} is generated by $\frac{p}{q}$, where $(p, q) = 1, q \neq 0$.

Now $\frac{p}{q} + 1 \in \mathbb{Q}$. So $\exists n \in \mathbb{Z}$ s.t. $\frac{p}{q} + 1 = n \left(\frac{p}{q} \right)$, i.e., $(n-1)p = q$.

Since $(p, q) = 1$, from Theorem 6, Unit 1 you know that $q \mid (n-1)$, say $qr = n-1$, where $r \in \mathbb{Z}$.

Then $(n-1)p = q$ gives $pr = 1$.

This is only possible if $p = 1, r = 1$ or $p = -1, r = -1$. In either case, $\frac{p}{q} = \frac{1}{n-1}$.

Now consider $\frac{1}{3(n-1)} \in \mathbb{Q}$.

Since $\mathbb{Q} = \langle \frac{1}{n-1} \rangle$, $\exists m \in \mathbb{Z}$ s.t. $m \left(\frac{1}{n-1} \right) = \frac{1}{3(n-1)}$.

This gives $m = \frac{1}{3}$, which is not possible.

Hence, our assumption that \mathbb{Q} is cyclic must be wrong.

Thus, \mathbb{Q} is not cyclic.

So you have seen examples of finite, as well as infinite, abelian groups which are not cyclic. Try to solve the following exercises now.

E16) Is D_8 cyclic? Why, or why not?

E17) Prove that a non-abelian group must have a proper non-trivial subgroup.

Now let us look at another special property of cyclic groups. To understand this property, consider \mathbb{Z} . You know that $n\mathbb{Z} \leq \mathbb{Z} \forall n \in \mathbb{Z}$. The question is, what are the other subgroups of \mathbb{Z} ? The following theorem answers this.

Theorem 6: Any subgroup of a cyclic group is cyclic.

Further, if $G = \langle x \rangle$, and $H \leq G$, then $H = \{e\}$ or $H = \langle x^n \rangle$, where n is the least positive integer such that $x^n \in H$.

Proof: Let $G = \langle x \rangle$ be a cyclic group and H be a subgroup of G . If $H = \{e\}$, then $H = \langle e \rangle$, and hence, H is cyclic.

Suppose $H \neq \{e\}$. Then $\exists n \in \mathbb{Z}$ such that $x^n \in H, n \neq 0$.

Since H is a subgroup, $(x^n)^{-1} = x^{-n} \in H$. Therefore, there exists a positive integer m (i.e., n or $-n$) such that $x^m \in H$.

Thus, the set $S = \{t \in \mathbb{N} \mid x^t \in H\}$ is not empty.

Hence, by the well-ordering principle, S has a least element, say k .

We will show that $H = \langle x^k \rangle$.

Now, $\langle x^k \rangle \subseteq H$, since $x^k \in H$(9)

Conversely, let x^n be an arbitrary element in H . By the division algorithm, $n = mk + r$ for some $m, r \in \mathbb{Z}, 0 \leq r < k$.

So $x^r = x^{n-mk} = x^n \cdot (x^k)^{-m} \in H$, since $x^n, x^k \in H$.

But k is the least positive integer such that $x^k \in H$.

Therefore, x^r can be in H only if $r = 0$.

And then, $n = mk$, and $x^n = (x^k)^m \in \langle x^k \rangle$.

Thus, $H \subseteq \langle x^k \rangle$(10)

From (9) and (10), we conclude that $H = \langle x^k \rangle$, that is, H is cyclic. ■

Let us consider an example of the use of Theorem 6.

Example 8: Every non-trivial subgroup of \mathbb{Z} is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Hence, all the subgroups of \mathbb{Z} are known.

Solution: Let $H \leq \mathbb{Z}$, $H \neq \{0\}$.

Since $\mathbb{Z} = \langle 1 \rangle$, $H = \langle m \rangle = m\mathbb{Z}$, where m is the least positive integer in H , by Theorem 6.

Now, Theorem 6 says that every subgroup of a cyclic group is cyclic. Are you wondering if the converse is true? Well, there are groups whose proper subgroups are all cyclic, without the group being cyclic. You will see such examples in Unit 5, Block 2. Hence, the converse of Theorem 6 is not true.

Now, in Example 8 you have found that all the distinct subgroups of \mathbb{Z} are known. What about other cyclic groups? Well, it turns out that we know exactly how many subgroups a finite cyclic group has, and we can list them all! This is what the following theorem allows us to do.

Theorem 7: Let G be a finite cyclic group of order n . For every positive divisor m of n , G has a **unique** subgroup of order m . Further, these are the only subgroups of G .

Proof: Let $G = \langle g \rangle$, where $o(g) = n$. There are actually three statements to be proved here:

- i) if $m \mid n \exists H \leq G$ s.t. $o(H) = m$;
- ii) if $H \leq G, K \leq G$ s.t. $o(H) = o(K)$, then $H = K$; and
- iii) if $H \leq G$, then $o(H) \mid n$.

We shall first prove (i). So, let $n = mr$, and let $o(g^r) = s$. Then s is the least positive integer s.t. $(g^r)^s = e$, i.e., $g^{rs} = e$.

Since $o(g) = n$, Theorem 2 tells us that $n \mid rs$.

So $n \leq rs$, i.e., $mr \leq rs$, i.e.,

$$m \leq s. \quad \dots(11)$$

Now, $(g^r)^m = g^n = e$. So, again by Theorem 2 (ii), $s \mid m$, i.e.,

$$s \leq m. \quad \dots(12)$$

From (11) and (12), we find $s = m$.

Thus, $H = \langle g^r \rangle \leq G$ of order m , i.e., $H = \langle g^{\frac{n}{m}} \rangle$ is of order m .

Now let us prove (ii), i.e., the uniqueness part of the theorem.

Suppose $H = \langle g^r \rangle$ and $K = \langle g^t \rangle$ are both subgroups of G of order m , where $n = mr$.

Now $m = o(g^t) = \frac{n}{(n, t)} = \frac{mr}{(mr, t)}$. So, $r = (mr, t)$.

Thus, $r \mid t$, say $t = vr$, $v \in \mathbb{N}$.

So $g^t = (g^r)^v \in H$.

Thus, $K \subseteq H$.

But both these sets have the same number of elements, m .

Hence, $K = H$.

Now, for proving (iii), let $H \leq G$. Then, by Theorem 6, you know that

$H = \langle g^s \rangle$, where s is the least positive integer such that $g^s \in H$.

By the division algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $n = qs + r$, $0 \leq r < s$.

So $g^{n-qs} = g^r$.

Since $g^n = e$ and $g^s \in H$, $g^{-qs} \in H$.

Thus, $g^r \in H$. As $r < s$, this is only possible if $r = 0$. Then $n = qs$.

Now, as in the proof of (i) above, you can show that $o(H) = q$, and $q \mid n$. Thus,

H corresponds to the divisor q of n . ■

Now, suppose $G = \langle g \rangle$ is a cyclic group, and $H = \langle g^m \rangle$ and $K = \langle g^n \rangle$ are subgroups of G . When is $H \leq K$? This would happen iff $H \subseteq K$. So, what is the relationship, if any, between m and n ? You will actually find the answer to this in the proof of Theorem 8. However, first consider the following example.

Example 9: In Example 8 you have seen that any subgroup of \mathbb{Z} is of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$. Let $m\mathbb{Z}$ and $k\mathbb{Z}$ be two subgroups of \mathbb{Z} . Show that $m\mathbb{Z}$ is a subgroup of $k\mathbb{Z}$ if and only if $k \mid m$.

Solution: We need to show that $m\mathbb{Z} \subseteq k\mathbb{Z} \Leftrightarrow k \mid m$.

Now $m\mathbb{Z} \subseteq k\mathbb{Z} \Rightarrow m \in k\mathbb{Z} \Rightarrow m = kr$ for some $r \in \mathbb{Z}$
 $\Rightarrow k \mid m$.

Conversely, suppose $k \mid m$. Then, $m = kr$ for some $r \in \mathbb{Z}$.

Now consider any $n \in m\mathbb{Z}$, and let $t \in \mathbb{Z}$ such that $n = mt$.

So $n = mt = (kr)t = k(rt) \in k\mathbb{Z}$.

Since n was an arbitrary element of $m\mathbb{Z}$, this shows that $m\mathbb{Z} \subseteq k\mathbb{Z}$.

Thus, we have shown that $m\mathbb{Z} \leq k\mathbb{Z}$ iff $k \mid m$.

Generalising from Example 9, consider the following theorem, comprising three statements actually!

Theorem 8: Let $G = \langle g \rangle$, $H = \langle g^m \rangle$ and $K = \langle g^n \rangle$.

- i) $H \leq K$ iff $n \mid m$;
- ii) $H \cap K = \langle g^s \rangle$, where s is the l.c.m of m and n ;
- iii) $HK \leq G$ and $HK = \langle g^d \rangle$, where $d = (m, n)$.

[Note that if $+$ is the operation, then (iii) says $H + K = \langle d \rangle$, where $d = (m, n)$.]

Proof: We leave the proof of (i) to you (see E19).

ii) Since $H \cap K \leq G$, $H \cap K = \langle g^s \rangle$, for some $s \in \mathbb{N}$.

Since $H \cap K$ is a subgroup of both H and K , by (i) above, $m \mid s$ and $n \mid s$. Thus, s is a common multiple of m and n .

Now let t be any common multiple of m and n . Then, by (i), $\langle g^t \rangle \leq H$ and $\langle g^t \rangle \leq K$. Hence $\langle g^t \rangle \leq H \cap K = \langle g^s \rangle$.

$\therefore s \mid t$.

Hence, by definition of the l.c.m in Unit 1, s is the l.c.m of m, n .

iii) By Theorem 5, G is abelian. Hence, $HK \leq G$.

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

For $h \in H, k \in K, h = (g^m)^{m_1}$ and $k = (g^n)^{n_1}$ for some $m_1, n_1 \in \mathbb{Z}$.

So $hk = g^{mm_1+nn_1} = g^{dd_1}$ for some $d_1 \in \mathbb{Z}$, where $d = (m, n)$.

Thus, $HK \subseteq \langle g^d \rangle$(13)

Also, by Unit 1, you know that $d = mr + ns$ for some $r, s \in \mathbb{Z}$.

So $g^d = g^{mr+ns} = (g^m)^r \cdot (g^n)^s \in HK$.

Hence, $\langle g^d \rangle \subseteq HK$(14)

By (13) and (14), $HK = \langle g^d \rangle$. ■

Now consider an important remark related to a set operation that Theorem 8 is silent about.

Remark 3: Theorem 8 does not talk of $H \cup K$. In Unit 3, you have seen that

$H \cup K \leq G$ iff $H \subseteq K$ or $K \subseteq H$. Thus, in the context of Theorem 8,

$H \cup K \leq G$ iff $n \mid m$ or $m \mid n$, by Theorem 8(i). So, for example,

$\langle \bar{3} \rangle \cup \langle \bar{5} \rangle \not\leq \mathbb{Z}_{15}$. You should verify this.

Theorems 7 and 8 give us a complete picture of the subgroups of a finite cyclic group. Theorem 7 also tells us that the subgroup of order m , where $m \mid n$, is

$\langle g^{\frac{n}{m}} \rangle$. Let us apply this understanding now in some cases.

Example 10: Find all the subgroups of U_{12} , the group of the 12th roots of unity.

Solution: The positive divisors of 12 are 1, 2, 3, 4, 6, 12.

Let $U_{12} = \langle \zeta \rangle$, where ζ is of order 12, i.e., ζ is a primitive 12th root of unity.

Then $A_1 = \{1\} = \langle \zeta^{12} \rangle$ is of order 1.

Next, $A_2 = \langle \zeta^{\frac{12}{2}} \rangle = \langle \zeta^6 \rangle$ is of order 2. Similarly,

$A_3 = \langle \zeta^4 \rangle, A_4 = \langle \zeta^3 \rangle, A_5 = \langle \zeta^2 \rangle, A_6 = \langle \zeta \rangle = U_{12}$ are the subgroups of U_{12} of orders 3, 4, 6 and 12, respectively.

By Theorem 8, $A_1 \leq A_2 \leq A_4 \leq A_6$, and $A_1 \leq A_3 \leq A_5 \leq A_6$.

We show this relationship in a **subgroup diagram**, in Fig.2.

A generator of U_n is called a **primitive n th root of unity**.

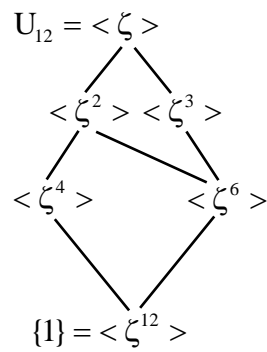


Fig.2: A subgroup diagram for U_{12} . Each line connecting a subgroup H below and K above it, shows that $H \leq K$.

Example 11: Find all the subgroups of \mathbb{Z}_{30} , and give a subgroup diagram for \mathbb{Z}_{30} .

Solution: Recall that $\mathbb{Z}_{30} = \langle \bar{1} \rangle$.

Now the positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30.

Thus, the subgroups of \mathbb{Z}_{30} of these orders are, respectively,

$$\langle \bar{30} \rangle = \{\bar{0}\},$$

$$\langle \bar{15} \rangle = \{\bar{0}, \bar{15}\},$$

$$\langle \bar{10} \rangle = \{\bar{0}, \bar{10}, \bar{20}\},$$

$$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}, \bar{24}\},$$

$$\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}\},$$

$$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \bar{21}, \bar{24}, \bar{27}\},$$

$$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}, \bar{24}, \bar{26}, \bar{28}\},$$

$$\langle \bar{1} \rangle = \mathbb{Z}_{30}.$$

Consider the diagrammatic representation of the subgroup structure of \mathbb{Z}_{30} , given in Fig.3. This shows, for example, that $\langle \bar{6} \rangle \leq \langle \bar{3} \rangle$ and $\langle \bar{6} \rangle \leq \langle \bar{2} \rangle$.

Similarly, $\langle \bar{30} \rangle \leq \langle \bar{15} \rangle$, which is a subgroup of both $\langle \bar{3} \rangle$ and $\langle \bar{5} \rangle$.

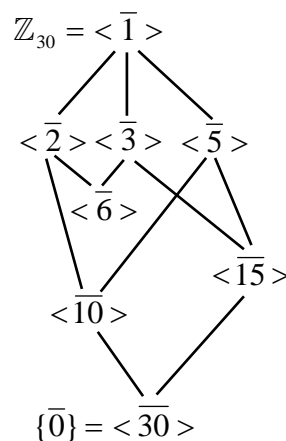


Fig.3: Subgroup diagram for \mathbb{Z}_{30} .

Example 12: Find $\langle 15 \rangle + \langle 18 \rangle$ and $\langle 15 \rangle \cap \langle 18 \rangle$ in \mathbb{Z} .

Solution: From Theorem 8(iii), $\langle 15 \rangle + \langle 18 \rangle = \langle d \rangle$, where $d = (15, 18) = 3$.

So $\langle 15 \rangle + \langle 18 \rangle = \langle 3 \rangle$.

Similarly, by Theorem 8(ii), $\langle 15 \rangle \cap \langle 18 \rangle = \langle s \rangle$, where $s = \text{l.c.m of } 15, 18 = 90$.

Thus, $\langle 15 \rangle \cap \langle 18 \rangle = \langle 90 \rangle$.

Now, why don't you try the following exercises?

E18) Which subgroups of \mathbb{Z} is $9\mathbb{Z}$ a subgroup of? Give reasons for your answer.

E19) i) If $G = \langle g \rangle$ is finite, $H = \langle g^m \rangle$, $K = \langle g^r \rangle$, for $m, r \in \mathbb{Z}$, under what conditions on m and r is $H \leq K$? Give reasons for your answer.

ii) If $G = \langle g \rangle$ is infinite, $H = \langle g^m \rangle$, $K = \langle g^n \rangle$, for some $m, n \in \mathbb{Z}$, prove that $H \leq K$ iff $n \mid m$.

E20) Give the subgroup diagram of \mathbb{Z}_{12} . Compare its structure with that of U_{12} in Fig.2. What do you conclude?

E21) Find all the subgroups of \mathbb{Z}_{25} , and give the corresponding subgroup diagram.

E22) Show that \mathbb{Z}_p has no proper non-trivial subgroup, where p is a prime.

E23) Find all the subgroups of \mathbb{Z}_n , $n \geq 2$.

E24) Find generators of $\langle \bar{4} \rangle + \langle \bar{6} \rangle$ and $\langle \bar{4} \rangle \cap \langle \bar{6} \rangle$ in \mathbb{Z}_{30} .

E25) Find a generator each of HK and $H \cap K$, where

$$H = \langle \zeta^8 \rangle, K = \langle \zeta^{10} \rangle \text{ in } U_{12}.$$

E26) Let G be a cyclic group. Can G be the union of its proper subgroups? Give reasons for your answers.

Let us now go back to the point made in Corollary 1(ii). You can see that the number of different generators of $\langle g \rangle$, where $o(g) = n$, is the number of elements of $\langle g \rangle$ of order n . By Corollary 1, this is the number of positive integers less than n and relatively prime to n . This number is given by the Euler phi-function, named after the famous Swiss mathematician, Leonhard Euler (pronounced *oiler*). (You have already met him in an earlier unit!).

Definition: The **Euler phi-function** $\phi: \mathbb{N} \rightarrow \mathbb{N}$ is defined as follows:

$\phi(1) = 1$, and



Fig.4: Leonhard Euler
(1707-1783)

$\phi(n)$ = the number of natural numbers less than n and relatively prime to n , for $n \geq 2$.

For example, $\phi(2) = 1$ and $\phi(6) = 2$ (since the only positive integers less than 6 and relatively prime to 6 are 1 and 5).

So, the number of distinct generators that the finite group $\langle g \rangle$ has is $\phi(n)$, where $n = o(g)$.

Now, this leads us to another question: how many elements of order d does $\langle g \rangle$ have, for each positive divisor d of $n = o(g)$?

You know that the only element of order 1 is e , and you know that the number of elements in G of order n is $\phi(n)$. What about the other divisors of n ? Consider the following result.

Theorem 9: Let $G = \langle g \rangle$ be of order n , and let d be a positive divisor of n . Then the number of elements of G of order d is $\phi(d)$.

Proof: In Theorem 7, you have seen why $g^{\frac{n}{d}}$ is of order d . Let $\frac{n}{d} = m$, and let $g^m = a$. Consider the unique subgroup $H = \langle a \rangle$ of G of order d . From Theorem 7, and the discussion above, you know that the number of distinct generators of H is $\phi(d)$.

Hence, the number of distinct elements of G of order d is $\phi(d)$. ■

Let us consider an example of what Theorem 9 tells us.

Example 13: How many elements of order 2 and of order 5 do \mathbb{Z}_{50} , U_{17} and U_{25} have? Can you find the elements, if they exist?

Solution: Note that $o(\mathbb{Z}_{50}) = 50$, $o(U_{17}) = 17$, $o(U_{25}) = 25$.

Since $2 \mid 50$ and $5 \mid 50$, \mathbb{Z}_{50} has $\phi(2) = 1$ and $\phi(5) = 4$ elements of order 2 and 5, respectively. Note that $\phi(5) = 4$, since 5 is a prime, and hence, is relatively prime to each of 1, 2, 3, 4.

The element of order 2 in \mathbb{Z}_{50} is $\overline{25}$.

The elements of order 5 in \mathbb{Z}_{50} are $m \cdot \overline{10}$, where $(m, 5) = 1$.

These are $\overline{10}$, $\overline{20}$, $\overline{30}$, $\overline{40}$, corresponding to $m = 1, 2, 3, 4$, respectively.

Next, since U_{17} is of order 17 and $2 \nmid 17$, $5 \nmid 17$, U_{17} has no element of order 2 or of order 5.

Finally, since $2 \nmid 25$, U_{25} has no element of order 2. Since $5 \mid 25$, U_{25} has $\phi(5) = 4$ elements of order 5.

These are ζ^{5m} , where $(m, 5) = 1$, i.e., ζ^5 , ζ^{10} , ζ^{15} , ζ^{20} , where ζ is a primitive 25th root of unity.

Try solving the following exercises now.

E27) Show that

- i) $\phi(p) = p - 1$, for any prime p ,
- ii) $n = \sum_{d|n} \phi(d)$, (**Hint:** Use Theorem 7.)
- iii) $\phi(mn) \neq \phi(m)\phi(n)$, in general. (In Unit 8 you will see that $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$, for $m, n \in \mathbb{N}$.)

E28) Find all the distinct generators of $\langle \overline{25} \rangle$ in \mathbb{Z}_{30} , and of $\langle \zeta^3 \rangle$ in U_{10} .

So far, you have spent quite some study time on subgroups of finite cyclic groups. What do we know about the subgroups of infinite cyclic groups, apart from the fact that they are also cyclic? Let's see.

Theorem 10: Let $G = \langle g \rangle$ be an infinite cyclic group, and $x \in G$, $x \neq e$. Then $\langle x \rangle$ is also an infinite cyclic group.

Proof: Firstly, by Theorem 6, you know that $x = g^n$ for some $n \in \mathbb{N}$. So, by Theorem 4(i), $o(x)$ is infinite. Thus, $\langle x \rangle = \langle g^n \rangle$ is infinite. ■

Let us consider \mathbb{Z} . You know that this is an infinite cyclic group generated by 1 or (-1) . Can \mathbb{Z} be generated by any other element? Think about this while studying the following example.

Example 14: Show that if $\langle g \rangle$ is infinite and $\langle g^n \rangle = \langle g \rangle$ for some $n \in \mathbb{Z}$, then $n = 1$ or -1 .

Solution: By E3, you know that for any cyclic group $\langle g \rangle$, $\langle g \rangle = \langle g^{-1} \rangle$.

Now, let $\langle g^n \rangle = \langle g \rangle$, where g is of infinite order. Then $g \in \langle g^n \rangle$. So

$\exists m \in \mathbb{Z}$ s.t. $g^{nm} = g$. Then, by Theorem 2, $nm = 1$.

Since $n, m \in \mathbb{Z}$, this is possible only when $n = 1$ or -1 .

From Example 14, you can see that $\mathbb{Z} = \langle 1 \rangle$ or $\mathbb{Z} = \langle -1 \rangle$, and these are the only possible generators of \mathbb{Z} .

Try doing some exercises now.

E29) Is the cyclic subgroup $\langle 1 \rangle$, of the group \mathbb{C}^* of non-zero complex numbers, infinite? Why?

E30) Which of the following statements is true? Give reasons for your answers.

- i) If H is an infinite cyclic group, and a group G contains H , then G is cyclic.
- ii) An infinite cyclic group has only one finite subgroup.
- iii) There is an infinite cyclic group which has 4 distinct generators.

Now, let us go back to Example 6 for a moment. You noted that K_4 is not a cyclic group. However, it does have a set of generators, as you will now see.

4.4 SET OF GENERATORS

In the previous section, you saw that if g is an element of a group G , then $\langle g \rangle$ is the smallest subgroup of G containing g . Let us see if this idea can be extended to a set of two elements of G .

Let $S = \{a, b\}$ be a subset of a group G . Let $H \leq G$ s.t. $S \subseteq H$. Then $\{a^m \mid m \in \mathbb{Z}\}$ and $\{b^n \mid n \in \mathbb{Z}\}$ will be subsets of H . Also, elements of the form $a^2 b^3 a^{-3} b^7$ will be in H . (Note that we can't write $a^2 b^3 a^{-3} b^7$ as $a^{-1} b^{10}$ since H may not be abelian.)

Now suppose $K \leq G$ s.t. $S \subseteq K$. Then, as above, $\{a^m \mid m \in \mathbb{Z}\} \subseteq K$, $\{b^n \mid n \in \mathbb{Z}\} \subseteq K$, and products of the kind $b a b a^2$ are also in K .

Hence, all these sets and elements lie in $H \cap K$. In fact, they lie in the intersection of all the subgroups of G containing S , which is also a subgroup of G containing S . This leads us to the following definition.

Definition: Let G be a group. The **subgroup of G generated by $S = \{a, b\}$** is the smallest subgroup of G containing S . This subgroup is denoted by $\langle a, b \rangle$, or by $\langle S \rangle$.

In fact, $\langle S \rangle$ is the intersection of all subgroups of G containing S .

For example, D_6 is generated by $\{r, R_{120}\}$, where $r^2 = I$, $R_{120}^3 = I$ and $r \circ R_{120} = R_{120}^{-1} \circ r$.

As another example, K_4 (in Example 6) is generated by $\{a, b\}$.

Let us generalise what you have just seen for $S = \{a, b\}$ to any non-empty set S .

Let G be a group and S be a non-empty subset of G .

Consider the family \mathcal{F} , of all subgroups of G that contain S , that is,

$$\mathcal{F} = \{H \mid H \leq G \text{ and } S \subseteq H\}.$$

We claim that $\mathcal{F} \neq \emptyset$. Why? Doesn't $G \in \mathcal{F}$?

Next, by Theorem 6 of Unit 3, $\bigcap_{H \in \mathcal{F}} H$ is a subgroup of G .

Note that

$$i) \quad S \subseteq \bigcap_{H \in \mathcal{F}} H,$$

ii) $\bigcap_{H \in \mathcal{F}} H$ is the smallest subgroup of G containing S . (Because if K is a subgroup of G containing S , then $K \in \mathcal{F}$. Therefore, $\bigcap_{H \in \mathcal{F}} H \subseteq K$.)

These observations lead us to the following definitions.

Definitions: Let S be a non-empty subset of a group G .

- i) The smallest subgroup of G containing S is called the **subgroup generated by the set S** , and is denoted by $\langle S \rangle$.
Thus, $\langle S \rangle = \bigcap \{H \mid H \leq G, S \subseteq H\}$.
- ii) If $\langle S \rangle = G$, then we say that G is **generated by the set S** , and that S is a **set of generators of G** , or a **generating set of G** .
- iii) If the set S is finite, we say that $\langle S \rangle$ is **finitely generated**.

For example, a cyclic group $\langle g \rangle$ is a finitely generated group, as is $\langle a, b \rangle$.

Note that if $\{a, b\}$ generates $\langle a, b \rangle$, then $\{a, b, ab\}$ also generates $\langle a, b \rangle$ as $ab \in \langle a, b \rangle$. So **the generating set of a subgroup is not unique**.

Before giving more examples, we will give an alternative way of describing $\langle S \rangle$. This theorem makes it much easier, than the definition, to obtain $\langle S \rangle$.

Theorem 11: If S is a non-empty subset of a group G , then

$$\langle S \rangle = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in S \text{ and } n_i \in \mathbb{Z} \text{ for } 1 \leq i \leq k, k \in \mathbb{N}\}.$$

Note that in Theorem 11 the a_i are not necessarily distinct, since G may not be abelian.

Proof: Let $A = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in S \text{ and } n_i \in \mathbb{Z} \text{ for } 1 \leq i \leq k\}$.

Since $a_1, \dots, a_k \in S \subseteq \langle S \rangle$, and $\langle S \rangle$ is a subgroup of G , $a_i^{n_i} \in \langle S \rangle$

$\forall i = 1, \dots, k$. Therefore, $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \in \langle S \rangle$,

i.e., $A \subseteq \langle S \rangle$(15)

Now, let us see why $\langle S \rangle \subseteq A$. We will show that A is a subgroup containing S . Then, by the definition of $\langle S \rangle$, it will follow that $\langle S \rangle \subseteq A$.

Since any $a \in S$ can be written as $a = a^1$, $S \subseteq A$.

Since $S \neq \emptyset$, $A \neq \emptyset$.

Now let $x, y \in A$. Then $x = a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$, $y = b_1^{m_1} b_2^{m_2} \dots b_r^{m_r}$, $a_i, b_j \in S$ and $n_i, m_j \in \mathbb{Z}$ for $1 \leq i \leq k, 1 \leq j \leq r$.

$$\begin{aligned} \text{Then } xy^{-1} &= (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}) (b_1^{m_1} b_2^{m_2} \dots b_r^{m_r})^{-1} \\ &= (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}) (b_r^{-m_r} \dots b_1^{-m_1}) \in A, \text{ by definition.} \end{aligned}$$

Thus, by Theorem 2, Unit 3, A is a subgroup of G .

Thus, A is a subgroup of G containing S .

Hence, $\langle S \rangle \subseteq A$(16)

From (15) and (16), $\langle S \rangle = A$. ■

Note that if $(G, +)$ is a group generated by S , then any element of G is of the form $n_1 a_1 + n_2 a_2 + \dots + n_r a_r$, where $a_1, a_2, \dots, a_r \in S$ and $n_1, n_2, \dots, n_r \in \mathbb{Z}$.

Here the a_i can be taken as distinct since G is abelian.

Let us consider an example.

Example 15: You know that \mathbb{Z} is generated by $\{1\}$, or by $\{-1\}$. Show that \mathbb{Z} is also generated by the set of odd integers $S = \{\pm 1, \pm 3, \pm 5, \dots\}$.

Solution: Let $m \in \mathbb{Z}$. Then $m = 2^r s$ where $r \geq 0$ and $s \in S$. Thus, $m \in \langle S \rangle$.

So $\mathbb{Z} \subseteq \langle S \rangle$.

Of course, $\langle S \rangle \subseteq \mathbb{Z}$, since $S \subseteq \mathbb{Z}$.

Thus, $\langle S \rangle = \mathbb{Z}$.

From Example 15, you can see that a cyclic group $\langle g \rangle$ can be generated by a much bigger set too. Thus, $\langle g \rangle = \langle g, g^2, g^3 \rangle$, for example, since $g^2, g^3 \in \langle g \rangle$.

A remark about notation, here.

Remark 4: If $G = \langle S \rangle$, and $S = \{a_1, a_2, \dots, a_n\}$ is finite, we usually write $G = \langle a_1, a_2, \dots, a_n \rangle$, leaving out the curly brackets.

Try solving the following exercises now.

E31) Show that a subset S of \mathbb{N} generates \mathbb{Z} iff there exist s_1, \dots, s_k in S and n_1, \dots, n_k in \mathbb{Z} such that $n_1s_1 + \dots + n_ks_k = 1$.

E32) Show that if S generates a group G and $S \subseteq T \subseteq G$, then T also generates G .

E33) Show that $D_{2n} = \langle r, R \rangle$, where r is a reflection and $R = R_\theta$, where $\theta = \frac{360}{n}$, as discussed in Sec.2.4.3, Unit 2.

E34) If $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$, show that $G_1 \times G_2$ is not always cyclic. Also find a generating set for $G_1 \times G_2$. (This is linked with E27(iii).)

In Unit 8 you will see that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if $(m, n) = 1$.

In Unit 9, you will see that S_n is also finitely generated $\forall n \in \mathbb{N}$.

With this we come to the end of our discussion on generators. We also end this unit here. Let us now summarise what you have studied in it.

4.5 SUMMARY

In this unit, we have discussed the following points.

1. The order of an element x of a group G , $o(x)$, is the order of the cyclic subgroup $\langle x \rangle$ of G .
2. If $o(x)$ is finite, then $o(x)$ is the least positive integer n s.t. $x^n = e$.
3. If $o(x) = n$ and $x^s = e$ for some $s \in \mathbb{Z}$, then $n \mid s$.
4. If $o(x)$ is infinite, then $x^m \neq x^n$ if $m \neq n$, $\forall m, n \in \mathbb{Z}$.
5. $o(g) = o(xgx^{-1}) \forall x, g \in G$, where G is a group.

6. Let G be a group, and $g \in G$.
- If g is of infinite order, then g^m is also of infinite order for every $m \in \mathbb{Z}^*$.
 - If $o(g) = n$, then $o(g^m) = \frac{n}{(n, m)} \forall m = 1, \dots, n-1$.
7. Examples of finite and infinite cyclic groups.
8. Every cyclic group is abelian.
9. Every subgroup of a cyclic group is cyclic.
10. Let G be a finite cyclic group of order n . For every positive divisor m of n , G has a unique subgroup of order m . Further, these are the only subgroups of G .
11. Let $G = \langle g \rangle$ and let $H = \langle g^m \rangle$ and $K = \langle g^n \rangle$.
- $H \leq K$ iff $n \mid m$,
 - $H \cap K = \langle g^s \rangle$, where s is the l.c.m of m and n ,
 - $HK \leq G$ and $HK = \langle g^d \rangle$, where $d = (m, n)$.
[Note that if $+$ is the operation, then (iii) says that $H + K = \langle d \rangle$, where $d = (m, n)$.]
12. Let $G = \langle g \rangle$ be of order n , and let d be a positive divisor of n . Then the number of elements of G of order d is $\phi(d)$, where ϕ is the Euler phi-function.
13. The definition, and examples, of a subgroup of a group G generated by $S \subseteq G$, $S \neq \emptyset$. This is denoted by $\langle S \rangle$.
14. If $G = \langle S \rangle$, then $G = \langle T \rangle$ for any $T \supseteq S$. In particular, $G = \langle G \rangle$.
15. The direct product of cyclic groups need not be cyclic.

4.6 SOLUTIONS / ANSWERS

E1) i) $R_{90} \neq I$, $R_{90}^2 = R_{180} \neq I$, $R_{90}^3 = R_{270} \neq I$, $R_{90}^4 = R_{360} = I$.
 $R_{180} \neq I$, $R_{180}^2 = R_{360} = I$.
 Thus, $o(R_{90}) = 4$, $o(R_{180}) = 2$.

ii) Here $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \neq I$, $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I$,
 $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq I$, $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.
 Thus, $o(A) = 4$.

iii) Verify that $n \cdot \bar{1} \neq \bar{0}$ for $n \in \{1, 2, \dots, 9\}$ and $10 \cdot \bar{1} = \overline{10} = \bar{0}$.

Thus, $o(\bar{1}) = 10$.

Note that $\mathbb{Z}_{10} = \langle \bar{1} \rangle$.

iv) For any m , $0 < m < n-1$, $\bar{m} \in \mathbb{Z}_n$, and $\bar{m} = m \cdot \bar{1} \neq \bar{0}$, since $n \nmid m$.
Next, $\bar{n} = n \cdot \bar{1} = \bar{0}$. Thus, $o(\bar{1}) = n$.

v) Since $n(-5) \neq 0 \forall n \in \mathbb{N}$, $o(-5)$ is infinite.

vi) Let $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$. Then $nA = \begin{bmatrix} 2n & 3n \\ 4n & 5n \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \forall n \in \mathbb{N}$.

Hence, $o(A)$ is infinite.

E2) Since $H \neq \{e\}$, $\exists a \neq e$ in H . Since $a \neq e$, $a \neq e^r$ for any $r \in \mathbb{Z}$.
 $\therefore a \notin \langle e \rangle$. $\therefore H \neq \langle e \rangle$.

E3) We will show that $\langle a \rangle \subseteq \langle a^{-1} \rangle$ and $\langle a^{-1} \rangle \subseteq \langle a \rangle$.

Now, any element of $\langle a \rangle$ is $a^n = (a^{-1})^{-n}$, for $n \in \mathbb{Z}$.

$\therefore a^n \in \langle a^{-1} \rangle$. $\therefore \langle a \rangle \subseteq \langle a^{-1} \rangle$.

Similarly, you should show that $\langle a^{-1} \rangle \subseteq \langle a \rangle$.

$\therefore \langle a \rangle = \langle a^{-1} \rangle$.

E4) Let $H \leq G$ s.t. $a \in H$. Then, $\langle a \rangle \subseteq H$, by Theorem 1.

Thus, $\langle a \rangle \subseteq \cap \{H \mid H \leq G \text{ and } a \in H\}$.

Also $\langle a \rangle \leq G$ s.t. $a \in \langle a \rangle$.

So $\cap \{H \mid H \leq G \text{ and } a \in H\} \subseteq \langle a \rangle$.

Hence, $\langle a \rangle = \cap \{H \mid H \leq G \text{ and } a \in H\}$.

E5) From E1(iv), you know that $o(\bar{1}) = n$.

So $\langle \bar{1} \rangle \leq \mathbb{Z}_n$ and both have the same order. Hence, $\mathbb{Z}_n = \langle \bar{1} \rangle$.

E6) Since $A \neq \mathbf{0}$, $a_{ij} \neq 0$ for some $i=1, 2, j=1, 2, 3$.

Then $na_{ij} \neq 0 \forall n \in \mathbb{N}$.

Hence, $nA \neq \mathbf{0} \forall n \in \mathbb{N}$.

Thus, $o(A)$ is infinite.

E7) $A \neq I$, $A^2 = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} = I$ if $r=1$. So $o(A) = 2$ if $r=1$.

Now, suppose $r \neq 1$.

In general, you should verify that $A^{2n+1} \neq I \forall n \in \mathbb{N}$, and $A^{2n} = \begin{bmatrix} r^n & 0 \\ 0 & r^n \end{bmatrix}$.

Thus, if r is a real n th root of unity, then $o(A) = 2n$. Otherwise, $o(A)$ is infinite.

E8) Here ϕ is the identity element.

If $A = \phi$, $o(A) = 1$.

If $A \neq \phi$, $A \Delta A = \phi$. Hence, $o(A) = 2$.

E9) i) Let $d = (n, m)$. Then $d \mid n$ and $d \mid m$.

By Theorem 4, $o(g^m) = \frac{n}{d}$.

Also $o(g^{(n,m)}) = o(g^d) = \frac{n}{(n,d)} = \frac{n}{d}$, since $d \mid n$.

Hence, $o(g^m) = o(g^{(n,m)})$.

ii) $G = \langle g^m \rangle$ iff $o(g^m) = n$ iff $(m, n) = 1$, by Theorem 4(ii).

E10) $o(\bar{1}) = 18$ in \mathbb{Z}_{18} . So,

$$o(\bar{2}) = o(2 \cdot \bar{1}) = \frac{18}{(18, 2)} = 9.$$

$$o(\bar{4}) = \frac{18}{(18, 4)} = \frac{18}{2} = 9. \text{ (Note that } \bar{4} = 2 \cdot \bar{2}, \text{ but } o(\bar{4}) = o(\bar{2}).)$$

$$\text{Also, } o(\bar{5}) = \frac{18}{(18, 5)} = \frac{18}{1} = 18. \text{ (Thus, } \mathbb{Z}_{18} = \langle \bar{5} \rangle \text{ also.)}$$

E11) Let $G = \langle g \rangle$, where $o(g) = n$. Let $x \in G$. Then $x = g^m$ for some m , $0 \leq m < n$.

If $x = e$, then $o(x) = 1$ and $1 \mid n$.

If $x \neq e$, then $o(x) = o(g^m) = \frac{n}{(n, m)}$. Hence, $o(x) \mid n$. Let $o(x) = r$.

Since $r \mid n$, let $n = rs$.

$$\text{Then } x^{o(G)} = x^n = x^{rs} = (x^r)^s = e.$$

E12) Since $o(\zeta) = 10$, $o(\zeta^3) = \frac{10}{(10, 3)} = 10$.

E13) $o(x^2) = \frac{15}{(15, 2)} = 15$, $o(x^6) = \frac{15}{(15, 6)} = \frac{15}{3} = 5$, $o(x^{10}) = \frac{15}{(15, 10)} = 3$.

E14) $o(x) = n$. So $x^m \cdot x^{n-m} = x^n = e$.

$$\text{Thus, } (x^m)^{-1} = x^{n-m}.$$

Hence, by E3, $\langle x^m \rangle = \langle x^{n-m} \rangle$.

Hence, $o(x^m) = o(x^{n-m})$, that is, $\frac{n}{(n, m)} = \frac{n}{(n, n-m)}$.

Hence, $(n, m) = (n, n-m)$.

E15) Since $(30, 25) = (30, 5)$, from E14, $\langle \bar{25} \rangle = \langle \bar{5} \rangle$. Hence,

$$\langle \bar{25} \rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}\}.$$

$$\langle \zeta^7 \rangle = \langle \zeta \rangle = U_{10}, \text{ since } (7, 10) = 1.$$

E16) Since D_8 is not abelian, it cannot be cyclic.

E17) Let G be a non-abelian group. Then $G \neq \{e\}$.

Let $g \in G, g \neq e$. Then $\langle g \rangle \leq G, \langle g \rangle \neq \{e\}$. Also $G \neq \langle g \rangle$, since G is non-abelian.

Hence, $\langle g \rangle$ is a proper non-trivial subgroup of G .

E18) From Example 9, $9\mathbb{Z} \leq m\mathbb{Z}$ iff $m \mid 9$, i.e., $m = 1, 3, 9$.

Thus, $9\mathbb{Z}$ is a subgroup of only $\mathbb{Z}, 3\mathbb{Z}$ and $9\mathbb{Z}$.

E19) i) We will prove that $H \leq K$ iff $r \mid m$.

First, if $H \leq K$, then $g^m \in \langle g^r \rangle = K$.

By the division algorithm, $m = qr + r'$ for some $q, r' \in \mathbb{Z}, 0 \leq r' < r$.

So $g^m \cdot (g^r)^{-q} \in K$, i.e., $g^{r'} \in K$.

But, by Theorem 6, r is the least positive integer s.t. $g^r \in K$.

Hence, $r' = 0$, i.e., $m = qr$, i.e., $r \mid m$.

Conversely, if $r \mid m$, then $m = rs$ for some $s \in \mathbb{Z}$.

So $g^m = (g^r)^s \in K$. Hence, $H \subseteq K$, i.e., $H \leq K$, by E10, Unit 3.

ii) As in Example 9, show that if $H \leq K, n \mid m$.

Then show that if $n \mid m, H \leq K$.

E20) The subgroups of \mathbb{Z}_{12} are

$\{\bar{0}\} = \langle \bar{12} \rangle, \langle \bar{6} \rangle, \langle \bar{4} \rangle, \langle \bar{3} \rangle, \langle \bar{2} \rangle, \langle \bar{1} \rangle = \mathbb{Z}_{12}$.

The diagram is as in Fig.5 below. It is structurally the same as the diagram in Fig.2, where $\langle \zeta^i \rangle$ is replaced by $\langle \bar{i} \rangle$.

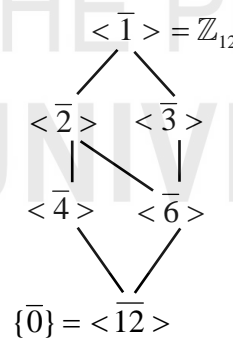


Fig.5: A subgroup diagram for \mathbb{Z}_{12} .

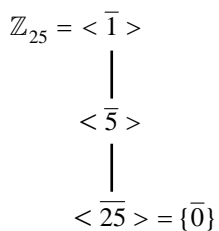


Fig.6: A subgroup diagram for \mathbb{Z}_{25} .

E21) The positive divisors of 25 are 1, 5, 25. Hence, the subgroups of \mathbb{Z}_{25} are $\langle \bar{1} \rangle, \langle \bar{5} \rangle, \langle \bar{25} \rangle$.

The corresponding diagram is given in Fig.6.

E22) $\mathbb{Z}_p = \langle \bar{1} \rangle$, where $\bar{1}$ is the congruence class of 1(mod p).

So $o(\mathbb{Z}_p) = p$. Since the only divisors of p are 1 and p , by Theorem 7 the only subgroups of \mathbb{Z}_p are $\langle \bar{1} \rangle$ and $\langle \bar{p} \rangle = \langle \bar{0} \rangle$.

Hence, \mathbb{Z}_p has no non-trivial proper subgroup.

E23) By Theorem 6, any subgroup H is of the form $\langle \bar{m} \rangle$, where m is the least positive integer s.t. $\bar{m} \in H$.

Further, by Theorem 7, if m_1, m_2, \dots, m_r are the positive divisors of n , then the subgroups are H_1, H_2, \dots, H_r , where $H_i = \langle \overline{\frac{n}{m_i}} \rangle$.

E24) $\mathbb{Z}_{30} = \langle \bar{1} \rangle$, where $o(\bar{1}) = 30$.

The l.c.m of $\bar{4}$ and $\bar{6}$ in \mathbb{Z}_{30} is $\bar{12}$ and $(\bar{4}, \bar{6}) = \bar{2}$.

So $\langle \bar{4} \rangle \cap \langle \bar{6} \rangle = \langle \bar{12} \rangle$ and $\langle \bar{4} \rangle + \langle \bar{6} \rangle = \langle \bar{2} \rangle$.

E25) $HK = \langle \zeta^8 \rangle \langle \zeta^{10} \rangle = \langle \zeta^d \rangle$, where $d = (8, 10) = 2$.

$H \cap K = \langle \zeta^\ell \rangle$, where $\ell = \text{l.c.m of } 8, 10 = 40$.

Now $\zeta^{40} = \zeta^4$ in U_{12} . So

$H \cap K = \langle \zeta^4 \rangle$.

E26) From Unit 3, you know that if A and B are subgroups of G then

$A \cup B \leq G$ iff $A \subseteq B$ or $B \subseteq A$.

Thus, whenever the union of proper subgroups is a subgroup, it can only be a proper subgroup. Hence, it can never be G .

E27) i) For any prime $p, (m, p) = 1 \forall m$ s.t. $1 \leq m < p$, by the Fundamental Theorem of Arithmetic. Hence, $\phi(p) = p - 1$.

ii) By Theorem 7, for each $d | n, \langle g^{n/d} \rangle$ is a unique subgroup of order d of $\langle g \rangle$, where $o(g) = n$.

Also, the number of generators of $\langle g^{n/d} \rangle$ is $\phi(d)$.

Further, for each i s.t. $1 \leq i \leq n, o(g^i) = d$ for some $d | n$.

Hence, $n = \sum_{d|n} \phi(d)$.

iii) $\phi(4) = 2$, since 1 and 3 are relatively prime to 4.

Also $\phi(2) = 1$.

Hence, $\phi(4) = \phi(2 \times 2) \neq \phi(2)\phi(2)$.

E28) Since $\langle \overline{25} \rangle = \langle \bar{5} \rangle$, $o(\overline{25}) = 6$.

The number of elements in \mathbb{Z}_{30} of order 6 is $\phi(6) = 2$.

These are $1 \cdot \overline{25}$ and $5 \cdot \overline{25}$, i.e., $\overline{25}$ and $\bar{5}$.

$o(\zeta^3) = 10$, since $(3, 10) = 1$.

$\phi(10) = 4$, the numbers being 1, 3, 7, 9.

Thus, the distinct generators of $\langle \zeta^3 \rangle$ are $\zeta, \zeta^3, \zeta^7, \zeta^9$.

E29) $\langle 1 \rangle = \{1\}$, since $1^n = 1 \forall n \in \mathbb{Z}$.

Hence, $\langle 1 \rangle$ is finite.

E30) i) False. E.g., $\mathbb{Z} \leq \mathbb{Q}$, but \mathbb{Q} is not cyclic, as you have seen in Example 7.

ii) True. By Theorem 10, $\{e\}$ is the only finite subgroup.

iii) False, see Example 14.

E31) First suppose $\mathbb{Z} = \langle S \rangle$.

Since $1 \in \mathbb{Z}$, $\exists n_1, \dots, n_k \in \mathbb{Z}$ and $s_1, \dots, s_k \in S$ s.t. $1 = \sum_{i=1}^k n_i s_i$.

Conversely, let $1 = n_1 s_1 + \dots + n_k s_k$, $n_i \in \mathbb{Z}$, $s_i \in S$.

Then for any $m \in \mathbb{Z}$, $m = m \cdot 1 = m(n_1 s_1 + \dots + n_k s_k) \in \langle S \rangle$.

So $\mathbb{Z} \subseteq \langle S \rangle$.

Since $S \subseteq \mathbb{Z}$, $\langle S \rangle \subseteq \mathbb{Z}$.

Thus, $\mathbb{Z} = \langle S \rangle$.

E32) $G = \langle S \rangle$ and $S \subseteq T$. So $G = \langle S \rangle \subseteq \langle T \rangle \leq G$.

Hence, $G = \langle T \rangle$.

E33) From Unit 2, you know that any element of D_{2n} is of the form R^i or

rR^i , $i = 0, 1, \dots, n-1$. Hence, $D_{2n} \subseteq \langle r, R \rangle \subseteq D_{2n}$.

Thus, $D_{2n} = \langle r, R \rangle$.

E34) Consider $\mathbb{Z} \times \mathbb{Z}$. If it were cyclic, with a generator (x, y) , then

$(1, 0) = (mx, my)$ and $(0, 1) = (nx, ny)$ for some $m, n \in \mathbb{Z}$. So

$mx = 1$, $my = 0$, $nx = 0$, $ny = 1$.

$my = 0 \Rightarrow m = 0$ or $y = 0$. But then $mx = 1$ and $ny = 1$ is not possible.

We reach a contradiction.

Hence, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Any element of $G_1 \times G_2$ is of the form

$(g_1^{n_1}, g_2^{n_2}) = (g_1^{n_1}, e_2)(e_1, g_2^{n_2}) = (g_1, e_2)^{n_1}(e_1, g_2)^{n_2}$, $n_1, n_2 \in \mathbb{Z}$, where e_1 and e_2 are the identities of G_1 and G_2 , respectively.

Hence, $G_1 \times G_2 = \langle (g_1, e_2), (e_1, g_2) \rangle$.

MISCELLANEOUS EXAMPLES AND EXERCISES

"A miscellany is a collection with a natural ordering relation."

J. E. Littlewood
British mathematician

The few examples and exercises, given below cover the concepts and processes you have studied in this block. Studying the examples, and solving the exercises, will give you a better understanding of the concepts concerned. This will also give you more practice in solving such problems.

Example 1: Which of the following statements are true? Give reasons for your answers.

- i) The domain of a binary operation on a set S is S .
- ii) If (G, \cdot) is an abelian group, then $x^2 = e \forall x \in G$.
- iii) If $n, m \in \mathbb{N}$, then $n, m = nm$.

Solution: i) False. The domain is $S \times S$.

ii) False. For instance, \mathbb{Z} is abelian, but $2n \neq 0 \forall n \neq 0$.

iii) True. Here we use the unique factorisation theorem.

Let $n = p_1^{n_1} \dots p_r^{n_r}$ and $m = p_1^{m_1} \dots p_r^{m_r}$, where $n_i \geq 0, m_i \geq 0$ for $i = 1, \dots, r$.

Let $s_i = \min(n_i, m_i)$ and $t_i = \max(n_i, m_i)$ for $i = 1, \dots, r$. Then

$$(n, m) = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r} \text{ and } [n, m] = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}.$$

(For example, consider 15 and 100. Here $15 = 2^0 \cdot 3^1 \cdot 5^1$ and $100 = 2^2 \cdot 3^0 \cdot 5^2$. So $(15, 100) = 2^0 \cdot 3^0 \cdot 5^1$ and $[15, 100] = 2^2 \cdot 3^1 \cdot 5^2$.)

Also $s_i + t_i = n_i + m_i \forall i = 1, \dots, r$.

$$\begin{aligned} \text{Then } (n, m)[n, m] &= p_1^{s_1+t_1} \cdot p_2^{s_2+t_2} \dots p_r^{s_r+t_r} \\ &= p_1^{n_1+m_1} \dots p_r^{n_r+m_r} \\ &= (p_1^{n_1} \dots p_r^{n_r})(p_1^{m_1} \dots p_r^{m_r}) \\ &= nm. \end{aligned}$$

Example 2: Let $G = GL_2(\mathbb{Q})$. Let $X \in G$. Prove that the operation $*$, defined

on $G \times G$ by $A * B = X^{-1}ABX$, is a binary operation on G .

Further, is $(G, *)$ a group? Why, or why not?

Solution: First, for $A, B \in G$, $\det(A) \neq 0, \det(B) \neq 0$.

$$\therefore \det(X^{-1}ABX) = [\det(X)]^{-1} \det(A) \det(B) \det(X) \neq 0.$$

Also, all the entries of $X^{-1}ABX$ are from \mathbb{Q} .

Thus, $X^{-1}ABX \in G$.

Thus, $*$ is closed on G .

Next, note that there is no $Y \in G$ s.t. $A * Y = A \forall A \in G$.

This is because $A * Y = A$ iff $Y = A^{-1}XAX^{-1}$.

So, for example, if A does not commute with X , then

$$\begin{aligned} I * Y &= X^{-1}YX = X^{-1}A^{-1}XAX^{-1}X \\ &= X^{-1}A^{-1}XA \neq I. \end{aligned}$$

Hence, $(G, *)$ is not a group.

Example 3: Prove that if $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ is a positive integer, then $a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9}$.

Hence prove that a is a multiple of 9 iff $9 \mid (a_0 + a_1 + \cdots + a_n)$.

Solution: For $m \in \mathbb{N}$, $10^m = (10^m - 1) + 1 = (10 - 1)(10^{m-1} + 10^{m-2} + \cdots + 10 + 1) + 1$
 $= 9(10^{m-1} + \cdots + 1) + 1$

Hence, $a = 9[a_n(10^{n-1} + \cdots + 1) + a_{n-1}(10^{n-2} + \cdots + 1) + \cdots + a_2(10 + 1) + a_1] + (a_n + a_{n-1} + \cdots + a_1 + a_0)$.

$\therefore a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9}$.

Now, $9 \mid a \Leftrightarrow a \equiv 0 \pmod{9} \Leftrightarrow a_n + a_{n-1} + \cdots + a_0 \equiv 0 \pmod{9}$

$\Leftrightarrow 9 \mid (a_n + \cdots + a_0)$.

Example 4: Show that $(\mathbb{Z}, *)$ is a group, where

$*$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$: $*(m, n) = m + n + a$ for a fixed $a \in \mathbb{Z}$.

Solution: First check that $*$ is a well-defined binary operation on \mathbb{Z} .

Next, check that $(m * n) * p = m * (n * p) \forall m, n, p \in \mathbb{Z}$, using the properties that $+$ is associative and commutative in \mathbb{Z} .

Thirdly, check that $m * (-a) = m = (-a) * m \forall m \in \mathbb{Z}$.

Finally, check that $m * (-2a - m) = (-2a - m) * m = (-a) \forall m \in \mathbb{Z}$.

Hence, $(\mathbb{Z}, *)$ is a group.

Example 5: Define a relation \sim on \mathbb{R} by ' $x \sim y$ iff $x - y \in \mathbb{Z}$.' Check whether or not \sim is an equivalence relation on \mathbb{R} . If it is, find $[\pi]$. If \sim is not an equivalence relation on \mathbb{R} , find a subset of \mathbb{R} on which it is an equivalence relation.

Solution: Since $x - x = 0 \in \mathbb{Z} \forall x \in \mathbb{R}$, \sim is reflexive.

Also show why \sim is symmetric and transitive.

Hence, \sim is an equivalence relation on \mathbb{R} .

Next, $[\pi] = \{x \in \mathbb{R} \mid x \sim \pi\} = \{x \in \mathbb{R} \mid x - \pi \in \mathbb{Z}\}$

$= \{\pi + n \mid n \in \mathbb{Z}\}$.

Miscellaneous Exercises

E1) Check whether or not $A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ and $B = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\}$

are subgroups of $(M_2(\mathbb{R}), +)$.

Is $A \cap GL_2(\mathbb{R}) \leq (GL_2(\mathbb{R}), \cdot)$? Why, or why not?

E2) Give an example of a proper non-trivial cyclic subgroup of $(\wp(X), \Delta)$, where $X = \{x_1, x_2\}$.

- E3) If G is a group s.t. $(xy)^2 = x^2y^2 \forall x, y \in G$, then G is abelian. Is this statement true? Give reasons for your answer.
- E4) Show that $(\mathbb{Z}[\sqrt{n}], +)$ is a group, where n is a square-free integer.
- E5) Find $o(A)$, where $A = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}$, treating A as an element of $M_2(\mathbb{Z}_7)$, and as an element of $GL_2(\mathbb{Z}_7)$.
- E6) Is D_6 a subgroup of D_8 ? Why, or why not?
- E7) i) Let G be an abelian group and $T = \{g \in G \mid o(g) < \infty\}$. Show that $T \leq G$. (T is called the **torsion subgroup** of G .)
 ii) Find the torsion subgroup of $\mathbb{Z} \times K_4$.
- E8) Which of the following statements are true? Justify your answers.
 i) If G is a group and $n \in \mathbb{N}$, $\{g^n \mid g \in G\}$ is a subgroup of G .
 ii) If G is a non-abelian group and $n \in \mathbb{N}$, $\{g \in G \mid o(g) = n\}$ is a subgroup of G .
 iii) \mathbb{Z}_{45} has exactly 6 distinct subgroups.
 iv) If G is a group and $x, y \in G$, of orders n and m , respectively, then $o(xy) = [n, m]$, the l.c.m of n and m .
 v) If G is an infinite group s.t. $x \in G$, with $o(x)$ being infinite, then $G = \langle x \rangle$.
- E9) Prove that if X is an infinite set, then the set of permutations, $S(X)$, is infinite.
- E10) i) If $\sigma = (1\ 2\ 3\ 4\ 5\ 6) \in S_{10}$, then for which $n \in \mathbb{N}$ is σ^n also a 6-cycle?
 ii) Prove that if $\sigma = (1\ 2 \dots m)$, then σ^n is a cycle of length m iff $(n, m) = 1$. Here $m, n \in \mathbb{N}$.
- E11) Show that if G is a non-cyclic group of order n , then G has no element of order n .
- E12) Write the permutation $(3\ 5\ 7)(1\ 3\ 5)(5\ 7)$ as a product of disjoint cycles. Is this permutation even? Give reasons for your answer.
- E13) Find the orders of the following elements in the group $(\mathbb{Z}_{36}, +)$:
 $\bar{1}, -\bar{1}, \bar{5}, \bar{6}, \bar{13}, -\bar{13}$.
- E14) Under what conditions on c will $(\mathbb{Z}, *)$ be a group, where $*$ is defined by $a * b = ab + a + b + c$, for a fixed $c \in \mathbb{Z}$?
- E15) Check whether or not $GL_2(\mathbb{Z}_4)$ and $GL_2(\mathbb{Z}_5)$ are groups w.r.t. matrix multiplication.

SOLUTIONS / ANSWERS

E1) A and B are subgroups of $(M_2(\mathbb{R}), +)$, applying the subgroup test.

$$A \cap GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a^2 \neq b^2, a, b \in \mathbb{R} \right\}. \text{ This is a subgroup of}$$

$(GL_2(\mathbb{R}), \cdot)$, by the subgroup test.

E2) For any $A \in \wp(X)$, $A \Delta A = \emptyset$, $(A \Delta A) \Delta A = A, \dots$

So, $A^n = \emptyset$ if n is even, and $A^n = A$ if n is odd.

Thus, $\langle A \rangle = \{\emptyset, A\}$.

Hence, if $A = \{x_1\}$, then $\langle A \rangle$ is a proper non-trivial cyclic subgroup of $\wp(X)$.

E3) True. Since $xyxy = xxyy \forall x, y \in G$, by cancellation on the left and on the right, we get $yx = xy \forall x, y \in G$, i.e., G is abelian.

E4) $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$ and $\mathbb{Z}[\sqrt{n}] \neq \emptyset$.

Now, if $a + b\sqrt{n}, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, then

$$(a + b\sqrt{n}) - (c + d\sqrt{n}) = (a - c) + (b - d)\sqrt{n} \in \mathbb{Z}[\sqrt{n}].$$

Hence, $\mathbb{Z}[\sqrt{n}] \leq \mathbb{C}$. Thus, $(\mathbb{Z}[\sqrt{n}], +)$ is a group.

E5) For $n \in \mathbb{N}$, $n \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{n} & \bar{0} \\ \bar{n} & \bar{n} \end{bmatrix}$.

Thus, the least n for which $nA = \mathbf{0}$ is $n = 7$.

$\therefore o(A) = 7$ in $M_2(\mathbb{Z}_7)$.

$A \in GL_2(\mathbb{Z}_7)$ also, since $\det(A) = \bar{1} \neq \bar{0}$.

$$\text{Now, } A = I + \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{0} \end{bmatrix}.$$

$$\text{So, } A^n = I + \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{n} & \bar{0} \end{bmatrix}, n \in \mathbb{N}.$$

$\therefore o(A) = 7$ in $GL_2(\mathbb{Z}_7)$, since $7 \cdot \bar{1} = \bar{0}$.

E6) Since $R_{120} \in D_6$ and $R_{120} \notin D_8$, $D_6 \not\subseteq D_8$. Hence, $D_6 \not\leq D_8$.

E7) i) Firstly, $e \in T$. So $T \neq \emptyset$.

Next, for $g \in T$, $o(g^{-1}) = o(g) < \infty$. So $g^{-1} \in T$.

Finally, if $g_1, g_2 \in T$, then $o(g_1 g_2) \leq o(g_1) o(g_2) < \infty$.

So, $g_1 g_2 \in T$.

Thus, $T \leq G$.

ii) Note that $o((a, b)) = \max(o(a), o(b)) \forall a \in \mathbb{Z}, b \in K_4$.

Also, the only element in \mathbb{Z} with finite order is 0 ; and

$o(x) < \infty \forall x \in K_4$. Thus, $T = \{(0, x) \mid x \in K_4\} = \{0\} \times K_4$.

- E8) i) This is true if G is abelian, not otherwise. Look at S_3 and $n = 3$, to get a counter-example for when G is non-abelian.
- ii) False. Again, take $G = S_3$ and $n = 2$, for a counter-example.
- iii) True. For each positive divisor of 45, there is a unique subgroup of \mathbb{Z}_{45} . These divisors are 1, 3, 5, 9, 15, 45.
- iv) False. For example, consider $\mathbb{Z}_8 = \langle \bar{1} \rangle$.
Then $o(\bar{2}) = 4$ and $o(\bar{4}) = 2$, i.e., $o(\bar{2} \cdot \bar{2}) = 2 \neq [4, 4]$.
- v) False. For example, $\mathbb{Z} = \langle 1 \rangle \neq \langle 2 \rangle$, but $o(2)$ is infinite.

E9) Let $X = \{x_1, x_2, \dots\}$.

Then $(x_i \ x_{i+1}) \in S(X) \ \forall i \in \mathbb{N}$.

Also, $(x_i \ x_{i+1}) \neq (x_j \ x_{j+1})$ unless $i = j$, since $(x_i \ x_{i+1})$ fixes x_j , or x_{j+1} , or both, if $i \neq j$; but $(x_j \ x_{j+1})$ moves both x_j and x_{j+1} .

Hence, $S(X)$ contains the infinitely many transpositions $(x_i \ x_{i+1})$, $i \in \mathbb{N}$.

Hence, $S(X)$ is infinite.

- E10) i) $\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$,
 $\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2)$,
 $\sigma^6 = I$, $\sigma^7 = \sigma$, and so on.

Thus, σ^n is a 6-cycle only for $n = 1, 5, 1+6, 5+6, \dots$, i.e.,
 $n \in \{1+6k, 5+6k \mid k \in \mathbb{N}\}$.

Note that σ^n will be a 6-cycle iff $o(\sigma^n) = 6 = o(\sigma)$.

But $o(\sigma^2) = \frac{o(\sigma)}{2} \neq o(\sigma)$. Similarly, $o(\sigma^3) = \frac{o(\sigma)}{3}$.

In general, $o(\sigma^n) = \frac{6}{(6, n)}$.

- ii) In this case, σ^n is an m -cycle iff $o(\sigma^n) = m$.

Also, $o(\sigma^n) = \frac{m}{(n, m)}$.

$\therefore \sigma^n$ is an m -cycle iff $\frac{m}{(n, m)} = m$, i.e., iff $(n, m) = 1$.

- E11) You can show the contrapositive of the statement, i.e., prove that if G has an element x of order n , then $G = \langle x \rangle$.
 Here, note that $\langle x \rangle \leq G$ and both have the same order.

E12) $(3\ 5\ 7)(1\ 3\ 5)(5\ 7) = (5\ 3\ 7\ 1)$, a 4-cycle.

Since $(5\ 3\ 7\ 1) = (5\ 1)(5\ 7)(5\ 3)$, a product of 3 transpositions, it is an odd permutation.

E13) $o(\bar{1}) = 36$, as $35 \cdot \bar{1} \neq \bar{0}$ and $36 \cdot \bar{1} = \bar{0}$; $o(-\bar{1}) = 36$;

$$o(\bar{5}) = 36, \text{ as } (5, 36) = 1; o(\bar{6}) = 6; o(\bar{13}) = 36, o(-\bar{13}) = o(\bar{23}) = 36.$$

E14) Check that $*$ is a well-defined binary operation on \mathbb{Z} .

Since $(\mathbb{Z}, *)$ is a group, $*$ is associative on \mathbb{Z} .

Hence, show that c must be 0.

Then the additive identity must be 0.

However, then no element in \mathbb{Z}^* has an inverse w.r.t. $*$. (Why?)

Thus, for no c is $(\mathbb{Z}, *)$ a group.

$$E15) \text{GL}_2(\mathbb{Z}_4) = \left\{ \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z}_4) \mid \bar{a}\bar{d} - \bar{b}\bar{c} \neq \bar{0} \right\}.$$

Now $\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix} \in \text{GL}_2(\mathbb{Z}_4)$. Suppose $\begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix}$ is its inverse. Then

$$\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}.$$

So $\bar{2}\bar{d} = \bar{1}$ in \mathbb{Z}_4 . Hence, $4 \mid (1 - 2d)$, i.e., $4x = 1 - 2d$ for some $x \in \mathbb{Z}$. So

$2d + 4x = 1$ in \mathbb{Z} , i.e., $2(d + 2x) = 1$ in \mathbb{Z} , which is not possible.

Thus, not every element has an inverse in $\text{GL}_2(\mathbb{Z}_4)$. Hence, it is not a group w.r.t. matrix multiplication.

However, $(\text{GL}_2(\mathbb{Z}_5), \cdot)$ is a group, which you should check.