Master of Science in Mathematics

(M.Sc. Mathematics)

Abstract Algebra

(OMSMCO202T24)

Self-Learning Material
(SEM - II)

Jaipur National University
Centre for Distance and Online Education

Established by Government of Rajasthan
Approved by UGC under Sec 2(f) of UGC ACT 1956
&
NAAC A+ Accredited

TABLE OF CONTENTS

EXPERT COMMITTEE

1. **Dr. Vikas Gupta**
Dean
Department of Mathematics
LNMIIT, Jaipur

2. Dr. Nawal Kishor Jangid
Department of Mathematics
SKIT, Jaipur

COURSE COORDINATOR

Mr. Praveen Kumar
Dept. of Basic Sciences
JNU, Jaipur

UNIT PREPARATION

Unit Writers	Assisting & Proof reading	Unit Editor
Dr. Sanju Jangid Department. of Basic Sciences JNU, Jaipur Unit 1 -5	Prof. Hoshiyar Singh Department. of Basic Sciences JNU, Jaipur	Dr. Yogesh Khandelwal Department. of Basic Sciences JNU, Jaipur
Mr. Babulal Saini Dept. of Basic Sciences JNU, Jaipur Unit 6 - 10		
Mr. Mohammed Asif Dept. of Basic Sciences JNU, Jaipur Unit 11 - 14		

Secretarial Assistance:
Mr. Mukesh Sharma

COURSE INTRODUCTION

Abstract algebra is a branch of mathematics that studies algebraic systems in a broad manner. Unlike elementary algebra, which deals with specific systems like the real numbers or polynomials, abstract algebra focuses on more general structures and their properties.

Abstract algebra is foundational for many areas of mathematics and provides the language and framework for many advanced topics in both pure and applied mathematics. The course is of four credits and divided into 14 units. There are sections and subsections in each unit. Each unit starts with a statement of objectives that outlines the goals we hope you will accomplish.

Course Outcomes:

At the completion of the course, a student will be able to:

1. Recall the various algebraic structures.
2. Explain the mathematical objects called groups.
3. Apply the basic concepts to develop theorems.
4. Analyze the significance of the notions of cosets, normal subgroups, and factor groups.
5. Evaluate the fundamental concepts in field theory.
6. Develop the classification of finite fields.

Acknowledgements:

The content we have utilized is solely educational in nature. The copyright proprietors of the materials reproduced in this book have been tracked down as much as possible. The editors apologize for any violation that may have happened, and they will be happy to rectify any such material in later versions of this book.

UNIT - 1

Preliminaries

Learning objectives

Understanding Basic Algebraic Structures, gain familiarity with fundamental algebraic structures such as groups, rings, and fields. Learn their definitions, properties, and examples.

Structure

1.1 A Short Note on Proofs

Abstract mathematics is different from other sciences. In laboratory sciences such as chemistry and physics, scientists perform experiments to discover new principles and verify theories. Although mathematics is often motivated by physical experimentation or by computer simulations, it is made rigorous through the use of logical arguments. In studying abstract mathematics, we take what is called an axiomatic approach; that is, we take a collection of objects S and assume some rules about their structure. These rules are called axioms. Using the axioms for S, we wish to derive other information about S by using logical arguments. We require that our axioms be consistent; that is, they should not contradict one another. We also demand that there not be too many axioms. If a system of axioms is too restrictive, there will be few Ex's of the mathematical structure.

A statement in logic or mathematics is an assertion that is either true or false. Consider the following Ex's:

- $3 + 56 - 13 + 8/2$.
- All cats are black.
- $2 + 3 = 5$.

1.2 Sets and Equivalence Relations

Set Theory

A set is a well-defined collection of objects; that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set. The objects that belong to a set are called its elements or members. We will denote sets by capital letters, such as A or X; if a is an element of the set A, we write $a \in A$.

A set is usually specified either by listing all of its elements inside a pair of braces or by stating the property that determines whether or not an object x belongs to the set. We might write

$X = \{x_1, x_2, \ldots, x_n\}$

for a set containing elements $x_1, x_2, \ldots, x_n$ or

$X = \{x: x \text{ satisfies } P\}$.

Examples of Sets

Some standard sets in mathematics are:

- Set of natural numbers, $N = \{1, 2, 3, \ldots\}$
- Set of whole numbers, $W = \{0, 1, 2, 3, \ldots\}$
- Set of integers, $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Set of rational numbers, $Q = \{p/q \mid q \text{ is an integer and } q \neq 0\}$
- Set of irrational numbers, $Q' = \{x \mid x \text{ is not rational}\}$
- Set of real numbers, $R = Q \cup Q'$

All these are infinite sets. But there can be finite sets as well.

$A = \{2, 4, 6, 8\}$ is an EX of a finite set that may be used to represent the collection of even natural numbers smaller than 10.

Parts of a Set

Either elements or members of a set are the objects that make up the set. Curly brackets encompass the components of a set, which are separated by commas. '∈' is the symbol indicates that an element is contained in the set.

Ex:- $A = \{2, 4, 6, 8\}$

Here, $2 \in A$, $4 \in A$, $6 \in A$, $8 \in A$.

The sign '∉' is indicate an element that is not a part of the set.

Ex: $3 \notin A$. i.e. 3 is not a part of the set A.

Cardinality (cardinal number or Number of element) of a Set:

A set's cardinal number, cardinality, or order indicates how many items there are in total. For natural even integers n (A) = 4 that are smaller than 10. A collection of distinct elements is referred to as a set. All of a set's elements must be connected to one another and possess a common property in order for a set to be defined. For instance, if we establish a set whose members are the names of the months in a year, we may state that the months themselves make up every element of the set.

Representation of the Sets:

There are different set notations are used in set theory to represent sets. Each of them has a separate set of components. There are three set notations used to represent sets:

- Roster form
- Set builder form

Let us understand each of these forms with an EX.

Set of first five even natural numbers		
Semantic Form	Roster Form	Set Builder Form
A set of first five even natural numbers	{2, 4, 6, 8, 10}	{x ∈ N | x ≤ 10 and x is even}

Table 1.1 : Representation of Sets

Venn diagram for the Visual Representation of Sets

A Venn diagram is a depiction of sets in which a circle represents each set. The elements of a set are included within each circle. There are instances where a rectangle encircled by circles is used to symbolize the universal set. The relationships between the given sets are depicted in the Venn diagram.

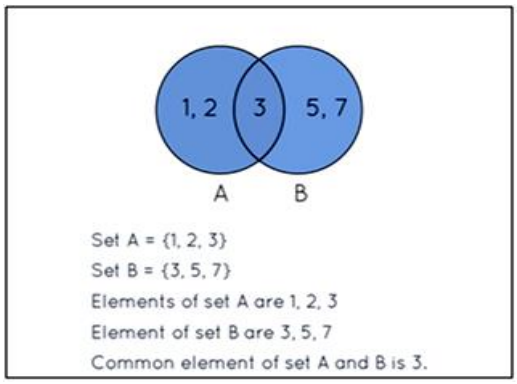


Figure 1.1 : Venn diagram

Sets Symbols

The components of a particular set are denoted by set symbols. The set theory symbols and their meanings are displayed in the following table.

Symbols	Meaning
{ }	Symbol of set
U	Universal set
n(X)	Cardinal number of set X
b ∈ A	'b' is an element of set A
a ∉ B	'a' is not an element of set B
∅	Null or empty set
A U B	Set A union set B
A ∩ B	Set A intersection set B
A ⊆ B	Set A is a subset of set B
B ⊇ A	Set B is the superset of set A

Table 1.2 : Sets Symbols

Types of Sets

A set in mathematics is a group of unique items that are each regarded as a separate entity. In mathematics, sets are basic objects. Here are various types of sets with brief explanations:

1. **Countable (Finite) Set**: A set with a limited number of elements.

   Ex: {1,2,3,4,5}

2. **Uncountable (Infinite) Set**: A set having infinite number of elements.

   Ex: {0, 1,2,3,…}

3. **Void Set (Empty Set or Null Set)**: A having no elements.

   It is denoted by " $\emptyset$ or {}".

4. **Singleton Set**: A set with exactly one element.

   Ex: {a}

5. **Subset**: The set whose elements are all contained within another set.

   Ex: If A = {1,2,3,4 } and B = {3,4}, then B is a subset of A.

6. **Proper Subset**: A subset that is not equal to the original set (i.e., it contains fewer elements).

   Ex: If A={1,2,3}, B={1,2} is a proper subset of A.

7. **Power Set**: Power set is the set of all subsets of a given set.

   Ex: A={1,2}, then power set of A is {$\emptyset$,{1},{2},{1,2}}

8. **Universal Set**: The set that contains all the objects under consideration, usually denoted by U.

   Ex: If we are considering all natural numbers, then U could be the set of all natural numbers.

9. **Complement of a Set**: The complement of a set of those elements which are in the universal set but are not in the given set.

   Ex: If U = {1,2,3,4,5} $and\ A = \{1,2\}$, then the complement of A is {3,4,5}

10. **Union of Sets**: A set containing all elements of the given sets.

    Notation: A∪B

    Ex: If A={1,2} and B={2,3}, then A∪B={1,2,3}.

11. **Intersection of two Sets**: A set containing only the common elements of the given sets.

    Notation: A∩B

    Ex: If A = {1,2} and B = {2,3}, then A ∩ B = {2}.

12. **Difference of two Sets**: A set containing those elements that are in one set but not in another.

    Denoted by " A−B"

    Ex: If A={1,2,3} and B={2,3}, then A−B={1}.

13. **Disjoint Sets**: Having no elements in common.

    Ex: $A = \{1,2\}$ and $B = \{3,4\}$

14. **Equivalent Sets**: Sets that have the same number of elements.

    Ex: $A=\{1,2,3\}$ and $B=\{a,b,c\}$

15. **Equal Sets**: Sets that contain exactly the same elements.

    Ex: If $A = \{1,2,3\}$ and $B = \{3,2,1\}$, then A=B.

16. **Cartesian product**: The set of all ordered pairs from two sets.

    Denoted by "A×B"

    Ex: If $A = \{1,2\}$ and $B = \{a, b\}$, then $A \times B = \{(1, a), (1, b), (2, a), (2, b)\}$.

Understanding these types of sets and their properties is fundamental in set theory and various areas of mathematics.

Venn Diagram for Different types of sets

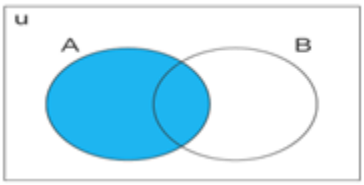


Figure 1.2 : Set A

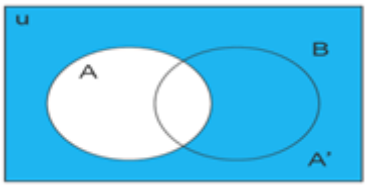


Figure 1.3 : A' is the complement of A

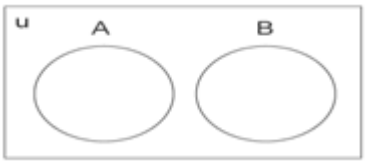


Figure 1.4 : Disjoint sets of A and B

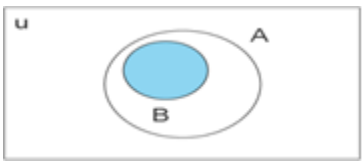


Figure 1.5 : B is a Proper subset of A

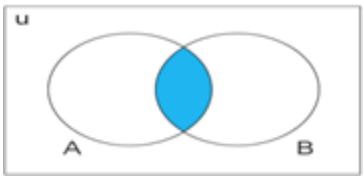


Figure 1.6 : A n B

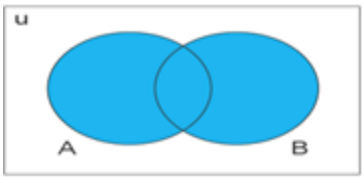


Figure 1.7 : A U B

In the above figure, the shaded portions in "blue" show the set that they are labelled with.

Sets Formulas in Set Theory

For any two overlapping sets A and B,

- $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
- $n(A \cap B) = n(A) + n(B) - n(A \cup B)$
- $n(A) = n(A \cup B) + n(A \cap B) - n(B)$
- $n(B) = n(A \cup B) + n(A \cap B) - n(A)$
- $n(A - B) = n(A \cup B) - n(B)$
- $n(A - B) = n(A) - n(A \cap B)$

For any two sets A and B that are disjoint,

- $n(A \cup B) = n(A) + n(B)$
- $A \cap B = \emptyset$

Laws of Sets

1. **Commutative Law**:
    - **Union**: $A \cup B = B \cup A$
    - **Intersection**: $A \cap B = B \cap A$
2. **Associative Law**:
    - **Union**: $(A \cup B) \cup C = A \cup (B \cup C)$
    - **Intersection**: $(A \cap B) \cap C = A \cap (B \cap C)$
3. **Distributive Law**:
    - **Union over Intersection**: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
    - **Intersection over Union**: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. **Identity Law**:
    - **Union with Empty Set**: $A \cup \emptyset = A$
    - **Intersection with Universal Set**: $A \cap U = A$
    - **Union with Universal Set**: $A \cup U = U$
    - **Intersection with Empty Set**: $A \cap \emptyset = \emptyset$
5. **Idempotent Law**:
    - **Union**: $A \cup A = A$
    - **Intersection**: $A \cap A = A$
6. **Complementary Law**:
    - **Double Complement**: $(Ac)c = A(Ac)c$

- **De Morgan's Laws**:
  - $(A \cup B)c = Ac \cap Bc$
  - $(A \cap B)c = Ac \cup Bc$

7. **Absorption Law**:
   - $A \cup (A \cap B) = A$
   - $A \cap (A \cup B) = A$
8. **Complement Laws**:
   - $A \cup A^c = U$
   - $A \cap A^c = \emptyset$
9. **Null and Universal Sets**:
   - **Union with Universal Set**: $A \cup U = U$
   - **Intersection with Universal Set**: $A \cap U = A$
   - **Union with Empty Set**: $A \cup \emptyset = A$
   - **Intersection with Empty Set**: $A \cap \emptyset = \emptyset$
10. **Subset Property**:

    If $A \subseteq B$, then:
    - $A \cup B = B$
    - $A \cap B = A$

Understanding these properties is essential for working with sets, as they provide the rules for how sets interact and how to manipulate them in various mathematical contexts.

1.3 Summary

"Preliminaries of Abstract Algebra" typically cover foundational concepts and structures essential for understanding abstract algebraic systems. Here's a brief summary:

- Sets and Functions
- Binary Operations.
- Groups
- Subgroups
- Cosets and Lagrange's Theorem

1.4 Keywords

Keywords for the preliminaries of abstract algebra typically include:

- Sets
- Functions
- Binary operations
- Groups
- Subgroups
- Cosets

1.5 Self Assessment Questions

1. Define a group and list its four defining properties.
2. Explain what a subgroup is and provide an EX.
3. What is Lagrange's theorem, and what does it state about the order of subgroups?
4. Define a normal subgroup and explain its significance in group theory.
5. Describe what a quotient group is and how it is constructed.

1.6 Case Study

Cryptography is the practice of secure communication in the presence of adversaries. It relies heavily on abstract algebra, particularly group theory, for designing secure cryptographic systems.

Question: Alice and Bob want to communicate securely over an insecure channel, such as the internet, without Eve, the eavesdropper, intercepting their messages.

1.7 References

1. Bhattacharya, P. B., Jain, S. K., & Nagpaul, S. R. (1994). Preliminaries.

UNIT - 2

The Integers

Learning objectives

- Recognize the fundamentals of mathematical induction as a mathematical proof technique.
- Discover how to use the mathematical induction principle to develop and verify claims.
- Acquire the capacity to discern when the use of mathematical induction to the proof of claims is suitable.
- Recognize number theory's foundational idea—the Division Algorithm.
- Discover how any number may be expressed as the product of a divisor and a quotient, with a remainder, using the Division Algorithm.
- Examine how to use the Division Algorithm to get an integer's divisibility qualities.

Structure

2.1 Mathematical Induction

Mathematical induction is a fundamental proof writing technique that may be applied to any well-organized collection to prove a given proposition.

Suppose P(n) is a statement for n natural number then it can be proved using the Principle of Mathematical Induction, Firstly we will prove for P(1) then let P(k) is true then prove for P(k+1). If P(k+1) holds true. Hence P(n) is true by the principle of mathematical induction.

Principle of Mathematical Induction Statement

Any statement P(n) which is for "n" natural number can be proved using the Principle of Mathematical Induction by following the below steps,

Step 1: Verify if the statement is true for trivial cases (n = 1) i.e. check if P(1) is true.

Step 2: Assume that the statement is true for n = k for some $k \geq 1$ i.e. P(k) is true.

Step 3: If the truth of P (k) implies the truth of P (k + 1), then the statement P (n) is true for all $n \geq 1$.

Ex. 1:

Prove that $n^3 + 2n$ are always divisible by 3, for any +ve number n.

Solution:

Let, P (n): $n^3 + 2n$ is divisible by 3.

Step 1: Basic Step

Firstly we prove that P (1) is true. Let n = 1 in $n^3 + 2n$

$= 13 + 2(1)$

$= 3$

As 3 is divisible by 3. Hence, P (1) is true.

Step 2: Assumption Step

Let us assume that P (K) is true

Then, $k^3 + 2k$ is divisible by 3

Thus, we can write it as $k^3 + 2k = 3n$, (where n is any positive integer)….(i)

Step 3: Induction Steps

Now we have to prove that algebraic expression $(k + 1)^3 + 2(k + 1)$ is divisible by 3

$= (k + 1)^3 + 2(k + 1)$

$= k^3 + 3k^2 + 5k + 3$

$= (k^3 + 2k) + (3k^2 + 3k + 3)$

From eq(i)

$= 3n + 3(k^2 + k + 1)$

$= 3(n + k^2 + k + 1)$

As it is a multiple of 3 we can say that it is divisible by 3.

Thus, P(k+1) is true i.e. $(k + 1)^3 + 2(k + 1)$ is be divisible by 3. Now by the Principle of Mathematical Induction, we can say that, P(n): $n^3 + 2n$ is divisible by 3 is true.

Ex. 2:

Prove $a_n = a_1 + (n – 1)\, d$, is the general term of any arithmetic sequence.

Solution:

For n = 1, we have $a_n = a_1 + (1 – 1)\, d = a_1$, so the formula is true for n = 1,

Let us assume that the formula $a_k = a_1 + (k – 1)$ is true for all natural numbers.

We shall now prove that the formula is also true for k+1, so now we have,

$a_{k+1} = a_1 + [(k + 1) – 1]\, d = a_1 + k \cdot d$.

We assumed that $a_k = a_1 + (k – 1)\, d$, and by the definition of an arithmetic sequence $a_{k+1} – a_k = d$,

Then, $a_{k+1} – a_k$

$= (a_1 + k \cdot d) – (a_1 + (k – 1)d)$

$= a_1 – a_1 + kd – kd + d$

$= d$

Thus the formula is true for k + 1, whenever it is true for k. And we initially showed that the formula is true for n = 1. Thus the formula is true for all natural numbers.

2.2 The Division Algorithm.

The division algorithm is a fundamental theorem in arithmetic that provides a way to divide integers and express the result in terms of a quotient and a remainder. The formal statement of the “division algorithm” is:

For any integers a and b (with $b \neq 0$), there exist unique integers q (the quotient) and r (the remainder) such that: $a=bq+r$ where $0 \leq r < |b|$.

Here's how the division algorithm works, broken down into steps:

1. **Given Integers**: Start with two integers a (the dividend) and b (the divisor), where $b \neq 0$.
2. **Determine Quotient**: Find the largest integer q such that $bq \leq a$. This q is the quotient.
3. **Compute Remainder**: Calculate the remainder r by subtracting bq from a: $r = a - bq$
4. **Check Remainder**: Ensure that the remainder rrr satisfies the condition $0 \leq r < |b|$. If it does, then q and r are the quotient and remainder, respectively.

Ex. 3: Divide 17 by 5.

1. **Given**: $a = 17$, $b = 5$.
2. **Determine Quotient**: Find the largest integer q such that $5q \leq 17$.
    - $5 \times 0 = 0$ (too small)
    - $5 \times 1 = 5$ (too small)
    - $5 \times 2 = 10$ (still less than 17)
    - $5 \times 3 = 15$ (still less than 17)
    - $5 \times 4 = 20$ (too large)

    The largest q that satisfies $5q \leq 175$ is $q = 3$.
3. **Compute Remainder**: Calculate r: $r = 17 - 5 \times 3 = 17 - 15 = 2$
4. **Check Remainder**: Ensure $0 \leq r < 5$.

    $0 \leq 2 < 5$ is true.

So, the quotient is $q = 3$ and the remainder is $r = 2$. Therefore: $17 = 5 \times 3 + 2$

Division Algorithm for Polynomials

The division of polynomials may be expressed as follows using the polynomial division method, provided that $g(x) \neq 0$ and that p(x) and g(x) are the two polynomials. The formula for p(x) is $q(x) \times g(x) + r(x)$, where r(x) , here degree of r(x) should be smaller than g(x).

P(X) is the dividend.

The divisor is □(□).

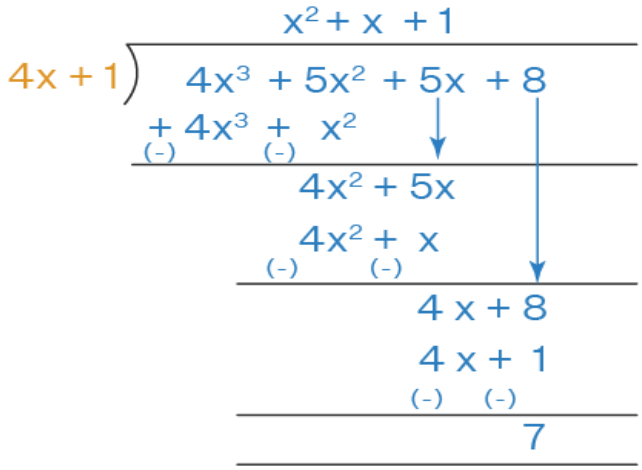
This is the quotient, q(x). This is the remainder, r(x).

Dividend = (Divisor × Quotient) + Remainder.

Ex. 4:

When the polynomial $4x^3 + 5x^2 + 5x + 8$ is divided by $(4x + 1)$, find the quotient and the remainder, then use the division procedure to confirm the outcome.

Solution:



We will now verify the division algorithm.

$p(x) = q(x) \times g(x) + 1(x)$

$4x^3 + 5x^2 + 5x + 8 = (x^2 + x + 1)(4x + 1) + 7$

$4x^3 + 5x^2 + 5x + 8 = 4x^3 + 4x^2 + 4x + x^2 + x + 1 + 7$

$4x^3 + 5x^2 + 5x + 8 == 4x^3 + 5x^2 + 5x + 8$

Thus, the division algorithm is verified.

Procedure to Divide a Polynomial by another Polynomial

Step 1: Sort the exponents decreasingly by dividend and divisor.

Step 2: By dividing the highest "degree term of the dividend by the highest degree term of the divisor", one may find the first term of the residual.

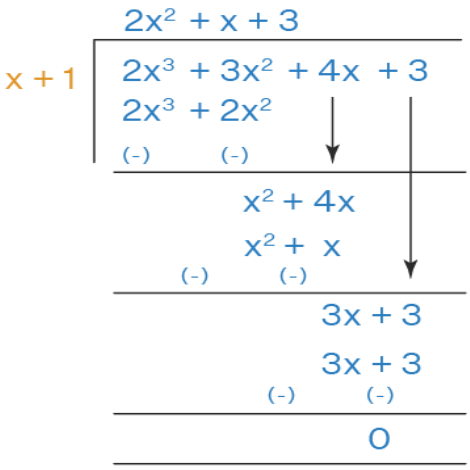
Proceed to "multiply the divisor by the current quotient and deduct the result from the current dividend".

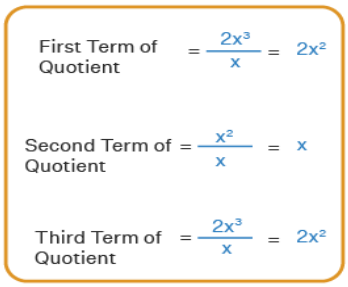
Step 3: A new dividend will come from this.

Step 4: To get the next term of the quotient, "divide the highest degree term of the new dividend obtained in step 3 by the largest degree term of the divisor".

Step 5: Up until the degree of the residual is less than the degree of the divisor, keep performing steps 3 and 4.

Ex 5: Divide 2x3 + 3x2 + 4x + 3 by x + 1.





Here $p(x) = 2x^3 + 3x^2 + 4x + 3$, $g(x) = x + 1$, $q(x) = 2x^2 + x + 3$ and $r(x) = 0$. Try verifying the division algorithm for polynomials now.

2.3 Summary

- Mathematical induction is a powerful technique used to prove statements about integers or sequences.
- Mathematical induction is often used to prove statements about sums, products, divisibility, inequalities, and properties of recursively defined structures.
- Understanding the Division Algorithm is crucial for various areas of mathematics, including number theory, algebra, and cryptography. It provides a systematic way to understand the structure of integers and polynomials under division.

2.4 Keywords

- Mathematical Induction
- Base Case
- Inductive Step
- Induction Hypothesis

- Principle of Mathematical Induction
- Division Algorithm
- Quotient
- Remainder
- Divisor
- Integer Division

2.5 Self Assessment questions

1. What is mathematical induction, and how does it operate?
2. Describe how, when employing mathematical induction, it is crucial to define a base case.
3. Explain how a demonstration by mathematical induction works at the inductive phase.
4. Describe the Division Algorithm and the importance of number theory to it.
5. How are the main elements of the Division Algorithm connected to one another?
6. Describe how to divide two numbers using the Division Algorithm with an EX.

2.6 Case Study

Using an unreliable channel, Alice and Bob wish to put in place a secure communication system. To protect the secrecy and integrity of their communications, they choose to employ cryptographic methods grounded in mathematical concepts.

Question: To protect against adversarial assaults, they must set up a secure key exchange mechanism and encryption system.

2.7 References

1. Rosen, K. H. (2011). *Discrete Mathematics and Its Applications* (7th ed.). McGraw-Hill Education.
2. Graham, R. L., Knuth, D. E., & Patashnik, O. (1994). *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley.
3. Hardy, G. H., & Wright, E. M. (2008). *An Introduction to the Theory of Numbers* (6th ed.). Oxford University Press.

UNIT – 3

Groups

Learning objectives

A basic field of study with numerous applications in mathematics and other fields, group theory is a subfield of abstract algebra. When studying group theory, the following are typical learning goals:

- Understanding Groups
- Group Operations
- Subgroups
- Group Homomorphisms
- Isomorphism

Structure

3.1 Integer Equivalence Classes and Symmetries

The Integers mod □

In algebraic theory and applications, the integers mod □ have become a crucial component. They are utilized in the fields of mathematics in coding theory, cryptography, and error detection in identifying codes.

It is well known that if n divides □−□, then two numbers, a and b, are identical mod n. Additionally, the integers mod n divide □ into □ distinct equivalency classes; we will refer to the collection of these equivalency classes as □□. Examine the numbers modulo 12 and the associated division of the numbers:

$$[0]=\{\ldots,-12,0,12,24,\ldots\},$$

$$[1]=\{\ldots,-11,1,13,25,\ldots\},$$

$$\vdots$$

$$[11]=\{\ldots,-1,11,23,35,\ldots\}.$$

The equivalency classes [0], [1],…, [11] will be denoted by 0,1,…,11, correspondingly, when there can be no doubt about it. Arithmetic on □□ is possible. Define addition modulo n for two numbers, a and b, as (a+b) (mod□), or the residual obtained by dividing b by □. In a similar vein, multiplication modulo n is expressed as (□□)(mod□), or the residual obtained from dividing □□ by □.

Ex 1:

The subsequent instances demonstrate integer arithmetic modulo □:

7+4≡1 (mod5) 7· 3≡1 (mod5)

3+5≡0 (mod8) 3· 5≡7 (mod8)

3+4≡7 (mod12) 3· 4≡0 (mod12).

Solution

Specifically, take note that the product of two nonzero values modulo □ may equal 0 modulo n.

Proposition:

Let □□ be the set of equivalence classes of the integers mod □ and □,,∈□□.

1. Addition and multiplication are commutative:

□+□≡□+□ (mod □)

□□≡□□ (mod □).

2. Addition and multiplication are associative:

(□+□)+□≡□+ (□+□) (mod □)

(□□)□≡□ (□□) (mod □).

3. **There are both additive and multiplicative identities:**

$a+0 \equiv a \pmod{n}$

$a \cdot 1 \equiv a \pmod{n}$.

4. **Multiplication distributes over addition:**

(□+□)≡□□+ (mod □).

5. **For every integer □ there is an additive inverse −□:**

□+ (−□) ≡0 (mod □).

3.2 Definitions and Examples

Definitions

Group

A group is a set S with an operation $\circ: S \times S \to S$ satisfying the following properties:

Identity: There exists an element $e \in S$ such that for any $f \in S$ we have $e \circ f = f \circ e = f$.

Inverses: For any element $f \in S$ there exists $g \in S$ such that $ff\circ = e$.

Associativity: For any $f, g, h \in S$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

Examples

A group is (Z,+). Addition is associative, the identity is 0, and the inverse of a ´ Z is -a. Both complex and real numbers using the binary operator + create groups equally. However, the natural numbers N that have the operation + do not form a group, and neither does (Z,-).

Solve 1-(2-3) as well as (1-2)-3. The binary operation -- isn't associative on Z because of their differences.

"The" unimportant group. Since there is only one binary operation on a one element set, let G={e} be a one element set, and let be the binary operation on G defined by e*e=e. Then, the trivial group is a group denoted by (G,*).

3.3 Sub-groups

Assume that G is a group and that the operation is multiplication (or addition, depending on the situation). If a subset H of G forms a group under the same operation as G, then H is

termed a subgroup of G. In other words, H fulfills the identity element, closure, associativity, and inverses group axioms.

Ex 2 :

- In the additive group of integers (Z,+), the set of even integers is a subgroup because it is closed under addition, contains the identity element 0, and each element has its inverse in the set.
- In the multiplicative group of non-zero rational numbers (Q^* ,$\cdot$), the set of positive rational numbers is a subgroup.

Proper Sub-group: A subgroup H of a group GGG is considered proper if H is not equal to G itself.

Generating Sub-groups: A subgroup generated by a subset S of a group G is the smallest subgroup of G containing all elements of S. It consists of all possible finite products and inverses of elements in S.

3.4 Summary

Mathematical entities called groups are made up of a set and an operation. Group theory is a subfield of abstract algebra that studies groups.

- Definition of Groups
- EXs of Groups
- Subgroups

3.5 Keywords

Keywords of group theory encompass its fundamental concepts, techniques, and applications. Here's a list:

- Group
- Subgroup
- Homomorphism
- Isomorphism
- Coset

3.6 Self Assessment questions

1. Describe a group and the four requirements that it has to meet.
2. Give two and three group instances, illustrating both finite and infinite groups.
3. Define a subgroup. Give an instance.
4. State and describe the Lagrange theorem. In group theory, how is it useful?
5. Describe how two groups are homomorphic. Give an instance.

3.7 Case Study

Public-key cryptography altered the way secure communication is carried out by introducing asymmetric encryption for the first time. Whereas symmetric encryption uses a single secret key shared by both parties, public-key cryptography uses a pair of keys: a public key for encryption and a private key for decryption. Group theory forms a substantial part of the mathematical foundations of public-key cryptography.

3.8 References

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. Wiley.
2. Robinson, D. J. S. (1996). *A course in the theory of groups* (2nd ed.). Springer.

Unit – 4

Cyclic group

Learning objectives

Studying cyclic groups usually has the following learning goals:

- Recognizing the Definition
- Recognizing Groups that Cycle
- Cyclic Group Properties
- Producers and Commands
- Utilizations and Illustrations

Structure

4.1 Cyclic Subgroups

A cyclic subgroup of a group is a subgroup that is "generated by a single element", called a generator. More formally:

Given a group G and an element g in G, the cyclic subgroup generated by g, denoted ⟨ g⟩ , is the smallest subgroup of G that contains g.

In other words, ⟨ g⟩ consists of all powers of g and their inverses, along with the identity element of the group. Symbolically:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

Ex 1. Assume that we examine all multiples of 3 (positive and negative), taking into account that 3 ∈ Z. This is represented as a set by 3Z = {..., −3, 0, 3, 6,...}. That 3Z is a subgroup of the integers is evident. Since all other group elements may be obtained by taking multiples of

3, element 3 determines this subgroup entirely. Three "generates" each element in the subgroup.

Ex 2. The multiplicative group of nonzero rational numbers, Q∗ , has H as a subgroup if H = {2^n: n ∈ Z}. H contains ab−1 = 2m2 −n = 2m−n if a = 2^m and b = 2^n. The element 2 determines a subgroup of Q∗ by H.

Theorem 4.1

Assume that a is any element of the group G. Then, a subgroup of G is the set ⟨a⟩ = {a^k: k ∈ Z}. Moreover, the smallest subgroup of G that includes an element is ⟨ a⟩ .

Proof. The identity is in (a) since a 0 = e. If g and h are any two elements in (a), then by the definition we can write g = am and h = a n for some integers m and n. So gh = a^m a^n = $a^{m÷n}$ is again in (a). Finally, if g = a^n , then the inverse g −1 = a^{-n} is also in (a). Clearly, any subgroup H of G containing a must contain all the powers of a by closure; hence, H contains (a). Therefore, (a) is the smallest subgroup of G containing a.

4.2 Multiplicative Group of Complex Numbers

The complex numbers are defined as

$C = \{a + bi : a, b \in R\}$,

where $i^2 = -1$. If z = a + bi, then a is the real part of z and b is the imaginary part of z.

To add two complex numbers z = a + bi and w = c + di, we just add the corresponding real and imaginary parts: z + w = (a + bi) + (c + di) = (a + c) + (b + d)i.

Remembering that $i^2 = -1$, we multiply complex numbers just like polynomials. The product of z and w is (a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac − bd) + (ad + bc)i.

Every nonzero complex number z = a + bi has a multiplicative inverse; that is, there exists a z^{-1} ∈ C ∗ such that $zz^{-1} = z^{-1} z = 1$. If z = a + bi, then z^{-1} = a − bi /$a^2 + b^2$.

4.3 Summary

A cyclic group is a fundamental concept in abstract algebra, characterized by being generated by a single element.

4.4 Keywords

- Cyclic Group
- Generator.
- Order
- Subgroup
- Finite
- Infinite

4.5 Self Assessment questions

1. Define a cyclic group and explain what it means for a group to be cyclic.
2. What is a generator in the context of cyclic groups? Provide an EX of a generator in a specific cyclic group.
3. Consider the group of integers under addition Z. Is this group cyclic? If so, what is a generator for this group?
4. True or False: Every subgroup of a cyclic group is cyclic. Justify your answer.
5. Determine the order of the cyclic subgroup generated by g=3 in the group $\square_{10}$ (integers modulo 10 under addition).

4.6 Case Study

Web applications often require users to authenticate themselves before accessing sensitive information or performing certain actions. One common method of authentication involves the use of authentication tokens, which are small pieces of data that serve as proof of the user's identity. Cyclic groups can be utilized to create secure authentication tokens that are resistant to tampering and forgery.

Question: Consider a web application that allows users to access their personal accounts after logging in with a username and password. To enhance security, the application implements authentication tokens using cyclic group-based cryptography.

4.7 References

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. Wiley.
2. Robinson, D. J. S. (1996). *A course in the theory of groups* (2nd ed.). Springer.

Unit - 5

Permutation groups

Learning objectives

The learning objectives of studying permutation groups typically include:

- Understanding Permutations.
- Definition of Permutation Groups
- Cyclic Notation
- Properties of Permutation Groups
- Cayley's Theorem

Structure

5.1 Definitions and Notations

A permutation is a one-to-one onto mapping to itself that looks like this: let G be a non-empty set.

- The degree of permutation is the total number of elements in a finite set G.
- If G has n items, then P is referred to as the set of all n-degree permutations.
- The Symmetric group of degree n is another name for P_n.
- Additionally, S_n represents P_n.

Reading the Symbol of Permutation

Suppose that a permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}.$$

Initially, we see that two rows with numbers are printed in a little bracket. One is the smallest number and six is the greatest. We start with the left side of the first row, which reads as follows: image of 1 is 2, image of 2 is 3, image of 3 is 1, image of 4 is 4, image of 5 is 6, and image of 6 is 5. It is also possible to write the above as follows: 1. Starting from the left side of the first row, 2 moves to 3, 2 moves to 4, 3 moves to 5, 4 moves to 6, then 6 moves to 5. A two-length cycle is called a permutation.

5.2 Dihedral Groups

The dihedral group of order 2_n, denoted D_n or D_{2n}, is the group of symmetries of a regular n-sided polygon. It has 2_n elements: n rotations and n reflections.

The group □□ consists of 2□ elements, which can be depicted as follows:

- n rotations, denoted by R_0, $R_{360/n}$, $R_{(360)(2)/n}$..., $R_{(n-1)360/n}$, where □□(360)/□ represents a rotation of (360i/n)(360□/□) degrees clockwise about the center of the polygon.
- n reflections, denoted by "F_0,F_1,F_2,...,$F_{(n-1),}$" where □ represents a reflection of a line passing through the center of the polygon and one of its vertices.

Ex 1:

The symmetric group of a regular pentagon is called the □5 dihedral group of order 10. Ten components make up this structure, which can be seen as pentagon rotations and reflections. The □5 Cayley table:

○	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
e	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	e	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	e	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	e	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	e	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s	rs	r^2s	r^3s	r^4s	e	r	r^2	r^3	r^4
rs	rs	r^2s	r^3s	r^4s	s	r	r^2	r^3	r^4	e
r^2s	r^2s	r^3s	r^4s	s	rs	r^2	r^3	r^4	e	r
r^3s	r^3s	r^4s	s	rs	r^2s	r^3	r^4	e	r	r^2
r^4s	r^4s	s	rs	r^2s	r^3s	r^4	e	r	r^2	r^3

5.3 Summary

A fundamental mathematical idea in group theory and combinatory is a permutation group. A composition of permutations constitutes the group operation of a permutation group, which is a group whose members are permutations of a set. Bijective mappings known as permutations are used to rearrange a set's elements.

There are two ways to express permutations: disjoint cycle notation, in which every cycle is a permutation, and cycle notation, in which components are moved cyclically.

The group that is symmetric The group of all n element permutations is denoted by Sn. It is widely used in group theory and combinatory as a basic EX of a permutation group.

Order, cycle structure, and cycle durations are only a few of the characteristics of permutation groups. Comprehending these attributes facilitates the examination of the configuration and conduct of permutation groups.

5.4 Keywords

- Permutation Group
- Permutation
- Symmetric Group
- Cycle Notation
- Cycle Structure
- Order
- Generators

5.5 Self Assessment questions

1. Define a permutation group and explain what it means for a group to be a permutation group.
2. Consider the “symmetric group S4”, which consists of all permutations of the set {1, 2, 3, 4}. What is the order of this group?
3. Explain the concept of cycle notation for permutations and provide an EX of how to represent a permutation in cycle notation.
4. True or False: Every permutation group is finite. Justify your answer.
5. Consider the permutation σ= (1 2 3) (4 5) in S5. What is the order of σ?

5.6 Case Study

In computer security, Role-Based Access Control (RBAC) is a widely used model for managing access to resources within an organization. RBAC assigns permissions to users based on their roles, rather than directly assigning permissions to individual users. Permutation groups can be utilized to represent and manage RBAC policies efficiently.

Question: Consider a large organization with multiple departments, each containing various employees with different roles and responsibilities. The organization wants to implement an RBAC system to manage access to sensitive information and resources.

5.7 References

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. Wiley.
2. Robinson, D. J. S. (1996). *A course in the theory of groups* (2nd ed.). Springer.

Unit – 6

Cosets and Lagrange's Theorem

Learning objectives

When learning about cosets and Lagrange's theorem in group theory, the following are usually the learning objectives:

- Comprehending Cosets
- Lagrange Theorem
- Use Cases
- Explanations in general
- Verification Methods

Structure

6.1 Cosets

Definition

Let $(G,*)$ be a group, H a subgroup of G, and $g \in G$.

- The left coset of H by g is $gH := \{g*h : h \in H\}$.
- The right coset of H by g is $Hg := \{h*g : h \in H\}$.

We write □:□ for the set of left cosets of H by elements of G

so :□={□□:□∈□}, and |□:□| use for its size.

Similarly, we write □:□ is the set of right cosets of the set H by elements of G.

Ex :

- The 3-cycle $(1,2,3)\in S_4$ has order 3, so $H=\langle(1,2,3)\rangle$ is equal to $\{e,(1,2,3),(1,2,3)^2=(1,3,2)\}$.
- Then $(1,2)H=\{(1,2),(1,2)(1,2,3),(1,2)(1,3,2)\}=\{(1,2),(2,3),(1,3)\}$
  $H(1,2)=\{(1,2),(1,2,3)(1,2),(1,3,2)(1,2)\}=\{(1,2),(1,3),(2,3)\}$.
  So in this case, $(1, 2)\ H=H\ (1, 2)$.
- The 2-cycle $(1,2)\in S_3$ has order 2, so $H:=\langle(1,2)\rangle$ is equal to $\{e,(1,2)\}$. Then
  $(2, 3)H=\{(2,3),(2,3)(1,2)\}=\{(2,3),(1,3,2)\}$
  $H(2,3)=\{(2,3),(1,2)(2,3)\}=\{(2,3),(1,2,3)\}$ So in this case $(2,3)H\neq H(2,3)$.

6.2 Lagrange's Theorem

Theorem (Lagrange's Theorem)

Let G be a finite group and let H be a subgroup. Then $|□|=|□:□||□|=|□:□||□|$. In particular, the order of H divides the order of G.

Proof.

Let the distinct left cosets of H in G be $□_1□,\ldots,□$, so $□=|□:□|$. The left cosets of H are the equivalences classes for an equivalence relation ~ on G. Therefore they are a partition of G, and $|□|=|□_1□|+\cdots+|□_□□|$. Since $|g_iH|=|H|$ by Lemma we get $|□|=□|□|=|□:□||□|$. The result for right cosets is similar.

Or

Let H be any subgroup with an order 'n' of a finite group G of order m. Let us consider the coset breakdown of G with respect to H. Now considering that each coset of aH comprises n different elements.

Let H = {h1, h2… hn}, then ah1, ah2… ahn are the n number of distinct members of aH.

Suppose, ahi=ahj⇒hi=hj be the cancellation law of G. Now G is a finite group, so the number of discrete left cosets will also be finite, say p. So, the total number of elements of all cosets is np which is equal to the total number of elements of G. Hence, m=np

p = m/n

This shows that n, the order of H, divides m i.e., is a divisor of m, the order of the finite group G. We also see that the index p is also a divisor of the order of the group.
Hence, proved, |G| = |H|

6.3 Summary

Basic ideas in group theory, a subfield of abstract algebra, include cosets and Lagrange's Theorem. Cosets allow a group to be divided into discrete subsets, and Lagrange's theorem provides a basic correspondence between the orders of subgroups and the parent group's order. This theorem is fundamental to algebraic structures, with wide applications ranging from group theory and other fields.

6.4 Keywords

- Coset
- Left Coset
- Right Coset
- Partition
- Index
- Lagrange's Theorem

6.5 Self Assessment questions

1. Define a left coset and a right coset of a subgroup H in a group G.
2. Explain how cosets partition a group and discuss whether two cosets can overlap.
3. Compute left and right cosets of a given subgroup in a specific group.
4. State Lagrange's theorem and explain its significance in group theory.
5. Apply Lagrange's theorem to determine the possible orders of subgroups in a finite group.

6.6 Case Study

In modern cryptography, understanding the structure of finite groups is crucial for designing secure encryption algorithms. Lagrange's theorem plays a significant role in analyzing the security and efficiency of cryptographic protocols.

Question: A group of cryptographers is tasked with designing a new cryptographic algorithm based on group theory principles. They want to ensure that the algorithm is secure and resistant to attacks based on mathematical properties of groups.

6.7 Reference

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. Wiley.
2. Robinson, D. J. S. (1996). *A course in the theory of groups* (2nd ed.). Springer.

Unit - 7

Isomorphism

Learning objectives

- The idea of isomorphism is used in many disciplines, including chemistry, computer science, and mathematics.
- Recognize the meaning of isomorphism across vector spaces, fields, rings, groups, and graphs, among other mathematical structures.
- Discover the formal methods for demonstrating the isomorphism of two structures.
- Examine the characteristics of order, structure, and algebraic features that are maintained under isomorphism.
- Solve issues in graph theory, linear algebra, abstract algebra, and other areas of mathematics by using the idea of isomorphism.
- Know the importance of isomorphism in representation and modeling of mathematics.

Structure

7.1 Definition

An isomorphism is a mapping from one set to another in modern algebra that conserve the binary associations between the elements of the sets. The set of natural numbers can be transfer onto the set of even natural numbers, for EX, by multiplying each natural number by two.

Let A and B be two sets with elements a_n and b_m.

Then "*" denote the corresponding binary operations, which act on any two members a set. The sets are isomorphic and f and its inverse are isomorphisms if there is a mapping f such that $f(a_j * a_k) = f(a_j) * f(a_k)$ and its inverse mapping f^{-1} such that $f^{-1}(b_r * b_s) = f^{-1}(b_r)$ — $f^{-1}(b_s)$.

If the both sets A and B are the same, then f is called an automorphism.

7.2 Direct Products

In my book, I have a theorem that says the following:

Let □ be a group. If $□_1, □_2$ are subgroups such that:

- $□_1, □_2 ◅ □$
- $□_1 □_2 = □$
- $□_1 ∩ □_2 = \{□□\}$

Then $□ ≅ □_1 × □_2$

Later, there is a remark that says that the converse of the theorem also holds. So, I suppose this means, that if we have that $□ ≅ □_1 × □_2$ for subgroups $□_{1,2}$, then the three conditions listed above hold.

The 'proof' goes as follows:

If $□ = □_1 × □_2$, then $□ = □_1 □_2$ with $_1 = □_1 × \{□□_2\}$ and $H_2 = \{□□_1\} × □_2$. The groups $□_{1,2}$ are normal in □ and $□_1 ∩ □_2 = \{□\}$

7.3 Summary

A term Isomorphism used in several fields, such as computer science, chemistry, and mathematics. Fundamentally, isomorphism characterizes a structural resemblance between two things in which despite variations in representation or appearance, the fundamental characteristics and connections between them stay the same.

In mathematics, mappings between mathematical structures like groups, rings, and graphs are common EXs of isomorphism. A bijective mapping between two structures is said to be isomorphic if it maintains the essential characteristics and connections between them.

7.4 Keywords

- Structure-preserving mappings
- Mathematical structures
- Graphs, networks
- Bijective mapping
- Algebraic properties

7.5 Self Assessment questions

1. Define isomorphism and explain its significance in mathematics.
2. What are the key properties preserved under isomorphism between mathematical structures?
3. Provide EXs of isomorphic structures in mathematics, such as groups, rings, or graphs.
4. How do you formally prove that two mathematical structures are isomorphic?
5. Explain how the concept of isomorphism is applied in computer science, particularly in the context of data structures and algorithms

7.6 Case Study

A multinational corporation (MNC) operates in multiple countries and relies heavily on its network infrastructure for communication, data transfer, and collaboration. Ensuring the security of its network infrastructure is paramount to protect sensitive corporate data and maintain business continuity.

Question: The MNC faces the challenge of securely transmitting sensitive data between its branches offices located in different countries. Traditional encryption methods are not sufficient due to the diverse regulatory requirements and potential vulnerabilities associated with centralized encryption systems. Fomulate.

7.7 References

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. Wiley.
2. Robinson, D. J. S. (1996). *A course in the theory of groups* (2nd ed.). Springer.

CHAPTER- 8

Normal Subgroups and Factor Groups

Learning objectives

- Understand the difference between a normal subgroup and a subgroup.
- Explore the properties of normal subgroups, such as closure under conjugation by elements of the group.
- Explore the properties of quotient groups, including the group operation and the relationship between elements of the quotient group and cosets.

Structure

8.1 Factor Groups and Normal Subgroups

Let □ be a group and □ its **normal subgroup**. Now, let □ be a subgroup of □/□. To prove that □=□/□ for some subgroup □ of □ that contains □.

Given a normal subgroup □, we have the canonical projection □:□→□/□. Let □ be a subgroup of □/□. Then □=□$^{-1}$ (□) is a subgroup of □. □∈□, hence □$^{-1}$ (□) =□⊆□. So, □ is a normal subgroup of □.

Ex 1:

If □ be an abelian group the prove that Every subgroup □ of □ is a normal subgroup.

Solution

We know, *h*=*h*□ for all □∈□ and *h*∈□,

Then, gH=Hg.

Theorem

Let N be a normal subgroup of a group G. The cosets of N in G form a group G/N of order [G: N].

Proof

Here we use G /N, the group operation is (aN)(bN)=abN. Group multiplication must be demonstrated to be well-defined, meaning it must be unaffected by the selection of a coset representative. Given cN=dN and aN-bN. We have to demonstrate that.

$(aN)(cN)=acN=bdN=(bN)(dN)$.

Then $a=bn_1$ and c $=dn_2$ for some n_1 and n_2 in N. Hence,

$$acN=bn_1dn_2N$$
$$=bn_1dN$$
$$=bn_1Nd$$
$$=bNd$$
$$=bdN.$$

The remainder of the theorem is easy: $eN=N$ is the identity and $g^{-1}N$ is the inverse of gN. The order of G/N is, of course, the number of cosets of N in G.

8.2 The Simplicity of the Alternating Group

Z_p is the class of all simple group instances when p is prime. Since these groups don't have any appropriate subgroups other from the identity-only subgroup, they are trivially simple. It is more difficult to locate other instances of simple groupings. On the other hand, for n≥5, we can demonstrate that the alternate group, An, is simple.

Lemma

Prove that the alternating group A is generated by 3- cycles for n≥3

Proof

First of all take 3-cycles lead to An.

Since (a, b) = (b,a)

(a, b)(a,c)=identity

= (a, c, b) (a, c, d)

= (a, c, b).

8.3 Summary

Normal subgroups and quotient groups are powerful tools in group theory, providing a framework for understanding group structure and symmetries. They have applications across various fields of

mathematics and play a crucial role in theoretical and applied research. Understanding these concepts is essential for students and researchers in algebra, cryptography, and related areas of mathematics.

8.4 Keywords

- Subgroup
- Conjugation
- Invariant
- Quotient group
- Coset
- Factorization

8.5 Self-Assessment questions

1. What is a normal subgroup?
2. How do you determine if a subgroup is normal in a group?
3. Define the factor group (or quotient group).
4. What role does a normal subgroup play in the formation of a factor group?
5. Explain the significance of cosets in the context of factor groups.
6. What is the relationship between the order of a normal subgroup and the order of the factor group?
7. State and explain Lagrange's theorem as it relates to factor groups.
8. How are factor groups used to study the structure of a group?
9. Can you provide an EX of a normal subgroup and its corresponding factor group?
10. What is the significance of the isomorphism theorems in the context of factor groups?

8.6 Case Study

Normal subgroups and factor groups are fundamental concepts in abstract algebra, playing a pivotal role in understanding group structure and symmetry. This case study explores their significance through an EX in the context of group theory.

Consider the dihedral group □$_6$, the group of symmetries of a regular hexagon. Let □denote a clockwise rotation by □/3 and□denote a reflection across a diagonal. We will examine the normal subgroups and factor groups of □$_6$ to gain insights into its structure.

8.7 References

1. Dummit, D. S., & Foote, R. M. (2004). Abstract Algebra (3rd ed.). Wiley.
2. Herstein, I. N. (2003). Topics in Algebra (2nd ed.). Wiley.

Unit - 9

Homomorphism

Learning objectives

- Understand the key properties of homomorphisms, such as preserving the group operation.
- Explore how homomorphisms arise in different mathematical structures, such as rings, fields, and vector spaces.
- Explore conditions under which a homomorphism is injective or surjective.

Structure

9.1 Group Homomorphisms

A **group homomorphism** is a function between two groups that respects the group structure. Specifically, if th binary composition of two sets (G,&) and (H,$*$) are groups, then a function $\phi: G \rightarrow H$ is called a homomorphism if for all $a,b \in G$:

$\phi(a\&b)=\phi(a) * \phi(b)$

i.e. image of the product of two elements under the composition of homomorphism is equal to the product of the images of the two elements.

Properties

1. Preservation of Identity: A group homomorphism maps the identity element of G to the identity element of HHH. If eG is the identity in G and eH is the identity in H, then

$$\phi(eG)=eH.$$

2. Preservation of Inverses: A group homomorphism maps inverses to inverses. For every $a \in G$,

$$\square(\square^{-1}) = \square(\square)^{-1}$$

Examples

1. **Trivial Homomorphism**: The map ϕ:G→H defined by $\phi(g)=eH$ for all g∈Gg is a homomorphism. This is called the trivial homomorphism.
2. **Identity Homomorphism**: The map "ϕ:G→G "defined by $\phi(g)=g$ for all g∈G is a homomorphism is called the identity homomorphism.
3. **Inclusion Homomorphism**: If H is a subgroup of G, the inclusion map ι:H→G defined by $\iota(h)=h$ for all h∈H is a homomorphism.
4. **Determinant**: The determinant function det:GL(n,R)→R^*, where GL(n,R) is the group of n×n invertible matrices with real entries, is a homomorphism.

9.2 The Isomorphism Theorems

Let □ be a group. Let □ ◃ □. Then a natural homomorphism exists from □ to □/□, given by □↦□□.

First Isomorphism Theorem: Let $\phi:G\to G'$ be a group homomorphism. Let E be the subset of G that is mapped to the identity of G'. E is called the kernel of the map ϕ. Then $E \triangleleft G$ and $G/E \cong im\phi$.

An automorphism is an isomorphism from a group G to itself. Let $g\in G$. Then the map that sends $a\in G$ to $g^{-1}ag$ is an automorphism. Automorphisms of this form are called inner automorphisms, otherwise they are called outer automorphisms. Note that all inner automorphisms of an abelian group reduce to the identity map.

Second Isomorphism Theorem: Let G be a group. Let $H \triangleleft G$. If A is any subgroup of G, then $H\cap A$ is normal and $A/(H\cap A)\cong HA/H$

Proof: Let $A= \{1,a_1,a_2,..\}$. Then the image of A under the natural map from G to G/H is $HA=H\cup Ha_1\cup Ha_2\cup....$ Now HA is a subgroup by the Product Theorem because $HA=AH$ since H is normal, and H is normal in HA, thus $HA/H=\{H,Ha_1,Ha_2,...\}$

Lastly, the kernel of the natural map from G to G/H when restricted to A is clearly $H\cap A$, and applying the first isomorphism theorem proves the result.

Third Isomorphism Theorem: If $H \triangleleft G$ and $H \triangleleft A \triangleleft G$ then $A/H \triangleleft G/H$ and $G/HA/H \cong G/A$. Conversely, every normal subgroup of G/H is of the form A/H for some $H \triangleleft A \triangleleft G$.

Proof: Consider the map from $G/H \to G/A$ that sends Hx to Ax. The map is well-defined because $Hx=Hy$ implies $xy-1 \in H \subset A$ whence $Ax=Ay$.This map is homomorphic because $HxHy=Hxy$ is mapped to $Axy=AxAy$. The kernel of the map consists of all elements of G/H that get mapped to A, in other words, elements of the form Hx with $Ax=A$. This happens if and only if $x \in A$, thus the kernel consists of the cosets of the form Ha for $a \in A$. That is, the kernel is precisely A/H. By the first isomorphism theorem, A/H is therefore normal in G/H and we have $G/HA/H \cong G/A$.Conversely, suppose $A'=\{H, Ha_1, Ha_2, \ldots\}$is a normal subgroup of G/H. Then we know that $A=H \cup Ha_1 \cup Ha_2 \cup \ldots$ is a subgroup of G, and it remains to show A is normal. Since A' is normal, we have for all $x \in G$, $\in A, HxHaHx_{-1}=Ha'$for some $a' \in A$. In particular, by picking the identity for the first and third occurrences of H in the equation, $xHax^{-1} \subset Ha'$ for some $a' \in A$, and hence $xAx^{-1} \subset H \cup Ha_1 \cup Ha_2 \cup \ldots \subset A$. Swapping x with its inverse gives the reverse inclusion $xAx-1 \supset A$, thus $A=x-1Ax$, that is, A is normal.

9.3 Summary

Homomorphism are fundamental tools in algebraic structures, providing a way to study and compare different objects based on their algebraic properties. They help reveal the underlying structure and symmetries of mathematical systems, leading to deeper insights and discoveries in mathematics and its applications.

9.4 Keywords

- Group Theory
- Kernel
- Injective
- Surjective
- Isomorphism

9.5 Self-Assessment questions

1. What is a homomorphism in abstract algebra?
2. How does a homomorphism preserve the group operation?

3. Define the kernel of a homomorphism.
4. What is the significance of the image of a homomorphism?
5. Explain the difference between an injective and a surjective homomorphism.
6. What is an isomorphism between groups?
7. State the First Isomorphism Theorem and its significance.
8. Can you provide an EX of a homomorphism between two groups?
9. How do homomorphisms relate to quotient groups?
10. In what other mathematical structures are homomorphisms defined, besides groups?

9.6 Case Study

In cryptography, secure multiparty computation allows multiple parties to jointly compute a function over their private inputs without revealing these inputs to each other. Homomorphic encryption enables computations to be performed on encrypted data without decrypting it, making it an essential tool for MPC protocols.

Consider a scenario where several voters wish to conduct a private election without revealing their votes to anyone else. Homomorphic encryption can be used to achieve this while ensuring the integrity and confidentiality of the voting process.

9.7 References

1. Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University.
2. Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes.

Unit - 10

Matrix Groups and Symmetry

Learning objectives

- Explore the properties of matrix groups, including closure, associativity, identity element, and inverse element.
- Understand how these properties are verified in the context of matrix operations.
- Investigate specific applications of matrix groups in geometry, physics, and other fields.

Structure

10.1 Matrix Groups

A group where the elements are square matrices, the group inverse is just the matrix inverse, and the group multiplication law is matrix multiplication. A unitary matrix group is the same as any other matrix group.

Prior to studying matrix groups, we need to review some fundamental concepts from linear algebra. A linear transformation is among the most basic concepts in linear algebra.

A **linear transformation or linear map** $T: R^n \rightarrow R^m$ is a mapping of vector addition and scalar multiplication; i.e. vectors x and y in R^n and a scalar $a \in R$,

$$T(x + y) = T(x).T(y)$$

$$T(ay) = aT(y).$$

An m x n matrix with entries in R represents a linear transformation from R^n to R^m. If we write vectors $x = (x_1, ..., X_n)$ and $y = (y_1 \ldots\ldots, Y_n)$ in R^n as column matrices, then an $m \times n$ matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \ldots\ldots & a_{1n} \\ a_{21} & a_{22} \ldots\ldots & a_{2n} \\ \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} \ldots\ldots & a_{mn} \end{pmatrix}$$

maps the vectors to R^m linearly by matrix multiplication. Observe that if α is a real number, $A(x+y) = Ax + Ay$ and $\alpha Ax = A(\alpha x)$, where $\begin{pmatrix} x_1 \\ x_1 \\ x_n \end{pmatrix}$. We will often abbreviate the matrix A by writing (a_{ij}).

Key Types of Matrix Groups:

1. **General Linear Group GL(n,F):**
    - The general linear group GL(n,F) is the group of all invertible n×n matrices with entries from a field F.
    - **Notation:** GL(n,F)
    - **Properties:** The set of all n×n invertible matrices under matrix multiplication.
      GL(n,F)={A∈ M(n,F)| det(A)≠0}
      where M(n,F) denotes the set of all n×n matrices over F.
2. **Special Linear Group SL(n,F):**
    - The special linear group SL(n,F) is the subgroup of GL(n,F) consisting of matrices with determinant equal to 1.
    - **Notation:** SL(n,F)
    - **Properties:** The set of all n×n matrices with determinant 1.
      SL(n,F)={A∈ GL(n,F)| det(A)=1}
3. **Orthogonal Group O(n)O(n)O(n):**
    - The orthogonal group O(n) is the group of n×n orthogonal matrices.
    - **Notation:** O(n)
    - **Properties:** A matrix A is orthogonal if $A^T \square = \square$, where A^T is the transpose of A and I is the identity matrix.
      O(n)={A∈ GL(n,R)| A^TA=I}
4. **Special Orthogonal Group SO(n):**
    - The special orthogonal group SO(n) is the subgroup of O(n) consisting of matrices with determinant equal to 1.

- **Notation:** SO(n)
- **Properties:** The set of all n×n orthogonal matrices with determinant 1.
  $SO(n)=\{A\in O(n)|\ \det(A)=1\}$

5. **Unitary Group U(n):**
   - The unitary group U(n) is the group of n×n unitary matrices.
   - **Notation:** U(n)
   - **Properties:** A matrix A is unitary if $A* A=I$, where $A*$ is the conjugate transpose of A.
     $U(n)=\{A\in GL(n,C)|\ A* A=I\}$
6. **Special Unitary Group SU(n):**
   - The special unitary group SU(n) is the subgroup of U(n) consisting of matrices with determinant equal to 1.
   - **Notation:** SU(n)
   - **Properties:** The set of all n×n unitary matrices with determinant 1.
     $SU(n)=\{A\in U(n)|\ \det(A)=1\}$

10.2 Symmetry

An isometry or rigid motion in R^n is a distance- preserving function f from R^n to R^n. This means that *f* must satisfy ||f(x)-f(y)||=||x-y|| for all x, y Є R". It is not difficult to show that *f* must be a one-to-one map. By Theorem, any element in (n) is an isometry on R^n; however, (n) does not include all possible isometries on R^n. Translation by a vector x, (x)=x+y is also an isometry; however, T cannot be in O(n) since it is not a linear map.

Our main focus is on isometries in R^2. As a matter of fact, the only isometries in R^2 are the translations, combinations, and rotations and reflections about the origin. For EX, a glide reflection is a translation followed by a reflection (Figure 10.1). In R^n all isometries are given in the same manner. The proof is very easy to generalize.

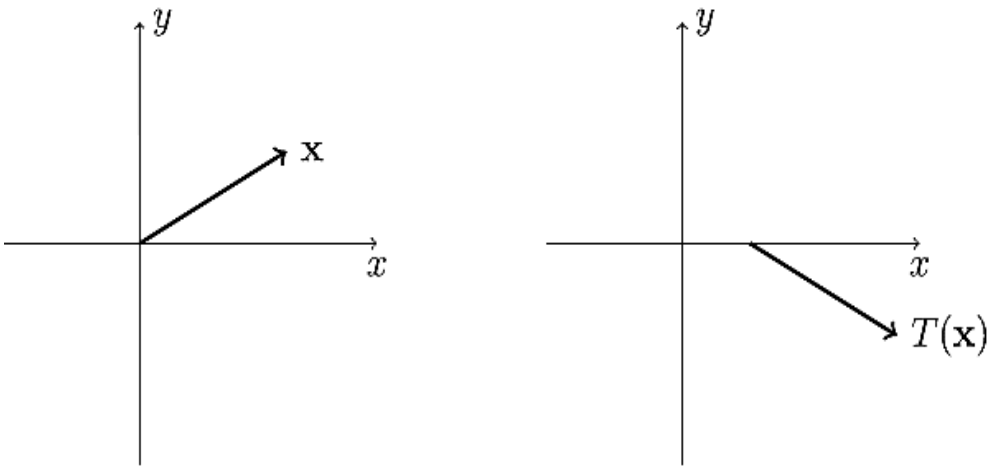


Figure 10.1 Glide reflections

A symmetry group in R^n is a subgroup of the group of isometries on R^n that fixes a set of points $X \subset R^n$. It is important to realize that the symmetry group of X depends both on R^n and on X. For EX, the symmetry group of the origin in R^1 is Z_2, but the symmetry group of the origin in R^2 is O(2).

10.3 Summary

Matrix groups and their applications to symmetry form a fundamental area of study in mathematics and physics. By understanding these groups, we gain insights into the structural and transformational properties of various systems, from geometric shapes to fundamental particles in the universe. This knowledge is crucial for advancements in both theoretical and applied sciences.

10.4 Keywords

1. General Linear Group GL(n, $\mathbb{R}$)
2. Special Linear Group SL(n, $\mathbb{R}$)
3. Orthogonal Group O(n)
4. Special Orthogonal Group SO(n)
5. Unitary Group U(n)

10.5 Self-Assessment questions

1. What is a matrix group?
2. Give an Ex of a matrix group and its application in real-world symmetry.
3. Define the special orthogonal group(3). What does it represent?

4. How do matrix groups preserve symmetry in geometric objects?
5. Explain the significance of determinants in matrix groups like (□,ℝ)and□□(□,ℝ).
6. What role do unitary matrices play in describing symmetries in quantum mechanics?
7. How does representation theory relate to matrix groups and symmetries?
8. What is the difference between a Lie group and a Lie algebra?
9. Give an EX of a group action involving a matrix group and its effect on a geometric object.
10. Why are matrix groups important in studying physical symmetries?

10.6 Case Study

Crystallography is the study of the arrangement of atoms in crystalline solids. Matrix groups play a crucial role in describing the symmetries found in crystal structures, providing insights into their physical and chemical properties.

Crystals exhibit various symmetrical properties due to the repeating arrangement of atoms. Matrix groups help characterize these symmetries, which impact the crystal's physical, mechanical, and optical behavior.

10.7 References

1. Arfken, G. B., Weber, H. J., & Harris, F. E. (2012). Mathematical Methods for Physicists (7th ed.). Academic Press.
2. Hall, B. C. (2015). Lie Groups, Lie Algebras, and Representations: An Elementary Introduction (2nd ed.). Springer.

Unit - 11

The structure of Groups

Learning objectives

- Identify and understand Ex's of groups: Recognize EXs of groups, including familiar groups like integers under addition and non-familiar groups.
- Understand the definition of a group: Define and provide EXs of a group, emphasizing the four key properties (closure, associativity, identity element, and inverse element).
- Define subgroups and identify EXs of subgroups within larger groups.

Structure

11.1 Finite Abelian Groups

A finite abelian group is a group satisfying the following equivalent conditions:

1. It is both finite and abelian.
2. It is isomorphic to a direct product of finitely many finite cyclic groups.
3. It is isomorphic to a direct product of abelian groups of prime power order.
4. It is isomorphic to a direct product of cyclic groups of prime power order.

Properties

As any finite group, a finite abelian group is pure torsion.

Proposition 1: If a finite Abelian group □ has order |□|=□ a prime number, then it is the cyclic group ℤ□.

Proposition 2: If □ is a finite Abelian group and □∈ℕ is a prime number that divides the order |□|, then equivalently

- □ has an element of order □;
- □ has a subgroup of order □.

This is Cauchy's theorem restricted to abelian groups.

Theorem (fundamental theorem of finite abelian groups)

Every finite abelian group is the direct sum of cyclic groups of prime power order (its p-primary groups).

11.2 Solvable Groups

A subnormal series of a group G is a finite sequence of subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

where H_i is H_i+1's normal subgroup. A series is referred to as normal if every subgroup H_i; is normal in G. The number of appropriate inclusions determines the length of a normal or subnormal series.

Ex 1 : Any Series of subgroup of an abelian group is a normal series

Solution

Consider the following series of groups:

$$Z \supset 9Z \supset 45Z \supset 180Z \supset \{0\},$$

$$Z_{24} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}.$$

A subnormal (normal) series $\{K_j\}$ is a ***refinement of a subnormal (normal) series*** $\{H_i\}$ if $\{H_i\} \subset \{K_j\}$. That is, each H_i is one of the K_j.

If all of the component groups in a subnormal series $\{H_i\}$ of a group G are simple, that is, if none of the factor groups in the series include a normal subgroup, then the series is a composition series. If every factor group is simple, then a normal series $\{H_i\}$ of G is a main series.

If every factor group H_i+1/H_i; is abelian and the group G has a subnormal series $\{H_i\}$, then the group is solvable. When we examine Galois theory and the solution of polynomial equations, solveable groups will be crucial.

11.3 Summary

A summary outlines the foundational structure and properties of groups in abstract algebra, providing a framework for deeper study and application.

11.4 Keywords

- Group
- Binary Operation
- Closure
- Associativity
- Identity Element

11.5 Self-Assessment questions

1. Define a group. What are the four key properties that characterize a group?
2. What is an Abelian group? Give an Ex. also.
3. Explain the closure property in the context of groups.
4. What is the identity element in a group?
5. How do you determine if a subset of a group is a subgroup?
6. What is a cyclic group? Provide an EX.
7. Define a group homomorphism. What is its kernel?
8. What does it mean for two groups to be isomorphic?
9. Describe the difference between a left coset and a right coset.
10. State Lagrange’s Theorem. What is its significance in group theory?

11.6 Case Study

Think about "Tech Innovators Inc.," a fictitious business that prides itself on its cutting-edge goods and exciting workplace culture. Numerous teams inside the organization are engaged in various initiatives, and it is crucial to comprehend the ways in which the composition of these teams affects their productivity, unity, and overall success.

Question: How do the diversity and skills of group members at Tech Innovators Inc. impact the group's performance and creativity?

11.7 References

1. Gallian, J. A. (2017). Contemporary Abstract Algebra (9th ed.). Cengage Learning.
2. Rotman, J. J. (1995). An Introduction to the Theory of Groups (4th ed.). Springer-Verlag.

CHAPTER-12
Group Actions

Learning objectives

- Explore EXs of group actions, such as permutation actions and matrix actions.
- Study properties of group actions, including the identity action, inverse action, and compatibility with group multiplication.
- Apply group actions to solve problems in combinatory, geometry, and number theory.

Structure

12.1 Group acting on Sets

Let X be a set and G be a group. A (left) action of G on X is a map G x X ⟶ X given by ((g,x) ⟶ gx, where

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

Under these considerations X is referred to as a G-set. Take note that there is no requirement that X be connected to G in any manner. True, each group G acts on each set X through the trivial action ((g,x)⟶x); yet group actions become more intriguing when the set X is connected to the group in some way.

Ex 1:

Let $G=GL_2(R)$ and $X=R^2$.

Solution

Then G acts on X by left multiplication. If $v \in R^2$ and I is the identity matrix, then $Iv=v$. If A and B are 2×2 invertible matrices, then $(AB)v=A(Bv)$ since matrix multiplication is associative.

Ex 2:

Let G=D4 be the symmetry group of a square. If X={1,2,3,4} is the set of vertices of the square, then we can consider D4 to consist of the following permutations:

{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)}.

Solution

The elements of D4 act on X as functions. The permutation (13)(24) acts on vertex 1 by sending it to vertex 3, on vertex 2 by sending it to vertex 4, and so on. It is easy to see that the axioms of a group action are satisfied.

12.2 The Class Equation

A simple kind of counting argument that arises from decomposing a finite G-set into a union of its orbits is known as a class equation, class formula, or orbit decomposition formula. There are several basic uses of this in group theory.

Statement

Let G be a group and let A be a G-set (given by a homomorphism G→homset (A,A) of monoids, with which is associated an action a:G×A→A). Recall that A is connected in the category of G-sets if A is inhabited and the action is transitive; in this case, choosing an element aЄA, there is a surjection of G-sets G→A sending 1→a, and this induces an isomorphism G/Stab(a) ≅ A where Stab(a) is the stabilizer of a and G/Stab(a) is the G-set consisting of left cosets of Stab(a).

More generally, as a coproduct of its linked components, which are commonly referred to as the orbits of the action, every G-set A permits a canonical decomposition. Selecting a representative element ax inside each orbit x indicates that G-sets are isomorphically represented.

$A \cong \sum_{\text{orbits}x} G/\text{Stab}(a_x)$.

By taking G and A to be finite and counting elements, we get an equation of the form

$|A| = \sum_{\text{orbits}x} |G|/|\text{Stab}(a_x)|$

An EX of this equation is referred to as a class equation. Many beneficial results may be obtained by carefully selecting groups G and G-sets A; some EXs of these applications are shown below. These results are frequently obtained in conjunction with number-theoretic reasoning.

Notice that reading the class equation equivalently as

$\sum_{\text{orbits}x} 1/|\text{Stab}(ax)| = |A|/|G|$

it expresses the groupoid cardinality of the action groupoid of G acting on A.

Applications

Centers of □-groups

Let p be a prime; recall that a p-group is a finite group whose order is a power of p. A basic structural result is the following.

Proposition 1. A non-trivial p-group G has a nontrivial center (G).

Proof. Let G act on itself by the conjugation action $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$. In this case an orbit $\text{Orb}(h)$ is usually called the conjugacy class of h, and $\text{Orb}(h)$ is trivial (consists of exactly one element h) iff h belongs to $Z(G)$. In any case $|\text{Orb}(h)| = |G|/|\text{Stab}(h)|$ divides $|G| = p^n$, and therefore p divides $|\text{Orb}(h)|$ if h is noncentral. In this case the class equation takes the form

$|G| = |(G)| + \sum_{\text{nontrivialorbits}x} |G|/|\text{Stab}(a_x)|$

and now since p divides $|G|$ as well as each term in the sum over nontrivial orbits, it must also divide $|Z(G)|$. In particular, (G) has more than one element.

It follows by induction that p-groups are solvable, since the center is a normal subgroup and the quotient GG) is also a p-group. Since a group obtained from an abelian group by repeated central extensions is nilpotent, p-groups are in fact nilpotent

Number of fixed points

An elementary observation that is frequently useful is that the number of fixed points of an involution on a finite set S has the same parity as S. This is a statement about Z(2)-sets; we

generalize this to a statement about G-sets for general p-groups G. (Again, a fixed point of a G- set is an element whose orbit is a singleton.)

Proposition : If G is a p-group acting on a set A, then
|A|=|Fix(A) modp.
As special cases, if there is just one fixed point, then |A|=1modp, and if p divides |A|, then p divides |Fix(A)|.

Proof. The class equation takes the form

$$|A|=|\mathrm{Fix}(A)|+\sum_{\text{nontrivialorbits}x}|G|/|\mathrm{Stab}(a_x)|$$

where p divides each summand over nontrivial orbits on the right, since G is a p-group. Now reduce mod p.

12.3 Summary

Group actions provide a powerful tool for understanding the structure of groups and their interactions with other mathematical objects. They play a central role in group theory and have diverse applications in many areas of mathematics.

12.4 Keywords

- Group action
- Permutation
- Transformation
- Set
- Group

12.5 Self-Assessment questions

1. What is a group action?
2. How does a group act on a set?
3. What are orbits in the context of group actions?
4. Define stabilizer in a group action.
5. What is the identity element's role in a group action?
6. Explain the concept of a transitive group action.
7. What does it mean for a group action to be faithful?

8. Define a free group action.
9. What is the orbit-stabilizer theorem?
10. How are group actions used to study symmetry?

12.6 Case Study

Symmetry plays a fundamental role in various branches of science and engineering, including chemistry, physics, and computer graphics. Understanding the symmetries present in an object or structure is crucial for analyzing its properties and behavior. Group actions provide a powerful framework for studying symmetry transformations and their applications. This case study explores the use of group actions in symmetry analysis, focusing on the symmetries of geometric shapes.

Objective: To demonstrate how group actions can be used to analyze the symmetries of geometric objects and structures, and to illustrate their practical applications in symmetry analysis.

12.7 References

1. Serre, J. P. (2003). Linear Representations of Finite Groups (Vol. 42). Springer Science & Business Media.
2. Fulton, W., & Harris, J. (2004). Representation Theory: A First Course. Springer Science & Business Media.

CHAPTER-13

The Sylow Theorems

Learning objectives

- Review foundational concepts in group theory, including groups, subgroups, normal subgroups, and group homomorphisms.
- Apply the Sylow Theorems to determine the number and structure of Sylow subgroups in various finite groups.
- Apply the Sylow Theorems to determine the number and structure of Sylow subgroups in various finite groups.

Structure

13.1 The Sylow Theorems

Assume that p is a prime that divides G, a finite group of order n. In this case, $n=p^f u$, where p does not divide u. Remember that a p-subgroup of maximal order pf is a Sylow p-subgroup. The existence and conjugacy of Sylow p-subgroups, as well as the fact that their number is $\equiv 1 \mod p$, are basic facts of group theory.

Existence of Sylow □-subgroups:

Theorem If G has order n and p^k is a prime power dividing n, then there is a subgroup of G of order p^k.

Proof. First we show that Sylow subgroups exist. We start by observing that if a group H has a p-Sylow subgroup P, then so does any subgroup G. To prove this, first note that if we let G act on H/P by left translation, then the stabilizer of any element hP is $G \cap hPh^{-1}$, a p-group

since hPh^{-1} is. Then note that since H/P has cardinality prime to p, so must one of its connected components $G/\mathrm{Stab}(a_x)$ in its G-set decomposition

$$H/P \cong \sum_{\text{orbits}x} G/\mathrm{Stab}(a_x),$$

and this makes $\mathrm{Stab}(a_x)$ a p-Sylow subgroup of G.

Then, if G is of order n, apply this observation to the embedding

$$G \hookrightarrow^{\text{Cayley}} \mathrm{Perm}(|G|) \cong S_n \hookrightarrow \mathrm{GL}_n(\mathbb{Z}/(p)) = H$$

where we embed the symmetric group S_n via permutation matrices into the group H of $n \times n$ invertible matrices over $\mathbb{Z}/(p)$. The group H has order $(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})$, with maximal p-factor $p^{n(n-1)/2}$. It thus has a p-Sylow subgroup given by unitriangular matrices, i.e., upper-triangular matrices with all 1's on the diagonal. Therefore p-Sylow subgroups P exist for any finite group G.

Finally, note that, P is solvable and therefore has a composition series

$\{1\}=P_0 \subset P_1 \subset \ldots \subset P$

where each P_k has order p^k.

Theorem If H is a p-subgroup of G and P is a Sylow p-subgroup, then $g^{-1}Hg \subseteq P$ for some $g \in G$. In particular, all Sylow p-subgroups are conjugate to one another.

Proof. G acts on the set of cosets G/P as usual by left translation, and we may restrict the action to the p-subgroup H. By maximality of P, we see $|G/P|$ is prime to p, ans so, $|\mathrm{Fix}(G/P)|$ is also prime to p. In particular, Fix (G/P) has at least one element, say gP. We infer that $hgP=gP$ for all $h \in H$, or that $g^{-1}hgP=P$ for all $h \in H$, and this implies that $g^{-1}Hg \subseteq P$.

Theorem The number of Sylow p-subgroups of G is $\equiv 1 \mathrm{mod} p$.

Proof. Let Y be the set of Sylow p-subgroups; G acts on Y by conjugation. As all Sylow p-subgroups are conjugate, there is just one orbit of the action, and the stabilizer of an element $P \in Y$ is just the normalizer (P) (by definition of normalizer). Thus $Y \cong G/(P)$ as G-sets.

Restrict the action to the subgroup P. Of course the element $P \in Y$ is a fixed point of this restricted action, and if Q is any other fixed point, it means $xQx^{-1}=Q$ for all $x \in P$, whence $P \subseteq (Q)$. Now: P, are both Sylow p-subgroups of $N(Q)$ and are therefore conjugate to each other (as seen within the group $N_G(Q)$). But Q is already fixed by the conjugation action in its stabilizer (Q), so we conclude $P=Q$. We conclude Fix(Y) has exactly one element.

Corollary: If □ is a group of order □=□^□□ where □ is prime to □, then the number □_□ of □-Sylow subgroups divides □.

Proof. Because □ acts transitively on □-Sylow subgroups, the number □_□ divides |□|=□^□□. We have □□□+□□□□=1 for some integers □,. Since □□ divides both terms of the left side of □□□□+□□□□□=□, it divides □.

The Sylow theorems are routinely used throughout group theory. As a sample application: if □, are distinct primes, with □^2≢1mod□ and □≢1mod□, then any group of order □^2□ is abelian. (For EX, a group of order 2023=7· 17^2 must be commutative.)

We have □_□|□, but □_□≠□, so □□=1. Arguing similarly we have □_□|□^2 but □_□≠□ and □_□≠□^2, so □□=1. The □-Sylow subgroup □ of order □^2 and the □-Sylow subgroup □ of order □ are both abelian. □∩□={1} since □,□ are relatively prime, and □,□ are normal subgroups of □ since □□,□□ are both 1. It follows that □□ is a subgroup of order □^2□, hence □□=□. Thus to prove □ abelian, it suffices to show that if □∈□ and □∈□, then □ and □ commute, i.e., □□□^−1□^−1=1. But by normality of □, the element (□□□^−1)^−1 belongs to □; similarly, the element (□□^−1□^−1) belongs to □, and so □□□^−1□^−1∈□∩□={1}.

13.2 EXs and Applications

Example 1 :

We may ascertain that A_5 has subgroups of orders 2, 3, 4, and 5 by applying the Sylow Theorems. The orders of A_5's Sylow p-subgroups are 3, 4, and 5. The number of Sylow p-subgroups As is precisely given by the Third Sylow Theorem.

Solution

There are either one or six Sylow 5-subgroups in A_5, as the number of Sylow 5-subgroups must divide 60 and also be congruent to 1(mod5). Every subgroup of Sylow 5 is conjugate. If there was just one Sylow 5-subgroup, it would be a normal subgroup of As as it is conjugate to itself. This is not conceivable since As has no normal subgroups; hence, we have identified exactly six unique Sylow 5-subgroups of A_5.

Application

We can demonstrate a number of helpful finite group conclusions thanks to the Sylow Theorems. If certain assumptions hold, we may frequently draw a lot of conclusions about groups of a certain order using them.

Theorem

If p and q are distinct primes with p<q, then every group G of order pq has a single subgroup of order q and this subgroup is normal in.G. Hence, G cannot be simple. Furthermore, if $q \not\equiv 1 (\mathrm{mod} p)$, then G is cyclic.

Ex 2:

Every group of order 1515 is cyclic.

Solution

This is true because 15=5.3 and $5 \not\equiv 1 (\mathrm{mod} 3)$

13.3 Summary

The Sylow Theorems are vital tools in group theory, providing deep insights into the structure and properties of finite groups. They are essential for anyone studying abstract algebra and play a significant role in various mathematical proofs and applications.

13.4 Keywords

- Sylow Theorems
- Sylow p-subgroup
- Prime order
- Conjugate subgroups
- Group theory

13.5 Self-Assessment questions

1. What do The Sylow Theorems state?
2. What is a Sylow p-subgroup?
3. How many Sylow p-subgroups are there in a finite group?
4. What is the significance of conjugacy in the context of The Sylow Theorems?
5. Can you explain the divisibility condition in the third Sylow Theorem?

6. How do The Sylow Theorems contribute to the classification of finite groups?
7. What is the role of The Sylow Theorems in proving the simplicity of certain groups?
8. How are The Sylow Theorems applied in counting subgroups within a finite group?
9. What is the connection between The Sylow Theorems and group actions?
10. Can you provide an EX of how The Sylow Theorems are used to analyze the structure of a specific group?

13.6 Case Study

The Sylow Theorems, a fundamental set of results in group theory, provide insights into the structure of finite groups. Named after the Norwegian mathematician Ludwig Sylow, these theorems offer powerful tools for analyzing group composition and classification. This case study explores the application of The Sylow Theorems in understanding the structure of finite groups and solving problems in various mathematical contexts.

Objective: To demonstrate the practical significance of The Sylow Theorems by applying them to analyze the structure of finite groups and solve specific problems related to group theory.

13.7 References

1. Hungerford, T. W. (1974). Algebra. Springer.
2. Dummit, D. S., & Foote, R. M. (2004). Abstract Algebra (3rd ed.). John Wiley & Sons.

CHAPTER-14

Rings

Learning objectives

- Understand the concept of ideals, including left ideals, right ideals, and two-sided ideals, and their role in ring theory.
- Apply ring theory concepts to solve problems in various fields such as number theory, algebraic geometry, and cryptography.
- Develop the ability to construct and understand proofs related to rings and their properties.

Structure

14.1 Rings

Let R be a non-empty set and let addition (+) and multiplication (.) be two binary operations defined on it. In the event that the following criteria are met, R is considered to constitute a ring with respect to addition (+) and multiplication (.):

1. (R,+) is a commutative group, or an abelian group.
2. The semigroup (R.)

The left distributive law a (b+c) = a.b + a.c and the right distributive property (b+c).a = b.ac.a hold for any three items a, b, and c $\in$ R.

Therefore a non- empty set R is a ring w.r.t to binary operations + and . if the following conditions are satisfied.

1. For all a, b $\in$ R, a+b $\in$ R,

2. For all a, b, c Є R a+(b+c)=(a+b)+c,
3. There exists an element in R, denoted by 0 such that a+0=a for all a R
4. For every a Є R there exists an y Є R such that a+y=0. y is usually denoted by -a
5. a+b=b+a for all a, b Є R.
6. a.b Є R for all a, b Є R.
7. a.(b.c)=(a.b).c for all a, b, c Є R
8. For any three elements a, b, c Є R a.(b+c) =a.b + a.c and (b+c).a =b.ac.a. And the ring is denoted by (R, +, .).

Ex 1: (Z, +) is a commutative group .(Z, .) is a semi-group. The distributive law also holds. So, ((Z, +, .) is a ring.

Ex 2 : The set S = {0, 1, 2, 3, 4} is a ring with respect to operation addition modulo 5 & multiplication modulo 5.

14.2 Integral Domains and Fields

Let's review a few definitions quickly. If □ is a nonzero element in a commutative ring □, and □ is a zero divisor of □ if □∈□ is some nonzero element such that □□=0. If there are no zero divisors for a commutative ring with identity, it is referred to as an integral domain. We refer to an element □ as a unit if it has a multiplicative inverse and is a member of a ring □ with identity. R□ is referred to be a division ring if each nonzero element in it is a unit. A field is a commutative division ring.

Ex 3:

If $i^2=-1$, then the set $Z[i]=\{m+ni:m,n\in Z\}$ forms a ring known as the Gaussian integers. It is easily seen that the Gaussian integers are a subring of the complex numbers since they are closed under addition and multiplication. Let $\alpha=a+bi$ be a unit in Z[i].$Z[i]$. Then $\alpha^{-}=a-bi$ is also a unit since if $\alpha\beta=1$, then $\alpha^{-}\beta^{-}=1$. If $\beta=c+di$,

Solution

Then $1=\alpha\beta\alpha^{-}\beta^{-}=(a^2+b^2)(c^2+d^2)$.

Therefore, a^2+b^2 must either be 1 or −1; or, equivalently, $a+bi=\pm1$ or $a+bi=\pm i$. Therefore, units of this ring are ±1 and ±i; hence, the Gaussian integers are not a field. We will leave it as an exercise to prove that the Gaussian integers are an integral domain.

Ex 4:

The set Q(√2)=(a+b√2:a,bEQ} is a field. The inverse of an element a+b√2 in Q(√2) is

Solution

$(a/(a^2-2b^2))+(-2b\sqrt{2}/a^2-2b^2)$.

We have the following alternative characterization of integral domains.

Theorem

Every finite integral domain is a field.

Proof

Let D be a finite integral domain and D^* be the set of nonzero elements of D. We must show that every element in D^* has an inverse. For each $a \in D^*$ we can define a map $\lambda_a: D^* \to D^*$ by $\lambda_a(d)=ad$. This map makes sense, because if $a \neq 0$ and $d \neq 0$, then $ad \neq 0$. The map λ_a is one-to-one, since for $d_1, d_2 \in D^*$,

$$ad_1=\lambda_a(d_1)=\lambda_a(d_2)=ad_2$$

implies $d_1=d_2$ by left cancellation. Since D^* is a finite set, the map λ^a must also be onto; hence, for some $d \in D^*$, $\lambda_a(d)=ad=1$. Therefore, aa has a left inverse. Since D is commutative, dd must also be a right inverse for a. Consequently, D is a field.

We write r+……..+r (n times) as nr for any nonnegative integer n and any element r in a ring R. A ring R's characteristic is defined as the smallest positive number n that ensures nr=0 for every r Є „ R. In the event that such an integer is nonexistent, R's characteristic is defined as 0.We'll refer to R by its feature.

Ex 5:

For every prime p, Z_p is a field of characteristic p.

Solution

According to Proposition, Z_p is a field since each nonzero element has an inverse. Since the order of every nonzero element in the abelian group Z_p equals p, if an is any nonzero element in the field, then pa=0.

Theorem

The characteristic of an integral domain is either prime or zero.

Proof

Let D be an integral domain and suppose that the characteristic of D is nn with $n\neq 0$. If n is not prime, then $n=ab$, where $1<a<n$ and $1<b<n$. By Lemma, we need only consider the case $n1=0$. Since

$$0 = n1 = (ab)1 = (a1)(b1)$$

and there are no zero divisors in D, either $a1=0$ or $b1=0$. Hence, the characteristic of D must be less than n, which is a contradiction. Therefore, n must be prime.

14.3 Ring Homeomorphisms and Ideals

Let □ and □′ be rings and let □:□↦□′ is called a ring homomorphism and □ an ideal of □. Prove that [□] is an ideal of [□], and now we have take an example to show that [□] need not be an ideal of □′.

Let □′ be an ideal of either [□] or R', and show that $□^{-1}$[□′] is an ideal of R.

I just started learning ideals so I am having a lot of trouble with this. I know that the kernel of □ is an ideal, but I don't know how I can use this.

In order to show that (□) is an ideal we must show that it is an additive group and closed under multiplication in (□)

Showing (□) is an additive group

Identity

So as 0∈ □ and □ is a ring homomorphism we have that (0)=0∈ □(□)

Closure

Now take □,∈ □(□) then by definition of □(□) there must exists □,□∈ □ such that □(□)=□ and □(□)=□. Now as □ is an ideal we have that □+□∈ □ and so □(□+□)∈ □(□), then as □ is a ring homomorphism we have that □(□+□)=□(□)+□(□)=□+□∈ □(□).

Inverses

If we have □∈(□) then by definition there must be an □∈ □ such that □(□)=□ now as □ is an ideal we have that $□^{-1}$∈ □ and so □($□^{-1}$)∈ □(□). Now as □ is a ring homomorphism we have that ($□^{-1}$) =$(□)^{-1}$=$□^{-1}$∈ □(□)

So we have that (□) is an additive subgroup of (□)

Now to show that it is an ideal we have to show that if we have □∈(□) then □□(□)⊂□(□) and □(□)□⊂□(□)

Showing (□) is **closed under multiplication** of (□)

Now if□∈ (□) then there must be an □′∈ □ such that (□′)=□

Then as $r'□⊂□$ we have that (□′□) =(□′)□(□) ⊂□(□) (same argument for □ on the right)

Ex of image of an ideal is not an ideal

We can define the inclusion map □:□→□ and then take an ideal in □ say 3□ then f (3□) is not an ideal in □.

Suppose that it was, then noting that 1∉(3□). But by the definition of ideal we must have, 1/3∈Q, (1/3) ×3∈(3□) which gives a contradiction.

Note: as □ is a field then it has only the two trivial ideals so it follows directly from this.

14.4 Summary

Overall, ring theory provides a unifying framework for studying a wide range of algebraic structures and their applications across mathematics and beyond.

14.5 Keywords

- Ring
- Commutative Ring
- Ring with Unity
- Division Ring
- Field

14.6 Self-Assessment questions

1. What is a ring in abstract algebra?
2. Define a commutative ring.
3. What is the identity element in a ring with unity?
4. Give an EX of a division ring.
5. What is an ideal in a ring?
6. Explain the difference between a left ideal and a right ideal.
7. What is a quotient ring?
8. Define a ring homomorphism.

9. What is the kernel of a ring homomorphism?
10. Give an EX of a polynomial ring.

14.7 Case Study

Cryptography is the science of securing communication. Modern cryptographic systems often rely on complex mathematical structures, including ring theory. This case study explores how ring theory is applied in cryptographic algorithms, specifically focusing on the construction and analysis of cryptographic schemes using polynomial rings.

Objective: To understand the role of ring theory in designing secure cryptographic algorithms, particularly those based on polynomial rings, and to explore their application in public-key cryptography.

14.8 References

1. Herstein, I. N. (1999). Abstract Algebra (3rd ed.). John Wiley & Sons.
2. Hungerford, T. W. (2003). Algebra (Graduate Texts in Mathematics, Vol. 73). Springer.