P R E F A C E

This book on **'Abstract Algebra'** has been specially written as per latest syllabus of **'Abstract Algebra'** in **CSIR NET MATHEMATICAL SCIENCE EXAM**.

In addition this book will prove very useful for students preparing for various national level competitive examinations such as SET, GATE, TIFR, NBHM, IIT, JNU, DU, BHU, HCU, Deemed, Private, State, and Central University PhD Entrance Exams.

The author possesses a very long and rich experience of teaching mathematics and has first-hand experience of the problems and difficulties that students generally face.

The salient features of this book are:

1. The matter has been presented in a simple and lucid language so that student themselves shall be able to understand the concepts given and solution of the problems.
2. Each chapter open with necessary definitions and proofs of a standard results and theorems. These in turn are followed by solved examples which has been classified in various types and methods. This classification will help the students to revise the subject matter at the time of examination without losing any confidence.
3. Care has been taken not to omit important steps so that student can understand everything by themselves. Furthermore, a set of unsolved assignments is given in end of each chapter to instill confidence in the students.
4. The presentation in book is uncluttered, with plenty of clear outline diagrams.

In view of this special features, it is sincerely hoped that this book will surely serve its purpose.

All valuable suggestions for further improvement of the book will be highly appreciated.

A C K N O W L E D G E M E N T

Writing this book **"Abstract Algebra"** has been an incredible journey. All the chapters have taken a final shape after endless inputs of time and effort. Though many colleagues assisted me in compiling this book, I first of all would like to thank all students at Institute for advanced Studies (IFAS), who have helped me to learn and implement the concepts and ideas of Abstract Algebra in its simplest form.

I would like to specially mention the effort made by Mr. Radheshyam Choudhary, Director IFAS Publications, who extended immense support in myriad ways for bringing out the book in its present form.

My special thanks to Mr. Manoj Gunjal, Mr. Rohit Muranjan, Mr. Vikas Yadav, Mr. Mahesh Shelke, Mr. Raja Raman, Mr. Gaurav Kumar, Mr. Omkar Girkar and Mr. Md. Sohail for suggestions and providing valuable contributions. This book is a team effort, and producing it would be impossible without outstanding people of IFAS publication. I am thankful to the team at IFAS Publication, It has been a pleasure to work with Vikendra Mehta and Kuldeep Singh Rathore who took great care during the copy-editing and production processes of this book and finally my humble greetings to all who put their significant efforts and are unmentioned.

INDEX

SECTION–I

GROUP THEORY

Unit. No.	Contents	Page No.
1.	**SETS, RELATIONS AND FUNCTIONS**	
1.1	Definition of Set	01
1.2	Representation of a Set	01
1.3	Classification of Sets	01
1.4	Definition of Subset	01
1.5	Power Set	02
1.6	Universal Set	02
1.7	Intersection of two Sets	02
1.8	Difference of two Sets	02
1.9	Complement of a Set	02
1.10	Union of two Sets	02
1.11	Symmetric Difference of two Sets	02
1.12	Cartesian product of two Sets	03
1.13	Relations	03
1.14	Types of Relations	03
1.15	Equivalence Relation	04
1.16	Function	04
2.	**NUMBER THEORY**	
2.1	Congruence Relation of $\mathbb{Z}$	06
2.2	Diophantine Equation	06
3.	**GROUPS AND SUBGROUPS**	
3.1	Definition of Binary Operation	18
3.2	Definition of Algebraic Structure	18
3.3	Definition of Associative Binary Operation	18
3.4	Definition of Existence of Identity Element	18
3.5	Definition of Existence of Inverse Element	19
3.6	Definition of Abelian Group	19
3.7	Definition of Non-Abelian Group	19
3.8	Definition Subgroup	21
3.9	Definition Coset	21
3.10	Lagrange's Theorem	22
3.11	Product of Subgroups	22

3.12 Definition Homomorphism 22
3.13 Definition Cyclic Group 23
4. GROUPS AND SUBGROUPS
4.1 Klein's Four Group (K_4) 28
4.2 Group of Bijection or Symmetric Group 28
4.3 Permutation Group on 3-Symbols or S_3 30
4.4 Permutation Group on 4-Symbols or S_4 30
4.5 Quaternion Group 32
4.6 Dihedral Group or D_n(n≥3) 32
4.7 Group of order 2p (p-odd prime) 32
4.8 Group of order pq (p, q prime p<q) 32
4.9 External Direct Product of Groups 32
4.10 Group of Order 8 33
4.11 Group of Non-zero Complex Number ($\mathbb{C}^*$, .) 33
4.12 Group of Rational Number ($\mathbb{Q}$, +) 33
4.13 General Linear Group Gl(n,$\mathbb{F}$) 33
5. CLASS EQATION OF GROUPS
5.1 Definition of Conjugate Element in a Group 36
5.2 Definition of Relation of Conjugacy 36
5.3 Definition of Conjugacy Classes 36
5.4 Definition of Self-conjugate Element 36
5.5 Definition of Centre of a Group 36
5.6 Definition of Centralizer or Normalizer of a in G 36
5.7 Definition of Class Equation 37
5.8 Class Equation of Some Important Groups 37
6. NORMAL SUBGROUPS AND QUOTIENT
6.1 Conjugacy of Subgroups 42
6.2 Normal Subgroups.....42
6.3 Definition of Proper Normal Subgroup 42
6.4 Definition of Simple Group 42
6.5 Quotient Group 43
6.6 Maximal Subgroup 43
7. HOMOMORPHISM
7.1 Some Important definitions and Examples 49
7.2 Properties of Isomorphism and Automorphism 50
7.3 Properties of Homomorphism 52
7.4 Some Important Theorems 52
7.5 Algorithm for counting of Homomorphism from G to G' 53
7.6 Counting of Homomorphism from an Infinite Cyclic Group to any Finite Group 56

7.7 Counting of Homomorphism from Finite Group to Infinite Cyclic Group 56
7.8 Counting of Homomorphism from an Infinite cyclic Group to an Infinite cyclic Group 56
7.9 Counting of Homomorphism from Finite Cyclic Group to any Finite Group 56
7.10 Counting of Homomorphism from Non-Cyclic Groups 56
7.11 Other important Counting of Homomorphism 57

8. SYLOW THEOREMS

8.1 Definition of P-Group 62
8.2 Cauchy's Theorem for Finite Groups 62
8.3 Index Theorem 62
8.4 Definition of Embedded Group 62
8.5 Sylow Theorems 62
8.6 Internal Direct Product 63
8.7 Fundamental Theorem of Finite Abelian Groups 63
8.8 Number of Non-isomorphic Abelian Groups 63

S E C T I O N – II

R I N G T H E O R Y

Unit. No.	*Contents*	*Page No.*

1. IMPORTANT STRUCTURE OF RING & BASIC DEFINITIONS

1.1 Definition of Ring 70
1.2 Definition of Zero Element 70
1.3 Definition of Unity Element 70
1.4 Definition of Commutative Ring (CR) 70
1.5 Definition of Ring with Unity (RU) 70
1.6 Definition of Commutative Ring with Unity (CRU) 70
1.7 Definition of Unit Element 70
1.8 Definition of Zero Divisor 70
1.9 Definition of Integral Domain 70
1.1 Definition of Field 70
1.11 Definition of Idempotent Element 70
1.12 Definition of Nilpotent Element 70
1.13 Definition of Characteristic of Ring 70
1.14 Definition of Factor 70
1.15 Definition of Irreducible Element 71
1.16 Definition of Prime Element 71

2. IRREDUCIBILITY OF POLYNOMIAL

2.1 Division Algorithm 74
2.2 Definition of Greatest Common Divisor (GCD) 74
2.3 Definition of Least Common Multiple (LCM) 74
2.4 Definition of Irreducible Polynomial 74

3. IDEAL & THEIR TYPES

3.1 Subring & Ideal 83
3.2 Quotient Rings 85
3.3 Ring Homomorphism 85
3.4 Kernel of Homomorphism 86
3.5 Isomorphism 86
3.6 List of Some Important Theorems 87
3.7 Chinese Remainder Theorem 87
3.8 ED, PID, UFD 87

4. FIELD EXTENSION & GALOIS THEORY

4.1 Field Extension 97
4.2 Splitting Field & Multiple Roots 99
4.3 Finite Fields 99

SECTION – I

GROUP THEORY

CHAPTER 1

SETS, RELATIONS & FUNCTIONS

1.1 Definition Set:

A set is a well-defined collection of objects.

(Here well-defined means there is no confusion between inclusion & exclusion of the objects)

Some important sets:

$\mathbb{N}$ = The set of natural nos.

$\mathbb{W}$ =The set of whole nos.

$\mathbb{Z}$ =The set of integers

$\mathbb{Z}^+$= The set of +ve integers

$\mathbb{Z}^-$=The set of negative integers

$\mathbb{Q}$ =The set of rational numbers

$\mathbb{Q}^C$=The set of irrational numbers

$\mathbb{R}$ =The set of real number

$\mathbb{C}$ =The set of complex numbers

1.2 Representation of a Sets:

1.2.1 Roaster form/ Tabular form: In this method a set is represented by listing all its elements.

Ex: - If A be the set of natural number less than 10 then we can write A = {1,2,3,4,5,6,7,8,9}.

- In Roaster form elements can't be repeated.

  Ex: If A be the set of all letters in the word CHANDAN, then we can write in Roaster form as

  $A = \{C, H, A, N, D\}$

- In Roaster form order of arrangement doesn't matter

  Ex: {1,2,3} represents the same set as {1,3,2}

1.2.2 Set-Builder Form: In this form elements of the set are not listed but these are represented by some common property.

Ex: If A be the set of natural number less than 10 then we can write A in set builder form as

$A = \{x: x \in \mathbb{N} \,\&\, 1 \leq x < 10\}$.

1.3 Classification of Sets:

1.3.1 Definition Finite Set: A set is called finite if its elements can be counted.

Ex: A = $\{x : x\ is\ a\ student\ of\ IFAS\}$

1.3.2 Definition Infinite Set: A set is called Infinite if its elements can't be counted.

Ex: $\mathbb{N}$

1.3.3 Definition **Empty set / Null set**: A set which has no elements is said to be an empty/null/void set and denoted by ϕ.

Ex: $A = \{x: x \in \mathbb{R} \,\&\, x^2 + 1 = 0\}$

1.3.4 Definition **Singleton set**: A set which has only one element is known as singleton set.

Ex: A = $\{x : x\ is\ even\ prime\}$

1.3.5 Definition **Equal set**: If the Sets A and B have same elements then they are called equal.

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

1.3.6 Definition **Equivalent set**: If the Sets A and B have same no. of elements then they are called equivalent set.

Ex: A = {1,2,3} and B = $\{a, b, c\}$ then A is equivalent to B or A ≈ B

- Equal set always equivalent but equivalent set need not be equal
- Two sets A and B are called equivalent sets if there exist one to one correspondence between them.

1.3.7 Definition Disjoint Sets: Two sets are said to be disjoint if they don't have any common element.

Ex: - A = $\{x: x\ is\ solution\ of\ x^2 + 6x + 8 = 0\}$ & B = {10, 11} Then A and B are called disjoint set.

1.4 Definition Subset:

A set A is called subset of a set $B\ if\ \forall\ x \in A \implies x \in B$ & written as A ⊆ B.

Some Facts About Subset:

- Every set is the subset of itself
- If A ⊆ B and B ⊆ A then A = B
- Empty set is the subset of every set

1.4.1 Definition Proper Subset: If $A \subseteq B\, s.t. A \neq \phi \text{ and } A \neq B$, Then A is said to be proper subset of B & B is called superset of A.

$i.e.$ we can write A ⊂ B or B ⊃ A

Ex: $A = \{[e^x] | \, x \in \mathbb{R}\}, [.]$ denotes the greatest integer function. $i.e.$ A ⊂ $\mathbb{R}$

- A & ϕ are called **improper** subsets of A & all the other subsets are called proper subset

1.5 Power Set:

A set of all subsets of set A is called power set of A & denoted by P(A).

⟶ If $|A| = n$, then the number of subsets of $A = |P(A)| = 2^n$

1.6 Universal Set:

A universal set is a set which contains all the elements or objects of other concerned sets, including its own elements. denoted by the symbol U.

Ex: if X = {2, 4, 6, 8}, Y= {3, 7, 9, 11} & Z = {4, 8, 11} Then we can define the universal set of X, Y, and Z as

U = {2, 3, 4, 6, 7, 8, 9, 11}.

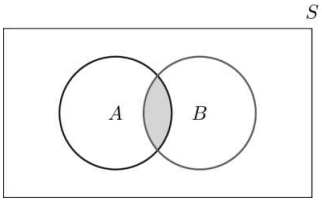
1.7 Intersection of Two Set:

The intersection of two sets A and B, denoted by $A \cap B$, & defined as $A \cap B == \{x | x \in A \text{ and } x \in B\}$

$i.e.$ intersection consists of all elements that are both in A and B.

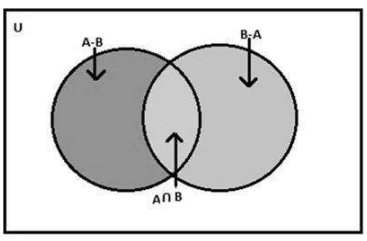
Ex: If $A = \{1,2\}$ & $B = \{2,3\}$ then $A \cap B = \{1,2\} \cap \{2,3\} = \{2\}$.

In the given figure the intersection of sets A and B is shown by the shaded area in the Venn diagram.



1.8 Difference of Two Set:

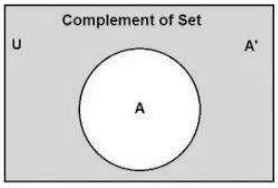
If A and B are two sets then the difference between two sets denoted by A \ B and defined as $A \setminus B = \{x | \, x \in A \text{ but } x \notin B\}$



1.9 Complement of a Set:

If U is a universal set and A be any subset of U then the set of all members of the universal set U which are not the elements of A is called complement of A. It is denoted by A′ & defined as A′ = {x : x ∈ U and x ∉ A}

Also, it can be said that the difference of the universal set U and the subset A gives us the complement of set A.



1.10 Union of Two Set:

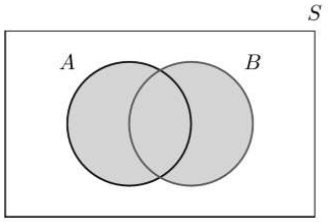
The union of two sets is a set containing all elements that are in A or in B (possibly both) denoted by A ∪ B & defined as $A \cup B = \{x | x \in A \text{ or } x \in B\}$

Ex: $A = \{1,2\}$ & $B = \{2,3\}$ then $A \cup B = \{1,2\} \cup \{2,3\} = \{1,2,3\}$.

$i.e.$ we can write x ∈ (A∪B) if and only if (x ∈ A) or (x ∈ B).

- A∪B = B∪A

In the given figure the union of sets A and B is shown by the shaded area in the Venn diagram.



Similarly,

We can define the union of three or more sets.

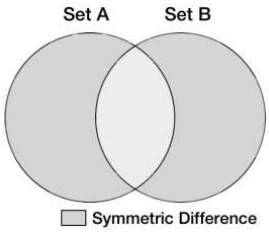
In particular, if $A_1, A_2, A_3 \ldots . A_n$ are n sets, then we can write this union more

compactly by $U_{i=1}^{n} A_i$ & also for $A_1, A_2, A_3 \ldots . A_n$...their union can be written as $U\ A_i \text{ or } U_{i=1}^{\infty} A_i$

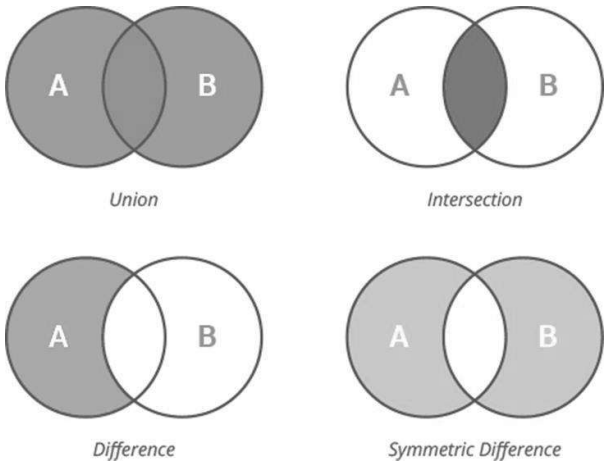
1.11 Symmetric Difference of Two Set:

Symmetric difference between two sets A & B is denoted by

A ∆ B & defined by $A \ \Delta \ B = (A \cup B) \setminus (A \cap B)$



Venn diagram for Union, Intersection, Difference and Symmetric difference:



1.12 Cartesian Product of Two Sets: If A and B are any two sets then Cartesian product of two sets denoted by A × B & defined as

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

Ex: $A = \{1,2,3\}$ & $B = \{a, b\}$ then

$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

B × A = $\{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$

Important observation:

- If $|A| = n$ & $|B| = m$ then $|A \times B| = mn$
- If $A \neq \phi$ & $B \neq \phi$ then $A \times B \neq B \times A$ iff $A \neq B$
- If $A \neq \phi$ & $B \neq \phi$ then $A \times B = B \times A$ iff $A = B$
- If either $A = \phi$ or $B = \phi$ then $A \times B = B \times A = \phi$
- If $|A| = n$ & $|B| = m$ then $|P(A \times B)| = 2^{mn}$

1.13 Relation: If A and B are any two sets then the subset of A × B represents a relation (say R) defined from A to B.

Ex: Let A = {1, 2, 3, 4, 5, 6}. Define a relation R from A to A by $R = \{(x, y) : y = x + 1\}$

- If $|A| = n$ & $|B| = m$ then total no. of distinct relation defined from Set A to Set B = Total no. of subsets of $A \times B = |P(A \times B)|$

1.13.1 Domain of relation: The set of all first elements of the ordered pairs in a relation R from a set A to a set B is called the domain of the relation R.

Ex: Let A = {1, 2, 3, 4, 5, 6}. Define a relation R from A to A by $R = \{(x, y) : y = x + 1\}$

1.13.2 Codomain of relation: If R is the relation defined from set A to set B then the whole set B is called the codomain of the relation R

Ex: Let A = {1, 2, 3, 4, 5, 6}. Define a relation R from A to A by R = {(x, y) : y = x + 1 }

1.13.3 Range of the relation: The set of all second elements in a relation R defined from a set A to a set B is called the range of the relation R.

- Range ⊆ Codomain

Ex: Let A = {1, 2, 3, 4, 5, 6}. Define a relation R from A to A by $R = \{(x, y) : y = x + 1\}$

1.14 Types of Relation

1.14.1 Empty Relation: $\phi = S \subseteq A \times B$ is called an empty Relation defined from Set A to Set B.

1.14.2 Identify Relation: if A be any non-empty set the Relation I_A is called $\forall\, a \in A, (a, a) \in I_A$ & $\forall\, a \neq b, (a, b) \notin I_A$.

Ex: $A = \langle 1, 2, 3 \rangle$

$I_A \subseteq A \times A$ & $I_A = \langle (1, 1), (2, 2), (3, 3) \rangle$

- If $|A| = n, |I_A| = n$

1.14.3 Reflexive Relation: If A be any set & if S_A is a Relation defined on A s.t. $I_A \subseteq S_A$ then S is called a reflexive Relation defined on A.

Ex. $A = \langle 1, 2, 3 \rangle$

$I_A = \langle (1, 1), (2, 2), (3, 3) \rangle$

$S_A = \langle (1, 1), (2, 2), (3, 3), (1, 2) \rangle$

- Identity Relation ⇒ Reflexive relation
- If $|A| = n, |S_A| \geq |I_A| = n$
- Total number of Reflexive relations defined on set A, if $|A| = n$ is equal to $2^{n^2 - n}$

1.14.4 Irreflexive Relation: If A be any set, $|A| = n$ & S_A is a relation defined on A is called Irreflexive if $S_A \cap I_A = \phi$

Ex: $A = \langle 1, 2, 3 \rangle$

$S'_A = \langle (1, 2), (1, 3) \rangle$

If $A = \langle 1, 2, 3 \rangle$

$R \subseteq A \times A$ $s.t.$ $R = \langle (1, 1), (1, 2), (1, 3) \rangle$

- Total number of Irreflexive Relation defined on A = $2^{n^2 - n}$
- ∃ some Relations which are neither Reflexive nor Irreflexive.

1.14.5 Symmetric Relation: If A be any set & S be a Relation defined on set A $s.t.$ $\forall\, (a, b) \in S, (b, a) \in S$ then S is called symmetric Relation defined on A

Ex: $A = \langle 1, 2, 3 \rangle$