

BASIC ABSTRACT ALGEBRA

Second edition



Basic abstract algebra

Second edition

P. B. BHATTACHARYA
Formerly, University of Delhi
S. K. JAIN
Ohio University

St. Stephen's College, Delhi

S. R. NAGPAUL





Published by the Press Syndicate of the University of Cambridge The Pitt Building, Trumpington Street, Cambridge CB2 1RP 40 West 20th Street, New York, NY 10011-4211, USA 10 Stamford Road, Oakleigh, Melbourne 3166, Australia

© Cambridge University Press 1986, 1994

First edition published 1986 Second edition published 1994 Reprinted 1995

Library of Congress Cataloging-in-Publication Data is available.

A catalogue record for this book is available from the British Library.

ISBN 0-521-46081-6 hardback ISBN 0-521-46629-6 paperback

Transferred to digital printing 2001



For PARVESH JAIN
To whom we owe more than we can possibly expres



Contents

Preface to the second edition		page xiii	
Preface to	xiv		
Glossary of symbols		xviii	
	Part I Preliminaries		
Chantar 1	Sata and mannings	2	
Chapter	Sets and mappings 1. Sets	3	
		3	
	2. Relations	9	
	3. Mappings	14	
	4. Binary operations	21	
	5. Cardinality of a set	25	
Chapter 2	Integers, real numbers, and complex numbers	30	
	1. Integers	30	
	2. Rational, real, and complex numbers	35	
	3. Fields	36	
Chapter 3	Matrices and determinants	39	
- ··•	1. Matrices	39	
	2. Operations on matrices	41	
	3. Partitions of a matrix	46	
	4. The determinant function	47	
	5. Properties of the determinant function	49	
	6. Expansion of det A	53	
		55	

vii



viii Contents

Part II Groups

Chapter 4	Groups	61
Chapter 4	Semigroups and groups	61
	2. Homomorphisms	69
	3. Subgroups and cosets	72
	4. Cyclic groups	82
	5. Permutation groups	84
	6. Generators and relations	90
Chapter 5	Normal subgroups	91
F	1. Normal subgroups and quotient groups	91
	2. Isomorphism theorems	97
	3. Automorphisms	104
	4. Conjugacy and G-sets	107
Chapter 6	Normal series	120
Chapter 5	1. Normal series	120
	2. Solvable groups	124
	3. Nilpotent groups	126
Chapter 7	Permutation groups	129
F	1. Cyclic decomposition	129
	2. Alternating group A_n	132
	3. Simplicity of A_n	135
Chapter 8	Structure theorems of groups	138
1	1. Direct products	138
	2. Finitely generated abelian groups	141
	3. Invariants of a finite abelian group	143
	4. Sylow theorems	146
	5. Groups of orders p^2 , pq	152
	Part III Rings and modules	
Chapter 9	Rings	159
Chapter	1. Definition and examples	159
	2. Elementary properties of rings	161
	3. Types of rings	163
	4. Subrings and characteristic of a ring	168
	5. Additional examples of rings	176



Contents		ix
Chapter 10	Ideals and homomorphisms	179
- 1	1. Ideals	179
	2. Homomorphisms	187
	3. Sum and direct sum of ideals	196
	4. Maximal and prime ideals	203
	5. Nilpotent and nil ideals	209
	6. Zorn's lemma	210
Chapter 11	Unique factorization domains and euclidean	
	domains	212
	1. Unique factorization domains	212
	2. Principal ideal domains	216
	3. Euclidean domains	217
•	4. Polynomial rings over UFD	219
Chapter 12	Rings of fractions	224
•	1. Rings of fractions	224
	2. Rings with Ore condition	228
Chapter 13	Integers	233
1	1. Peano's axioms	233
	2. Integers	240
Chapter 14	Modules and vector spaces	246
,	1. Definition and examples	246
	2. Submodules and direct sums	248
	3. R-homomorphisms and quotient modules	253
	4. Completely reducible modules	260
	5. Free modules	263
	6. Representation of linear mappings	268
	7. Rank of a linear mapping	273
	Part IV Field theory	
Chapter 15	Algebraic extensions of fields	281
r	1. Irreducible polynomials and Eisenstein	
	criterion	281
	2. Adjunction of roots	285
	3. Algebraic extensions	289
	4. Algebraically closed fields	295



x Co	ntents	
Chapter 16	Normal and separable extensions Splitting fields Normal extensions 	300 300 304
	3. Multiple roots	304
	4. Finite fields	310
	5. Separable extensions	316
Chapter 17	-	322
	1. Automorphism groups and fixed fields	322
	2. Fundamental theorem of Galois theory3. Fundamental theorem of algebra	330 338
Chapter 18	*	240
	problems 1. Roots of unity and cyclotomic polynomials	340 340
	2. Cyclic extensions	344
	3. Polynomials solvable by radicals	348
	4. Symmetric functions	355
	5. Ruler and compass constructions	358
	Part V Additional topics	
Chapter 19	· ·	367
	1. $\operatorname{Hom}_{R}(\oplus M_{i}, \oplus M_{i})$	367
	2. Noetherian and artinian modules	368
	 Wedderburn-Artin theorem Uniform modules, primary modules, and 	382
	Noether-Lasker theorem	388
Chapter 20		392
	1. Preliminaries	392
	2. Row module, column module, and rank	393
	3. Smith normal form	394
Chapter 21	Finitely generated modules over a PID	402
	1. Decomposition theorem	402
	2. Uniqueness of the decomposition	404
	3. Application to finitely generated abelian	
	groups	408
	4. Rational canonical form	409
	5. Generalized Jordan form over any field	418



Con	tents	Xi
Chapter 22	Tensor products	426
•	1. Categories and functors	426
	2. Tensor products	428
	3. Module structure of tensor product	431
	4. Tensor product of homomorphisms	433
	5. Tensor product of algebras	436
Solutions to	odd-numbered problems	438
Selected bib	liography	476
Index		477



Preface to the second edition

The following are the main features of the second edition.

More than 150 new problems and examples have been added. The new problems include several that relate abstract concepts to concrete situations. Among others, we present applications of *G*-sets, the division algorithm and greatest common divisors in a given euclidean domain. In particular, we should mention the combinatorial applications of the Burnside theorem to real-life problems. A proof for the constructibility of a regular *n*-gon has been included in Chapter 18.

We have included a recent elegant and elementary proof, due to Osofsky, of the celebrated Noether-Lasker theorem.

Chapter 22 on tensor products with an introduction to categories and functors is a new addition to Part IV. This chapter provides basic results on tensor products that are useful and important in present-day mathematics.

We are pleased to thank all of the professors and students in the many universities who used this textbook during the past seven years and contributed their useful feedback. In particular, we would like to thank Sergio R. Lopez-Permouth for his help during the time when the revised edition was being prepared. Finally, we would like to acknowledge the staff of Cambridge University Press for their help in bringing out this second edition so efficiently.

P. B. Bhattacharya

S. K. Jain

S. R. Nagpaul

xiii



Preface to the first edition

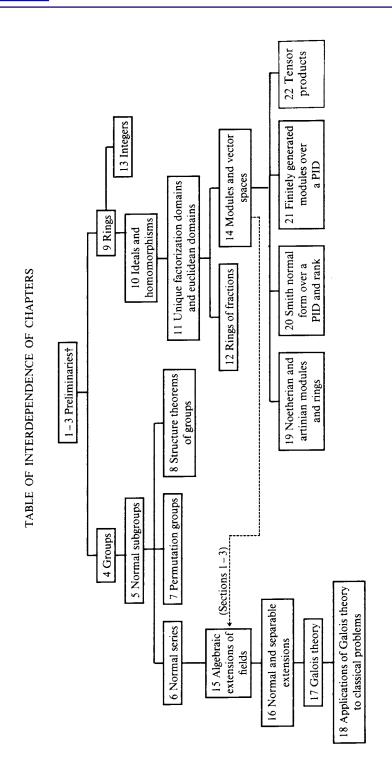
This book is intended for seniors and beginning graduate students. It is self-contained and covers the topics usually taught at this level.

The book is divided into five parts (see diagram). Part I (Chapters 1-3) is a prerequisite for the rest of the book. It contains an informal introduction to sets, number systems, matrices, and determinants. Results proved in Chapter 1 include the Schröder-Bernstein theorem and the cardinality of the set of real numbers. In Chapter 2, starting from the well-ordering principle of natural numbers, some important algebraic properties of integers have been proved. Chapter 3 deals with matrices and determinants. It is expected that students would already be familiar with most of the material in Part I before reaching their senior year. Therefore, it can be completed rapidly, skipped altogether, or simply referred to as necessary.

Part II (Chapters 4–8) deals with groups. Chapters 4 and 5 provide a foundation in the basic concepts in groups, including G-sets and their applications. Normal series, solvable groups, and the Jordan-Hölder theorem are given in Chapter 6. The simplicity of the alternating group A_n and the nonsolvability of S_n , n > 4, are proved in Chapter 7. Chapter 8 contains the theorem on the decomposition of a finitely generated abelian group as a direct sum of cyclic groups, and the Sylow theorems. The invariants of a finite abelian group and the structure of groups of orders p^2 , pq, where p, q are primes, are given as applications.

Part III (Chapters 9-14) deals with rings and modules. Chapters 9-11 cover the basic concepts of rings, illustrated by numerous examples, including prime ideals, maximal ideals, UFD, PID, and so forth. Chapter 12 deals with the ring of fractions of a commutative ring with respect to a multiplicative set. Chapter 13 contains a systematic development of

xiv



† To be read as and when needed.



xvi Preface to the first edition

integers, starting from Peano's axioms. Chapter 14 is an introduction to modules and vector spaces. Topics discussed include completely reducible modules, free modules, and rank.

Part IV (Chapters 15–18) is concerned with field theory. Chapters 15 and 16 contain the usual material on algebraic extensions, including existence and uniqueness of algebraic closure, and normal and separable extensions. Chapter 17 gives the fundamental theorem of Galois theory and its application to the fundamental theorem of algebra. Chapter 18 gives applications of Galois theory to some classical problems in algebra and geometry.

Part V (Chapters 19–21) covers some additional topics not usually taught at the undergraduate level. Chapter 19 deals with modules with chain conditions leading to the Wedderburn-Artin theorem for semi-simple artinian rings. Chapter 20 deals with the rank of a matrix over a PID through Smith normal form. Chapter 21 gives the structure of a finitely generated module over a PID and its applications to linear algebra.

Parts II and III are almost independent and may be studied in any order. Part IV requires a knowledge of portions to Parts II and III. It can be studied after acquiring a basic knowledge of groups, rings, and vector spaces. The precise dependence of Part IV on the rest of the book can be found from the table of interdependence of chapters.

The book can be used for a one-year course on abstract algerba. The material presented here is in fact somewhat more than most instructors would normally teach. Therefore, it provides flexibility in selection of the topics to be taught. A two-quarter course in abstract algebra may cover the following: groups – Chapters 4, 5, and 7 (Section 1) and 8; rings – Chapters 9, 10, 11, and 14 (Sections 1–3); field theory – Chapters 15, 16, and 18 (Section 5). A two-semester course in abstract algebra can cover all of the material in Parts II, III, and IV.

Numerous examples have been worked out throughout the book to illustrate the concepts and to show the techniques of solving problems. There are also many challenging problems for the talented student. We have also provided solutions to the odd-numbered problems at the end of the book. We hope these will be used by students mostly for comparison with their own solutions.

Numbering of theorems, lemmas, and examples is done afresh in each chapter by section. If reference is made to a result occurring in a previous chapter, then only the chapter number is mentioned alongside. In all cases the additional information needed to identify a reference is provided.

The book has evolved from our experience in teaching algebra for many years at the undergraduate and graduate levels. The material has been class tested through mimeographed notes distributed to the students.



Preface to the first edition

vvii

We acknowledge our indebtedness to numerous authors whose books have influenced our writing. In particular, we mention P. M. Cohn's *Algebra*, Vols. 1, 2, John Wiley, New York, 1974, 1977, and S. Lang's *Algebra*, Addison-Wesley, Reading, MA, 1965.

During the preparation of this book we received valuable help from several colleagues and graduate students. We express our gratitude to all of them. We also express our gratefulness to Ohio University for providing us the facilities to work together in the congenial environment of its beautiful campus.

It is our pleasant duty to express our gratitude to Professor Donald O. Norris, Chairman, Department of Mathematics, Ohio University, whose encouragement and unstinted support enabled us to complete our project. We also thank Mrs. Stephanie Goldsberry for the splendid job of typing.

P. B. Bhattacharya

S. K. Jain

S. R. Nagpaul



Glossary of symbols

```
A
                        for all
                        there exists
Ε
                        is an element of
\in
                        is not an element of
\{x \in A | P(x)\}
                        set of all x \in A satisfying condition P(x)
                        power set of x
\mathcal{P}(x)
                        family indexed by set \Lambda
(X_i)_{i\in\Lambda}
\bigcup X_i
                        union of (X_i)_{i \in \Lambda}
\bigcap_{i\in\Lambda}X_i
                        intersection of (X_i)_{i \in \Lambda}
X \times Y
                        Cartesian product of X and Y
Ø
                        empty set
                        is a subset of
\subset or \subseteq
                        is a proper subset of
\subsetneq
\supset or \supseteq
                       contains
                        properly contains
                       implies
\Rightarrow
                       if and only if
                       if and only if
iff
                       f is a map of X into Y
f: X \to Y
                       image of x \in X under f: X \to Y
f(x)
                       y = f(x) where f: X \to Y, x \in X, y \in Y
f: x \mapsto y
                       composition
                       Euler's function
φ
```

xviii



Glossary of symbols	
(<i>a</i> , <i>b</i>)	in number theory, the greatest common divisor of a and b ; in rings and modules, the ideal or submodule generated by a and b
a b	a divides b
$a \not b$	a does not divide b
δ_{ij}	Kronecker delta
det	determinant
$\operatorname{sgn} \sigma$	± 1 , according as the permutation σ is even or odd
e_{ij}	square matrix with 1 in (i, j) position, 0 elsewhere
n	the set of positive integers $\{1,2,3,,n\}$
N	set of all natural numbers
Z	set of all integers
Q	set of all rational numbers
R	set of all real numbers
C	set of all complex numbers
¢	the cardinal of the continuum (cardinality of the reals)
$Z/(n)$ or Z_n	integers modulo n
X or card X	cardinality of X
G	order of group G
[S]	subgroup generated by S
C_n	cyclic group of order n
S_n	as a group, the symmetric group of degree n ; as a ring,
	the ring of $n \times n$ matrices over S
A_n	alternating group of degree n
D_n $GL(m, F)$	dihedral group of degree n group of invertible $m \times m$ matrices over F
	center of G
Z(G)	is a normal subgroup of
$\overrightarrow{A/B}$	quotient group (ring, module) of A modulo B
[L:K]	in groups, the index of a subgroup K in a group L ; in
[2.11]	vector spaces, the dimension of a vector space L over K ;
	in fields, the degree of extension of L over K
$N(S) (N_H(S))$	normalizer of S (in H)
$C(S)(C_H(S))$	conjugate class of S (with respect to H)
$\prod_{i \in \Lambda} X_i$	product of $(X_i)_{i \in \Lambda}$
$\oplus \sum_{i \in \Lambda} X_i$	direct sum of $(X_i)_{i \in \Lambda}$
$\operatorname{Im} f$	image of homomorphism f
Ker f	kernel of homomorphism f
G	is isomorphic into (embeddable)
~	is isomorphic onto



xx Glossary	to Symbols
R^{op}	opposite ring of R
(S)	ideal (submodule) generated by S
$(S)_{r}$	right ideal generated by S
$(S)_1$	left ideal generated by S
$\sum_{i \in \Lambda} X_i$	sum of right or left ideals (submodules) $(X_i)_{i \in \Lambda}$
R[x]	polynomial ring over R in one indeterminate x
$R[x_1,,x_n]$	polynomial ring over R in n indeterminates, $x_1,,x_n$
R[[x]]	formal power series ring
$R\langle x\rangle$	ring of formal Laurent series
$Z(p^{\infty})$	rationals between 0 and 1 of the form m/p^n , $m,n > 0$ under the binary operation "addition modulo 1"
$\operatorname{Hom}_{R}(X,Y)$	set of all R-homomorphisms of R-module X to R-module Y
Hom(X,Y)	set of all homomorphisms of X to Y
$\operatorname{End}(X)$	endomorphisms of X
$\operatorname{Aut}(X)$	automorphisms of X
R_{S}	localization of a ring R at S
$F(\alpha)$	subfield generated by F and α
F[S]	subring generated by F and S
F(S)	subfield generated by F and S
$\frac{GF(q)}{\overline{F}}$	Galois field (finite field) with q elements
\overline{F}	algebraic closure of F
E_H	fixed field of H
G(E/F)	Galois group of automorphisms of E over F
$\phi_n(x)$	cyclotomic polynomial of degree n
$M \otimes_R N$	tensor product of M_R and $_RN$
	end of the proof