BASIC ABSTRACT ALGEBRA
Second edition
Basic abstract algebra

Second edition

P. B. BHATTACHARYA
Formerly, University of Delhi

S. K. JAIN
Ohio University

S. R. NAGPAUL
St. Stephen’s College, Delhi
For
PARVESH JAIN
To whom we owe more than we can possibly expres
## Contents

Preface to the second edition .... xiii
Preface to the first edition .... xiv
Glossary of symbols .... xviii

### Part I Preliminaries

**Chapter 1 Sets and mappings**
1. Sets .... 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**
1. Integers .... 30
2. Rational, real, and complex numbers .... 35
3. Fields .... 36

**Chapter 3 Matrices and determinants**
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
# Contents

## Part II Groups

**Chapter 4** Groups
1. 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
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
1. Normal series 120
2. Solvable groups 124
3. Nilpotent groups 126

**Chapter 7** Permutation groups 129
1. Cyclic decomposition 129
2. Alternating group $A_n$ 132
3. Simplicity of $A_n$ 135

**Chapter 8** Structure theorems of groups 138
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
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

<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Ideals and homomorphisms</th>
<th>ix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ideals</td>
<td>179</td>
</tr>
<tr>
<td>2.</td>
<td>Homomorphisms</td>
<td>179</td>
</tr>
<tr>
<td>3.</td>
<td>Sum and direct sum of ideals</td>
<td>187</td>
</tr>
<tr>
<td>4.</td>
<td>Maximal and prime ideals</td>
<td>196</td>
</tr>
<tr>
<td>5.</td>
<td>Nilpotent and nil ideals</td>
<td>203</td>
</tr>
<tr>
<td>6.</td>
<td>Zorn’s lemma</td>
<td>209</td>
</tr>
</tbody>
</table>

Chapter 11  
Unique factorization domains and euclidean domains  
1. Unique factorization domains  
2. Principal ideal domains  
3. Euclidean domains  
4. Polynomial rings over UFD  

Chapter 12  
Rings of fractions  
1. Rings of fractions  
2. Rings with Ore condition  

Chapter 13  
Integers  
1. Peano’s axioms  
2. Integers  

Chapter 14  
Modules and vector spaces  
1. Definition and examples  
2. Submodules and direct sums  
3. R-homomorphisms and quotient modules  
4. Completely reducible modules  
5. Free modules  
6. Representation of linear mappings  
7. Rank of a linear mapping  

Part IV  Field theory  

Chapter 15  
Algebraic extensions of fields  
1. Irreducible polynomials and Eisenstein criterion  
2. Adjunction of roots  
3. Algebraic extensions  
4. Algebraically closed fields  

© Cambridge University Press  www.cambridge.org
<table>
<thead>
<tr>
<th>Chapter 16</th>
<th>Normal and separable extensions</th>
<th>300</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Splitting fields</td>
<td>300</td>
</tr>
<tr>
<td>2.</td>
<td>Normal extensions</td>
<td>304</td>
</tr>
<tr>
<td>3.</td>
<td>Multiple roots</td>
<td>307</td>
</tr>
<tr>
<td>4.</td>
<td>Finite fields</td>
<td>310</td>
</tr>
<tr>
<td>5.</td>
<td>Separable extensions</td>
<td>316</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 17</th>
<th>Galois theory</th>
<th>322</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Automorphism groups and fixed fields</td>
<td>322</td>
</tr>
<tr>
<td>2.</td>
<td>Fundamental theorem of Galois theory</td>
<td>330</td>
</tr>
<tr>
<td>3.</td>
<td>Fundamental theorem of algebra</td>
<td>338</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 18</th>
<th>Applications of Galois theory to classical problems</th>
<th>340</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Roots of unity and cyclotomic polynomials</td>
<td>340</td>
</tr>
<tr>
<td>2.</td>
<td>Cyclic extensions</td>
<td>344</td>
</tr>
<tr>
<td>3.</td>
<td>Polynomials solvable by radicals</td>
<td>348</td>
</tr>
<tr>
<td>4.</td>
<td>Symmetric functions</td>
<td>355</td>
</tr>
<tr>
<td>5.</td>
<td>Ruler and compass constructions</td>
<td>358</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part V</th>
<th>Additional topics</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Noetherian and artinian modules and rings</th>
<th>367</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>$\text{Hom}_R (\bigoplus M_i \oplus M_j)$</td>
<td>367</td>
</tr>
<tr>
<td>2.</td>
<td>Noetherian and artinian modules</td>
<td>368</td>
</tr>
<tr>
<td>3.</td>
<td>Wedderburn–Arin theorem</td>
<td>382</td>
</tr>
<tr>
<td>4.</td>
<td>Uniform modules, primary modules, and Noether–Lasker theorem</td>
<td>388</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>Smith normal form over a PID and rank</th>
<th>392</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Preliminaries</td>
<td>392</td>
</tr>
<tr>
<td>2.</td>
<td>Row module, column module, and rank</td>
<td>393</td>
</tr>
<tr>
<td>3.</td>
<td>Smith normal form</td>
<td>394</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21</th>
<th>Finitely generated modules over a PID</th>
<th>402</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Decomposition theorem</td>
<td>402</td>
</tr>
<tr>
<td>2.</td>
<td>Uniqueness of the decomposition</td>
<td>404</td>
</tr>
<tr>
<td>3.</td>
<td>Application to finitely generated abelian groups</td>
<td>408</td>
</tr>
<tr>
<td>4.</td>
<td>Rational canonical form</td>
<td>409</td>
</tr>
<tr>
<td>5.</td>
<td>Generalized Jordan form over any field</td>
<td>418</td>
</tr>
</tbody>
</table>
### Contents

| 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 bibliography 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 Ososky, 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-Permoult 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
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
TABLE OF INTERDEPENDENCE OF CHAPTERS

1-3 Preliminaries

4 Groups

5 Normal subgroups

6 Normal series

7 Permutation groups

8 Structure theorems of groups

9 Rings

10 Ideals and homomorphisms

11 Unique factorization domains and Dedekind domains

12 Rings of fractions

13 Integral domains

14 Modules and vector spaces

15 Algebraic extensions of fields

16 Normal and separable extensions

17 Galois theory

18 Noetherian and artinian modules and rings

19 Smith normal form over a PID and rank

20 Tensor products

21 Finitely generated modules over a PID

22 Torsion products

† To be read as and when needed.
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 algebra. 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

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

\forall \quad \text{for all}
\exists \quad \text{there exists}
\in \quad \text{is an element of}
\notin \quad \text{is not an element of}
(x \in A | P(x)) \quad \text{set of all } x \in A \text{ satisfying condition } P(x)
\mathcal{P}(x) \quad \text{power set of } x
\{X_i\}_{i \in A} \quad \text{family indexed by set } A
\bigcup_{i \in A} X_i \quad \text{union of } (X_i)_{i \in A}
\bigcap_{i \in A} X_i \quad \text{intersection of } (X_i)_{i \in A}
X \times Y \quad \text{Cartesian product of } X \text{ and } Y
\emptyset \quad \text{empty set}
\subseteq \quad \text{is a subset of}
\subset \quad \text{is a proper subset of}
\supseteq \quad \text{contains}
\supset \quad \text{properly contains}
\implies \quad \text{implies}
\iff \quad \text{if and only if}
\text{iff} \quad \text{if and only if}
f: X \to Y \quad f \text{ is a map of } X \text{ into } Y
f(x) \quad \text{image of } x \in X \text{ under } f: X \to Y
f: X \to Y \quad y = f(x) \text{ where } f: X \to Y, x \in X, y \in Y
\circ \quad \text{composition}
\phi \quad \text{Euler’s function}
Glossary of symbols

\((a,b)\) in number theory, the greatest common divisor of \(a\)
and \(b\); in rings and modules, the ideal or submodule
generated by \(a\) and \(b\)

\(a\mid b\) \(a\) divides \(b\)

\(a \not| b\) \(a\) does not divide \(b\)

\(\delta_{ij}\) Kronecker delta

\(\det\) determinant

\(\text{sgn } \sigma\) \(\pm 1\), according as the permutation \(\sigma\) is even or odd

\(\epsilon_{ij}\) square matrix with 1 in \((i,j)\) position, 0 elsewhere

\(\mathbb{N}\) the set of positive integers \(\{1, 2, 3, ..., n\}\)

\(\mathbb{Z}\) set of all natural numbers

\(\mathbb{Z}\) set of all integers

\(\mathbb{Q}\) set of all rational numbers

\(\mathbb{R}\) set of all real numbers

\(\mathbb{C}\) set of all complex numbers

\(\mathfrak{c}\) the cardinal of the continuum (cardinality of the reals)

\(\mathbb{Z}/(n)\) or \(\mathbb{Z}_n\) integers modulo \(n\)

\(|X|\) or \(\text{card } X\) 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 \(n\)

\(D_n\) dihedral group of degree \(n\)

\(\text{GL}(m, F)\) group of invertible \(m \times m\) matrices over \(F\)

\(Z(G)\) center of \(G\)

\(\triangleleft\) is a normal subgroup of

\(A/B\) quotient group (ring, module) of \(A\) modulo \(B\)

\([L:K]\) in groups, the index of a subgroup \(K\) in a group \(L\); in
vector spaces, the dimension of a vector space \(L\) over \(K\);
in fields, the degree of extension of \(L\) over \(K\)

\(N(S)\) \((N_G(S))\) normalizer of \(S\) (in \(H\))

\(C(S)\) \((C_G(S))\) 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 \((X_i)_{i \in \Lambda}\)

\(\text{Im } f\) image of homomorphism \(f\)

\(\text{Ker } f\) kernel of homomorphism \(f\)

\(\cong\) is isomorphic into (embeddable)

\(\simeq\) is isomorphic onto
\textbf{xx} \hspace{1cm} \textbf{Glossary to Symbols}

$R^{\text{op}}$ \hspace{1cm} \text{opposite ring of } R

$(S)$ \hspace{1cm} \text{ideal (submodule) generated by } S

$(S)_R$ \hspace{1cm} \text{right ideal generated by } S

$(S)_L$ \hspace{1cm} \text{left ideal generated by } S

$\sum_{i \in \Lambda} X_i$ \hspace{1cm} \text{sum of right or left ideals (submodules) } (X_i)_{i \in \Lambda}

$R[x]$ \hspace{1cm} \text{polynomial ring over } R \text{ in one indeterminate } x

$R[x_1, \ldots, x_n]$ \hspace{1cm} \text{polynomial ring over } R \text{ in } n \text{ indeterminates, } x_1, \ldots, x_n

$R[[x]]$ \hspace{1cm} \text{formal power series ring}

$R\langle x \rangle$ \hspace{1cm} \text{ring of formal Laurent series}

$\mathbb{Z}\langle p, \infty \rangle$ \hspace{1cm} \text{rationals between } 0 \text{ and } 1 \text{ of the form } m/p^n, m, n > 0 \text{ under the binary operation } \text{“addition modulo } 1”

$\text{Hom}_R(X, Y)$ \hspace{1cm} \text{set of all } R\text{-homomorphisms of } R\text{-module } X \text{ to } R\text{-module } Y

$\text{Hom}(X, Y)$ \hspace{1cm} \text{set of all homomorphisms of } X \text{ to } Y

$\text{End}(X)$ \hspace{1cm} \text{endomorphisms of } X

$\text{Aut}(X)$ \hspace{1cm} \text{automorphisms of } X

$R_S$ \hspace{1cm} \text{localization of a ring } R \text{ at } S

$F(\alpha)$ \hspace{1cm} \text{subfield generated by } F \text{ and } \alpha

$F[S]$ \hspace{1cm} \text{subring generated by } F \text{ and } S

$F(S)$ \hspace{1cm} \text{subfield generated by } F \text{ and } S

$G_F(q)$ \hspace{1cm} \text{Galois field (finite field) with } q \text{ elements}

$\overline{F}$ \hspace{1cm} \text{algebraic closure of } F

$E_H$ \hspace{1cm} \text{fixed field of } H

$G(E/F)$ \hspace{1cm} \text{Galois group of automorphisms of } E \text{ over } F

$\phi_n(x)$ \hspace{1cm} \text{cyclotomic polynomial of degree } n

$M \otimes_R N$ \hspace{1cm} \text{tensor product of } M_R \text{ and } \_N

$\Box$ \hspace{1cm} \text{end of the proof}