Frequently Used Notation

$f^{-1}(A)$	the inverse image or preimage of A under f
$a \mid b$	a divides b
(a, b)	the greatest common divisor of a, b also the ideal generated by a, b
$\|A\|, \|x\|$	the order of the set A, the order of the element x
$\mathbb{Z}, \mathbb{Z}^+$	the integers, the positive integers
$\mathbb{Q}, \mathbb{Q}^+$	the rational numbers, the positive rational numbers
$\mathbb{R}, \mathbb{R}^+$	the real numbers, the positive real numbers
$\mathbb{C}, \mathbb{C}^\times$	the complex numbers, the nonzero complex numbers
$\mathbb{Z}/n\mathbb{Z}$	the integers modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	the (multiplicative group of) invertible integers modulo n
$A \times B$	the direct or Cartesian product of A and B
$H \leq G$	H is a subgroup of G
Z_n	the cyclic group of order n
D_{2n}	the dihedral group of order $2n$
S_n, S_Ω	the symmetric group on n letters, and on the set Ω
A_n	the alternating group on n letters
Q_8	the quaternion group of order 8
V_4	the Klein 4–group
$\mathbb{F}_N$	the finite field of N elements
$GL_n(F)$, $GL(V)$	the general linear groups
$SL_n(F)$	the special linear group
$A \cong B$	A is isomorphic to B
$C_G(A)$, $N_G(A)$	the centralizer, and normalizer in G of A
$Z(G)$	the center of the group G
G_s	the stabilizer in the group G of s
$\langle A \rangle$, $\langle x \rangle$	the group generated by the set A, and by the element x
$G = \langle \ldots \mid \ldots \rangle$	generators and relations (a presentation) for G
$\ker \varphi$, $\operatorname{im} \varphi$	the kernel, and the image of the homomorphism φ
$N \trianglelefteq G$	N is a normal subgroup of G
gH, Hg	the left coset, and right coset of H with coset representative g
$\|G : H\|$	the index of the subgroup H in the group G
$\operatorname{Aut}(G)$	the automorphism group of the group G
$Syl_p(G)$	the set of Sylow p-subgroups of G
n_p	the number of Sylow p-subgroups of G
$[x, y]$	the commutator of x, y
$H \rtimes K$	the semidirect product of H and K
$\mathbb{H}$	the real Hamilton Quaternions
$R^\times$	the multiplicative group of units of the ring R
$R[x]$, $R[x_1, \ldots, x_n]$	polynomials in x, and in $x_1, \ldots, x_n$ with coefficients in R
RG, FG	the group ring of the group G over the ring R, and over the field F
$\mathcal{O}_K$	the ring of integers in the number field K
$\varinjlim A_i$, $\varprojlim A_i$	the direct, and the inverse limit of the family of groups A_i
$\mathbb{Z}_p$, $\mathbb{Q}_p$	the p-adic integers, and the p-adic rationals
$A \oplus B$	the direct sum of A and B

$LT(f)$, $LT(I)$	the leading term of the polynomial f, the ideal of leading terms
$M_n(R)$, $M_{n\times m}(R)$	the $n \times n$, and the $n \times m$ matrices over R
$M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$	the matrix of the linear transformation φ with respect to bases $\mathcal{B}$ (domain) and $\mathcal{E}$ (range)
$\mathrm{tr}(A)$	the trace of the matrix A
$\mathrm{Hom}_R(A, B)$	the R-module homomorphisms from A to B
$\mathrm{End}(M)$	the endomorphism ring of the module M
$\mathrm{Tor}(M)$	the torsion submodule of M
$\mathrm{Ann}(M)$	the annihilator of the module M
$M \otimes_R N$	the tensor product of modules M and N over R
$\mathcal{T}^k(M)$, $\mathcal{T}(M)$	the k^{th} tensor power, and the tensor algebra of M
$\mathcal{S}^k(M)$, $\mathcal{S}(M)$	the k^{th} symmetric power, and the symmetric algebra of M
$\bigwedge^k(M)$, $\bigwedge(M)$	the k^{th} exterior power, and the exterior algebra of M
$m_T(x)$, $c_T(x)$	the minimal, and characteristic polynomial of T
$\mathrm{ch}(F)$	the characteristic of the field F
K/F	the field K is an extension of the field F
$[K : F]$	the degree of the field extension K/F
$F(\alpha)$, $F(\alpha, \beta)$, etc.	the field generated over F by α or α, β, etc.
$m_{\alpha,F}(x)$	the minimal polynomal of α over the field F
$\mathrm{Aut}(K)$	the group of automorphisms of a field K
$\mathrm{Aut}(K/F)$	the group of automorphisms of a field K fixing the field F
$\mathrm{Gal}(K/F)$	the Galois group of the extension K/F
$\mathbb{A}^n$	affine n-space
$k[\mathbb{A}^n]$, $k[V]$	the coordinate ring of $\mathbb{A}^n$, and of the affine algebraic set V
$\mathcal{Z}(I)$, $\mathcal{Z}(f)$	the locus or zero set of I, the locus of an element f
$\mathcal{I}(A)$	the ideal of functions that vanish on A
$\mathrm{rad}\, I$	the radical of the ideal I
$\mathrm{Ass}_R(M)$	the associated primes for the module M
$\mathrm{Supp}(M)$	the support of the module M
$D^{-1}R$	the ring of fractions (localization) of R with respect to D
R_P, R_f	the localization of R at the prime ideal P, and at the element f
$\mathcal{O}_{v,V}$, $\mathbb{T}_{v,V}$	the local ring, and the tangent space of the variety V at the point v
$\mathfrak{m}_{v,V}$	the unique maximal ideal of $\mathcal{O}_{v,V}$
$\mathrm{Spec}\, R$, $\mathrm{mSpec}\, R$	the prime spectrum, and the maximal spectrum of R
$\mathcal{O}_X$	the structure sheaf of $X = \mathrm{Spec}\, R$
$\mathcal{O}(U)$	the ring of sections on an open set U in $\mathrm{Spec}\, R$
$\mathcal{O}_P$	the stalk of the structure sheaf at P
$\mathrm{Jac}\, R$	the Jacobson radical of the ring R
$\mathrm{Ext}_R^n(A, B)$	the n^{th} cohomology group derived from Hom_R
$\mathrm{Tor}_n^R(A, B)$	the n^{th} cohomology group derived from the tensor product over R
A^G	the fixed points of G acting on the G-module A
$H^n(G, A)$	the n^{th} cohomology group of G with coefficients in A
Res , Cor	the restriction, and corestriction maps on cohomology
$\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq G)$	the stability group of the series $1 \trianglelefteq A \trianglelefteq G$
$\|\|\theta\|\|$	the norm of the character θ
$\mathrm{Ind}_H^G(\psi)$	the character of the representation ψ induced from H to G

ABSTRACT ALGEBRA

Third Edition

David S. Dummit
University of Vermont

Richard M. Foote
University of Vermont

John Wiley & Sons, Inc.

ASSOCIATE PUBLISHER	Laurie Rosatone
ASSISTANT EDITOR	Jennifer Battista
FREELANCE DEVELOPMENTAL EDITOR	Anne Scanlan-Rohrer
SENIOR MARKETING MANAGER	Julie Z. Lindstrom
SENIOR PRODUCTION EDITOR	Ken Santor
COVER DESIGNER	Michael Jung

This book was typeset using the Y&Y TeX System with DVIWindo. The text was set in Times Roman using *MathTime* from Y&Y, Inc. Titles were set in OceanSans. This book was printed by Malloy Inc. and the cover was printed by Phoenix Color Corporation.

This book is printed on acid-free paper.

ISBN 0-471-43334-9

WIE 0-471-45234-3

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Dedicated to our families
especially
Janice, Evan, and Krysta
and
Zsuzsanna, Peter, Karoline, and Alexandra

Contents

Preface xi

Preliminaries 1

0.1 Basics 1
0.2 Properties of the Integers 4
0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n 8

Part I – GROUP THEORY 13

Chapter 1 Introduction to Groups 16

1.1 Basic Axioms and Examples 16
1.2 Dihedral Groups 23
1.3 Symmetric Groups 29
1.4 Matrix Groups 34
1.5 The Quaternion Group 36
1.6 Homomorphisms and Isomorphisms 36
1.7 Group Actions 41

Chapter 2 Subgroups 46

2.1 Definition and Examples 46
2.2 Centralizers and Normalizers, Stabilizers and Kernels 49
2.3 Cyclic Groups and Cyclic Subgroups 54
2.4 Subgroups Generated by Subsets of a Group 61
2.5 The Lattice of Subgroups of a Group 66

Chapter 3 Quotient Groups and Homomorphisms 73

3.1 Definitions and Examples 73
3.2 More on Cosets and Lagrange's Theorem 89
3.3 The Isomorphism Theorems 97
3.4 Composition Series and the Hölder Program 101
3.5 Transpositions and the Alternating Group 106

Chapter 4 Group Actions 112

4.1 Group Actions and Permutation Representations 112
4.2 Groups Acting on Themselves by Left Multiplication—Cayley's Theorem 118
4.3 Groups Acting on Themselves by Conjugation—The Class Equation 122
4.4 Automorphisms 133
4.5 The Sylow Theorems 139
4.6 The Simplicity of A_n 149

Chapter 5 Direct and Semidirect Products and Abelian Groups 152

5.1 Direct Products 152
5.2 The Fundamental Theorem of Finitely Generated Abelian Groups 158
5.3 Table of Groups of Small Order 167
5.4 Recognizing Direct Products 169
5.5 Semidirect Products 175

Chapter 6 Further Topics in Group Theory 188

6.1 p-groups, Nilpotent Groups, and Solvable Groups 188
6.2 Applications in Groups of Medium Order 201
6.3 A Word on Free Groups 215

Part II – RING THEORY 222

Chapter 7 Introduction to Rings 223

7.1 Basic Definitions and Examples 223
7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings 233
7.3 Ring Homomorphisms an Quotient Rings 239
7.4 Properties of Ideals 251
7.5 Rings of Fractions 260
7.6 The Chinese Remainder Theorem 265

Chapter 8 Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains 270

8.1 Euclidean Domains 270
8.2 Principal Ideal Domains (P.I.D.s) 279
8.3 Unique Factorization Domains (U.F.D.s) 283

Chapter 9 Polynomial Rings 295

9.1 Definitions and Basic Properties 295
9.2 Polynomial Rings over Fields I 299
9.3 Polynomial Rings that are Unique Factorization Domains 303
9.4 Irreducibility Criteria 307
9.5 Polynomial Rings over Fields II 313
9.6 Polynomials in Several Variables over a Field and Gröbner Bases 315

Part III – MODULES AND VECTOR SPACES 336

Chapter 10 Introduction to Module Theory 337

10.1 Basic Definitions and Examples 337
10.2 Quotient Modules and Module Homomorphisms 345
10.3 Generation of Modules, Direct Sums, and Free Modules 351
10.4 Tensor Products of Modules 359
10.5 Exact Sequences—Projective, Injective, and Flat Modules 378

Chapter 11 Vector Spaces 408

11.1 Definitions and Basic Theory 408
11.2 The Matrix of a Linear Transformation 415
11.3 Dual Vector Spaces 431
11.4 Determinants 435
11.5 Tensor Algebras, Symmetric and Exterior Algebras 441

Chapter 12 Modules over Principal Ideal Domains 456

12.1 The Basic Theory 458
12.2 The Rational Canonical Form 472
12.3 The Jordan Canonical Form 491