Table of Contents

I. GROUPS 1
1. Sets and Mappings 1
2. Products and Operations 3
3. Relations 4
4. Properties of the Integers 5
5. Groups 7
6. Elementary Properties of Groups 7
7. Subgroups 9
8. Cyclic and Finite Groups 10
9. Cosets and Normal Subgroups 11
10. Homomorphism 13
11. Quotient Groups 14
12. The Fundamental Theorem 16
13. Direct Products 17
14. Finite Cyclic Groups 19
15. Finite Abelian Groups 20
16. Permutation Groups 22
17. Computation of Transforms 24
18. The Regular Representation of a Group 25
19. Composition Series 26
20. References 28

II. RINGS AND FIELDS 29
1. Rings 29
2. Ring Homomorphism 30
3. The Characteristic of a Ring 31
4. Ideals 33
5. Difference Rings 35
6. Polynomials over a Ring 37
7. Construction of $\mathfrak{R}[x]$ 37
8. The Division Algorithm 38
9. Polynomials in n Independent Indeterminates 40
10. Integral Domains and Fields 41
11. Divisibility in a Commutative Ring 43
12. Prime and Maximal Ideals 44
13. The Ring of Integers 45
14. Factorization Theory in $\mathfrak{F}[x]$ 48
15. Ideal Theory in $\mathfrak{F}[x]$ 50
16. References 51

III. VECTOR SPACES AND MATRICES 52
1. Vector Spaces 52
2. Sums of Subspaces 53
3. Vector Spaces over a Field 55
4. Linear Mappings 56
5. The Space of n-tuples 57
6. Matrices 58
7. The Vector Space $\mathfrak{M}_{m,n}$ 61
8. The Matrix of a Linear Mapping 62
9. The Sign of a Permutation 64
10. Determinants 66
11. Non-singular Matrices 68
12. The Effect of a Change of Basis 68
13. Elementary Transformations over $\mathfrak{J}$ 70
14 Equivalence in $\mathfrak{F}$ and Determinantal Rank 72
15. Linear Systems 75
16. Equivalence in $\mathfrak{F}[x]$ 78
17. The Ring $\mathfrak{M}_n$ over $\mathfrak{F}[x]$ 82
18. Similarity of Square Matrices 83
19. Characteristic and Minimum Functions 83
20. The Companion Matrix of a Polynomial 85
21. Nilpotent Matrices 88
22. The Jordan Canonical Form 88
23. The Characteristic Roots of a Polynomial 94
24. References 95

IV. THEORY OF ALGEBRAIC EXTENSIONS 96
1. Simple Extensions 96
2. Algebraic Extensions of Finite Degree 97
3. Subfields 97
4. Splitting Fields 98
5. Composites 100
6. Binomial and Trinomial Equations 101
7. Separable Polynomials and Fields 102
8. The Artin Lemmas 105
9. Normal Fields 106
10. Characterizations of Normality 108
11. The Galois Group of an Equation 111
12. The Fundamental Theorems of the Galois Theory 112
13. Simple Extensions 114
14. The Characteristic Function of a Field 118
15. The Normal Basis Theorem 119
16. The Trace Theorem 121
17. References 122

V. FINITE FIELDS 123
1. Number of Elements 123
2. Existence and Uniqueness 124
3. The Cyclic Group $\mathfrak{F}^*$ 124
4. Primitive Roots Modulo m 125
5. The Galois Group of a Finite Field 127
6. Dedekind's Formula 128
7. Polynomials Belonging to an Exponent 130
8. Polynomials Belonging to a Prime 132
9. A Construction of Irreducible Polynomials 133
10. The Exceptional Case 135
11. Irreducible Polynomials of Even Degree 137
12. Applications 138
13. Polynomials of Degree p over $\mathfrak{F}_q$, $q = p^n$ 140
14. Dickson's Theorem 141
15. Generation of Irreducible Polynomials 142
16. The Cubing Transformation 143
17. Determination of Primitive Irreducible Polynomials 145
18. Miscellaneous Results 149
19. Historical Notes 155

APPENDIXES

I. TABLE OF LEAST PRIMITIVE ROOTS 157

II. EXTRACT FROM JACOBI'S CANON 158

III. BUSSEY'S TABLES 159

IV. IRREDUCIBLE POLYNOMIALS OVER $\mathfrak{F}_2$ 161

INDEX 163