Contents

Preface xi

Chapter 1. A Brief Classical Introduction 1

§1.1. Quadratic Forms as Polynomials 1

§1.2. Representation and Equivalence; Matrix Connections; Discriminants 4

Exercises 7

§1.3. A Brief Historical Sketch, and Some References to the Literature 7

Chapter 2. Quadratic Spaces and Lattices 13

§2.1. Fundamental Definitions 13

§2.2. Orthogonal Splitting; Examples of Isometry and Non-isometry 16

Exercises 20

§2.3. Representation, Splitting, and Isotropy; Invariants $u(F)$ and $s(F)$ 21

§2.4. The Orthogonal Group of a Space 26

§2.5. Witt's Cancellation Theorem and Its Consequences 29

§2.6. Witt's Chain Equivalence Theorem 34

§2.7. Tensor Products of Quadratic Spaces; the Witt ring of a field 35

Exercises 39

§2.8. Quadratic Spaces over Finite Fields 40

§2.9. Hermitian Spaces 44

Exercises 49

Chapter 3. Valuations, Local Fields, and p-adic Numbers 51
§3.1. Introduction to Valuations 51
§3.2. Equivalence of Valuations; Prime Spots on a Field 54
Exercises 58
§3.3. Completions, $\mathbb{Q}_p$, Residue Class Fields 59
§3.4. Discrete Valuations 63
§3.5. The Canonical Power Series Representation 64
§3.6. Hensel's Lemma, the Local Square Theorem, and Local Fields 69
§3.7. The Legendre Symbol; Recognizing Squares in $\mathbb{Q}_p$ 74
Exercises 76

Chapter 4. Quadratic Spaces over $\mathbb{Q}_p$ 81
§4.1. The Hilbert Symbol 81
§4.2. The Hasse Symbol (and an Alternative) 86
§4.3. Classification of Quadratic $\mathbb{Q}_p$-Spaces 87
§4.4. Hermitian Spaces over Quadratic Extensions of $\mathbb{Q}_p$ 92
Exercises 94

Chapter 5. Quadratic Spaces over $\mathbb{Q}$ 97
§5.1. The Product Formula and Hilbert's Reciprocity Law 97
§5.2. Extension of the Scalar Field 98
§5.3. Local to Global: The Hasse–Minkowski Theorem 99
§5.4. The Bruck–Ryser Theorem on Finite Projective Planes 105
§5.5. Sums of Integer Squares (First Version) 109
Exercises 111

Chapter 6. Lattices over Principal Ideal Domains 113
§6.1. Lattice Basics 114
§6.2. Valuations and Fractional Ideals 116
§6.3. Invariant factors 118
§6.4. Lattices on Quadratic Spaces 122
§6.5. Orthogonal Splitting and Triple Diagonalization 124
§6.6. The Dual of a Lattice 128
Exercises 130
§6.7. Modular Lattices 133
§6.8. Maximal Lattices 136
§6.9. Unimodular Lattices and Pythagorean Triples 138

§6.10. Remarks on Lattices over More General Rings 141
Exercises 142

Chapter 7. Initial Integral Results 145
§7.1. The Minimum of a Lattice; Definite Binary $\mathbb{Z}$-Lattices 146
§7.2. Hermite's Bound on $\min L$, with a Supplement for $k[x]$-Lattices 149
§7.3. Djokovič's Reduction of $k[x]$-Lattices; Harder's Theorem 153
§7.4. Finiteness of Class Numbers (The Anisotropic Case) 156
Exercises 158

Chapter 8. Local Classification of Lattices 161
§8.1. Jordan Splittings 161
§8.2. Nondyadic Classification 164
§8.3. Towards 2-adic Classification 165
Exercises 171

Chapter 9. The Local-Global Approach to Lattices 175
§9.1. Localization 176
§9.2. The Genus 178
§9.3. Maximal Lattices and the Cassels–Pfister Theorem 181
§9.4. Sums of Integer Squares (Second Version) 184
Exercises 187
§9.5. Indefinite Unimodular $\mathbb{Z}$-Lattices 188
§9.6. The Eichler–Kneser Theorem; the Lattice $\mathbb{Z}^n$ 191
§9.7. Growth of Class Numbers with Rank 196
§9.8. Introduction to Neighbor Lattices 201
Exercises 205

Chapter 10. Lattices over $\mathbb{F}_q[x]$ 207
§10.1. An Initial Example 209
§10.2. Classification of Definite $\mathbb{F}_q[x]$-Lattices 210
§10.3. On the Hasse–Minkowski Theorem over $\mathbb{F}_q(x)$ 218
§10.4. Representation by $\mathbb{F}_q[x]$-Lattices 220
Exercises 223

Chapter 11. Applications to Cryptography 225
§11.1. A Brief Sketch of the Cryptographic Setting 225
§11.2. Lattices in $\mathbb{R}^n$ 227

§11.3. LLL-Reduction 230
§11.4. Lattice Attacks on Knapsack Cryptosystems 235
§11.5. Remarks on Lattice-Based Cryptosystems 239

Appendix: Further Reading 241

Bibliography 245