Lectures on

FINITE FIELDS and GALOIS RINGS

Zhe-Xian Wan
Chinese Academy of Sciences, China
Contents

1 Sets and Integers .................................................. 1
  1.1 Sets and Maps .............................................. 1
  1.2 The Factorization of Integers ........................... 7
  1.3 Equivalence Relation and Partition .................... 15
  1.4 Exercises ................................................... 18

2 Groups ................................................................. 21
  2.1 The Concept of a Group and Examples ................. 21
  2.2 Subgroups and Cosets ...................................... 31
  2.3 Cyclic Groups .............................................. 38
  2.4 Exercises ................................................... 45

3 Fields and Rings .................................................. 49
  3.1 Fields ....................................................... 49
  3.2 The Characteristic of a Field .......................... 58
  3.3 Rings and Integral Domains .............................. 64
  3.4 Field of Fractions of an Integral Domain ............. 67
  3.5 Divisibility in a Ring .................................... 70
  3.6 Exercises ................................................... 72

4 Polynomials ......................................................... 75
  4.1 Polynomial Rings ........................................... 75
  4.2 Division Algorithm ....................................... 80
4.3 Euclidean Algorithm ........................................ 83
4.4 Unique Factorization of Polynomials ...................... 93
4.5 Exercises ..................................................... 99

5 Residue Class Rings ........................................... 101
5.1 Residue Class Rings ........................................ 101
5.2 Examples ..................................................... 106
5.3 Residue Class Fields ......................................... 108
5.4 More Examples ............................................... 111
5.5 Exercises ..................................................... 114

6 Structure of Finite Fields ..................................... 115
6.1 The Multiplicative Group of a Finite Field ................ 115
6.2 The Number of Elements in a Finite Field ................. 120
6.3 Existence of Finite Field with $p^n$ Elements ............. 122
6.4 Uniqueness of Finite Field with $p^n$ Elements .......... 127
6.5 Subfields of Finite Fields ................................... 128
6.6 A Distinction between Finite Fields of Characteristic 2 and Not 2 ........................................... 130
6.7 Exercises ..................................................... 133

7 Further Properties of Finite Fields ............................ 137
7.1 Automorphisms .............................................. 137
7.2 Characteristic Polynomials and Minimal Polynomials ....... 140
7.3 Primitive Polynomials ....................................... 145
7.4 Trace and Norm ............................................. 148
7.5 Quadratic Equations ........................................ 155
7.6 Exercises ..................................................... 158

8 Bases .......................................................... 161
8.1 Bases and Polynomial Bases .................................. 161
8.2 Dual Bases .................................................... 166
CONTENTS

<table>
<thead>
<tr>
<th>8.3</th>
<th>Self-dual Basis</th>
<th>173</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4</td>
<td>Normal Bases</td>
<td>180</td>
</tr>
<tr>
<td>8.5</td>
<td>Exercises</td>
<td>189</td>
</tr>
</tbody>
</table>

9 Factoring Polynomials over Finite Fields | 191

9.1 Factoring Polynomials over Finite Fields | 191
9.2 Factorization of $x^n - 1$ | 202
9.3 Cyclotomic Polynomials | 206
9.4 The Period of a Polynomial | 210
9.5 Exercises | 216

10 Irreducible Polynomials over Finite Fields | 219

10.1 On the Determination of Irreducible Polynomials | 219
10.2 Irreducibility Criterion of Binomials | 221
10.3 Some Irreducible Trinomials | 225
10.4 Compositions of Polynomials | 231
10.5 Recursive Constructions | 237
10.6 Composed Product and Sum of Polynomials | 241
10.7 Irreducible Polynomials of Any Degree | 244
10.8 Exercises | 246

11 Quadratic Forms over Finite Fields | 249

11.1 Quadratic Forms over Finite Fields of Characteristic Not 2 | 249
11.2 Alternate Forms over Finite Fields | 255
11.3 Quadratic Forms over Finite Fields of Characteristic 2 | 258
11.4 Exercises | 268

12 More Group Theory and Ring Theory | 271

12.1 Homomorphisms of Groups, Normal Subgroups and Factor Groups | 271
12.2 Direct Product Decomposition of Groups | 279
12.3 Some Ring Theory | 284
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4</td>
<td>Modules</td>
<td>292</td>
</tr>
<tr>
<td>12.5</td>
<td>Exercises</td>
<td>295</td>
</tr>
<tr>
<td>13</td>
<td>Hensel's Lemma and Hensel Lift</td>
<td>297</td>
</tr>
<tr>
<td>13.1</td>
<td>The Polynomial Ring $\mathbb{Z}_p[x]$</td>
<td>297</td>
</tr>
<tr>
<td>13.2</td>
<td>Hensel's Lemma</td>
<td>300</td>
</tr>
<tr>
<td>13.3</td>
<td>Factorization of Monic Polynomials in $\mathbb{Z}_p[x]$</td>
<td>302</td>
</tr>
<tr>
<td>13.4</td>
<td>Basic Irreducible Polynomials and Hensel Lift</td>
<td>304</td>
</tr>
<tr>
<td>13.5</td>
<td>Exercises</td>
<td>308</td>
</tr>
<tr>
<td>14</td>
<td>Galois Rings</td>
<td>309</td>
</tr>
<tr>
<td>14.1</td>
<td>Examples of Galois Rings</td>
<td>309</td>
</tr>
<tr>
<td>14.2</td>
<td>Structure of Galois Rings</td>
<td>313</td>
</tr>
<tr>
<td>14.3</td>
<td>The $p$-adic Representation</td>
<td>316</td>
</tr>
<tr>
<td>14.4</td>
<td>The Group of Units of a Galois Ring</td>
<td>319</td>
</tr>
<tr>
<td>14.5</td>
<td>Extension of Galois Rings</td>
<td>323</td>
</tr>
<tr>
<td>14.6</td>
<td>Automorphisms of Galois Rings</td>
<td>327</td>
</tr>
<tr>
<td>14.7</td>
<td>Generalized Trace and Norm</td>
<td>331</td>
</tr>
<tr>
<td>14.8</td>
<td>Exercises</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>335</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>339</td>
</tr>
</tbody>
</table>