

# CONTENTS

---

<i>Preface</i>	vii
<b>Part 1: Algebraic preliminaries</b>	1
<b>1 Groups, fields and vector spaces</b>	3
1.1. <i>Groups</i>	3
1.2. <i>Fields</i>	8
1.3. <i>Vector spaces</i>	9
<b>2 The axiom of choice, and Zorn's lemma</b>	14
2.1. <i>The axiom of choice</i>	14
2.2. <i>Zorn's lemma</i>	14
2.3. <i>The existence of a basis</i>	15
<b>3 Rings</b>	18
3.1. <i>Rings</i>	18
3.2. <i>Integral domains</i>	20
3.3. <i>Ideals</i>	21
3.4. <i>Irreducibles, primes and unique factorization domains</i>	24
3.5. <i>Principal ideal domains</i>	27
3.6. <i>Highest common factors</i>	29
3.7. <i>Polynomials over unique factorization domains</i>	31
3.8. <i>The existence of maximal proper ideals</i>	34
3.9. <i>More about fields</i>	35
<b>Part 2: The theory of fields, and Galois theory</b>	37
<b>4 Field extensions</b>	39
4.1. <i>Introduction</i>	39
4.2. <i>Field extensions</i>	40
4.3. <i>Algebraic and transcendental elements</i>	42
4.4. <i>Algebraic extensions</i>	46
4.5. <i>Monomorphisms of algebraic extensions</i>	48
<b>5 Tests for irreducibility</b>	49
5.1. <i>Introduction</i>	49

5.2. Eisenstein's criterion	51
5.3. Other methods for establishing irreducibility	52
<b>6 Ruler-and-compass constructions</b>	<b>54</b>
6.1. Constructible points	54
6.2. The angle $\pi/3$ cannot be trisected	57
6.3. Concluding remarks	58
<b>7 Splitting fields</b>	<b>59</b>
7.1. Splitting fields	60
7.2. The extension of monomorphisms	62
7.3. Some examples	67
<b>8 The algebraic closure of a field</b>	<b>71</b>
8.1. Introduction	71
8.2. The existence of an algebraic closure	72
8.3. The uniqueness of an algebraic closure	75
8.4. Conclusions	77
<b>9 Normal extensions</b>	<b>78</b>
9.1. Basic properties	78
9.2. Monomorphisms and automorphisms	80
<b>10 Separability</b>	<b>82</b>
10.1. Basic ideas	82
10.2. Monomorphisms and automorphisms	83
10.3. Galois extensions	84
10.4. Differentiation	85
10.5. The Frobenius monomorphism	87
10.6. Inseparable polynomials	88
<b>11 Automorphisms and fixed fields</b>	<b>91</b>
11.1. Fixed fields and Galois groups	91
11.2. The Galois group of a polynomial	94
11.3. An example	96
11.4. The fundamental theorem of Galois theory	97
11.5. The theorem on natural irrationalities	99
<b>12 Finite fields</b>	<b>101</b>
12.1. A description of the finite fields	101
12.2. An example	102
12.3. Some abelian group theory	103
12.4. The multiplicative group of a finite field	105
12.5. The automorphism group of a finite field	105
<b>13 The theorem of the primitive element</b>	<b>107</b>
13.1. A criterion in terms of intermediate fields	107
13.2. The theorem of the primitive element	108
13.3. An example	109
<b>14 Cubics and quartics</b>	<b>110</b>
14.1. Extension by radicals	110
14.2. The discriminant	111
14.3. Cubic polynomials	113

14.4. Quartic polynomials	115
<b>15</b> Roots of unity	118
15.1. Cyclotomic polynomials	118
15.2. Irreducibility	120
15.3. The Galois group of a cyclotomic polynomial	121
<b>16</b> Cyclic extensions	123
16.1. A necessary condition	123
16.2. Abel's theorem	124
16.3. A sufficient condition	125
16.4. Kummer extensions	128
<b>17</b> Solution by radicals	131
17.1. Soluble groups: examples	131
17.2. Soluble groups: basic theory	132
17.3. Polynomials with soluble Galois groups	134
17.4. Polynomials which are solvable by radicals	135
<b>18</b> Transcendental elements and algebraic independence	139
18.1. Transcendental elements and algebraic independence	139
18.2. Transcendence bases	141
18.3. Transcendence degree	143
18.4. The tower law for transcendence degree	144
18.5. Lüroth's theorem	145
<b>19</b> Some further topics	147
19.1. Generic polynomials	147
19.2. The normal basis theorem	150
19.3. Constructing regular polygons	152
<b>20</b> The calculation of Galois groups	155
20.1. A procedure for determining the Galois group of a polynomial	155
20.2. The soluble transitive subgroups of $\Sigma_p$	158
20.3. The Galois group of a quintic	161
20.4. Concluding remarks	162
Index	163