
Contents

Acknowledgments	xi
Preface	xiii
List of Mathematical Symbols	xvii
Chapter 1. The Structures of Ring and Field	1
1.1. Rings	1
1.1.1. The ring structure	1
1.1.2. Cardinal of a ring	3
1.1.3. Commutative ring	3
1.1.4. Homomorphism and isomorphism of rings	4
1.1.5. Examples of rings	4
1.1.6. Sub-ring of a ring	10
1.1.7. Ideal of a ring	12
1.1.8. Quotient ring	14
1.1.9. Unitary ring	15
1.1.10. Characteristic of a unitary ring	16
1.1.11. Unit in a unitary ring	17
1.1.12. Zero divisor in a ring	18
1.1.13. Integrity ring	20
1.2. Fields	20
1.2.1. The field structure	20
1.2.2. Cardinal of a field	23
1.2.3. Commutative field	23

1.2.4. Isomorphism and automorphism of fields	23
1.2.5. Examples of fields	24
1.2.6. Sub-field of a field	30
1.2.7. Characteristic of a field	31
Chapter 2. Galois Fields	33
2.1. Generalities	33
2.1.1. Wedderburn's theorem	33
2.1.2. Galois field	34
2.2. Extension of a field: a typical example	37
2.3. Extension of a field: the general case	41
2.3.1. Reducible, irreducible and prime polynomials	42
2.3.2. Examples of (ir)reducible and prime polynomials	45
2.3.3. Quotient field	49
2.3.4. Group structures	51
2.3.5. Primitive element and primitive polynomial	53
2.3.6. Logarithm of a field element	58
2.3.7. Practical rules for constructing a Galois field	59
2.3.8. Examples of extensions of fields	61
2.3.9. Matrix realization of a Galois field	76
2.4. Sub-field of a Galois field	81
2.4.1. $\mathbb{GF}(p^\ell)$ sub-field of $\mathbb{GF}(p^m)$	81
2.4.2. Characteristic of the sub-fields of $\mathbb{GF}(p^m)$	82
2.5. Factorizations	82
2.5.1. Powers of elements of $\mathbb{GF}(p^m)$	82
2.5.2. Solutions of $\xi^{p^m} - \xi = 0$	83
2.5.3. Product of all the elements of $\mathbb{GF}(p^m)^*$	86
2.5.4. Factorization of $\xi^{p^m} - \xi$ in prime polynomials	87
2.5.5. Factorization of a prime polynomial	90
2.6. The application trace for a Galois field	95
2.6.1. Trace of an element	95
2.6.2. Frobenius automorphism	96
2.6.3. Elementary properties of the trace	98
2.6.4. Linearity of the trace	104
2.6.5. Trace in terms of the roots of a prime polynomial	107

2.7. Bases of a Galois field	108
2.7.1. Generalities	108
2.7.2. Field bases	109
2.7.3. Dual and self-dual bases	115
2.8. Characters of a Galois field	118
2.8.1. Additive characters	118
2.8.2. Multiplicative characters	125
2.9. Gaussian sums over Galois fields	130
2.9.1. Gauss sum over \mathbb{Z}_d	130
2.9.2. Quadratic Gauss sum and quadratic characters	131
2.9.3. Gauss sum over $\mathbb{GF}(p^m)$	132
2.9.4. Weil sum over $\mathbb{GF}(p^m)$	133
Chapter 3. Galois Rings	135
3.1. Generalities	136
3.1.1. Principal ideal of a commutative ring	136
3.1.2. Galois ring	136
3.2. Construction of a Galois ring	137
3.2.1. Elements of \mathbb{Z}_{p^s}	137
3.2.2. The $\mathbb{Z}_{p^s} \rightarrow \mathbb{Z}_p$ and $\mathbb{Z}_{p^s}[\xi] \rightarrow \mathbb{Z}_p[\xi]$ homomorphisms	138
3.2.3. Basic irreducible polynomial	140
3.2.4. Extension of a base ring	141
3.2.5. Isomorphism of two Galois rings	142
3.2.6. Sub-ring of a Galois ring	143
3.2.7. adic (p -adic) decomposition	143
3.3. Examples and counter-examples of Galois rings	145
3.3.1. Counter-examples	145
3.3.2. Examples	149
3.4. The application trace for a Galois ring	153
3.4.1. Generalized Frobenius automorphism and trace	153
3.4.2. Elementary properties of the trace	154
3.5. Characters of a Galois ring	155

3.6. Gaussian sums over Galois rings	156
3.6.1. Gauss sum over $\mathbb{GR}(p^s, m)$	156
3.6.2. Weil sum over $\mathbb{GR}(p^s, m)$	156
Chapter 4. Mutually Unbiased Bases	159
4.1. Generalities	161
4.1.1. Unbiased bases	161
4.1.2. Example: $d = 2$	161
4.1.3. Interests of MUBs for quantum mechanics	162
4.1.4. Well-known results	163
4.2. Quantum angular momentum bases	165
4.2.1. Standard basis for $SU(2)$	165
4.2.2. Non-standard bases for $SU(2)$	167
4.2.3. Bases in quantum information	168
4.3. $SU(2)$ approach to mutually unbiased bases	172
4.3.1. A master formula for $d = p$ (p prime)	172
4.3.2. Examples: $d = 2$ and 3	175
4.3.3. An alternative formula for $d = p$ (p odd prime)	177
4.3.4. Weyl pairs	177
4.3.5. MUBs and the special linear group	183
4.3.6. MUBs for d power of a prime	184
4.4. Galois field approach to mutually unbiased bases	189
4.4.1. Weyl pair for $\mathbb{GF}(p^m)$	190
4.4.2. Bases in the frame of $\mathbb{GF}(p^m)$	191
4.4.3. MUBs in the frame of $\mathbb{GF}(p^m)$	193
4.5. Galois ring approach to mutually unbiased bases	194
4.5.1. Bases in the frame of $\mathbb{GR}(2^2, m)$	194
4.5.2. MUBs in the frame of $\mathbb{GR}(2^2, m)$	195
4.5.3. One- and two-qubit systems	196
Chapter 5. Appendix on Number Theory and Group Theory	199
5.1. Elements of number theory	199
5.1.1. Euler function	199
5.1.2. Möbius function	200
5.1.3. Root of unity	201
5.1.4. Cyclotomic polynomials	203

5.1.5. Residue	205
5.1.6. Quadratic residue	206
5.1.7. Gauss sums	210
5.2. Elements of group theory	214
5.2.1. Axioms of group	214
5.2.2. Direct product of groups	215
5.2.3. Homomorphism, isomorphism and automorphism of groups	216
5.2.4. Conjugate classes	216
5.2.5. Sub-group	217
5.2.6. Cyclic group	217
5.2.7. Cosets	218
5.2.8. Lagrange's theorem	219
5.2.9. Order of a group element	219
5.2.10. Quotient group	220
5.2.11. Abstract group - group table	220
5.2.12. Examples of groups	222
5.2.13. Representations of a group	225
5.2.14. Orthogonality relations	227
Bibliography	233
Index	243