Galois Fields

Chapter 1: A Review of Modern Algebra

groups, subgroups, cosets, normal subgroups, factor group, cyclic subgroups,
order, generators, additive cyclic subgroups,
rings, ideals, residue classes, residue class rings, principle ideals,
the example Z_n = modulo-n, the Division Algorithm,
the Factorization Theorem, the Euclidean Division Algorithm, relative primeness,
the fact that Z/(n) = Z_n is a field if n is prime

Chapter 2: The Galois Fields GF(p)

GF(p) = Z_p , facts about

Chapter 3: Polynomials

the field F underlying a polynomial, polynomials form a ring,
quotient and remainder polynomials, irreducible polynomials,
the construction GF(p^m) = Poly[x,GF(p)] / (f(x),m),
ground field and extension field, f(x) must be irreducible.

Chapter 4: The Galois Fields GF(q=p^m)

m-tuple notation, facts about the order of an element, roots of f(x),
{ GF(q) - 0, • } is cyclic, exponents, primitive elements α,
all GF(q) field elements are roots of x^{q-1}- 1, examples

Chapter 5: Minimum Polynomials

minimum polynomials, monic, primitive polynomials,
period, conjugate set of α, finding primitive polynomials,

Chapter 6: The Galois Field Table

how to construct a complete GF(q) field algebra from any primitive polynomial

Chapter 7: Galois-Based Cyclic Codes

linear block codes, symbols, parity check, data words, code words, matrices G and H,
dual code, minimum distance d, error-correction of t-symbol errors in a codeword,
the syndrome, major codes, code history
cyclic codes, cyclic vs systematic basis, implementation of encoders, CRC,
proof that cyclic codes are cyclic, the standard array as an ideal,
the connection between cyclic codes and Galois Fields,
general BCH codes, narrow-sense BCH codes, Hamming codes,
Reed Solomon Codes, digital filters

Chapter 8: Matrix representations of Galois Fields

a review of matrix algebra, characteristic polynomial of a matrix
polynomials of a matrix, the Cayley-Hamilton theorem, ways to think of a remainder,
matrix representation of a Galois Field, the compansion matrix forms, examples