Sidong Guo

0.1 Galois Fields

Fundamentals for understanding Non-binary codes like BCH and Reed-Solomon

Definition 0.1

A Galois Field, or finite field, is defined as a set $(\mathbb{F}, +, \times)$ with two operations such that:
1.$(\mathbb{F}, +)$is a commutative group with identity 0
2.$(\mathbb{F}, \times)$is a commutative group with identity 1
3.Multiplication distributes over addition

☞ **Remark**
$\forall$ a in $\mathbb{F}$, there necessarily exists a additive inverse and multiplicative inverse with $a + (-a) = 0$ and $a * a^{-1} = 1$; a(b+c)=ab+ac.

Definition 0.2

A field $\mathbb{F}$ with a finite number, q of elements is $\mathbb{F}_q$

Theorem 0.1

Any integer $n \in \mathbb{N}^*$ can be factored into an unique product of prime numbers

☞ **Remark**
Proof by Contradiction

Theorem 0.2

let $m, n \in \mathbb{Z}$ with greatest common divisor g. Then, $\exists a, b \in \mathbb{Z}$ such that $g = am + bn$

Theorem 0.3

For any prime p, $\mathbb{Z}_p = [0, p-1]$ forms a field under modulo p addition and multiplication. The characteristic of the field is p

☞ **Remark**
It is easily provable that both $(\mathbb{Z}_p; +_{modp})$ and $(\mathbb{Z}_p; \times_{modp})$ are groups because in fact:

$$\forall m \in \mathbb{Z}_p \qquad m + 0 = 0 + m = m \tag{1}$$

$$\forall m \in \mathbb{Z}_p \qquad m \times 1 = 1 \times m = m \tag{2}$$

Also by definition $gcd(p, m) = 1$, then by Theorem 2 we have $1 = ap + bm$, and therefore there exists a such that $bm = 1 \mod p$

Theorem 0.4

Every field $\mathbb{F}$ with a prime number p of elements is isomorphic to $\mathbb{Z}_p$ via the correspondence:

$$(i)1 \in \mathbb{F} \Leftrightarrow i \in \mathbb{Z}_p \tag{3}$$

Theorem 0.5

if $\alpha, \beta \in \mathbb{F}_q$ with characteristic p prime, then $(\alpha+\beta)^p = \alpha^p + \alpha^p$

Definition 0.3

A non-zero polynomial f(x) of degree m over $\mathbb{F}$ has expression:

$$f(x) = \sum_{i=1}^{m} f_i x^i \quad with \quad [f_i]_{i[1,m]} \in \mathbb{F}^m \quad and \quad f_m \neq 0 \tag{4}$$

☞ **Remark**

A monic polynomial of degree m has $f_m = 1$; Polynomials over a field has coefficients within the field; The set of all polynomials over $\mathbb{F}$ is $\mathbb{F}[x]$

Theorem 0.6

If $\mathbb{F}_q$ is a Galois field and there exists a prime polynomial $g(x) \in \mathbb{F}_q[x]$ of degree m, then $\mathbb{F}_{g(x)}$ with addition and multiplication modulo $g(x)$ in $\mathbb{F}_q[x]$ is a field with q^m elements

Definition 0.4

if $f(x) \in \mathbb{F}_q[x]$ has a degree 1 factor $(x-\alpha)$, then α is a root of $f(x)$

Theorem 0.7

A monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree m has at most m roots in $\mathbb{F}_q$, $\beta_{i i\in[1,m]}$, then the unique factorization is

$$f(x) = \prod_{i=1}^{m} (x - \beta_i) \tag{5}$$

Theorem 0.8

A minimal polynomial w.r.t $\mathbb{F}_q$ of $\beta \in \mathbb{F}_{q^m}^*$ is a lowest degree monic polynomial M_β in $\mathbb{F}_q[x]$ such that $M_\beta(\beta) = 0$

☞ **Remark**

The polynomial $x^4 - 1$ factorizes over GF(2)[x]as:

$$x^4 - 1 = x(x+1)(x^2+x+1) \tag{6}$$

of which (x^2+x+1) is primitive; a polynomial of degree n is primitive over galois field GF(2) if it has polynomial order $2^n - 1$