Finite Fields

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

September 25, 2014

Fields

Definition

A set F together with two binary operations $+$ and $*$ is a field if

- F is an abelian group under $+$ whose identity is called 0
- $F^* = F \setminus \{0\}$ is an abelian group under $*$ whose identity is called 1
- For any $a, b, c \in F$

$$a * (b + c) = a * b + a * c$$

Definition

A finite field is a field with a finite cardinality.

Example

$\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$ with mod p addition and multiplication where p is a prime. Such fields are called prime fields.

Some Observations

Example

- $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$
- $2^5 = 2 \bmod 5$, $3^5 = 3 \bmod 5$, $4^5 = 4 \bmod 5$
- All elements of $\mathbb{F}_5$ are roots of $x^5 - x$
- $2^2 = 4 \bmod 5$, $2^3 = 3 \bmod 5$, $2^4 = 1 \bmod 5$
- $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ is cyclic

Example

- $F = \{0, 1, y, y + 1\}$ under $+$ and $*$ modulo $y^2 + y + 1$
- $y^4 = y \bmod (y^2 + y + 1)$, $(y + 1)^4 = y + 1 \bmod (y^2 + y + 1)$
- All elements of F are roots of $x^4 - x$
- $(y + 1)^2 = y \bmod (y^2 + y + 1)$, $(y + 1)^3 = 1 \bmod (y^2 + y + 1)$
- $F^* = \{1, y, y + 1\}$ is cyclic

Field Isomorphism

Definition

Fields F and G are isomorphic if there exists a bijection $\phi : F \to G$ such that

$$\begin{aligned} \phi(\alpha + \beta) &= \phi(\alpha) \oplus \phi(\beta) \\ \phi(\alpha \star \beta) &= \phi(\alpha) \otimes \phi(\beta) \end{aligned}$$

for all $\alpha, \beta \in F$.

Example

- $F = \left\{ a_0 + a_1 x + a_2 x^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $x^3 + x + 1$
- $G = \left\{ a_0 + a_1 x + a_2 x^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $x^3 + x^2 + 1$

Uniqueness of a Prime Field

Theorem

Every field F with a prime cardinality p is isomorphic to $\mathbb{F}_p$

Proof.

- Let F be any field with p elements where p is prime
- F has a multiplicative identity 1
- Consider the additive subgroup $S(1) = \langle 1 \rangle = \{1, 1+1, \ldots\}$
- By Lagrange's theorem, $|S(1)|$ divides p
- Since $1 \neq 0$, $|S(1)| \geq 2 \implies |S(1)| = p \implies S(1) = F$
- Every element in F is of the form $\underbrace{1 + 1 + \cdots + 1}_{i \text{ times}}$
- F is a field under the operations
  $\underbrace{1 + 1 + \cdots + 1}_{i \text{ times}} + \underbrace{1 + 1 + \cdots + 1}_{j \text{ times}} = \underbrace{1 + 1 + \cdots + 1}_{i+j \bmod p \text{ times}}$ and
  $\underbrace{1 + 1 + \cdots + 1}_{i \text{ times}} * \underbrace{1 + 1 + \cdots + 1}_{j \text{ times}} = \underbrace{1 + 1 + \cdots + 1}_{ij \bmod p \text{ times}}$

Proof of F being Isomorphic to $\mathbb{F}_p$

Consider the bijection $\phi : F \to \mathbb{F}_p$

$$\phi\left(\underbrace{1+1+\cdots+1}_{i\text{ times}}\right) = i \bmod p$$

$$\begin{aligned}\phi\left(\underbrace{1+\cdots+1}_{i\text{ times}}+\underbrace{1+\cdots+1}_{j\text{ times}}\right) &= \phi\left(\underbrace{1+\cdots+1}_{i+j\text{ times}}\right)\\ = (i+j) \bmod p &= i \bmod p + j \bmod p\end{aligned}$$

$$\begin{aligned}\phi\left(\underbrace{[1+\cdots+1]}_{i\text{ times}}*\underbrace{[1+\cdots+1]}_{j\text{ times}}\right) &= \phi\left(\underbrace{1+\cdots+1}_{ij\text{ times}}\right)\\ = ij \bmod p &= (i \bmod p)\,(j \bmod p)\end{aligned}$$

Subfields

Definition

A nonempty subset S of a field F is called a subfield of F if

- $\alpha + \beta \in S$ for all $\alpha, \beta \in S$
- $-\alpha \in S$ for all $\alpha \in S$
- $\alpha * \beta \in S \setminus \{0\}$ for all nonzero $\alpha, \beta \in S$
- $\alpha^{-1} \in S \setminus \{0\}$ for all nonzero $\alpha \in S$

Example

$F = \{0, 1, x, x + 1\}$ under $+$ and $*$ modulo $x^2 + x + 1$
$\mathbb{F}_2$ is a subfield of F

Characteristic of a Field

Definition

Let F be a field with multiplicative identity 1. The characteristic of F is the smallest integer p such that

$$\underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ times}} = 0$$

Examples

- $\mathbb{F}_2$ has characteristic 2
- $\mathbb{F}_5$ has characteristic 5
- $\mathbb{R}$ has characteristic 0

Theorem

The characteristic of a finite field is prime

Prime Subfield of a Finite Field

Theorem

Every finite field has a prime subfield.

Examples

- $\mathbb{F}_2$ has prime subfield $\mathbb{F}_2$
- $F = \{0, 1, x, x + 1\}$ under $+$ and $*$ modulo $x^2 + x + 1$ has prime subfield $\mathbb{F}_2$

Proof.

- Let F be any field with q elements
- F has a multiplicative identity 1
- Consider the additive subgroup $S(1) = \langle 1 \rangle = \{1, 1 + 1, \ldots\}$
- $|S(1)| = p$ where p is the characteristic of F
- $S(1)$ is a subfield of F and is isomorphic to $\mathbb{F}_p$

□

Order of a Finite Field

Theorem

Any finite field has p^m elements where p is a prime and m is a positive integer.

Example

- $F = \{0, 1, x, x+1\}$ has 2^2 elements

Proof.

- Let F be any field with q elements and characteristic p
- F has a subfield isomorphic to $\mathbb{F}_p$
- F is a vector space over $\mathbb{F}_p$
- F has a finite basis $v_1, v_2, \ldots, v_m$
- Every element of F can be written as $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m$ where $\alpha_i \in \mathbb{F}_p$

□

Polynomials over a Field

Definition

A nonzero polynomial over a field F is an expression

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_m x^m$$

where $f_i \in F$ and $f_m \neq 0$. If $f_m = 1$, $f(x)$ is said to be monic.

Definition

The set of all polynomials over a field F is denoted by $F[x]$

Examples

- $\mathbb{F}_3 = \{0, 1, 2\}$, $x^2 + 2x \in \mathbb{F}_3[x]$ and is monic
- $x^2 + 5$ is a monic polynomial in $\mathbb{R}[x]$

Divisors of Polynomials over a Field

Definition

A polynomial $a(x) \in F[x]$ is said to be a divisor of a polynomial $b(x) \in F[x]$ if $b(x) = q(x)a(x)$ for some $q(x) \in F[x]$

Example

$x - i\sqrt{5}$ is a divisor of $x^2 + 5$ in $\mathbb{C}[x]$ but not in $\mathbb{R}[x]$

Definition

Every polynomial $f(x)$ in $F[x]$ has trivial divisors consisting of nonzero elements in F and $\alpha f(x)$ where $\alpha \in F \setminus \{0\}$

Examples

- In $\mathbb{F}_3[x]$, $x^2 + 2x$ has trivial divisors 1,2, $x^2 + 2x$, $2x^2 + x$
- In $\mathbb{F}_5[x]$, $x^2 + 2x$ has trivial divisors 1, 2, 3, 4, $x^2 + 2x$, $2x^2 + 4x$, $3x^2 + x$, $4x^2 + 3x$

Prime Polynomials

Definition

An irreducible polynomial is a polynomial of degree 1 or more which has only trivial divisors.

Examples

- In $\mathbb{F}_3[x]$, $x^2 + 2x$ has non-trivial divisors x, $x + 2$ and is not irreducible
- In $\mathbb{F}_3[x]$, $x + 2$ has only trivial divisors and is irreducible
- In any $F[x]$, $x + \alpha$ where $\alpha \in F$ is irreducible

Definition

A monic irreducible polynomial is called a prime polynomial.

Constructing a Field of p^m Elements

- Choose a prime polynomial $g(x)$ of degree m in $\mathbb{F}_p[x]$
- Consider the set of remainders when polynomials in $\mathbb{F}_p[x]$ are divided by $g(x)$

$$R_{\mathbb{F}_p,m} = \left\{ r_0 + r_1 x + \cdots + r_{m-1} x^{m-1} \middle| r_i \in \mathbb{F}_p \right\}$$

- The cardinality of $R_{\mathbb{F}_p,m}$ is p^m
- $R_{\mathbb{F}_p,m}$ with addition and multiplication mod $g(x)$ is a field

Examples

- $R_{\mathbb{F}_2,2} = \{0, 1, x, x+1\}$ is a field under $+$ and $*$ modulo $x^2 + x + 1$
- $R_{\mathbb{F}_2,3} = \left\{ r_0 + r_1 x + r_2 x^2 \middle| r_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $x^3 + x + 1$

Factorization of Polynomials

Theorem

Every monic polynomial $f(x) \in F[x]$ can be written as a product of prime factors

$$f(x) = \prod_{i=1}^{k} a_i(x)$$

where each $a_i(x)$ is a prime polynomial in $F[x]$. The factorization is unique, up to the order of the factors.

Examples

- In $\mathbb{F}_2[x]$, $x^3 + 1 = (x + 1)(x^2 + x + 1)$
- In $\mathbb{C}[x]$, $x^2 + 5 = (x + i\sqrt{5})(x - i\sqrt{5})$
- In $\mathbb{R}[x]$, $x^2 + 5$ is itself a prime polynomial

Roots of Polynomials

Definition

If $f(x) \in F[x]$ has a degree 1 factor $x - \alpha$ for some $\alpha \in F$, then α is called a root of $f(x)$

Examples

- In $\mathbb{F}_2[x]$, $x^3 + 1$ has 1 as a root
- In $\mathbb{C}[x]$, $x^2 + 5$ has two roots $\pm i\sqrt{5}$
- In $\mathbb{R}[x]$, $x^2 + 5$ has no roots

Theorem

In any field F, a monic polynomial $f(x) \in F[x]$ of degree m can have at most m roots in F. If it does have m roots $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, then the unique factorization of $f(x)$ is

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m).$$

Multiplicative Cyclic Subgroups in a Field

Theorem

In any field F, the multiplicative group F^* of nonzero elements has at most one cyclic subgroup of any given order n. If such a subgroup exists, then its elements $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ satisfy

$$x^n - 1 = (x - 1)(x - \beta)(x - \beta^2) \cdots (x - \beta^{n-1}).$$

Examples

- In $\mathbb{R}^*$, cyclic subgroups of order 1 and 2 exist.
- In $\mathbb{C}^*$, cyclic subgroups exist for every order n.

Multiplicative Cyclic Subgroups in a Field

Proof of Theorem.

- Let S be a cyclic subgroup of F^* having order n.
- Then $S = \{\beta, \beta^2, \ldots, \beta^{n-1}, \beta^n = 1\}$ for some $\beta \in S$.
- For every $\alpha \in S$, $\alpha^n = 1 \implies \alpha$ is a root of $x^n - 1 = 0$.
- Since $x^n - 1$ has at most n roots in F, S is unique.
- Since β^i is a root, $x - \beta^i$ is a factor of $x^n - 1$ for $i = 1, \ldots, n$
- By the uniqueness of factorization, we have

$$x^n - 1 = (x - 1)(x - \beta)(x - \beta^2) \cdots (x - \beta^{n-1}).$$

□

Factoring $x^q - x$ over a Field F_q

- Let F_q be a finite field of order q
- For any $\beta \in F_q^*$, let $S(\beta) = \{\beta, \beta^2, \ldots, \beta^n = 1\}$ be the cyclic subgroup of F_q^* generated by β
- The cardinality $|S(\beta)|$ is called the multiplicative order of β and $\beta^{|S(\beta)|} = 1$
- By Lagrange's theorem, $|S(\beta)|$ divides $|F_q^*| = q - 1$
- So for any $\beta \in F_q^*$, $\beta^{q-1} = 1$

Theorem

In a finite field F_q with q elements, the nonzero elements of F_q are the $q - 1$ distinct roots of $x^{q-1} - 1$

$$x^{q-1} - 1 = \prod_{\beta \in F_q^*} (x - \beta).$$

The elements of F_q are the q distinct roots of $x^q - x$, i.e. $x^q - x = \prod_{x \in F_q} (x - \beta)$

Factoring $x^q - x$ over a Field F_q

Example

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

$$\begin{aligned} (x-1)(x-2)(x-3)(x-4) &= x^4 - 10x^3 + 35x^2 - 50x + 24 \\ &= x^4 - 1 \\ x(x-1)(x-2)(x-3)(x-4) &= x^5 - x \end{aligned}$$

Example

$F = \{0, 1, y, y+1\} \subset \mathbb{F}_2[y]$ under $+$ and $*$ modulo $y^2 + y + 1$

$$\begin{aligned} (x-1)(x-y)(x-y-1) &= x^3 - x^2(y+1+y+1) \\ &\quad + x(y+y+1+y^2+y) \\ &\quad - y^2 - y \\ &= x^3 - 1 \\ x(x-1)(x-y)(x-y-1) &= x^4 - x \end{aligned}$$

F_q^* is Cyclic

- A primitive element of F_q is an element α with $|S(\alpha)| = q - 1$
- If α is a primitive element, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\} = F_q^*$
- To show that F_q^* is cyclic, it is enough to show that a primitive element exists
- By Lagrange's theorem, the multiplicative order $|S(\beta)|$ of every $\beta \in F_q^*$ divides $q - 1$
- The size d of a cyclic subgroup of F_q^* divides $q - 1$
- The number of elements having order d in a cyclic subgroup of size d is $\phi(d)$
- In F_q^*, there is at most one cyclic group of each size d
- All elements in F_q^* having same multiplicative order d have to belong to the same subgroup of order d

F_q^* is Cyclic

- The number of elements in F_q^* having order less than $q-1$ is at most
$$\sum_{d:d|(q-1),d\neq q-1} \phi(d)$$
- The Euler numbers satisfy
$$q-1 = \sum_{d:d|(q-1)} \phi(d)$$
so we have
$$q-1-\sum_{d:d|(q-1),d\neq q-1} \phi(d) = \phi(q-1)$$
- F_q^* has at least $\phi(q-1)$ elements of order $q-1$
- Since $\phi(q-1) \geq 1$, F_q^* is cyclic

Summary of Results

- Every finite field has a prime subfield isomorphic to $\mathbb{F}_p$
- Any finite field has p^m elements where p is a prime and m is a positive integer.
- Given an irreducible polynomial $g(x)$ of degree m in $\mathbb{F}_p[x]$, the set of remainders $R_{\mathbb{F}_p,m}$ is a field under $+$ and $*$ modulo $g(x)$
- The nonzero elements of a finite field F_q are the $q-1$ distinct roots of $x^{q-1}-1$
- The elements of F_q are the q distinct roots of $x^q - x$
- F_q^* is cyclic

Some More Results

- Every finite field F_q having characteristic p is isomorphic to a polynomial remainder field $F_{g(x)}$ where $g(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree m
- All finite fields of same size are isomorphic
- Finite fields with p^m elements exist for every prime p and integer $m \geq 1$

Questions? Takeaways?