Lecture 11 : Finite Fields I

Objectives

(1) Existence and uniqueness of finite fields.
(2) Algebraic closure of a finite field.
(3) Finite subgroup of the multiplicative group of a field is cyclic.
(4) Gauss' formula for the number of monic irreducible polynomials of a given degree over a finite field.

Key words and phrases: Finite field, Gauss' formula for irreducible polynomials,

---

A finite field F of prime characteristic p contains a prime field $\mathbb{F}_p$. Since F is a finite dimensional vector space over $\mathbb{F}_p$, $|F| = p^n$, where $n = [F : \mathbb{F}_p]$. We usually write $p^n = q$.

Proposition 11.1. *Let K and L be finite fields of cardinality $q = p^n$, where p is a prime number. Then K and L are isomorphic.*

Proof. Since $|K^\times| = q - 1$, by Lagrange's theorem $x^{q-1} = 1$ for all $x \in K^\times$. Thus every element of K is a root of the polynomial $x^q - x = f(x)$. Hence K is a splitting field of $f(x)$ over $\mathbb{F}_p$. Since any two splitting fields of $f(x)$ over $\mathbb{F}_p$ are isomorphic, $K \simeq L$. □

Notation: We shall denote a finite field with p^n elements by $\mathbb{F}_{p^n}$.

Corollary 11.2 (Wilson). *Let p be a prime number. Then*

$$(p-1)! \equiv -1(\ mod\ p).$$

Proof. The assertion is clear for $p = 2$. Let p be odd. Since $\mathbb{F}_p$ is the set of roots of $x^{p^n} - x$, taking $n = 1$ we get

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1)).$$

Putting $x = 0$ we obtain $(p-1)! \equiv -1(\ \mathrm{mod}\ p)$. □

Proposition 11.3. *For any prime p and any $n \in \mathbb{N}$, there exists a finite field of cardinality p^n. An algebraic closure $\mathbb{F}_p^a$ of $\mathbb{F}_p$ has a unique subfield with p^n elements for every $n \in \mathbb{N}$ and*

$$\mathbb{F}_p^a = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}.$$

Proof. Let $q = p^n$. Then $\mathbb{F}_p^a$ contains a unique splitting field of $x^q - x = f(x)$ over $\mathbb{F}_p$. Let

$$K = \{\alpha \in \mathbb{F}_p^\alpha \mid f(\alpha) = 0\}.$$

Then K is a field. The polynomial $x^q - x$ is separable since its derivative is -1. Hence K has q elements. Therefore K is the required finite field with q elements. Let a be algebraic over $\mathbb{F}_p$ and $[\mathbb{F}_p(a) : \mathbb{F}_p] = n$. Then $\mathbb{F}_p(a)$ has p^n elements. Hence $a \in \mathbb{F}_{p^n}$. Thus $\mathbb{F}_p^a = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$. □

Theorem 11.4. *Let U be a finite subgroup of the multiplicative group $F^\times$ of a field F. Then U is cyclic.*

Proof. Let $|U| = n$. By Lagrange's Theorem $x^n = 1$ for all $x \in U$. Since U is an abelian group, by the structure theorem for finite abelian groups, there exist $d_1, d_2, \ldots, d_r \in \mathbb{N}$ such that $n = d_1 d_2 \ldots d_r$, $d_1 \mid d_2 \mid \cdots \mid d_r$, and

$$U \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

Thus each $x \in U$ satisfies $x^{d_r} - 1 = 0$. But $x^{d_r} - 1$ has atmost d_r roots. Thus $n = d_r$ and so U is cyclic. □

Counting irreducible polynomials over finite fields

Let $N_q(n)$ denote the number of irreducible polynomials of degree n over a finite field F_q. We derive a formula, due to Gauss, for $N_q(n)$. Let α be a cyclic generator of $F_{q^n}^\times$. Then $F_{q^n} = F_q(\alpha)$ and $\deg \operatorname{irr}(\alpha, F_q) = [F_{q^n} : F_q] = n$. Hence $N_q(n) \geq 1$. Recall the Möbius inversion formula. Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions so that

$$f(n) = \sum_{d \mid n} g(d).$$

Then

$$g(n) = \sum_{d \mid n} f(n/d)\mu(d),$$

where μ is the Möbius function $\mu : \mathbb{N} \to \mathbb{N}$ defined as

$$\mu(n) = \begin{cases} 1 \text{ for } n = 1 \\ (-1)^r \text{ if } n = p_1 \dots p_r, \text{ where } p_1, \dots, p_r \text{ are distinct primes,} \\ 0 \text{ if } \ p^2 | n \text{ for some prime } p. \end{cases}$$

Theorem 11.5 (Gauss). *The number of irreducible monic polynomials of degree n over $\mathbb{F}_q$ is given by*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Proof. Let $f(x)$ be a monic irreducible polynomial in $\mathbb{F}_q[x]$. We show that $f(x) \mid x^{q^n} - x$ if and only if $\deg f \mid n$.

Suppose $f(x) \mid x^{q^n} - x$. Then $\mathbb{F}_{q^n}$ contains all the roots of $f(x)$. Let α be a root of $f(x)$. Then $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$. Thus $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d = \deg f \mid n$.

Conversely, let $d = \deg f \mid n$. Let $f(\alpha) = 0$, where $\alpha \in \mathbb{F}_q^a$. Let β be another root of $f(x)$ in $\mathbb{F}_q^a$. Then there exists an embedding $\sigma : \mathbb{F}_q(\alpha) \to \mathbb{F}_q(\beta)$ such that $\sigma(\alpha) = \beta$. Since $F_q(\alpha)$ is a splitting field of $x^{q^d} - x$ over $\mathbb{F}_q$, so is $\sigma(\mathbb{F}_q(\alpha)) = \mathbb{F}_q(\beta)$. But $\mathbb{F}_q^a$ has only one splitting field of $x^{q^d} - x$, hence $\beta \in F_q(\alpha)$. Thus $f(x) \mid x^{q^n} - x$.

Notice that $x^{q^n} - x$ is a separable polynomial. Hence

$$x^{q^n} - x = \prod_{d|n} f_1^{(d)}(x) \cdots f_{N_q(d)}^{(d)}(x),$$

where $f_1^{(d)}(x), \dots, f_{N_q(d)}^{(d)}(x)$ are all the degrees d irreducible polynomials over F_q. Equate degrees to get $q^n = \sum_{d|n} d N_q(d)$. By Möbius inversion

$$n N_q(n) = \sum_{d|n} \mu(n/d) q^d.$$

□