Class109: Finite Fields

Virendra Sule

Denoted $\mathbb{F}_p$ or $GF(p)$ for a prime p. Is the ring $\mathbb{Z}_p$ of numbers modulo p

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$$

with addition $+$, multiplication . modulo p. For example

$$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$2 + 5 = 0$, $2.5 = 3$, $6 + 6 = 5$, $5.6 = 2$. Every nonzero element has inverse, $2.4 = 1$, $3.5 = 1$, $4.2 = 1$. This follows in general because $(a, p) = 1$ for $a \neq 0$ hence $\exists\ x, y$ such that $ax + py = 1$, $ax = 1$ mod p. Because of this nonzero elements of $\mathbb{F}_p$ denoted $\mathbb{F}_p^*$ form a group $|\mathbb{F}_p| = p$, $|\mathbb{F}_p^*| = p - 1$.

Finite field with q elements

$\mathbb{F}_q$ or $GF(q)$. When q is not prime the structure is more complex. Characteristic of $\mathbb{F}_q$, or $\operatorname{char}\mathbb{F}_q$ is the smallest number p such that

$$p = 1 + 1 + \ldots + 1 = 0 \text{ } p \text{ times sum of } 1$$

$p < q$ for otherwise $q = 0$. If $p = ab$ then either $a = 0$ or $b = 0$. Hence $a, b \leq p$ is possible only when $a = 1, b = p$ or $a = p, b = 1$. Hence p is prime. The field $\mathbb{F}_p \subset \mathbb{F}_q$. So $\mathbb{F}_q$ is a finite dimensional vector space over $\mathbb{F}_p$. Let $v_1, v_2, \ldots, v_m$ be a basis of $\mathbb{F}_q$ wrt scalars $\mathbb{F}_p$, then it follows that $q = p^m$ as every element of $\mathbb{F}_q$ is

$$a_1 v_1 + \ldots + a_m v_m$$

$\mathbb{F}_q$ is called m-degree *extension* of $\mathbb{F}_p$. Similarly if $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$ and $p = \operatorname{char}\mathbb{F}_{q_1}$ then $q_1 = p^{m_1}$, $q_2 = p^{m_2}$ and $q_2 = (q_1)^d$. Hence $m_1 | m_2$.

Draw the tower $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$ of all subfields of $\mathbb{F}_{2^{30}}$. All divisors of 30 are $\{1, 2, 3, 5, 6, 10, 15, 30\}$ these can be the degrees of extensions of subfields.

$$\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^{10}} \subset \mathbb{F}_{2^{30}}$$
$$\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^6} \subset \mathbb{F}_{2^{30}}$$
$$\mathbb{F}_2 \subset \mathbb{F}_{2^5} \subset \mathbb{F}_{2^{10}} \subset \mathbb{F}_{2^{30}}$$
$$\mathbb{F}_2 \subset \mathbb{F}_{2^5} \subset \mathbb{F}_{2^{15}} \subset \mathbb{F}_{2^{30}}$$
$$\mathbb{F}_2 \subset \mathbb{F}_{2^3} \subset \mathbb{F}_{2^6} \subset \mathbb{F}_{2^{30}}$$
$$\mathbb{F}_2 \subset \mathbb{F}_{2^3} \subset \mathbb{F}_{2^{15}} \subset \mathbb{F}_{2^{30}}$$

Binomial theorem

Let $\mathbb{F}_q$ has char p. Then

$$(x+y)^{p^k} = x^{p^k} + y^{p^k}$$

since scalars in $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$ are taken modulo p, by standard formula

$$(x+y)^{p^k} = \sum_{i=0}^{i=p^k} \binom{p^k}{i} x^i y^{p^k-i} \mod p$$

For intermediate values of i other than 0 or p^k,

$$\binom{p^k}{i} \mod p = 0$$

Let S_q denote the set of all roots of the polynomial $f(X) = X^q - X$ i.e. considering

$$f(X) = \prod_i^q (X - \lambda_i)$$

and $S_q = \{\lambda_i\}$. $f'(X) = qX^{q-1} - 1 = -1 \mod p$. Hence $f'(X)$ has no roots and hence $f(X)$ has no multiple roots. Since $X^q - X = X(x^{q-1} - 1)$ all the roots are 0 and $q - 1$ roots of unity. By the binomial theorem for $x, y \neq 0$

$$x^q = x, (x + y)^q = x^q + y^q = x + y$$

similarly S_q is closed under product $(xy)^q = xy$ hence the set S_q is a field with q elements, i.e. $\mathbb{F}_q$. Inverses exist for all nonzero x as $1 = x^{q-1} = xx^{q-2}$.

Example of extension of binary field

Consider $\mathbb{F}_2$ and a polynomial $f(X) = X^2 + X + 1$ with $\mathbb{F}_2$ co-efficients. This polynomial is *irreducible* over $\mathbb{F}_2$ since factoring would mean having roots 1 or 0 but $f(0) \neq 0$, $f(1) \neq 0$. Hence the symbol θ outside $\mathbb{F}_2$ can be called a root of $f(X)$. Hence θ must satisfy the relation

$$\theta^2 = \theta + 1$$

The numbers $\{1, \theta\}$ are considered as vectors over $\mathbb{F}_2$ and form their linear span

$$R = \{a.1 + b.\theta\}$$

The vectors $\{1, \theta\}$ are LI over $\mathbb{F}_2$. To see this let $a + b\theta = 0$. If $a \neq 0$ then $\theta = ab^{-1}$ is in $\mathbb{F}_2$ hence $a = 0$ which implies $b = 0$. Hence $|R| = 2^2$. Using the rule $\theta^2 = \theta + 1$, R is closed under multiplication and addition and has inverse of the same kind, $(1 + \theta)(\theta^2) = 1$, $(\theta)(\theta + 1) = \theta^2 + \theta = 1$. Hence

$$R = \{0, 1, \theta, 1 + \theta\}$$

is a field with $q = 2^2 = 4$ elements.

By analogy with above example we see that if $\mathbb{F}_q$ is a finite field of char p and $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree m then $\mathbb{F}_{q^m}$ is the set of all elements

$$\{a_1 + a_2\theta + \ldots + a_m\theta^m\}$$

where θ is a root of $f(X)$ added to the base field of constants $\mathbb{F}_q$ and completing the field by addition, multiplication and inverse. The extension field is denoted $\mathbb{F}_{q^m}$ and thus is equal to the polynomials $\mathbb{F}_q[\theta]$ where $f(\theta) = 0$ is the rule followed for its arithmetic.

Example

Consider $f(X) = X^3 + X + 1$ and show that this is irreducible over $\mathbb{F}_2$. Let θ be a root of $f(X)$. Then

$$\mathbb{F}_{2^3} = \{a + b\theta + c\theta^2\}$$

Observe that all these elements satisfy the equation $X^{2^3} - X = 0$. $\theta^3 = \theta + 1$. Find inverse of θ, $\theta(\theta^2 + 1) = \theta^3 + \theta = 1$.
The equation $X^{q-1} = 1$ is also equivalent to Lagrange's theorem since the order of $\mathbb{F}_q^* = q - 1$. Hence another way to find an inverse is to observe $XX^{q-2} = 1$. For example $\theta^2(\theta^2)^{2^3-2} = 1$. Hence $(\theta^2)^{-1} = (\theta^2)^6 = (\theta^3)^4 = (\theta+1)^4 = \theta^4+1 = (\theta(\theta+1)+1) = \theta^2+\theta$.

Extension of Finite Field

Briefly understand the concept of extension rigorously. Let $\mathbb{F}_q$ be a finite field of characteristic p, then as observed before, $q = p^m$ for some $m > 1$ and $\mathbb{F}_q$ is the splitting field of the polynomial $X^q - X$ (the set of all its roots) which consists of 0 and $q - 1$ roots of unity. Let $f(X)$ is an irreducible polynomial over $\mathbb{F}_q$. Denote the ring of polynomials over $\mathbb{F}_q$ by $\mathbb{F}_q[X]$. The Euclidean algorithm holds over $\mathbb{F}_q[X]$. If f, g are polynomials and $g \neq 0$ then there exist unique polynomials h and r such that

1. $0 \leq \deg r < \deg g$
2. $f = hg + r$

Construct the residue class ring denoted $\mathbb{F}_q[X]/f(X)$ defined as the set $R = \mathbb{F}_q[X] \mod f(X)$ if $\deg f(X) = m$ then R is the vector space of polynomials of degree $\leq (m-1)$ and is generated as span of vectors

$$\{0, 1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{(m-1)}\}$$

by taking linear combinations over $\mathbb{F}_q$. The element $\bar{x} = X + (f(X))$ is the equivalence class of polynomials with residue X when divided by $f(X)$. Hence clearly

$$f(\bar{x}) = 0$$

hence $\bar{x}$ is a root of $f(X)$ which did not exist in $\mathbb{F}_q$ and is added to extend $\mathbb{F}_q$ to define the arithmetic in $\mathbb{F}_q$. Now one shows that the it from the extended Euclidean algorithm show that every non-zero element of R has an inverse modulo $f(X)$. This makes R a field and due to linear independence of the vectors in the above set is a degree m extension field of $\mathbb{F}_q$.

Consequence of $\mathbb{F}_q$ as splitting field

The Binomial theorem and the observation that $\mathbb{F}_q$ is the splitting field of the polynomial $X^q - X$ shows that

1. For every prime p (here it is char of $\mathbb{F}_q$) and m there is a finite field $\mathbb{F}_q = \mathbb{F}_{p^m}$.
2. For a prime divisor d of m and any irreducible polynomial of degree p^d the field $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_q$.
3. Every irreducible factor of degree d of $X^q - X$ generates a subfield as residue class ring R as above.