Lecture 5

5 Finite Field

5.1 Finite field of characteristic p

- Characteristic of a field F : The additive order of 1 in F, and it must be a prime number p.

- A finite field F of characteristic p is a vector space over $\mathbb{F}_p = \mathbb{Z}/(p)$, and hence $\#F = p^n$ for some n.

- The multplicative group $F^\times$ of F of order $q = p^n$ has order $q-1$, and every $\alpha \in F^\times$ satisfies the equation $X^{q-1} = 1$. Hence the every element of F satisfies

  $$f(X) = X^q - X = 0.$$

  This implies that the plynomial $f(X)$ has q distinct roots in F, ane we have

  $$f(X) = \prod_{\alpha \in F} (X - \alpha).$$

  Thus F is a splitting field of $f(X) \in \mathbb{F}_p[X]$, the smallest extension of $\mathbb{F}_p$ which contains all roots of $f(X)$.

- The splitting field is unique up to isomorphism (Homework 1), and the isomorphism class of F dependes only of the order $q = p^n$. Thus we have confirmed that if there exists a field of order q, then its isomorphism class is unique.

- **Examples :** A splitting field of $X^4 - X \in \mathbb{F}_2[X]$ is isomorphic to $\mathbb{F}_2[Y]/(Y^2+Y+1)$.

  Proof. In fact, we have a factorization

  $$X^4 - X = X(X-1)(X-Y)(X-(Y+1)).$$

  □

- **Theorem 5.1.1 :** For each prime p and each integer $n \geq 1$, there exists a finite field of order $q = p^n$ unique up to isomorphism (hence we denote it by $\mathbb{F}_q$).

Proof. Consider the splitting field F of

$$X^q - X = f(X)$$

in the algebraic closure $\mathbb{F}_p^{\text{alg}}$. We will show first of all that the set of roots of $f(X)$, namely

$$\{\alpha \in \mathbb{F}_p^{\text{alg}}\,;\ f(\alpha) = 0\} \tag{2}$$

forms a field. In fact, the followings are easy to check :

1. $0, 1$ are roots of $f(X)$.
2. If α, β are roots of $f(X)$, so are $\alpha + \beta$ and $\alpha\beta$.
3. If $\alpha \neq 0$ is a root of $f(X)$, so is α^{-1}.
4. If α is a root of $f(X)$, so is $-\alpha$.

This implies in particular that the splitting field F of $f(X)$ is equal to the set (2) of roots of $f(X)$.

Now, since the derivative of $f(X)$ is -1, $f(X)$ has no multiple roots (Homework 2), and hence the set (2) of roots of $f(X)$ contains exactly q elements. □

5.2 Multiplicative group $F^\times$

- **Theorem 5.2.1 :** The multiplicative group $F^\times$ of a finite field F is cyclic.

Proof. If α has order m, then it is a root of $f(X) = X^m - 1$. On the other hand, $f(X) = 0$ has at most m roots in F. Therefore, we have

$$\#\{\alpha \in F^\times\,;\ \alpha^m = 1\} \leq m \tag{3}$$

for any m. Notice that $F^\times$ is abelian.

Assume that $F^\times$ is not cyclic, then by the fundamental theorem of abelian groups, there is some prime r such that $F^\times$ contains a subgroup isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$. Then the number of elements of order r is more than $r^2 - 1 > r$. This contradicts to (3). □

5.3 Homework

1. Show that the splitting field of $f(X) \in k[X]$ is unique up to isomorphism.

2. Show that if $f(X) \in k[X]$ has a multiple root, then $f(X), f'(X)$ have common factor in $k[X]$.

3. Find the splitting field of $X^{p^8} - 1$ over $\mathbb{F}_p$.

4. Let p be prime and $q = p^n$. Show that every element of $\mathbb{F}_q$ has a unique p-th root in $\mathbb{F}_q$.

5. Suppose K is a field of characteristic p, and let $\alpha \in K$. Show that if α has no p-th root in K, then $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integers n.

6. Show that every element of a finite field can be written as a sum of two squares in that field.