Course 12

2.9 Finite fields

Recall that the *characteristic* of a ring R (denoted by $char(R)$) is the order of the identity element 1 of R in the group $(R,+)$. We have seen that the characteristic of a field is either a prime number or infinite. Throughout this section F will be a field.

Theorem 2.9.1 *A finite field F of prime characteristic p contains p^n elements for some $n \in \mathbb{N}^*$.*

Proof. Let $a_1 \in F^*$. We claim that $0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1$ are pairwise distinct. Indeed, if $i \cdot a_1 = j \cdot a_1$ for some $0 \leq i \leq j \leq p-1$, then $(j-i) \cdot a_1 = 0$ and $0 \leq j-i \leq p-1$. Since $\text{char}(F) = p$, we have $j - i = 0$, and thus $i = j$.

If $F = \{0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1\}$, we are done. Otherwise, let us choose $a_2 \in F \setminus \{0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1\}$. We claim that $k_1a_1 + k_2a_2$ are pairwise distinct for all $0 \leq k_1, k_2 \leq p-1$. Indeed, if $k_1a_1 + k_2a_2 = l_1a_1 + l_2a_2$ for some $0 \leq k_1, k_2, l_1, l_2 \leq p-1$, then we must have $k_2 = l_2$. Otherwise, we would have $a_2 = (l_2 - k_2)^{-1}(k_1 - l_1)a_1$. This contradicts the choice of a_2. Since $k_2 = l_2$, we deduce that $k_1 = l_1$. As F has only finitely many elements, we can continue the procedure and obtain elements $a_1, \dots, a_n$ such that

$$a_i \in F \setminus \{k_1a_1 + \cdots + k_{i-1}a_{i-1} \mid k_1, \dots, k_{i-1} \in \mathbb{Z}_p\}$$

for all $2 \leq i \leq n$, and consequently,

$$F = \{k_1a_1 + \cdots + k_na_n \mid k_1, \dots, k_n \in \mathbb{Z}_p\}.$$

In the same manner, we can show that $k_1a_1 + \cdots + k_na_n$ are pairwise distinct for all $k_i \in \mathbb{Z}_p, i = 1, \dots, n$. It follows that $|F| = p^n$. $\square$

Definition 2.9.2 *A polynomial $f \in F[X]$ with $deg(f) \geq 1$ is called* reducible *over F if there are $g, h \in F[X]$ with $deg(g), deg(h) \geq 1$ such that $f = g \cdot h$. Also, f is called* irreducible *over F if it is not reducible over F.*

Example 2.9.3 (a) $f = X^2 + 2 \in \mathbb{Z}_3[X]$ is reducible, because $f(1) = 0$.

(b) $f = X^4 + 2X^2 + 1 = (X^2 + 1)^2$ is reducible in $\mathbb{Z}_3[X]$, but f has no root in $\mathbb{Z}_3$.

Theorem 2.9.4 *Let $f \in F[X]$ be such that $deg(f) = n \geq 1$. Then the quotient ring*

$$F[X]/(f) = \{g \bmod f \mid g \in F[X]\} = \{a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}$$

is a field if and only if f is irreducible.

Proof. Suppose first that $F[X]/(f)$ is a field. Assume that f is reducible, say $f = g \cdot h$ for some $g, h \in F[X]$ with $deg(g), deg(h) \geq 1$. But then $g \cdot h = f = 0$ in $F[X]/(f)$, which implies $g = 0$ or $h = 0$, contradiction. Hence f is irreducible.

Conversely, suppose that f is irreducible. Then for every $g \in F[X]/(f)$, f and g are relatively prime. As in the case of numbers, one may show that there are $u, v \in F[X]$ such that $1 = uf + vg$. This implies that $vg = 1$ in $F[X]/(f)$, hence g is invertible in $F[X]/(f)$. Thus, $F[X]/(f)$ is a field. $\square$

Lemma 2.9.5 *Let A be a subfield of F with $|A| = q$, and let $a \in F$. Then $a \in A$ if and only if $a^q = a$.*

Proof. Suppose first that $a \in A$. If $a = 0$, then we clearly have $a^q = a$. Assume next that $a \neq 0$. Say $A^* = \{a_1, \dots, a_{q-1}\}$. Note that we also have $A^* = \{aa_1, \dots, aa_{q-1}\}$. Then $a_1 \cdots a_{q-1} = (aa_1) \cdots (aa_{q-1})$, which implies $a_1 \cdots a_{q-1} = a^{q-1}a_1 \cdots a_{q-1}$. Then $a^{q-1} = 1$, and so $a^q = a$.

Conversely, suppose that $a^q = a$. Let $f = X^q - X \in F[X]$. Then f has at most q roots in F. But all elements of A are roots of f and $|A| = q$, hence $A = \{\text{all roots of } f \text{ in } F\}$. So every $a \in F$ such that $a^q = a$ is a root of f, hence $a \in A$. $\square$

Theorem 2.9.6 *For any prime p and $n \in \mathbb{N}^*$, there exists a unique finite field with $q = p^n$ elements. This is denoted by F_q or $GF(q)$ (the Galois field with q elements).*

Proof. (Existence) Let $f \in \mathbb{Z}_p[X]$ be irreducible with $deg(f) = n$ (one may show that there exists such a polynomial!). Then

$$\mathbb{Z}_p/(f) = \{a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_p\}$$

is a field with p^n elements.

(Uniqueness) Let F_1 and F_2 be two fields with p^n elements. Let F be the smallest field containing F_1 and F_2, and let $f = X^{p^n} - X \in F[X]$. Then $F_1 = \{\text{all roots of } f \text{ in } F\} = F_2$. □

Example 2.9.7 The fields with less than 20 elements are: $F_2 \cong \mathbb{Z}_2$, $F_3 \cong \mathbb{Z}_3$, F_4, $F_5 \cong \mathbb{Z}_5$, $F_7 \cong \mathbb{Z}_7$, F_8, F_9, $F_{11} \cong \mathbb{Z}_{11}$, $F_{13} \cong \mathbb{Z}_{13}$, F_{16}, $F_{17} \cong \mathbb{Z}_{17}$, $F_{19} \cong \mathbb{Z}_{19}$.

One may also show that:

Theorem 2.9.8 *If F is a finite field, then $(F^*, \cdot)$ is a cyclic group.*

Example 2.9.9 Let us construct $F_8 = F_{2^3}$.

Here $p = 2$ and $n = 3$, so that we need $f \in \mathbb{Z}_2[X]$ irreducible of degree 3.

For instance, $X^3 + 1$ is reducible, because it has the root 1.

Let us try

$$f = X^3 + X + 1 \in \mathbb{Z}_2[X]\,.$$

If f were reducible, then f would be the product of a polynomial of degree 2 and a polynomial of degree 1, hence it would have a root in $\mathbb{Z}_2$. But $f(0) = 1$ and $f(1) = 1$. Hence f is irreducible.

Now we have

$$\begin{aligned} F_8 &= \mathbb{Z}_2[X]/(f) = \{a_0 + a_1X + a_2X^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_2\} \\ &= \{0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1\}. \end{aligned} \tag{2.1}$$

This is called the *polynomial representation* of the field and is convenient for addition and subtraction.

We also know that $(F_8^*, \cdot)$ is a cyclic group. Let us find a generator of it.

Since we work modulo $f \in \mathbb{Z}_2[X]$, we know that $X^3 + X + 1 = 0$.

Let us compute the powers of the first non-trivial element, namely X. In algorithms we compute $X^3 \bmod f = X + 1$, $X^4 \bmod f = X^2 + X$ etc. Here we use (i):

$$\begin{cases} X^3 = -X - 1 = X + 1 \\ X^4 = X^2 + X \\ X^5 = X^3 + X^2 = X^2 + X + 1 \\ X^6 = X^4 + X^3 = X^2 + X + X + 1 = X^2 + 1 \end{cases}$$

Since all are different, we have $F_8^* = \langle X \rangle$, hence

$$F_8 = \{0, 1, X, X^2, X^3, X^4, X^5, X^6\}. \tag{2.2}$$

This form is called the *power representation* of the field and is convenient for multiplying and dividing.

The **Discrete Logarithm Problem** is to determine the correspondence between the forms (2.1) and (2,2) of a finite field. This is a difficult computational problem, and it is used in Cryptography.

Here we get the following table of discrete logarithms:

y	$\log_X y$
1	0
X	1
$X+1$	3
X^2+1	6
X^2+X	4
X^2+X+1	5