CHAPTER II

FINITE FIELD

This chapter contains some properties of finite field which are needed in the sequel. The materials of this chapter are drawn from references [1], [4], [5], [6], [8], [9].

2.1 Definition. A finite field is a field with a finite number of elements.

2.2 Theorem. Let F be a finite field of characteristic $p \neq 0$. Then F has p^m elements for some $m > 0$.

Proof. Since F is a finite field of characteristic $p \neq 0$, F contains a subfield K isomorphic to $\mathbb{Z}_p$. Thus K has p elements. F is a vector space over K and since F is finite it is certainly finite-dimensional as a vector space over K. Suppose that $[F:K] = m$, then F has a basis of m elements over K. Let such a basis be $v_1, \ldots, v_m$. Then every element in F has a unique representation in the form $a_1v_1 + \ldots + a_mv_m$ where $a_1, \ldots, a_m$ are all in K. Thus the number of elements in F is the number of $a_1v_1 + \ldots + a_mv_m$ as the $a_1, \ldots, a_m$ range over K. Since each coefficient can have p values, F must clearly have p^m elements.

2.3 Lemma. Let F be a finite field with p^m elements. Then every element a in F satisfies $a^{p^m} = a$.

Proof. If $a = 0$ the assertion of the lemma is trivially true.

On the other hand, the non-zero elements of F form a group under multiplication of order p^m-1. Let $a \in F \setminus \{0\}$. Then $O(a) \mid p^m-1$. Thus $p^m-1 = k \cdot O(a)$, where k is a positive integer. Consequently, $a^{p^m-1} = a^{k \cdot O(a)} = (a^{O(a)})^k = 1$. Multiplying this relation by a we obtain that $a^{p^m} = a$. That is all elements of F are roots of the polynomial $X^{p^m} - X$.

2.4 Theorem. Let F be a finite field with p^m elements. Then F is the splitting field of the polynomial $X^{p^m} - X$.

Proof. Consider the polynomial $X^{p^m} - X \in \mathbb{Z}_p[X]$. Then the polynomial $X^{p^m} - X$ has at most p^m roots. By Lemma 2.3, we know p^m such roots, namely all the elements of F. Let $F = \{a_1, \ldots, a_{p^m}\}$. Now $X^{p^m} - X$ must be divisible by $\prod_{i=1}^{p^m} (X-a_i)$. Since both $X^{p^m} - X$ and $\prod_{i=1}^{p^m} (X-a_i)$ are monic polynomials with the same degrees, we have

$$X^{p^m} - X = \prod_{i=1}^{p^m} (X-a_i) \quad \in F[X],$$

that is, $X^{p^m} - X$ splits into linear factors in F. However, it cannot split into linear factors in any smaller field for that field would have to have all the roots of this polynomial and so would have to have at least p^m elements. Thus F is the splitting field of $X^{p^m} - X$ over $\mathbb{Z}_p$.

2.5 Theorem. Any two finite fields with the same numbers of elements are isomorphic.

Proof. Let the number of elements in these fields be p^m, where p is a prime and m is a positive integer. Since these finite fields have p^m elements, they are both splitting fields of the polynomial $X^{p^m} - X$ over $\mathbb{Z}_p$ by Theorem 2.4. Hence by Theorem 1.9, they are isomorphic.

2.6 Lemma. The polynomial $f(X) \in K[X]$ has a multiple root if and only if $f(X)$ and $f'(X)$ have a nontrivial common factor.

Proof. Without loss of generality, we may assume that the roots of $f(X)$ all lie in K. If $f(X)$ has a multiple root c then $f(X) = (X-c)^m g(X)$ where $m > 1$ and $f'(X) = m(X-c)^{m-1}g(X)+(X-c)^m g'(X)$. This says that $f(X)$ and $f'(X)$ have the common factor $(X-c)$, thereby proving the lemma in one direction.

On the other hand, if $f(X)$ has no multiple root then $f(X) = a(X-c_1)\ldots(X-c_n)$ where the c_i's are all distinct. But then $f'(X) = \sum_{i=1}^{n} a(X-c_1)\ldots\widehat{(X-c_i)}\ldots(X-c_n)$ where the $\widehat{\ }$ denotes the term that is omitted. Then no root of $f(X)$ is a root of $f'(X)$, for $f'(c_j) \neq 0$ for all $j = 1,\ldots, n$, since the roots are all distinct. However, if $f(X)$ and $f'(X)$ have a nontrivial common factor, they have a common root, namely, any root of this common factor. Thus $f(X)$ and $f'(X)$ have no nontrivial common factor, and so the lemma has been proved in the other direction.

2.7 Lemma. If K is a field of characteristic $p \neq 0$, then the polynomial $X^{p^m} - X \in K[X]$, for $m \geqslant 1$, has distinct roots.

Proof. Let $f(X) = X^{p^m} - X \in K[X]$. Then $f'(X) = p^m X^{p^m - 1} - 1 = -1$, since K is of characteristic p. Hence $f(X)$ and $f'(X)$ are relatively prime and by Lemma 2.6, $X^{p^m} - X$ has no multiple roots.

2.8 Lemma. Let F be a field with ch.F = p, where p is a prime. Then

(i) $ne = 0$ (e is the identity of F) if and only if $n \in p\mathbb{Z}$.

(ii) For any non-zero element $a \in F$, $na = 0$ if and only if $n \in p\mathbb{Z}$.

Proof. (i) Assume $ne = 0$. By the Division Algorithm, there exist $q, r \in \mathbb{Z}$ such that $n = pq+r$ where $0 \leqslant r < p$. Hence $ne = pqe+re$. Since ch.F = p, $pqe = 0$. It follows now that $re = 0$ since $ne = 0$ and $pqe = 0$. Since $r < p$, $r = 0$. Consequently, $n = pq$, that is, $n \in p\mathbb{Z}$. Conversely, assume $n \in p\mathbb{Z}$. Then $n = pt$ for some $t \in \mathbb{Z}$, and so $ne = pte$. Since ch.F = p, $pte = 0$, and thus $ne = 0$.

(ii) Let $a \neq 0 \in F$. Then $na = (ne)\cdot a = 0$ if and only if $ne = 0$. But by part (i), $ne = 0$ if and only if $n \in p\mathbb{Z}$. Thus part (ii) is proved.

2.9 Theorem. Let F be a field with ch.F = p, where p is a prime. For $a, b \in F$, we have

(i) $(a+b)^p = a^p + b^p$;

(ii) $(a-b)^p = a^p - b^p$.

Proof. (i) By the binomial expansion,

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$

$$= b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + a^p.$$

For $0 < i < p$, we have $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p\cdot(p-1)\dots 2.1}{i!(p-i)(p-i-1)\dots 2.1} = p\cdot M_i$,

where $M_i = \frac{(p-1)\dots(p-i+1)}{i!}$. By part (ii) of Lemma 2.8, $\binom{p}{i} = 0$ for $0 < i < p$. Hence $(a+b)^p = a^p + b^p$.

(ii) We write

$$(a-b)^p = (a+(-b))^p$$

(2-1) $$= a^p + (-1)^p b^p ,$$

where the last equal sign follows from part (i). If $p \neq 2$, p is odd and $(a-b)^p = a^p - b^p$. If $p = 2$, we have $1 + 1 = 0$ or $1 = -1$. Thus from (2-1) we have $(a-b)^2 = a^2 + b^2 = a^2 - b^2$ as we want to prove.

2.10 Theorem. For every prime number p and every positive integer m, there exists a field with p^m elements.

Proof. Consider $f(X) = X^{p^m} - X \in \mathbb{Z}_p[X]$. Let $F \supset \mathbb{Z}_p$ be the splitting field of f(X). Let $K = \{a \in F \mid a^{p^m} = a\}$. The elements of K are the roots of $X^{p^m} - X$ which, by Lemma 2.7, are distinct. Thus K has p^m elements.

We will now show that K is a field. Let $a, b \in K$, then $a^{p^m} = a$, $b^{p^m} = b$ and so by Theorem 2.9 we get

$$(a-b)^{p^m} = a^{p^m} - b^{p^m}$$

$$= a - b.$$

Thus $a - b \in K$. Also if $b \neq 0$, then $(a/b)^{p^m} = a^{p^m} / b^{p^m} = a/b$, whence $a/b \in K$. Consequently, K is a subfield of F and so is a field.

Hence the theorem is proved.

2.11 <u>Remark</u>. From now on the finite field with precisely p^n elements will be denoted by $GF\,[p^n]$.

2.12 <u>Lemma</u>. If G is a finite abelian group then there is an integer $m \leqslant |G|$, where $|G|$ denotes the number of elements in G, such that

(i) $a^m = 1$ for all $a \in G$,

and (ii) there exists an element $g \in G$ whose order is m.

<u>Proof</u>. This theorem is easy if $|G| = p^k$ for a prime p. We simply choose m as the maximal order of the elements in G and let g be any element of order m. Since $m \mid p^k$, $m = p^s$ where $s \leqslant k$. Then if $a \in G$ has order p^h, by the choice of s, it follows that $h \leqslant s$ so that $a^{p^s} = (a^{p^h})^{p^{s-h}} = 1$.

In general $|G| = p_1^{k_1} \cdots p_n^{k_n}$ and $G = S_{p_1} \times \cdots \times S_{p_n}$, where $S_p = \{ x \mid x \in G \text{ and } x^{p^r} = 1 \text{ for some integer } r \}$, (see [4, Theorem 5.18, pp. 144-145]). Let g_i be the element of maximal order $p_i^{s_i}$ in S_{p_i}. Clearly $m = p_1^{s_1} \cdots p_n^{s_n}$ is the desired integer, and $g = g_1 \cdots g_n$ is the desired element of G.

2.13 Theorem. The multiplicative group of non-zero elements of a finite field is cyclic.

Proof. Let F be a finite field with p^n elements. Let $F^* = F \sim \{0\}$. Since F^* is abelian we may apply Lemma 2.12. Let m be the positive integer such that for $0 \neq a \in F$ we have $a^m = 1$, and let $g \in F$ have order m. Since $a^m = 1$ for all non-zero a, it follows that $X^m = 1$ has $p^n - 1$ distinct roots in F, hence $m \geq p^n - 1$; however, since the order of g is m it must be that $m \leq p^n - 1$ —the order of the group. Hence $m = p^n - 1$ and so the group is cyclic, and g is its generator.

2.14 Theorem. Let F be a field with ch.F = p, where p is a prime. Define

$$F^p = \left\{ f^p \mid f \in F \right\}.$$

Then the assignment $\theta : f \longmapsto f^p$ is an isomorphism of F onto F^p.

Proof. θ is clearly well-defined.

To show that θ is a homomorphism. Let a, b $\in$ F. Then by Theorem 2.9, we get

$$\begin{aligned} \theta(a+b) &= (a+b)^p \\ &= a^p + b^p \\ &= \theta(a)+\theta(b). \end{aligned}$$

$$\theta(ab) = (ab)^p$$
$$= a^p b^p$$
$$= \theta(a)\theta(b).$$

To show that θ is 1-1. Let a, $b \in F$ such that $\theta(a) = \theta(b)$. Then $a^p = b^p$ and so $0 = a^p - b^p = (a-b)^p$, by Theorem 2.9. Since F is an integral domain, $a-b = 0$. We have therefore $a = b$, that is, $\theta(a) = \theta(b)$ implies $a = b$.

To show that θ is onto. Let $y \in F^p$. Then there exists an element $x \in F$ such that $x^p = y$.

Hence θ is an isomorphism of F onto F^p.

2.15 Corollary. Let F be a field with ch.F = p, where p is a prime. If F is finite, then $F^p = F$.

Proof. Since F is isomorphic to F^p by Theorem 2.14, the cardinal number of F is equal to the cardinal number of F^p. Moreover, if F is finite, then we have $F = F^p$.

2.16 Lemma. Let K be a subfield of $F = GF[p^n]$. Then there exists an integer m such that K has p^m elements, and $m \mid n$.

Proof. Since F has characteristic p, so does K, and hence K has p^m elements for some integer $m > 0$. Next we consider F as a vector space over K. Since F is finite, it has a finite basis over K, say $\{e_1, \ldots, e_s\}$ is a basis of F over K. Then F has $(p^m)^s = p^{ms}$ elements, whence $ms = n$ and $m \mid n$.

2.17 <u>Theorem</u>. $F = GF[p^n]$ has a subfield K with p^m elements if and only if $m \mid n$. Moreover, K is unique.

<u>Proof</u>. If F has a subfield with p^m elements, then $m \mid n$ by Lemma 2.16. Conversely, let $m \mid n$ and $n = ms$, where $s \in \mathbb{Z}^+$. Then $F^* = F \setminus \{0\}$ has

$$p^n-1 = p^{sm}-1 = (p^m-1)(p^{(s-1)m}+p^{(s-2)m}+\dots+1)$$

elements. Since $(p^m-1) \mid (p^n-1)$ and since F^* is cyclic, it has a unique cyclic subgroup K^* with p^m-1 elements, and say with generator b. Then for any integer k, $(b^k)^{p^m-1}-1 = 0$, whence $(b^k)^{p^m} - b^k = 0$. Thus, each element in K^* satisfies $X^{p^m} - X = 0$, and so each of the p^m elements in the field $K = K^* \cup \{0\}$ satisfies the equation $X^{p^m} - X = 0$. Since K^* is the unique subgroup of F with p^m-1 elements, it follows that K is unique, for the existence of another field K' with p^m elements would imply that there is a second subgroup of F^* with p^m-1 elements.

From now on, we shall have deduced some important properties of the $GF[p^{nm}]$ with respect to the included field, the $GF[p^n]$.

2.18 <u>Lemma</u>. Let f(X) be an irreducible polynomial over $\mathbb{Z}_p$, where p is a prime, and deg. f = n. Then the field $\mathbb{Z}_p[X]/(f(X))$ has p^n elements.

<u>Proof</u>. Let A = (f(X)). Any element in $\mathbb{Z}_p[X]/(f(X))$ is a coset of the form g(X)+ A where $g(X) \in \mathbb{Z}_p[X]$. Now, given any polynomial $g(X) \in \mathbb{Z}_p[X]$, by the Division Algorithm for polynomial

$$g(X) = t(X)\cdot f(X) + r(X) ,$$

where $r(X) = 0$ or deg. $r(X) <$ deg. $f(X)$. If $r(X) \neq 0$, then

$$r(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} ,$$

where the a's belong to $\mathbb{Z}_p$. Consequently, we have

$$\begin{aligned} g(X) + A &= a_0 + a_1X + \dots + a_{n-1}X^{n-1} + t(X)\cdot f(X) + A \\ &= a_0 + a_1X + \dots + a_{n-1}X^{n-1} + A, \end{aligned}$$

since $t(X)\cdot f(X)$ is in A. By the addition and multiplication in $\mathbb{Z}_p[X]/(f(X))$, we have

$$g(X) + A = (a_0 + A) + a_1(X+A) + \dots + a_{n-1}(X+A)^{n-1}.$$

If we put $\bar{X} = X+A$, then every element in $\mathbb{Z}_p[X]/(f(X))$ is of the form

$$a_0 + a_1\bar{X} + \dots + a_{n-1}\bar{X}^{n-1}$$

with the a's belong to $\mathbb{Z}_p$. There are only a finite number p of choices for each coefficient a_i, hence $\mathbb{Z}_p[X]/(f(X))$ has p^n elements.

2.19 <u>Theorem</u>. Let $F = GF[p^n]$. Let β be a root of an irreducible polynomial $f(X) \in F[X]$. Then $F(\beta) = GF[p^{nm}]$, where m is a degree of f(X).

<u>Proof</u>. By Lemma 2.18, $F[X]/(f(X))$ has $(p^n)^m = p^{nm}$ elements. Since β is a root of f(X), $F(\beta)$ is isomorphic to $F[X]/(f(X))$ by Theorem 1.18. Therefore the number of elements in $F(\beta)$ is p^{nm}, that is, $F(\beta) = GF[p^{nm}]$.

The materials from now on are due to L.E.Dickson [5,§§23-25,§§31].

2.20 Lemma. Let $f(X)$ be an irreducible polynomial in $GF[p^n][X]$ and $\deg. f = m$. Then $f(X) \mid X^{p^{nm}} - X$.

Proof. Let $g(X)$ be any polynomial in $GF[p^n][X]$. Dividing $g(X)$ by $f(X)$, we obtain

$$g(X) \equiv a_0 + a_1X + \ldots + a_{m-1}X^{m-1} \qquad (\text{mod } f(X)),$$

where the a's belong to $GF[p^n]$. Since there are p^n of choices for each coefficient a_i, the residue

$$(2\text{-}2) \qquad a_0 + a_1X + \ldots + a_{m-1}X^{m-1},$$

has p^{nm} distinct forms. Let we denote these p^{nm} distinct residues of the form (2-2) by

$$(2\text{-}3) \qquad X_i \qquad (i = 0, 1, \ldots, p^{nm} - 1),$$

where X_0 is the residue zero. Consider the products by a fixed residue $X_j \neq X_0$,

$$(2\text{-}4) \qquad X_jX_i \qquad (i = 0, 1, \ldots, p^{nm} - 1).$$

We claim that the products (2-4) are all distinct and different from X_0; for if $X_jX_k = X_jX_q$ whenever $k \neq q$ and $k,q \in \{0,1,\ldots, p^{nm}-1\}$, then we have $X_k = X_q$, this is not possible since $X_i, i = 0,1,\ldots,p^{nm}-1$, are all distinct, moreover, since $X_j \neq X_0$, then $X_jX_i \neq X_0$, $i=0\ 1,\ldots,p^{nm}-1$. Therefore the residues obtained on dividing the products (2-4) by $f(X)$ must coincide apart from their order with the residues (2-3).

Forming the products of the residues not zero in each series,

$$\prod_{i=1}^{p^{nm}-1} X_j X_i \equiv \prod_{i=1}^{p^{nm}-1} X_i \qquad (\text{mod } f(X)).$$

Since $\prod_{i=1}^{p^{nm}-1} X_i \neq 0$, we obtain

$$X_j^{p^{nm}-1} \equiv 1 \qquad (\text{mod } f(X)).$$

Consequently,

$$X_j^{p^{nm}-1}-1 \equiv 0 \qquad (\text{mod } f(X)).$$

Taking for X_j the particular residue X, the proof of the theorem follows.

2.21 Lemma. Let $f(X) \in GF[p^n][X]$. Then for every integer t, we have the following identity in the field :

$$f(X^{p^{nt}}) = [f(X)]^{p^{nt}}.$$

Proof. Let

$$f(X) = a_0 + a_1 X + \ldots + a_k X^k ,$$

where the a's belong to the $GF[p^n]$, so that by Lemma 2.3

(2-5) $$a_i^{p^n} = a_i \qquad (i = 0, 1, \ldots, k).$$

Raising f(X) to the power p and noting that the multinomial coefficients of the product terms (that is, those not p^{th} powers) are multiples of p, we have the identity,

$$[f(X)]^{p} = a_0^p + a_1^p X^p + \dots + a_k^p X^{kp} + p\cdot q_1(X).$$

By induction, we obtain the formula

$$[f(X)]^{p^s} = a_0^{p^s} + a_1^{p^s} X^{p^s} + \dots + a_k^{p^s} X^{kp^s} + p\cdot q_s(X).$$

Applying (2-5), we obtain in the $GF[p^n][X]$ the identity :

$$[f(X)]^{p^n} = a_0 + a_1 X^{p^n} + \dots + a_k X^{kp^n} = f(X^{p^n}).$$

Hence the lemma now follows by induction.

2.22 Lemma. Let $f(X) \in GF[p^n][X]$ be an irreducible polynomial of degree m. If $f(X)$ divides the polynomial $X^{p^{nt}} - X$, then the integer t is a multiple of m.

Proof. Let $t = sm + r$, where $0 \leqslant r < m$. By Lemma 2.20 , we have

$$X^{p^{nt}} - X = (X^{p^{nsm}})^{p^{nr}} - X \equiv X^{p^{nr}} - X \qquad (\text{mod } f(X)).$$

Hence, if $X^{p^{nt}} - X$ be divisible by $f(X)$ in the $GF[p^n][X]$, we have

$$X^{p^{nr}} \equiv X \qquad (\text{mod } f(X)). \tag{2-6}$$

Let $g(X) \in GF[p^n][X]/(f(X))$. Then by Lemma 2.18, we have p^{nm} distinct of $g(X)$. Denote $g(X)$ by the expression

$$a_0 + a_1\bar{X} + \dots + a_{m-1}\bar{X}^{m-1} ,$$

where the a's belong to $GF[p^n]$ and $\bar{X} = X + (f(X))$. By Lemma 2.21, we derive from (2-6)

$$[g(X)]^{p^{nr}} = g(X^{p^{nr}}) \equiv g(X) \qquad (\text{mod } f(X)),$$

or equivalently,

$$(2\text{-}7) \qquad \mu^{p^{nr}} \equiv \mu \qquad (\mathrm{mod}\ f(X)).$$

The congruence (2-7) is satisfied by the p^{nm} expressions $g(X)$, which are distinct modulo $f(X)$, therefore it has p^{nm} solutions in $GF[p^{nm}]$. On the other hand, we have at most p^{nr} solutions of (2-7) since the congruence (2-7) has degree p^{nr}. Since $r < m$, $p^{nr} < p^{nm}$. It follows that the congruence must be an identity, whence $r = 0$. Consequently, $t = sm$ and therefore we have proved the lemma.

2.23 <u>Theorem</u>. Let $f(X)$ and $g(X)$ belong to and are irreducible in the $GF[p^n][X]$ and are of the respective degrees m and t. Let t be a divisor of m. Then the roots of congruence

$$(2\text{-}8) \qquad g(X) \equiv 0 \qquad (\mathrm{mod}\ f(X))$$

are

$$X_1,\ X_1^{p^n},\ X_1^{p^{2n}},\ \ldots,\ X_1^{p^{n(t-1)}},$$

if X_1 is one root of (2-8) necessarily belonging to the $GF[p^{nm}]$.

<u>Proof</u>. By Lemma 2.21, we have in the $GF[p^n][X]$ the identity

$$g(X^{p^{nr}}) = [g(X)]^{p^{nr}}.$$

Hence, if X_1 is a root of (2-8), so is every $X_1^{p^{nr}}$. Since $g(X)$ is an irreducible polynomial of degree t in $GF[p^n][X]$, we have

$$X_1^{p^{nt}} - X_1 = g(X_1) \cdot h(X_1) \equiv 0 \qquad (\mathrm{mod}\ f(X)),$$

by virtue of Lemma 2.20. Using Lemma 2.22, we see that since m being a multiple of t, $g(X) \mid X^{p^{nm}} - X$. Consequently, we have

$$X_1^{p^{nm}} - X_1 = g(X_1) \cdot h'(X_1) \equiv 0 \quad (\mathrm{mod}\ f(X)),$$

or equivalently,

$$X_1^{p^{nm}} \equiv X_1 \quad (\mathrm{mod}\ f(X)).$$

We next prove that the above t powers of X_1 are distinct modulo $f(X)$.

Indeed, if

$$X_1^{p^{na}} \equiv X_1^{p^{nb}} \quad (\mathrm{mod}\ f(X))$$

for $a < b < t$, we would have, upon raising it to the power $p^{n(m-a)}$,

$$X_1^{p^{nm}} \equiv X_1 \equiv X_1^{p^{n(m+b-a)}} \quad (\mathrm{mod}\ f(X)).$$

So that, by Lemma 2.22, $m+b-a$ would be divisible by m. Hence $b = a$.

2.24 <u>Corollary</u>. We have in the $GF[p^{nm}]$ the decomposition

$$g(X) = (X-X_1)(X-X_1^{p^n})\dots(X-X_1^{p^{n(t-1)}}).$$

In particular, $f(X) = 0$ has in the $GF[p^{nm}]$ the distinct roots

$$X, X^{p^n}, \dots, X^{p^{n(m-1)}} .$$