ALGEBRAIC SYSTEMS AND COMBINATORICS – FINITE FIELDS –

K. ASAI

Abstract. This is an introductory text of a brief theory of finite fields. Beginning with polynomial rings, we overview the following: prime fields, finite polynomial fields, field extensions, splitting fields, structure of finite fields, primitive elements, Frobenius cycles, cyclotomic polynomials, and functions between finite fields. Many examples and exercises help the readers understand the contents.

1 Polynomial Rings 1.1 gcds

A field is briefly defined to be a set with four possible operations: '$+, -, \cdot, /$', without zero division. Any elements are supposed to satisfy ordinary laws with respect to those operations. $\mathbb{Q} = \{\text{all rational numbers}\}$, $\mathbb{R} = \{\text{all real numbers}\}$ and $\mathbb{C} = \{\text{all complex numbers}\}$ are examples of fields.

A ring is defined to be a set with three possible operations: '$+, -, \cdot$', where any elements are supposed to satisfy ordinary laws similar to those for fields, with respect to those operations:

$$
\begin{array}{cc}
a+b=b+a & \text{(commutativity)} \\
(a+b)+c=a+(b+c) & \text{(associativity)} \\
a+0=0+a=a & \text{(the additive identity (zero) exists)} \\
a+(-a)=(-a)+a=0 & \text{(the additive inverse exists)} \\
(ab)c=a(bc) & \text{(associativity)} \\
a1=1a=a & \text{(the multiplicative identity (unity) exists)} \\
a(b+c)=ab+ac & \text{(distributivity)} \\
(a+b)c=ac+bc & \text{(distributivity)}
\end{array} \tag{1}
$$

A ring satisfying $ab = ba$ for all a, b is called commutative. An extreme example of a commutative ring is $\{0\}$, called the zero ring or the trivial ring where $0 = 1$.

If an element a of a ring R has an element $b \in R$ such that

$$ab = ba = 1, \tag{2}$$

then a is called a unit or an invertible element of R, and b is called the (multiplicative) inverse element of a, denoted by a^{-1}. By definition, $(a^{-1})^{-1} = a$.

Let R be a commutative ring. The ring $M_n(R)$ of all square matrices of order n over R (all entries are contained in R) is called the matrix ring of degree n over R. In general, matrix rings are not commutative for $n \geq 2$.

Besides the above $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, the set of all integers $\mathbb{Z}$ is an easy example of a commutative ring. Also, the set of all polynomials in several variables $x_1, \ldots, x_n$ with coefficients in R is another example of a commutative ring, called the polynomial ring in $x_1, \ldots, x_n$ over R, denoted by $R[x_1, \ldots, x_n]$. We often deal with the polynomial ring $R[x]$ in one variable x. A polynomial in $R[x]$ is called a polynomial over R.

A field is precisely defined to be a nontrivial commutative ring where every nonzero element is a unit.

Let K be a field and let $g_1(x), \ldots, g_n(x)$ be polynomials in $K[x]$. The greatest common divisor (gcd) of $g_1(x), \ldots, g_n(x)$ is defined to be a common divisor of them with the greatest degree, and is denoted by $\gcd(g_1(x), \ldots, g_n(x))$. Here, the gcd is not necessarily in $K[x]$, it may belong to $L[x]$ for some extension field L of K (L is a field including K). But in the proof of Theorem 1, we show that the gcd is unique up to a constant multiple, and can be chosen from $K[x]$. Denote by $\deg f(x)$ the degree of $f(x)$[1]. Let $d(x) = \gcd(g_1(x), \ldots, g_n(x))$. We have the following fundamental theorem concerning gcds.

Theorem 1. *There exist polynomials $m_1(x), \ldots, m_n(x)$ in $K[x]$ such that*

$$d(x) = m_1(x)g_1(x) + m_2(x)g_2(x) + \cdots + m_n(x)g_n(x). \tag{3}$$

Example 1. Let $K = \mathbb{Q}$, $g_1(x) = x^2 - 1$, $g_2(x) = x^3 - 1$. Then

$$d(x) = x - 1 = -x(x^2 - 1) + x^3 - 1 = -xg_1(x) + g_2(x). \tag{4}$$

Proof of Theorem 1. Let $e(x)$ be a nonzero polynomial of minimum degree in $K[x]$, written in the form (3), say,

$$e(x) = m_1(x)g_1(x) + m_2(x)g_2(x) + \cdots + m_n(x)g_n(x). \tag{5}$$

First, for the gcd $d(x)$, we have $d(x) \mid g_i(x)$ for all i, say, $g_i(x) = d(x)s_i(x)$. Hence

$$\begin{aligned} e(x) &= m_1(x)d(x)s_1(x) + \cdots + m_n(x)d(x)s_n(x) \\ &= d(x)[m_1(x)s_1(x) + \cdots + m_n(x)s_n(x)]. \end{aligned} \tag{6}$$

Therefore $d(x) \mid e(x)$. $(*)$

Next, for all i, let $g_i(x) = e(x)q_i(x) + r_i(x)$ $(\deg r_i(x) < \deg e(x))$. Then we have

(7)

$$\begin{aligned} r_i(x) &= g_i(x) - [m_1(x)g_1(x) + \cdots + m_n(x)g_n(x)]q_i(x). \\ &= -m_1(x)q_i(x)g_1(x) - \cdots - m_{i-1}(x)q_i(x)g_{i-1}(x) + (1 - m_i(x)q_i(x))g_i(x) \\ &\quad -m_{i+1}(x)q_i(x)g_{i+1}(x) - \cdots - m_n(x)q_i(x)g_n(x). \end{aligned}$$

Consequently, $r_i(x)$ is expressed in the form (3). If $r_i(x) \not\equiv 0$ for some i, then $r_i(x)$ is a nonzero polynomial of less degree than $e(x)$, written in the form (3). This contradicts the assumption that $e(x)$ has the minimum degree.

[1]The degree of a polynomial $f(x)$ is defined as the highest degree of its terms when $f(x)$ is expressed in its canonical form as a sum of monomials. Hence the degree of a nonzero constant polynomial is 0, whereas the degree of the zero polynomial is undefined. For convenience, however, the degree of 0 is usually defined to be $-\infty$.

Therefore we see $r_i(x) \equiv 0$ for all i, that is, $e(x) \mid g_i(x)$ for all i. Hence $e(x)$ is a common divisor of $g_1(x), \ldots, g_n(x)$. But by $(*)$ and that $d(x)$ is the gcd, $e(x)$ should be $(\text{const}) \cdot d(x)$, which completes the proof. (q.e.d.)

If $d(x) = 1$, Theorem 1 is rewritten in the form specifying a necessary and sufficient condition.

Corollary 1. *For* $\gcd(g_1(x), \ldots, g_n(x)) = 1$*, it is necessary and sufficient that there exist polynomials* $m_1(x), \ldots, m_n(x)$ *in* $K[x]$ *such that*

$$m_1(x)g_1(x) + m_2(x)g_2(x) + \cdots + m_n(x)g_n(x) = 1. \tag{8}$$

Theorem 1 and Corollary 1 are often used when $n = 2$:

$$\begin{gathered} m_1(x)g_1(x) + m_2(x)g_2(x) = d(x), \\ g_1(x) \text{ and } g_2(x) \text{ are relatively prime} \iff m_1(x)g_1(x) + m_2(x)g_2(x) = 1. \end{gathered} \tag{9}$$

Also, there are analogous results in the case of the gcd of several integers. The proof is similar to the polynomial case, which is an exercise for readers.

1.2 irreducibility

Let K be a field. A nonconstant polynomial is called irreducible over K if it is a polynomial over K and has no factorization into two nonconstant polynomials over K. For example, $x^3 - 1 = (x-1)(x^2+x+1)$ is reducible over $\mathbb{Q}$, while $x^2 + x + 1$ is irreducible over $\mathbb{Q}$, and reducible over $\mathbb{C}$: $x^2+x+1 = (x-\alpha)(x-\beta)$, $\alpha, \beta = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.

(exercise) Is a polynomial of degree 1 irreducible?
(exercise) Is there a polynomial of degree > 1 irreducible over $\mathbb{C}$?

Theorem 2. *If* $p(x), q(x)$ *are irreducible over* K*, then they are relatively prime (*$\gcd = \text{const}$*) or* $p(x) = (\text{const})q(x)$*.*

Proof. Let $d(x)$ be the gcd of $p(x), q(x)$. By Theorem 1, $d(x)$ is in $K[x]$. If $d(x) \neq \text{const}$, from the irreducibility of $p(x), q(x)$, we have $p(x) = (\text{const})d(x)$ and $q(x) = (\text{const})d(x)$. If $d(x) = \text{const}$, $p(x), q(x)$ are relatively prime by definition. (q.e.d.)

	1	2	3	4	5	6
1	1					6
2	2					5
3	3					4
4	4					3
5	5					2
6	6	5	4	3	2	1

	2	3	4	5	6	7	8	9	10
2									9
3	6					10		5	8
4	8		5		2		10		7
5	10			3				1	6
6	1		2		3		4		5
7									4
8	5	2	10	7	4	1	9	6	3
9	7	5						4	2
10	9	8	7	6	5	4	3	2	1

TABLE 1

2 Finite Fields $\mathbb{F}_p$ $(= GF(p))$ 2.1 definition

Let p be a prime number and consider the set:

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}. \tag{10}$$

We can define the four operations in $\mathbb{F}_p$ modulo p.

Example 2. Consider $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. We have $1 + 3 = 4$, $2 + 3 = 5 = 0 \longrightarrow -2 = 3$, $-3 = 2$. Also we have $3 \cdot 3 = 9 = 4$, $2 \cdot 3 = 6 = 1 \longrightarrow 3^{-1} = 2$ (2 is the inverse element of 3), and $2^{-1} = 3$. $4 \cdot 4 = 16 = 1$, hence $4^{-1} = 4$. $1 - 3 = -2 = 5 - 2 = 3$, etc.

Theorem 3. *Let p be a prime number. For arbitrary nonzero $a \in \mathbb{F}_p$, there exists the inverse element a^{-1} of a in $\mathbb{F}_p$, say, $aa^{-1} = a^{-1}a = 1$.*

Proof. Let a be as above. Since $1 \leq a \leq p-1$ and p is a prime, we have $\gcd(a, p) = 1$. Thus $ma + np = 1$, i.e., $ma = 1 - np = 1$. Let $m + n'p = m'$ be an element of $\mathbb{F}_p$. Then $m'a = am' = (m + n'p)a = 1 + n'pa = 1$. Hence $m' = a^{-1}$. (q.e.d.)

Table 1 includes the multiplication tables of $\mathbb{F}_7$ and $\mathbb{F}_{11}$.

The set $\mathbb{F}_p$ allows the four operations, satisfies (1) and commutative. Hence $\mathbb{F}_p$ is a field. As $\mathbb{F}_p$ is a field with finite p elements, it is called a finite field (and is sometimes called a Galois field denoted by $GF(p)$). The characteristic of $\mathbb{F}_p$ is p, which is defined in the next section.

2.2 characteristics

Let K be a field. Consider the sum of n copies of the identity of K:

$$(n) = \underbrace{1 + 1 + \cdots + 1}_{n}. \tag{11}$$

The characteristic of K, often denoted $\mathrm{char}(K)$, is defined as follows. If there is some positive integer n such that $(n) = 0$, then $\mathrm{char}(K)$ is the least such n. Otherwise, $\mathrm{char}(K) = 0$. This definition also applies to arbitrary rings.

In general, a field with finite elements is called a finite field. Let K be a finite field. Since K is finite, there exist only finite possible values of (n) for all positive integers n. Thus for some $m > n$, we have $(m) = (n)$. Adding -1 by n times to both sides, we have $(m - n) = 0$. Hence we have $\mathrm{char}(K) > 0$.

Theorem 4. *For a field (resp. a finite field) K, $\mathrm{char}(K)$ is a prime number or 0 (resp. a prime number).*

Proof. By reduction to absurdity. We have already seen that every finite field has positive characteristic. Hence it suffices to show that no field has composite number characteristic m. Suppose K is a field of characteristic m. Let $m = pq$, $p, q > 1$. Then it holds that $(m) = (p)(q)$. Since $p, q < m$, $(p), (q) \neq 0$. Then $(m)(q)^{-1} = (p)$. But as $(m) = 0$, we have $(p) = 0$. (contradiction) (q.e.d.)

2.3 finite polynomial rings over finite fields

Let K be a field, and $g(x)$ be a polynomial of degree n over K. Consider the ring $K[x]$ of all polynomials over K. Now we make a new ring L from $K[x]$ by identifying two elements $f(x)$ and $\tilde{f}(x)$ if and only if $g(x) \mid (f(x) - \tilde{f}(x))$.

Let $f(x) = \tilde{f}(x)$ and $h(x) = \tilde{h}(x)$ be two pairs of elements identified with each other. Then we have

$$\begin{aligned} f(x) \pm h(x) &= \tilde{f}(x) \pm \tilde{h}(x) \\ f(x)h(x) &= \tilde{f}(x)\tilde{h}(x). \end{aligned} \tag{12}$$

Hence the identification in L is compatible with the three operations $(+, -, \cdot)$.

For an element $f(x)$ in L of degree $\geq n$, we have $f(x) = g(x)q(x) + r(x)$, with residue $r(x)$ of degree $< n$. Then $f(x)$ is identified with $r(x)$. (In particular, $g(x)$ is identified with 0.) Hence we can represent any element of L by a polynomial of degree $< n$. Also, any two distinct polynomials $f(x), h(x)$ of degree $< n$ are never identified with each other because a nonzero polynomial $f(x) - h(x)$ of degree $< n$ is not divisible by $g(x)$ of degree n. Therefore we can regard L as a ring of all polynomials over K of degree $< n$. Hence, if K is a finite field, L is a finite ring, i.e. a ring of finite elements. L is called "$K[x]$ modulo $g(x)$" denoted by $L = K[x]/g$.

Example 3. Let $K = \mathbb{F}_3 = \{0, 1, 2\}$, $g(x) = x^2 + 1$ (irreducible over K), and $L = K[x]/g$. As $x^2 + 1 = 0$, we have $x^3 + x = x(x^2 + 1) = 0$. The degree of $x^3 + x^2 + 2$ can be reduced as follows: $x^3 + x^2 + 2 = (x^2 + 1)(x + 1) - x + 1 = (3 - 1)x + 1 = 2x + 1$. Similarly all polynomials in L can be represented in the form $ax + b$, where $a, b \in \mathbb{F}_3$. Hence there are 9 elements in L. The inverses are listed below.

a	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
a^{-1}	−								

(13)

For example, the inverse of $x + 1$ is $x + 2$, because $(x + 1)(x + 2) = x^2 + 3x + 2 = (x^2 + 1) + 3x + 1 = 1$.

Example 4. Let $K = \mathbb{F}_5$, $g(x) = x^4 + 4x^2 + 4x + 3$, and $L = K[x]/g$. In such a case, it is difficult to calculate the inverse of a given polynomial $a(x)$. We often use Euclidean algorithm to solve this problem. Let $a(x) = x^3 + 2x^2 + 4$.

$$\begin{array}{ll} g(x) & = a(x)(x+3) + 3x^2 + 1 \\ a(x) & = (3x^2+1)(2x+4) + 3x \\ 3x^2+1 & = (3x)(x) + 1 \end{array} \tag{14}$$

Hence

$$\begin{aligned} 1 &= 3x^2 + 1 - 3x \cdot x \\ &= 3x^2 + 1 - (a(x) - (3x^2+1)(2x+4))x \\ &= (3x^2+1)(2x^2+4x+1) - a(x) \cdot x \\ &= (g(x) - a(x)(x+3))(2x^2+4x+1) - a(x) \cdot x \\ &= a(x)(-(x+3)(2x^2+4x+1) - x) + g(x)(2x^2+4x+1) \\ &= a(x)(3x^3+x+2) + g(x)(2x^2+4x+1). \end{aligned} \tag{15}$$

By this equality, we have $a(x)(3x^3+x+2) = 1$, say, $a(x)^{-1} = 3x^3 + x + 2$.

(exercise) Find the inverse of $a(x) = x^5$ in the above L.

2.4 irreducibility over finite fields

The most easy way to confirm the irreducibility of polynomials over a finite field is to use the factor theorem: i.e., $f(x) = (x-\alpha)g(x) \iff f(\alpha) = 0$. But this method is only effective to find a factor of degree 1. For example, letting $K = \mathbb{F}_2$, we have the values of $f(\alpha)$ below.

α	0	1
x^2+1	1	0
x^2+x+1	1	1

(16)

According to this result, we see that $x^2 + 1$ is reducible over $\mathbb{F}_2$, but $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. We can also apply this for polynomials of degree 3. But for polynomials of degree ≥ 4, we can not see by this method whether $f(x) = g(x)h(x)$, where g, h are of degree ≥ 2.

Example 5. For $p \leq 23$, we have the table of the irreducibility of x^2+1 and x^2+x+1 over $\mathbb{F}_p$ as follows. ($\circ$: irreducible)

(17)

	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$	$\mathbb{F}_{11}$	$\mathbb{F}_{13}$	$\mathbb{F}_{17}$	$\mathbb{F}_{19}$	$\mathbb{F}_{23}$
x^2+1									
x^2+x+1									

3 Homomorphisms and Isomorphisms

3.1 definition

Let L, M be fields or rings. A mapping $\phi : L \longrightarrow M$ is called a homomorphism from L to M if ϕ satisfies the following:

$$\begin{array}{ll} \phi(a+b) = \phi(a) + \phi(b) & (\text{for all } a, b \in L) \\ \phi(ab) = \phi(a)\phi(b) & (\text{for all } a, b \in L) \\ \phi(1) = 1. & \end{array} \tag{18}$$

A bijective homomorphism is called an isomorphism. If there exists an isomorphism from L to M, then L is called isomorphic to M, denoted by $L \simeq M$. A surjective homomorphism is called an epimorphism, while an injective homomorphism is called a monomorphism. An isomorphism (resp. homomorphism) $\phi : L \longrightarrow L$ is called an automorphism (resp. endomorphism) of L. Next let L and M have a common subset K. An isomorphism (resp. homomorphism) $\phi : L \longrightarrow M$ which fixes every element of K is called a K-isomorphism (resp. K-homomorphism). Furthermore, a K-isomorphism (resp. K-homomorphism) $\phi : L \longrightarrow L$ is called a K-automorphism (resp. K-endomorphism) of L.

(exercise) For a homomorphism $\phi : L \longrightarrow M$, show that $\phi(0) = 0$, $\phi(-a) = -\phi(a)$, and for every unit a of L, $\phi(a^{-1}) = (\phi(a))^{-1}$.

(exercise) For a homomorphism $\phi : L \longrightarrow M$, and for all $a_1, a_2, \ldots, a_n \in L$, show the following:

$$\begin{array}{l} \phi(a_1 + a_2 + \cdots + a_n) = \phi(a_1) + \phi(a_2) + \cdots + \phi(a_n) \\ \phi(a_1 a_2 \ldots a_n) = \phi(a_1)\phi(a_2)\ldots\phi(a_n). \end{array} \tag{19}$$

(exercise) For homomorphisms (resp. isomorphisms) $\phi : L \longrightarrow M$, $\psi : M \longrightarrow N$, show $\psi \circ \phi : L \longrightarrow N$ is also a homomorphism (resp. an isomorphism).

(exercise) Show that (1) $L \simeq L$, (2) $L \simeq M \implies M \simeq L$, (3) $L \simeq M$, $M \simeq N \implies L \simeq N$.

3.2 extended homomorphisms

Let L, M be fields. For an arbitrary mapping $\phi : L \longrightarrow M$, we extend it to $\tilde{\phi} : L[x] \longrightarrow M[x]$ by

$$\tilde{\phi}(c_0 + c_1 x + c_2 x^2 + \cdots + c_r x^r) = \phi(c_0) + \phi(c_1)x + \phi(c_2)x^2 + \cdots + \phi(c_r)x^r. \tag{20}$$

That is, ϕ operates on the coefficients.

Theorem 5. *A homomorphism (resp. isomorphism) $\phi : L \longrightarrow M$ is extended to a homomorphism (resp. isomorphism) $\tilde{\phi} : L[x] \longrightarrow M[x]$.*

Proof. We see that $\tilde{\phi} : L[x] \longrightarrow M[x]$ satisfies the following:

$$\begin{aligned} &\tilde{\phi}(f(x)+g(x)) = \tilde{\phi}(f(x)) + \tilde{\phi}(g(x)) \\ &\tilde{\phi}(f(x)g(x)) = \tilde{\phi}(f(x))\tilde{\phi}(g(x)) \\ &\tilde{\phi}(1) = 1. \end{aligned} \tag{21}$$

Hence $\tilde{\phi}$ is a homomorphism. If ϕ is a bijection, we see $\tilde{\phi}$ is also a bijection. (q.e.d.)

Let K be a common subfield of L and M. It follows from this theorem that

Corollary 2. *(i) A K-homomorphism (resp. K-isomorphism) $\phi : L \longrightarrow M$ is extended to a $K[x]$-homomorphism (resp. $K[x]$-isomorphism) $\tilde{\phi} : L[x] \longrightarrow M[x]$.*
(ii) A K-automorphism of L is extended to a $K[x]$-automorphism of $L[x]$.

(exercise) (1) Confirm (21). (2) Show that ϕ is a bijection $\implies$ $\tilde{\phi}$ is a bijection.
For simplicity, we write hereafter $\tilde{\phi} = \phi$ if confusion does not occur.

3.3 residue class rings

Let R be a ring. A nonempty subset I of R is called an ideal of R if I satisfies

$$\begin{aligned} &x, y \in I \implies x - y \in I \qquad \text{and} \\ &r \in R,\ x \in I \implies rx, xr \in I. \end{aligned} \tag{22}$$

Then we can construct a residue class ring:

$$R/I = \{I + r \mid r \in R\}, \tag{23}$$

where

$$I + r = \{x + r \mid x \in I\} \tag{24}$$

is a residue class of r modulo I. We often write simply as $I + r = [r]$. Two operations of R/I are defined by

$$\begin{array}{llll} [r] + [s] & = (I+r) + (I+s) & = I + (r+s) & = [r+s] \\ [r]\,[s] & = (I+r)(I+s) & = I + rs & = [rs]. \end{array} \tag{25}$$

Consider the commutative ring $R = \mathbb{Z}$. For a positive integer n, denote by $n\mathbb{Z}$ the set of all multiples of n. Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and a residue class ring $\mathbb{Z}_n$ is defined as

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\}, \tag{26}$$

which is a finite commutative ring of characteristic n. We see $\mathbb{F}_p \simeq \mathbb{Z}_p$. (exercise)

Next let $R = K[x]$ be a polynomial ring and $I = (g)$ be an ideal generated by $g(x)$:

$$I = (g) = \{f(x) \in K[x] \mid g(x) \mid f(x)\}. \tag{27}$$

Then we can show that

$$K[x]/g \simeq K[x]/(g). \tag{28}$$

Indeed, take $\phi : K[x]/g \longrightarrow K[x]/(g)$ defined by

$$\phi(f(x)) = [f(x)], \tag{29}$$

then we see ϕ is well defined and gives an isomorphism. (exercise)

4 Finite Polynomial Fields 4.1 definition

Let K be a field, and $g(x)$ be a polynomial over K. Consider the ring $L = K[x]/g$.

Theorem 6. *L is a field if and only if $g(x)$ is irreducible over K.*

Proof. Let $g(x)$ be an irreducible polynomial of degree n over K. Take any nonzero element $h(x)$ in L. One can regard $h(x)$ as a polynomial of degree $< n$. Thus, $g(x)$ and $h(x)$ are relatively prime. Hence by Corollary 1, there exists polynomials $m(x)$ and $n(x)$ such that

$$m(x)g(x) + n(x)h(x) = 1, \tag{30}$$

that is, $n(x)h(x) = 1 - m(x)g(x) = 1$ in L. Therefore $h^{-1}(x) = n(x)$. As $h(x)$ is arbitrary, L is a field.

Next let $g(x) = h(x)k(x)$ ($h(x), k(x)$: nonconstants) be a reducible polynomial. Then both of $h(x), k(x)$ have no inverses because if $h^{-1}(x) = n(x)$ exists, we have $0 = n(x)g(x) = k(x)$, which is a contradiction. (q.e.d.)

As we have seen in Example 3, L is a field when $K = \mathbb{F}_3$, $g(x) = x^2 + 1$. Also, we have fields L for the "$\circ$" pairs $K[x]/g$ in Example 5. In general, for a finite field K and an irreducible polynomial $g(x)$ over K, $L = K[x]/g$ is called a finite polynomial field over K.

4.2 field extensions

Let L be a field and K be a subset of L. If K itself is a field with respect to the field operations in L, then K is called a subfield of L, or L is called an extension field of K. This relation between K and L is called a field extension, denoted by L/K. For example, the field L in Example 3 is an extension field of $\mathbb{F}_3$. If a subfield M of L is also an extension field of K, then M is called an intermediate field of the field extension L/K.

For a field extension L/K, it is always valid that

$$\begin{array}{ll} a + b \in L & (\text{for all } a, b \in L), \\ ka \in L & (\text{for all } a \in L,\ k \in K). \end{array} \tag{31}$$

This shows that L is a vector space over K. If the dimension of L over K ($\dim_K L$) is finite n, L/K is called a finite extension of degree n, and we write $n = [L : K]$.

Theorem 7. *Let M/L and L/K be finite extensions, then M/K is also a finite extension, and it is valid that $[M : K] = [M : L][L : K]$.*

Proof. Let a basis of M over L be $\langle f_1, \ldots, f_m \rangle$, and a basis of L over K be $\langle e_1, \ldots, e_l \rangle$. By definition, for every element $w \in M$, there exists a unique expression:

$$w = v_1 f_1 + v_2 f_2 + \cdots + v_m f_m \qquad (v_1, \ldots, v_m \in L). \tag{32}$$

And the coefficients v_i are also expressed uniquely as

$$v_i = u_{i1} e_1 + u_{i2} e_2 + \cdots + u_{il} e_l \qquad (u_{i1}, \ldots, u_{il} \in K). \tag{33}$$

Therefore we have

$$\begin{aligned} w &= \textstyle\sum_{i=1}^{m} (u_{i1} e_1 + u_{i2} e_2 + \cdots + u_{il} e_l) f_i \\ &= \textstyle\sum_{i=1}^{m} \sum_{j=1}^{l} u_{ij} (e_j f_i). \end{aligned} \tag{34}$$

Next we confirm linear independence of $(e_j f_i)$ over K. Let

$$\begin{aligned} 0 &= \textstyle\sum_{i=1}^{m} \sum_{j=1}^{l} k_{ij} (e_j f_i) && (k_{ij} \in K) \\ &= \textstyle\sum_{i=1}^{m} (k_{i1} e_1 + k_{i2} e_2 + \cdots + k_{il} e_l) f_i. \end{aligned} \tag{35}$$

By linear independence of $\langle f_1, \ldots, f_m \rangle$, we have

$$k_{i1} e_1 + k_{i2} e_2 + \cdots + k_{il} e_l = 0. \tag{36}$$

Hence by linear independence of $\langle e_1, \ldots, e_l \rangle$, we have $k_{ij} = 0$. Therefore $(e_j f_i)$ $(i = 1, \ldots, m;\ j = 1, \ldots, l)$ is a basis of M over K. Thus $[M : K] = ml = [M : L][L : K]$. (q.e.d.)

Let K be a finite field of characteristic p. Then K has elements $0, 1, 2, \ldots, p-1$, and these form a field $\mathbb{F}_p$. Thus, $\mathbb{F}_p$ is a subfield of K. From this, it follows that every field of characteristic p contains a subfield $\mathbb{F}_p$. In this sense, $\mathbb{F}_p$ is the minimal field called a prime field. Since K is finite, K is a finite dimensional vector space over $\mathbb{F}_p$. Let $[K : \mathbb{F}_p] = n$. There exists a basis $\langle e_1, \ldots, e_n \rangle$ of K. Then an arbitrary element a in K is uniquely expressed in the linear form:

$$a = c_1 e_1 + c_2 e_2 + \cdots + c_n e_n \quad (c_i \in \mathbb{F}_p). \tag{37}$$

Therefore we have $K = \{c_1 e_1 + c_2 e_2 + \cdots + c_n e_n \mid c_1, \ldots, c_n \in \mathbb{F}_p\}$. From this, it follows that K consists of p^n elements.

The following shows the possible numbers of the elements of finite fields.

(38)

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
y/n	−															

Let $g(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_p$. Let L be a finite polynomial field $\mathbb{F}_p[x]/g$. Then we have

$$L = \{c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \mid c_0, \ldots, c_{n-1} \in \mathbb{F}_p\}. \tag{39}$$

Hence the cardinality of L is p^n.

4.3 examples in characteristic 0

Let us consider familiar fields of characteristic 0. All fields containing $\mathbb{Q}$ are regarded as characteristic 0. We know that $\mathbb{Q}$ is a subfield of $\mathbb{R}$, which is a subfield of $\mathbb{C}$. Every element of $\mathbb{C}$ is expressed uniquely by $a+bi$, which shows that $\langle 1, i\rangle$ is a basis of $\mathbb{C}$ over $\mathbb{R}$. Hence $[\mathbb{C}:\mathbb{R}]=2$. But it is known that $\mathbb{R}/\mathbb{Q}$ is not a finite extension.

Besides $\mathbb{R}$, there are many intermediate fields of $\mathbb{C}/\mathbb{Q}$. We denote by $\mathbb{Q}(\alpha)$ the smallest intermediate field of $\mathbb{C}/\mathbb{Q}$ containing α, that is called the field generated by the adjunction of α to $\mathbb{Q}$.

For example, $\mathbb{Q}(\sqrt{2}\,)$ is an extension field of $\mathbb{Q}$ consists of the elements: $a+b\sqrt{2}$, where a and b are arbitrary rational numbers. It is easy to show that the set $\{a+b\sqrt{2}\,\}$ is closed under the four operations. $\mathbb{Q}(\sqrt{3}\,)$ is a similar example of an extension field of $\mathbb{Q}$. It is easily seen that $[\mathbb{Q}(\sqrt{2}\,):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3}\,):\mathbb{Q}]=2$.

Next consider the smallest intermediate field of $\mathbb{C}/\mathbb{Q}$ containing both of $\sqrt{2}$ and $\sqrt{3}$, which is denoted by $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$. It does not suffice to express the elements in the form $a+b\sqrt{2}+c\sqrt{3}$, because $\sqrt{2}\times\sqrt{3}=\sqrt{6}$, which is not represented in the form $a+b\sqrt{2}+c\sqrt{3}$ (exercise). In fact, $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ is equal to the set

$$L=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}. \tag{40}$$

We see that L is indeed included in $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ because all of $\sqrt{2},\sqrt{3},\sqrt{6}$ are included in $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$. And we see L is closed under the four operations. For $(+,-)$, trivial, and for $\times$, we have

$$\begin{aligned}&(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\,)(p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}\,)\\ &=(ap+2bq+3cr+6ds)+(aq+bp+3cs+3dr)\sqrt{2}\\ &+(ar+cp+2bs+2dq)\sqrt{3}+(as+dp+br+cq)\sqrt{6}.\end{aligned} \tag{41}$$

It is little more laborious to show that L is closed under division. It suffices to show that every nonzero element x has its inverse x^{-1}. Let $x=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ and we rationalize the denominator of $\frac{1}{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}}$.

$$\begin{aligned}&\frac{1}{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}}\\ &=\frac{(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\,)}{(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\,)(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\,)}\\ &=\frac{(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\,)}{[(\quad\;\;)+(\quad\;\;)\sqrt{2}\,][(\quad\;\;)-(\quad\;\;)\sqrt{2}\,]}\\ &=\frac{(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}\,)(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\,)}{(\quad\;\;)^2-2(\quad\;\;)^2}.\end{aligned} \tag{42}$$

Hence L is closed under the four operations. Together with $L\subset\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ and minimality of $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$, we have $L=\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$. We see that $\langle 1,\sqrt{2},\sqrt{3},\sqrt{6}\,\rangle$ is a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ over $\mathbb{Q}$. Therefore we have $[\mathbb{Q}(\sqrt{2},\sqrt{3}\,):\mathbb{Q}]=4$.

Now we return to the general case in arbitrary characteristic. Let L be a field. For subfields K_1,K_2 of L, $K_1\cap K_2$ is also a subfield of L (exercise). More generally, for infinitely many subfields K_λ ($\lambda\in\Lambda$) of L, $\bigcap_{\lambda\in\Lambda}K_\lambda$ is also a subfield of L.

Let $\alpha_1,\dots,\alpha_n$ be elements of L and K be a subfield of L. An extension field $K(\alpha_1,\dots,\alpha_n)$ of K is defined as the smallest intermediate field of L/K containing $\alpha_1,\dots,\alpha_n$, which is the intersection of all intermediate field of L/K containing

$\alpha_1, \ldots, \alpha_n$, called the field generated by the adjunction of $\alpha_1, \ldots, \alpha_n$ to K. Especially, a field extension $K(\alpha)/K$ is called a simple extension and α is called a primitive element of the extension.

4.4 splitting fields

In the world of characteristic 0, the field $\mathbb{C}$ has a nice property that every polynomial over $\mathbb{C}$ is completely factored. This property is called that $\mathbb{C}$ is an algebraically closed field. Therefore we can assume the existence of the roots of every polynomial. Over finite fields, we are not familiar to the roots of irreducible polynomials. The roots of them, however, are considered to exist in some extension field.

Theorem 8. *Let K be a field and $g(x)$ be irreducible over K. Then $g(x)$ has a root in the extension field $L = K[y]/g$.*

Proof. Let us take the element y in L. Indeed, y satisfies that $g(y) = 0$. (q.e.d.)

By this theorem, a polynomial $g(x)$ over K has a root α_1 in an extension field L. If $g(x)$ is not completely factored over L, i.e.,

$$g(x) = (x - \alpha_1)g_2(x)g_3(x)\ldots g_s(x), \tag{43}$$

then we take a further extension filed M of L, where $g_2(x)$ has a root α_2. Then over M,

$$g(x) = (x - \alpha_1)(x - \alpha_2)h_3(x)h_4(x)\ldots h_t(x). \tag{44}$$

Repeating this process, we get an extension field where $g(x)$ is completely factored:

$$g(x) = a(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n), \tag{45}$$

i.e., $g(x)$ has all roots in the field. In general, the minimal extension field N of K where a polynomial $g(x)$ is completely factored is called the splitting field of $g(x)$, that is generated by the adjunction of all roots of $g(x)$ to K, say, $N = K(\alpha_1, \ldots, \alpha_n)$. In Section 5.2, we prove that all splitting fields of $g(x)$ are isomorphic to each other.

Corollary 3. *An arbitrary polynomial $g(x)$ over K is completely factored over the splitting field of $g(x)$.*

Next we introduce the minimal polynomial of an element of some extension field.

Theorem 9. *Let $g(x)$ be an irreducible polynomial of degree n over a field K. Let α be a root of $g(x)$ in some extension field L of K. Then for every nonzero polynomial $f(x)$ over K of degree $< n$, we have $f(\alpha) \neq 0$ in L.*

Proof. It is clear that $g(x)$ and $f(x)$ are relatively prime. Thus we have $m(x)g(x) + n(x)f(x) = 1$. Hence $m(\alpha)g(\alpha) + n(\alpha)f(\alpha) = n(\alpha)f(\alpha) = 1$. It shows that $f(\alpha) \neq 0$. (q.e.d.)

By this theorem, we see that $g(x)$ is a polynomial of least degree over K with a root α. If another irreducible polynomial $h(x)$ over K has a root α, then by Theorem 2, $h(x) = (\text{const})g(x)$ or $g(x)$ and $h(x)$ are relatively prime. But as we have seen in the above proof, the only possibility is $h(x) = (\text{const})g(x)$. Therefore an irreducible polynomial over K with a root α is unique up to a constant multiple, which is called the minimal polynomial of α over K.

Theorem 10. *Let K be a field and $g(x)$ be an irreducible polynomial of degree n over K. Let α be a root of $g(x)$. Then every element of $L = K(\alpha)$ is uniquely expressed by a polynomial $h(\alpha)$ of degree $< n$. Hence $[L : K] = n$. In particular, if K is a finite field with q elements, we have $|L| = q^n$.*

Proof. First of all, L is regarded as the set of all rational functions of α with coefficients in K. For a polynomial $f(x)$, if we divide it by $g(x)$ we have $f(x) = g(x)q(x) + r(x)$ ($\deg r(x) < n$), and so $f(\alpha) = r(\alpha)$. Hence any element of L can be written as $\frac{r(\alpha)}{s(\alpha)}$, where the degrees of r, s are less than n. Since $g(x)$ and $s(x)$ are relatively prime, we have $m(x)g(x) + n(x)s(x) = 1$, thus $n(\alpha)s(\alpha) = 1$. Therefore $\frac{r(\alpha)}{s(\alpha)} = r(\alpha)n(\alpha)$, which can be expressed by a polynomial $h(\alpha)$ of degree $< n$. If $h(\alpha) = f(\alpha)$ for some distinct polynomials of degree $< n$, then $h(x) - f(x)$ is of degree $< n$ and has a root α. By Theorem 9, it is impossible. Consequently every element of L is uniquely expressed by $h(\alpha)$. Therefore $\langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\rangle$ is a basis of L over K, and so $[L : K] = n$.

Finally, let $|K| = q$. We have

$$L = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} \mid c_0, \ldots, c_{n-1} \in K\}. \tag{46}$$

Therefore $|L| = q^n$. (q.e.d.)

Theorem 11. *Let $g(x)$ be irreducible over K, and α be a root of $g(x)$ given in some extension field of K. Then $K[x]/g \simeq K(\alpha)$.*

Proof. Define a mapping $\phi : K[x]/g \longrightarrow K(\alpha)$ by

$$\phi(h(x)) = h(\alpha). \tag{47}$$

This is well-defined for every polynomial in $K[x]/g$, that is, if $f(x) = h(x)$ in $K[x]/g$, then $f(\alpha) = h(\alpha)$.

Let $\deg g(x) = n$. By Theorem 10, any element of $K(\alpha)$ is expressed by $h(\alpha)$ of degree $< n$, which is an image of $h(x)$ in $K[x]/g$. Hence ϕ is a surjection.

Next let $f(x), h(x)$ be distinct polynomials of degree $< n$. By Theorem 9, it follows from $\deg(f(x) - h(x)) < n$ that $f(\alpha) - h(\alpha) \neq 0$. Hence ϕ is an injection.

The equalities (18) are easily certified (exercise). Therefore ϕ is an isomorphism, i.e., $K[x]/g \simeq K(\alpha)$. (q.e.d.)

By this theorem, it is shown that

Corollary 4. *The extension field $K(\alpha)$ of K is uniquely determined (up to isomorphism) by the minimal polynomial $g(x)$ of α.*

The isomorphism ϕ that appears in the proof of Theorem 11 clearly fixes every element of K, and so ϕ is a K-isomorphism.

Example 6. We have the following examples of extension fields:

(48)

K	$\mathbb{R}$	$\mathbb{Q}$	$\mathbb{F}_2$
$g(x)$	x^2+1	x^2-2	x^2+x+1
$K[x]/g$	$\mathbb{R}(i)=\mathbb{C}$	$\mathbb{Q}(\sqrt{2}\,)$	$\mathbb{F}_2(\alpha)$

5 Finite Fields 5.1 a polynomial $x^q - x$

Let K be a finite field with $q = p^n$ elements. Consider a polynomial $\pi_K(x)$ associated with K defined as a monic polynomial (the coefficient of the highest term = 1) over K of degree q such that for all $a \in K$, $\pi_K(a) = 0$. Let $K = \{0, a_1, \ldots, a_{q-1}\}$. From $\pi_K(0) = 0$, using the factor theorem, it follows that $\pi_K(x) = xf(x)$, and again, from $a_1 f(a_1) = 0$, it follows that $\pi_K(x) = x(x - a_1)g(x)$. Iterating this, we have the following.

$$\pi_K(x) = x(x - a_1)(x - a_2)\cdots(x - a_{q-1}) \tag{49}$$

Theorem 12. $\pi_K(x) = x^q - x$.

Proof. Let a be an arbitrary nonzero element of K. For the collection of nonzero elements $a_1, a_2, \ldots, a_{q-1}$, we see that $aa_1, aa_2, \ldots, aa_{q-1}$ are also distinct nonzero elements, only a permutation of $a_1, \ldots, a_{q-1}$. (If $aa_i = aa_j$, we have $a_i = a_j$.) Thus, making the product of them, we have

$$a_1 a_2 \ldots a_{q-1} = (aa_1)(aa_2)\ldots(aa_{q-1}) = a^{q-1} a_1 a_2 \ldots a_{q-1}. \tag{50}$$

Hence we have $a^{q-1} = 1$ for all nonzero a. Therefore $a(a^{q-1} - 1) = a^q - a = 0$ for all $a \in K$. (q.e.d.)

By this theorem we have $x^{q-1} - 1 = (x - a_1)(x - a_2)\cdots(x - a_{q-1})$. From the relation between roots and coefficients, it follows that $a_1 + \cdots + a_{q-1} = 0$, $a_1 a_2 + a_1 a_3 + \cdots + a_{q-2} a_{q-1} = 0$, etc, and $a_1 a_2 \ldots a_{q-1} = -1$. (exercise)

Next let L be a finite field of characteristic p and let $q = p^n$.

Theorem 13. *For arbitrary elements $a, b \in L$, we have $(a + b)^q = a^q + b^q$. Also $(p - 1)^q = p - 1$.*

Proof. $(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + b^p$. Here, for all $1 \le i \le p - 1$, $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$ is a multiple of p, because p is not divisible by any of $2, 3, \ldots, i$ and

$$\binom{p}{i} = p \frac{(p-1)(p-2)\ldots(p-i+1)}{i(i-1)\cdots 1} = p \cdot (\text{integer}). \tag{51}$$

Thus, $(a+b)^p = a^p + b^p$. Taking pth power of itself, $(a+b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2}$. Iterating this, we have $(a + b)^q = a^q + b^q$.

Next for odd q, it is clear that $(p-1)^q = (-1)^q = -1 = p-1$. If $q = 2^n$, then $p = 2$, and so $(p - 1)^q = 1^q = 1 = p - 1$ is also clear. (q.e.d.)

Theorem 14. *If the polynomial $\pi(x) = x^q - x$ is completely factored over L, then all roots of $\pi(x)$ compose a finite field K with q elements.*

Proof. Let the collection of all roots of $\pi(x)$ be K. First, since $0, 1 \in L$ are clearly roots of $\pi(x)$, we have $0, 1 \in K$. According to Theorem 13, for arbitrary $a, b \in K$,

$$\begin{aligned} &(a+b)^q = a^q + b^q = a + b \\ &(ab)^q = a^q b^q = ab \\ &(-a)^q = (-1)^q a^q = -a. \end{aligned} \tag{52}$$

Hence $a+b$, ab, $-a$ are also elements of K. And from $a(a^{-1})^q = a^q(a^{-1})^q = (aa^{-1})^q = 1^q = 1$, it follows that $(a^{-1})^q = a^{-1}$, i.e., $a^{-1} \in K$. Therefore K is closed under the four operations.

By Theorem 15 stated later, we see that all roots of $\pi(x)$ are distinct q elements. (q.e.d.)

By Corollary 3, there exists an extension field L conformable to Theorem 14. Therefore Theorem 14 assures the existence of a finite field with q elements.

Corollary 5. *There exists a finite field with q elements if and only if q is a power of a prime number.*

It is convenient to introduce the derivatives of arbitrary polynomials. For $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, define $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. Then the following holds.

$$\begin{aligned} &(f(x) + g(x))' = f'(x) + g'(x) \\ &(kf(x))' = kf'(x) \\ &(f(x)g(x))' = f'(x)g(x) + f(x)g'(x) \end{aligned} \tag{53}$$

(exercise) Show the above formulas.

Theorem 15. *Over a field of characteristic p, $\pi(x) = x^q - x$ has no multiple roots.*

Proof. If $\pi(x)$ has a multiple root α then $x^q - x = (x-\alpha)^2 g(x)$. Differentiating both sides, we have

$$\begin{aligned} qx^{q-1} - 1 &= 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) \\ -1 &= (x-\alpha)(2g(x) + (x-\alpha)g'(x)). \end{aligned} \tag{54}$$

Putting $x = \alpha$, we have $-1 = 0$. (contradiction) (q.e.d.)

Theorem 15 is generalized as follows.

Theorem 16. *Let $n = p^r m$, and let p and m be relatively prime. Over a field of characteristic p, all roots of $x^n - 1$ are p^r-tuple roots.*

Proof. First, we show $x^m - 1$ has no multiple roots. In a similar manner of the above proof, if $x^m - 1$ has a multiple root α, then $x^m - 1 = (x-\alpha)^2 g(x)$. Differentiating both sides,

$$m x^{m-1} = (x-\alpha)(2g(x) + (x-\alpha)g'(x)). \tag{55}$$

Putting $x = \alpha$, we have $m\alpha^{m-1} = 0$. Since p, m are relatively prime, $m\alpha^{m-1} \neq 0$. (contradiction)

Next for $n = p^r m$, by Theorem 13, we have $(x^m - 1)^{p^r} = (x^m)^{p^r} + (-1)^{p^r} = x^n - 1$. This shows that all roots of $x^n - 1$ are p^r-tuple as desired. (q.e.d.)

5.2 uniqueness of the q-element field

This section is devoted to the fundamental theorem for finite fields:

Theorem 17. *Let L, M be finite fields of q elements. Then $L \simeq M$.*

This theorem tells that the structure of finite fields is determined only by the number of the elements. We denote by $\mathbb{F}_q$ the field of q elements. To prove this theorem, we need the following.

Theorem 18. *Let K be a field and $f(x)$ be a polynomial over K. The splitting field of $f(x)$ is unique up to isomorphism.*

Proof. Let L and M be the splitting fields of a polynomial $f(x)$ over K. Let $f(x) = g_1(x)g_2(x)\dots\ g_s(x)$ be a factorization into irreducible factors over K. Let L_1 and M_1 be subfields of L and M, respectively, such that each of L_1 and M_1 is generated by the adjunction of a root of $g_1(x)$ to K. By Corollary 4, we have $L_1 \simeq M_1$. Let $\phi : L_1 \longrightarrow M_1$ be a K-isomorphism. By Corollary 2, it is extended to a $K[x]$-isomorphism $\phi : L_1[x] \longrightarrow M_1[x]$, where ϕ operates on the coefficients of polynomials.

Let $f(x) = h_1(x)h_2(x)\dots h_t(x)$ be a further factorization into irreducible factors over L_1. Since ϕ fixes $f(x)$, we have

$$\phi(f(x)) = \phi(h_1(x)\dots h_t(x)) = \phi(h_1(x))\dots\phi(h_t(x)) = h_1^*(x)\dots h_t^*(x) = f(x). \quad (56)$$

Therefore over M_1, we have $f(x) = h_1^*(x)h_2^*(x)\dots h_t^*(x)$. Now we adjoin a root α of $h_1(x)$ to L_1 to have $L_2 = L_1(\alpha)$. Similarly, we adjoin a root α^* of $h_1^*(x)$ to M_1 to have $M_2 = M_1(\alpha^*)$. By Theorem 11, we have $L_2 \simeq L_1[x]/h_1$, and $M_2 \simeq M_1[x]/h_1^*$.

Now we prove $\phi : L_1[x]/h_1 \longrightarrow M_1[x]/h_1^*$ is an isomorphism. First ϕ is well-defined because for $u(x)$ and $\tilde{u}(x) = u(x) + m(x)h_1(x)$, we have $\phi(\tilde{u}(x)) = \phi(u(x)) + \phi(m(x))h_1^*(x) = \phi(u(x))$.

Next ϕ has clearly the property of a homomorphism (21). Then we show ϕ is a bijection. Let $u_1(x) \neq u_2(x)$ in $L_1[x]/h_1$. Since $u_1(x) - u_2(x)$ is not divisible by irreducible $h_1(x)$, $u_1(x) - u_2(x)$ and $h_1(x)$ are relatively prime, i.e., $m(x)(u_1(x) - u_2(x)) + n(x)h_1(x) = 1$. Thus $\phi(m(x))(\phi(u_1(x)) - \phi(u_2(x))) + \phi(n(x))h_1^*(x) = 1$. Therefore we have $\phi(u_1(x)) \neq \phi(u_2(x))$ in $M_1[x]/h_1^*$. This shows that ϕ is an injection.

Finally, take arbitrary $v(x) = b_0 + b_1x + \dots + b_rx^r$ in $M_1[x]/h_1^*$. Since ϕ is an isomorphism from L_1 to M_1, there exist a_i satisfying $\phi(a_i) = b_i$. Hence for $u(x) = a_0 + a_1x + \dots + a_rx^r$, $\phi(u(x)) = v(x)$. Thus ϕ is a surjection. Therefore it is proved that ϕ is an isomorphism.

Seeing that a mapping $\psi : L_2 \longrightarrow M_2$ is composed of the above-mentioned isomorphisms which fix every element of K, ψ is a K-isomorphism and we have $L_2 \simeq M_2$. Since $f(x)$ has a finite degree, iterating the above argument, we reach $L \simeq M$. (q.e.d.)

By this theorem, we can give a proof of Theorem 17.

Proof. Let L and M be finite fields of $q = p^n$ elements. By Section 4.2, L and M are of characteristic p. Then L and M have a common subfield $\mathbb{F}_p$. By Theorem 12, $\pi_L(x) = \pi_M(x) = x^q - x$. Therefore both of L and M are generated by the adjunction of all roots of $x^q - x$. Hence by Theorem 18, we have $L \simeq M$. (q.e.d.)

By Theorem 17 and Corollary 5, we have

Corollary 6. *There exists a unique finite field of q elements up to isomorphism if and only if q is a power of a prime number.*

Example 7. Let α, β and γ be roots of irreducible polynomials x^2+1, x^2+x+2 and x^2+2x+2 over $K = \mathbb{F}_3$, respectively. Let $L = K(\alpha)$, $M = K(\beta)$, $N = K(\gamma)$. They are finite fields of 9 elements. Hence by Theorem 17, they are isomorphic to each other. Thus, there exist isomorphisms $\phi : L \longrightarrow M$, $\psi : M \longrightarrow N$.

It is shown that for all $a \in K$, $\phi(a) = a$ (exercise). Therefore to construct isomorphisms, it suffices to find that the image of α by ϕ, and the image of β by ψ.

Assume $\phi(\alpha) = m\beta + n$, $\psi(\beta) = r\gamma + s$, where $m, n, r, s \in \mathbb{F}_3$. From $\alpha^2 + 1 = 0$, it follows that

$$\begin{aligned} &\phi(\alpha^2+1) = [\phi(\alpha)]^2 + \phi(1) = (m\beta+n)^2 + 1 \\ &= m^2\beta^2 + 2mn\beta + n^2 + 1 = 0. \end{aligned} \tag{57}$$

As $m \neq 0$, this is the minimal polynomial of β. But by definition, we have $\beta^2+\beta+2 = 0$. Thus we have $m^2\beta^2+2mn\beta+n^2+1 = m^2(\beta^2+\beta+2)$. Hence $2mn = m^2$, $n^2+1 = 2m^2$. Solving these equations, we have $(m, n) = (1, 2)$ or $(2, 1)$. Therefore $\phi(\alpha) = \beta + 2$ or $\phi(\alpha) = 2\beta + 1$.

Similarly, from $\beta^2 + \beta + 2 = 0$, it follows that

$$\begin{aligned} &\psi(\beta^2+\beta+2) = [\psi(\beta)]^2 + \psi(\beta) + \psi(2) \\ &= (r\gamma+s)^2 + (r\gamma+s) + 2 \\ &= r^2\gamma^2 + (2rs+r)\gamma + s^2 + s + 2 = 0. \end{aligned} \tag{58}$$

Comparing with $\gamma^2+2\gamma+2 = 0$, we have $r^2\gamma^2+(2rs+r)\gamma+s^2+s+2 = r^2(\gamma^2+2\gamma+2)$. Hence $2rs + r = 2r^2$, $s^2 + s + 2 = 2r^2$. Solving these equations, we have $(r, s) = (2, 0)$ or $(1, 2)$. Therefore $\psi(\beta) = 2\gamma$ or $\psi(\beta) = \gamma + 2$.

The following table summarizes the above result.

(59)

L	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
M								$2\beta+2$	
M				$2\beta+1$	$2\beta+2$				
N							$2\gamma+2$		
N						$2\gamma+1$			

6 Structure of Finite Fields

6.1 iterated extensions

We have shown that the q-element field $\mathbb{F}_q$ is unique up to isomorphism. In this section, we study the structure of finite fields in the viewpoint of subfield inclusion.

Given a sequence of fields $L_0, L_1, \ldots, L_s$ such that L_i/L_{i-1} is a field extension for every $i = 1, \ldots, s$, a field extension L_s/L_0 is called an iterated extension. Let L/K be a field extension and let $\alpha_1, \ldots, \alpha_s$ be elements in L. Then it holds that $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ (exercise).

Let $K = \mathbb{F}_2$, and let α be a root of an irreducible polynomial $x^2 + x + 1$ over K. Let $L = K(\alpha)$, and let $\tilde{\alpha}$ be a root of an irreducible polynomial $x^2 + x + \alpha$ over L. Let $M = L(\tilde{\alpha})$. The following is a table of the elements of K, L and M.

K	0	1						
L	0	1	α	$\alpha+1$				
M	0	1	α	$\alpha+1$	$\tilde{\alpha}$	$\tilde{\alpha}+1$	$\tilde{\alpha}+\alpha$	$\tilde{\alpha}+\alpha+1$
	$\alpha\tilde{\alpha}$	$\alpha\tilde{\alpha}+1$	$\alpha\tilde{\alpha}+\alpha$	$\alpha\tilde{\alpha}+\alpha+1$	$(\alpha+1)\tilde{\alpha}$	$(\alpha+1)\tilde{\alpha}+1$	$(\alpha+1)\tilde{\alpha}+\alpha$	$(\alpha+1)\tilde{\alpha}+\alpha+1$

It is clear that $L \simeq \mathbb{F}_4$, $M \simeq \mathbb{F}_{16}$. Hence it is valid that $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$. (exercise: Make the multiplication table of L.)

We can construct $\mathbb{F}_{16}$ in another way. Let u be a root of an irreducible polynomial $x^4 + x + 1$ over K and $N = K(u)$. Then we see that $N \simeq \mathbb{F}_{16}$ and there exists a K-isomorphism $\phi : M \longrightarrow N$. To find ϕ, we factor $x^4+x+1 = (x^2+x+\alpha)(x^2+x+\alpha+1)$ in L (exercise). Furthermore, in M, we obtain

$$\begin{array}{ll} x^2 + x + \alpha & = (x - \tilde{\alpha})(x - (\tilde{\alpha} + 1)) \\ x^2 + x + \alpha + 1 & = (x - (\tilde{\alpha} + \alpha))(x - (\tilde{\alpha} + \alpha + 1)). \end{array} \tag{60}$$

By ϕ, $f(x) = x^4 + x + 1$ is invariant when ϕ act on the coefficients, and then

$$\phi(f(x)) = (x - \phi(\tilde{\alpha}))(x - \phi(\tilde{\alpha} + 1))(x - \phi(\tilde{\alpha} + \alpha))(x - \phi(\tilde{\alpha} + \alpha + 1)) = f(x). \tag{61}$$

Consequently, there are four possibilities of ϕ:

$$\begin{array}{ll} \phi(\tilde{\alpha}) = u & \phi(\tilde{\alpha} + 1) = u \\ \phi(\tilde{\alpha} + \alpha) = u & \phi(\tilde{\alpha} + \alpha + 1) = u. \end{array} \tag{62}$$

From upper two equalities, it follows that $\phi(\tilde{\alpha}) = u$ or $\phi(\tilde{\alpha}) = u+1$. Next let $\phi(\tilde{\alpha}+\alpha) = u$, $\phi(\tilde{\alpha}) = t$. By $\tilde{\alpha}^2 + \tilde{\alpha} = \alpha$, we have $\phi(\tilde{\alpha}^2 + \tilde{\alpha}) = t^2 + t = \phi(\alpha)$. Thus $\phi(\tilde{\alpha} + \alpha) = \phi(\tilde{\alpha}) + \phi(\alpha) = t + t^2 + t = t^2 = u$. Here $t^2 - u = t^2 + u^4 + 1 = (t + u^2 + 1)^2 = 0$. Hence $t = u^2 + 1$, i.e., $\phi(\tilde{\alpha}) = u^2 + 1$. Similarly, from $\phi(\tilde{\alpha} + \alpha + 1) = u$, it follows that $\phi(\tilde{\alpha}) = u^2$. Finally, we have the table of the isomorphisms ϕ (Table 2).

In the above example, we see that $\mathbb{F}_{2^1} \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}$, where $1 \mid 2 \mid 4$. In general, we have the following.

Theorem 19. *$\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ is a field extension $\iff$ $m \mid n$.*

M	0	1	α	$\alpha+1$
N	0	1	u^2+u	u^2+u+1
N	0	1	u^2+u	u^2+u+1
N				
N	0	1	u^2+u+1	u^2+u
M	$\tilde{\alpha}$	$\tilde{\alpha}+1$	$\tilde{\alpha}+\alpha$	$\tilde{\alpha}+\alpha+1$
N				
N	$u+1$	u	u^2+1	u^2
N	u^2+1	u^2	u	$u+1$
N	u^2	u^2+1	$u+1$	u
M	$\alpha\tilde{\alpha}$	$\alpha\tilde{\alpha}+1$	$\alpha\tilde{\alpha}+\alpha$	$\alpha\tilde{\alpha}+\alpha+1$
N	u^3+u^2	u^3+u^2+1	u^3+u	u^3+u+1
N				
N	u^3	u^3+1	u^3+u^2+u+1	u^3+u^2+u
N	u^3+u^2+u+1	u^3+u^2+u	u^3	u^3+1
M	$(\alpha+1)\tilde{\alpha}$	$(\alpha+1)\tilde{\alpha}+1$	$(\alpha+1)\tilde{\alpha}+\alpha$	$(\alpha+1)\tilde{\alpha}+\alpha+1$
N	u^3+u^2+u	u^3+u^2+u+1	u^3	u^3+1
N	u^3+1	u^3	u^3+u^2+u+1	u^3+u^2+u
N	u^3+u^2+1	u^3+u^2	u^3+u	u^3+u+1
N				

TABLE 2

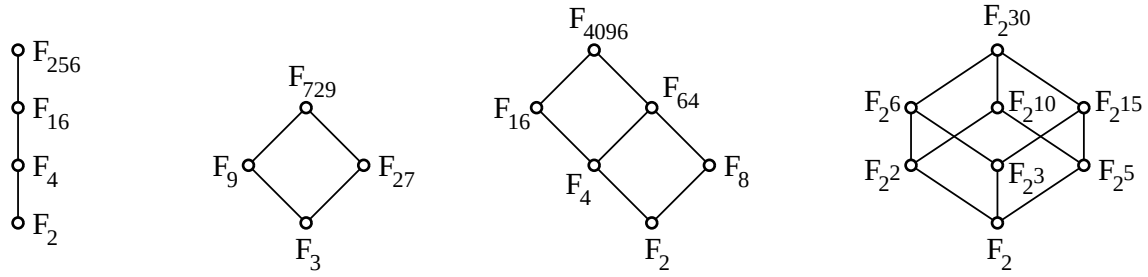

FIGURE 1

Proof. At this stage we prove only ($\Longrightarrow$). Let $\mathbb{F}_{q^n} = L$, $\mathbb{F}_{q^m} = K$, and L/K be a field extension. Then L is regarded as a vector space over K. Let the basis of L be $\langle e_1, \ldots, e_l \rangle$. We have

$$L = \{k_1 e_1 + k_2 e_2 + \cdots + k_l e_l \mid k_1, \ldots, k_l \in K\}. \tag{63}$$

Hence $|L| = |K|^l$. Combining it with $|L| = q^n$ and $|K| = q^m$, we have $q^n = (q^m)^l = q^{ml}$. Therefore $m \mid n$. (q.e.d.)

We have several examples of inclusion relations between finite fields in Figure 1. Each diagram is isomorphic to the lattice D_n of positive divisors of some positive integer n, ordered by division.

6.2 factorization of $\pi_K(x)$

We begin with the following theorems:

Theorem 20. *Let $f(x)$ and $g(x)$ be polynomials over K. Assume $g(x)$ is irreducible over K. Then $g(x) \mid f(x)$ if and only if $f(x)$ and $g(x)$ have a common root α.*

Proof. Let $f(x)$, $g(x)$ have a common root α. As $g(x)$ is irreducible, the gcd of $f(x)$ and $g(x)$ should be a constant or $g(x)$. For the former case, we have $m(x)f(x)+n(x)g(x) = 1$, which leads to $0 = m(\alpha)f(\alpha) + n(\alpha)g(\alpha) = 1$. (contradiction) Therefore the latter case is valid.

Conversely, let $g(x) \mid f(x)$, i.e., $f(x) = m(x)g(x)$. We know $g(x)$ has a root α in some extension field, and it is clear that $f(\alpha) = m(\alpha)g(\alpha) = 0$. (q.e.d.)

Theorem 21. *Let $f(x), g_1(x), \ldots, g_s(x)$ be polynomials over K, and any two of $g_1(x), \ldots, g_s(x)$ be relatively prime. Assume $g_i(x) \mid f(x)$ for all i. Then we have $(g_1(x) \ldots g_s(x)) \mid f(x)$.*

Proof. If we consider the splitting field of $g_1(x) \ldots g_s(x)f(x)$, and use the unique factorization property, then this theorem is similar to the case of division of integers. Here we present another proof.

Induction on s. For $s = 1$, trivial and assume valid for $s - 1$. Let $g_1(x), \ldots, g_s(x)$ be as in the theorem. First we show any two of $g_1(x)g_2(x), g_3(x), g_4(x), \ldots, g_s(x)$ are also relatively prime. From the assumption for $g_1(x), g_2(x), g_3(x)$, it follows, for some $m_i(x)$, $\tilde{m}_3(x)$, that $m_1(x)g_1(x) + m_3(x)g_3(x) = 1$ and $m_2(x)g_2(x) + \tilde{m}_3(x)g_3(x) = 1$. Consequently,

$$\begin{aligned} m_1(x)g_1(x)g_2(x) + m_3(x)g_2(x)g_3(x) &= g_2(x) \\ m_2(x)g_1(x)g_2(x) + \tilde{m}_3(x)g_1(x)g_3(x) &= g_1(x). \end{aligned} \tag{64}$$

Thus, for some $n_i(x)$ ($g_i(x) = g_i$, etc. for short),

$$n_2(m_1g_1g_2 + m_3g_2g_3) + n_1(m_2g_1g_2 + \tilde{m}_3g_1g_3) = 1, \tag{65}$$

and therefore

$$m(x)g_1(x)g_2(x) + n(x)g_3(x) = 1. \tag{66}$$

Repeating similar arguments, we see that $g_1(x)g_2(x) \ldots g_{s-1}(x)$ and $g_s(x)$ are relatively prime. $(*)$

By induction's hypothesis, we have $(g_1(x) \ldots g_{s-1}(x)) \mid f(x)$, and of course $g_s(x) \mid f(x)$. Hence if the theorem is valid for $s = 2$, it follows from $(*)$ that $(g_1(x) \ldots g_s(x)) \mid f(x)$.

For $s = 2$, we have, for some $m(x), n(x)$, $m(x)g_1(x) + n(x)g_2(x) = 1$, and $f(x) = g_1(x)d_1(x) = g_2(x)d_2(x)$. Then

(67)
$$0 = m(x)(g_1(x)d_1(x) - g_2(x)d_2(x)) = (1 - n(x)g_2(x))d_1(x) - m(x)g_2(x)d_2(x).$$
$$\therefore\ d_1(x) = g_2(x)(n(x)d_1(x) + m(x)d_2(x)).$$
$$\therefore\ f(x) = g_1(x)g_2(x)(n(x)d_1(x) + m(x)d_2(x)). \qquad \text{(q.e.d.)}$$

The following is immediately derived from Theorem 21.

Corollary 7. *Let $f(x)$ be a polynomial over K, and let $g_1(x), \dots, g_s(x)$ be irreducible polynomials over K, none of which be a constant multiple of any other $g_j(x)$. Assume $g_i(x) \mid f(x)$ for all i. Then we have $(g_1(x) \dots g_s(x)) \mid f(x)$.*

For convenience, we write $\pi_{\mathbb{F}_q}(x) = x^q - x = \pi_q(x)$. Let $K = \mathbb{F}_q$, and $g(x)$ be an arbitrary irreducible polynomial of degree n over K. Let α be a root of $g(x)$. Let $L = K(\alpha)$. By Theorem 10, we have $|L| = q^n$. Hence $L \simeq \mathbb{F}_{q^n}$, and $\pi_L(x) = x^{q^n} - x \equiv \pi_{q^n}(x)$. Here as $\alpha \in L$, we have $\pi_L(\alpha) = \pi_{q^n}(\alpha) = 0$. Therefore together with $g(\alpha) = 0$ and irreducibility of $g(x)$, from Theorem 20 it follows that $g(x) \mid \pi_{q^n}(x)$. Since $g(x)$ is arbitrary, for all irreducible polynomials $g_i(x)$ over K of degree n, we have $g_i(x) \mid \pi_{q^n}(x)$. If $g_1(x), \dots, g_s(x)$ satisfy that each of them is not a constant multiple of any other $g_j(x)$, then by Corollary 7 we have $(g_1(x) \dots g_s(x)) \mid \pi_{q^n}(x)$, i.e.,

Theorem 22. *Let $j_{qn}(x) = \prod g_i(x)$, where the product runs over all monic irreducible polynomials over $\mathbb{F}_q$ of degree n. Then it holds that $j_{qn}(x) \mid \pi_{q^n}(x)$.*

Next we state further factorability of $\pi_{q^n}(x)$.

Theorem 23. *It holds that* $m \mid n \iff q^m - 1 \mid q^n - 1 \iff \pi_{q^m}(x) \mid \pi_{q^n}(x)$.

Proof. First we show $m \mid n \iff q^m - 1 \mid q^n - 1$. Let $n = ms + r$, $0 \le r < m$. We have

(68)
$$\begin{aligned} q^n - 1 &= (q^m - 1)(q^{n-m} + q^{n-2m} + \cdots + q^{n-sm}) + q^{n-sm} - 1 \\ &= (q^m - 1)(q^{n-m} + q^{n-2m} + \cdots + q^r) + q^r - 1. \end{aligned}$$

Therefore we see $m \mid n \iff r = 0 \iff q^m - 1 \mid q^n - 1$.

A similar argument is applied to show the rest part, i.e., $q^m - 1 \mid q^n - 1 \iff x^{q^m-1} - 1 \mid x^{q^n-1} - 1 \iff \pi_{q^m}(x) \mid \pi_{q^n}(x)$. (q.e.d.)

By this theorem, we see that if $m \mid n$, then $\pi_{q^m}(x) \mid \pi_{q^n}(x)$, and therefore $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, because first we can consider a field $\mathbb{F}_{q^n}$ of all roots of $\pi_{q^n}(x)$, and then by Theorem 14, all roots of $\pi_{q^m}(x)$ form $\mathbb{F}_{q^m}$. This proves Theorem 19 ($\Longleftarrow$).

Theorem 24. *Let m, n be positive integers, and assume m is not a divisor of n. Let $g(x)$ be an irreducible polynomial of degree m over $\mathbb{F}_q$. Then $g(x)$ is not a divisor of $\pi_{q^n}(x)$.*

Proof. By reduction to absurdity. Suppose $g(x) \mid \pi_{q^n}(x)$. By Theorem 20, we have a common root α of $g(x)$ and $\pi_{q^n}(x)$. Hence we have $\alpha \in \mathbb{F}_{q^n}$. Next consider an extension field $L = \mathbb{F}_q(\alpha)$. Then $\mathbb{F}_{q^n}/L$ is a field extension. But by Theorem 10, we have $|L| = q^m$, and by Theorem 19, $m \mid n$. (contradiction) (q.e.d.)

According to Theorems 22 and 23, for every divisor m of n, we have $j_{qm}(x) \mid \pi_{q^m}(x) \mid \pi_{q^n}(x)$. Furthermore, by Theorem 24, there is no irreducible divisor $g(x)$ of $\pi_{q^n}(x)$, where the degree of $g(x)$ is not a divisor of n. And also, by Theorem 15, $\pi_{q^n}(x)$ has no multiple roots. These results are summarized as follows.

Theorem 25. *$\pi_{q^n}(x)$ is factored into irreducible factors over $\mathbb{F}_q$:*

$$\pi_{q^n}(x) = \prod_{m|n} j_{qm}(x). \tag{69}$$

Example 8. (1) $\pi_{2^n}(x) = x^{2^n} - x$ is factored over $\mathbb{F}_2$ as follows:

$$x^4 - x = x(x+1)(x^2+x+1), \qquad x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1),$$
$$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x+1)(x^4+x^3+1).$$

(2) $\pi_{3^2}(x) = x^9 - x$ is factored over $\mathbb{F}_3$ as follows: (see Example 7)

$$x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

(3) Let α be a root of x^2+x+1 in $\mathbb{F}_4$. $\pi_{4^2}(x) = x^{16} - x$ is factored over $\mathbb{F}_4$ as follows: (see Section 6.1)

$$\begin{aligned} x^{16} - x = \; & x(x+1)(x+\alpha)(x+\alpha+1)(x^2+\alpha x+1)(x^2+(\alpha+1)x+1) \\ & \cdot(x^2+x+\alpha)(x^2+x+\alpha+1)(x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+\alpha+1). \end{aligned}$$

(exercise) Confirm the above equalities.

(exercise) Let $\pi_{81}(x) = g_1(x)\dots g_s(x)h_1(x)\dots h_t(x)$ be a factorization into irreducible factors over $\mathbb{F}_9$. Let the degree of $g_1(x), \dots, g_s(x)$ be 1, and $\deg h_i(x) > 1$. (1) Determine $\deg h_i(x)$. (2) Determine s and $g_i(x)$. (3) Determine t.

(exercise) For $n \le 6$, determine the number of all irreducible monic polynomials over $\mathbb{F}_9$ of degree n.

6.3 normal extensions

Let K be a finite field and M be an extension field of K. Let $g(x)$ be an arbitrary irreducible polynomial over K with a root α in M. Then $L = K(\alpha)$ is a subfield of M and $\pi_L(x)$ and $g(x)$ have a common root α. Hence by Theorem 20, $g(x) \mid \pi_L(x)$. This means that all roots of $g(x)$ are contained in L, i.e., L is the splitting field of $g(x)$. Now we have shown that a field extension M/K has a property: every irreducible polynomial over K with a root in M is always completely factored over M. This property is called that M/K is a normal extension.

Theorem 26. *Every field extension of finite fields is normal.*

7 Primitive Elements 7.1 groups

In this section we introduce the basic notions of group theory, because we need them to study the primitive elements of finite fields. A set G is called a group with an operation $*$ if a binary operation $*$ is defined on G, G is closed under $*$, i.e., $a, b \in G \implies a * b \in G$, and the following group axioms are satisfied.

- The associative law holds, i.e., for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- There exists an element e such that for all $a \in G$, $a * e = e * a = a$.
  The element e is called the identity (element) of G, often denoted by $1 = 1_G$.
- For every $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = 1$.
  The element b is called the inverse (element) of a, denoted by a^{-1}.

The operation $*$ is usually multiplication $(\cdot)$ or addition $(+)$. In the former case G is called a multiplicative group, while in the latter case G is called an additive group. The identity of an additive group is usually denoted by 0, called zero, and the additive inverse of a is denoted by $-a$.

If $a * b = b * a$ for all a, b in G, then G is called an Abelian (commutative) group. Any additive group is supposed to be Abelian, but several multiplicative groups are not Abelian.

Let G, G' be groups. A mapping $\phi : G \longrightarrow G'$ is called a homomorphism from G to G' if ϕ satisfies

$$\phi(a * b) = \phi(a) * \phi(b) \qquad (\text{for all } a, b \in G). \tag{70}$$

A bijective homomorphism is called an isomorphism. If there exists an isomorphism from G to G', then G is called isomorphic to G', denoted by $G \simeq G'$.

A direct product $G_1 \times G_2$ of groups is a group defined by

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}, \tag{71}$$

where the operation is defined by $(g_1, g_2) * (g_1', g_2') = (g_1 * g_1', g_2 * g_2')$. We see that $1_{G_1 \times G_2} = (1_{G_1}, 1_{G_2})$ and $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. A direct product $G_1 \times \cdots \times G_s$ of more than two groups is defined similarly.

(exercise) For an additive group $\mathbb{R}$ and a multiplicative group $\mathbb{R}^+$ of all positive real numbers, show $\mathbb{R} \simeq \mathbb{R}^+$.

(exercise) Show $\mathbb{R} \times \mathbb{R} \simeq \mathbb{C}$.

Hereafter, we consider a multiplicative group G and write $a \cdot b = ab$ for short. If a subset H of G also forms a group with the operation of G, then H is called a subgroup of G. This is usually represented by $H \leq G$. It is clear that G and $\{1\}$ are subgroups of G, which are called trivial subgroups. For a subgroup H of G, define

$$aH = \{ah \mid h \in H\}, \qquad Ha = \{ha \mid h \in H\}. \tag{72}$$

The set aH (respectively, Ha) is called the left (respectively, right) coset of a modulo H, and any set which is the left (respectively, right) coset of some element is called a left (respectively, right) coset of G modulo H. Since any element a in G is contained in the cosets aH and Ha, we have the left/right coset decomposition of G modulo H:

$$G = \bigcup_{a \in G} aH = \bigcup_{b \in G} Hb. \tag{73}$$

If $aH \cap bH \neq \varnothing$, $ah_1 = bh_2 \in aH \cap bH$, then for any ah in aH, we have $ah = bh_2h_1^{-1}h = bh' \in bH$. Therefore $aH \subset bH$, similarly $bH \subset aH$, and hence $aH = bH$. It is also valid that $Ha \cap Hb \neq \varnothing \implies Ha = Hb$. Therefore both of (73) are disjoint unions if identical cosets are omitted.

If H yields finitely many distinct left/right cosets of G, then the number of the left cosets is equal to the number of the right cosets, which is called the index of H in G, denoted by $(G : H)$. In this case we have the finite left/right coset decomposition of G modulo H:

$$\begin{aligned} G &= H \cup a_2H \cup a_3H \cup \cdots \cup a_sH \\ G &= H \cup Hb_2 \cup Hb_3 \cup \cdots \cup Hb_s. \end{aligned} \tag{74}$$

In general, for any subsets A, B of G, we define the multiplication of them as

$$AB = \{ab \mid a \in A,\ b \in B\}. \tag{75}$$

Then we see that the associative law $(AB)C = A(BC)$ holds. Definition (75) is a generalization of aH and Ha when they are regarded as $\{a\}H$ and $H\{a\}$, respectively.

Next if a subgroup H of G satisfies that

$$aH = Ha \qquad (\text{for all } a \in G), \tag{76}$$

then H is called a normal subgroup of G, denoted by $H \triangleleft G$. In this case we can identify left and right cosets, and the set of all cosets forms a new group:

$$G/H = \{Ha \mid a \in G\} \tag{77}$$

called the quotient group of G modulo H, with the operation defined by (75). Indeed,

$$(Ha)(Hb) = H(aH)b = H(Ha)b = (HH)(ab) = H(ab), \tag{78}$$

which is some coset of G, and hence G/H is closed under the operation. Other group axioms are confirmed easily. If G is Abelian, it is unnecessary to distinguish left and right cosets, and of course every subgroup is normal. A group with no nontrivial normal subgroup is called a simple group.

(exercise) In G/H, show that $1_{G/H} = H$ and $(Ha)^{-1} = Ha^{-1}$.

(exercise) Let K be a field. Let $GL(n, K)$ denote the general linear group of degree n, the set of all nonsingular matrices of order n over K. Let $SL(n, K)$ denote the special linear group of degree n, the set of all matrices of order n over K, whose determinants are equal to 1. Show that $GL(n, K)$ is a multiplicative group and $SL(n, K)$ is a normal subgroup of $GL(n, K)$.

(exercise) Let S_n be the symmetric group of degree n, the group of all permutations on n letters. Let A_n be the alternating group of degree n, the group of all even permutations on n letters. Show that S_n is a multiplicative group and A_n is a normal subgroup of S_n.

If G contains finite number of elements, then G is called a finite group, and the cardinality $|G|$ is called the order of G. If H is a subgroup of G, then we have $|H| = |aH| = |Ha|$ for all $a \in G$, i.e., all cosets contain the same number of elements. Therefore by (74), we have $|H| \mid |G|$ (Lagrange's theorem), and if H is normal then $|G/H| = |G|/|H| = (G : H)$.

For subgroups G_1, G_2 of G, $G_1 \cap G_2$ is also a subgroup of G. More generally, for infinitely many subgroups G_λ $(\lambda \in \Lambda)$ of G, $\bigcap_{\lambda\in\Lambda} G_\lambda$ is also a subgroup of G.

Given any subset S of G, the subgroup generated by S is defined to be the intersection of all subgroups of G containing S, that is, the smallest subgroup of G containing S, which is denoted by $\langle S\rangle$. It is equal to the subgroup consists of all products of elements of S and their inverses. If $G = \langle S\rangle$, then S is called a generating set of G.

Let a be an element of G. The subgroup generated by $\{a\}$ is written simply as $\langle a\rangle$, that is explicitly expressed as

$$\langle a\rangle = \{1, a^{\pm 1}, a^{\pm 2}, \dots\}. \tag{79}$$

If the least positive integer e such that $a^e = 1$ exists, then e is called the order of a denoted by $\mathrm{ord}(a)$. If there is no such positive integer e, then define $\mathrm{ord}(a) = \infty$. If $\mathrm{ord}(a) = e$, we have

$$\langle a\rangle = \{1, a, a^2, \dots, a^{e-1}\}, \qquad |\langle a\rangle| = \mathrm{ord}(a). \tag{80}$$

(exercise: Determine the inverse of a^k.) A group G is called cyclic if it is generated by one element a (a is a generator of G), i.e., $G = \langle a\rangle$.

Let G be a finite group, then every element has a finite order (exercise). Since $\langle a\rangle$ is a subgroup of G of finite order, by Lagrange's theorem, we have $|\langle a\rangle| \mid |G|$, i.e., $\mathrm{ord}(a) \mid |G|$.

Theorem 27. *Let G be a finite group. Then the order of each element of G is a divisor of $|G|$.*

(exercise) Show that a group of prime order is simple and cyclic.

Theorem 28. *Let G be an Abelian group. Suppose the maximum order e of the finite order elements exists. Then for every finite order element g in G, we have* $\mathrm{ord}(g) \mid e$.

Proof. By reduction to absurdity. Let $\mathrm{ord}(a) = e$, the maximum order of the finite order elements, and $\mathrm{ord}(b) = k < \infty$. Suppose $k \nmid e$. Now let $d = \gcd(e, k)$. Then there exists a decomposition $d = d_1 d_2$ such that $\gcd(e_1, k_1) = 1$, where $e_1 = e/d_1$, $k_1 = k/d_2$ (exercise). Let $a_1 = a^{d_1}$, $b_1 = b^{d_2}$. Then obviously $\mathrm{ord}(a_1) = e_1$, $\mathrm{ord}(b_1) = k_1$. Let $c = a_1 b_1$, $H = \langle c\rangle$. Since e_1, k_1 are relatively prime, we have $me_1 + nk_1 = 1$ for some integers m, n. Hence

$$\begin{aligned} c^{me_1} &= a_1^{me_1} b_1^{1-nk_1} = 1 \cdot b_1 = b_1 \\ c^{nk_1} &= a_1^{1-me_1} b_1^{nk_1} = a_1 \cdot 1 = a_1. \end{aligned} \tag{81}$$

Consider subgroups $I = \langle a_1\rangle$, $J = \langle b_1\rangle$. From (81), it follows that I, J are subgroups of H, and therefore $|I|, |J|$ are divisors of $|H|$. However, as $|I| = e_1$, $|J| = k_1$ are relatively prime, we have $(e_1 k_1) \mid |H|$. On the other hand, $c^{e_1 k_1} = a_1^{e_1 k_1} b_1^{e_1 k_1} = 1$. Therefore $|H| = \mathrm{ord}(c) = e_1 k_1$. Here $e_1 k_1 = ek/d = \mathrm{lcm}\,(e, k)$, and as $k \nmid e$, we have $\mathrm{lcm}\,(e, k) > e$. Hence

$$\mathrm{ord}(c) = e_1 k_1 = \mathrm{lcm}\,(e, k) > e. \tag{82}$$

This contradicts to that e is the maximum order. (q.e.d.)

7.2 existence of primitive elements

Let K be a field. We denote by $K^\times$ the set of all nonzero elements of K. Then $K^\times$ is considered as an Abelian multiplicative group, and called the multiplicative group of K. Next consider a finite field $\mathbb{F}_q$. Then $\mathbb{F}_q^\times$ is finite, and every element of $\mathbb{F}_q^\times$ has a finite order. If an element a in $\mathbb{F}_q$ is a generator of $\mathbb{F}_q^\times$, i.e., $\langle a\rangle = \mathbb{F}_q^\times$, then a is called a primitive element of $\mathbb{F}_q$. By (80),

$$a \text{ is primitive} \iff \langle a\rangle = \mathbb{F}_q^\times \iff \operatorname{ord}(a) = q-1. \tag{83}$$

Therefore we have

Theorem 29. *An element a in $\mathbb{F}_q$ is primitive if and only if* $\operatorname{ord}(a) = q-1$.

Since $\mathbb{F}_q^\times$ is finite, the maximum order e of the elements of $\mathbb{F}_q^\times$ exists. Let $\operatorname{ord}(a) = e$. Then by Theorem 28, the order of every element x is a divisor of e. Therefore for all x in $\mathbb{F}_q^\times$ we have $x^e = 1$, that is, all $(q-1)$ elements of $\mathbb{F}_q^\times$ are roots of $x^e - 1$. However, this polynomial has at most e roots. Therefore, we have $e \geq q-1$, but by Theorem 27, $e \mid |\mathbb{F}_q^\times| = q-1$, thus $e = q-1$. Consequently, a is a primitive element of $\mathbb{F}_q$. Thus we have the following.

Theorem 30. *Every finite field has a primitive element, i.e., the multiplicative group of every finite field is cyclic.*

Once this theorem is proved, we can enumerate the exact number of the primitive elements of $\mathbb{F}_q$. Let a be a primitive element. We have

$$\mathbb{F}_q = \{0, a, a^2, \dots, a^{q-1}\}. \tag{84}$$

Namely, all nonzero elements are expressed by powers of a. The order of a^k is the least positive integer e such that $a^{ke} = 1$. Obviously, we have $ke = \operatorname{lcm}(k, q-1)$. Thus

$$\begin{aligned} a^k \text{ is primitive} &\iff e = q-1 \iff \operatorname{lcm}(k, q-1) = k(q-1) \\ &\iff k \text{ and } (q-1) \text{ are relatively prime.} \end{aligned} \tag{85}$$

For any positive integer n, define Euler's totient function $\varphi(n)$ as the number of positive integers $k \leq n$ which are prime to n. Then we have

Theorem 31. *The number of the primitive elements of $\mathbb{F}_q$ is equal to $\varphi(q-1)$.*

Let e be a divisor of $q-1$. For every element a^k of order e, we have $\operatorname{lcm}(k, q-1)/k = e$. Hence $(q-1)/\gcd(k, q-1) = e$, say,

$$\begin{aligned} \gcd(k, q-1) = (q-1)/e \equiv h &\iff \gcd(k/h, (q-1)/h) = 1 \\ &\iff \gcd(k/h, e) = 1. \end{aligned} \tag{86}$$

Letting $m = k/h$, we have

Theorem 32. *For a divisor e of $q-1$, the number of the elements of order e in $\mathbb{F}_q$ is equal to $\varphi(e)$. For a primitive element a, every element of order e is expressed as $a^{(q-1)m/e}$, where m is prime to e $(1 \leq m \leq e)$.*

Example 9. (1) Let $K = \mathbb{F}_3$ and α be a root of an irreducible polynomial $x^2 + 1$ over K. Let $L = K(\alpha)$. All primitive elements of L and the orders of all elements are determined as follows.

(87)

	1	2	3	4	5	6	7	8	order
1	1								1
2	2								
α	α								
$\alpha+1$	$\alpha+1$			2					
$\alpha+2$	$\alpha+2$								
2α	2α	2	α	1					4
$2\alpha+1$	$2\alpha+1$								
$2\alpha+2$	$2\alpha+2$			2					

(2) The number of the primitive elements of $\mathbb{F}_q$ are as follows, where $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16$.

(88)

q	2	3	4	5	7	8	9	11	13	16
#		1					4			

8 Frobenius Cycles 8.1 basic theorems

Let $K = \mathbb{F}_q$ be a finite field and $L = \mathbb{F}_{q^n}$ be an extension field of K. Let us consider a mapping $\tau : L \longrightarrow L$ defined by

$$\tau(x) = x^q. \tag{89}$$

The mapping τ is called the K-Frobenius transformation of L.

Given x in L, if we operate τ repeatedly, we have a sequence:

$$x,\ x^q,\ x^{q^2}, \ldots,\ x^{q^{n-1}},\ x^{q^n} = x, \tag{90}$$

because $x^{q^n} - x = 0$. Let m be the least positive integer such that $x^{q^m} = x$, then (90) is written as

$$x, x^q, \ldots, x^{q^m} = x, x^q, \ldots, x^{q^m} = x, \ldots, x, x^q, \ldots, x^{q^m} = x. \tag{91}$$

Hence m should be a divisor of n. Then the sequence

$$x, x^q, x^{q^2}, \ldots, x^{q^m} = x \tag{92}$$

consists of distinct elements except for $x = x^{q^m}$, because if $x^{q^i} = x^{q^j}$ for some $1 \leq i < j \leq m$, then

$$x^{q^{m-j+i}} = (x^{q^i})^{q^{m-j}} = (x^{q^j})^{q^{m-j}} = x^{q^m} = x \quad \text{(contradiction)}. \tag{93}$$

The sequence (92) is called a K-Frobenius cycle of length m in L.

By definition, for the K-Frobenius cycle (92), another K-Frobenius cycle beginning with x^{q^i} consists of the same elements as in (92), obtained by cyclic shift:

$$x^{q^i}, x^{q^{i+1}}, \ldots, x^{q^m} = x, x^q, \ldots, x^{q^i}. \tag{94}$$

Consequently, if two K-Frobenius cycles have a common element, then they contain the same elements. This means that all elements are divided into disjoint K-Frobenius cycles. We say that (92) and (94) are equivalent.

Theorem 33. *All elements of L are divided into disjoint K-Frobenius cycles, the lengths of which are divisors of $n = [L : K]$.*

Now the following holds.

Theorem 34. *The K-Frobenius transformation of L is a K-automorphism of L.*

Proof. First of all, for all $x, y \in L$,

$$\begin{aligned} &\tau(x+y) = (x+y)^q = x^q + y^q = \tau(x) + \tau(y) \qquad (\because \text{ Theorem 13}) \\ &\tau(xy) = (xy)^q = x^q y^q = \tau(x)\tau(y). \end{aligned} \tag{95}$$

Thus τ is a homomorphism.

Next we confirm τ is a bijection. Let x, y be elements of L. Suppose $\tau(x) = \tau(y)$. By the following equalities:

$$\begin{aligned} (\tau \circ \tau \circ \cdots \circ \tau)(x) = \tau^n(x) = x^{q^n} = x = \tau^{n-1}(\tau(x)) \\ (\tau \circ \tau \circ \cdots \circ \tau)(y) = \tau^n(y) = y^{q^n} = y = \tau^{n-1}(\tau(y)), \end{aligned} \tag{96}$$

we have $x = y$. Thus τ is an injection.

Let y be an arbitrary element of L. Then take $x = \tau^{n-1}(y)$, then

$$\tau(x) = \tau(\tau^{n-1}(y)) = \tau^n(y) = y. \tag{97}$$

Thus τ is a surjection.

Finally, let x be an element of K. Then $x^q = x$, and therefore $\tau(x) = x$. (q.e.d.)

K-Frobenius cycles have several important properties. Let us consider a K-Frobenius cycle (92). Let $\mathrm{ord}(x) = e$, $y = x^{q^i}$ and $\mathrm{ord}(y) = e'$. Then $y^e = x^{q^i e} = (x^e)^{q^i} = 1$. Hence $e \geq e'$. However, since $y^{q^{m-i}} = (x^{q^i})^{q^{m-i}} = x^{q^m} = x$, we have $x^{e'} = y^{q^{m-i}e'} = (y^{e'})^{q^{m-i}} = 1$. Hence $e \leq e'$. Therefore $e = e'$, i.e.,

Theorem 35. *Each K-Frobenius cycle consists of elements of the same order.*

For primitive elements, it follows from this theorem that

Corollary 8. *If a K-Frobenius cycle contains a primitive element, then the others are also primitive elements.*

(exercise) Show that the length of a K-Frobenius cycle of primitive elements of L is equal to n.

Let a be a primitive element of L and $g(x)$ be the minimal polynomial of a over K. As a is primitive, we have $K(a) = L$, and therefore by Theorem 10, the degree of $g(x)$ is equal to $[L : K] = n$, say,

Theorem 36. *Let $g(x)$ be the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^n}$. Then the degree of $g(x)$ is equal to n.*

By Corollary 2 and Theorem 34, the K-Frobenius transformation τ is extended to a $K[x]$-automorphism of $L[x]$. We write $\tau(f(x)) = \tau f(x)$ for short.

Theorem 37. *All elements of a K-Frobenius cycle form all roots of some irreducible polynomial over K.*

Proof. Let $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^m} = \alpha$ be a K-Frobenius cycle in L. Then α is a root of $\pi_{q^m}(x)$. Hence, by Theorem 20, the minimal polynomial $g(x)$ of α over K is an irreducible factor of $\pi_{q^m}(x)$. By Theorem 25, the degree s of $g(x)$ is a divisor of m. (i)

On the other hand, by Theorem 26, L/K is a normal extension. Hence $g(x)$ is completely decomposed in L:

$$g(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_s). \tag{98}$$

Let us operate τ on both sides. Since $g(x)$ is a polynomial over K, we have $\tau g(x) = g(x)$, and

$$g(x) = \tau g(x) = (x - \tau(\alpha))(x - \tau(\alpha_2)) \ldots (x - \tau(\alpha_s)). \tag{99}$$

Hence for all $0 \leq i \leq m - 1$,

$$g(x) = \tau^i g(x) = (x - \tau^i(\alpha))(x - \tau^i(\alpha_2)) \ldots (x - \tau^i(\alpha_s)). \tag{100}$$

Thus all elements of the K-Frobenius cycle $\alpha, \tau(\alpha), \tau^2(\alpha), \ldots, \tau^{m-1}(\alpha)$ are roots of $g(x)$, and therefore $\deg g(x) \geq m$. (ii)

Frobenius cycles	lengths	orders	irred. polyn.	primitive?
$0, \quad 0$	1	$-$	x	no
$1, \quad 1$	1	1	$x+2$	no
$a, \quad a^3, \quad a$	2	8	x^2+x+2	yes
$a^2, \quad a^6, \quad a^2$	2	4	x^2+1	no
$a^4, \quad a^4$	1	2	$x+1$	yes
$a^5, \quad a^7, \quad a^5$	2	8	x^2+2x+2	yes

TABLE 3

By (i),(ii) we have $\deg g(x) = m$ and

$$g(x) = (x-\alpha)(x-\tau(\alpha))(x-\tau^2(\alpha))\dots(x-\tau^{m-1}(\alpha)). \qquad \text{(q.e.d.)} \tag{101}$$

Given an irreducible polynomial $g(x)$ over K, take the splitting field M of $g(x)$, and apply Theorem 37 to M. We see that $g(x)$ has simple roots all of which make one Frobenius cycle. Together with Theorem 35, we have the following.

Theorem 38. *All roots of an irreducible polynomial are distinct elements of the same order. In particular, all roots of the minimal polynomial of a primitive element are distinct primitive elements.*

In this sense, the minimal polynomial $g(x)$ over K of a primitive element α of L is called a primitive polynomial over K. By Theorem 36, $\deg g(x) = n = [L:K]$, but we can consider primitive polynomials of arbitrary degree if we select a new field extension L'/K. In any case, it is determined by a polynomial itself whether the polynomial is primitive or not, because $K(\alpha) \simeq K[x]/g$, and it is completely determined by $g(x)$ whether $x \in K[x]/g$ is primitive or not.

By Theorem 20 (or Theorem 33), distinct monic primitive polynomials never have common roots. By Theorem 31, we see the number of the primitive elements of L. Summarizing them, we have

Theorem 39. *The number of the monic primitive polynomials over K of degree n is equal to $\varphi(q^n-1)/n$.*

Example 10. Let $K = \mathbb{F}_3, L = \mathbb{F}_9, \alpha$ be as in Example 9. Let $a = \alpha + 1$ be a primitive element of L. We have K-Frobenius cycles in L and corresponding irreducible polynomials in Table 3 (equivalent cycles omitted).

	Frobenius cycles					lengths	orders	irred. polyn.	primitive?
0,	0					1	–	x	no
1,	1					1	1	$x+1$	yes
α,	α^2,	α^4,	α^8,	α		4	15	x^4+x+1	yes
α^3,	α^6,	α^{12},	α^9,	α^3		4	5	$x^4+x^3+x^2+x+1$	no
α^5,	α^{10},	α^5				2	3	x^2+x+1	yes
α^7,	α^{14},	α^{13},	α^{11},	α^7		4	15	x^4+x^3+1	yes

TABLE 4

8.2 cyclic representations

Here the terminology "cyclic representation" is used for a table showing correspondence between powers of a fixed primitive element a and expressions by polynomials in a of least degree. For example, we give a cyclic representation of $\mathbb{F}_{16}$. Let $K=\mathbb{F}_2$, and α be a root of an irreducible polynomial x^4+x+1 over K. Let $L=K(\alpha)\simeq\mathbb{F}_{16}$. Then α is a primitive element of L and

(102)

$\alpha^0=$	1				1000	$\alpha^8=$	1		$+\alpha^2$		1010
$\alpha^1=$		α			0100	$\alpha^9=$		α		$+\alpha^3$	0101
$\alpha^2=$			α^2		0010	$\alpha^{10}=$	1	$+\alpha$	$+\alpha^2$		1110
$\alpha^3=$				α^3	0001	$\alpha^{11}=$		α	$+\alpha^2$	$+\alpha^3$	0111
$\alpha^4=$	1	$+\alpha$			1100	$\alpha^{12}=$	1	$+\alpha$	$+\alpha^2$	$+\alpha^3$	1111
$\alpha^5=$		α	$+\alpha^2$		0110	$\alpha^{13}=$	1		$+\alpha^2$	$+\alpha^3$	1011
$\alpha^6=$			α^2	$+\alpha^3$	0011	$\alpha^{14}=$	1			$+\alpha^3$	1001
$\alpha^7=$	1	$+\alpha$		$+\alpha^3$	1101	$\alpha^{15}=$	1				1000

This table enables us quick calculation in $\mathbb{F}_{16}$, e.g.,

$$\begin{aligned}&\alpha^5+\alpha^6+\alpha^{14}=(\alpha+\alpha^2)+(\alpha^2+\alpha^3)+(1+\alpha^3)=1+\alpha=\alpha^4,\\&(1+\alpha+\alpha^3)^8=(\alpha^7)^8=\alpha^{56}=\alpha^{15\cdot3+11}=\alpha^{11}=\alpha+\alpha^2+\alpha^3.\end{aligned}\tag{103}$$

Example 11. Let K, L, α be as above. K-Frobenius cycles in L and corresponding irreducible polynomials are found in Table 4.

For example, let us determine the irreducible polynomial $g(x)$ with the roots $\alpha^3,\alpha^6,\alpha^{12},\alpha^9$. Let $g(x)=x^4+ax^3+bx^2+cx+d$ $(a,b,c,d\in K)$. As $g(\alpha^3)=0$, we have

$$\begin{aligned}&\alpha^{12}+a\alpha^9+b\alpha^6+c\alpha^3+d\\=\;&(1+\alpha+\alpha^2+\alpha^3)+a(\alpha+\alpha^3)+b(\alpha^2+\alpha^3)+c\alpha^3+d\\=\;&(1+d)+(1+a)\alpha+(1+b)\alpha^2+(1+a+b+c)\alpha^3\;=0.\\\therefore\;&1+d=1+a=1+b=1+a+b+c=0.\end{aligned}\tag{104}$$

Solving this, we have $a=b=c=d=1$, and therefore $g(x)=x^4+x^3+x^2+x+1$.

8.3 the automorphism group of a finite field

Let $K = \mathbb{F}_q$, and $L = \mathbb{F}_{q^n}$ be an extension field of K. Let G be the totality of K-automorphisms of L. For two elements τ, σ in G, $\tau \circ \sigma$ is also an element of G (exercise). It is clear that $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$. The identity $= \mathrm{id}$ is contained in G. For every element τ in G, there exists τ^{-1} because τ is a bijection, and one sees that τ^{-1} is also a K-automorphism. Therefore G is a group with the composition operation $\circ$, called the K-automorphism group of L. Clearly, the K-Frobenius transformation τ is an element of G. We have the following.

Theorem 40. *The K-automorphism group G of L consists of $\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}$, where τ is the K-Frobenius transformation of L. In other words, G is cyclic generated by τ, i.e., $G = \langle \tau \rangle$.*

Proof. Let τ be the K-Frobenius transformation of L. First, it is clear that $\mathrm{id} = \tau^n, \tau, \tau^2, \ldots, \tau^{n-1}$ form $\langle \tau \rangle$ and are clearly contained in G. Therefore it suffices to show that for any K-automorphism σ of L, we have $\sigma = \tau^i$ for some i. Now take a primitive polynomial $g(x)$ over K, having roots $a_1, a_2, \ldots, a_n$ of primitive elements of L, i.e.,

$$g(x) = (x - a_1)(x - a_2) \ldots (x - a_n). \tag{105}$$

Let σ be an arbitrary K-automorphism of L. As in the proof of Theorem 37, operate σ on $g(x)$ to get

$$g(x) = \sigma g(x) = (x - \sigma(a_1))(x - \sigma(a_2)) \ldots (x - \sigma(a_n)). \tag{106}$$

On the other hand, by (101) we have

$$g(x) = (x - a_1)(x - \tau(a_1)) \ldots (x - \tau^{n-1}(a_1)). \tag{107}$$

This shows that $\sigma(a_1) = \tau^i(a_1)$ for some $0 \leq i \leq n - 1$.

Next for an arbitrary element x in $L^\times$, we have $x = a_1^s$ for some s because a_1 is primitive. Then

$$\sigma(x) = \sigma(a_1^s) = (\sigma(a_1))^s = (\tau^i(a_1))^s = \tau^i(a_1^s) = \tau^i(x). \tag{108}$$

Obviously, $\sigma(0) = \tau^i(0) = 0$. Therefore $\sigma = \tau^i$ as desired. (q.e.d.)

We have already seen that the K-Frobenius transformation τ fixes every element of K. Conversely, it is valid that every element fixed by τ is always contained in K. Indeed, let $x \in L$ satisfy $\tau(x) = x^q = x$, then x is a root of $\pi_K(x)$, hence $x \in K$.

Theorem 41. *An element x in L is invariant under the K-Frobenius transformation of L if and only if $x \in K$.*

Corollary 9. *An element x in L is invariant under the K-automorphism group of L if and only if $x \in K$.*

9 Cyclotomic Polynomials 9.1 definition

We have seen that several elements of $\mathbb{F}_q$ ($q = p^n$) of the same order e gather together and form the root set of some irreducible polynomial over $\mathbb{F}_p$ (Theorem 38). The order e should divide $|\mathbb{F}_q^\times| = q-1$ (Theorem 27), and conversely, for each positive divisor e of $q-1$, there exists an element of $\mathbb{F}_q$ of order e. Indeed, let a be a primitive element of $\mathbb{F}_q$, then $a^{(q-1)/e}$ is clearly of order e, and every order-e element is written as $a^{(q-1)m/e}$ with a positive integer $m \leq e$ which is prime to e (Theorem 32).

From this point of view, we have

Theorem 42. *Elements of order e are contained in $\mathbb{F}_q$ if and only if $e \mid q-1$, and if exist, the number of those elements are $\varphi(e)$. Also, for any extension field L of $\mathbb{F}_q$, L contains no other order-e elements than those in $\mathbb{F}_q$.*

Consequently, for elements of order e, we only have to consider the minimal field of characteristic p containing such elements. An element of order e is also called a primitive eth root of unity.

Now define a polynomial:

$$Q_e(x) = (x-\zeta_1)(x-\zeta_2)\dots(x-\zeta_{\varphi(e)}), \tag{109}$$

where $\zeta_1, \dots, \zeta_{\varphi(e)}$ are all primitive eth roots of unity. This polynomial is called the eth cyclotomic polynomial over $\mathbb{F}_p$.

Theorem 43. *Primitive eth roots of unity are expressed by powers of each other.*

Proof. Let $\zeta_1 = a^{(q-1)/e}$ be a primitive eth root of unity, then we have the totality $\zeta_1, \zeta_1^{m_2}, \zeta_1^{m_3}, \dots, \zeta_1^{m_s}$ of primitive eth roots of unity, where $m_1 = 1, m_2, \dots, m_s \leq e$ are prime to e. Let $\zeta_1^{m_i} = \zeta_i$. Since m_i and e are relatively prime, we have $m_i k + el = 1$ for some integers k, l. Then

$$\zeta_i^k = \zeta_1^{m_i k} = \zeta_1^{1-el} = \frac{\zeta_1}{(\zeta_1^e)^l} = \zeta_1. \tag{110}$$

Hence ζ_1 and ζ_i are expressed by powers of each other. Thus, for any i, j, we see that ζ_i and ζ_j are also expressed by powers of each other as desired. (q.e.d.)

By this theorem, using an arbitrary element ζ of order e, we have

$$Q_e(x) = \prod_m (x - \zeta^m), \tag{111}$$

where the product runs over all positive integers $m \leq e$ which are prime to e.

It is necessary to note that if e is a multiple of the characteristic p, then it is impossible to find $q = p^n$ such that $e \mid q-1$ (exercise). Thus there are no primitive eth roots of unity for any multiple e of p. On the contrary, if e is not a multiple of p, then there exists a primitive eth root of unity in some extension field of $\mathbb{F}_p$.

Theorem 44. *A primitive eth root of unity exists in some extension field of $\mathbb{F}_p$ if and only if e is not a multiple of p.*

Proof. Let e not be a multiple of p. Let $g(x) = x^e - 1$ be a polynomial over $\mathbb{F}_p$. By Theorem 16, $g(x)$ has no multiple roots in the splitting field of $g(x)$. Obviously all roots $\alpha_1, \alpha_2, \ldots, \alpha_e$ of $g(x)$ form a multiplicative group G (exercise). Let s be the maximum order of the elements of G. Obviously, $s \mid e$. Furthermore, by Theorem 28, the order of each element of G divides s. Therefore every α_i in G is a root of $x^s = 1$. However G contains exactly e elements. Hence we have $s \geq e$, and together with $s \mid e$, we have $s = e$. Thus a primitive eth root of unity exists. A proof of the converse is already seen. (q.e.d.)

By definition (109), we see that $Q_e(x)$ is a polynomial over $\mathbb{F}_p$. Indeed, by Theorem 35, the set $Z_e = \{\zeta_1, \zeta_2 \ldots, \zeta_{\varphi(e)}\}$ of all order-e elements is divided into disjoint $\mathbb{F}_p$-Frobenius cycles. By Theorem 37, each cycle forms all roots of an irreducible polynomial $p_i(x)$ over $\mathbb{F}_p$. Hence

$$Q_e(x) = p_1(x) \ldots p_s(x) \tag{112}$$

is a polynomial over $\mathbb{F}_p$. Next we prove the following.

Theorem 45. *Assume n is not a multiple of p. Over a finite field of characteristic p, it holds that*

$$x^n - 1 = \prod_{e \mid n} Q_e(x). \tag{113}$$

Proof. Let K be the splitting field of $g(x) = x^n - 1$ over $\mathbb{F}_p$. For any divisor e of n, every element ζ in K of order e satisfies $\zeta^n = 1$, i.e., ζ is a root of $g(x)$, while for any nondivisor e of n, no element of K of order e is a root of $g(x)$. Hence we have

$$x^n - 1 = \prod_{e \mid n} \prod_j (x - \zeta_{ej})^{m(e,j)}, \tag{114}$$

where ζ_{ej} runs over all elements of K of order e. But as n is not a multiple of p, it follows from Theorem 16 that $g(x)$ has no multiple roots. Therefore

$$x^n - 1 = \prod_{e \mid n} \prod_j (x - \zeta_{ej}). \tag{115}$$

This equality is equivalent to (113). (q.e.d.)

Example 12. For given p and e which are relatively prime, we have the least $q = p^n$ such that $e \mid q - 1$, i.e., $\mathbb{F}_q$ contains the primitive eth roots of unity.

p	2							3					5				
e	3	5	7	9	11	13	15	2	4	5	7	8	2	3	4	6	7
q																	

9.2 Möbius inversion formula

The Möbius inversion formula is a very convenient tool which gives the solutions to certain systems of algebraic equations. Let N be a positive integer and $F(n), G(n)$ be two functions defined on the set D_N of all positive divisors n of N. For any positive integer n, define the Möbius function $\mu(n)$ as follows.

$$\mu(n) = \begin{cases} 1 & (n = 1) \\ (-1)^k & (n \text{ is the product of } k \text{ distinct primes}) \\ 0 & (n \text{ is divisible by the square of some prime}) \end{cases} \tag{116}$$

Theorem 46. *We have $\sum_{m|n} \mu(m) = \delta_{1n}$, where δ_{mn} is the Kronecker delta, i.e., $\delta_{mn} = 1$ whenever $m = n$, and otherwise $\delta_{mn} = 0$.*

Proof. Let $n = p_1^{e_1} \dots p_r^{e_r}$ be the decomposition into prime factors. Then $\mu(m)$ has a nonzero value iff $m = p_{i_1} \dots p_{i_s}$. Therefore the summation is given by

$$\begin{aligned} \sum_{m|n} \mu(m) &= \sum_{s=0}^{r} \sum_{1 \le i_1 < \dots < i_s \le r} \mu(p_{i_1} \dots p_{i_s}) = \sum_{s=0}^{r} \sum_{1 \le i_1 < \dots < i_s \le r} (-1)^s \\ &= \sum_{s=0}^{r} \binom{r}{s} (-1)^s = (1-1)^r = \delta_{1n}. \qquad \text{(q.e.d.)} \end{aligned} \tag{117}$$

Theorem 47 (Möbius inversion formula). *The following two systems of linear equations are equivalent.*

$$F(n) = \sum_{m|n} G(m) \qquad (n \in D_N) \tag{118}$$

$$G(n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) F(m) \qquad (n \in D_N) \tag{119}$$

Also, the following two systems of algebraic equations are equivalent.

$$F(n) = \prod_{m|n} G(m) \qquad (n \in D_N) \tag{120}$$

$$G(n) = \prod_{m|n} F(m)^{\mu\left(\frac{n}{m}\right)} \qquad (n \in D_N) \tag{121}$$

Proof. We give a proof of the latter (multiplicative) case. Assume the system of equations (120). We substitute (120) for the right-hand side of (121). Then

$$\begin{aligned} \prod_{m|n} F(m)^{\mu\left(\frac{n}{m}\right)} &= \prod_{m|n} \left(\prod_{k|m} G(k) \right)^{\mu\left(\frac{n}{m}\right)} &&= \prod_{m|n} \prod_{k|m} G(k)^{\mu\left(\frac{n}{m}\right)} \\ &= \prod_{\substack{(k,m) \\ k|m|n}} G(k)^{\mu\left(\frac{n}{m}\right)} &&= \prod_{k|n} \prod_{k|m|n} G(k)^{\mu\left(\frac{n}{m}\right)} \\ &= \prod_{k|n} G(k)^{\sum_{k|m|n} \mu\left(\frac{n}{m}\right)} &&= G(n). \end{aligned} \tag{122}$$

The last equality is confirmed as follows:

$$\sum_{\substack{m \\ k|m|n}} \mu\left(\frac{n}{m}\right) = \sum_{\substack{m_1 \\ m_1|\frac{n}{k}}} \mu\left(\frac{n/k}{m_1}\right) = \sum_{m_1|\frac{n}{k}} \mu(m_1) = \delta_{nk}. \tag{123}$$

A proof of (121) $\Longrightarrow$ (120) is completed similarly. A proof of the additive case is reserved for an exercise. (q.e.d.)

So far, we have several interesting formulas of the form (120). Important examples are (69) and (113). Let $\tilde{n}_{qn}$ denote the number of the monic irreducible polynomials over $\mathbb{F}_q$ of degree n. Comparing the degrees of both sides of (69) and (113), we obtain

$$q^n = \sum_{m|n} m\tilde{n}_{qm}; \quad n = \sum_{m|n} \varphi(m) \tag{124}$$

for every positive integer n. By using the Möbius inversion formula, several equalities are derived from the formulas (69), (113) and (124).

Theorem 48. *It holds that*

$$j_{qn}(x) = \prod_{m|n} (x^{q^m} - x)^{\mu(\frac{n}{m})}; \qquad \tilde{n}_{qn} = \frac{1}{n}\sum_{m|n} \mu\left(\frac{n}{m}\right) q^m \tag{125}$$

$$Q_n(x) = \prod_{m|n} (x^m - 1)^{\mu(\frac{n}{m})}; \qquad \varphi(n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) m. \tag{126}$$

Example 13. By the first equality of (125), we have

$$j_{q6}(x) = \frac{(x^q - x)(x^{q^6} - x)}{(x^{q^2} - x)(x^{q^3} - x)}. \tag{127}$$

(exercise) (1) Determine $j_{q1}(x)$. (2) Determine $j_{32}(x)$. (3) Determine $j_{23}(x)$. (4)* Determine $j_{26}(x)$.

By the first equality of (126), we have

$$Q_{30}(x) = \frac{(x^2 - 1)(x^3 - 1)(x^5 - 1)(x^{30} - 1)}{(x - 1)(x^6 - 1)(x^{10} - 1)(x^{15} - 1)}. \tag{128}$$

(exercise) (1) Determine $Q_1(x)$, $Q_2(x)$ over $\mathbb{F}_3$. (2) Determine $Q_3(x)$ over $\mathbb{F}_5$. (3) Determine $Q_4(x)$ over $\mathbb{F}_3$. (4) Determine $Q_5(x)$ over $\mathbb{F}_2$. (5) Determine $Q_6(x)$ over $\mathbb{F}_7$. (6) Determine $Q_p(x)$ over $\mathbb{F}_3$ for every prime $p \neq 3$. (7) Determine $Q_{p^2}(x)$ over $\mathbb{F}_2$ for every prime $p \neq 2$. (8) Determine $Q_{30}(x)$ over $\mathbb{F}_7$.

By the second equality of (125), we have

$$\tilde{n}_{q6} = \frac{1}{6}(q - q^2 - q^3 + q^6) \tag{129}$$

$$\tilde{n}_{q,30} = \frac{1}{30}(-q + q^2 + q^3 + q^5 - q^6 - q^{10} - q^{15} + q^{30}). \tag{130}$$

(exercise) (1) Determine $\tilde{n}_{2n}$ for $n \leq 6$. (2) Determine $\tilde{n}_{3n}$ for $n \leq 6$. (3) Determine $\tilde{n}_{9n}$ for $n \leq 4$.

By the second equality of (126), we can determine the value of Euler's totient function by mechanical calculation.

(exercise) (1) Determine $\varphi(500)$. (2) Determine $\varphi(666)$. (3) Determine $\varphi(9991)$.

10 Functions Between Finite Fields

10.1 polynomial expression

This section is devoted to a treatment of general functions between finite fields. In the case of characteristic 0, a function is not, in general, expressible in a explicit form. If we add several suitable conditions to the functions, then they are expressed in various forms, power series, rational expressions, polynomials, etc. In the case of finite fields, it is very different to the above case, every function is expressed by a polynomial.

Let $K = \mathbb{F}_q$ be a finite field. Consider a function $f : K^n \longrightarrow K$ of n variables. Write $f = f(x_1, \ldots, x_n)$. We first prove the following general theorem.

Theorem 49. *A function $f : K^n \longrightarrow K$ is uniquely expressed in the form:*

$$f(x_1, \ldots, x_n) = \sum_{0 \leq i_1, \ldots, i_n < q} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}, \tag{131}$$

where the coefficients are elements of K.

Proof. By induction on the number of the variables n. First we approve the theorem for $n = 1$, this is shown later. Next assume the theorem for $n-1$. Let $f(x_1, \ldots, x_n)$ be a function. For every fixed value $(x_1, \ldots, x_{n-1})$, $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1})(x_n)$ is a function of a variable x_n, and by the hypothesis, we have

$$f(x_1, \ldots, x_{n-1})(x_n) = a_0 + a_1 x_n + a_2 x_n^2 + \cdots + a_{q-1} x_n^{q-1}, \tag{132}$$

where $a_0, \ldots, a_{q-1}$ depend on the value of $(x_1, \ldots, x_{n-1})$. Then we see that $(x_1, \ldots, x_{n-1}) \longrightarrow a_j$ defines a function $a_j(x_1, \ldots, x_{n-1})$, which is by the induction's hypothesis, expressed in the form (131). Therefore (132) is also expressed in the form (131).

Next we show the uniqueness of the expression (131). Suppose another expression:

$$f(x_1, \ldots, x_n) = \sum_{0 \leq i_1, \ldots, i_n < q} b_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}, \tag{133}$$

then by (131) and this, we have (132) and

$$f(x_1, \ldots, x_{n-1})(x_n) = b_0 + b_1 x_n + b_2 x_n^2 + \cdots + b_{q-1} x_n^{q-1}, \tag{134}$$

where a_i, b_i are polynomial in $\tilde{x} = (x_1, \ldots, x_{n-1})$. By the theorem for $n = 1$, for each fixed value of $\tilde{x}$, the right-hand side of (132) and (134) should coincide. Consequently, $a_i = b_i$ for all $\tilde{x}$, and then by induction's hypothesis, $a_i(x_1, \ldots, x_{n-1}) = b_i(x_1, \ldots, x_{n-1})$ as a polynomial.

Finally, we prove the theorem for $n = 1$. Let $\mathbb{F}_q = \{0, 1, \theta_2, \theta_3, \ldots, \theta_{q-1}\}$. For $f(x) = a_0 + a_1 x + \cdots + a_{q-1} x^{q-1}$, we have

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 1 \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{q-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \theta_{q-1} & \theta_{q-1}^2 & \ldots & \theta_{q-1}^{q-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix} = \begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(\theta_{q-1}) \end{pmatrix}. \tag{135}$$

Since the matrix on the left-hand side of (135) is nonsingular, the coefficients $a_0, a_1, \ldots, a_{q-1}$ are uniquely determined. (q.e.d.)

For practical use, we give a formula expressing the coefficients $a_{i_1 \ldots i_n}$ in (131). The key of a proof of the formula is the fact:

Theorem 50. *The summation*

$$\sum_{\theta \in \mathbb{F}_q^\times} \theta^d \tag{136}$$

vanishes for every nonzero integer d satisfying $-(q-2) \leq d \leq q-2$.

Proof. As we have seen in Section 5.1, the elementary symmetric function e_j of the nonzero elements of $\mathbb{F}_q$ of degree j, $1 \leq j \leq q-2$, vanishes. According to the elementary theorem of symmetric functions, every power sum p_d of degree d is expressed by a polynomial (without a constant term) in e_j's with $1 \leq j \leq d$, and therefore (136) vanishes for $1 \leq d \leq q-2$. For negative $-d \geq -(q-2)$, we see that

$$\sum_{\theta \in \mathbb{F}_q^\times} \theta^{-d} = \sum_{\theta \in \mathbb{F}_q^\times} \theta^d = 0. \qquad \text{(q.e.d.)} \tag{137}$$

By this theorem, we have the following general formula:

Theorem 51. *The coefficients in* (131) *is expressed by*

$$a_{i_1 \ldots i_n} = (-1)^{s+t} \sum_{\substack{x_{j_1}, \ldots, x_{j_s} \in \mathbb{F}_q^\times \\ x_{k_1}, \ldots, x_{k_t} \in \mathbb{F}_q}} \left[f(x_1, \ldots, x_n) x_{j_1}^{-i_{j_1}} \ldots x_{j_s}^{-i_{j_s}} \right]_{x_{l_1} = \cdots = x_{l_u} = 0}, \tag{138}$$

where

$$\begin{cases} 1 \leq i_{j_1}, \ldots, i_{j_s} \leq q-2 \\ i_{k_1} = \cdots = i_{k_t} = q-1 \\ i_{l_1} = \cdots = i_{l_u} = 0. \end{cases} \tag{139}$$

Proof. Let $g = f(x_1, \ldots, x_n) x_{j_1}^{-i_{j_1}} \ldots x_{j_s}^{-i_{j_s}}$. Since $1 \leq i_{j_1}, \ldots, i_{j_s} \leq q-2$, the degree d with respect to x_j of each term in g satisfies $-(q-2) \leq d \leq q-2$ for every $j = j_1, \ldots, j_s$. Thus by Theorem 50,

$$\sum_{x_j \in \mathbb{F}_q^\times} g = (q-1) \sum (\text{constant terms of } g \text{ concerning } x_j). \tag{140}$$

Therefore

$$\tilde{g} = \sum_{x_{j_1}, \ldots, x_{j_s} \in \mathbb{F}_q^\times} g = (q-1)^s \sum (\text{constant terms of } g \text{ concerning } x_{j_1}, \ldots, x_{j_s}). \tag{141}$$

Next if we put $x_l = 0$ in $\tilde{g}$ for all $l = l_1, \ldots, l_u$, then $\tilde{g}$ becomes $\tilde{g}_0$, and only constants with respect to $x_{l_1}, \ldots, x_{l_u}$ remain. Finally, we obtain

$$\sum_{x_{k_1}, \ldots, x_{k_t} \in \mathbb{F}_q} \tilde{g}_0 = (q-1)^t \sum (\text{coefficients of } x_{k_1}^{q-1} \ldots x_{k_t}^{q-1} \text{ of } \tilde{g}_0) = (q-1)^{s+t} a_{i_1 \ldots i_n}. \tag{142}$$

This proves (138). (q.e.d.)

Example 14. (1) Let $f(x,y)$ be a function $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ defined by the following table.

$$\begin{array}{c|cccc} x & 0 & 0 & 1 & 1 \\ y & 0 & 1 & 0 & 1 \\ f & 1 & 0 & 0 & 1 \end{array} \tag{143}$$

Let $f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{11}xy$. By Theorem 51, we have

$$\begin{array}{l} a_{00} = f(0,0) = 1 \\ a_{10} = (-1)\cdot[f(0,0) + f(1,0)] = 1 \\ a_{01} = (-1)\cdot[f(0,0) + f(0,1)] = 1 \\ a_{11} = (-1)^2\cdot[f(0,0) + f(1,0) + f(0,1) + f(1,1)] = 0. \end{array} \tag{144}$$

Hence $f(x,y) = 1 + x + y$.
(2) Let $m(x,y,z)$ be the majority function $\mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ of 3 variables, i.e., $m(x,y,z) = 1$ if and only if at least 2 of 3 variables have a value 1. That is,

$$\begin{array}{c|cccccccc} x & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ y & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ z & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ m & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \tag{145}$$

(exercise) Find a polynomial expression of $m(x,y,z)$.
(3) (exercise) Find a polynomial expression of the majority function $m(v,w,x,y,z)$ of 5 variables. Hint: It should be a symmetric function.

10.2 reduction of variables

As seen in Section 8.2, there exists a 1-1 correspondence between $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$, i.e., if we fix a root a of irreducible polynomial of degree n over $\mathbb{F}_q$, every element $(x_1,\ldots,x_n)$ in $\mathbb{F}_q^n$ corresponds to an element $x_1a^{n-1}+x_2a^{n-2}+\cdots+x_n$ in $\mathbb{F}_{q^n}$. Thus we can consider a function $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ of n variables as a function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ of one variable.

In Example 14 (2), the function $m : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ can be regarded as one from $\mathbb{F}_8$ to $\mathbb{F}_2$. Let a be a primitive element of $\mathbb{F}_8$ defined as a root of $x^3 + x + 1$. We give a 1-1 correspondence $\mathbb{F}_2^3 \longrightarrow \mathbb{F}_8$ by $(x,y,z) \longrightarrow xa^2 + ya + z$. Then the function m is rewritten as

$$\begin{array}{c|cccccccc} x & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 \\ \hline m & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \tag{146}$$

Let $m(x) = a_0 + a_1x + \cdots + a_7x^7$. According to Theorem 51, we have

$$\begin{array}{rl} a_0 = & m(0) = 0 \\ a_i = & (-1)\displaystyle\sum_{x\in\mathbb{F}_8^\times} x^{-i}m(x) \qquad (1 \le i \le 6) \\ a_7 = & (-1)\displaystyle\sum_{x\in\mathbb{F}_8} m(x) = 0. \end{array} \tag{147}$$

From this it follows that

$$m(x) = a^3x + a^6x^2 + a^6x^3 + a^5x^4 + a^3x^5 + a^5x^6. \quad \text{(exercise)} \tag{148}$$

This function consists of two $\mathbb{F}_2$-Frobenius cycles. That is,

$a^3x,$	$a^6x^2,$	a^5x^4
$a^6x^3,$	$a^5x^6,$	a^3x^5

(149)

It is not an accidental phenomenon. In general, we have the following.

Theorem 52. *Let $f(x_1, \ldots, x_n)$ be the polynomial expression of a function $\mathbb{F}_{q^s}^n \longrightarrow \mathbb{F}_q$ of n variables. Then the set of all terms of $f(x_1, \ldots, x_n)$ consists of several $\mathbb{F}_q$-Frobenius cycles.*

Proof. For each fixed $(x_1, \ldots, x_n)$, $f = f(x_1, \ldots, x_n)$ has a value in $\mathbb{F}_q$. Consequently, f is invariant by $\mathbb{F}_q$-Frobenius transformation τ, i.e.,

$$\tau f = f \tag{150}$$

for all $(x_1, \ldots, x_n)$. Hence by Theorem 49, both sides of (150) should coincide as a polynomial. The left-hand side is a polynomial obtained by shifting each term of f along a Frobenius cycle. This assures the contents of the theorem. (q.e.d.)

10.3 vector valued functions

An m-tuple of functions are considered as a correspondence $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$, called a vector valued function. As already done in the previous section, we can give 1-1 correspondences between $\mathbb{F}_q^n$ and $L = \mathbb{F}_{q^n}$, and also $\mathbb{F}_q^m$ and $M = \mathbb{F}_{q^m}$. Therefore we can reduce f to a function of one variable: $f : L \longrightarrow M$. To express it in a polynomial form, we should extend the working field to $N = \mathbb{F}_{q^s}$, where $s = \mathrm{lcm}\,(n, m)$, so that N includes both of L and M. The target polynomial $f(x)$ is, however, defined only on the domain L and therefore we do not have to treat the case that the variable x is not contained in L. The summation ranges of the formulas in Theorems 49 and 51 depend on the field of the domain but not on the codomain. Therefore we can write $f(x)$ as a polynomial of degree $\leq q^n - 1$, i.e.,

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{q^n-1}x^{q^n-1}, \tag{151}$$

where the coefficients are contained in N.

For example, consider the correspondence $f = (f_1, f_2) : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^2$:

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
f_1	0	1	1	0	1	0	0	1
f_2	1	1	0	1	0	0	0	1

(152)

Let a, b and c be primitive elements of $\mathbb{F}_8$, $\mathbb{F}_4$ and $\mathbb{F}_{64}$, defined by $a^3 = a^2+1$, $b^2 = b+1$, and $c^6 = c + 1$, respectively. We now give correspondences $\mathbb{F}_2^3 \longrightarrow \mathbb{F}_8$ and $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_4$

in the similar manner as in the previous section. Then we reduce f to the function $f : \mathbb{F}_8 \longrightarrow \mathbb{F}_4$ below.

(153)

x	0	1	a	a^2	a^3	a^4	a^5	a^6
f	1	b^2	b	b	0	b^2	1	0

Let $f(x) = a_0 + a_1x + \cdots + a_7x^7$. By using Theorem 51, we have

$$\begin{aligned} a_0 = &\quad m(0) = 1 \\ a_i = &\quad (-1)\sum_{x\in\mathbb{F}_8^\times} x^{-i}f(x) \qquad (1 \le i \le 6) \\ a_7 = &\quad (-1)\sum_{x\in\mathbb{F}_8} f(x) = 1 + b^2 + b + b + b^2 + 1 = 0. \end{aligned} \tag{154}$$

More concretely, for $1 \le i \le 6$,

$$a_i = b^2 + a^{6i}b + a^{5i}b + a^{3i}b^2 + a^{2i}. \tag{155}$$

Noting the relations $a = c^9$ and $b = c^{21}$ (exercise), we obtain

$$\begin{aligned} f(x) = &\quad 1 + c^{21}x + c^{21}x^2 + c^{45}x^3 + c^{21}x^4 + c^{54}x^5 + c^{27}x^6 \\ = &\quad 1 + bx + bx^2 + a^5x^3 + bx^4 + a^6x^5 + a^3x^6. \quad \text{(last exercise)} \end{aligned} \tag{156}$$

This function consists of three $\mathbb{F}_4$-Frobenius cycles, i.e.,

(157)

1		
bx,	bx^4,	bx^2
a^5x^3,	a^6x^5,	a^3x^6

Thanks for Your Collaboration

'02/12/xx,'07/09/18,'08/10/30,'09/12/10,'10/12/16,'12/11/19,'13/12/12,'15/12/3,'19/10/18:, '20/10/26,'22/11/4,'23/11/29.

Center for Mathematical Sciences, University of Aizu, Aizu-Wakamatsu, Fukushima 965-8580, Japan

Email address: k-asai@u-aizu.ac.jp