

Chapter 2. Finite Fields (Chapter 3 in the text)



1. Group Structures
2. Constructions of Finite Fields $\text{GF}(2^n)$ and $\text{GF}(p^n)$
3. Basic Theory of Finite Fields
4. The Minimal Polynomials
5. Trace Functions
6. Subfields

1. Group Structures

- Groups and Cyclic Groups
- Rings and Fields

Definition 1 A group is a set G together with a binary operation $*$ on G such that the following three properties hold:

(i) $*$ is *associative*; that is,
for any $a, b, c \in G$, $a*(b*c)=(a*b)*c$.

(ii) There is an *identity* or (*unity*) element e in G such that for all $a \in G$,
$$a*e = e*a = a.$$

(iii) For each $a \in G$, there exists an *inverse element* $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e .$$

Sometimes, we denote the group as a triple $(G, *, e)$. If the group also satisfies

(iv) For all $a, b \in G$,
$$a*b = b*a,$$
then the group is called *abelian* or *commutative*.

Example 1 Let

- Z , the set consisting of all integers
 - Q , the set of all rational numbers
- + and \times are ordinary addition and multiplication.

Then $(Z, +, 0)$ $(Q, +, 0)$ $(Q^*, \times, 1)$

are all groups where Q^* is the all nonzero rational numbers.

Furthermore, they are abelian.

How about $(Z^*, \times, 1)$?

One of the most important structures in crypto: Residues modulo n .

Let n be a positive integer ($n > 1$) and Z_n represent the set of remainder of all integers on division n , i.e.,

$$Z_n = \{0, 1, 2, \dots, n-1\}.$$

We define $a + b$ and ab the ordinary sum and product of a and b reduced by modulo n , respectively.

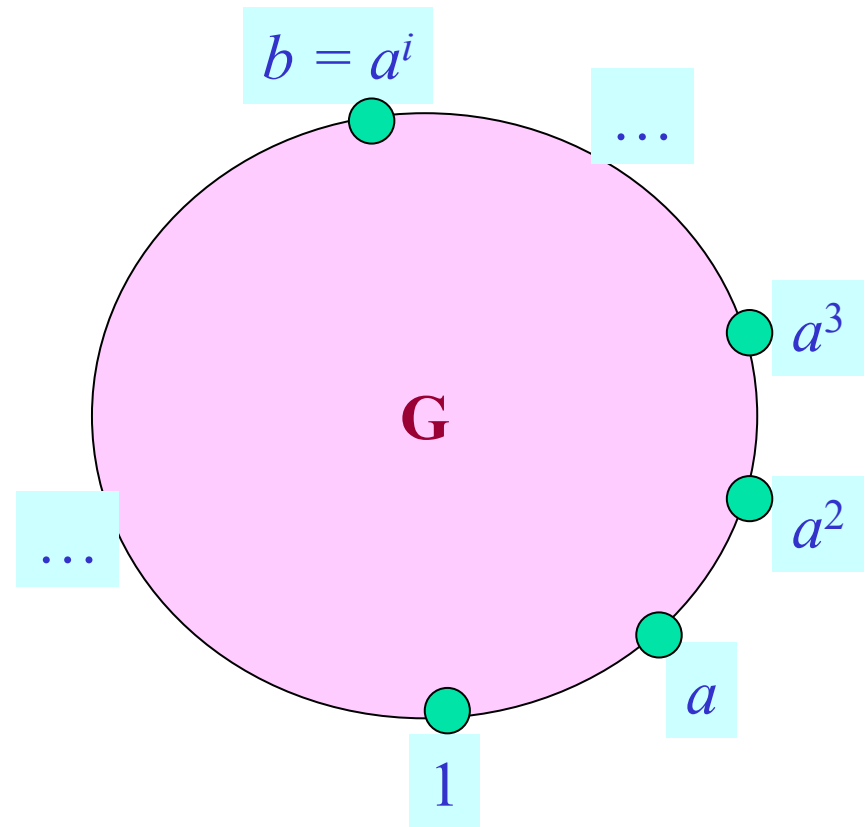
Let

$$Z_n^* = \{a \in Z_n \mid a \neq 0\}.$$

Proposition 1

- (a) $(Z_n, +, 0)$ forms a group,
- (b) $(Z_p^*, \times, 1)$ forms a group for any prime p .

Definition 2 A multiplicative group G is said to be *cyclic* if there is an element $a \in G$ such that for any $b \in G$ there is some integer i with $b = a^i$. Such an element a is called a *generator* of the cyclic group, and we write $G = \langle a \rangle$.



Examples

- $(\mathbb{Z}_6, +, 0)$, cyclic group with generators 1 and 5.

- $(\mathbb{Z}_3^*, \times, 1)$, cyclic group with generator 2.

$$\mathbb{Z}_3^* = \{1, 2\} = \langle 2 \rangle = \{2^0 = 1, 2\}, 2^2 = 1 \pmod{3}.$$

- $(\mathbb{Z}_7^*, \times, 1)$, cyclic group, 3 is a generator:

$$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1 \pmod{7}$$

However, $2^3 = 1 \pmod{7}$. Thus 2 is not a generator of \mathbb{Z}_7^* .

- $(\mathbb{Z}_5^*, \times, 1)$, cyclic group, 2 is a generator.

$$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1 \pmod{5}, \text{ thus } \mathbb{Z}_5^* = \langle 2 \rangle.$$

i.e., every element in \mathbb{Z}_5^* can be written into a power of 2.

Finite Group

Definition 3 A group is called finite if it contains finite many elements. The number of elements in G is called the order of G , denoted as $|G|$.

Rings and Fields

E.g.

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$ are rings.
- $(\mathbb{Z}_n, +, \times)$ forms a ring, called the residue class ring modulo n .
- $(\mathbb{Z}_4, +, \times)$ is a ring.

Definition 4 A *ring* $(R, +, \times)$ is a set R , together with two binary operations, denoted by $+$ and \times , such that:

(i) R is an abelian group with respect to $+$.

(ii) \times is *associative*, that is,

$$(a \times b) \times c = a \times (b \times c) \text{ for all } a, b, c \in R.$$

(iii) The *distributive* laws hold; that is, for all $a, b, c \in R$, we have

$$a \times (b + c) = a \times b + a \times c \text{ and}$$

$$(b + c) \times a = b \times a + c \times a.$$

Let $(F, +, \times)$ be a ring, and let
 $F^* = \{a \in F \mid a \neq 0\}$,
the set of elements of F that are
non zero.

Definition 5 A *field* is a ring
 $(F, +, \times)$ such that F^* together
the multiplication \times forms a
commutative group.

Definition 6 A *finite field* is a field
that contains a finite number of
elements, this number is called the
order of the field.
Finite fields are called *Galois fields*
after their discoverer.

$(\mathbb{Z}_2, +, \times)$ forms a finite field

+	0	1
0	0	1
1	1	0

\times	0	1
0	0	0
1	0	1

E. g.

- $(\mathbb{Q}, +, \times)$,
- $(\mathbb{R}, +, \times)$ and
- $(\mathbb{C}, +, \times)$ are fields

where \mathbb{R} is the set of all real numbers,
and \mathbb{C} , the set of all complex numbers.



Proposition 2 Let p be a prime, then
 $(\mathbb{Z}_p, +, \times)$ is a finite field with order p .
This field is denoted as $\text{GF}(p)$.

2 Constructions of Finite Fields $GF(2^n)$ and $GF(p^n)$



Step 1 Select n , a positive integer and p a prime.

Step 2 Choose that $f(x)$ is an irreducible polynomial over $GF(p)$ of degree n .

Step 3 We agree that α is an element that satisfies $f(\alpha) = 0$.
Let

For two elements $g(\alpha), h(\alpha)$ in $GF(p^n)$, we write

$$g(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \text{ and} \\ h(\alpha) = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}.$$

Addition:

$$g(\alpha) + h(\alpha) \\ = (a_0 + b_0) + (a_1 + b_1)\alpha + \dots + (a_{n-1} + b_{n-1})\alpha^{n-1}$$

Multiplication:

$$g(\alpha)h(\alpha) = r(\alpha)$$

where $r(x)$ is the remainder of $g(x)h(x)$ divided by $f(x)$.

$$GF(p^n) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in GF(p)\}$$

Example 7. Let $p = 2$ and $f(x) = x^3 + x + 1$. Then $f(x)$ is irreducible over $\text{GF}(2)$. Let α be a root of $f(x)$, i.e., $f(\alpha) = 0$. The finite field $\text{GF}(2^3)$ is defined by

$$\text{GF}(2^3) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a^i \in \text{GF}(2)\}.$$

Table 1. $\text{GF}(2^3)$, defined by $f(x) = x^3 + x + 1$ and $f(\alpha) = 0$.

As a 3-tuple	As a polynomial	As a power of α
000 =	0	= 0
001 =	1	= 1
010 =	α	= α
100 =	α^2	= α^2
011 =	$1 + \alpha$	= α^3
110 =	$\alpha + \alpha^2$	= α^4
111 =	$1 + \alpha + \alpha^2$	= α^5
101 =	$1 + \alpha^2$	= α^6
$\alpha^7 = 1$		

Computation in GF(2³):

We take $g(\alpha) = 1 + \alpha$ and $h(\alpha) = \alpha + \alpha^2$.

Addition:

$$\begin{aligned}g(\alpha) + h(\alpha) &= (1 + \alpha) + (\alpha + \alpha^2) \\ &= 1 + \alpha^2 \in \text{GF}(2^3)\end{aligned}$$

Multiplication:

$$\begin{aligned}g(\alpha)h(\alpha) &= (1 + \alpha)(\alpha + \alpha^2) \\ &= \alpha + \alpha^2 + \alpha^2 + \alpha^3 \\ &= \alpha + 2\alpha + \alpha^3 \\ &= \alpha + \alpha^3 = 1 \\ &\text{(since } \alpha^3 + \alpha + 1 = 0 \text{).}\end{aligned}$$

On the other hand,

$$g(\alpha) = 1 + \alpha = \alpha^3 \text{ and}$$

$$h(\alpha) = \alpha + \alpha^2 = \alpha^4$$

We may compute the product of $g(\alpha)$ and $h(\alpha)$ as follows

$$g(\alpha)h(\alpha) = \alpha^3 \alpha^4 = \alpha^7 = 1$$

3 Basic Theory of Finite Fields

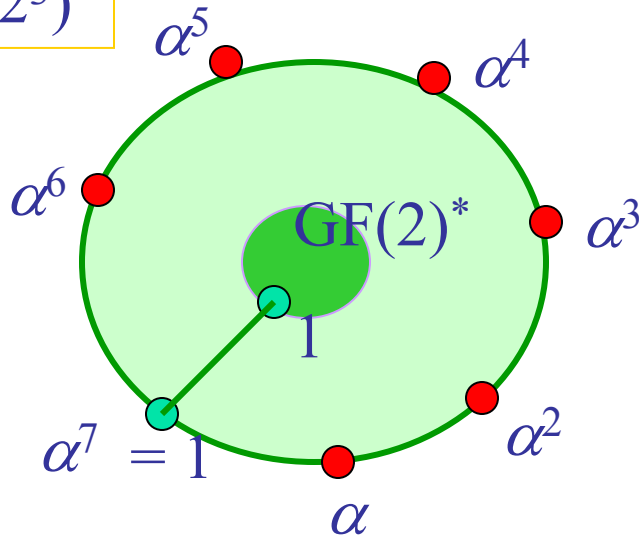


A. Primitive Elements and Primitive Polynomials

Fact 1 For any finite field F , its multiplicative group F^* , the set of non zero element of F , is cyclic.

Definition. A generator of the cyclic group $GF(p^n)^*$ is called a primitive element of $GF(p^n)$. A polynomial having a primitive element as zero is called a primitive polynomial.

$GF(2^3)^*$



E.g Since $\alpha^3 + \alpha + 1 = 0$, then $x^3 + x + 1$ is a primitive polynomial over $GF(2)$.

- $x^4 + x + 1$ is a primitive polynomial over $GF(2)$.

How about $f(x) = x^4 + x^3 + x^2 + x + 1$? Is it primitive?

$f(x)$ is irreducible over $GF(2)$. So we can use $f(x)$ to define $GF(2^4)$. Let α be a root of $f(x)$.

$$\alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$$

$$\alpha^5 = \alpha(1 + \alpha + \alpha^2 + \alpha^3)$$

$$= \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1$$

Thus, α is not a primitive element of $GF(2^4)$, so $f(x)$ is not primitive.

Remark. The tables of primitive polynomials over $GF(2)$ of degree ≤ 229 can be found at Alfred J. Menezes, Paul C. Van Vorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp161.

B. Structure of $GF(p^n)$

Let $GF(p^n)$ be defined by $f(\alpha) = 0$ where $f(x)$ is primitive, then the elements in the field have the following two representations.

$$GF(p^n) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in GF(p)\} \quad (\text{vector representation})$$

$$= \{\alpha^i \mid 0 \leq i < p^n - 1, i = \infty\} \quad (\text{exponential representation})$$

(we define $0 = \alpha^\infty$)

Remark. Vector representation is efficient for computation of addition and the exponential representation is efficient for computation of multiplication.

For small field, for example, $p = 2$ and $n < 40$, it is much more efficient than to use the exponential representation for computation of multiplication and the vector representation for that of addition where it stores the add 1 table for conversion from the vector representation to the exponential representation.

Discrete Logarithm in $GF(p^n)$



Let α be a primitive element in $GF(p^n)$ and β , an arbitrary nonzero element in $GF(p^n)$. Find k such that

$$\beta = \alpha^k$$

is called a discrete logarithm of β under the base α .

Zech's logarithm: For any $0 < k < p^n - 1$, find k' such that

$$\alpha^{k'} = \alpha^k + 1$$

4 Minimal Polynomials

Definition. Let $\alpha \in GF(p^n)$ and $m(x)$ be a monic polynomial over $GF(p)$,

$$m(x) = \sum_{i=0}^{r-1} c_i x^i + x^r, \quad c_i \in GF(p)$$

$m(x)$ is called a minimal polynomial (MP) of α if $m(x)$ is the polynomial with the lowest degree such that $m(\alpha) = 0$.

Properties of Minimal Polynomials

Suppose that $m(x)$ is the MP of $\alpha \in \text{GF}(p^n)$, then

(1) $m(x)$ is irreducible over $\text{GF}(p)$.

(2) $m(x) \mid x^{p^n} - x$

(3) the degree of $m(x)$ is a factor of n , i.e. $\deg m(x) \mid n$.

(4) the minimal polynomial of a primitive element of $\text{GF}(p^n)$ has degree n .

Algorithm for Finding Minimal Polynomial

Input:

- $f(x)$, a primitive polynomial over $GF(p)$ of degree n ;
- α , a root of $f(x)$;
- $\beta = \alpha^k$ an element in $GF(p^n)$.

Output: The minimal polynomial of β over $GF(p)$.

Procedure $MP(\beta)$

Step 1. Generate the finite field $GF(p^n)$ by $f(x)$

Step 2. Compute s such that s is the smallest number satisfying

$$k \equiv p^s k \pmod{p^n - 1}.$$

Step 3. Compute

$$m_\beta(x) = (x - \beta)(x - \beta^p) \cdots (x - \beta^{p^{s-1}}) \text{ in } GF(p^n).$$

Return $m_\beta(x)$

Example 8. For $\text{GF}(2^4)$, defined by $\alpha^4 + \alpha + 1 = 0$, compute the minimal polynomial of α^7 .

Solution. Applying *procedure_MP*(β), here we have $\beta = \alpha^7$ where $k = 7$. Compute s such that s is the smallest integer satisfying $7 \equiv 2^s \times 7 \pmod{15}$ (trial and error method), we have $s = 4$.

$$\begin{aligned}
 m_{\alpha^7}(x) &= (x - \alpha^7)(x - \alpha^{2 \cdot 7})(x - \alpha^{2^2 \cdot 7})(x - \alpha^{2^3 \cdot 7}) \\
 &= (x + \alpha^7)(x + \alpha^{14})(x + \alpha^{13})(x + \alpha^{11}) \\
 &= [x^2 + (\alpha^{14} + \alpha^7)x + \alpha^6][x^2 + (\alpha^{11} + \alpha^{13})x + \alpha^9] \\
 &= (x^2 + \alpha x + \alpha^6)(x^2 + \alpha^4 x + \alpha^9) \\
 &= x^4 + (\alpha^4 + \alpha)x^3 + (\alpha^9 + \alpha^5 + \alpha^6)x^2 + (\alpha^{10} + \alpha^{10})x + 1 \\
 &= x^4 + x^3 + (\alpha^9 + \alpha^5 + \alpha^6)x^2 + 1 \\
 &= x^4 + x^3 + 1
 \end{aligned}$$

Thus, $m_{\alpha^7}(x) = x^4 + x^3 + 1.$

5 Trace Functions

Definition. A trace function $Tr(x)$ of $GF(p^n)/GF(p)$ is a function from $GF(p^n)$ to $GF(p)$ defined as follows

$$Tr(x) = x + x^p + \cdots + x^{p^{n-1}}$$

$$Tr(x) : GF(p^n) \rightarrow GF(p)$$

Property 1.

(a) The trace function is a linear function.

(b) $(x + y)^p = x^p + y^p, \forall x, y \in GF(p^n)$.

Example 9. Let $GF(2^3)$ be defined by

$$\alpha^3 + \alpha + 1 = 0.$$

Compute $Tr(\alpha)$ and $Tr(\alpha^3)$.

Solution.

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^4$$

$$= \alpha + \alpha^2 + \alpha + \alpha^2 = 0$$

$$Tr(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^5$$

$$= (1 + \alpha) + (1 + \alpha^2) + (1 + \alpha + \alpha^2)$$

$$= 1$$

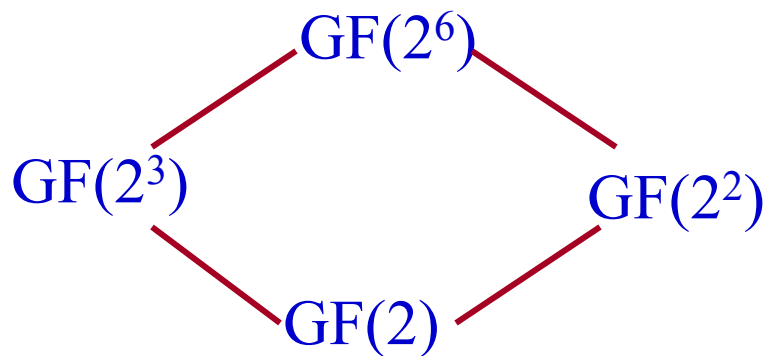
6. Subfields

A subfield of $GF(p^N)$ is a subset of $GF(p^N)$ which itself forms a field.

E is a subfield of $GF(p^N)$ if and only if
$$E = GF(p^m)$$
where $m \mid N$ (m is a factor of N), i.e.,
$$GF(p^m) \subset GF(p^N).$$

E.g. $GF(2^2) \subset GF(2^4)$

$GF(2^4) \subset GF(2^{12})$



We write $N = mn$ and denote the trace function from $GF(p^N)$ to $GF(p^m)$ as

$Tr_m^N(x)$, i.e.,

$Tr_m^N(x) = x + x^q + \cdots + x^{q^{m-1}}$, where $q = p^m$.

Property 2. (Transitivity)

For a field chain

$$GF(p) \subset GF(p^n) \subset GF(p^{mn})$$

we have

$$Tr_1^{mn}(x) = Tr_1^n(Tr_n^{mn}(x))$$

This is the underline structure of GMW sequences.

