Chapter 1

Finite Fields

This chapter aims at giving the main definitions and properties of finite fields which will be needed in the rest of the document. Much more details can be found in [McE87] and [LN83].

1.1 Definitions

Definition 1.1 (Field)**.** *A* field *is a set* $\mathbb{F}$ *with two operations* $+$ *and* $\times$ *satisfying the following properties:*

- $\mathbb{F}$ *is an Abelian group under* $+$ *with identity element* 0*;*
- *The nonzero elements of* $\mathbb{F}$ *form an Abelian group under* $\times$*, with identity element* 1*;*
- $\times$ *distributes over* $+$*, i.e.,* $a \times (b + c) = a \times b + a \times c$ *for any* $a, b, c \in \mathbb{F}$*.*

The number of elements in a field $\mathbb{F}$ is called the *order* of $\mathbb{F}$. The field is *finite* if it has a finite number of elements. Infinite fields include the real numbers, the rational numbers or the complex numbers. For any prime number p, the set of integers modulo p, $\mathbb{Z}/p\mathbb{Z}$ is a finite field.

Definition 1.2 (Characteristic)**.** *Let* $\mathbb{F}$ *be a multiplicative field. The characteristic of* $\mathbb{F}$ *is, if it exists, the smallest nonzero integer* c *such that*

$$\underbrace{1 + 1 + \cdots + 1}_{c \text{ times}} = 0 \; .$$

If there is no such integer, the characteristic is zero.

Clearly, a finite field $\mathbb{F}$ with q elements involves two groups: the additive group $\mathbb{F}$ of order q and the multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ of order $(q-1)$. The following notions are important when the multiplicative subgroup is considered.

Definition 1.3 (Order of an element in a group)**.** *Let* G *be a finite Abelian multiplicative group. For any fixed* $a \in G$*, the* subgroup generated by a*, denoted by* $\langle a \rangle$ *consists of all powers of* a*. Its order is called the order of* a*, i.e.,*

$$\mathsf{order}(a) = |\langle a \rangle| = \min\{i > 0 : a^i = 1\} \; .$$

Proposition 1.4. *Let G be a finite Abelian multiplicative group. For any $a \in G$, the order of a divides the order of G. In particular, $a^{|G|} = 1$.*

Proof. Let a be a fixed element in G. We define the following relation on G:

$$b\mathcal{R}c \Leftrightarrow \exists i : a^i \times b = c \; .$$

This is clearly an equivalence relation since it is reflexive, symmetric and transitive. All equivalence classes have size $\mathsf{order}(a)$ and they form a partition of G. This implies that $\mathsf{order}(a)$ divides the size of G. ◇

As a direct corollary, we get that the order of any nonzero element in a field with q elements divides $(q-1)$, leading to the following analogous of Fermat's little theorem.

Corollary 1.5. *Any element x in a finite field of order q satisfies $x^q = x$.*

1.2 Existence and uniqueness of finite fields

Now, we prove that the number of elements in a finite field must be a power of prime. Indeed, any finite field can be defined as a finite dimensional vector space over the field of integers modulo p, for some prime p.

Theorem 1.6. *Let $\mathbb{F}$ be a finite field with q elements. Then, $q = p^m$ for some prime p.*
Indeed, the following properties hold:

- *$\mathbb{F}$ has characteristic p;*
- *$\mathbb{F}$ is a vector space over $\mathbb{F}_p$ of dimension m.*

Proof. Let γ_i denote the sum of i 1s:

$$\gamma_i = \underbrace{1 + \cdots + 1}_{i \text{ times}}$$

All γ_i belong to $\mathbb{F}_q$ and since $\mathbb{F}_q$ is finite, there exist i and j, $i < j$ such that $\gamma_i = \gamma_j$, implying that $\gamma_{j-i} = 0$. It follows that the characteristic of $\mathbb{F}_q$ is a nonzero integer c.

Suppose that c is not a prime, i.e., $c = ab$. Since multiplication distributes over addition

$$\gamma_a \times \gamma_b = \gamma_c = 0 \; .$$

Because $\mathbb{F}$ is a field, either γ_a or γ_b is zero, which contradicts the fact that $\mathbb{F}$ has characteristic c. Then, the characteristic of $\mathbb{F}$ is a prime p.

Moreover, $\mathbb{F}$ contains the set $\{0, 1, \gamma_2, \ldots, \gamma_{p-1}\}$ which corresponds to the field of integers modulo p, $\mathbb{F}_p$. Now, we can show that $(\mathbb{F}, +)$ is a vector space over $\mathbb{F}_p$ where the scalar multiplication $\cdot$ is defined by:

$$\forall \lambda \in \mathbb{F}_p, \forall x \in \mathbb{F}_q, \; \lambda \cdot x = \underbrace{x + \cdots + x}_{\lambda \text{ times}} \; .$$

Indeed, $\lambda \cdot x = x \times \gamma_\lambda$. Using that $\gamma_\lambda \times \gamma_\mu = \gamma_{\lambda\times\mu}$ and$\gamma_\lambda + \gamma_\mu = \gamma_{\lambda+\mu}$, we can check that

$$\begin{aligned}(\lambda+\mu)\cdot x &= x \times \gamma_{\lambda+\mu} = x \times (\gamma_\lambda + \gamma_\mu) = \lambda \cdot x + \mu \cdot x\\ (\lambda \times \mu)\cdot x &= x \times \gamma_{\lambda\times\mu} = x \times (\gamma_\lambda \times \gamma_\mu) = \lambda \cdot (\mu \times x)\\ \lambda \cdot (x+y) &= (x+y) \times \gamma_\lambda = x \times \gamma_\lambda + y \times \gamma_\lambda = \lambda \cdot x + \lambda \cdot y\\ 1 \cdot x &= x \times 1 = x\ .\end{aligned}$$

It follows that $\mathbb{F}$ is a vector space over $\mathbb{F}_p$, implying that its size q is equal to p^m for some $m > 0$. ◇

A common terminology is that a field with p^m elements is an *extension field* of $\mathbb{F}_p$ of degree m. Similarly, the field of complex numbers is an extension field of $\mathbb{R}$ of degree 2.

Using that the characteristic of a finite field is a prime, we deduce the following useful proposition.

Proposition 1.7. *Let $\mathbb{F}$ be a field of characteristic p. Then, for any $a, b \in \mathbb{F}$ and any integer $i > 0$, we have*

$$(a+b)^{p^i} = a^{p^i} + b^{p^i} \text{ and } (a-b)^{p^i} = a^{p^i} - b^{p^i}\ .$$

Proof. The second formula is a direct consequence of the first one by using that

$$a^{p^i} = ((a-b)+b)^{p^i} = (a-b)^{p^i} + b^{p^i}\ .$$

The first formula is proved by induction on i. For $i = 1$, we write

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

where the second equality comes from the fact that, for $1 \le i \le p-1$,

$$\binom{p}{i} = \frac{(p-i+1)\ldots(p-1)p}{i!} \equiv 0 \bmod p\ .$$

Indeed, p is a prime (from Theorem 1.6) and divides the numerator, while it cannot divide the denominator which is composed of integers smaller than p.

Then, the induction step consists in observing that

$$(a+b)^{p^i} = ((a+b)^p)^{p^{i-1}} = (a^p + b^p)^{p^{i-1}} = a^{p^i} + b^{p^i}\ .$$

◇

Now, it can be proved that, for any $q = p^m$ where p is a prime, there exists a finite field with q elements. Moreover, this field is unique up to isomorphism. This motivates the following notation: $\mathbb{F}_q$ denotes the field with q elements. Another common notation is $GF(q)$, which stands for Galois field.

The next theorem uses the notion of *splitting field* of a univariate polynomial: for a given field $\mathbb{F}$, we consider a polynomial $P \in \mathbb{F}[X]$, i.e., a polynomial in X with coefficients in $\mathbb{F}$. The splitting field of P over $\mathbb{F}$ is then the smallest field which contains all roots of P. Such a field exists, is an extension of $\mathbb{F}$ and is unique up to an isomorphism which keeps the elements of $\mathbb{F}$ fixed [LN83, Theorem 1.91]. For instance, the splitting field of $X^2 + 1$ over $\mathbb{R}$ is the field of complex numbers.

Theorem 1.8. *For any prime p and any nonzero integer m, there exists a finite field of order p^m. Any finite field of order p^m is isomorphic to the splitting field of the polynomial $X^{p^m} - X$ over $\mathbb{F}_p$.*

Proof.

- *Existence:* We want to show that the splitting field $\mathbb{F}$ of $P(X) = X^{p^m} - X$ over $\mathbb{F}_p$ is a field with p^m elements. First, all roots of P are distinct. Indeed, a is a multiple root of a polynomial P if and only if it is a root of P and of its derivative P'. This comes from the fact that, for $P(X) = (X-a)^k Q(X)$ with $k > 0$, $P'(X) = k(X-a)^{k-1}Q(X) + (X-a)^k Q'(X)$. For $P(X) = X^{p^m} - X$, we get $P'(X) = -1$ over $\mathbb{F}_p$, implying that P has no multiple root. Now, the set $\mathcal{S}$ of all roots of P, i.e., of all a such that $a^{p^m} = a$, is a subfield of $\mathbb{F}$ since it satisfies the following three conditions:
  - $\mathcal{S}$ contains 0 and 1 since $P(0) = P(1) = 0$.
  - For any $a, b \in \mathcal{S}$, $(a-b)$ belongs to $\mathcal{S}$: indeed, from Proposition 1.7
$$(a-b)^{p^m} = a^{p^m} - b^{p^m} = a - b\ .$$
  - For any nonzero $a, b \in \mathcal{S}$, $(a \times b^{-1})$ belongs to $\mathcal{S}$: we use that
$$(a \times b^{-1})^{p^m} = a^{p^m} \times (b^{p^m})^{-1} = a \times b^{-1}\ .$$

  Then, by definition of the splitting field, $\mathcal{S} = \mathbb{F}$ and it has cardinality q^m.

- *Uniqueness:* Let $\mathbb{F}$ be a field of order p^m. Then, from Theorem 1.6, $\mathbb{F}$ has characteristic p. It follows from Proposition 1.4 that the order of any nonzero element in the multiplicative group $\mathbb{F}^*$ divides $(p^m - 1)$. Thus, any nonzero element $a \in \mathbb{F}$ satisfies $a^{p^m-1} = 1$, implying that any $a \in \mathbb{F}$ satisfies $P(a) = a^{p^m} - a = 0$. In other words, any element in $\mathbb{F}$ is a root of P. Since P has exactly p^m roots, $\mathbb{F}$ is the splitting field of P over $\mathbb{F}_p$, which is unique up to an isomorphism which keeps the elements of $\mathbb{F}$ fixed.

◇

As a direct corollary, we get a necessary and sufficient condition for belonging to a field with q elements.

Corollary 1.9. *An element x belongs to a field with q elements, $q = p^m$ for some prime p, if and only if $x^q = x$.*

1.3 Multiplicative group of a finite field

Since $\mathbb{F}_q$ with $q = p^m$ is a vector space over $\mathbb{F}_p$, every element in $\mathbb{F}_q$ can be represented as an m-tuple of integers modulo p. Adding two elements then consists in adding the two tuples coordinate-wise. But, this representation is not appropriate for multiplying elements. Instead, efficient multiplication exploits the structure of the multiplicative group $(\mathbb{F}_q^*, \times)$.

Definition 1.10. *Let G be a finite Abelian multiplicative group. An element a in G is called a* generator of G *if its order is equal to the size of G. The group G is said to be* cyclic *if it contains a generator, i.e., if there exists g such that*

$$G = \langle g \rangle = \{g^i, 0 \leq i < |G|\} .$$

The number of generators in a cyclic group is determined by the Euler ϕ-function.

Proposition 1.11. *The Euler ϕ-function is defined over the set of integers by*

$$\phi(n) = |\{i, 1 \leq i \leq n : \gcd(i, n) = 1\}| .$$

Then, the number of generators in any finite cyclic group of order n is equal to $\phi(n)$.

Proof. Let G be a cyclic group of order n and g be a generator of G, i.e.,

$$G = \{g^i, 0 \leq i < n\} .$$

Then, the number of generators of G is the number of integers i such that $\mathsf{order}(g^i) = n$, i.e., n is the smallest integer r such that $g^{ir} = 1$. Since g is a generator, $g^{ir} = 1$ if and only if n divides ir. Then, there is no $r < n$ such that $n|ir$ if and only if i is coprime with n. ◇

It is well-known that the Euler ϕ-function satisfies the following property (see e.g. [McE87, Page 35] for a proof):

$$\sum_{d|n} \phi(d) = n .$$

By inverting this formula (see [McE87, Pages 60-65]), we get

- If p is a prime, then $\phi(p) = p - 1$;
- If $\gcd(n, m) = 1$, then $\phi(nm) = \phi(n)\phi(m)$;
- If $n = \prod_i p_i^{m_i}$, then $\phi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$;

We know that, if r does not divide $(q-1)$, there is no element of order r in $\mathbb{F}_q^*$. Using the Euler ϕ-function, we can now determine the number of elements of order r when r divides $(q-1)$.

Theorem 1.12. *For any integer r such that $r|(q-1)$, the number of elements of order r in the multiplicative group $\mathbb{F}_q^*$ is equal to $\phi(r)$ and $\mathbb{F}_q^*$ has a unique subgroup of order r.*

Proof. By definition, the elements of order r in $\mathbb{F}_q^*$ correspond to the roots of $X^r - 1$ in $\mathbb{F}_q^*$. Let $a \in \mathbb{F}_q^*$ be an element of order r. Then, the cyclic group generated by a corresponds to the set of all roots of $X^r - 1$. Indeed, any element in $\langle a \rangle$ is a root of $X^r - 1$, and $\langle a \rangle$ has order r while $X^r - 1$ has at most r roots. Therefore, the elements of order r in $\mathbb{F}_q^*$ correspond to the multiplicative subgroup $\langle a \rangle$. Moreover, we know from Proposition 1.11 that $\langle a \rangle$ contains $\phi(r)$ elements of order r, implying that, if there exists an element of order r in $\mathbb{F}_q^*$, then there are exactly $\phi(r)$ such elements. Using that the order of an element divides $(q-1)$ (Proposition 1.4) and that $\sum_{r|(q-1)} \phi(r) = q - 1$, we get that there exist $\phi(r)$ elements of order r for any $r|(q-1)$. ◇

An immediate consequence of the previous theorem is that the number of generators of the multiplicative group $\mathbb{F}_q^*$ is $\phi(q-1)$ which is nonzero.

Corollary 1.13. *The multiplicative group $\mathbb{F}_q^*$ is a cyclic group of order $(q-1)$. Each generator of $\mathbb{F}_q^*$ is called a* primitive element *of $\mathbb{F}_q$.*

1.4 Constructing finite fields

We now need to link the additive structure of a finite field coming from the vector space interpretation and the multiplicative structure coming from the representation of all nonzero elements by the powers of a primitive element.

Theorem 1.14. *Let p be a prime and P be an irreducible polynomial of degree m with coefficients in $\mathbb{F}_p$. Then, the set of all residue classes modulo P is a field with p^m elements.*

Proof. We consider the set $\mathbb{F}$ of all polynomials in $\mathbb{F}_p[X]$ with degree at most $(m-1)$, since it is a set of representatives of the residue classes modulo P. It is clear that this set $\mathbb{F}$ is an Abelian group under addition modulo P in $\mathbb{F}_p[X]$ with identity element 0. If $\times$ denotes the multiplication modulo P in $\mathbb{F}_p[X]$, we get that the product of two elements in $\mathbb{F}$ lie in $\mathbb{F}$. Also, $\times$ is commutative and distributes over addition. Therefore, we only have to prove that, for any element A in $\mathbb{F}$ there exists a $B \in \mathbb{F}$ such that $A \times B = 1$. By definition of the multiplicative law, this means that the two polynomials satisfy

$$A(X)B(X) \equiv 1 \bmod P(X) \ .$$

This can be directly deduced from the Bezout's identity: since P is irreducible, then any polynomial A with degree at most $(m-1)$ is coprime with P implying that there exist two polynomials U and V in $\mathbb{F}_p[X]$ such that

$$A(X)U(X) + P(X)V(X) = 1 \ .$$

Thus, we get that $B(X) = U(X) \bmod P(X)$ is the multiplicative inverse of A. ◇

The field with p^m elements can then be constructed from any irreducible polynomial of degree m.

Example 1.1. Constructing $\mathbb{F}_8$. The polynomial $P(X) = X^3 + X + 1$ is irreducible over $\mathbb{F}_2$, otherwise it would have a factor of degree 1, i.e., a root in $\mathbb{F}_2$, while $P(0) = P(1) = 1$. Then, $\mathbb{F}_{2^3}$ can be represented by all triples (a, b, c) of elements in $\mathbb{F}_2$, or equivalently by all polynomials of the form $aX^2 + bX + c$ in $\mathbb{F}_2[X]$. Then, addition and multiplication correspond to the addition and multiplication modulo $P(X)$ of $(aX^2 + bX + c)$ in $\mathbb{F}_2[X]$. For instance,

$$\begin{aligned} (1,1,0) + (0,1,1) &= (X^2 + X) + (X + 1) = (1,0,1) \\ (1,1,0) \times (0,1,1) &= (X^2 + X)(X + 1) \bmod P(X) = (X^3 + X) \bmod P(X) = (0,0,1) \ . \end{aligned}$$

The notation is usual simplified by denoting by α the residue class of X, which corresponds to the element $(0,1,0)$. Since by construction $P(\alpha) = 0$, we then say that $\mathbb{F}_{2^3}$ is obtained from $\mathbb{F}_2$ by adjoining a root of P. With this notation, the elements of $\mathbb{F}_8$ can be seen as quadratic polynomials in α. They are then added and multiplied in the ordinary way and we use that $P(\alpha) = 0$, i.e., $\alpha^3 = \alpha + 1$, to reduce powers of α of degree greater than or equal to 3. For instance,

$$\alpha^4 = \alpha^3\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha \ .$$

By computing the successive powers of α, we can check that α is a primitive element of $\mathbb{F}_8$ as shown in the following table. Indeed, we know from Theorem 1.12 that $\mathbb{F}_8^*$ contains $\phi(1) =$

1 element of order 1 and $\phi(7) = 6$ elements of order 7, implying that all elements different from 1 are generators of $\mathbb{F}_8^*$.

powers of α	$-$	α^0	α	α^2	α^3	α^4	α^5	α^6
polynomials in α	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1

We observe that this correspondence leads to efficient multiplication. For instance, we check with this table that $(\alpha^2+\alpha)(\alpha+1)$ corresponds to $\alpha^4 \cdot \alpha^3 = \alpha^7 = 1$, as previously computed. $\diamond$

1.5 Minimal polynomials

We know that any element $a \in \mathbb{F}_{p^m}$ is a root of $X^{p^m} - X$. But a given $a \in \mathbb{F}_{p^m}$ may also satisfy a lower-degree equation with coefficients in $\mathbb{F}_p$.

Definition 1.15. *The* minimal polynomial over $\mathbb{F}_p$ *of an element $a \in \mathbb{F}_{p^m}$ is the lowest-degree monic polynomial M_a with coefficients in $\mathbb{F}_p$ such that $M_a(a) = 0$.*

Proposition 1.16. *Let $a \in \mathbb{F}_{p^m}$ and M_a be its minimal polynomial over $\mathbb{F}_p$. Then*

1. *M_a is irreducible over $\mathbb{F}_p$;*
2. *$\deg M_a \leq m$;*
3. *If a is a root of $P \in \mathbb{F}_p[X]$, then M_a divides P. In particular, M_a divides $X^{p^m} - X$.*
4. *M_a is the minimal polynomial of all a^{p^i} for $1 \leq i \leq m$.*

Proof.

1. If M_a is not irreducible, there exist two monic polynomials P and Q in $\mathbb{F}_p[X]$ of degree less than $\deg M_a$ such that $M_a = PQ$. Since $M_a(a) = 0$, we have $P(a)Q(a) = 0$, implying that one of these two polynomials, for instance P, satisfies $P(a) = 0$ and $\deg P < \deg M_a$. This contradicts the fact that M_a is the lowest-degree polynomial in $\mathbb{F}_p[X]$ with a as a root.

2. Since $\mathbb{F}_{p^m}$ is a vector space of dimension m over $\mathbb{F}_p$, the $(m+1)$ elements $1, a, a^2, \ldots, a^m$ cannot be linearly independent, i.e., there exist $\lambda_0, \ldots, \lambda_m \in \mathbb{F}_p$ such that

$$\sum_{i=0}^{m} \lambda_i a^i = 0 \, .$$

   Then, a is a root of $P(X) = \sum_{i=0}^{m} \lambda_i X^i$. It follows that the degree of M_a is at most m.

3. If $P(a) = 0$, we write

$$P(X) = Q(X)M_a(X) + R(X)$$

   with $0 \leq \deg R < \deg M_a$. Then, $R(a) = 0$, leading to $R = 0$ since there is no polynomial in $\mathbb{F}_p[X]$ with a as a root of degree less than $\deg M_a$. It follows that M_a divides P. In particular, M_a divides $X^{p^m} - X$ from Corollary 1.5.

4. Obviously, we need to prove the assertion for $i = 1$ only. Let $P(X) = \sum_i c_i X^i$ be a polynomial with coefficients in $\mathbb{F}_p$. Then, from Proposition 1.7, $P(X)^p = \sum_i c_i^p X^{ip}$. Moreover, since all c_i are in $\mathbb{F}_p$, we deduce from Corollary 1.5 that $P(X)^p = P(X^p)$. It follows that the minimal polynomial of a^p is the lowest-degree polynomial P such that $P(a^p) = 0$, or equivalently $P(a) = 0$. Then P is the minimal polynomial of a.

◇

The elements of the form a^{p^i} are called the *conjugates of a with respect to $\mathbb{F}_p$*.

Proposition 1.17. *Let $a \in \mathbb{F}_{p^m}$ and d be the smallest integer r such that*

$$a^{p^r} = a \ ,$$

or equivalently the smallest integer r such that

$$p^r \equiv 1 \bmod \mathsf{order}(a) \ .$$

Then, d divides m and it corresponds to the number of distinct conjugates of a with respect to $\mathbb{F}_p$. Moreover, the minimal polynomial of a over $\mathbb{F}_p$ is

$$M_a(X) = \prod_{i=0}^{d-1} (X - a^{p^i}) \ .$$

Proof. We first observe that $a^{p^r} = a$ implies that the order of a divides $(p^r - 1)$, or equivalently that $p^r \equiv 1 \bmod \mathsf{order}(a)$. Conversely, if $p^r \equiv 1 \bmod \mathsf{order}(a)$, then $a^{p^r} = a$. Therefore the two definitions of d are equivalent. Also, d divides m: if we write $m = cd + r$ with $0 \leq r < d$, we get that

$$a = a^{p^m} = a^{p^{cd} p^r} = \left(a^{p^{cd}}\right)^{p^r} = a^{p^r} \ ,$$

which contradicts the fact that d is the smallest integer satisfying this property.

Now, we show that the set $\{a^{p^i}, 0 \leq i < m\}$ has size d. Since this set is finite, we denote by (j_0, r) the pair of indices with the lowest r such that $a^{p^{j_0+r}} = a^{p^{j_0}}$. Then, $a^{p^{j_0}(p^r-1)} = 1$, implying that the order of a divides $p^{j_0}(p^r - 1)$. However, $\mathsf{order}(a)$ is a divisor of $(p^m - 1)$ (from Prop 1.4), and then it is coprime with p^{j_0}. We then deduce that $\mathsf{order}(a)$ divides $(p^r - 1)$. As a consequence, r is the smallest integer such that $a^{p^r} = a$, which corresponds to the definition of d. Thus, the set $\{a^{p^i}, 0 \leq i \leq m\}$ has cardinality d.

Since all a^{p^i} have the same minimal polynomial as a, we deduce that $P(X) = \prod_{i=0}^{d-1}(X - a^{p^i})$ divides $M_a(X)$. Moreover, all coefficients of P are in $\mathbb{F}_p$. Indeed, we have that $P(X^p) = (P(X))^p$. But for any polynomial $Q(X) = \sum_i c_i X^i$, $Q(X)^p = Q(X^p)$ is equivalent to

$$\sum_i c_i^p X^{ip} = \sum_i c_i X^{ip} \Leftrightarrow \sum_i (c_i^p - c_i) X^{ip} = 0 \ .$$

Then, $\sum_i (c_i^p - c_i) X^{ip}$ is the zero polynomial, that means that all its coefficients are zero, i.e., $c_i^p = c_i$. Using Corollary 1.9, we obtain that all coefficients lie in $\mathbb{F}_p$. Then, P is the minimal polynomial of a. ◇

A consequence of Proposition 1.17 together with Theorem 1.8 is that the product of all distinct minimal polynomials of elements of $\mathbb{F}_q$ is equal to $X^q - X$.

A natural notion for describing the conjugates of an element is the following.

Definition 1.18. *For any integer i, the cyclotomic coset of i modulo (p^m-1) is the set*

$$\{i, pi, p^2i, p^3i, \ldots, p^{d-1}i\}$$

where d is the smallest integer such that $p^d \equiv 1 \bmod p^m - 1$.

Example 1.2. Minimal polynomials of the elements of $\mathbb{F}_8$. We come back to the construction of $\mathbb{F}_8$ by adjoining to $\mathbb{F}_2$ a root $P(X) = X^3 + X + 1$, as in Example 1.1. We can now compute the minimal polynomials of all elements in $\mathbb{F}_8$. We compute all cyclotomic cosets, namely all sets $C(i) = \{i2^j \bmod 7, 0 \leq j < 3\}$. We then get $C(1) = \{1, 2, 4\}$ and $C(3) = \{3, 6, 5\}$. We deduce the conjugacy classes of all elements in $\mathbb{F}_8^*$.

cyclotomic coset	conjugate elements	minimal polynomial
$\{0\}$	1	$X+1$
$\{1,2,4\}$	$\alpha, \alpha^2, \alpha^4$	X^3+X+1
$\{3,5,6\}$	$\alpha^3, \alpha^5, \alpha^6$	X^3+X^2+1

By construction, $M_\alpha(X) = X^3 + X + 1$. The minimal polynomial of α^3 can be computed in several ways, e.g., by searching for a linear combination of α^3, α^5 and α^6 which vanishes or by expanding $(X+\alpha^3)(X+\alpha^5)(X+\alpha^6)$. Also, we only need to observe that M_{α^3} has degree 3 and that the coefficient of X^2 is the sum of the three roots, namely $\alpha^3+\alpha^5+\alpha^6 = 1$. Since M_{α^3} is irreducible over $\mathbb{F}_2$, it has an odd number of nonzero coefficients, implying that $M_{\alpha^3}(X) = X^3 + X^2 + 1$.

We can check that factoring X^8+X over $\mathbb{F}_2$ leads to the product of all minimal polynomials:

$$X^8 + X = X(X+1)(X^3+X+1)(X^3+X^2+1)\ .$$

$\diamond$

For any primitive element $\alpha \in \mathbb{F}_{p^m}$, the minimal polynomial of α^i is the product of all $(X - \alpha^s)$ where s varies in the cyclotomic coset of i modulo $(p^m - 1)$. Clearly, any primitive element in $\mathbb{F}_{p^m}$ has m conjugates, implying that its minimal polynomial has maximal degree.

Corollary 1.19. *If a is a primitive element of $\mathbb{F}_{p^m}$ then M_a has degree m. Such a polynomial is called* a primitive polynomial.

Constructing $\mathbb{F}_{p^m}$ from two different irreducible polynomials P of degree m leads to two isomorphic versions of the field. However, choosing P to be a primitive polynomial has the advantage that any nonzero element can also be written as a power of α where α is a root of P. A table of all monic irreducible polynomials (and their orders) of small degree over $\mathbb{F}_p$ for $p \in \{2, 3, 5, 7\}$ can be found in [LN83, Pages 553-562]. Also, Table D in [LN83, Page 563] provides a primitive polynomial of degree m over $\mathbb{F}_2$ for $1 \leq m \leq 100$. This last table is then very helpful for constructing finite fields of characteristic 2.

Example 1.3. Constructing $\mathbb{F}_9$. For constructing $\mathbb{F}_9$, we choose an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_3$. For instance, $P(X) = X^2 + X + 2$ since it can be easily checked that P has no root in $\mathbb{F}_3$. Then, $\mathbb{F}_9$ is obtained from $\mathbb{F}_3$ by adjoining a root of P. With this notation, the elements of $\mathbb{F}_9$ can be seen as polynomials of degree 1 in α where $\alpha^2 = 2\alpha + 1$. For instance,

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

We then get the following correspondence between the representation of the elements by powers of α, and the representation by affine polynomials in α, showing that α is a primitive element of $\mathbb{F}_9$.

powers of α	$-$	α^0	α	α^2	α^3	α^4	α^5	α^6	α^7
affine polynomials in α	0	1	α	$2\alpha+1$	$2\alpha+2$	2	2α	$\alpha+2$	$\alpha+1$

We can also construct $\mathbb{F}_9$ by adjoining a root β of another irreducible polynomial of degree 2 over $\mathbb{F}_3$, for instance $Q(X) = X^2+1$. Then, by definition, $\beta^2 = -1 = 2$. We can then easily check that $\beta^3 = 2\beta$, and $\beta^4 = 1$. Therefore, β has order 4 and does not generate the multiplicative group $\mathbb{F}_9^*$: the multiplicative subgroup generated by β is $\{1, 2, \beta, 2\beta\}$. However, since $\mathbb{F}_9$ contains $\phi(8) = 4$ generators, we deduce that any of the other four elements of $\mathbb{F}_9$, i.e., $(\beta+1), (\beta+2), (2\beta+1)$ and $(2\beta+2)$, generates $\mathbb{F}_9^*$. For instance, the following table shows that $(\beta+1)$ is a generator of $\mathbb{F}_9$:

powers of $(\beta+1)$	$\beta+1$	$(\beta+1)^2$	$(\beta+1)^3$	$(\beta+1)^4$	$(\beta+1)^5$	$(\beta+1)^6$	$(\beta+1)^7$
affine polys in β	$\beta+1$	2β	$2\beta+1$	2	$2\beta+2$	β	$\beta+2$

We have then constructed two versions of $\mathbb{F}_9$, from two different irreducible polynomials. However, these two versions are isomorphic since we can check that the function ψ of $\mathbb{F}_9$ defined by

$$\psi(a\alpha + b) = a(\beta+1) + b$$

for any a and b in $\mathbb{F}_3$ is a field isomorphism. Indeed, for $x = (a\alpha+b)$ and $y = (c\alpha+d)$, we have $\psi(x+y) = \psi(x) + \psi(y)$. Moreover,

$$\psi(\alpha)^2 = (\beta+1)^2 = 2\beta = 2(\beta+1)+1 = \psi(2\alpha+1) = \psi(\alpha^2)\ .$$

We then deduce that, for $x = a\alpha+b$ and $y = c\alpha+d$,

$$\psi(xy) = ac\psi(\alpha^2) + (ad+bc)\psi(\alpha) + bd = ac\psi(\alpha)^2 + (ad+bc)\psi(\alpha) + bd = \psi(x)\psi(y)\ .$$

We can also compute the minimal polynomials over $\mathbb{F}_3$ of all elements $(\beta+1)^i$ in $\mathbb{F}_9$. We observe that there are 3 cyclotomic cosets of size 2 and two of size 1. The sizes of the cyclotomic cosets correspond to the degrees of the minimal polynomials. The constant coefficient of any minimal polynomial is equal to the product of its roots, which is easily determined from the previous table. For minimal polynomials of degree 2, the coefficient of X is equal to the sum of the two conjugate elements. For instance, the minimal polynomial of $(\beta+1)^2$ has degree 2 since its roots are $(\beta+1)^2$ and $(\beta+1)^6$. The coefficient of X is then $(\beta+1)^2+(\beta+1)^6 = 2\beta+\beta = 0$, and the constant coefficient is $(\beta+1)^8 = 1$. We directly deduce that the minimal polynomial of $(\beta+1)^2$ is X^2+1.

cyclotomic coset	conjugate elements	minimal polynomial
$\{0\}$	1	$X+2$
$\{1,3\}$	$(\beta+1), (\beta+1)^3$	X^2+2X+2
$\{2,6\}$	$(\beta+1)^2, (\beta+1)^6$	X^2+1
$\{4\}$	$(\beta+1)^4$	$X+1$
$\{5,7\}$	$(\beta+1)^5, (\beta+1)^7$	X^2+X+2

Again, we can check that the product of all minimal polynomials corresponds to the factorisation of $X^9 - X$ over $\mathbb{F}_3$:

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

◇

1.6 Subfields

We have seen that the multiplicative group $\mathbb{F}_{p^m}$ contains some multiplicative subgroups which correspond to the cyclic groups generated by the elements of order r with $r|m$. We can also characterise the subfields of $\mathbb{F}_q$. We first need the following useful lemma.

Lemma 1.20. *Let n be an integer $n \geq 2$, and i and j be two nonzero integers. Then*

$$(n^i - 1)|(n^j - 1) \text{ if and only if } i|j .$$

Proof. Using that, for any k and any x,

$$x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + 1) ,$$

we deduce that, if $j = ik$, then $(n^i - 1)$ divides $(n^{ik} - 1)$.

Conversely, we write $j = qi + r$ with $0 \leq r < i$. Then,

$$n^j - 1 = n^r(n^{qi} - 1) + (n^r - 1) .$$

If $(n^i - 1)$ divides the left-hand term, then it divides $(n^r - 1)$ since we have proved that it divides $(n^{qi} - 1)$. This is impossible unless $r = 0$ because $r < i$. ◇

Now, we can prove the following.

Theorem 1.21. *Every subfield of $\mathbb{F}_{p^m}$ has order p^d where d is a positive divisor of m. Conversely, if d is a positive divisor of m, then there exists exactly one subfield of $\mathbb{F}_{p^m}$ with p^d elements.*

Proof. We first show that any subfield of $\mathbb{F}_{p^m}$ has size p^d with $d|m$. Let $\mathbb{F}$ be a subfield of $\mathbb{F}_{p^m}$. Obviously, $\mathbb{F}$ is a finite field with characteristic p implying that it has order p^d for some integer d. From Corollary 1.13, there exists some α which generates $\mathbb{F}$. This element has then order $(p^d - 1)$. From Proposition 1.4, we deduce that $(p^d - 1)$ divides $(p^m - 1)$, which implies from Lemma 1.20 that d is a divisor of m.

Conversely, we now consider a positive divisor d of m. Using Lemma 1.20, $(p^d - 1)$ is a divisor of $(p^m - 1)$. It follows from Theorem 1.12 that $\mathbb{F}_{p^m}$ contains some element of order $(p^d - 1)$. Let

$$\mathbb{F} = \{x \in \mathbb{F}_{p^m} : x^{p^d} = x\} .$$

Then, we can easily check that $\mathbb{F}$ is a field since for any $x, y \in \mathbb{F}$, $(x-y)^{p^d} = x^{p^d} - y^{p^d} = x - y$ and $(xy^{-1})^{p^d} = x^{p^d}(y^{p^d})^{-1} = xy^{-1}$. Moreover, it contains at least an element of order $(p^d - 1)$. Therefore, $\mathbb{F}$ has size p^d. Clearly, there is only one subfield of $\mathbb{F}_{p^m}$ of order $(p^d - 1)$, otherwise the polynomial $x^{p^d} - x$ would have more than p^d roots. ◇

Example 1.4. Subfields of $\mathbb{F}_{2^6}$. From the previous theorem, $\mathbb{F}_{2^6}$ has three (nontrivial) subfields of order 2, 2^2 and 2^3 respectively. Indeed, if we consider a primitive element α in $\mathbb{F}_{2^6}$, we can check that, for any $d|6$,

$$\{0\} \cup \langle \alpha^{\frac{63}{2^d-1}} \rangle$$

is a subfield of order 2^d since $\alpha^{\frac{63}{2^d-1}}$ is an element of order (2^d-1). The three subfields of $\mathbb{F}_{2^6}$ are then:

$$\{0,1\}, \{0,1,\alpha^{21},\alpha^{42}\} \text{ and } \{0,1,\alpha^9,\alpha^{18},\alpha^{27},\alpha^{36},\alpha^{45},\alpha^{54}\} .$$

If we now focus on the multiplicative subgroups of $\mathbb{F}_{2^6}^*$, we get the subgroups of order 3 and 7 derived from the previous subfields, and two additional subgroups of respective orders 9 and 21, namely

$$\langle \alpha^7 \rangle \text{ and } \langle \alpha^3 \rangle .$$

◇

Exercises

Exercise 1.1. Prove that the integers modulo n do not form a field if n is not prime.

Exercise 1.2. If $q \neq 2$, show that

$$\sum_{x \in \mathbb{F}_q} x = 0 .$$

Exercise 1.3. Without factoring $X^{63}+X$ over $\mathbb{F}_2$, determine how many irreducible factors it has over $\mathbb{F}_2$ and their degrees.

Exercise 1.4. Construction of $\mathbb{F}_{16}$.

1. Let α be a root of X^4+X+1. Compute all successive powers of α. Is α a primitive element in $\mathbb{F}_{16}$?
2. Compute $\alpha^7 \times \alpha^{11}$ and $\alpha^7 + \alpha^{11}$ in $\mathbb{F}_{16}$.
3. Determine all non-trivial multiplicative subgroups of $\mathbb{F}_{16}^*$.
4. Determine the order of each element in $\mathbb{F}_{16}$.
5. Compute the minimal polynomial of α, of α^5, of α^3 and of α^7.
6. Let β be a root of $X^4+X^3+X^2+X+1$. Is the set $\{1,\beta,\beta^2,\beta^3\}$ a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_2$?

Bibliography

[LN83] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, 1983.

[McE87] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, 1987.