

The Structure of Finite Fields

Henry D. Pfister

October 6th, 2006 (rev. 0)
October 24rd, 2012 (rev. 1.1)
November 1st, 2013 (rev. 1.2)

1 Preliminaries

1.1 Whole Numbers

The set of natural numbers is defined to be $\mathbb{N} \triangleq \{0, 1, 2, \dots\}$, the set of all integers is defined to be $\mathbb{Z} \triangleq \{\dots, -2, -1, 0, 1, 2, \dots\}$, and the set of positive integers is defined to be $\mathbb{Z}^+ \triangleq \{1, 2, \dots\}$.

Definition 1.1. For integers $a, b, c \in \mathbb{Z}^+ \setminus \{1\}$, we say c is **composite** if it can be written as $c = ab$. According to this definition, 1 is not composite.

Definition 1.2. We say an integer $d \in \mathbb{Z}$ **divides** $m \in \mathbb{Z}$ iff $m = dq$ for some $q \in \mathbb{Z} \setminus \{0\}$. This is denoted $d \mid m$. If d does not divide m , then we write $d \nmid m$.

Definition 1.3. The division of $m \in \mathbb{Z}$ by $d \in \mathbb{Z} \setminus \{0\}$ results in a quotient $q \in \mathbb{Z}$ and a remainder $r \in \mathbb{Z}$ that must satisfy $m = qd + r$ and $|r| < |d|$. In general, there may be multiple (q, r) pairs which satisfy these conditions (e.g., r may be positive or negative). By convention, we define the remainder function $R_d[m] \rightarrow r$ by requiring that $r \geq 0$.

Definition 1.4. An integer $p \in \mathbb{Z}^+ \setminus \{1\}$ is **prime** if it is not composite. By convention, 1 is not prime. Since a prime cannot be written as a product, it follows that a prime is only divisible by ± 1 and $\pm p$.

Definition 1.5. The **greatest common divisor** of $a, b \in \mathbb{Z}^+$ is the largest $k \in \mathbb{Z}^+$ such that $k \mid a$ and $k \mid b$. This element is denoted $\gcd(a, b)$.

Definition 1.6. The **least common multiple** of $a, b \in \mathbb{Z}^+$ is the smallest $k \in \mathbb{Z}^+$ such that $a \mid k$ and $b \mid k$. This element is denoted $\text{lcm}(a, b)$.

Theorem 1.7 (Euclid). For $a_1, a_2 \in \mathbb{Z}^+$ with $a_2 < a_1$, the **Euclidean algorithm** recursively computes the decreasing sequence $a_{n+2} = R_{a_{n+1}}[a_n]$ which terminates when $a_m = 0$ with $a_{m-1} = \gcd(a_1, a_2)$. Furthermore, the greatest common divisor can be written as $\gcd(a_1, a_2) = u_{m-1}a_1 + v_{m-1}a_2$ for some $u_{m-1}, v_{m-1} \in \mathbb{Z}$.

Proof. Since $R_d[a]$ is the remainder after a is divided by d , we have $a_n = a_{n+1}q_{n+1} + a_{n+2}$ (with $a_{n+2} < a_{n+1}$) and therefore $a_{n+2} = a_n - a_{n+1}q_{n+1}$. Let $d_n = \gcd(a_n, a_{n+1})$ and notice that $d_n \mid a_n$ and $d_n \mid a_{n+1}$ implies that $d_n \mid a_n - a_{n+1}q_{n+1}$ (i.e., $d_n \mid a_{n+2}$). This implies that both d_n, d_{n+1} divide a_{n+1} and a_{n+2} , but $d_{n+1} = \gcd(a_{n+1}, a_{n+2})$ is the largest such integer so $d_{n+1} \geq d_n$.

On the other hand, $d_{n+1} \mid a_{n+1}$ and $d_{n+1} \mid a_n - a_{n+1}q_{n+1}$ implies $d_{n+1} \mid a_n$. This implies that both d_{n+1} divides both a_{n+1} and a_n , but $d_n = \gcd(a_n, a_{n+1})$ is the largest such integer so $d_n \geq d_{n+1}$. Thus, we have established that, for $n = 1, \dots, m-1$,

$$\gcd(a_n, a_{n+1}) = \gcd(a_{n+1}, a_{n+2}).$$

It follows that $d_{m-1} = d_1$ and that the algorithm returns $\gcd(a_1, a_2)$

Finally, we observe that, if $a_i = u_i a_1 + v_i a_2$ for $i = 3, \dots, n+1$, then $a_{n+2} = u_n a_1 + v_n a_2 - q_{n+1}(u_{n+1} a_1 + v_{n+1} a_2)$. This gives the recursions $u_{n+2} = u_n - q_{n+1} u_{n+1}$ and $v_{n+2} = v_n - q_{n+1} v_{n+1}$, starting from $u_3 = 1$ and $v_3 = q_2$. \square

Remark 1.8. It is straightforward to generalize Theorem 1.7 to an arbitrary Euclidean domain (e.g., polynomials over a field).

Exercise 1.9. Generalize the Euclidean algorithm to polynomials over a field and prove the natural analog of Theorem 1.7 for that case.

Lemma 1.10 (Euclid). *For integers $a, b, c \in \mathbb{Z}^+ \setminus \{1\}$, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. If $\gcd(a, b) = 1$, then the extended Euclidean algorithm gives $1 = ua + vb$. Multiplying by c gives $c = uac + vbc$. Since $a \mid uac$ and $a \mid vbc$ (e.g., $a \mid bc$ by hypothesis), we find that $a \mid c$. \square

Remark 1.11. This lemma is commonly used to prove uniqueness in the fundamental theorem of arithmetic (i.e., that a positive integer has a unique decomposition into prime factors). Surprisingly, the simplest proof of this appears to depend on the Euclidean algorithm.

Corollary 1.12. *An integer $p \in \mathbb{Z}^+ \setminus \{1\}$ is prime iff, for any $a, b \in \mathbb{Z}^+ \setminus \{1\}$, $p \mid ab$ implies $p \mid a$ or $p \mid b$. By induction, one may also conclude that, if p is prime, then $p \mid \prod_{i=1}^n a_i$ implies $p \mid a_i$ for some $i \in \{1, \dots, n\}$.*

Proof. For the “if”, we prove the contrapositive. If p is not prime, then p is composite and there exists $a, b \in \mathbb{Z}^+ \setminus \{1\}$ such that $p = ab$. For these values, $p \mid ab$ but $p \nmid a$ and $p \nmid b$. For the “only if”, we prove it directly. If p is prime, then $\gcd(p, a) \in \{1, p\}$ and either $p \mid a$ or $\gcd(p, a) = 1$. In the first case, we’re done and in the second, we can apply Lemma 1.10 to show that $p \mid b$. For the final statement, the inductive step is $p \mid a_n \prod_{i=1}^{n-1} a_i$ implies $p \mid a_n$ or $p \mid \prod_{i=1}^{n-1} a_i$. \square

Theorem 1.13 (Fundamental Theorem of Arithmetic). *Any number $a \in \mathbb{Z}^+ \setminus \{1\}$ can be expressed uniquely as a product of primes, $a = \prod_{i=1}^r p_i^{n_i}$, where $n_i \geq 1$ and $p_{i+1} > p_i$.*

Proof. First, we note that a can be decomposed into a product of primes simply splitting any composite factor until none remain. To prove uniqueness, suppose that $a = \prod_{i=1}^r p_i^{n_i} = \prod_{j=1}^s q_j^{m_j}$ is the minimal positive integer with more than one prime factorization. If $p_i = q_j$ for any $i \in \{1, \dots, r\}$ and $j \in \{1, \dots, s\}$, then we can divide all terms by the common factor and this contradicts the minimality of a . Therefore, we can assume that $p_i \neq q_j$ for all $i \in \{1, \dots, r\}$ and $j \in \{1, \dots, s\}$. But, $p_1 \mid \prod_{j=1}^s q_j^{m_j}$ (i.e., $p_1 \mid a$) and Corollary 1.12 together imply that $p_1 \mid p_j$ for some $j \in \{1, \dots, s\}$. Since $p_1 \neq q_j$ for $j \in \{1, \dots, s\}$, this contradicts the fact that a prime q_j is divisible only by ± 1 and $\pm q_j$. Therefore, there is no integer with more than one prime factorization. \square

1.2 Groups

Definition 1.14. Let G be a group with n elements. The size of G is known as the order or the cardinality of the group and is denoted $\text{ord}(G) = n$ or $|G| = n$.

Definition 1.15. Let (G, \diamond) be a group with operation \diamond and identity e . The **order** of an element $g \in G$ is denoted $\text{ord}(g)$ and is the smallest positive integer k such that $\underbrace{g \diamond g \diamond \dots \diamond g}_{k \text{ times}} = e$. If no such integer

exists, then $\text{ord}(g) = \infty$.

Remark 1.16. It is worth noting that $\text{ord}(g) \leq |G|$. To see this, consider the sequence $g, g \diamond g, g \diamond g \diamond g, \dots$ and observe that $\text{ord}(g) \leq |G|$ as long as the sequence does not repeat before reaching e . Now, suppose that it does repeat before reaching e . In that case, the k -th element equals the j -th element for some $j < k$. But, multiplying both elements by the inverse of the j -th element implies that $(k - j)$ -th element must have been e . The resulting contradiction shows that the sequence must reach e before repeating.

Definition 1.17. Let G be a group and A be a subset of G . The subgroup generated by A is denoted $\langle A \rangle$ and is the smallest subgroup of G which contains all elements in A .

Lemma 1.18. *Let (G, \cdot) be a finite group with $A \subset G$. If we define $A_n = \{a_1 a_2 \dots a_n \mid a_i \in A\}$, then there is an N such that $A_n = \langle A \rangle$ for all $n > N$.*

Proof. Since A_n is composed only of products of elements from A , we have $A_n \subseteq \langle A \rangle$ for all $n \in \mathbb{N}$. Let m be the minimum order of any element in A . Since $e \in A_m$, we have $e \in A_{mt}$ (for integer $t \geq 1$) and therefore $A_{m(t+1)} \subseteq A_{mt}$. If $A_{m(t+1)} \neq A_{mt}$, then $A_{m(t+1)}$ must have at least one more element than A_{mt} . Therefore, if $|G| = n$ is finite, we conclude that $A_{mn} = \langle A \rangle$. \square

Theorem 1.19 (Lagrange). *Let G be a group with subgroup H . Then $|G| = |H| [G : H]$ where $[G : H]$ is index (i.e., number of cosets) of H in G .*

Sketch of Proof. Coset decomposition gives a rectangular table with $[G : H]$ rows and $\text{ord}(H)$ columns. Each row is a distinct coset of H and, therefore, the table contains all elements in G . \square

Corollary 1.20. *For any finite group G and $g \in G$, we have $\text{ord}(g) \mid \text{ord}(G)$.*

Proof. Let $H = \langle g \rangle$ be the cyclic subgroup formed by g and apply Theorem 1.19. \square

Lemma 1.21. *Let (G, \cdot) be a finite group. If $g \in G$ has order $n = \text{ord}(g)$, then $\text{ord}(g^i) = n / \gcd(i, n)$. For $g, h \in G$ with $gh = hg$ and $\gcd(\text{ord}(g), \text{ord}(h)) = 1$, one finds that $\text{ord}(gh) = \text{ord}(g) \text{ord}(h)$.*

Proof. If $(g^i)^k = e$, then $n \mid ik$ and the minimal $k \in \mathbb{Z}^+$ is $\frac{\text{lcm}(i, n)}{i} = \frac{n}{\gcd(i, n)}$. For the second, if $gh = hg$, then $(gh)^i = g^i h^i = 1$ implies $g^i = h^{-i}$. Let k be the minimal $i \in \mathbb{Z}^+$ satisfying $g^i = h^{-i}$ and notice that $a = g^k = h^{-k}$ implies $a \in \langle g \rangle \cap \langle h \rangle$. But, $F = \langle g \rangle \cap \langle h \rangle = \{e\}$ because, for all $f \in F$, Corollary 1.20 shows $\text{ord}(f) \mid \text{ord}(g)$ and $\text{ord}(f) \mid \text{ord}(h)$. Therefore, $\text{ord}(f) \leq \gcd(\text{ord}(g), \text{ord}(h)) = 1$ and $f = e$. Finally, we see that $g^k = h^{-k} = e$ implies $k = \text{lcm}(\text{ord}(g), \text{ord}(h)) = \text{ord}(g) \text{ord}(h)$. \square

Theorem 1.22 (Cauchy). *For any finite group (G, \cdot) , if $p \mid \text{ord}(G)$ for prime p , then G has an element of order p .*

Proof. This is true in general, but we prove it only for abelian groups. The proof is by induction. For the base, we first prove the statement for any finite abelian group G where $p \mid \text{ord}(G)$ and G only has trivial subgroups (e.g., the identity and the group itself are the trivial subgroups). In this case, all non-identity elements of G must have $\text{ord}(g) = p$ because any other value implies a non-trivial subgroup.

For the inductive step, consider any finite abelian group G that satisfies $p \mid \text{ord}(G)$ and has a non-trivial subgroup. Let g be any non-identity element. If $p \mid \text{ord}(g)$, then $g^{\text{ord}(g)/p}$ is an element of order p . If p does not divide $\text{ord}(g)$, then let $H = \langle g \rangle$ be the cyclic group it generates.

Since $\text{ord}(G) = \text{ord}(G/H) \text{ord}(H)$ by Lagrange's theorem, we see that $p \mid \text{ord}(G/H)$ because $p \nmid \text{ord}(H)$. In this case, G/H contains an element x of order p by the inductive hypothesis. The definition of G/H shows that $x = yH$ for some $y \in G$. Let $m = \text{ord}(y)$ and observe that $x^m = (yH)^m = (y^m)H = H$. Hence, it follows that $p \mid m$ and $y^{m/p}$ is an element of order p in G . \square

Definition 1.23. An element, g , in a group G is **primitive** if $\text{ord}(g) = \text{ord}(G)$. If such an element exists, it generates the entire group and the group is cyclic.

Definition 1.24. The **Euler totient function** $\phi(n)$ equals the number of positive integers less than or equal to n that are relatively prime to n . For $n = \prod_{i=1}^m p_i^{k_i}$, one finds that

$$\phi(n) \triangleq n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \phi\left(\prod_{i=1}^m p_i^{k_i}\right) = \prod_{i=1}^m p_i^{k_i} \left(1 - \frac{1}{p_i}\right).$$

Corollary 1.25. *In a cyclic group with n elements, there are $\phi(n) \geq 1$ primitive elements. If $d \mid n$, then there are $\phi(d)$ elements of order d .*

Proof. Let g have order n so that $G = \langle g \rangle$ is a cyclic group with n elements. Then, $h = g^i$ has order $\frac{n}{\gcd(i, n)}$, which equals n if $\gcd(i, n) = 1$ (i.e., if i is relatively prime to n). This gives $\phi(n)$ primitive elements and the formula shows $\phi(n) \geq 1$ for $n \geq 1$. All subgroups of G are cyclic groups generated by g^i for some i . Therefore, the elements of order d in G are precisely the $\phi(d)$ primitive elements in $H = \langle g^{n/d} \rangle$. \square

Lemma 1.26. *Let (G, \cdot) be an abelian group and $m = \max_{g \in G} \text{ord}(g)$. Then, for all $g \in G$, $\text{ord}(g) \mid m$ and g^m is the identity.*

Proof. Fix $g \in G$ and let $h \in G$ have order $m = \prod_{i=1}^n p_i^{r_i}$ for primes p_1, \dots, p_n . If there is a prime p such that $p \mid \text{ord}(g)$, then $p = p_i$ for some $i = 1, \dots, n$. Otherwise, $g' = g^{\text{ord}(g)/p}$ has order p , $p \nmid m$ implies $\gcd(p, m) = 1$, and Lemma 1.21 implies $\text{ord}(g'h) = \text{ord}(g') \text{ord}(h) = pm > m$, which contradicts the definition of m . Likewise, if $p_i^{r_i+1} \mid \text{ord}(g)$, then $g' = g^{\text{ord}(g)/p_i^{r_i+1}}$ has order $p_i^{r_i+1}$ and $h' = h^{p_i^{r_i}}$ has order $m/p_i^{r_i}$. Since $\gcd(p_i^{r_i+1}, m/p_i^{r_i}) = 1$, Lemma 1.21 implies that $\text{ord}(g'h') = p_i m > m$, which contradicts the definition of m . Therefore, $\text{ord}(g) = \prod_{i=1}^n p_i^{s_i}$ for $0 \leq s_i \leq r_i$ and $\text{ord}(g) \mid m$. It follows naturally that g^m is the identity. \square

2 Finite Fields

In this section, we will consider some of basic structural properties of finite fields. A finite field with q elements will be denoted \mathbb{F}_q , and we will find that finite fields only exist if $q = p^m$ for prime p and some integer $m \geq 1$. The set of invertible elements is denoted $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

2.1 Basics

Definition 2.1. A **field** is a set F with two binary operations $+$ and \cdot such that $(F, +)$ is an abelian group with identity labeled “0”, $(F \setminus \{0\}, \cdot)$ is an abelian group with identity labeled “1”, and the operation \cdot distributes over $+$: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Definition 2.2. The **characteristic** of a field F is denoted $\text{char}(F)$ and is the smallest positive integer k such that $\underbrace{1 + \cdots + 1}_k = 0$. If no such integer exists, then the characteristic is defined to be 0.

Remark 2.3. It is worth noting that $\text{char}(F) \leq |F|$. To see this, let G be the additive group of F and observe that, if $\text{ord}_G(1) < \infty$, then we have $\text{char}(F) = \text{ord}_G(1) \leq |G|$ because 0 is the identity in G . Similarly, if $\text{ord}_G(1) = \infty$, then $\text{char}(F) = 0$. Thus, $\text{char}(F) \leq |G| = |F|$.

Theorem 2.4. For any finite field F , the characteristic is prime.

Proof. For any $a, b \in \mathbb{Z}^+ \setminus \{1\}$, assume $\text{char}(F) = ab$ and is therefore not prime. Then, $\underbrace{1 + \cdots + 1}_a \neq 0$, $\underbrace{1 + \cdots + 1}_b \neq 0$, and applying the distributive law repeatedly shows that

$$\underbrace{(1 + \cdots + 1)}_a \underbrace{(1 + \cdots + 1)}_b = \underbrace{1 + \cdots + 1}_{ab} = 0. \quad (1)$$

This leads to a contradiction because F^* must be an abelian group but it is not closed under multiplication. Therefore, the characteristic of F is prime. \square

Definition 2.5. The smallest subfield of a field F is called the **prime subfield**.

Theorem 2.6. For any finite field F , the additive subgroup generated by 1 has $\text{char}(F)$ elements and is the prime subfield.

Proof. Using Theorem 2.4, we see that $p = \text{char}(F)$ is prime. The set generated by 1 under addition is a subgroup of the additive group of F with p elements, and will be denoted $K = \{1, 2, \dots, p-1, 0\}$. Using the natural multiplication that is defined by addition and the distributive law (see 1), we see that K is also closed under multiplication. Moreover, this multiplication is isomorphic to integer multiplication modulo p .

Now, we must show that every element of $K^* = K \setminus \{0\}$ has a multiplicative inverse. Therefore, for any $a \in K^*$, we consider the list

$$a1, a2, \dots, a(p-1),$$

where multiplication is done modulo p because $\underbrace{1 + \cdots + 1}_p = 0$.

If the i th element on the list is zero, then we have $ai = pk$. Since p is prime, this implies that $p \mid a$ or $p \mid i$. But, both of these are impossible because $a, i \in \{1, 2, \dots, p-1\}$. Therefore, all elements are non-zero. Next, suppose that the i th and j th element (with $j > i$) on the list are equal. This implies that $a(j-i) = pk$ with $1 \leq a \leq p-1$ and $1 \leq j-i \leq p-2$. This is a contradiction, however, because p is prime and $p \mid a(j-i)$ but $p \nmid a$ and $p \nmid j-i$. Therefore, all elements on the list are distinct and one of them must be 1. If the i th element on the list is 1, then $a^{-1} = \underbrace{1 + \cdots + 1}_i$. Since $a \in K^*$ was arbitrary,

all elements have multiplicative inverses and K is a field.

Since all subfields must include the additive subgroup generated by 1 and this field contains only these elements, we find that K is the prime subfield. \square

Theorem 2.7. The quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements iff p is prime.

Proof. Clearly $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with identity. We need only to show that every non-zero element has an inverse iff p is prime. If p is prime, then the proof of Theorem 2.6 actually contains the proof we need. If p is not prime, then Theorem 2.4 shows it is not a field. \square

Theorem 2.8. *There exists no finite field of size other than p^m for prime p .*

Proof. Assume a finite field F of size n with $n \neq p^m$ for prime p exists and let $\text{char}(F)$ be the additive order of 1. Then, there exists two distinct primes $p, p' \in \mathbb{N}$ such that $p \mid n$ and $p' \mid n$. Using Theorem 1.22, we see that the additive group of F must have a cyclic subgroup both with p and p' elements. Let a, a' be the generators of a subgroups with p, p' elements and notice that $\underbrace{(a + \cdots + a)}_p = a \underbrace{(1 + \cdots + 1)}_p = 0$ and $a' \underbrace{(1 + \cdots + 1)}_{p'} = 0$. Since a, a' have additive orders greater than 1, they are not zero and the previous statement implies that $\text{char}(F) \mid p$ and $\text{char}(F) \mid p'$. Since a prime is only divisible by 1 and itself, we find that $\text{char}(F) = 1$ (i.e., 1 is the additive identity so $1 = 0$). This contradicts the field properties and therefore we must conclude that no finite field F of size $n \neq p^m$ exists. \square

Definition 2.9. An element $\alpha \in \mathbb{F}_q^*$ is **primitive** if its multiplicative order satisfies $\text{ord}(\alpha) = q - 1$. We will see shortly that such an element always exists and generates the multiplicative group.

Lemma 2.10. *Let F be a subfield of K and $p(x) \in F[x]$ be a polynomial of degree $d \geq 1$. Then, $p(x)$ has at most d roots in K .*

Proof. Let $Z(d)$ be the maximum number of roots of a degree d polynomial and consider induction on d . If $d = 1$, then one can easily solve for the unique root $z \in F$ and $Z(1) = 1$. If $d > 1$ and $p(z) = 0$ for some $z \in K$, then division by $(x - z)$ gives

$$r(x) = p(x) - (x - z)q(x),$$

where $\deg(q(x)) = d - 1$ and $\deg(r(x)) < 1$. The latter implies that $r(x)$ is a constant and substituting $x = z$ shows that $r(x) = 0$. Therefore, $p(x)$ has at most one more root than $q(x)$. This implies $Z(d + 1) \leq Z(d) + 1$ for $d \geq 1$ and induction gives $Z(d) \leq d$. \square

Theorem 2.11. *The $q - 1$ elements of \mathbb{F}_q^* have the following properties:*

1. *They are in one-to-one correspondence to the roots of the polynomial $x^{q-1} - 1$ and*

$$\prod_{\alpha \in \mathbb{F}_q^*} (x - \alpha) = x^{q-1} - 1.$$

2. *They form a cyclic group.*
3. *There exists an element, α , of order $q - 1$ (i.e., a primitive element) and*

$$\prod_{i=0}^{q-2} (x - \alpha^i) = x^{q-1} - 1.$$

Proof. First, we prove (1). Since \mathbb{F}_q^* is an abelian group with $q - 1$ elements under multiplication, we find that $\text{ord}(\alpha) \mid (q - 1)$ for all $\alpha \in \mathbb{F}_q^*$. This means that $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$ and therefore all elements of \mathbb{F}_q^* are roots of the polynomial $x^{q-1} - 1 = 0$. Since $x^{q-1} - 1 = 0$ has at most $q - 1$ roots and \mathbb{F}_q^* has exactly $q - 1$ distinct elements, it follows that the roots of $x^{q-1} - 1$ are in one-to-one correspondence with \mathbb{F}_q^* . The formula follows because unique factorization implies any two monic polynomials with the same roots must be equal.

Now, we prove (2). Let $d = \max_{\alpha \in \mathbb{F}_q^*} \text{ord}(\alpha)$ be maximum multiplicative order of any element in \mathbb{F}_q^* and suppose that $d \neq q - 1$. It is clear that $d > q - 1$ implies the contradiction $\text{ord}(\mathbb{F}_q^*) > q - 1$. Next, we consider $d < q - 1$ and use Lemma 1.26 to see that $\text{ord}(\alpha) \mid d$ for all $\alpha \in \mathbb{F}_q^*$. This implies that $x^d - 1 = 0$ for all $x \in \mathbb{F}_q^*$. Since the fundamental theorem of algebra implies that $x^d - 1$ has at most d roots, this gives the contradiction $\text{ord}(\mathbb{F}_q^*) < q - 1$ and we conclude that $d = q - 1$. Finally, any group with an element whose order equals the size of the group must be cyclic.

Lastly, we prove (3). Let $\alpha \in \mathbb{F}_q^*$ have $\text{ord}(\alpha) = q - 1$. Then, $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ and the stated product equals the product from (1). \square

2.2 Subfields and Extension Fields

Definition 2.12. An **extension field** K of a field F is a field which contains F as a proper subset.

Definition 2.13. A non-constant polynomial, $a(x)$, with coefficients in the field F (i.e., $a(x) \in F[x]$) is called **reducible** over F if it can be written as a product of multiple non-constant polynomials in $F[x]$. Otherwise, it is called **irreducible** (or **prime**) over F .

Lemma 2.14. For non-constant polynomials $a(x), b(x), c(x) \in F[x]$, if $a(x) \mid b(x)c(x)$ and $\gcd(a(x), b(x)) = 1$, then $a(x) \mid c(x)$.

Proof. If $\gcd(a(x), b(x)) = 1$, then the extended Euclidean algorithm for polynomials gives $1 = u(x)a(x) + v(x)b(x)$. Multiplying by $c(x)$ gives $c(x) = u(x)a(x)c(x) + v(x)b(x)c(x)$. Since $a(x) \mid u(x)a(x)c(x)$ and $a(x) \mid v(x)b(x)c(x)$ (e.g., by hypothesis $a(x) \mid b(x)c(x)$), we find that $a(x) \mid c(x)$. \square

Exercise 2.15. Use Lemma 2.14 to prove that each monic polynomial in $\mathbb{F}_q[x]$ has a unique factorization (up to the order of the factors) into the product of monic irreducible polynomials in $\mathbb{F}_q[x]$.

Theorem 2.16. The quotient ring $K = \mathbb{F}_q[x]/\langle p(x) \rangle$ is an extension field of \mathbb{F}_q with q^m elements iff $p(x)$ is an irreducible polynomial over \mathbb{F}_q of degree m .

Proof. The proof is very similar to the case of integers modulo a prime. Since K consists of polynomials over a field, it is automatically a commutative ring with identity. Therefore, we must prove only that each element in K^* has a multiplicative inverse. To do this, we fix $a(x) \in K$ and enumerate $a(x)b(x)$ for all $b(x) \in K$. We assume each coset in K is represented by its minimal degree coset leader and therefore $\gcd(a(x), p(x)) = 1$ because $\deg(a(x)) < \deg(p(x))$.

If some element on this list is 0, then $a(x)b(x) \bmod p(x) = 0$ implies $p(x) \mid a(x)b(x)$. But, then Lemma 2.14 implies that $p(x) \mid b(x)$, which gives a contradiction because $\deg(b(x)) < \deg(p(x))$. This implies that multiplication by $a(x)$ is closed on K^* .

Next, suppose that elements $a(x)b(x)$ and $a(x)c(x)$ are equal for $b(x) \neq c(x)$. This implies that $a(x)(b(x) - c(x)) = d(x)p(x)$ and $p(x) \mid a(x)(b(x) - c(x))$. As in the previous case, this gives a contradiction because $\deg(a(x)) < \deg(p(x))$ and $\deg(b(x) - c(x)) < \deg(p(x))$. Therefore, all elements on the list are distinct and one of them must be 1. \square

Remark 2.17. Since modulo $p(x)$ arithmetic is essentially the same as polynomial arithmetic along with the identity $p(x) = 0$, one can think of the element x as a root of the polynomial $p(x)$. For example, the quotient ring $K = \mathbb{R}[x]/\langle x^2 + 1 \rangle$ is isomorphic to the ring $\{a + bx \mid a, b \in \mathbb{R}\}$ where $x = \sqrt{-1}$ is the complex root of $x^2 + 1$. This is the canonical construction of the complex field as an extension field of the real numbers.

Definition 2.18. A polynomial $p(x) \in \mathbb{F}_q[x]$ is called **primitive** if it is irreducible and $x + p(x)\mathbb{F}_q[x]$ is a primitive element in the finite field $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/\langle p(x) \rangle$. This is equivalent to the condition $x^j \bmod p(x) \neq 1$ for $j = 1, 2, \dots, q^m - 2$.

Remark 2.19. While there are many ways to think about the extension field $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/\langle p(x) \rangle$, the following provides a rather concrete picture. For a primitive polynomial $p(x) = \sum_{i=0}^m p_i x^i$ with coefficients in \mathbb{F}_q , let the companion matrix $A \in \mathbb{F}_q^{m \times m}$ be

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & -p_0/p_m \\ 1 & 0 & \dots & 0 & -p_1/p_m \\ 0 & 1 & \dots & 0 & -p_2/p_m \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -p_{m-1}/p_m \end{bmatrix}.$$

Then, the ring of matrices $M = \{0, I, A, A^2, \dots, A^{q^m-2}\} \subset \mathbb{F}_q^{m \times m}$ is isomorphic to the finite field \mathbb{F}_{q^m} . In particular, all finite fields are isomorphic to a subset of finite-dimensional matrices over $\{0, 1, \dots, p-1\} \subset \mathbb{Z}$ with modulo p arithmetic. Finally, we note that the Cayley-Hamilton Theorem implies that $\sum_{i=0}^m p_i A^i = 0$ (i.e., the matrix A is a root of $p(x)$).

Lemma 2.20. In a field F with prime characteristic p , we have $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$ for all $\alpha, \beta \in F$. Repeated application of this rule gives $(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}$.

Proof. Using the Binomial Theorem, we get

$$(\alpha + \beta)^p = \sum_{i=0}^p \binom{p}{i} \alpha^i \beta^{p-i} = \alpha^p + \beta^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i \beta^{p-i}.$$

Consider the formula $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}$ and observe that, since p is prime, $i \nmid p$ for $i = 2, \dots, p-1$. So $p \mid \binom{p}{i}$ for $i = 1, \dots, p-1$ and this implies that $\frac{(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}$ is integer and that $\binom{p}{i} \pmod p = 0$. Applying the stated rule to $((\alpha - \beta) + \beta) = \alpha$ gives $(\alpha - \beta)^p + \beta^p = \alpha^p$ and proves the \pm part. \square

Theorem 2.21. *The finite field $K = \mathbb{F}_{p^m}$ for prime p contains the subfield $F = \mathbb{F}_{p^n}$ iff $n \mid m$. If, in addition, α is primitive in K , then $\beta = \alpha^{(p^m-1)/(p^n-1)}$ is primitive in F .*

Proof. First, we observe that

$$p^{ab} - 1 = (p^a - 1) \sum_{i=0}^{b-1} p^{ia} = (p^a - 1) d,$$

where $d = \sum_{i=0}^{b-1} p^{ia}$ is an integer. Next, we show that $p^n - 1 \mid p^m - 1$ iff $n \mid m$. To start, we use division to write $m = nt + r$ with $0 \leq r < n$ and observe that

$$p^m - 1 = p^{nt+r} - 1 = p^r (p^{nt} - 1) + p^r - 1 = p^r (p^n - 1) \left(\sum_{i=0}^{t-1} p^{in} \right) + p^r - 1.$$

If $r = 0$, then we see that $p^n - 1 \mid p^m - 1$. If $r \neq 0$, then $0 < p^r - 1 < p^n - 1$ and dividing both sides by $p^n - 1$ shows that $p^n - 1 \nmid p^m - 1$. If $p^n - 1 \nmid p^m - 1$, then there is no multiplicative subgroup of K with $p^n - 1$ elements and therefore no subfield with p^n elements.

The above factoring trick also allows one to write

$$x^{p^{ab}-1} - 1 = x^{(p^a-1)d} - 1 = (x^{p^a-1} - 1) \sum_{i=0}^{d-1} x^{i(p^a-1)}.$$

If $n \mid m$, then choosing $a = n$ and $b = m/n$ shows that $x^{p^n-1} - 1 \mid x^{p^m-1} - 1$. Let $q = p^n$ and $Q = p^m$. Since the non-zero elements of K are in one-to-one correspondence with the roots of $x^q - 1$, the statement $x^{q-1} - 1 \mid x^{Q-1} - 1$ implies that K contains a subset of $q - 1$ elements that satisfy $x^{q-1} - 1 = 0$. Using this, we define the sets $S = \{x \in K \mid x^q - x = 0\}$ and $S^* = \{x \in K \mid x^{q-1} - 1 = 0\} = S \setminus \{0\}$. The set S^* is closed under multiplication because $(\alpha\beta)^{q-1} = \alpha^{q-1}\beta^{q-1} = 1$ for $\alpha, \beta \in S^*$. This set S is closed under addition because Theorem 2.20 implies that, for $\alpha, \beta \in S$,

$$(\alpha + \beta)^q = (\alpha^q + \beta^q) = \alpha + \beta.$$

The subset S forms a subgroup of the additive group of K because it is closed under addition. The set S^* forms a subgroup of the multiplicative group of K because S^* is closed under multiplication. Since the distributive property is inherited from K , we see that S is a subfield with $q = p^n$ elements. Finally, if α is primitive in K , then $\beta = \alpha^{(p^m-1)/(p^n-1)}$ has order $p^n - 1$ and is therefore primitive in F . \square

Definition 2.22. A **splitting field** of a polynomial $a(x) \in F[x]$ is an extension field where $a(x)$ can be written as a product of linear factors.

Theorem 2.23. *Every polynomial $a(x) \in \mathbb{F}_q[x]$ has a splitting field.*

Proof. First, we write $a(x)$ as a product of irreducible (over \mathbb{F}_q) polynomials

$$a(x) = \prod_{i=1}^n a_i(x)$$

and let $d_i = \deg(a_i(x))$. Since the roots of any degree- d irreducible polynomial must lie in the extension field \mathbb{F}_{q^d} , so we simply need a field that contains $\mathbb{F}_{q^{d_i}}$ for $i = 1, \dots, n$. Theorem 2.21 shows that \mathbb{F}_{q^d} with $d = \text{lcm}(d_1, d_2, \dots, d_n)$ will suffice because $d_i \mid d$ for $i = 1, \dots, n$. \square

2.3 Minimal Polynomials and Conjugates

Let K be an extension field of \mathbb{F}_q with $Q = q^m$ elements.

Definition 2.24. The conjugates of $\beta \in K$ with respect to \mathbb{F}_q are the elements in the sequence $\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \dots$. Let d be the smallest positive integer such that $\beta^d = \beta$. Then, there are d distinct elements in the sequence and the conjugacy class of $\beta \in K$ with respect to \mathbb{F}_q is $C_{\beta, \mathbb{F}_q} = \{\beta, \beta^q, \beta^{q^2}, \dots, \beta^{q^{d-1}}\}$. It is easy to verify that $|C_{\beta, \mathbb{F}_q}| = d \leq m$ because $\beta^{q^m} = \beta$ for all $\beta \in K$.

Definition 2.25. The minimal polynomial of $\beta \in K$ with respect to F is the minimal-degree monic polynomial $p(x) \in F[x]$ such that $p(\beta) = 0$. This polynomial is denoted $m_{\beta, F}(x)$.

Lemma 2.26. *The minimal polynomial $m_{\beta, F}(x)$ is unique and irreducible over F .*

Proof. Suppose $a(x), b(x) \in F[x]$ are two distinct monic polynomials of minimal degree that satisfy $a(\beta) = b(\beta) = 0$ for an element $\beta \in K \supset F$. Then, the polynomial $c(x) = a(x) - b(x)$ satisfies $c(\beta) = 0$ and has $\deg(c(x)) < \deg(a(x))$. Multiplying $c(x)$ by a constant to make it monic provides a contradiction to the minimality of $a(x)$ and $b(x)$. Therefore, the minimal polynomial is unique.

Next, we assume $m_{\beta, F}(x)$ has degree d and is not irreducible. In this case, $m_{\beta, F}(x) = a(x)b(x)$ with $\deg(a(x)), \deg(b(x)) \in \{1, \dots, d-1\}$. Since either $a(\beta) = 0$ or $b(\beta) = 0$, assume wlog that $a(\beta) = 0$. But, then $a(x)$ contradicts the minimal degree of $m_{\beta, F}(x)$. \square

Theorem 2.27. *The minimal polynomial of $\beta \in K$ w.r.t. \mathbb{F}_q satisfies $m_{\beta, \mathbb{F}_q}(\beta^{q^j}) = 0$ for all $j \in \mathbb{N}$. Therefore, it is given by*

$$m_{\beta, \mathbb{F}_q}(x) \triangleq \prod_{\alpha \in C_{\beta, \mathbb{F}_q}} (x - \alpha) = \prod_{i=0}^{d-1} (x - \beta^{q^i}),$$

where $d = \deg(m_{\beta, \mathbb{F}_q}(x))$ is the smallest positive integer such that $\beta^d = \beta$.

Proof. For the first statement, let $m_{\beta, \mathbb{F}_q}(x) = \sum_{i=0}^{d'} a_i x^i$ with $a_i \in \mathbb{F}_q$ and use Lemma 2.20 to write

$$[m_{\beta, \mathbb{F}_q}(x)]^{q^j} = \sum_{i=0}^{d'} a_i^{q^j} x^{q^j i} = \sum_{i=0}^{d'} a_i x^{q^j i},$$

where $a_i^{q^j} = a_i^{q^{j-1}} = \dots = a_i$ because $a_i \in \mathbb{F}_q$. Therefore,

$$0 = [m_{\beta, \mathbb{F}_q}(\beta)]^{q^j} = m_{\beta, \mathbb{F}_q}(\beta^{q^j}).$$

From the first statement, we see that $m_{\beta, \mathbb{F}_q}(x)$ must have roots at β^{q^j} for all $j \in \mathbb{N}$. But, the distinct elements in this sequence are given by the first d elements. Therefore, the given formula constructs the minimal degree polynomial with these d roots. Finally, the resulting polynomial must be the minimal polynomial because it is monic, it is zero at $x = \beta$, and it has minimum degree. \square

It turns out that a polynomial has all of its coefficients in a subfield iff evaluation commutes with conjugation in the following sense.

Lemma 2.28. *A polynomial $a(x) \in K[x]$ with $\deg(a(x)) < Q - 1$ has all coefficients in the subfield $\mathbb{F}_q \subset K$ iff $[a(x)]^q = a(x^q)$ for all $x \in K$.*

Proof. First, we show that, if $a(x) \in \mathbb{F}_q[x]$, then $[a(x)]^q = a(x^q)$ for all x (i.e., in any field containing \mathbb{F}_q). To see this, we use Lemma 2.20 to write

$$[a(x)]^q = \left[\sum_{i=0}^n a_i x^i \right]^q = \sum_{i=0}^n a_i^q x^{qi} = \sum_{i=0}^n a_i (x^q)^i = a(x^q)$$

and observe that this holds for all x because $a_i^q = a_i$ for all $a_i \in \mathbb{F}_q$. On the other hand, if $\deg(a(x)) < Q - 1$ and $[a(x)]^q = a(x^q)$ for all $x \in K$, then we can show $a_i^q = a_i$. To do this, we let α be primitive in K and express a_k in terms of the Fourier transform with

$$\sum_{j=0}^{Q-2} a(\alpha^{-j})\alpha^{jk} = \sum_{i=0}^{Q-2} a_i \sum_{j=0}^{Q-2} \alpha^{j(k-i)} = \sum_{i=0}^{Q-2} a_i(Q-1)\delta_{i,k} = (Q-1)a_k,$$

where $\delta_{i,k}$ is the Kronecker delta because $\sum_{j=0}^{Q-2} \alpha^{j(k-i)} = \frac{\alpha^{(Q-1)(k-i)} - 1}{\alpha^{(k-i)} - 1} = 0$ if $k \not\equiv i \pmod{Q-1}$. Since $q = p^d$ for some integer d and $Q = q^m$, it follows that

$$(Q-1) \pmod{\text{char}(K)} = (Q-1) \pmod{p} = (p^{md} - 1) \pmod{p} = p - 1.$$

Therefore, $(p-1)(Q-1) \pmod{p} = (p^{md+1} - p - p^{md} + 1) \pmod{p} = 1$. Now, we use Lemma 2.20 to write

$$\begin{aligned} (a_k)^q &= \left((p-1) \sum_{j=0}^{Q-2} a(\alpha^{-j})\alpha^{jk} \right)^q = (p-1) \sum_{j=0}^{Q-2} [a(\alpha^{-j})]^q \alpha^{jkq} \\ &= (p-1) \sum_{j=0}^{Q-2} a(\alpha^{-qj}) \left(\sum_{i=0}^{Q-2} a_i \alpha^{-ji} \right)^q \alpha^{jkq} = (p-1) \sum_{j=0}^{Q-2} \sum_{i=0}^{Q-2} a_i \alpha^{-jiq} \alpha^{jkq} \\ &= (p-1) \sum_{i=0}^{Q-2} a_i \sum_{j=0}^{Q-2} \alpha^{qj(k-i)} = (p-1) \sum_{i=0}^{Q-2} a_i(Q-1)\delta_{i,k} = a_k. \end{aligned}$$

Finally, combining $a_k^q = a_k$ with $a_k \in \mathbb{F}_{q^m}$ shows that $a_k \in \mathbb{F}_q$. □