## 10.1 Existence and Uniqueness of Finite Fields

What are the basic features of finite fields?

**10.1.0 Proposition.** *For every finite field $K$, there exists a unique prime $p \in \mathbb{Z}$ such that $K$ contains a subfield isomorphic to $\mathbb{F}_p$. Moreover, $K$ is a finite extension of $\mathbb{F}_p$, and $|K| = p^n$ where $n := [K : \mathbb{F}_p]$.*

*Proof.* Every field of characteristic 0 contains a subfield isomorphic to $\mathbb{Q}$ and is thereby infinite. Thus, the field $K$ has characteristic $p$ for some prime $p \in \mathbb{Z}$. It follows that the ideal $\langle p \rangle$ in the ring $\mathbb{Z}$ is the kernel of the unique ring homomorphism from $\mathbb{Z}$ to $K$. By the First Isomorphism Theorem, the field $K$ contains a subring/subfield isomorphic to $\mathbb{F}_p := \mathbb{Z}/\langle p \rangle$.

The map $\mathbb{F}_p$ makes $K$ an extension field of $\mathbb{F}_p$. Following our usual practice, we identify $\mathbb{F}_p$ is its image and write $\mathbb{F}_p \subseteq K$. Now consider $K$ as an $\mathbb{F}_p$-vector space. The elements of $K$ give finitely many vector in $K$, whose space over $\mathbb{F}_p$ is obviously $K$. It follows that $K$ is a finite-dimensional $\mathbb{F}_p$-vector space, which means that $K$ is a finite field extension of $\mathbb{F}_p$. Furthermore, if $n := [K : \mathbb{F}_p]$, then there exists a basis $\alpha_1, \alpha_2, \dots, \alpha_n$ of $K$ over $\mathbb{F}_p$. Hence, for each $\beta \in K$, there exists $a_1, a_2, \dots, a_n \in \mathbb{F}_p$ such that $\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Since the $a_j$ can be any of the $p$ elements in $\mathbb{F}_p$, there are $p^n$ possibilities for $\beta$, and $|K| = p^n$. □

**10.1.1 Theorem.** *For any finite field $K$ with $q := p^n$ elements, we have*

- *$\alpha^n = \alpha$ for all $\alpha \in K$,*
- *$x^q - x = \prod_{\alpha \in K}(x - \alpha)$, and*
- *the field $K$ is a splitting field over $\mathbb{F}_p$ for $x^q - x \in \mathbb{F}_p[x]$.*

*Proof.* Since $K$ has $q$ elements, its multiplicative group $K^\times := K \setminus \{0\}$ is a group with $q-1$ elements. It follows that $\alpha^{q-1} = 1$ for all $\alpha \in K^\times$, so $\alpha^q = \alpha$ for all $\alpha \in K$. This proves the first part and shows that the $q$ elements of $K$ are roots of $x^q - x$. The second part follows because $x^q - x$ is monic of degree $q$. Hence, $x^q - x$ splits completely over $K$. Since every element of $K$ is a root, $x^q - x$ cannot splite complete over any strictly smaller field. Therefore, $K$ is the splitting field of $x^q - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. □

**10.1.2 Corollary.** *Two finite fields with the same number of elements are isomorphic.*

*Proof.* Let $q$ be the number of elements in a finite field $K$. By the previous theorem, $K$ is the splitting field of $x^q - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Since any two splitting fields of $x^q - x \in \mathbb{F}_p[x]$ are isomorphic, the claim follows. □

**10.1.3 Theorem.** *Given any prime $p \in \mathbb{Z}$ and any positive $n \in \mathbb{Z}$, there exists a finite field with $p^n$ elements.*

*Proof.* Fix $q := p^n$. Let $L$ be a field extension of $\mathbb{F}_p$ such that $x^q - x$ splits completely over $L$. Being in characteristic $p$, the derivative of

Copyright © 2026 by Gregory G. Smith

$x^q - x$ is $-1$, so $\gcd(x^q - x, (x^q - x)') = 1$. Thus, $x^q - x$ is separable and hence has distinct roots in $L$. This means that $K = \{\alpha \in L \mid \alpha^q = \alpha\}$ is a subset $L$ consisting of $q$ elements. For all $\alpha, \beta \in K$, we have

$$(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta\,, \quad (\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta\,, \qquad 1^q = 1\,,$$
$$(-\alpha)^q = (-1)^q\alpha^q = -\alpha\,, \qquad (\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}\,.$$

It follows that $K$ is a finite field with $q := p^n$ elements. □

**10.1.4 Corollary.** *For any nonconstant $f \in \mathbb{F}_p[x]$ and every positive $n \in \mathbb{Z}$, the number of roots of $f$ in $\mathbb{F}_{p^n}$ is the degree of the polynomial* $\gcd(f, x^{p^n} - x)$.

The algebraic closure of $\mathbb{F}_p$ is the field containing all roots of all polynomials of $\mathbb{F}_p$. Equivalently, we have

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}\,.$$

*Proof.* Set $q := p^n$ and let $g := \gcd(f, x^q - x)$. The Euclidean algorithm returns the same $g$ even if one replaces $\mathbb{F}_p$ with any larger field. Thus, we may compute the greatest common divisor in $\mathbb{F}_q[x]$. Since $x^q - x = \prod_{\alpha\in\mathbb{F}_q}(x - \alpha)$, it follows that $g$ is the product of the linear factors $x - \alpha$ that divide $f$. Since $x - \alpha$ divides $f$ if and only if $f(\alpha) = 0$, we obtain

$$g = \prod_{f(\alpha)=0} (x - \alpha)\,. \qquad \square$$

**10.1.5 Remark.** Consider $f = x^{11} + x^5 + 2x + 1 \in \mathbb{F}_7[x]$. Using *Macaulay2*, we observe that

$$\gcd(f, x^{7^3} - x) = x^3 - 3x^2 + x - 1\,,$$
$$\gcd(f, x^{7^8} - x) = x^8 + 3x^7 + x^6 + x^5 - 2x^4 + x^3 - 3x - 1\,,$$

so $f$ has three roots in $\mathbb{F}_{7^3}$ and eight roots in $\mathbb{F}_{7^8}$.

**10.1.6 Remark.** A field $K$ is *perfect* if the following equivalent conditions holds:

**(a)** Every irreducible polynomial over $K$ has no multiple roots in any field extension $K \subseteq L$.
**(b)** Every irreducible polynomial over $K$ has nonzero derivative.
**(c)** Every irreducible polynomial over $K$ is separable.
**(d)** Every finite extension of $K$ is separable.
**(e)** Every algebraic extension of $K$ is separable.
**(f)** Either $K$ has characteristic 0, or, when $K$ has positive characteristic $p$, every element of $K$ is a $p$th power.

Otherwise, $K$ is called *imperfect*.

Examples of perfect fields are

- Every field of characteristic zero, so $\mathbb{Q}$ and its finite extensions, as well as $\mathbb{R}$ and $\mathbb{C}$;
- Every finite field $\mathbb{F}_q$;
- Every algebraically closed field;
- The union of a set of perfect fields totally ordered by extension;
- Fields algebraic over a perfect field.

In many contexts, essentially all the fields that one encounters are perfect. Every imperfect field is necessarily transcendental over its prime subfield.

Copyright © 2026 by Gregory G. Smith

## 10.2 Galois Groups of Finite Fields

Can we describe the Galois correspondence over every finite field? We start by identifying the Galois group.

**10.2.0 Theorem.** *Let $p \in \mathbb{Z}$ be a positive prime and let $q := p^n$ for some positive $n \in \mathbb{N}$. The field extension $\mathbb{F}_p \subseteq \mathbb{F}_q$ is Galois of degree $n$, and the Frobenius map $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$, defined by $\alpha \mapsto \alpha^p$ for all $\alpha \in \mathbb{F}_q$, is an automorphism of $\mathbb{F}_q$ that restricts to the identity on $\mathbb{F}_p$. Moreover, the Frobenius map generates the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and there exists a group isomorphism*

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}\big/\langle n\rangle$$

*that sends $\varphi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ to the class $[1] \in \mathbb{Z}\big/\langle n\rangle$.*

*Proof.* Since the finite field $\mathbb{F}_q$ is the splitting field of the separable polynomial $x^q - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$, the field extension $\mathbb{F}_p \subseteq \mathbb{F}_q$ is Galois. We also have $[\mathbb{F}_q : \mathbb{F}_{!p}] = n$ because $q = p^n$.

In characteristic $p > 0$, the map $\varphi$ is a ring homomorphism. Since $0 = \varphi(\alpha) = \alpha^p$ implies that $\alpha = 0$, the Frobenius map is injective. As $|\mathbb{F}_q| < \infty$, the Frobenius map is also surjective and thereby an automorphism of $\mathbb{F}_q$. By Fermat's little theorem, the Frobenius map restricts to the identity on $\mathbb{F}_p$, so $\varphi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Since $\mathbb{F}_p \subseteq \mathbb{F}_q$ is Galois, we have $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = n$. It follows that the order of $\varphi$ divides $n$. Suppose that $\varphi^m = \mathrm{id}_{\mathbb{F}_q}$ where $0 < m < n$. Hence, we obtain

$$\varphi^m(\alpha) = \varphi^{m-1}(\alpha^p) = \cdots = \varphi(\alpha^{p^{m-1}}) = \alpha^{p^m}\,.$$

Thus, for the $m$-fold composite map $\varphi^m$ to be the identity, we must have $\alpha^{p^m} = \alpha$ for all $\alpha \in \mathbb{F}_q$. However, this would imply that the polynomial $x^{p^m} - x$ of degree $p^m < p^n = q$ has $q$ roots, which is impossible. Hence, the Frobenius map $\varphi$ has order $n$ and

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}\big/\langle n\rangle\,. \qquad \square$$

We next describe the indetermediate fields.

**10.2.1 Corollary.** *Let $p \in \mathbb{Z}$ be a positive prime. For all positive integers $m$ and $n$, the field $\mathbb{F}_{p^m}$ is isomorphic to a subfield of $\mathbb{F}_{p^n}$ if and only if $m$ divides $n$.*

*Proof.* Suppose that $\mathbb{F}_{p^m}$ is isomorphic to a subfield of $\mathbb{F}_{p^n}$. Since $\mathbb{F}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, the Tower Theorem gives

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]\,m\,.$$

This shows that $m$ divides $n$.

Conversely, suppose that $m$ divides $n$. The preceeding theorem establishes that the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic of order $n$, so it has a subgroup $H$ of order $n/m$. By the Galois correspondence, the fixed field $K := \mathbb{F}_{p^n}^H$ of $H$ is a field extension $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$ satisfying

$$[K : \mathbb{F}_p] = [\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : H] = \frac{|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|}{|H|} = \frac{n}{n/m} = m\,,$$

so $|K| = p^m$. The uniqueness of finite fields implies that the subfield $K$ of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_{p^m}$. $\square$

Copyright © 2026 by Gregory G. Smith

**10.2.2 Corollary.** *For any positive integers $m$ and $n$ where $m$ divides $n$, there exists a group isomorphism*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \cong \frac{\mathbb{Z}}{\langle \frac{n}{m} \rangle}$$

*that sends the $m$-fold Frobenius map $\varphi^m \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ to the congruency class $[1] \in \mathbb{Z}\big/\langle \frac{n}{m} \rangle$.*

*Proof.* By definition, we have

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) := \left\{ \sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \mid \sigma(\alpha) = \alpha \text{ for all } \alpha \in \mathbb{F}_{p^n} \right\}.$$

Every automorphism is a power of the Frobenius map, so $\sigma = \varphi^r$ for some positive $r \in \mathbb{N}$. It follows that

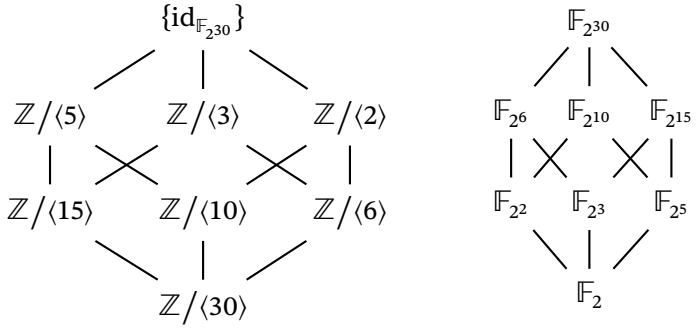
$$\varphi^r(\alpha) = \alpha \qquad \Leftrightarrow \qquad \alpha^{p^r} = \alpha\,.$$

On the other hand, the subfield $\mathbb{F}_{p^m}$ is precisely the set of roots of the polynomial $x^{p^m} - x$, so the equivalence holds if and only if $m$ divides $r$. Hence, we have $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$. Since $\varphi^n = \mathrm{id}_{\mathbb{F}_{p^n}}$, the order of $\varphi^m$ is $n/\gcd(m,n) = n/m = k$, so

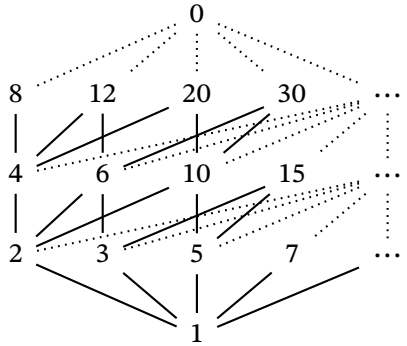
$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle \cong \frac{\mathbb{Z}}{\langle k \rangle}\,. \qquad \square$$

**10.2.3 Remark.** The subfields of the finite field $\mathbb{F}_{p^n}$ correspond to the subgroups of the cyclic group $\mathbb{Z}\big/\langle n \rangle$, whereas the subgroups of $\mathbb{Z}\big/\langle n \rangle$ correspond to positive divisors of $n$.

For the field $\mathbb{F}_{2^{30}}$, the Galois correspondence gives




**10.2.4 Remark.** For each prime $p \in \mathbb{Z}$ and any positive $n \in \mathbb{N}$, the lattice of subfields of $\mathbb{F}_{p^n}$ is isomorphic to a sublattice of the division lattice:




**10.2.5 Remark.** The *absolute Galois group* of $\mathbb{F}_p$ is

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) = \varprojlim \frac{\mathbb{Z}}{\langle n \rangle} = \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p\,.$$

No direct description is known for the absolute Galois group of the rational numbers.

Copyright © 2026 by Gregory G. Smith