4 Finite fields

Our goal in this section is to classify finite fields up to isomorphism and, given two finite fields, to describe when one of them is isomorphic to a subfield of the other. We begin with some general remarks about finite fields.

Let \( F \) be a finite field. As the additive group \((F, +)\) is finite, \( \text{char } F = p > 0 \) for some prime \( p \). Thus \( F \) contains a subfield isomorphic to the prime field \( F_p \), which we will identify with \( F_p \). Since \( F \) is finite, it is clearly a finite-dimensional vector space over \( F_p \). Let \( n = \dim_{F_p} F = [F : F_p] \). Then \( \#(F) = p^n \). It is traditional to use the letter \( q \) to denote a prime power \( p^n \) in this context.

We note that the multiplicative group \((F^{\ast}, \cdot)\) is cyclic. If \( \gamma \) is a generator, then every nonzero element of \( F \) is a power of \( \gamma \). In particular, \( F = F_p(\gamma) \) is a simple extension of \( F_p \).

With \( \#(F) = p^n = q \) as above, by Lagrange’s theorem, since \( F^{\ast} \) is a finite group of order \( q - 1 \), for every \( \alpha \in F^{\ast} \), \( \alpha^{q-1} = 1 \). Hence \( \alpha^q = \alpha \) for all \( \alpha \in F \), since clearly \( 0^q = 0 \). Thus every element of \( F \) is a root of the polynomial \( x^q - x \). (Warning: although \( \alpha^q = \alpha \) for every \( \alpha \in F \), it is not true that \( x^q - x \in F[x] \) is the zero polynomial.)

Define the function \( \sigma_p : F \to F \) by: \( \sigma_p(\alpha) = \alpha^p \). Since \( \text{char } F = p \), the function \( \sigma_p \) is a homomorphism, the Frobenius homomorphism. Clearly \( \ker \sigma_p = \{0\} \) since \( \alpha^p = 0 \iff \alpha = 0 \), and hence \( \sigma_p \) is injective. (In fact, by a HW problem, this is always true for homomorphisms from a field to a nonzero ring.) As \( F \) is finite, since \( \sigma_p \) is injective, it is also surjective and hence an isomorphism (by the pigeonhole principle). Thus, every element of \( F \) is a \( p^{\text{th}} \) power, so that \( F \) is perfect as previously defined. Note that every power \( \sigma_p^k \) is also an isomorphism. We have

\[
\sigma_p^2(\alpha) = \sigma_p(\sigma_p(\alpha)) = \sigma_p(\alpha^p) = (\alpha^p)^p = \alpha^{p^2},
\]
and so $\sigma_p^2 = \sigma_{p^2}$, where by definition $\sigma_{p^2}(\alpha) = \alpha^{p^2}$. An easy induction shows that $\sigma_p^k = \sigma_{p^k}$, where by definition $\sigma_{p^k}(\alpha) = \alpha^{p^k}$. Clearly, the result holds for $k = 1$ since both sides are then $\sigma_p$. Assuming the result inductively for a positive integer $k$, we have

$$\sigma_p^{k+1}(\alpha) = \sigma_p(\sigma_p^k(\alpha)) = (\alpha^{p^k})^p = \alpha^{p^{k+1}} = \sigma_{p^{k+1}}(\alpha).$$

In particular, taking $k = n$, where $\#(\mathbb{F}) = q = p^n$, we see that $\sigma_q(\alpha) = \alpha^q = \alpha$. Thus $\sigma_q = Id$.

More generally, for every positive integer $r$, we can define $\sigma_r : \mathbb{F} \rightarrow \mathbb{F}$ by: $\sigma_r(\alpha) = \alpha^r$. Then the same induction argument shows that $\sigma_q^k = \sigma_{r^k}$.

(However, $\sigma_r$ is a ring homomorphism $\iff r$ is a power of $p$.)

With this said, we can now state the classification theorem for finite fields:

**Theorem 4.1 (Classification of finite fields).** Let $p$ be a prime number.

(i) For every $n \in \mathbb{N}$, there exists a field $\mathbb{F}_q$ with $q = p^n$ elements.

(ii) If $\mathbb{F}$ and $\mathbb{F}'$ are two finite fields, then $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic $\iff \#(\mathbb{F}) = \#(\mathbb{F}')$.

(iii) Let $\mathbb{F}$ and $\mathbb{F}'$ be two finite fields, with $\#(\mathbb{F}) = q = p^n$ and $\#(\mathbb{F}') = q' = p^{n'}$. Then $\mathbb{F}'$ is isomorphic to a subfield of $\mathbb{F}$ $\iff m$ divides $n$ $\iff q = (q')^d$ for some positive integer $d$.

**Proof.** First, we prove (i). Viewing the polynomial $x^q - x$ as a polynomial in $\mathbb{F}_p[x]$, we know that there exists an extension field $E$ of $\mathbb{F}_p$ such that $x^q - x$ is a product of linear factors in $E[x]$, say

$$x^q - x = (x - \alpha_1) \cdots (x - \alpha_q)$$

where the $\alpha_i \in E$. We claim that the $\alpha_i$ are all distinct: $\alpha_i = \alpha_j$ for some $i \neq j$ $\iff x^q - x$ has a multiple root in $E$ $\iff x^q - x$ and $D(x^q - x)$ are not relatively prime in $\mathbb{F}_p[x]$. But $D(x^q - x) = qx^{q-1} - 1 = -1$, since $q$ is a power of $p$ and hence divisible by $p$. Thus the gcd of $x^q - x$ and $D(x^q - x)$ divides $-1$ and hence is a unit, so that $x^q - x$ and $D(x^q - x)$ are relatively prime. It follows that $x^q - x$ does not have any multiple roots in $E$.

Now define the subset $\mathbb{F}_q$ of $E$ by

$$\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\} = \{\alpha \in E : \alpha^q - \alpha = 0\} = \{\alpha \in E : \sigma_q(\alpha) = \alpha\}.$$

By what we have seen above, $\#(\mathbb{F}_q) = q$. Moreover, we claim that $\mathbb{F}_q$ is a subfield of $E$, and hence is a field with $q$ elements. Clearly $1 \in \mathbb{F}_q$. 

and more generally $\mathbb{F}_p \subseteq \mathbb{F}_q$. It suffices to show that $\mathbb{F}_q$ is closed under addition, subtraction, multiplication, and division. This follows since $\sigma_q$ is a homomorphism: If $\alpha, \beta \in \mathbb{F}_q$, i.e. if $\alpha^q = \alpha$ and $\beta^q = \beta$, then $(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta$. Similarly, $(\alpha \beta)^q = \alpha^q \beta^q = \alpha \beta$, and, if $\beta \neq 0$, then $(\alpha/\beta)^q = \alpha^q / \beta^q = \alpha / \beta$. In other words, then $\alpha \pm \beta, \alpha \beta$, and (for $\beta \neq 0$) $\alpha/\beta$ are all in $\mathbb{F}_q$. Hence $\mathbb{F}_q$ is a subfield of $E$, and in particular it is a field with $q$ elements. (Remark: $\mathbb{F}_q$ is the fixed field of $\sigma_q$, i.e. $\mathbb{F} = \{ \alpha \in E : \sigma_q(\alpha) = \alpha \}$.)

Next we prove (iii) in the special case that $\mathbb{F} = \mathbb{F}_q$. More generally, let $\mathbb{F}$ and $\mathbb{F}'$ be two finite fields with $\#(\mathbb{F}) = q = p^n$ and $\#(\mathbb{F}') = q' = p^m$. Clearly, if $\mathbb{F}'$ is isomorphic to a subfield of $\mathbb{F}$, which we can identify with $\mathbb{F}'$, then $\mathbb{F}$ is an $\mathbb{F}'$-vector space. Since $\mathbb{F}$ is finite, it is finite-dimensional as an $\mathbb{F}'$-vector space. Let $d = \dim_{\mathbb{F}'} \mathbb{F} = [\mathbb{F} : \mathbb{F}']$. Then $p^n = q = \#(\mathbb{F}) = (q')^d = p^{md}$, proving that $m$ divides $n$ and that $q$ is a power of $q'$. Conversely, suppose that $\mathbb{F}_q$ is the finite field with $q = p^n$ elements constructed in the proof of (i), so that $x^q - x$ factors into linear factors in $\mathbb{F}[x]$. Let $\mathbb{F}'$ be a finite field with $\#(\mathbb{F}') = q' = p^m$ and suppose that $q = p^n = (q')^d$, or equivalently $n = md$. We shall show first that $\mathbb{F}_q$ contains a subfield isomorphic to $\mathbb{F}'$ and then that every field with $q$ elements is isomorphic to $\mathbb{F}_q$, proving the converse part of (iii) as well as (ii).

As we saw in the remarks before the statement of Theorem 4.1, there exists a $\beta \in \mathbb{F}'$ such that $\mathbb{F}' = \mathbb{F}_p(\beta)$. Since $\beta \in \mathbb{F}'$, $\sigma_q(\beta) = \beta^q = \beta$, and hence

$$\beta^q = \beta(q)^d = (\sigma_q)^d(\beta) = \beta.$$ 

Thus $\beta$ is a root of $x^q - x$. Hence $\text{irr}(\beta, \mathbb{F}_p)$ divides $x^q - x$ in $\mathbb{F}_p[x]$, say $x^q - x = \text{irr}(\beta, \mathbb{F}_p) \cdot h$, with $\deg h < q = \deg(x^q - x) = q$ since $\deg \text{irr}(\beta, \mathbb{F}_p) \geq 1$. On the other hand, $x^q - x$ factors into linear factors in $\mathbb{F}_q[x]$, so that there is an equality in $\mathbb{F}_q[x]$ 

$$\text{irr}(\beta, \mathbb{F}_p) \cdot h = (x - \alpha_1) \cdots (x - \alpha_q).$$

Thus, for all $i$, $\alpha_i$ is a root of either $\text{irr}(\beta, \mathbb{F}_p)$ or of $h$. But since the $\alpha_i$ are all distinct and the number of roots of $h$ is at most $\deg h < q$, at least one of the $\alpha_i$ must be a root of $\text{irr}(\beta, \mathbb{F}_p)$. Hence $\text{irr}(\alpha_i, \mathbb{F}_p)$ divides $\text{irr}(\beta, \mathbb{F}_p)$. But both $\text{irr}(\alpha_i, \mathbb{F}_p)$ and $\text{irr}(\beta, \mathbb{F}_p)$ are monic irreducible polynomials, so we must have $\text{irr}(\alpha_i, \mathbb{F}_p) = \text{irr}(\beta, \mathbb{F}_p)$. Let $f = \text{irr}(\alpha_i, \mathbb{F}_p) = \text{irr}(\beta, \mathbb{F}_p)$. Then since $\mathbb{F}' = \mathbb{F}_p(\beta)$, $e\nu_\beta$ induces an isomorphism $\widehat{e}\nu_\beta : \mathbb{F}_p[x]/(f) \cong \mathbb{F}'$. On the other hand, we have $e\nu_{\alpha_i} : \mathbb{F}_p[x] \rightarrow \mathbb{F}_q$, with $\text{Ker} e\nu_{\alpha_i} = (f)$ as well, so there is an induced injective homomorphism $\widehat{e}\nu_{\alpha_i} : \mathbb{F}_p[x]/(f) \rightarrow \mathbb{F}_q$. The situation
is summarized in the following diagram:

\[
\begin{array}{c}
\mathbb{F}_p[x]/(f) \xrightarrow{\tilde{e}v_{\alpha_i}} \mathbb{F}_q \\
\downarrow \cong \\
\mathbb{F}'
\end{array}
\]

The homomorphism \( \tilde{e}v_{\alpha_i} \circ (\tilde{e}v_{\beta})^{-1} \) is then an injective homomorphism from \( \mathbb{F}' \) to \( \mathbb{F}_q \) and thus identifies \( \mathbb{F}' \) with a subfield of \( \mathbb{F}_q \). This proves the converse direction of (iii), for the specific field \( \mathbb{F}_q \) constructed in (i), and hence for any field which is isomorphic to \( \mathbb{F}_q \).

To prove (ii), note that, if \( \mathbb{F} \) and \( \mathbb{F}' \) are isomorphic, then clearly \( \#(\mathbb{F}) = \#(\mathbb{F}') \). Conversely, suppose that \( \mathbb{F}_q \) is the specific field with \( q \) elements constructed in the proof of (i) and that \( \mathbb{F} \) is another finite field with \( q \) elements. By what we have proved so far above, since \( q = (q)^1 \), \( \mathbb{F} \) is isomorphic to a subfield of \( \mathbb{F}_q \), i.e. there is an injective homomorphism \( \rho: \mathbb{F} \rightarrow \mathbb{F}_q \). But since \( \mathbb{F} \) and \( \mathbb{F}_q \) have the same number of elements, \( \rho \) is necessarily an isomorphism, i.e. \( \mathbb{F} \cong \mathbb{F}_q \). Hence, if \( \mathbb{F}' \) is yet another field with \( q \) elements, then also \( \mathbb{F}' \cong \mathbb{F}_q \) and hence \( \mathbb{F} \cong \mathbb{F}' \), proving (ii). Finally, the converse direction of (iii) now holds for every field with \( q \) elements, since every such field is isomorphic to \( \mathbb{F}_q \).

If \( q = p^n \), we often write \( \mathbb{F}_q \) to denote any field with \( q \) elements. Since any two such fields are isomorphic, we often speak of the field with \( q \) elements.

**Remark 4.2.** Let \( q = p^n \). The polynomial \( x^q - x \) is reducible in \( \mathbb{F}_p[x] \). For example, for every \( a \in \mathbb{F}_p \), \( x - a \) is a factor of \( x^q - x \). Using Theorem 4.1, one can show that the irreducible monic factors of \( x^q - x \) are exactly the irreducible monic polynomials in \( \mathbb{F}_p[x] \) of degree \( d \), where \( d \) divides \( n \). From this, one can show the following beautiful formula: let \( N_p(m) \) be the number of irreducible monic polynomials in \( \mathbb{F}_p[x] \) of degree \( m \). Then

\[
\sum_{d|n} dN_p(d) = p^n.
\]