Classification of Finite Fields

In these notes we use the properties of the polynomial $x^{p^d} - x$ to classify finite fields. The importance of this polynomial is explained by the following basic proposition.

**Proposition 1**  Factorization of $x^{p^d} - x$ over $\mathbb{F}$

Let $\mathbb{F}$ be a finite field with $p^d$ elements, where $p$ is prime and $d \geq 1$. Then every element of $\mathbb{F}$ is a root of $x^{p^d} - x$, and hence

$$x^{p^d} - x = \prod_{a \in \mathbb{F}} (x - a).$$

**PROOF**  If $a \in \mathbb{F}$, then by Fermat’s little theorem for fields $a^{p^d} = a$, so $a$ is a root of $x^{p^d} - x$. Since $\mathbb{F}$ has $p^d$ elements, these are all of the roots of $x^{p^d} - x$, and the given factorization follows.  

This is a generalization of our previous observation that

$$x^p - x \equiv (x - 1)(x - 2)\cdots(x - p) \pmod{p}$$

for any prime $p$. Indeed, this is the special case where $d = 1$ (and hence $\mathbb{F} = \mathbb{Z}_p$).

Though $x^{p^d} - x$ factors into linear factors over $\mathbb{F}$, the same is not true over $\mathbb{Z}_p$. Instead, the factorization of $x^{p^d} - x$ in $\mathbb{Z}_p[x]$ gives us information about the minimal polynomials for elements of $\mathbb{F}$. 

Proposition 2  Minimal Polynomials for Elements of $\mathbb{F}$

Let $\mathbb{F}$ be a finite field with $p^d$ elements, where $p$ is prime and $d \geq 1$, and let

$$x^{p^d} - x = m_1(x) m_2(x) \cdots m_n(x)$$

be the factorization of $x^{p^d} - x$ into irreducible polynomials in $\mathbb{Z}_p[x]$. Then:

1. The minimal polynomial for each element of $\mathbb{F}$ is one of the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$.

2. For each $i$, the number of elements of $\mathbb{F}$ with minimal polynomial $m_i(x)$ is equal to the degree of $m_i(x)$.

PROOF Since the elements of $\mathbb{F}$ are precisely the roots of $x^{p^d} - x$, each $m_i(x)$ must have a number of roots in $\mathbb{F}$ equal to its degree. Since $m_i(x)$ is irreducible, it must be the minimal polynomial for each of these roots. ■

EXAMPLE 1  Factors of $x^9 - x$ over $\mathbb{Z}_3$

The polynomial $x^9 - x$ factors over $\mathbb{Z}_3$ as follows:

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

Thus any field with 9 elements must have the elements 0, 1, and $-1$ as well as two roots of $x^2 + 1$, two roots of $x^2 + x - 1$, and two roots of $x^2 - x - 1$. ■

EXAMPLE 2  Factors of $x^{16} - x$ over $\mathbb{Z}_2$

Over $\mathbb{Z}_2$, the polynomial $x^{16} - x$ factors into irreducible polynomials as follows:

$$x^{16} - x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Then any field $\mathbb{F}$ with 16 elements must consist of the following:

- The elements 0 and 1,
- Two roots of $x^2 + x + 1$,
- Four roots of $x^4 + x + 1$,
- Four roots of $x^4 + x^3 + 1$, and
- Four roots of $x^4 + x^3 + x^2 + x + 1$. 

In particular, $\mathbb{F}$ must have two elements of degree 1 (the prime subfield), two elements of degree 2, and twelve elements of degree 4, which are the generators for $\mathbb{F}$. ■

As we can see from these examples, Proposition 2 gives quite a lot of information about any finite field. Indeed, we are ready to prove the following part of the classification.

**Theorem 3**  Uniqueness of Finite Fields

> Any two finite fields with the same number of elements are isomorphic.

**PROOF**  Suppose that $\mathbb{F}_1$ and $\mathbb{F}_2$ are two fields with $p^d$ elements, where $p$ is prime and $d \geq 1$. Let $a$ be a generator for $\mathbb{F}_1$, and recall that $a$ must have degree $d$. By Proposition 2, the minimal polynomial $m(x)$ for $a$ must be an irreducible factor of $x^{p^d} - x$ in $\mathbb{Z}_p[x]$. Then by Proposition 2, there is at least one element $b \in \mathbb{F}_2$ whose minimal polynomial is $m(x)$. Then $b$ has degree $d$, so $b$ is a generator for $\mathbb{F}_2$, and therefore $\mathbb{F}_1$ and $\mathbb{F}_2$ are both isomorphic to $\mathbb{Z}_p[x]/(m(x))$. ■

Because of this uniqueness theorem, it is common to denote “the” finite field with $p^d$ elements as $\mathbb{F}_{p^d}$. For example, the finite field with 9 elements is usually denoted $\mathbb{F}_9$ (instead of the notation $\mathbb{Z}_3[i]$ that we have been using).

**Irreducible Polynomials**

All that remains of the classification theorem is to prove that there exists a finite field with $p^d$ elements for every prime $p$ and every $d \geq 1$. Equivalently, we must show that for every prime $p$, there exist irreducible polynomials in $\mathbb{Z}_p[x]$ of every possible degree. We will prove this using the following theorem.

**Theorem 4**  Factorization of $x^{p^d} - x$

> Let $p$ be a prime and let $d \geq 1$. Then $x^{p^d} - x$ is the product of all irreducible polynomials in $\mathbb{Z}_p[x]$ whose degree divides $d$. 

The proof of this theorem consists of two lemmas.

**Lemma 5  Irreducible Factors of** $x^{p^d} - x$

Let $p$ be a prime, let $d \geq 1$, and let $m(x)$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree $k$. Then

$$m(x) \mid x^{p^d} - x \quad \text{if and only if} \quad k \mid d.$$  

**Proof** Let $\mathbb{F}$ be the field $\mathbb{Z}_p[x]/(m(x))$, and let $a \in \mathbb{F}$ be the residue class of $x$ modulo $m(x)$. Then $m(x)$ is the minimum polynomial for $a$, so $m(x)$ divides $x^{p^d} - x$ if and only if $a$ is a root of $x^{p^d} - x$. Let $\varphi : \mathbb{F} \to \mathbb{F}$ be the Frobenius automorphism. Then

$$\varphi^d(a) = a^{p^d},$$

so $a$ is a root of $x^{p^d} - x$ if and only if $\varphi^d(a) = a$. But $a$ is a generator for $\mathbb{F}$ and $\mathbb{F}$ has $p^k$ elements, so $\varphi^d(a) = a$ if and only if $k \mid d$.  

**Lemma 6  $x^{p^d} - x$ is Square-Free**

If $p$ is prime and $d \geq 1$, then all of the irreducible factors of $x^{p^d} - x$ are distinct.

We give a direct proof of this lemma using fields. Many sources instead use the fact that a polynomial $f(x)$ is square-free if and only if $f(x)$ and its derivative $f'(x)$ have no common factor. This is fairly obvious for polynomials over $\mathbb{C}$, but it can be proven for polynomials over any field.

**Proof** Let $m(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial that divides $x^{p^d} - x$. We must prove that $m(x)^2$ does not divide $x^{p^d} - x$.

Let $k$ be the degree of $m(x)$, and note that $k \mid d$ by the previous lemma. Then

$$x^{p^d} - x = (x^{p^k} - x) g(x)$$

where $g(x)$ is the polynomial

$$g(x) = \frac{x^{p^d} - x}{x^{p^k} - x} = \frac{x^{p^d-1} - 1}{x^{p^k-1} - 1} = \sum_{i=0}^{j-1} x^{i(p^k-1)}$$
with \( j = (p^d - 1)/(p^k - 1) \). (Here we have used the formula for the sum of a geometric progression.)

Now consider the field \( \mathbb{F} = \mathbb{Z}_p[x]/(m(x)) \), whose elements are the roots of the polynomial \( x^{p^k} - x \). Since \( x^{p^k} - x \) has no repeated roots over \( \mathbb{F} \), it must be divisible by \( m(x) \) but not \( m(x)^2 \). As for \( g(x) \), let \( a \) be an element of \( \mathbb{F} \) whose minimal polynomial is \( m(x) \). By Fermat’s little theorem for fields,

\[
a^{p^d - 1} = 1
\]

and hence

\[
g(a) = \sum_{i=0}^{j-1} a^{i(p^k - 1)} = \sum_{i=0}^{j-1} 1^i = j.
\]

Since \( j = (p^d - 1)/(p^k - 1) \) is not divisible by \( p \), we have that \( g(a) \neq 0 \) in \( \mathbb{F} \), and therefore \( m(x) \) does not divide \( g(x) \). We conclude that \( x^{p^d} \) is divisible by \( m(x) \) but not \( m(x)^2 \).

**Proof of Theorem 4** By Lemma 5, the irreducible factors of \( x^{p^d} \) are precisely the irreducible polynomials in \( \mathbb{Z}_p[x] \) of degree dividing \( d \). By Lemma 6, each of these factors appears exactly once in the irreducible factorization of \( x^{p^d} - 1 \).

**Example 3** Factorization of \( x^{25} - x \) over \( \mathbb{Z}_5 \)
There are exactly five irreducible linear polynomials over \( \mathbb{Z}_5 \):

\[
x, \quad x - 1, \quad x - 2, \quad x - 3, \quad x - 4.
\]

There are also ten irreducible quadratics. In particular, since 2 is not a quadratic residue modulo 5, the polynomials

\[
x^2 - 2, \quad (x - 1)^2 - 2, \quad (x - 2)^2 - 2, \quad (x - 3)^2 - 2, \quad (x - 4)^2 - 2
\]

are irreducible in \( \mathbb{Z}_5[x] \), and since 3 is not a quadratic residue modulo 5, the polynomials

\[
x^2 - 3, \quad (x - 1)^2 - 3, \quad (x - 2)^2 - 3, \quad (x - 3)^2 - 3, \quad (x - 4)^2 - 3
\]

are irreducible in \( \mathbb{Z}_5[x] \). According to Theorem 4, the product of these fifteen polynomials is \( x^{25} - x \).

**Example 4** Factorization of \( x^{81} - x \) over \( \mathbb{Z}_3 \)
Since \( 81 = 3^4 \), Theorem 4 tells us that \( x^{81} - x \) should be the product in \( \mathbb{Z}_3[x] \) of all irreducible polynomials of degree 1, 2, or 4. As we have seen, there are three
irreducible linear polynomials and three irreducible quadratic polynomials over $\mathbb{Z}_3$, with their product being $x^9 - x$:

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

Then

$$\frac{x^{81} - x}{x^9 - x} = x^{72} + x^{64} + x^{56} + x^{48} + x^{40} + x^{32} + x^{24} + x^{16} + x^{8} + 1$$

should be the product of all irreducible polynomials of degree 4 in $\mathbb{Z}_3[x]$. Since $72/4 = 18$, there are 18 such polynomials.

It follows from this that the field $\mathbb{F}_{81}$ with 81 elements has 3 elements of degree 1 (the prime subfield), 6 elements of degree 2, and 72 elements of degree 4, which are the generators for $\mathbb{F}_{81}$. ■

One quick corollary to Theorem 4 is the following.

**Corollary 7** Degrees of Elements of $\mathbb{F}_{p^d}$

> Let $\mathbb{F}$ be a field with $p^d$ elements, where $p$ is prime and $d \geq 1$. Then the degree of every element of $\mathbb{F}$ is a divisor of $d$.

**PROOF** By Theorem 4, every irreducible factor of $x^{p^d} - x$ has degree dividing $d$, and by Proposition 2 these are precisely the minimal polynomials for the elements of $\mathbb{F}_{p^d}$.

Indeed, there is a nice characterization of degrees in terms of the Frobenius automorphism.

**Corollary 8** Degrees and the Frobenius Automorphism

> Let $\mathbb{F}$ be a finite field, let $a \in \mathbb{F}$, and let $\varphi: \mathbb{F} \to \mathbb{F}$ be the Frobenius automorphism. Then the degree of $a$ is equal to the smallest positive integer $d$ for which $\varphi^d(a) = a$.

**PROOF** Let $p$ be the characteristic of $\mathbb{F}$, and let $m(x)$ be the minimal polynomial for $a$. Then the degree of $a$ is equal to the degree of $m(x)$, which by Theorem 4 is
the smallest value of \(d\) for which \(m(x) \mid x^{p^d} - x\). But \(m(x) \mid x^{p^d} - x\) if and only if \(a\) is a root of \(x^{p^d} - x\), i.e. if and only if \(\varphi^d(a) = a\). ■

We are finally ready to prove the existence of finite fields.

**Theorem 9  Existence of Finite Fields**

Let \(p\) be a prime and let \(d \geq 1\). Then there exists an irreducible polynomial in \(\mathbb{Z}_p[x]\) of degree \(d\), and hence there exists a finite field with \(p^d\) elements.

**PROOF** Suppose to the contrary that there are no irreducible polynomials in \(\mathbb{Z}_p[x]\) of degree \(d\). Then every irreducible factor of \(x^{p^d} - x\) must have degree less than \(d\), so \(x^{p^d} - x\) must divide the product

\[
\prod_{k=0}^{d-1} (x^{p^k} - x).
\]

But the degree of this product is

\[
\sum_{k=0}^{d-1} p^k = \frac{p^d - 1}{p - 1} < p^d,
\]

a contradiction. Thus there is at least one irreducible polynomial of degree \(d\). ■

**Quadratic Reciprocity**

As an application of finite fields, we provide a proof of quadratic reciprocity using Gauss sums. Really the only result about finite fields that we need is the following.

**Proposition 10  Existence of Roots of Unity**

Let \(p\) be a prime, and let \(n\) be a positive integer not divisible by \(p\). Then there exists a finite field \(\mathbb{F}\) of characteristic \(p\) that has an element of order \(n\).

**PROOF** Since \(p\) and \(n\) are relatively prime, there exists a \(d \geq 1\) so that

\[
p^d \equiv 1 \pmod{n}.
\]
Then \( n \) divides \( p^d - 1 \), so the field with \( p^d \) elements has an element of order \( n \).

For any prime \( q \), let \( g_q(x) \) be the Gauss polynomial

\[
g_q(x) = \sum_{k=1}^{q-1} \left( \frac{k}{q} \right) x^k.
\]

Recall that

\[
g_q(\omega)^2 = \left( \frac{-1}{q} \right) q
\]

for any primitive \( q \)th root of unity \( \omega \) in \( \mathbb{C} \), and

\[
g_q(\omega^k) = \left( \frac{k}{q} \right) g_q(\omega)
\]

for all \( k \in \{1, \ldots, q-1\} \). We wish to prove that \( g_q(x) \) has the same properties over any field.

**Proposition 11  Gauss Sums Over a Field**

Let \( \mathbb{F} \) be a field, let \( q > 2 \) be a prime, and let \( \omega \) be an element of order \( q \) in \( \mathbb{F} \). Then

\[
g_q(\omega)^2 = \left( \frac{-1}{q} \right) q
\]

in \( \mathbb{F} \). Moreover,

\[
g_q(\omega^k) = \left( \frac{k}{q} \right) g_q(\omega)
\]

in \( \mathbb{F} \) for all \( k \in \{1, \ldots, q-1\} \).

**PROOF**  Consider the polynomials

\[
f(x) = g_q(x)^2 - \left( \frac{-1}{q} \right) q \quad \text{and} \quad h_k(x) = g_q(x^k) - \left( \frac{k}{q} \right) g_q(x),
\]

where \( k \in \{1, \ldots, q-1\} \). Every primitive \( q \)th root of unity in \( \mathbb{C} \) is a root of \( f(x) \) as well as each \( h_k(x) \), which means that the \( q \)th cyclotomic polynomial \( \Phi_q(x) \) divides \( f(x) \) as well as each \( h_k(x) \).

Now, since \( \Phi_q(x) \) is monic, the quotients \( f(x)/\Phi_q(x) \) and \( h_k(x)/\Phi_q(x) \) have integer coefficients. It follows that \( \Phi_q(x) \) divides \( f(x) \) and each \( h_k(x) \) over any field \( \mathbb{F} \). In particular, if \( \omega \) is an element of a field \( \mathbb{F} \) with order \( q \), then \( \omega \) must be a root of \( \Phi_q(x) \) in \( \mathbb{F} \), so \( f(\omega) = 0 \) and \( h_k(\omega) = 0 \) for all \( k \in \{1, \ldots, q-1\} \).
**Theorem 12  Quadratic Reciprocity**

Let $2 < p < q$ be primes, and let

$$q^* = \left(\frac{-1}{q}\right).$$

Then $q^*$ is a quadratic residue modulo $p$ if and only if $p$ is a quadratic residue modulo $q$.

**PROOF**  Let $\mathbb{F}$ be a field of characteristic $p$ that has an element $\omega$ of order $q$, and let $r = g_q(\omega)$. By the previous proposition, $r^2 = q^*$. Then $q^*$ is a quadratic residue modulo $p$ if and only if $r \in \mathbb{Z}_p$.

Let $\varphi: \mathbb{F} \to \mathbb{F}$ be the Frobenius automorphism, and recall that $r \in \mathbb{Z}_p$ if and only if $\varphi(r) = r$. But

$$\varphi(r) = \varphi(g_q(\omega)) = g_q(\varphi(\omega)) = g_q(\omega^p) = \left(\frac{p}{q}\right) g_q(\omega) = \left(\frac{p}{q}\right) r.$$

Then $\varphi(r) = r$ if and only if $\left(\frac{p}{q}\right) = 1$, so $q^*$ is a quadratic residue modulo $p$ if and only if $p$ is a quadratic residue modulo $q$. ■