Finite Fields

In these notes we discuss the general structure of finite fields. For these notes, we always let 0 denote the additive identity in a field, and we let 1 denote the multiplicative identity. We also let

$$2 = 1 + 1, \qquad 3 = 1 + 1 + 1, \qquad 4 = 1 + 1 + 1 + 1, \qquad \ldots$$

Definition: Characteristic of a Field

We say that a field $\mathbb{F}$ has **finite characteristic** if there exists a positive integer n so that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

in $\mathbb{F}$. The smallest such n is called the **characteristic** of $\mathbb{F}$, and is denoted $\operatorname{char}(\mathbb{F})$.

That is, the characteristic of $\mathbb{F}$ is the smallest positive integer n for which $n = 0$ in $\mathbb{F}$. For example, $\mathbb{Z}_p$ has characteristic p for each prime p, but fields such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ do not have finite characteristic.

Proposition 1

Every finite field has finite characteristic

PROOF Let $\mathbb{F}$ be a finite field. Then the sequence $1, 2, 3, \ldots$ in $\mathbb{F}$ has only finitely many different terms, so there must exist positive intgers $m < n$ such that $m = n$ in $\mathbb{F}$. It follows that $n - m = 0$ in $\mathbb{F}$, so $\mathbb{F}$ has finite characteristic. ■

If $\mathbb{F}$ is a field of characteristic n, then the elements $\{0, 1, 2, \ldots, n-1\}$ of $\mathbb{F}$ obey the rules for addition and multiplication modulo n, and therefore form a copy of

$\mathbb{Z}_n$ inside of $\mathbb{F}$. Since $\mathbb{Z}_n$ has zero divisors when n is not prime, it follows that **the characteristic of a field must be a prime number**.

Thus every finite field $\mathbb{F}$ must have characteristic p for some prime p, and the elements $\{0, 1, 2, \ldots, p-1\}$ form a copy of $\mathbb{Z}_p$ inside of $\mathbb{F}$. This copy of $\mathbb{Z}_p$ is known as the **prime subfield** of $\mathbb{F}$.

EXAMPLE 1 Prime Subfield of $\mathbb{Z}_3[i]$

Recall that $\mathbb{Z}_3[i] = \mathbb{Z}_3[x]/\big(x^2+1\big)$ is a field with 9 elements:

$$0, \quad 1, \quad 2, \quad i, \quad i+1, \quad i+2, \quad 2i, \quad 2i+1, \quad 2i+2.$$

This field has characteristic 3, since $3 = 0$ in the field, and the prime subfield consists of the elements $\{0, 1, 2\}$. ■

More generally, if p is a prime and $m(x)$ is an irreducible polynomial over $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/\big(m(x)\big)$ is always a field of characteristic p, with prime subfield $\{0, 1, \ldots, p-1\}$.

The Frobenius Automorphism

We begin with a surprising identity that holds in any field of characteristic p.

Proposition 2 The Frobenius Identity

Let p be a prime, and let $\mathbb{F}$ be a field of characteristic p. Then

$$(a+b)^p \;=\; a^p + b^p$$

for all $a, b \in \mathbb{F}$.

PROOF By the binomial theorem

$$(a+b)^p \;=\; a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

But it is easy to see that $\binom{p}{k}$ is a multiple of p for all $k \in \{1, \ldots, p-1\}$, and is hence equal to 0 in $\mathbb{F}$. Thus all the middle terms drop out, leaving $(a+b)^p = a^p + b^p$. ■

Definition: Frobenius Automorphism
Let $\mathbb{F}$ be a field of characteristic p. The **Frobenius automorphism** of $\mathbb{F}$ is the function $\varphi\colon \mathbb{F} \to \mathbb{F}$ defined by
$$\varphi(a) = a^p.$$

Clearly $\varphi(ab) = \varphi(a)\,\varphi(b)$ for all $a, b \in \mathbb{F}$, and the Frobenius identity tells us that $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in \mathbb{F}$. It follows that φ can be applied to *any* expression by applying it to each part individually. For example, if $a, b, c \in \mathbb{F}$, then

$$\varphi\big(a^3 + b^2c\big) = \varphi(a)^3 + \varphi(b)^2\varphi(c).$$

Note that the properties of φ are similar to the properties of complex conjugation in $\mathbb{C}$. In particular, if $\overline{a}$ denotes the complex conjugate of a, then

$$\overline{ab} = \overline{a}\overline{b} \qquad \text{and} \qquad \overline{a+b} = \overline{a} + \overline{b}$$

for all $a, b \in \mathbb{C}$. Thus the Frobenius automorphism φ can be thought of as something similar to complex conjugation for finite fields.

EXAMPLE 2 The Frobenius Automorphism in $\mathbb{Z}_p[i]$
Recall that if p is a prime congruent to 3 modulo 4, then the field with p^2 elements can be described as $\mathbb{Z}_p[i]$, where i is a square root of -1. Let $\varphi\colon \mathbb{Z}_p[i] \to \mathbb{Z}_p[i]$ be the Frobenius automorphism. By Fermat's little theorem

$$\varphi(a) = a^p = a$$

for all $a \in \mathbb{Z}_p$. Moreover, we have

$$\varphi(i) = i^p = i^3 = -i.$$

It follows that
$$\varphi(a+bi) = \varphi(a) + \varphi(b)\,\varphi(i) = a - bi$$

for all $a, b \in \mathbb{Z}_p$. Thus the Frobenius automorphism is exactly the same as complex conjugation for this field. ■

EXAMPLE 3 The Frobenius Automorphism in $\mathbb{F}_4$
Let $\mathbb{F}_4 = \mathbb{Z}_2[x]/\big(x^2+x+1\big)$ be the field with 4 elements, and let $\varphi\colon \mathbb{F}_4 \to \mathbb{F}_4$ be the Frobenius automorphism $\varphi(a) = a^2$. Then

$$\varphi(0) = 0^2 = 0, \quad \varphi(1) = 1^2 = 1, \quad \varphi(x) = x^2 = x+1, \quad \varphi(x+1) = (x+1)^2 = x.$$

Thus φ fixes 0 and 1 and switches x with $x+1$. ■

EXAMPLE 4 The Frobenius Automorphism in $\mathbb{F}_8$

Let $\mathbb{F}_8 = \mathbb{Z}_2[x]/\big(x^3 + x + 1\big)$ be the field with 8 elements, and let $\varphi\colon \mathbb{F}_8 \to \mathbb{F}_8$ be the Frobenius automorphism $\varphi(a) = a^2$. Clearly $\varphi(0) = 0$ and $\varphi(1) = 1$, and it is easy to check that

$$\varphi(x) = x^2, \qquad \varphi\big(x^2\big) = x^2 + x, \qquad \varphi\big(x^2 + x\big) = x$$

and

$$\varphi(x+1) = x^2 + 1, \qquad \varphi\big(x^2+1\big) = x^2 + x + 1, \qquad \varphi\big(x^2 + x + 1\big) = x + 1.$$

Thus φ fixes 0 and 1 and permutes the remaining 6 elements of $\mathbb{F}_8$ in two three-cycles. ■

In all of these examples, the fixed points of the Frobenius automorphism were precisely the elements of the prime subfield. This is no accident.

Proposition 3 Fixed Points of the Frobenius Automorphism

Let $\mathbb{F}$ be a field of characteristic p, let φ be the Frobenius automorphism of $\mathbb{F}$, and let $a \in \mathbb{F}$. Then $\varphi(a) = a$ if and only if a lies in the prime subfield of $\mathbb{F}$.

PROOF Recall that the prime subfield of $\mathbb{F}$ is isomorphic to $\mathbb{Z}_p$, with $\varphi(a) = a^p$ for all $a \in \mathbb{F}$. By Fermat's little theorem, we know that $\varphi(a) = a^p = a$ for all elements a of the prime subfield. But every fixed point of φ must be a root of the polynomial $x^p - x$, and this polynomial can have at most p different roots in $\mathbb{F}$, so the fixed points of φ are precisely the elements $0, 1, \ldots, p-1$. ■

Again, this is analogous to complex conjugation, where the fixed points of complex conjugation are precisely the real numbers.

Orders of Elements

We collect here a few other facts about finite fields that we have collected.

Theorem 4 Fermat's Little Theorem for Finite Fields

Let $\mathbb{F}$ be a finite field with n elements. Then

$$a^n = a$$

for all $a \in \mathbb{F}$. Equivalently,

$$a^{n-1} = 1$$

for all $a \in \mathbb{F}^\times$.

PROOF The multiplicative group $\mathbb{F}^\times$ has $n-1$ elements. By Lagrange's theorem from group theory, it follows that the multiplicative order of any element of $\mathbb{F}^\times$ must divide $n-1$. Then $a^{n-1} = 1$ for all $a \in \mathbb{F}^\times$, and it follows that $a^n = a$ for all $a \in \mathbb{F}$. ■

Theorem 5 Primitive Element Theorem

Let $\mathbb{F}$ be a finite field with n elements. Then for each divisor k of $n-1$, there exist elements of $\mathbb{F}^\times$ of order k.

PROOF This was proven in the notes on cyclotomic polynomials. ■

Combining these two theorems together, we see that the orders of the elements of $\mathbb{F}$ are precisely the divisors of $n-1$.

Incidentally, we will show soon enough that every finite field with characteristic p has p^k elements for some positive integer k. Thus Fermat's little theorem for finite fields can be written as

$$a^{p^k} = a$$

for the elements of a field of order p^k. Equivalently

$$\varphi^k(a) = a$$

for all $a \in \mathbb{F}$, where φ is the Frobenius automorphism. Thus, for a field with p^k elements, every element will return to itself after k applications of the Frobenius automorphism.

Square Roots of 2

As an application of finite fields and the Frobenius automorphism, we determine for which primes p the field $\mathbb{Z}_p$ contains a square root of 2. The proof uses the field $\mathbb{F}$ with p^2 elements, which can be obtained by adjoining to $\mathbb{Z}_p$ the square root of any quadratic non-residue. That is,

$$\mathbb{F} \;=\; \mathbb{Z}_p[x]/\big(x^2 - a\big),$$

where a is any quadratic non-residue modulo p.

Theorem 6 Second Supplement to the Law of Quadratic Reciprocity

Let p be an odd prime. Then 2 is a quadratic residue modulo p if and only if

$$p \;\equiv\; \pm 1 \pmod{8}.$$

PROOF Let $\mathbb{F}$ be the field with p^2 elements. Observe that

$$(-3)^2 \;\equiv\; (-1)^2 \;\equiv\; 1^2 \;\equiv\; 3^2 \;\equiv\; 1 \pmod{8},$$

so $p^2 - 1$ must be a multiple of 8, and hence $\mathbb{F}$ has an element ω of order 8. Note then that $\omega^4 = -1$.

Let $r = \omega + \omega^{-1}$. Then

$$r^2 \;=\; \big(\omega + \omega^{-1}\big)^2 \;=\; \omega^2 + 2 + \omega^{-2} \;=\; 2 + \omega^{-2}\big(\omega^4 + 1\big) \;=\; 2.$$

Thus r and $-r$ are the square roots of 2 in $\mathbb{F}$. Then 2 is a quadratic residue modulo p if and only if $r \in \mathbb{Z}_p$.

To check whether $r \in \mathbb{Z}_p$, we apply the Frobenius automorphism to r and use Proposition 3. Let $\varphi\colon \mathbb{F} \to \mathbb{F}$ be the Frobenius automorphism, which is defined by $\varphi(a) = a^p$. Then

$$\varphi(r) \;=\; \varphi\big(\omega + \omega^{-1}\big) \;=\; \varphi(\omega) + \varphi(\omega)^{-1} \;=\; \omega^p + \omega^{-p} \;=\; \omega^k + \omega^{-k},$$

where $k \in \{-3, -1, 1, 3\}$ is the residue class of p modulo 8. We now break into cases depending on the value of k:

- If $p \equiv 1 \pmod{8}$, then $\varphi(r) = \omega + \omega^{-1} = r$, so $r \in \mathbb{Z}_p$ by Proposition 3, and hence 2 is a quadratic residue modulo p.
- Similarly, if $p \equiv -1 \pmod{8}$, then $\varphi(r) = \omega^{-1} + \omega = r$, so $r \in \mathbb{Z}_p$ and hence 2 is a quadratic residue modulo p.

- If $p \equiv -3 \pmod 8$, then $\varphi(r) = \omega^{-3} + \omega^{3} = -\omega - \omega^{-1} = -r \neq r$. By Proposition 3, it follows that $r \notin \mathbb{Z}_p$ by, so 2 is not a quadratic residue modulo p.
- Finally, if $p \equiv 3 \pmod 8$, then $\varphi(r) = \omega^{3} + \omega^{-3} = -\omega^{-1} - \omega = -r \neq r$, so again 2 is not a quadratic residue modulo p. ■.