Minimal Polynomials

In these notes we continue to develop the theory of finite fields. Our main goal in this theory is to prove the following classification theorem.

Theorem Classification of Finite Fields

1. *If $\mathbb{F}$ is a finite field of characteristic p, then $|\mathbb{F}|$ is a power of p.*
2. *For every prime p and every $d \geq 1$, there exists a finite field with p^d elements.*
3. *Any two finite fields with the same number of elements are isomorphic.*

Here **isomorphic** means that two fields have the same algebraic structure. That is, fields $\mathbb{F}_1$ and $\mathbb{F}_2$ are isomorphic if there exists a bijection $\psi \colon \mathbb{F}_1 \to \mathbb{F}_2$ satisfying

$$\psi(a+b) = \psi(a) + \psi(b) \qquad \text{and} \qquad \psi(ab) = \psi(a)\,\psi(b)$$

for all $a, b \in \mathbb{F}_1$.

EXAMPLE 1 The field $\mathbb{R}[x]/\big(x^2+1\big)$ is isomorphic to the complex numbers, with the isomorphism

$$\psi \colon \mathbb{R}[x]/\big(x^2+1\big) \to \mathbb{C}$$

being the function $\psi(a+bx) = a+bi$. ■

EXAMPLE 2 Though it is not obvious, the fields

$$\mathbb{F}_1 \;=\; \mathbb{Z}_2[x]\,/\,\big(x^3+x+1\big) \qquad \text{and} \qquad \mathbb{F}_2 \;=\; \mathbb{Z}_2[y]\,/\,\big(y^3+y^2+1\big)$$

are isomorphic via the isomorphism $\psi\colon \mathbb{F}_1 \to \mathbb{F}_2$ defined as follows:

$$\psi(0) = 0 \qquad \psi(x) = y+1 \qquad \psi\bigl(x^2\bigr) = y^2+1 \qquad \psi\bigl(x^2+x\bigr) = y^2+y$$

$$\psi(1) = 1 \qquad \psi(x+1) = y \qquad \psi\bigl(x^2+1\bigr) = y^2 \qquad \psi\bigl(x^2+x+1\bigr) = y^2+y+1$$

This bijection ψ preserves all of the arithmetic operations. For example,

$$\psi\bigl(x^2\bigr) + \psi(x) \;=\; \bigl(y^2+1\bigr) + (y+1) \;=\; y^2+y \;=\; \psi\bigl(x^2+x\bigr)$$

and

$$\psi(x)\,\psi(x+1) \;=\; (y+1)(y) \;=\; y^2+y \;=\; \psi\bigl(x^2+x\bigr) \;=\; \psi\bigl(x(x+1)\bigr). \qquad \blacksquare$$

Minimal Polynomials

We begin by associating a polynomial to each element of a finite field. Our definition here is a little bit different than the one we used in class, but it is equivalent and we will end up with all the same theorems.

> **Definition: Minimal Polynomial**
> Let $\mathbb{F}$ be a finite field of characteristic p, and let $a \in \mathbb{F}$. A **minimal polynomial** for a is an irreducible polynomial $m(x) \in \mathbb{Z}_p[x]$ such that $m(a) = 0$.

Recall that irreducible polynomials are required to be monic, and therefore a minimal polynomial $m(x)$ for an element a is always a monic polynomial.

EXAMPLE 3 Consider the field $\mathbb{Z}_3[i]$, which has characteristic 3. The minimal polynomials in $\mathbb{Z}_3[x]$ for the elements $0, 1, -1 \in \mathbb{Z}_3[i]$ are respectively

$$x, \qquad x-1, \qquad \text{and} \qquad x+1,$$

and these are the only elements of $\mathbb{Z}_3[i]$ whose minimal polynomials are linear.

The minimal polynomial for i is

$$m(x) \;=\; x^2+1,$$

which is irreducible in $\mathbb{Z}_3[x]$. This is also the minimal polynomial for $-i$, and indeed x^2+1 factors into $(x-i)(x+i)$ over $\mathbb{Z}_3[i]$.

Finally, the minimal polynomial for both $1+i$ and $1-i$ is

$$m(x) \;=\; (x-1)^2+1 \;=\; x^2+x-1$$

and the minimal polynomial for both $-1+i$ and $-1-i$ is

$$m(x) \;=\; (x+1)^2+1 \;=\; x^2-x-1. \qquad \blacksquare$$

EXAMPLE 4 Let p be a prime, let $m(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial, and let $\mathbb{F}$ be the field

$$\mathbb{F} = \mathbb{Z}_p[x]/\big(m(x)\big).$$

Let a denote the residue class of x modulo $m(x)$, i.e. the element of $\mathbb{F}$ corresponding to x. Then $m(a) = 0$ in $\mathbb{F}$, so m is the minimal polynomial for a. ■

Proposition 1 Polynomials with a as a Root

Let $\mathbb{F}$ be a finite field of characteristic p, let $a \in \mathbb{F}$, and let $m(x) \in \mathbb{Z}_p[x]$ be a minimal polynomial for a. Then for all $f(x) \in \mathbb{Z}_p[x]$,

$$f(a) = 0 \qquad \textit{if and only if} \qquad m(x) \mid f(x).$$

PROOF Let $f(x) \in \mathbb{Z}_p[x]$. If $m(x) \mid f(x)$, then since $m(a) = 0$ it follows that $f(a) = 0$. For the converse, suppose that $f(a) = 0$, and suppose to the contrary that $m(x) \nmid f(x)$. Since $m(x)$ is irreducible, it follows that $m(x)$ and $f(x)$ are relatively prime, so by Bézout's lemma there exist polynomials $b(x), c(x) \in \mathbb{Z}_p[x]$ such that

$$b(x)\,f(x) + c(x)\,m(x) = 1.$$

But since $f(a) = m(a) = 0$, substituting a for x gives the equation $0 = 1$, a contradiction. We conclude that $m(x) \mid f(x)$ whenever $f(a) = 0$. ■

For example, according to this proposition, the element $i \in \mathbb{Z}_3[i]$ is a root of a polynomial $f(x) \in \mathbb{Z}_3[x]$ if and only if $x^2 + 1$ divides $f(x)$.

It follows from this proposition that the minimal polynomial $m(x)$ for a must be a polynomial of the smallest possible degree that has a as a root. This was the definition of the minimal polynomial given in class.

Corollary 2 Congruence Modulo $m(x)$

Let $\mathbb{F}$ be a finite field of characteristic p, let $a \in \mathbb{F}$, and let $m(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial for a. Then for all $f(x), g(x) \in \mathbb{Z}_p[x]$,

$$f(a) = g(a) \qquad \textit{if and only if} \qquad f(x) \equiv g(x) \pmod{m(x)}.$$

PROOF Let $h(x) = f(x) - g(x)$. Then $f(a) = g(a)$ if and only if $h(a) = 0$. By Proposition 1, this occurs if and only if $m(x)$ divides $h(x)$, i.e. if and only if

$f(x) \equiv g(x) \pmod{h(x)}$. ■

For example, if $f(x)$ and $g(x)$ are polynomials over $\mathbb{Z}_3$, then

$$f(i) = g(i) \qquad \text{if and only if} \qquad f(x) \equiv g(x) \pmod{x^2+1}.$$

Proposition 3 Existence and Uniqueness of Minimal Polynomials

Let $\mathbb{F}$ be a finite field of characteristic p, and let $a \in \mathbb{F}$. Then a has a unique minimal polynomial in $\mathbb{Z}_p[x]$.

PROOF Let $n = |\mathbb{F}|$. By Fermat's little theorem for fields, we know that $a^n = a$, and hence a is a root of the polynomial $x^n - x$. Then a must be a root of some irreducible factor of $x^n - x$, and therefore a has at least one minimal polynomial $m(x)$.

For uniqueness, suppose that $m_1(x)$ and $m_2(x)$ are minimal polynomials for a. Then by Proposition 1 we know that $m_1(x) \mid m_2(x)$ and $m_2(x) \mid m_1(x)$, and since $m_1(x)$ and $m_2(x)$ are monic it follows that $m_1(x) = m_2(x)$. ■

Generators for Fields

There is a notion of a generator for a field. This is similar to, but distinct from, the notion of a primitive element.

Definition: Generator for a Field
Let $\mathbb{F}$ be a finite field of characteristic p. An element $a \in \mathbb{F}$ is called a **generator** for $\mathbb{F}$ if the set

$$\{f(a) \mid f(x) \in \mathbb{Z}_p[x]\}$$

is equal to $\mathbb{F}$.

That is, a is a generator for $\mathbb{F}$ if every element of $\mathbb{F}$ can be written as a polynomial involving a.

EXAMPLE 5 Generators for $\mathbb{Z}_3[i]$
The element i is a generator for $\mathbb{Z}_3[i]$, since each element of $\mathbb{Z}_3[i]$ can be written as a linear polynomial $a + bi$ involving i The element $1 + i$ is also a generator for $\mathbb{Z}_3[i]$,

since

$$a + bi \;=\; b(i+1) + (a-b)$$

for any element $a + bi \in \mathbb{Z}_3[i]$.

However, 1 is not a generator for $\mathbb{Z}_3[i]$, since $f(1) \in \{0, 1, 2\}$ for any polynomial $f(x) \in \mathbb{Z}_3[x]$. Indeed, none of the elements $0, 1, 2$ of the prime subfield is a generator for $\mathbb{Z}_3[i]$, but it is possible to show that each of the remaining six elements is a generator for $\mathbb{Z}_3[i]$. ■

Proposition 4 Primitive Elements Generate

Every finite field $\mathbb{F}$ has at least one generator. In particular, any primitive element of $\mathbb{F}^\times$ is a generator for $\mathbb{F}$.

PROOF Let $\mathbb{F}$ be a finite field, and let $a \in \mathbb{F}^\times$ be a primitive element. Then every nonzero element of $\mathbb{F}$ is a power of a, and can hence be written as $f(a)$ for some polynomial $f(x) = x^k$. Finally, the element $0 \in \mathbb{F}$ can be written as $z(a)$, where $z(x)$ is the zero polynomial. ■

We now prove that the structure of a finite field can be determined from the minimal polynomial for any generator.

Theorem 5 Structure of Finite Fields

Let $\mathbb{F}$ be a finite field of characteristic p, and let a be a generator for $\mathbb{F}$. Then $\mathbb{F}$ is isomorphic to the field

$$\mathbb{Z}_p[x]\,/\,\big(m(x)\big)$$

where $m(x)$ is the minimal polynomial for a.

PROOF Let $\psi\colon \mathbb{Z}_p[x]\,/\,\big(m(x)\big) \to \mathbb{F}$ be the function

$$\psi\big(f(x)\big) \;=\; f(a).$$

That is, ψ maps the residue class of each polynomial $f(x)$ to the element $f(a) \in \mathbb{F}$. From Corollary 2, we know that

$$f(x) \;\equiv\; g(x) \;\big(\mathrm{mod}\; m(x)\big) \qquad \text{if and only if} \qquad f(a) \;=\; g(a)$$

for all $f(x), g(x) \in \mathbb{Z}_p[x]$, and thus ψ is both well-defined and one-to-one. Moreover, since a is a generator for $\mathbb{F}$, the image of ψ is all of $\mathbb{F}$, and therefore ψ is a bijection. Finally, we have

$$\psi\big(f(x) + g(x)\big) \;=\; f(a) + g(a) \;=\; \psi\big(f(x)\big) + \psi\big(g(x)\big)$$

and

$$\psi\big(f(x)\,g(x)\big) \;=\; f(a)\,g(a) \;=\; \psi\big(f(x)\big)\,\psi\big(g(x)\big)$$

for all $f(x)$ and $g(x)$, which proves that ψ is an isomorphism. ■

EXAMPLE 6 Structure of $\mathbb{Z}_3[i]$

As we have seen, the minimal polynomial for the element $i \in \mathbb{Z}_3[i]$ is

$$m(x) \;=\; x^2 + 1.$$

Since i is a generator for $\mathbb{Z}_3[i]$, it follows that $\mathbb{Z}_3[i]$ is isomorphic to $\mathbb{Z}_3[x]/\big(x^2+1\big)$.

Similarly, recall that $1 + i$ is also a generator for $\mathbb{Z}_3[i]$. The minimal polynomial for $1 + i$ is

$$m(x) \;=\; (x-1)^2 + 1 \;=\; x^2 + x - 1,$$

so it follows that $\mathbb{Z}_3[i]$ is also isomorphic to $\mathbb{Z}_3[x]/\big(x^2+x-1\big)$ ■

As a consequence of Theorem 5, we now know the possible sizes of a finite field.

Corollary 6 Sizes of Finite Fields

If $\mathbb{F}$ is a finite field of characteristic p, then $|\mathbb{F}|$ is a power of p.

PROOF Let a be a generator for $\mathbb{F}$. By Theorem 5, the field $\mathbb{F}$ is isomorphic to

$$\mathbb{Z}_p[x]/\big(m(x)\big)$$

where $m(x)$ is the minimal polynomial for a. Then $\mathbb{F}$ has p^d elements, where d is the degree of $m(x)$. ■

More About Generators

We would like to prove a few more facts about generators, which will be useful later.

Definition: Degree of an Element
Let $\mathbb{F}$ be a finite field. The **degree** of an element $a \in \mathbb{F}$ is the degree of the minimal polynomial for a.

For example, an element of $\mathbb{F}$ has degree 1 if and only if it lies in the prime subfield of $\mathbb{F}$. We can use degree to give a nice characterization of the generators of $\mathbb{F}$.

Proposition 7 Degrees of the Generators

Let $\mathbb{F}$ be a finite field with p^d elements, where p is prime and $d \geq 1$. Then the generators for $\mathbb{F}$ are precisely the elements of $\mathbb{F}$ that have degree d.

PROOF Let $a \in \mathbb{F}$, let $m(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial for a, and consider the set

$$\{f(a) \mid f(x) \in \mathbb{Z}_p[x]\}.$$

By Corollary 2, the elements of this set are in one-to-one correspondence with the elements of $\mathbb{Z}_p[x]/\big(m(x)\big)$. In particular, this set has precisely p^k elements, where k is the degree of $m(x)$. Then this set is equal to all of $\mathbb{F}$ if and only if $k = d$. ■

For example, this proposition proves our previous assertion that each of the six elements of $\mathbb{Z}_3[i]$ of degree 2 is a generator for $\mathbb{Z}_3[i]$.

Next we would like to investigate the action of the Frobenius automorphism on the generators.

Proposition 8 Periods of the Generators

Let $\mathbb{F}$ be a field with p^d elements, where p is prime and $d \geq 1$. Let a be a generator for $\mathbb{F}$, and let $\varphi\colon \mathbb{F} \to \mathbb{F}$ be the Frobenius automorphism. Then for all $n \in \mathbb{N}$,

$$\varphi^n(a) = a \qquad \text{if and only if} \qquad d \mid n.$$

PROOF It suffices to prove that $\varphi^d(a) = a$ and that $\varphi^k(a) \neq a$ for $1 \leq k < d$. The first statement follows from Fermat's little theorem for fields, since

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

To prove the second statement, suppose to the contrary that $\varphi^k(a) = a$ for some $k < d$. Then for any polynomial $f(x) \in \mathbb{Z}_p[x]$, we have

$$\varphi^k\big(f(a)\big) \;=\; f\big(\varphi^k(a)\big) \;=\; f(a).$$

Since a is a generator for $\mathbb{F}$, we conclude that $\varphi^k(b) = b$ for all $b \in \mathbb{F}$. But this is impossible, since $x^{p^k} - x$ has at most p^k different roots in $\mathbb{F}$. ∎

Incidentally, it is possible to prove that for any element a of a finite field, the degree of a is equal to the smallest positive number k for which $\varphi^k(a) = a$, but we will not need this more general version.