27 Finite Fields (continued)

Previously, we constructed the finite field $\mathbb{F}_q$ for $q = p^n$, and showed that there is a unique such field. This construction had the unusual property that the field *consisted* of exactly the roots of a polynomial (where the polynomial was $x^q - x$), rather than just being *generated* by the roots of a polynomial.

There is more that we can say about the structure of finite fields.

27.1 The Multiplicative Group

Lemma 27.1
If F is any field and G is a finite subgroup of $F^\times$, then G is cyclic.

Example 27.2
If $F = \mathbb{C}$, then finite subgroups of $F^\times$ are the nth roots of unity

$$\left\{\exp \frac{2\pi i}{n}\right\} = \langle \zeta_n \rangle \cong \mathbb{Z}/n.$$

Proof of Lemma 27.1. By the classification of finite abelian groups, we know $G \cong \prod \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ for some integers n_i. So it's enough to check that no prime appears twice (meaning that every prime appears in the list of p_i at most once). Then we can use the Chinese Remainder Theorem to show that the product is cyclic, as all the p_i are then coprime. For example, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$ is cyclic, while $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not.

But suppose p appears twice. Then G contains a subgroup $\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$. But then G has at least p^2 elements of order dividing p, since there's p choices for the coordinate in each. This would mean the polynomial $x^p - 1$ has at least p^2 roots; but it has degree p, so this is impossible. $\square$

Corollary 27.3
For any finite field $\mathbb{F}_q$, its multiplicative group $\mathbb{F}_q^\times$ is cyclic, meaning $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)$.

Note 27.4
Although we know in theory that $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)$, in practice it's hard to compute how this isomorphism works — it is difficult to find a generator, or to figure out what power to raise the generator to in order to get a given element. Many cryptography and encryption protocols are based on this.

Corollary 27.5
We have $\mathbb{F}_q \cong \mathbb{F}_p(\alpha)$, and therefore, there exists an irreducible polynomial of any degree over $\mathbb{F}_p$.

Proof. There exists $\alpha \in \mathbb{F}_q$ which generates the multiplicative group; then α must generate $\mathbb{F}_q$ as an extension of $\mathbb{F}_p$, since every element of $\mathbb{F}_q$ is a *power* of α. (The converse is false — it is possible to find α which generates the extension but not the multiplicative group.)

Then $\mathbb{F}_q = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(Q)$ where Q is the minimal polynomial of α. So Q is an irreducible polynomial of degree n, where $q = p^n$. In particular, a procedure (in theory) to find an irreducible polynomial of degree n is to write down $\mathbb{F}_{p^n}$, find a multiplicative generator, and take its minimal polynomial. $\square$

27.2 Application to Number Theory

Finite fields arise in many areas of math and computer science — in particular, in number theory. One such example is $R/(p)$, where R is the ring of algebraic integers in a finite extension of $\mathbb{Q}$.

Example 27.6
If $p \equiv 3 \pmod 4$, then $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$ — it's a field since (p) is maximal.

The example we'll focus on is the extension $\mathbb{Q}(\zeta_\ell)$, where ℓ is a prime (it's possible to consider general ℓ, but the prime case is a bit simpler). We know this extension is $\mathbb{Q}[x]/(x^{\ell-1} + \cdots + 1)$, and we can check that its ring of algebraic integers is

$$R = \mathbb{Z}[x]/(x^{\ell-1} + \cdots + 1).$$

Guiding Question
For an (integer) prime p, when is $R/(p)$ a field (or equivalently, when is (p) maximal)?

It's clear that $R/(p) \cong \mathbb{F}_p[x]/(x^{\ell-1} + \cdots + 1)$, which means its dimension over $\mathbb{F}_p$ (as a vector space) is ℓ. So if $R/(p)$ is a field, then it must be $\mathbb{F}_{p^\ell}$.

We'll assume $p \neq \ell$.

Proposition 27.7
If $p \neq \ell$, then $R/(p)$ is a field if and only if $\operatorname{ord}_{\mathbb{F}_\ell^\times} p = \ell - 1$.

Here $\operatorname{ord}_{\mathbb{F}_\ell^\times} p$ denotes the multiplicative order of p mod ℓ; in particular, $\ell - 1$ is the largest possible order, since $\mathbb{F}_\ell^\times$ has $\ell - 1$ elements.

Proof. Let $\mathfrak{m}$ be a maximal ideal of R containing (p). Then we have $R/\mathfrak{m} \cong \mathbb{F}_{p^a}$ for some a. Let the image of ζ_ℓ in $R/\mathfrak{m}$ be $\overline{\zeta}_\ell$. Then we know $\overline{\zeta}_\ell^\ell = 1$ and therefore $\overline{\zeta_\ell}$ has multiplicative order ℓ; so since the multiplicative group of $\mathbb{F}_{p^a}$ has size $p^a - 1$, we get that $\ell \mid p^a - 1$.

Now if the order of p in $\mathbb{F}_\ell^\times$ is $\ell - 1$, then we must have $a \geq \ell - 1$. But it cannot be larger than $\ell - 1$. So then $a = \ell - 1$ and $R/\mathfrak{m} \cong R/(p)$, which means $R/(p)$ is a field. The converse can be proved similarly. $\square$

Example 27.8
Suppose $p = 3$ and $\ell = 5$. Then $\operatorname{ord}_5 3 = 4$, so $R/(3)$ is a field.

27.3 Multiple Roots

In our construction of finite fields, one step had to do with multiple roots and derivatives. In particular, we used the fact that a multiple root of P is also a root of P' in order to show that the Artin–Schreier polynomial doesn't have multiple roots.

Guiding Question
Let $P \in F[x]$ be an irreducible polynomial. Can P have multiple roots in its splitting field (or equivalently, in any extension)?

If α is such a root, then α is also a root of P', and therefore a root of $\gcd(P, P')$ as well (where $\gcd(P, P')$ is the polynomial Q which generates (P, P') as an ideal).

But P is irreducible, and $\deg P' < \deg P$. So if $P' \neq 0$, then this means $\gcd(P, P') = 1$, and no such α can exist. However, it's possible that $P' = 0$. So the question reduces to the following:

Guiding Question
When can we have a nonconstant polynomial with $P' = 0$?

We have $(x^n)' = nx^{n-1}$. If $n \geq 1$, then if the field has characteristic 0, this is always nonzero. Meanwhile, if the field has characteristic p, then this is zero if and only if $p \mid n$. So if $P' = 0$, then we must have

$$P(x) = Q(x^p) = a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_0,$$

where $p = \text{char}(F)$. So we want to see when such a polynomial is irreducible.

If $F = \mathbb{F}_q$ is finite, then we know $a^q = a$ for all $a \in F$. This means we can extract pth roots of the coefficients, since $(a^{p^{n-1}})^p = a$ — so we can write $a_i = b_i^p$ for some $b_i \in F$. Then we have

$$P(x) = b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_0^p.$$

But this allows us to extract a pth root of the *polynomial*: we then have

$$P = (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0)^p.$$

On the other hand, there exist examples of such irreducible P in infinite fields. For instance, take $F = \mathbb{F}_q(t)$ to be the field of rational functions in t (or equivalently, the fraction field of $\mathbb{F}_q[t]$), and $P(x) = x^p - t$. This is irreducible, but its derivative is identically 0.

We won't study examples like this, but it's good to know they exist — in every situation we care about, irreducible polynomials can't have multiple roots.

Definition 27.9
An extension E/F is **separable** if the minimal polynomial (over F) of every algebraic element $\alpha \in E$ has no multiple roots.

So if F has characteristic 0 or is finite, then every extension is separable. We'll only look at these instances, so we will generally assume all our extensions are separable.

27.4 Geometry of Function Fields

Another important example of a field is $\mathbb{C}(t)$; we can think of the extensions of $\mathbb{C}(t)$ via geometry. Let $F = \mathbb{C}(t)$, and suppose $E = F[x]/(P)$ is a finite extension of F, where P is an irreducible polynomial. As with integers, we can scale so that P is a primitive polynomial in $\mathbb{C}[t][x]$.

We can then think of P as a polynomial in two variables, meaning $P \in \mathbb{C}[t, x]$. So another way to think of these extensions is that $F = \text{Frac}(\mathbb{C}[t])$, and $E = \text{Frac}(R)$ where $R = \mathbb{C}[t, x]/(P)$.

As discussed earlier, these rings are worked with in algebraic geometry — to connect them to geometry, we consider the maximal spectrum

$$X = \text{MSpec}(R) = \{(a, b) \in \mathbb{C}^2 \mid P(a, b) = 0\}$$

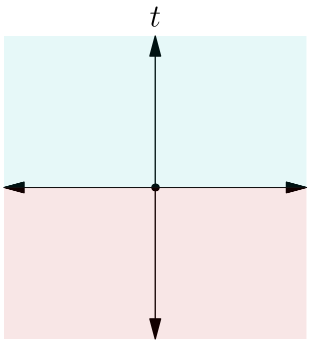
(which describes all maximal ideals of R). Also define $Y = \text{MSpec}(\mathbb{C}[t]) = \mathbb{C}$. Then we have a map $X \to Y$ sending $(a, b) \mapsto a$.

Student Question. *If P is irreducible, is R a field extension?*

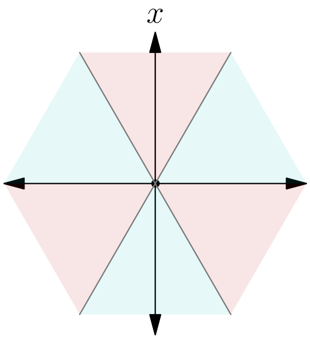
Answer. *No, R is not a field. Polynomials in two variables aren't a PID (so even if P is irreducible, (P) is generally not maximal) — if they were, algebraic geometry would be trivial.*

Example 27.10
Let $P(t, x) = x^n - t$.

Then $R \cong \mathbb{C}[x]$, where this map sends a complex number to its nth power (since $t = x^n$). Each point in $\mathbb{C}$ has n complex nth roots (except 0), giving a *ramified covering* (with a ramification point at 0). One way to represent this geometrically is to draw the t-plane and the x-plane. In the t-plane, we make a cut along the x-axis, turning it into two half-planes glued together.



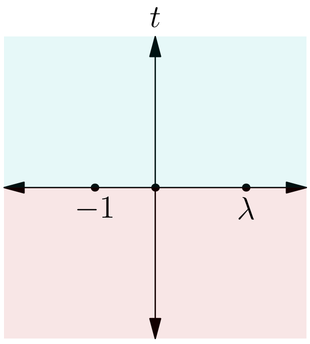
For a point on the x-plane, raising it to the nth power multiplies the angle by n. So we cut the x-plane into $2n$ pieces (colored by which half-plane their points are mapped to):



This describes the geometry of the map raising x to the nth power.

Example 27.11
Let $P(x,t) = x^2 - t(t+1)(t-\lambda)$. (Any P consisting of x^2 minus a cubic polynomial can be written in this form, by a change of variables.) For simplicity, assume $\lambda \in \mathbb{R}$.

We can again draw the $\mathbb{C}$-plane. We again have a ramified double covering, with three ramification points — $t = 0$, -1, and λ (for every other point, there are two square roots). So we can again make a cut and create two half-planes.



For each half-plane, its pre-image breaks into two pieces (corresponding to the two branches of the square root — we can start with the positive or negative one). So the pre-image consists of two blue rectangles and two red rectangles:

We then need to glue these rectangles together, by thinking about the values of these functions. When glued together, they look like a bagel (where we cut the bagel horizontally and through its middle).

Note 27.12

These situations require more background to describe rigorously, and for that reason they are usually not presented in algebra classes; but they are important examples of field extensions, and mathematicians often have these examples in mind even when constructing algebraic arguments about number fields.