6A. Finite and Cyclotomic Fields

Finite and Cyclotomic Fields

Finite fields are perfect

Lemma: Let F be a finite field. Then every element of F is a p^{th} power.

Proof: The map $\phi(x) = x^p$ is a field homomorphism from F to itself. Since it is injective and F is finite, it is surjective.

Lemma: Every irreducible polynomial over F is separable.

Proof: If $f(x)$ is irreducible and inseparable, then $f'(x) = 0$ so $f(x) = g(x^p)$. But then $f(x) = g(x)^p$, contradicting irreducibility.

Existence and uniqueness of finite fields

Proposition: Let p be a prime. Then there is a unique (up to isomorphism) finite field with p^n elements for every $n \geq 1$.

Proof: If F is a finite field of characteristic p, it is a finite dimensional vector space over F_p so has p^n elements where $n = [F : F_p]$. Consider the splitting field F of the polynomial $x^{p^n} - x$ over F_p. It is separable since its derivative is -1. Thus it has p^n distinct roots. Notice that, if α and β are roots of this polynomial, so are $\alpha\beta$, $\alpha + \beta$, and α^{-1}. Thus the p^n roots of the polynomial form a field. Thus F is exactly this set of p^n roots. Finally, let F be any finite field of characteristic p with p^n elements. The nonzero elements of F satisfy $x^{p^n-1} - 1 = 0$ since F^* is a finite abelian group with $p^n - 1$ elements. Therefore (including zero) the elements of F are the roots of $x^{p^n} - x$ so F is the splitting field of this polynomial. Since splitting fields are unique, all finite fields of order p^n are isomorphic.

We commonly write F_{p^d} or $\mathbb{F}_{p^d}$ for this unique field with p^d elements.

Multiplicative groups of finite fields are cyclic

Suppose F has p^n elements. Suppose that $d|(p^n - 1)$ so $x^d - 1$ divides $x^{p^n-1} - 1$. If $F^\times$ has an element of order d, it generates a cyclic subgroup of order d, and the elements of that cyclic subgroup are all roots of $x^d - 1$. In this case the number of elements of order d is $\phi(d)$. If $\psi(d)$ is the number of elements of order d, then we see that $\psi(d)$ is either $\phi(d)$ or zero, and in particular is at most $\phi(d)$.

Now by Lagrange's Theorem

$$p^n - 1 = \sum_{d|(p^n-1)} \psi(d).$$

On the other hand, by counting the elements of order d for each divisor of $p^n - 1$ in a cyclic group of order $p^n - 1$, we have

$$p^n - 1 = \sum_{d|(p^n-1)} \phi(d).$$

We conclude that $\psi(d) = \phi(d)$ for all d, so $\phi(p^n - 1) \geq 1$.

Counting irreducible polynomials mod p

How many irreducible polynomials of degree d are there over F_p?

Given such a polynomial, you get d elements of the field F_{p^d}, all of degree d over F.

Conversely, given an element of degree d over F in F_{p^d}, you get an irreducible polynomial; but there are d elements that give the same polynomial.

So the number of irreducible polynomials is

$$\frac{\|\{x \in F_{p^d} : F(x) = F_{p^d}\}\|}{d}$$

If d is prime, then an element of F_{p^d} is either of degree one or d. There are p elements of degree 1, and $p^d - p$ of degree d. So the number of irreducible polynomials of prime degree d is $(p^d - p)/d$.

For example, if $p = 2$ and $d = 5$, there are 6 irreducible polynomials of degree 5. They are irreducible factors of $x^{32} - x$ mod 2. According to wolfram alpha, they are:

$$\begin{array}{cc} x^5 + x^2 + 1 & x^5 + x^3 + 1 \\ x^5 + x^3 + x^2 + x + 1 & x^5 + x^4 + x^2 + x + 1 \\ x^5 + x^4 + x^3 + x + 1 & x^5 + x^4 + x^3 + x^2 + 1 \end{array}$$

Cyclotomic Polynomials and roots of unity

We let μ_n denote the complex roots of the polynomial $x^n - 1$. These are called the n^{th} roots of unity. If $\zeta \in \mu_n$, then

$$\zeta = e^{2\pi i a/n}$$

for some integer a.

The set μ_n is in fact a cyclic group of order n. Its generators are called the primitive n^{th} roots of unity. If $\zeta \in \mu_n$ is a primitive root of unity then

$$\zeta = e^{2\pi i a/n}$$

where $(a, n) = 1$.

The cyclotomic polynomials

The cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are the primitive n^{th} roots of unity.

Lemma: For all $n \geq 1$, the degree of $\Phi_n(x)$ is $\phi(n)$, and

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

This is because there are $\phi(n)$ primitive roots of unity in μ_n and every n^{th} root of unity is primitive of order d for some $d|n$.

Cyclotomic polynomials have integer coefficients

Lemma: $\Phi_n(x)$ is monic and belongs to $\mathbb{Z}[x]$.

Proof: The factorization of $x^n - 1$ in terms of $\Phi_d(x)$ gives a recursive algorithm for computing the Φ_d. Clearly $\Phi_1(x) = x - 1$ belongs to $\mathbb{Z}[x]$. Suppose that $\Phi_d(x)$ is monic and belongs to $\mathbb{Z}[x]$ for all $d < n$. Then $x^n - 1 = f(x)\Phi_n(x)$ where $f(x)$ is monic with integer coefficients. Then $(x^n - 1)/f(x)$ is monic with integer coefficients by polynomial division (or by Gauss's lemma if you want to be fancier).

The cyclotomic polynomials are irreducible

Theorem: The polynomials $\Phi_n(x)$ are irreducible.

Proof: We use results about the reduction mod p of $\Phi_n(x)$; in some sense this is a number theoretic result.

Suppose that $\Phi_n(x) = f(x)g(x)$ where $f(x)$ is irreducible. Let ζ be a root of $f(x)$. Choose a prime p not dividing n. Then ζ^p is again a primitive n^{th} root of unity, and therefore a root of either $f(x)$ or $g(x)$. Suppose it's a root of $g(x)$. Then since $g(\zeta^p) = 0$ it follows that ζ is a root of $g(x^p)$. Now $f(x)$ is irreducible, so it is the minimal polynomial for ζ, and therefore $f(x)$ divides $g(x^p)$:

$$g(x^p) = f(x)h(x)$$

Reduce this equation modulo p, and we have

$$\overline{g}(x^p) = \overline{g}(x)^p = \overline{f}(x)\overline{h}(x).$$

Then $\overline{f}(x)$ divides $\overline{g}(x)^p$ which means that $\overline{f}(x)$ and $\overline{g}(x)$ have a common factor mod p.

Now remember that

$$\Phi_n(x) = f(x)g(x).$$

This tells us that, mod p, $\Phi_n(x)$ has a multiple root (from the common factor of $f(x)$ and $g(x)$ mod p). But that would mean that $x^n - 1$ has a multiple root mod p, which can't be true. It's derivative is nx^{n-1} which is not zero mod p since p does not divide n. It follows that ζ^p must be a root of $f(x)$.

Retracing the argument, we've shown that, if ζ is a root of the factor $f(x)$, so is ζ^p for any p not dividing n. If α is any primitive n^{th} root of 1, then $\alpha = \zeta^a$ for some a relatively prime to n. But then $a = p_1 \cdots p_k$ where the p_i are primes not dividing n (not necessarily distinct). It follows that $\alpha = ((\zeta^{p_1})^{p_2})^{\cdots}$ is also a root of $f(x)$. In other words, all of the primitive n^{th} roots of one are roots of $f(x)$. That means that $f(x) = \Phi_n(x)$ and $g(x) = 1$, so $\Phi_n(x)$ is irreducible.

Corollary: The field $\mathbb{Q}(\mu_n)$ has degree $\phi(n)$ over $\mathbb{Q}$.

The cosine of twenty degrees

In our work on constructibility we claimed that the 60 degree angle could not be trisected because a twenty degree angle is not constructible. Now

$$2\cos 20^\circ = 2\cos 2\pi/18 = e^{\pi i/9} + e^{-\pi i/9}.$$

Now $e^{\pi i/9}$ is a primitive 18^{th} root of one and there are $\phi(18) = 6$ such; they are roots of $\Phi_{18}(x)$. Now

$$x^{18} - 1 = (x^9 - 1)(x^9 + 1)$$

but also

$$x^{18} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_9(x)\Phi_{18}(x)$$

Now:

$$\begin{gathered} Phi_1(x) = x - 1 \\ \Phi_2(x) = x + 1 \\ \Phi_3(x) = x^2 + x + 1 \\ \Phi_6(x) = x^2 - x + 1 \end{gathered}$$

so some algebra tells us that

$$\Phi_{18}(x) = \frac{x^9 + 1}{x^3 + 1} = x^6 - x^3 + 1.$$

This in turn means that, if $\zeta = e^{\pi i/9}$, then $\zeta^3 + \zeta^{-3} = 1$ (divide Φ_{18} by x^3). But

$$(\zeta + \zeta^{-1})^3 = \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1}) = 1 + 3(\zeta + \zeta^{-1}).$$

In other words $2\cos\frac{2\pi i}{18} = \zeta + \zeta^{-1}$ satisfies the cubic polynomial $x^3 - 3x - 1 = 0$.