6320-001 - SPRING 2021 - 4/01 LECTURE

(My apple pencil broke!)
Today:
Galois theory of finite fields
Cyclotomic polynomials/extensions

Let $\mathbb{F}_q$ be a field with $q = p^n$ elements. Let $[\mathbb{F} : \mathbb{F}_q] = k$ (the unique field with $q^k = p^{nk}$ elements).

Exercise: $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^k}$ if and only if $d|k$. This is terrible notation! One way you could make sense of this is fix an algebraic closure $\overline{\mathbb{F}_p}/\mathbb{F}_p$ (this is a choice!) then define $\mathbb{F}_{p^k}$ to be the splitting field of $x^{p^k} - x$ over $\mathbb{F}_p$ in $\overline{\mathbb{F}_p}$.

Exercise: Produce an algebraic closure of $\mathbb{F}_p$ without using axiom of choice. (Hint: Look at splitting fields of $x^{p^{n!}} - x$ to create a tower of extensions whose union is algebraically closed).

Let $\mathbb{F}_q$ be a field with $q = p^n$ elements. Let $[\mathbb{F} : \mathbb{F}_q] = k$ (the unique field with $q^k = p^{nk}$ elements).

Theorem. *$\mathbb{F}/\mathbb{F}_q$ is Galois with Galois group $\mathbb{Z}/kZ$ generated by the q-power Frobenius automorphism*

$$\mathrm{Frob}_q : \alpha \mapsto \alpha^q.$$

(I.e. there is an isomorphism $\mathbb{Z}/k\mathbb{Z} \to \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ sending 1 to Frob_q.)

Proof. Galois because it's a splitting field of $x^{|\mathbb{F}|} - x = x^{q^k} - x = x^{p^{nk}} - x$. (not necessary for the proof but good sanity check).

Claim: Just need to check (why?)
1) $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$
2) Check that the order of Frob_q is k.

For 1) – $x \mapsto x^q$ definitely fixes $\mathbb{F}_q$ because the elements of $\mathbb{F}_q$ are exaclty the roots of $x^q - x$, i.e. such that $x^q = x$ i.e. such that $\mathrm{Frob}_q(x) = x$.

For 2) – definitely $\mathrm{Frob}_q^k = \mathrm{Frob}_{q^k} = \mathrm{Id}$ on $\mathbb{F}$ because ... (same justification with q^k). So the order divides k; on the other hand, if $\mathrm{Frob}_q^d = \mathrm{Frob}_{q^d} = \mathrm{Id}$ for $d < k$ then everything in $\mathbb{F}$ satisfies $x^{q^d} = x$ but there are only q^d roots of this polynomial – contradiction since $|\mathbb{F}| = q^k > q^d$.

So this shows Frob_q generates a copy of $\mathbb{Z}/k\mathbb{Z} \leq \mathrm{Aut}(\mathbb{F}/\mathbb{F}_q)$. But we know that for any field extension $|\mathrm{Aut}(L/K)| \leq [L : K]$ with equality if and only if its Galois. Thus get

$$\mathbb{Z}/k\mathbb{Z} = \langle \mathrm{Frob}_q \rangle = \mathrm{Aut}(\mathbb{F}/\mathbb{F}_q).$$

□

Sentence to remember: Any extension of finite fields is Galois with Galois group cyclic generated by Frobenius. (**Note – this is absolutely central to modern number theory!**)

Note: it's quite unusual to have a field such that all of its extension are Galois. (Exercise: if there is a polynomial f(x) in K[x] whose Galois group is non-abelian then there is an extension that is not Galois [use the fundamental theorem]).

Cyclotomic polynomials / extensions of $\mathbb{Q}$.

The nth cyclotomic polynomial:

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - e^{2\pi i k/n}) \in \mathbb{C}[x]$$

The roots are the primitive nth roots of unity (primitive means $\zeta^n = 1$ but $\zeta^d \neq 1$ for $d|n$).

Alternative definition:

$$\Phi_n(x) = (x^n - 1)/\gcd(x^n - 1, \prod_{d|n, d \neq n} x^d - 1)$$

Thus $\Phi_n(x) \in \mathbb{Z}[x]$.

Another equivalent inductive definition:

$$\Phi_1(x) = x - 1, \text{ then } (x^n - 1)/\prod_{d|n, d \neq n} \Phi_d(x).$$

Lemma 1. *If K is a field, then the roots of $\Phi_n(x)$ in K are exactly the primitive nth roots of unity in K, i.e. the elements $\zeta \in K$ such that $\zeta^n = 1$ and $\zeta^d \neq 1$ for $d|n$, $d \neq n$.*

Proof. Prove inductively by applying the inductive definition. □

(Note if $K = \mathbb{F}_p$ then the image of $\Phi_n(x)$ in $K[x]$ is just given by reducinig coefficients mod p). A polynomial over the integers is simultaneously a polynomial over every single field (or even ring) because there is a unique map $\mathbb{Z} \to R$ for any ring R.

Theorem. *$\Phi_n(x)$ is irreducible (of degree $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(n)$ = number of numbers less than n coprime to n) and $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ is Galois, there is a canonical isomorphism*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}), \quad k \mapsto \sigma_k$$

such that $\sigma_k(\zeta) = \zeta^k$ for any nth root of unity in $\zeta \in \mathbb{Q}(e^{2\pi i/n})$.

Proof. Note: easy to see every automorphism must be of this form, but needs an argument to see that there is an automorphism that does this. HOWEVER, the extension is Galois because it's the splitting field of $x^n - 1$, so I know that $|\mathrm{Aut}|$ = degree of extension. So it suffices to show that the degree is $\phi(n)$. So it suffices to show that $\Phi_n(x)$ is the minimal polynomial of $e^{2\pi i/n}$, i.e. that it is irreducible – see next lemma. □

Lemma 2. *$\Phi_n(x)$ is irreducible (in $\mathbb{Q}[x]$ or equivalently $\mathbb{Z}[x]$).*

Example 0.1. If ℓ is a prime number then

$$\Phi_\ell(x) = (x^\ell - 1)/(x - 1) = 1 + x + x^2 + ... + x^{\ell-1}$$

is irreducible by Eisenstein (after substitution x-1=y).

But this doesn't generalize.

Proof of Lemma 2. Write $\zeta = e^{2\pi i/n}$. Write $\mathbb{Z}[\zeta] \subset \mathbb{C}$ smallest subring containing ζ and $\mathbb{Z}$. If I write $g(x)$ for the minimal polynomial (over $\mathbb{Q}$) of ζ, since it has integral coefficients then easy to check that

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[x]/g(x).$$

Pick a prime p not dividing n.

$$\mathbb{Z}[\zeta]/p \cong \mathbb{F}_p[x]/\overline{g}(x).$$

$\overline{g}$ = reduce coefficients mod p. Pick a map $\mathbb{F}_p[x]/\overline{g}(x) \to \overline{\mathbb{F}_p}$ (think about this – just choose an irreducible factor of $\overline{g}(x)$).

Then I get bijections

$$\{ \text{ Roots of } \Phi_n(x) \text{ in } \overline{\mathbb{F}}_p\} \leftrightarrow \{ \text{ Roots of } \Phi_n(x) \text{ in } \mathbb{Z}[\zeta]\} \leftrightarrow \{ \text{ Roots of } \Phi_n(x) \text{ in } \mathbb{C}\}$$

Because

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^k) \text{ in } \mathbb{Z}[\zeta][x]$$

gives a factorization also in $\overline{\mathbb{F}}_p$. Because p doesn't divide n this polynomial is separable (already $x^n - 1$ is).

This bijection preserves roots of $g(x)$. Now apply the Frobenius to see that the roots of $g(x)$ are preserved by raising by p powers! Apply for all p not dividing n, which generate $(\mathbb{Z}/n\mathbb{Z})^\times$. □