Last time: In the middle of showing $\Phi_n(x)$ irreducible

roots are primitive nth roots of unity.

Key observation:

Let $f(x) \in \mathbb{Z}[x]$ monic, integer coefficients, degree n, and separable.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\mathbb{C}$.

$$R = \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \subseteq \mathbb{C}$$

(smallest subring containing integers + these roots).

Can show that for any prime p, there is a map $R \to \overline{\mathbb{F}}_p$ ← an algebraic closure of $\mathbb{F}_p$.

(Take a maximal ideal in R/p; $R/p/m$ is a finite extension of $\mathbb{F}_p$ generated by $\alpha_1, \ldots, \alpha_n$)

$$r \longmapsto \bar{r}$$

$$\begin{tikzcd} R \arrow[r, "\text{red. mod } \mathfrak{P}"] & \overline{\mathbb{F}}_p \\ \mathbb{Z} \arrow[u] \arrow[r, "\text{reduction mod } p"] & \mathbb{F}_p \arrow[u] \end{tikzcd}$$

Write $\bar{f} \in \mathbb{F}_p[x]$ for the reduction of f mod p.

$$f = (x-\alpha_1) \cdots (x-\alpha_n) \in \mathbb{C}[x]$$
$$\in R[x].$$

$$\downarrow$$

$$\bar{f} = (x-\bar{\alpha}_1)(x-\bar{\alpha}_2) \cdots (x-\bar{\alpha}_n).$$

If $f \in \mathbb{F}_p[x]$ is separable then $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ are distinct.

$$
\begin{tikzcd}
\{\bar\alpha_1,\dots,\bar\alpha_n\} & \overline{\mathbb{F}_p} & & \mathbb{C} & \{\alpha_1,\dots,\alpha_n\} \\
& & R \arrow[ul] \arrow[ur] & & \\
& & \{\alpha_1,\dots,\alpha_n\} \arrow[ull] \arrow[urr, leftrightarrow] & &
\arrow[from=1-1, to=1-5, bend right=60, leftrightarrow]
\end{tikzcd}
$$

$\{\bar\alpha_1,\dots,\bar\alpha_n\}$ = roots of $\bar f$ in $\overline{\mathbb{F}_p}$

$\{\alpha_1,\dots,\alpha_n\}$ roots of f in $\mathbb{C}$

If $g(x) \in \mathbb{Z}[x]$ is a factor of $f(x)$ the bijection sends roots of

roots $\bar g(x)$ in $\overline{\mathbb{F}_p}$ $\longleftrightarrow$ roots of $f(x)$ in $\mathbb{C}$.

To show $\Phi_n(x)$ is irreducible. $\zeta = e^{2\pi i/n}$

$(x^n - 1)$ is separable if nx^{n-1} if $n \neq 0$ only root is 0

Take $p \nmid n$ then $\bar{\Phi}_n = \Phi_n \bmod p$ is separable $\Leftarrow$

$$\text{Roots in } \overline{\mathbb{F}_p} = \{\bar\zeta^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\} \longleftrightarrow \{\zeta^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\} = \text{Roots in } \mathbb{C},$$

$\left(\bar\zeta^k = \overline{\zeta^k}\right)$

Now suppose ζ^k is a root of g $\leftarrow$ an irreducible factor of $\Phi_n(x)$.

$\Downarrow$

$\bar\zeta^k$ is a root of $\bar g$

$\bar g \in \mathbb{F}_p[x]$ so $\mathrm{Frob}_p(\bar\zeta^k)$ is also a root of $\bar g$.

$\Rightarrow (\zeta^k)^p = \overline{\zeta}^{kp} \; (= \zeta^{kp})$

Thus ζ^{kp} is a root of g.

This applies for any root of g and any $p \nmid n$.

So if ζ^k is a root of g,
so is ζ^{kp} & ζ^{kp^2} . . .

& $\zeta^{kp^2 q} \ldots$ for $q \nmid n$
prime

primes $\nmid n$ generate $(\mathbb{Z}/n\mathbb{Z})^\times$

Once you know one root you know all of them!

Key points: · Frobenius is a polynomial map
· Roots of unity are powers of each other
(roots of $x^n - 1$ satisfy lots of algebraic relations)

Doesn't work as well for other $f \in \mathbb{Z}[x]$
but it does still give something

Argument above + a little bit of algebraic number theory.

Theorem: If $f \in \mathbb{Z}[x]$ monic separable
and p is a prime s.t. $\overline{f}$ ($= f$ mod p)
is separable then
Galois group of f (= Galois group of splitting field as a permutation group on the roots of f) contains

a permutation of cycle type $k_1, k_2, \ldots, k_m$.

where $\bar{f} = \bar{f}_1 \cdots \bar{f}_m$ irreducibles in $\mathbb{F}_p[x]$

$\deg f_i = k_i$.

(Galois group of $\bar{f}$ is generated by Frob — this cycle is Frob acting on the roots of $\bar{f}$.),

Application: For every n, there exists an irreducible degree n polynomial $f(x) \in \mathbb{Z}[x]$ s.t. Galois group of $f = S_n$.

Proof: Idea: Reverse engineer using the theorem

Know: a 2-cycle + $n-1$-cycle generate S_n.

Take $f_2(x) \in \mathbb{F}_2[x]$ to be degree n irreducible.

Take $f_3(x) \in \mathbb{F}_3[x]$ to factor as a degree 2 irreducible $\times$ distinct irreducibles of odd degree.

Take $f_5(x) \in \mathbb{F}_5[x]$ to factor as a degree $(n-1)$ irreducible $\times$ linear factor.

Chinese Remainder Theorem;

$\exists\ f \in \mathbb{Z}[x]$ monic
with f mod $2 = f_2$
f mod $3 = f_3$
f mod $5 = f_5$.

(raise to a suitable odd power)

$\Rightarrow$ Gal(f) has 2-cycle from mod 3
$(n-1)$ cycle from mod 5

Example: $f(x)$: $x^5 - 6x + 3$ has Galois group S_5:

1. Irreducible by Eisenstein at 3
2. Claim there are 3 real roots and 2 non-real roots in $\mathbb{C}$.

$\sim$ Intermediate value theorem
$-2, 0, 1, 2$
real root, root, root

so, at least 3 real roots.

$f'(x) = 5x^4 - 6$
$\leftarrow$ 2 real roots. $\left(\pm \sqrt[4]{\frac{6}{5}}\right)$

Derivative can only be zero twice
All roots simple (f separable).
between any 2 real roots
Mean value theorem
gives a root of f'!

$\Rightarrow$ at most 3 real roots of f.

$\Rightarrow$ f has a pair of complex conjugate complex roots

$G =$ Galois group Aut$(K/\mathbb{Q})$ K splitting field of $f(x)$ in $\mathbb{C}$.

then $(1) \Rightarrow 5 \mid |G|$

so G has an element of order 5

$G \subseteq S_5$

$\Rightarrow G$ has a 5-cycle.

$(2) \Rightarrow G$ contains a transposition (complex conjugation).

So G is S_5. ✓

What *is* the Galois group of a polynomial? (What is it measuring).

Observation:

Galois group of $x^n - 1$ over $\mathbb{Q}$ $= (\mathbb{Z}/n\mathbb{Z})^\times$ is small

How to see this at level of the roots

"Generically" Galois group of degree n polynomial is $= S_n$.

Small Galois group $\longleftrightarrow$ Lots of (unexpected!) algebraic relations between the roots

Galois group *is* the group of permutations of the roots preserving all algebraic relations between them

$\Downarrow$

Say $f(x) \in K[x]$ is separable

$\mathrm{Gal}(f)$: Take a splitting field L/K
then look at $\mathrm{Aut}(L/K)$.

. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f in L

$L = K(\alpha_1, \ldots, \alpha_n)$ $\qquad \alpha_1, \ldots, \alpha_n$ algebraic

$$K[x_1, \ldots, x_n] \overset{I = \text{kernel}}{\twoheadrightarrow} L$$

$x_i \to \alpha_i$ is surjective.

$$L = K[x_1, \ldots, x_n]/I.$$

If $g(x_1, \ldots, x_n) \in I$ that means
$$g(\alpha_1, \ldots, \alpha_n) = 0.$$
i.e. g is an algebraic relation between.

$$\mathrm{Aut}(L/K)$$
$$\Updownarrow$$

$$L \to L \quad \text{map of } K\text{-algebras}$$

$$\begin{array}{c} L \\ \| \\ K[x_1, \ldots, x_n]/I \end{array} \xrightarrow{\sigma} L$$

I know $f(x_1), f(x_2), \ldots, f(x_n)$ in I.

so x_i has to go to α_j

but if $g \in I$.

$$\Downarrow$$

$$g(\alpha_1, \dots, \alpha_n) = 0.$$

To get a map I need

$$g(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = 0.$$

The automorphisms of L/K are the permutations of the roots satisfying:

If $g \in K[x_1, \dots, x_n]$ is s.t. $g(\alpha_1, \dots, \alpha_n) = 0$

then $g(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = 0$.

$$L = K[x_1, \dots, x_n]/I$$ ← Ideal of all algebraic relations

$$|Gal(L/K)| = [L : K]$$

The bigger I is, the smaller degree.