

Last time: In the middle of showing $\bar{f}_n(x)$ irreducible

↑ roots are primitive
nth roots of unity.

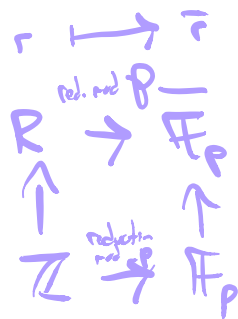
Key observation:

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

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

$R = \mathbb{Z}[\alpha_1, \dots, \alpha_n] \subseteq \mathbb{C}$
(smallest subring containing
integers + these roots).

Can show that for any prime p , there
is a map $R \rightarrow \mathbb{F}_p \leftarrow$ 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 $\alpha_1, \dots, \alpha_n$)

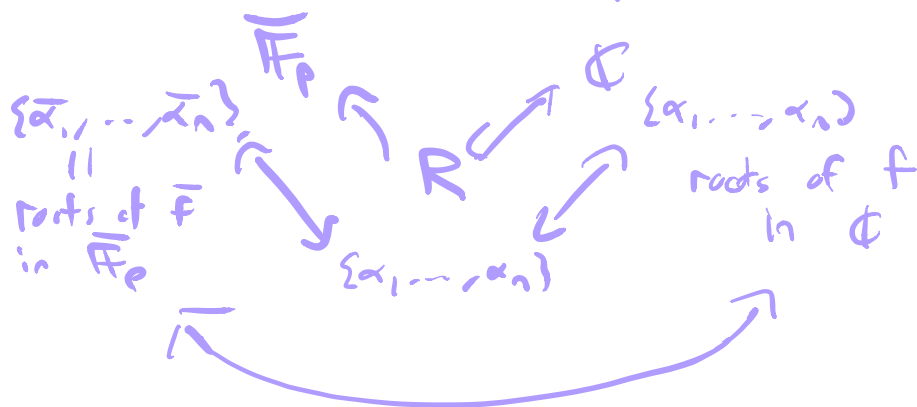
Write $\bar{f} \in \mathbb{F}_p[x]$ for the reduction of
 f mod p .

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

↓

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

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



If $g(x) \in \mathbb{Z}[x]$ is a factor of $f(x)$
 the bijection sends roots of
 roots $g(x)$ in $\bar{\mathbb{F}}_p \iff$ roots of $f(x)$ in Φ .

To show $\Phi_n(x)$ is irreducible.

Take $p \nmid n$ then $\bar{\mathbb{F}}_p = \mathbb{F}_p$ and Φ_n is separable \uparrow
 Roots in $\bar{\mathbb{F}}_p \iff$ Roots in Φ

$n \times n - 1$ if $n \neq 0$
 \uparrow
 $(x^n - 1)$ is

$$\left\{ \bar{\zeta}^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times \right\} \iff \left\{ \zeta^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times \right\},$$

$(\frac{1}{\bar{\zeta}^k})$

Now suppose $\bar{\zeta}^k$ is a root of $g \leftarrow$ an irreducible factor of $\Phi_n(x)$

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

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

$$\hookrightarrow (\bar{\zeta}^k)^p = \bar{\zeta}^{kp} (= \bar{\zeta}^{kp})$$

Thus $\bar{\zeta}^{kp}$ is a root of g .

This applied for any root of g and any $p \in \mathbb{N}$.

So if ζ^k is a root of g .

So is ζ^{kp} & ζ^{kp^2} ...

& $\zeta^{kp^{2a}}$ for $a \in \mathbb{N}$

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

Once you have one root you have 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 theory.

Theorem: If $f \in \mathbb{Z}[X]$ monic separable

and p is a prime s.t. \bar{f} ($= f \text{ mod } p$),

is separable then

Galois group of \bar{f} contains

(= Galois group of splitting field of \bar{f} as a permutation group on the roots of \bar{f}).

a permutation
of cycle type K_1, K_2, \dots, K_m .

where $\bar{f} = \bar{f}_1 \dots \bar{f}_m$ irreducibles
in $\mathbb{F}_q[x]$
 $\deg f_i = K_i$.

(Galois group of \bar{f} is
generated by Frob - this
cycle in 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 factors.

Chinese Remainder Theorem;

$\exists f \in \mathbb{Z}[x]$ monic

with $f \bmod 2 = f_2$

$f \bmod 3 = f_3$

$f \bmod 5 = f_5$

raise to a suitable odd power

$\Rightarrow \text{Gal}(f)$ has 2-cycle from mod 3
(1,2) 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
↑ ↑ ↑
root root root

so at least 3 real roots

$$f'(x) = 5x^4 - 6$$

\leftarrow 2 real roots. $(\pm \sqrt[4]{\frac{6}{5}})$

Derivative can only be zero twice

All roots simple (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 $\text{Aut}(K/\mathbb{Q})$ K splitting field

or $\tau(x)$ in \mathbb{Q} .

then (1) $\Rightarrow S \parallel G$

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 . \checkmark

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 \iff Lots of ^(unexpected!) algebraic relations between the roots

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



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

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

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

$L = K(\alpha_1, \dots, \alpha_n)$ $\alpha_1, \dots, \alpha_n$ algebraic

$K[x_1, \dots, x_n] \xrightarrow{I = \text{kernel}} L$
 $x_i \rightarrow \alpha_i$ is surjective.

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

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

$\text{Aut}(L/K)$

\uparrow
 \downarrow
 $L \rightarrow L$ map of K -algebras

\parallel
 $K[x_1, \dots, x_n] / I \xrightarrow{\sigma} L$

I know $f(x_1), f(x_2), \dots, f(x_n)$

so x_i has to go to α_j
in I .

or it is not I

$$p \in \mathbb{H} \iff g \in G.$$

\Downarrow

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

To get a map \mathbb{I} need

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

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

$$\text{If } g \in K(\alpha_1, \dots, \alpha_n) \text{ is s.t.}$$

$$g(\alpha_i, \dots, \alpha_i) = 0$$

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

$$L = K(\alpha_1, \dots, \alpha_n) / \mathbb{I} \leftarrow \mathbb{I} \text{ ideal of all algebraic relations}$$

$$|\text{Gal}(L/K)| = [L:K]$$

The bigger \mathbb{I} is,
the smaller degree.