When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 16.6; for Mon: 16.7.
- PS09 due Mon Apr 20. (But all deadlines are elastic.)
- Problem session Fri Apr 16, 10:30–noon as usual.
- Today's DJ: Trent

Galois theory in a nutshell

G(K/F) is gp of F-automorphisms of K

Suppose K/F is the splitting field of irred $f \in F[x]$.

- **Galois theory** relates the field theory properties of K/F (e.g., degree) and the group-theoretic properties of $G(K/F)$.
- $G(K/F)$ permutes roots $\alpha_1, \ldots, \alpha_n$ of f and are isomorphic to a transitive subgroup of S_n.
- Main Theorem: Galois correspondence.
- Signature problem: When can $\alpha_1, \ldots, \alpha_n$ be written as a function of the coefficients of $f(x)$ in an expression using only kth roots (generalizing quadatic formula)? If so, $f(x) = 0$ is **solvable by radicals**.

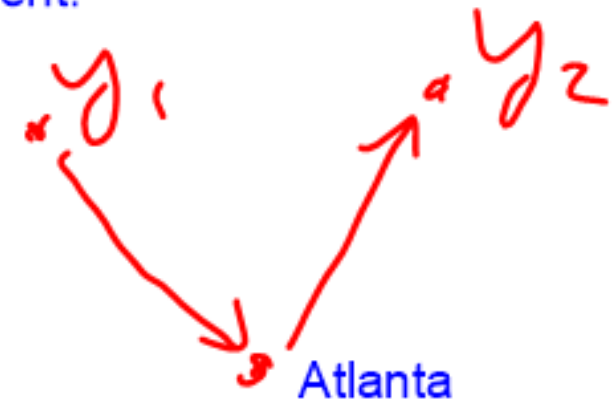
(Blue stuff is done; purple is today.)

Transitive permutation groups:

Ex: G = <(1 2 3 5 6),(4 5)> is transitive on {1,..6} because some combination of alpha and beta can eventually move any point in {1,...6} to any other point in {1,...,6}.

Non-ex: G = <(1 2 3 5),(4 6)> is not transitive on {1,...,6} b/c it has two orbits {1,2,3,5} and {4,6}.

Defn: G acts transitively on S if, for any x,y in S, there exists some g in G such that g(x)=y. Enuf to show that this works for one fixed x in S b/c of "FedEx" argument:



To prove transitivity, enuf to show that everything can be moved to and from Atlanta.

Proof of Fixed Field Theorem (in progress)

Recall:

Theorem

Irr poly over fixed field by symmetrization

H finite group of automorphisms of K, $F = K^H$. $\beta_1 \in K$, $\{\beta_1, \ldots, \beta_r\}$ the H-orbit of β_1. Then:

- $g(x) = (x - \beta_1) \ldots (x - \beta_r)$ *is the irr poly for β_1 over F.*
- β_1 *is algebraic over F of degree r. (So r divides $|H|$.)*

Theorem (Fixed Field Thm)

H a finite group of automorphisms of field K, $F = K^H$. Then K/F finite and $[K : F] = n = |H|$ (i.e., K/K^H is a Galois extension).

Proof of Fixed Field Thm: Last time, we showed that K/F is finite.

So let $K = F(\gamma)$, i.e., γ primitive. If $\sigma(\gamma) = \gamma$, then:

$\sigma \in H$

b/c H fixes F, σ fixes F and γ,
so σ fixes K, i.e., $\sigma = id$.

So $\mathrm{Stab}_H(\gamma) = \{1\}$. Orbit-Stabilizer and symmetrization:

$n = |H| = |Orb_H(\sigma)| \cdot |Stab_H(\sigma)|$

$n = |Orb_H(\gamma)|$

$= [K : F]$

Punchline: The Galois group is optimal (max symmetry) for G(K/(fixed field)). (We will see, and have seen, that G(K/(larger field)) does not have max symmetry.)

Example: Problem 16.5.1(a)

(sigma also fixes C)

$K = \mathbb{C}(t)$ (field of rational functions in one variable), $\sigma(t) = t^{-1}$, $F = K^H$, where

$\sigma^2(t) = \sigma(t^{-1}) = t$

$\sigma^2 = 1$

$$H = \langle \sigma \rangle = \{1, \sigma\}$$

$|H| = 2$

So $[K:F] = 2$

By symmetrizing, irr poly of t over F is:

$$g(x) = (x-t)(x-t^{-1})$$

$$= x^2 - (t+t^{-1})x + 1$$

So if $u = t + t^{-1}$, $g(x) = x^2 - ux + 1$

So t is F, u transcendental so $F = \mathbb{C}(u)$.

16.6: Galois extensions

Definition

An **intermediate field** L of K/F is such that $F \subseteq L \subseteq K$. L **proper** if $L \neq F, K$.

If L is an intermediate field of K/F, then

bigger field corresponds to smaller group!!!

$$G(K/L) \leq G(K/F)$$

auto K fix L

auto K fix F

big field, small group

L ⊇ F

G(K/L) ⊴ G(K/F)

Characterization of Galois extensions

Theorem

K/F finite, $G = G(K/F)$. TFAE:

1. *K/F is Galois, i.e., $|G| = [K : F]$.* max symmetry
2. *$K^G = F$.*
3. *K is a splitting field over F.*

So Galois extension = splitting field = fixed field is as small as possible.

Lemmas:

1. If H is a finite group of automorphisms of K, then K/K^H is Galois and $H = G(K/K^H)$.
2. Suppose $K = F(\gamma_1)$, f irr poly for γ_1 over F. Let $\gamma_1, \ldots, \gamma_r$ be the roots of f in K. There exists a unique $\sigma_i \in G(K/F)$ such that $\sigma_i(\gamma_1) = \gamma_i$, and $G(K/F) = \{\sigma_i\}$ has order r.
3. If $[K : F] < \infty$, then $G(K/F)$ finite and divides $[K : F]$.

transitivity, gamma 1 is Atlanta

Lemma (1) is Fixed Field Theorem; we prove others.

Proofs of Lemmas

Unique b/c F-automorphism det'd by gamma_1

(2) Suppose $K = F(\gamma_1)$, f irr poly for γ_1 over F. Let $\gamma_1, \ldots, \gamma_r$ be the roots of f in K. There exists a unique $\sigma_i \in G(K/F)$ such that $\sigma_i(\gamma_1) = \gamma_i$, and $G(K/F) = \{\sigma_i\}$ has order r. ← (orbit-stabilizer)

First, we know that G(K/F) must permute roots of f contained in K.
Second, we know that, because f irreducible:

$K = F(\gamma_1) \cong F[x]/(f) \cong F(\gamma_i)$

So $K \cong$ subfield $F(\gamma_i)$, $K = F(\gamma_i)$ (by deg)

So $\exists$ F-isom $\sigma_i : K \to K$ s.t. $\sigma_i(\gamma_1) = \sigma_i$ ☺

(3) If $[K : F] < \infty$, then $|G| = |G(K/F)|$ finite and divides $[K : F]$.
G finite by taking $K = F(\gamma)$ (primitive elt thm) and applying (2).
Consider K^G.

By Fixed Field Thm, |G| = [K:K^G].

$|G| = [K : K^G][K^G : F]$

K^G intermediate, so $[K : F] = [K : K^G][K^G : F]$

Proof of characterization of Galois extensions

Theorem

K/F finite, $G = G(K/F)$. TFAE:

1. *K/F is Galois, i.e., $|G| = [K : F]$.*
2. *$K^G = F$.* No extra elements in the fixed field of G(K/F).
3. *K is a splitting field over F.*

(1) $\Leftrightarrow$ (2): Fixed Field Theorem applied to $F \subseteq K^G \subseteq K$.

(1) $\Leftrightarrow$ (3): Let $n = [K : F]$, $K = F(\gamma_1)$. So $\deg(\gamma_1) =$

FFT => $|G| = [K : K^G]$

This $= [K : F]$ iff $|G| = [K : F]$

Consequences of Galois = splitting

Suppose K/F Galois, $G = G(K/F)$, $g \in F[x]$ splits completely in K with roots $\beta_1, \ldots, \beta_r$.

1. If K/F Galois, L intermediate, then K/L Galois, and

$$G(K/L) \qquad\qquad G(K/F)$$

2. G acts on $S = \{\beta_1, \ldots, \beta_r\}$.
3. If $K = F(\beta_1, \ldots, \beta_r)$, then operation on S is faithful, $G \leq S_r$.
4. If g irreducible, G acts transitively on S.

Main Theorem of Galois Theory

Theorem

K/F Galois, $G = G(K/F)$. Then we have a bijective correspondence

$$\{\textit{subgroups of } G\} \leftrightarrow \{\textit{intermediate fields}\}$$
$$H \mapsto K^H$$
$$G(K/L) \leftarrow L$$

Proof: