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: 16.7; for Wed: 16.8.
- PS10 due Mon Apr 27. (But all deadlines are elastic.)
- Today's DJ: ~~??~~ Ravi

Take-home exam 3: Due Mon May 4

Q: When do we have repeated roots of a polynomial?

A1: Because Ch 16 is all in characteristic 0, irreducible polynomials never have repeated roots.

A2: When a polynomial is reducible, of course we can have repeated roots, e.g., $(x-3)^2$ or any $g(x)^2$.

When we talk about "all of the roots of f(x)", check to see that f(x) is irreducible. Either it will be or repeated roots won't matter. (Or mistake!)

Galois theory in a nutshell

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 $G = G(K/F)$.
- G permutes roots $\alpha_1, \ldots, \alpha_n$ of f and is isomorphic to a transitive subgroup of S_n.
- Main Theorem: There is a bijective, inclusion-reversing correspondence between $H \leq G$ and $F \subseteq L \subseteq K$ sending H to fixed field K^H and L to $G(K/L) \leq G$.
- 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.)

Proof of characterization of Galois extensions

Lem: 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.

Theorem

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

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

K/F Galois iff
no surprise elts in fixed field of G
ifff
K splitting field.

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

(choose a prim elt for K/F)

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

f irr poly of $\gamma_1 \Rightarrow \deg f = n$

(3) $\Leftrightarrow$ all n roots of f in K.] subtlety

$\Leftrightarrow |G| = n \Leftrightarrow$ (1)

Subtle part of green arrow:

If all of roots of f are in K, then K contains splitting field of f and is generated by F and one of those roots, so K = splitting field of f.

Converse: If K is a splitting field of *something*, Splitting Field Theorem implies that if K contains one root of an irreducible, it contains all of them. So since K contains one root of f, it contains all of the roots of f.

Consequences of Galois = splitting

Suppose K/F Galois, $G = G(K/F)$, $g \in F[x]$ splits completely in K with roots $\beta_1, \ldots, \beta_r$. (g might not be irreducible)

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

   fix L, so also fix F

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

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.

From pf of thm above and lemma used to prove it.

kernel of action of G on the set S is trivial; works b/c if you fix F and betas, you fix K.

Note: We will later see/use a case where g is reducible and G acts non-transitively on S.

Main Theorem of Galois Theory

Theorem

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

$$\{\textit{subgroups of } G\} \leftrightarrow \{\textit{intermediate fields}\}$$

$$H \mapsto K^H \quad \text{subgps to fields map}$$

$$G(K/L) \hookleftarrow L \quad \text{fields to subgps map}$$

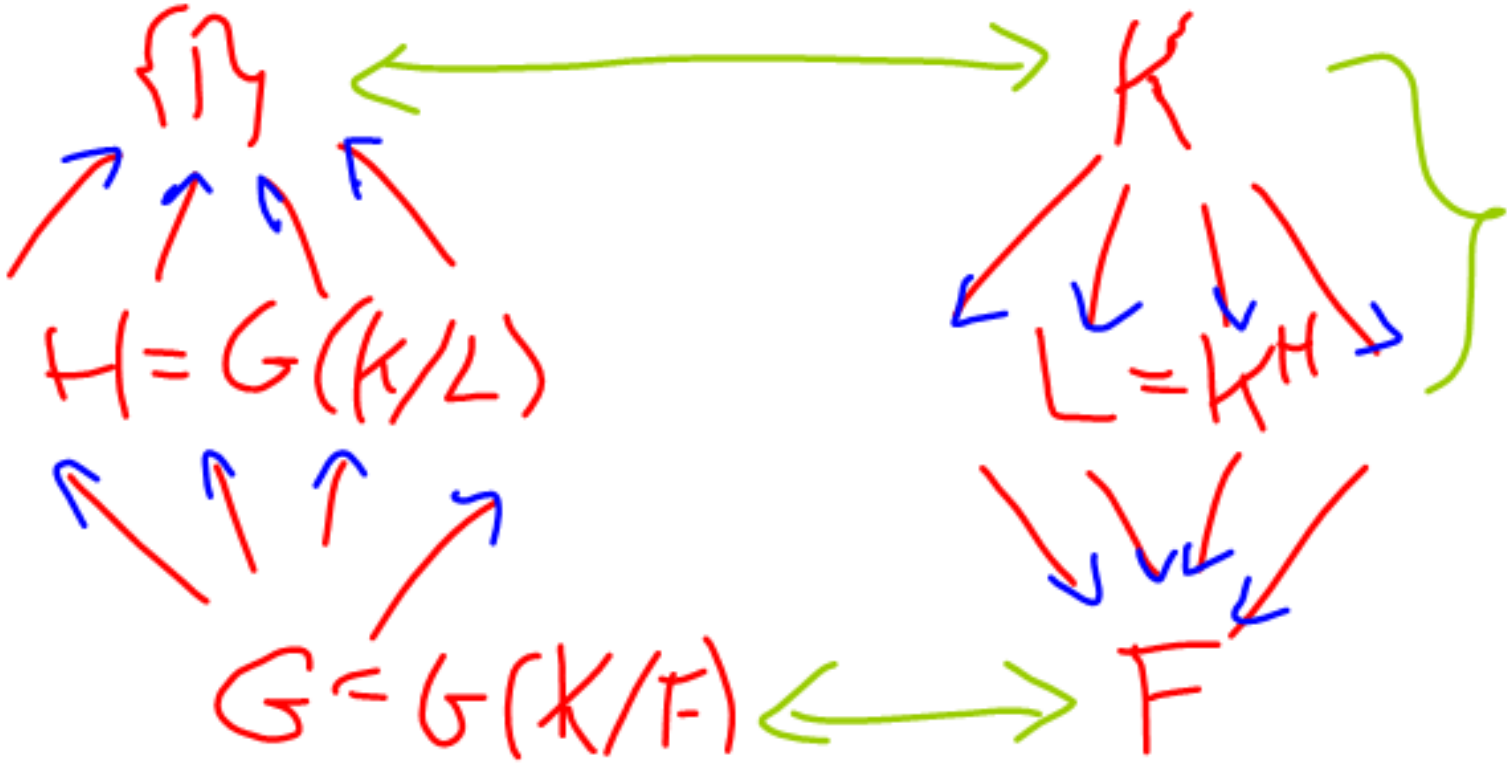
Proof: (proves that subgps to fields, then fields to subgps, is identity)

Maps are bijective iff invertible, so ETS two maps are inverses of each other.

Start with H $\leq$ G: The Fixed Field Thm says H = G(K/K^H), done.

Start with intermediate field L: Characterization of Galois extensions & Corollaries imply K/L Galois, and so L = the fixed field of G(K/L).

Picture of the Galois correspondence



$A \leftarrow B$ means $A \subset B$

Example: The biquadratic

Let $\alpha = \sqrt{5}$, $\beta = \sqrt{11}$, $\alpha\beta = \sqrt{55}$. K is splitting field of f over F

Let $F = \mathbb{Q}$, $K = F(\alpha, \beta)$, $f(x) = (x^2 - 5)(x^2 - 11)$. Not irreducible so not transitive.

$[K : F] = [F(\alpha\beta) : F(\alpha)][F(\alpha) : F] = 4.$ roots of f

Elements of $G = G(K/F)$ are: perms of $\{\alpha, -\alpha, \beta, -\beta\}$

$\sigma = (\alpha \ -\alpha)$ (like $(1\,2\,3\,4)$)

$\tau = (\beta \ -\beta)$

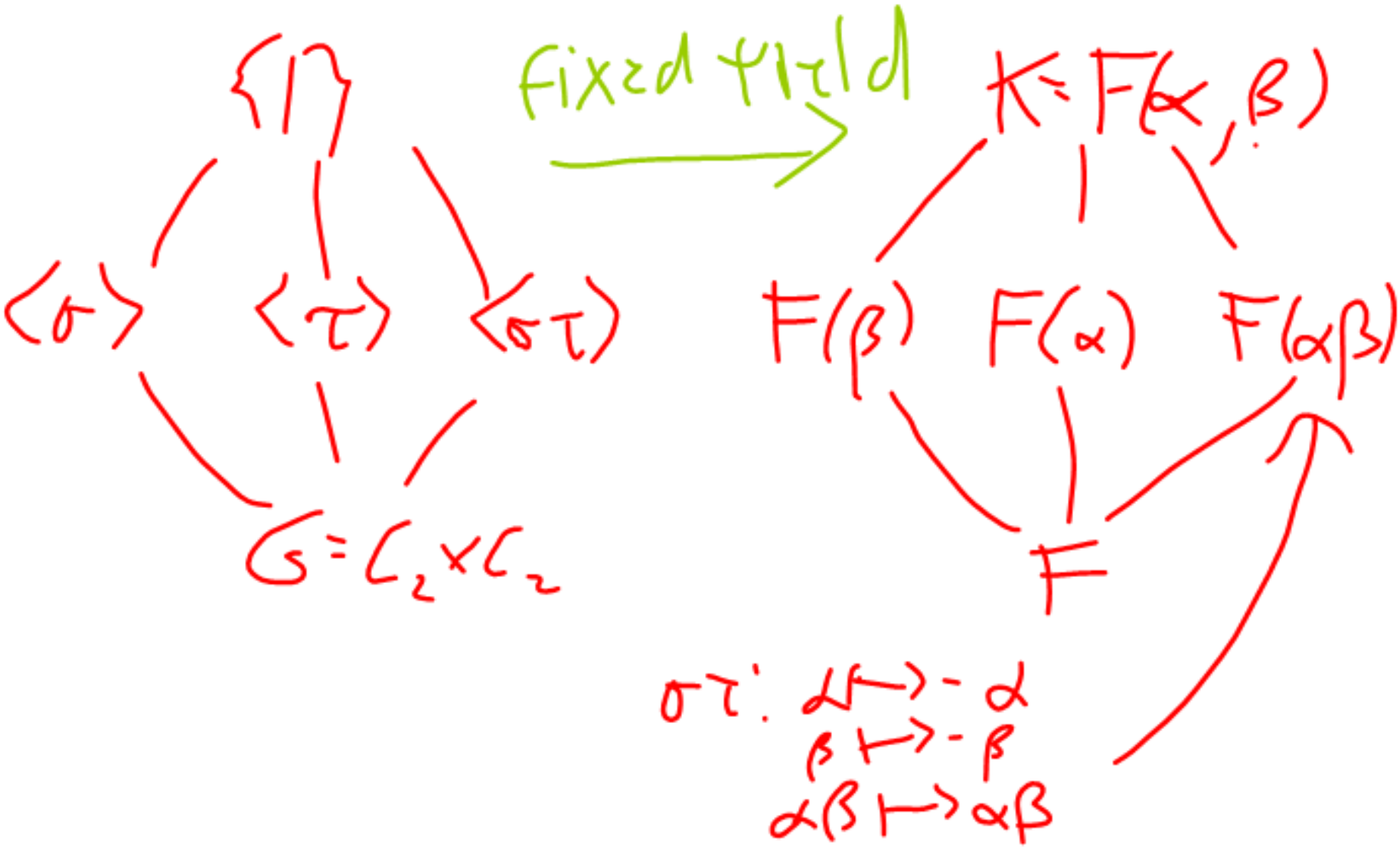
$\sigma\tau = (\alpha \ -\alpha)(\beta \ -\beta)$ and 1

$G = \{1, \sigma, \tau, \sigma\tau\}$.

Extension has degree 4, we found elements, so done.

The biquadratic, cont.

Subgroups of G vs. intermediate fields:



Normal subgroups and extensions

Galois theory of (intermediate over base) works less well than (big field over intermediate).

Theorem

Suppose K/F Galois, $G = G(K/F)$, $H \leq G$, $L = K^H$. Then L/F Galois iff $H \lhd G$, in which case $G(L/F) = G/H$.

Proof: Let $L = F(\epsilon_1)$, $g(x) \in F[x]$ irred poly for ϵ_1.
Splitting Theorem: g splits in K so roots $\epsilon_1, \ldots, \epsilon_r$ of g are in K. We also know:

- G acts on $\epsilon_1, \ldots, \epsilon_r$.
- G transitive b/c g irred (symmetrization).
- L Galois iff splitting iff all $\epsilon_i \in L$.
- $\epsilon_i \in L$ iff $L = F(\epsilon_i)$.
- $\mathrm{Stab}_G(\epsilon_1) = H$.

Normality, cont.

Choose $\sigma \in G$ such that $\sigma(\epsilon_1) = \epsilon_i$.
$\mathrm{Stab}_G(\epsilon_1) =$

So L splitting $H \lhd G$.

Normal subgroups

Now suppose L Galois $= H \lhd G$. What is kernel of action of G on $\{\epsilon_1, \ldots, \epsilon_r\}$?

Compare orders:
$|G/H| =$

$G(L/F) =$

Example: Splitting field of $x^3 - 2$