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: 16.7–16.8; for ~~Wed~~ Mon: 16.9.
- PS10 due Mon Apr 27. (But all deadlines are elastic.)
- Problem session Fri 10:30–noon.
- Today's DJ: Robert.

Recap of Galois Theory:

F char 0, K splitting field of f(x) in F[x]. G=G(K/F), group of F-automorphisms of K, i.e., the automorphisms of K that fix every element of F.

* Group-theoretic structure of G has close analogues in field-theoretic structure of K as an extension of F. (See: Main Thm of Galois Thy)
* Example: |G| = [K:F]

Current problem that we face: Given (irreducible) f(x) in F[x], K splitting field of f(x), how do we compute G=G(K/F)? [Classic Ph.D. qualifying exam question: Given irreducible f(x) in Z[x], compute G=G(K/F).]

Things we can use to compute G (besides |G| = [K:F])

* G permutes the roots of f(x), even if f(x) reducible.
* If f(x) irreducible, then G acts transitively on roots of f(x).

This "root permutation" representation of G is faithful (G isomorphic to its resulting image in S_n, where n = deg (f(x))), so G is isom to a (transitive) subgroup of S_n if f is irreducible.

(Aside: In my undergrad applied algebra later today, I'll mention one application of Galois theory to constructing error-correcting codes; but that's actually char 2.)

Main Theorem of Galois Theory

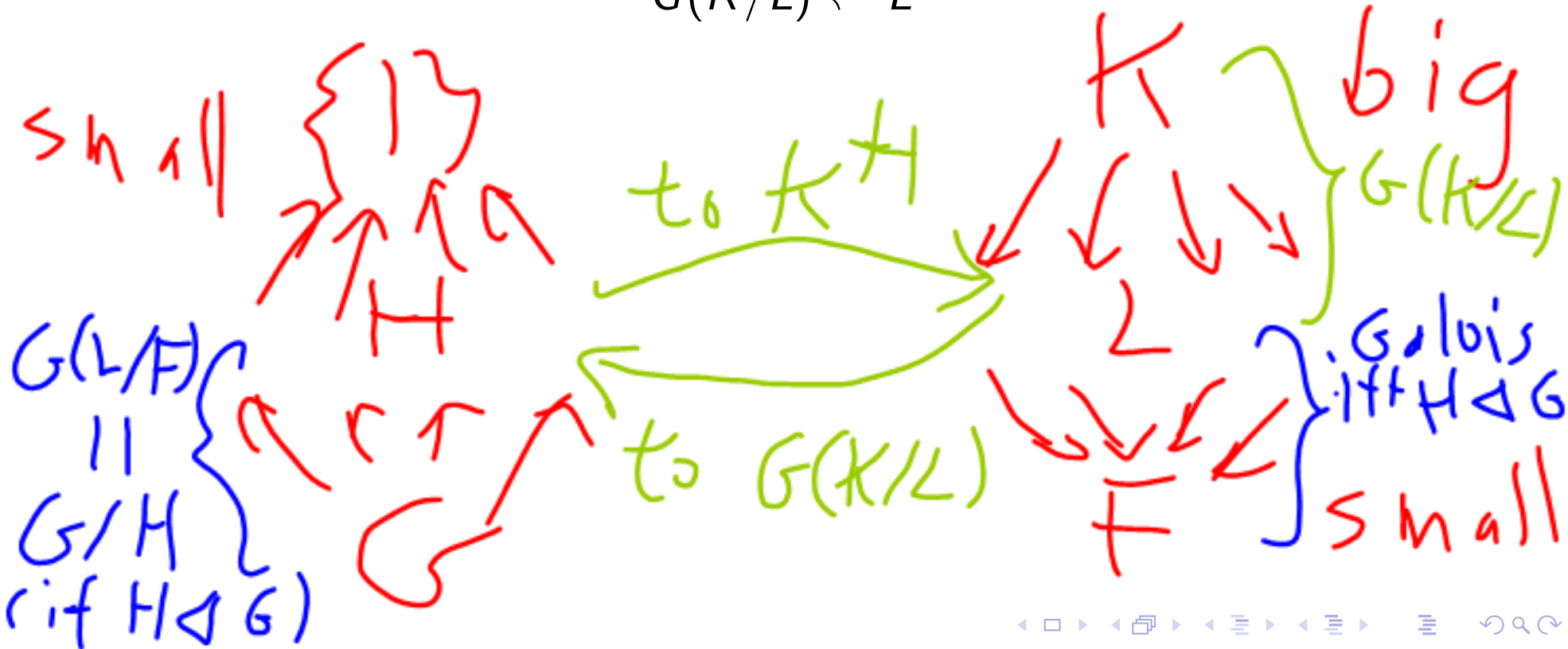
Theorem

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

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

$$H \mapsto K^H$$

$$G(K/L) \leftarrow L$$



Normal subgroups and extensions

Galois theory of (intermediate over base) works less well than (big field over intermediate). (more complicated/confusing)

Theorem

Suppose K/F Galois, $G = G(K/F)$, $H \leq G$, $L = K^H$. Then L/F Galois $\Leftrightarrow$ $H \lhd G$, 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 $\Rightarrow$ g splits in K so roots $\epsilon_1, \ldots, \epsilon_r$ of g are in K. We also know:

any irr w/ a root in K splits completely, not just the one we started off with.

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

(A) $\epsilon_i \in L = F(\epsilon_1)$

Then $F(\epsilon_i) \subseteq L$ (b/c $F \subseteq L$)

But since $\deg(\epsilon_i) = r$,

$$[F(\epsilon_i) : F] = r = [F(\epsilon_1) : F]$$

So $F(\epsilon_i)$ is r-dim subsp of r-dim space L.

Normality, cont.

$L = F(\epsilon_1)$

$\epsilon_1 .. \epsilon_r$ roots of $g(x)$

Always: Other stabilizers correspond to conjugates

Choose $\sigma_i \in G$ such that $\sigma_i(\epsilon_1) = \epsilon_i$.

$\mathrm{Stab}_G(\epsilon_i) =$

WTS $\sigma_i H \sigma_i^{-1}$ a conjugate of H.

S'pose $g \in \sigma_i H \sigma_i^{-1}$ Then $g = \sigma_i h \sigma_i^{-1}$ for some $h \in H$

$g(\epsilon_i) = \sigma_i g \sigma_i^{-1}(\epsilon_1) = \sigma_i h \sigma_i^{-1} \sigma_i(\epsilon_1)$

$= \sigma_i h(\epsilon_1) = \sigma_i(\epsilon_1) = \epsilon_i$

$H = \mathrm{stab}_L(\epsilon_1)$

So $g \in \mathrm{stab}_G(\epsilon_i)$

Other direction similar.

So L splitting $\Leftrightarrow$ all ϵ_i in L $\Leftrightarrow$ all ϵ_i stab by H $\Leftrightarrow$ all $\sigma H \sigma^{-1} = H$

$\Leftrightarrow H \triangleleft G$.

Normal subgroups

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

$= $ elts of G that stab all $\epsilon_1 \cdots \epsilon_r$

$=$ intersection of stabs ... even if $H \not\lhd G$

$=$ " of $\sigma H \sigma^{-1}$

$= H$.

(1st isomorphism theorem!!!!)

So action gives injection $G/H \to G(L/F)$. Compare orders:

$|G/H| = \dfrac{|G|}{|H|} = \dfrac{|G|}{|\mathrm{stab}_G(\epsilon_1)|} = |\mathrm{orb}_G(\epsilon_1)| = r$

$G(L/F) =$ deg of $\epsilon_1 = r$

$L = F(\epsilon_1)$

So $G/H \cong G(L/F)$

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

over $\mathbb{Q}$

roots $\alpha, \omega\alpha, \bar{\omega}\alpha$

$\alpha = \sqrt[3]{2}$, $\omega = e^{\frac{2\pi i}{3}}$

$\omega^3 = 1$

$\bar{\omega} = \omega^2$

G is transitive subgroup of S_3, so G = S_3 or G = A_3 = C_3.

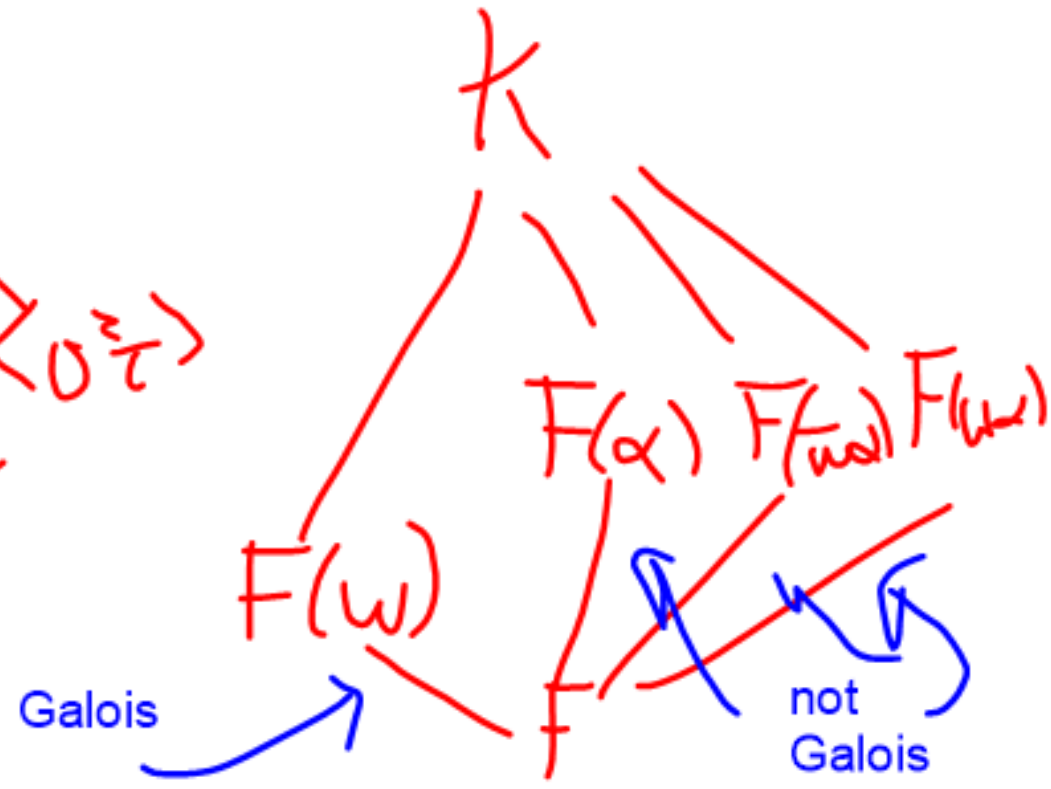
Complex conjugation fixes alpha and swaps other two roots, so G = S_3. So two elements of G must be:

$\sigma = (\alpha \ \omega\alpha \ \bar{\omega}\alpha)$

$\tau = (\omega\alpha \ \bar{\omega}\alpha)$

$\sigma\tau = (\alpha \ \omega\alpha)$

$Elts = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$



NB: $w = \frac{w\alpha}{\alpha}$, so $w \in k$.

$$\sigma(w) = \frac{\sigma(w\alpha)}{\sigma(\alpha)} = \frac{w^2\alpha}{w\alpha} = w$$

Transitive subgroups of S_n (esp. $n = 3$)

Transitive subgroups of S_n always include:

- Full symmetric group S_n
- Alternating group A_n (even permutations)
- Dihedral group $D_n = \langle (1\ 2\ \cdots\ n), (1\ n)(2\ n-1)\cdots \rangle$
- Cyclic group $C_n = \langle (1\ 2\ \cdots\ n) \rangle$

But also, any group of order n acts transitively on its elements, so any group can be a transitive subgroup of some S_n.

Note: When $n = 3$, $S_3 = D_3$, $A_3 = C_3$.

Generalities about cubics

Suppose

$$f(x) = x^3 - a_1x^2 + a_2x - a_3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

irreducible over F, K splitting field of f. Consider

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) = K,$$

where latter holds b/c $a_1 = \alpha_1 + \alpha_2 + \alpha_3$.
$[F(\alpha_1) : F] = 3$, and $[K : F]$ divides $6 = |S_n|$, so either

- $K = F(\alpha_1)$, $[K : F] = 3$, $G = A_3$ or
- $[K : F(\alpha_1)] = 2$, $[K : F] = 6$, $G = S_3$.

The (square root of the) discriminant

Let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

Note that

- $\delta \in K$.
- $\delta \neq 0$ because roots distinct (characteristic 0).
- $\delta = \pm\sqrt{D}$ (D discriminant; if $a_1 = 0$, $D = -4a_2^3 - 27a_3^2$)
- Action of $\sigma \in S_3$ on roots multiplies δ by sign of σ.

Computing Galois group of a cubic

Theorem

K splitting field of irr cubic f over F, D discriminant, $G = G(K/F)$.

- *If D is a square in F, $G = A_3$, $[K : F] = 3$.*
- *Otherwise, $G = S_3$, $[K : F] = 6$.*

Proof. Note that $\delta \in F \Leftrightarrow$ every permutation of G fixes δ.

Transitive subgroups of S_4

- Full symmetric group S_4
- Alternating group A_4 (even permutations)
- Dihedral group $D_4 = \langle (1\ 2\ 3\ 4), (1\ 4)(2\ 3) \rangle$
- Cyclic group $C_4 = \langle (1\ 2\ 3\ 4) \rangle$
- Klein 4-group $D_2 = \{\epsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Q: Given an irreducible quartic polynomial, which of these groups is its Galois group?
Next time. . . .