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: 16.9 and 16.11; for Mon: 16.12.
- Take-home exam 3 out tomorrow, due Mon. (But all deadlines are elastic.)
- Today's DJ: ?? Hsu

Problem session Fri: Discuss PS07-10, outstanding questions.

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 $G(K/L) \leq G$. Moreover, L/F is Galois iff $H = G(K/L) \lhd G$, in which case $G(L/F) = G/H$.
- Immediate problem: Given splitting field K of $f(x)$, compute $G(K/F)$.
- Eventual 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**.

Solvability starts with: Kummer extensions.

(Blue stuff is done; purple is today.)

K split of $f(x) = (x^2-2)(x^2-3)(x^2-5)$

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$|K:\mathbb{Q}| = 8$ so $|G| = 8$.

$S(X) =$ Sym on X

$|X| = n \Rightarrow S(X) \cong S_n$

G isom to subgp of

$S(\{\sqrt{2}, -\sqrt{2}\}) \times S(\{\sqrt{3}, -\sqrt{3}\}) \times S(\{\sqrt{5}, -\sqrt{5}\})$

This is because action of G preserves roots of (distinct) irreducible factors of f(x).

Before, when we said that "The action of G is faithful", that means that G is isom to a subgroup of the full group of symmetries preserving those orbits.

Proof of faithfulness of representation: If an element of G fixes all of the roots of f, we already know by defn of G(K/Q) that it fixes Q, so must fix all of K.

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 $D_2 = \{\epsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

symmetries of a square

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

A: Can almost completely resolve this by computation (but not quite).

(But in one case, the computation is complicated to describe.)

* There are methods (Jordan, 1870!!) for computing G(K/F) in general. But not practical, even with computers.
* Inverse Galois over C(t) solved by Riemann (late 1800s) w/ analysis + topology. (This would make a great expository master's thesis!)

Special case of quartic: $f(x) = x^4 + bx^2 + c$

I.e., roots of the form

$$\alpha = \sqrt{r + \sqrt{t}} \qquad \alpha' = \sqrt{r - \sqrt{t}}$$
$$-\alpha = \sqrt{r + \sqrt{t}} \qquad -\alpha' = \sqrt{r - \sqrt{t}}$$

G preserves square whose diagonals are $\pm\alpha$, $\pm\alpha'$. If f irreducible, G also transitive, so $G = D_4$, C_4, or D_2. Each contains

$$\rho = \sigma^2 = (\alpha \ -\alpha)(\alpha' \ -\alpha')$$

(180 deg rotation)

But hard to tell which other perms are actually automorphisms of K.

er

$f(x) = x^4 + bx^2 + c$, cont.

Let $N = \langle \rho \rangle = \langle (\alpha - \alpha)(\alpha' - \alpha') \rangle$. N fixes α^2 and $\alpha\alpha'$, each of which is the square root of an element of F. So if $L = F(\alpha^2, \alpha\alpha')$, we have

$$F \subseteq L \subseteq K^N \subseteq K.$$

Also $[K : K^N] = 2$ (Fixed Field Theorem) and $[K : F] \leq 8$ (Main Theorem and fact that $G \leq D_4$). So we can compute G by determining:

- What is $[L : F]$?
- Which elements send $\alpha \mapsto \alpha'$?

Full solution: 16.9 problems. We do one case.

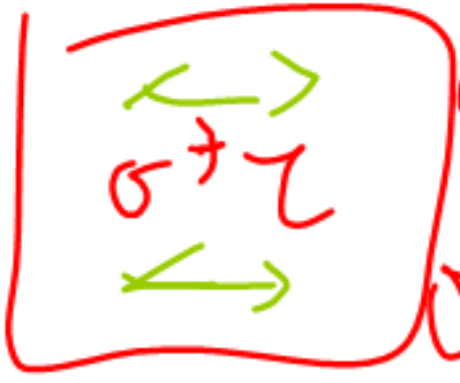
$\sigma = (\alpha\ i\alpha\ -\alpha\ -i\alpha)$

$\sigma^2 = P, \sigma^3 \in G$

$\sigma^2 = (\alpha\ -\alpha)\ (i\alpha\ -i\alpha)$

$\tau = (\alpha\ -\alpha)$

$\sigma^2\tau = (i\alpha\ -i\alpha)$



$\sigma^3\tau = (\alpha\ i\alpha)\ (-\alpha\ -i\alpha)$

$\sigma\tau = (\alpha\ -i\alpha)\ (-\alpha\ i\alpha)$

Example: $x^4 - 2$

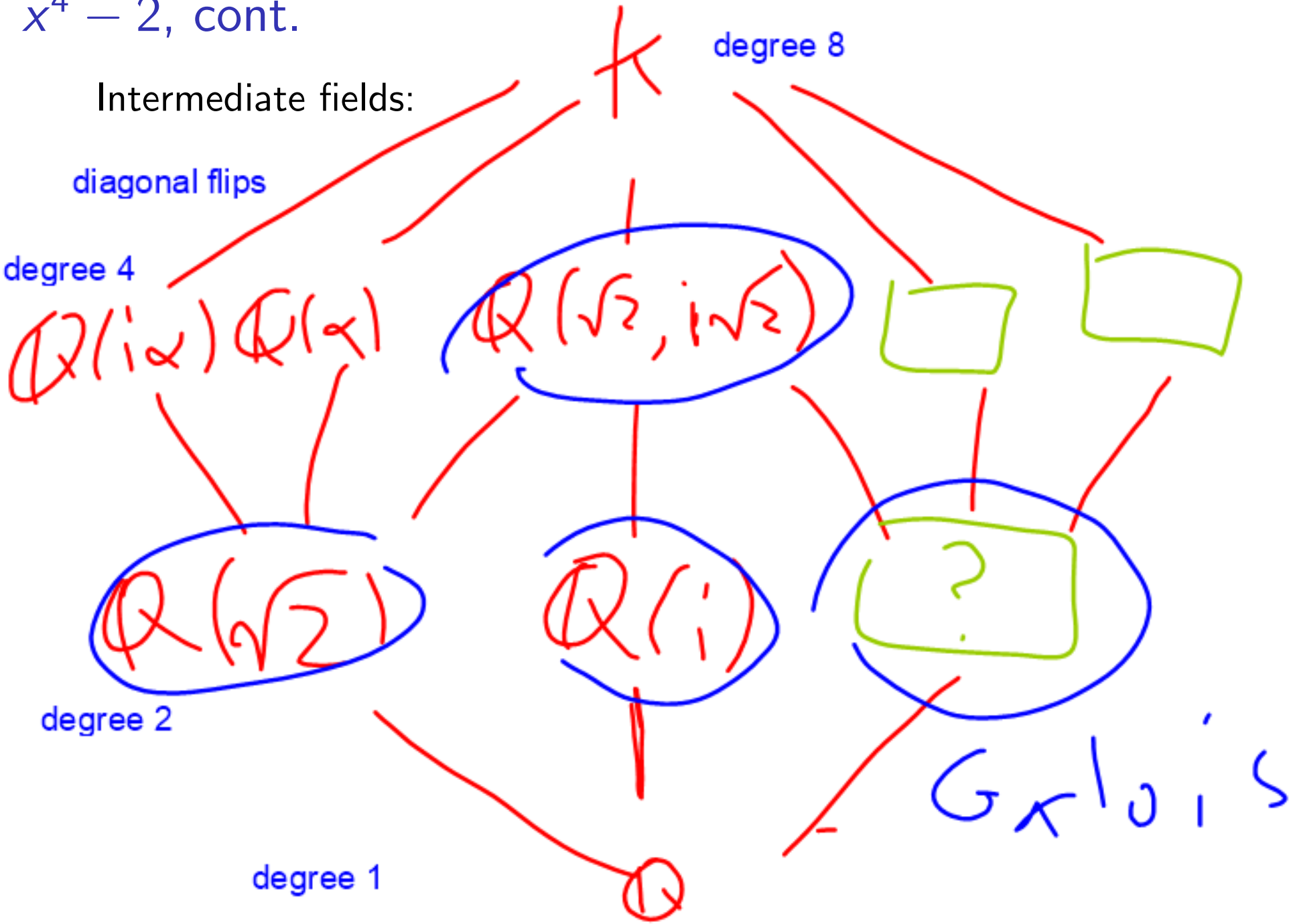
$\sigma = (\alpha \ \alpha' \ -\alpha \ -\alpha')$ (mult of roots by i)

Let $\alpha = \sqrt[4]{2}$. Roots are α, $-\alpha$, $\alpha' = i\alpha$, $-i\alpha$. Let $\tau = (\alpha \ -\alpha)$

$L = F(\alpha^2, \alpha\alpha') = F(\sqrt{2}, i\sqrt{2})$, so $[L : F] = 4$, $[K : F] = 8$, so $G = D_4$. Elements and subgroups of $G = G(K/F)$:

$x^4 - 2$, cont.

Intermediate fields:



$\sigma(\alpha) = i\alpha \qquad \sigma(i\alpha) = -\alpha$

$\sigma(i) = \sigma\left(\frac{i\alpha}{\alpha}\right)$

$= \frac{\sigma(i\alpha)}{\sigma(\alpha)} = \frac{-\alpha}{i\alpha} = i$

σ fixes i

The general quartic: δ

Let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4),$$

with $\delta^2 = D$ (discriminant).
As with the cubic, an odd permutation sends $\delta \mapsto -\delta$ and an even permutation fixes δ, so:

Theorem

If D is a square in F, then $G = A_4$ or D_2; otherwise $G = S_4$, D_4, or C_4.

(Analogous result holds for δ and D for any degree.)

The resolvent cubic

Let

$$\beta_a = \alpha_1\alpha_2 + \alpha_3\alpha_4 \quad \beta_b = \alpha_1\alpha_3 + \alpha_2\alpha_4 \quad \beta_c = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

Then

$$g(x) = (x - \beta_a)(x - \beta_b)(x - \beta_c)$$

is the resolvent cubic of f. Permutations of α_i preserve $\{\beta_a, \beta_b, \beta_c\}$, so:

coeffs of g are functions of alpha_i invariant under S_4
= polynomial combo of symmetric fns of alpha_i
= polynomial combo of coefficients of f

So g(x) in F[x], and is computable by (complicated) formula.

Also $\beta_a, \beta_b, \beta_c$ distinct, e.g.:

Resolvent cubic and G

Think of $G \subseteq S_4$, and let
$K = \{\epsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. K acts trivially on each of $\beta_a, \beta_b, \beta_c$, e.g.:

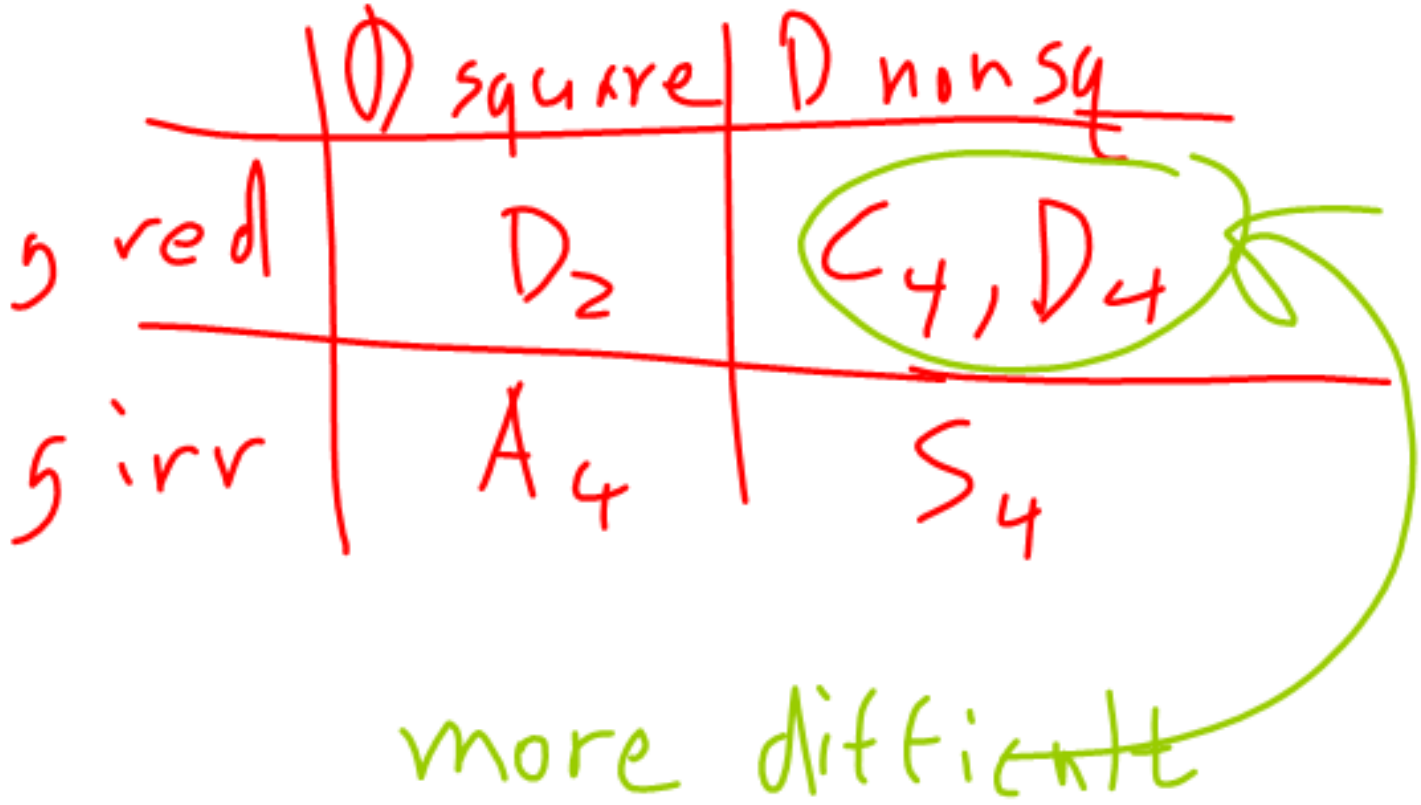
(exercise)

action of G on betas

So $G/(G \cap K)$ is isomorphic to some $\overline{G} \leq S_3$. 3 cases:

- g splits in F, $\overline{G}$ trivial, $G = K$.
- g has one root in F (say, $\beta_c \in F$), $\overline{G} \leq \langle (a\ b) \rangle$, $G = C_4$ or D_4.
- g irreducible, $\overline{G} = A_3$ or S_3, $G = A_4$ or S_4.

δ and resolvent cubic together



Kummer extensions

Definition

To say K/F is a **Kummer extension** means p prime, F subfield of $\mathbb{C}$, $\zeta = e^{2\pi i/p} \in F$, and K/F Galois of degree p.

Theorem

If K/F is a Kummer extension, then $K = F(\beta)$, where $\beta^p \in F$.

(I.e., elements of K are F-linear combinations of pth roots of elements of F.)

Proof of Kummer theorem

Theorem

If K/F is a Kummer extension, then $K = F(\beta)$, where $\beta^p \in F$.

Proof: Let $G = G(K/F) = \langle \sigma \rangle$ (since order p).

Considering K as a vector space over F, σ is an F-linear operator on K.:

Proof of Kummer Thm, cont.

Fact: Because σ finite order, σ can be diagonalized over $\mathbb{C}$ (!!!), with entries of diagonal form the eigenvalues of σ. Therefore, eigenvalues satisfy $\lambda^p = 1$. Can't have all $\lambda = 1$, so σ has some eigenvalue $\lambda \neq 1$ s.t. $\lambda^n = 1$.
So let $\beta \in K$ be an eigenvector of σ with eigenvalue $\lambda \neq 1$, and let $b = \beta^p$.

So $b \in F$. Furthermore,

So $\beta \notin F$. Then, since $[K : F] = p$ is prime, $K = F(\beta)$.