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: 16.8–16.9; for Wed: 16.9, 16.11.
- Take-home exam 3 due in 1 week. (But all deadlines are elastic.)
- Today's DJ: Apoorva.

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**.

(Blue stuff is done; purple is today.)

Q: How do you know which permutations are in G?

A: It's really difficult!

I don't personally know of any brute force methods for verifying if a particular permutation is in G(K/F). (Though let me get back to you on that.)

In practice, you narrow the list of suspects for G and use deduction to find certain elements of G, thus eliminating enough suspects to figure out what G is.

Basic method we'll see today: Find things that are left unchanged by a particular G, which will eliminate some suspects.

Q: In HW, we usually know the order of G, example: |G|=4, but how do we know if it's C_4 or Z/(2)xZ/(2)?

Partial answer: We can use some (known) images of field elements and the definition of automorphism to deduce the images of other elements.

Remind me to do sqrt(2+sqrt(2)) or sqrt(4+sqrt(7)) when we get to quartics.

Major open problem (open for ~100 years?): Inverse Galois conjecture

Conjecture: Given any finite group G, there exists some extension K of Q such that G(K/Q) = G.

Master's thesis: Explain work on Inverse Galois conjecture, e.g., how the conjecture can be solved (in some cases?) if K=C(t). (Or is it K/C(t)? I can't remember but I'll look it up before Wed.)

Last: Galois group of x^3-2.

Today: General case of cubics.

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) (n >= 3)
- Dihedral group $D_n = \langle (1\ 2\ \cdots\ n), (1\ n)(2\ n-1)\cdots \rangle$
- Cyclic group $C_n = \langle (1\ 2\ \cdots\ n) \rangle$

full & rotational symms of n-gon

reg

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

Discriminant D is this but squared

Let

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

Odd perms negate delta, even perms preserve delta (leave delta invariant).

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.

If sigma = (i i+1), σ negates $(\alpha_i - \alpha_{i+1})$, permutes other terms.

Every permutation is a product of transpositions of form (i i+1).

Computing Galois group of a cubic

Theorem

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

- *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.

So D is a square in F

every permutation of G is even.

G = A_3.

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?

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

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

I.e., roots of the form

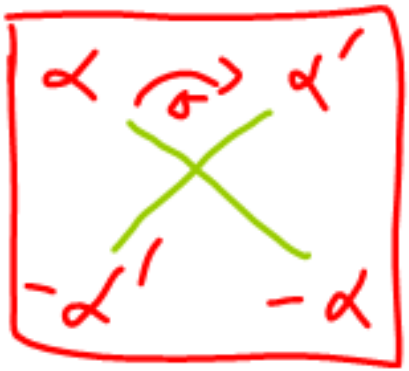
$$\alpha = \sqrt{r + \sqrt{t}} \qquad \alpha' = \sqrt{r - \sqrt{t}}$$

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

Note that any $\varphi \in G = G(K/F)$ has $\varphi(-\alpha) = -\varphi(\alpha)$. So $G(K/F)$ is a subgroup of the symmetries of a square:

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

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



Action of G preserves green "diagonals", so each element of G is a symmetry of this square.

$G \leq D_4 = \langle \sigma, \tau \rangle$

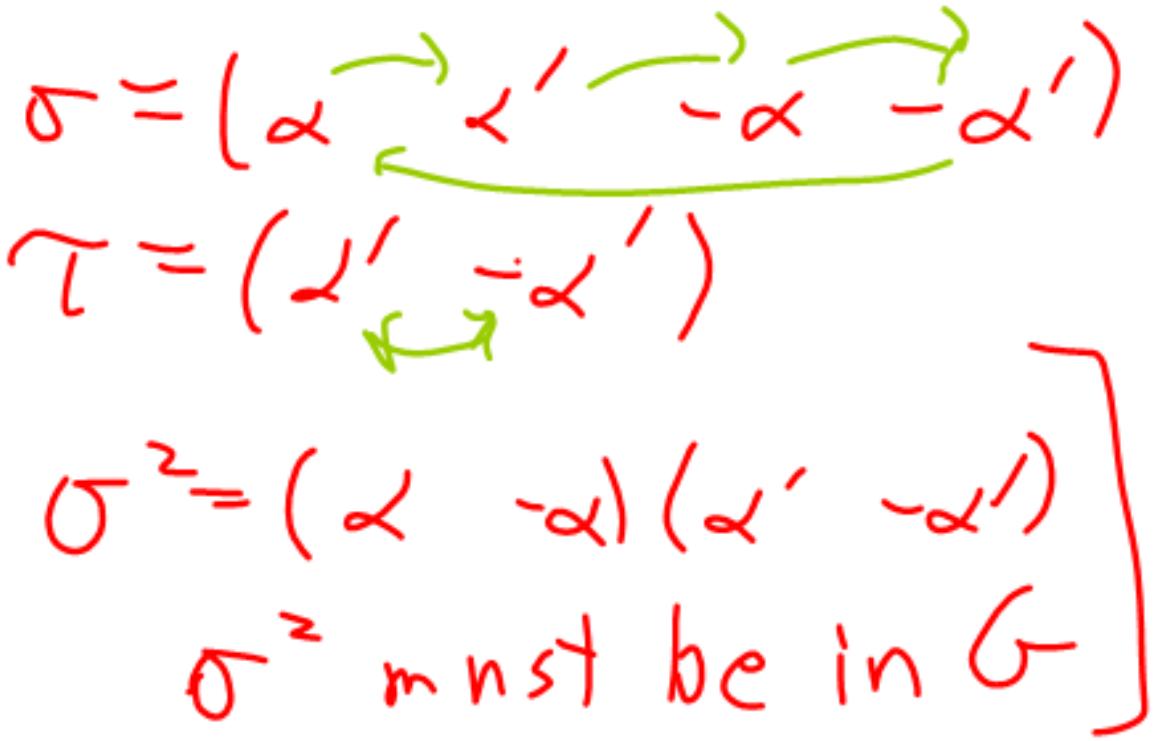
If f irreducible, G also transitive, so $G = D_4$, C_4, or D_2. Each contains

$(\alpha\ -\alpha)(\alpha'\ -\alpha')$

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

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

Elements of D_4, in better handwriting:



We use fields to show that G preserves square, and groups to show that G must contain sigma^2.

So we look for field elements invariant under sigma^2.

Q: Is sigma always in G?

A: If G = D_4 or C_4, yes; but not if G = D_2.

It can be the case that sigma is in G because it preserves green lines *setwise*, just not individually.

$f(x) = x^4 + bx^2 + c$, 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 $\alpha \mapsto \alpha'$?

G acts transitively on roots, so one such element must exist.

Full solution: 16.9 problems. We do one case.

Example: $x^4 - 2$

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

$[L : F]$ is:

$= [L : F(\alpha^2)][F(\alpha^2) : F]$, $\alpha^2 = \sqrt{2}$, $\alpha\alpha' = i\sqrt{2}$

$F(\alpha^2) \subseteq \mathbb{R}$, $L \not\subseteq \mathbb{R}$

$[L : F] = 4$

So $|G| = 8$, $G = D_4$

gp thy

$F(\alpha^2) = F(\sqrt{2})$

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

$L = K^N$

Field thy

Elements of $G = G(K/F)$:

$x^4 - 2$, cont.

Intermediate fields and subgroups:

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 $D = A_4$ or D_2; otherwise $D = S_4$, 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:

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.:

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, $\beta_c \in F$), $\overline{G} = \langle (a\ b) \rangle$, $G = C_4$ or D_4.
- g irreducible, $\overline{G} = A_3$ or S_3, $G = A_4$ or S_4.

δ and resolvent cubic together