Welcome back

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: 16.4–16.5; for Wed: 16.6.
- PS08 due today; PS09 due Mon Apr 20. (But all deadlines are elastic.)
- Today's DJ: Carlos.

Galois theory in a nutshell

Q: Why do these alpha exist?

Suppose K/F is the **splitting field** of an irreducible polynomial $f(x) \in F[x]$; i.e.,

We can always construct one alpha by F[x]/f(x), then repeat on what's left to factor.

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

A: They are assumed to exist for this defn; defn just names what happens when they exist.

and $K = F(\alpha_1, \dots, \alpha_n)$.

Note: we can always construct roots we need.

- **Galois theory** relates the field theory properties of K/F (e.g., degree) and the group-theoretic properties of the group of field automorphisms of K fixing F.
- These automorphisms must permute $\alpha_1, \dots, \alpha_n$ and are therefore isomorphic to a transitive subgroup of S_n.
- Signature problem: When can $\alpha_1, \dots, \alpha_n$ 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.)

Last: The Splitting Theorem

Theorem

Suppose K/F is a splitting field of $f(x) \in F[x]$. If $g(x) \in F[x]$ is irreducible and has at least one root in K, then $g(x)$ splits in K.

So a splitting field K ensures splitting not just of f, but of *any* irreducible g(x) with at least one root in K.

16.4 Isomorphisms of field extensions

(Galois theory is about automorphisms of....)

Definition

An F-**isomorphism** $\sigma : K/F \to K'/F$ is an isomorphism fixing F. If $K = K'$, get a F-**automorphism** (symmetry of K/F).

Definition

$G(K/F)$ is the group of all F-automorphisms of K/F, called the **Galois group** of K/F.

Definition

To say a finite extension K/F is a **Galois extension** means that $|G(K/F)| = [K : F]$. (As we'll see, this is largest possible.)

largest possible order of G(K/F)

Example: Complex conjugation is an $\mathbb{R}$-automorphism of the extension $\mathbb{C}/\mathbb{R}$, and $\mathbb{C}/\mathbb{R}$ is a Galois extension.

$G(\mathbb{C}/\mathbb{R}) = \{id, -\}$, $|=2$

Example: If d square-free, $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, and $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ is Galois.

symmetry in quad formula

Non **Example:** (to be proven) $\left|G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})\right| = 1$, so $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not Galois.

only Q-automorphism is identity

degree 3

First facts about F-isomorphisms

Pf 1. Apply sigma to f(alpha)=0.

1. $\sigma : K/F \to K'/F$ an F-isomorphism, $f(x) \in F[x]$. If α is a root of f in K, then $\sigma(\alpha)$ is a root of f in K'.
2. Suppose $K = F(\alpha_1, \ldots, \alpha_n)$. An F-isomorphism is determined by the images of $\alpha_1, \ldots, \alpha_n$; in particular, if σ is an automorphism of K/F that fixes $\alpha_1, \ldots, \alpha_n$, then σ is the identity.
3. Suppose $f(x) \in F[x]$ irreducible, α, α' roots of f in $K/F, K'/F$. There exists a unique F-isomorphism $\sigma : F(\alpha) \to F(\alpha')$ such that $\sigma(\alpha) = \alpha'$.

Existence:

$F(\alpha) \cong F[x]/(f)$

$F(\alpha') \cong$

So for example, if $K = f(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F and $\alpha_1, \ldots, \alpha_n$ are all of the roots of f, then we can think of elements of $G(K/F)$ as permutations of $\alpha_1, \ldots, \alpha_n$.

Proof that $\left|G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})\right| = 1$: $\omega^3 = 1$ $\left(\omega = e^{\frac{2\pi i}{3}}\right)$

Roots of x^3-2 are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

Elt of G( ) must permute the roots of x^3-2, but other roots not in $\mathbb{Q}(\sqrt[3]{2})$.

More about splitting fields

Splitting fields unique (up to isomorphism)

Theorem

If K_1/F, K_2/F are splitting fields of $f \in F[x]$, then K_1/F and K_2/F are F-isomorphic.

Proof. First show that any L/F contains at most one splitting field of f over F:

Splitting field of f in L must be F(roots of f in L), and these roots are the only possible roots of f in L, so both K1 and K2 = F(roots of f in L).

Primitive Elt Thm says that $K_1 = F(\gamma)$. Let $g(x)$ be irreducible poly of γ over F. (exists b/c gamma algebraic over F)
Let $L \supseteq K_2$ contain a root γ' of g, let $K' = F(\gamma')$.

First factor g into irrs over K_2, pick one irred factor g_1(x).

Then $L = K_2[x]/(g_1(x))$

By previous observations, K_1/F and K'/F are F-isomorphic, so K' is a splitting field of f(x). By previous case, K' = K_2.

16.5: Fixed fields

Definition

H a group of automorphisms of field K. **Fixed field** of H is

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

all elements of K fixed by *every* element of H.

K^H is a subfield of H, $H \leq G(K/K^H)$; in fact:

Theorem (Fixed Field Thm)

H a finite group of automorphisms of field K, $F = K^H$. Then K/F finite and $[K : F] = |H|$.

I.e., no "hidden" automorphisms of K over the fixed field K^H.

no "surprise" automorphisms

Irreducible polynomial via symmetrizing

Theorem

(What happens if beta_1 in F?)

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 $|H|$.)*

Proof that g is the irr poly. Let

orbit-stabilizer FTW!!!!!

$$g(x) = (x - \beta_1) \ldots (x - \beta_r) = x^r + b_1 x^{r-1} + \cdots + b_r.$$

Because beta_1 ... beta_r is an H-orbit, action of H permutes beta_1 ... beta_r.
But coeffs b_1 ... b_r of g(x) are elementary symmetric functions of the betas, so they don't change when you permute the betas.
So coeffs b_1 ... b_r are fixed by every element of H, i.e., b_1 ... b_r are in the fixed field of H, which by hypothesis, is F.

So each $b_i \in F$, i.e., $g(x) \in F[x]$.

Suppose $h(x) \in F[x]$, $h(\beta_1) = 0$.

WTS each β_i is root of h.

B/c β's H-orbit, $\exists \sigma_i \in H$ s.t. $\sigma_i(\beta_1) = \beta_i$.

Coeffs of h are in fixed field, so

$\Rightarrow \sigma(h(\beta_1)) = \sigma(0) \Rightarrow h(\sigma(\beta_1)) = 0$

$\Rightarrow h(\beta_i) = 0$

So each β_i is root of $h \Rightarrow$ each $(x - \beta_i)$ divides $h \Rightarrow g(x) = (x-\beta_1)\cdots(x-\beta_r)$ divides h.

So g divides h, i.e., g generates ideal of polys with root β_1.

Proof of Fixed Field Theorem

Theorem (Fixed Field Thm)

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

Lemma: IF K/F is algebraic but $[K : F] = \infty$, there is no upper bound for degrees of elements of K. (Proof: Make subfields of arbitrarily large degree.)

Proof of Fixed Field Thm: By symmetrizing, every element of K is algebraic. Lemma implies:

If [K:F] were infinite, then Lemma implies there would be elements of arbitrarily large degree. But previous result shows that degree of any elt of K over F is at most |H|.

Let $K = F(\gamma)$, i.e., γ primitive. If $\sigma(\gamma) = 1$, then:

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

Example: Problem 16.5.1(a)

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

$$H = \langle \sigma \rangle = \qquad\qquad |H| =$$

By symmetrizing, irr poly of t over F is:

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

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

Characterization of Galois extensions

Theorem

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

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

Lemmas:

1. If $[K : F] < \infty$, then $G(K/F)$ finite and divides $[K : F]$.
2. If H is a finite group of automorphisms of K, then K/K^H is Galois and $H = G(K/K^H)$.
3. 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.