Math 128B, Wed May 12

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Last reading of the semester: Ch. 32. and supplemental notes.
- PS10 due tonight; PS11 outline due Fri.
- Final exam, **Tue May 25**.

Problem session/checkin on Fri, on PS10 and PS11

Comprehensive, emphasizing PS10-11 somewhat.
But PS01-09 are fair game!

Final exam review, Mon May 24 9:45am

The Galois group of a field extension (Review)

F a field, E an extension of F.

An *automorphism* of E is a ring isomorphism $\varphi : E \to E$.

The *Galois group of E over F* is:

$$\mathrm{Gal}(E/F) = \{\varphi \in \mathrm{Aut}(E) \mid \varphi(x) = x \text{ for all } x \in F\}.$$

Automorphisms of E that fix everything in F.

If $H \leq \mathrm{Gal}(E/F)$, we define the *fixed field of H* to be

$$E_H = \{x \in E \mid \varphi(x) = x \text{ for all } \varphi \in H\}.$$

All elements of E that are fixed by every element of H.

(Most difficult part of Galois theory: Given E/F, compute Gal(E/F). See Math 221B, or Google "Inverse Galois problem".)

More examples

$E =$

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.

$\alpha = \sqrt[3]{7}$

$\omega = e^{2\pi i/3}$

$E = \mathbb{Q}(\alpha, \omega)$

Roots of: $\alpha, \alpha\omega, \alpha\omega^2$

$G = Gal(E/\mathbb{Q}) \simeq S_3$

e.g. $(\alpha\ \alpha\omega\ \alpha\omega^2) \in G$

$G =$ all perms of $\{\alpha, \alpha\omega, \alpha\omega^2\}$

~~**Example:** Splitting field of $x^4 - 2$ over $\mathbf{Q}$.~~

How does a permutation of those roots determine an automorphism of E fixing Q?

Recall $\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha\omega^2\}$

is basis for E over $\mathbb{Q}$.

$c_i \in \mathbb{Q}$

So elts of E are $c_1 1 + c_2\alpha + \cdots + c_6\alpha\omega^2$

So if $\varphi : E \to E$ ring homom.

and we know $\varphi(\alpha), \varphi(\alpha w), \varphi(\alpha w^2)$,

then $\varphi(\alpha^2) = \varphi(\alpha)^2$ ✓ $\varphi(1) = 1$

Ring homoms on a field preserve division!

$$\varphi(w) = \varphi\left(\frac{\alpha w}{\alpha}\right) = \frac{\varphi(\alpha w)}{\varphi(\alpha)}$$

So if we know values of phi on $\alpha, \alpha w, \alpha w^2$ then we know what phi must do to be a field automorphism.

The hard part is showing that you can actually extend this map consistently to get a valid automorphism.

Ex. E = sp. field of x^4-2 over $\mathbb{Q}$

$\alpha=\sqrt[4]{2}$, $i^4=1$; $E=\mathbb{Q}(\alpha,i)$

$G=\mathrm{Gal}(E/\mathbb{Q})\approx D_4$, symms of Roots of x^4-2:

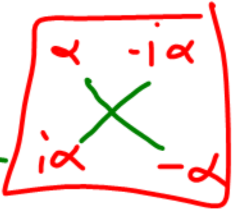
$G=\{e, (\alpha\ \ i\alpha\ \ -\alpha\ \ -i\alpha)$

$(\alpha\ \ -\alpha)(i\alpha\ \ -i\alpha),$

$(\alpha\ \ -i\alpha\ \ -\alpha\ \ i\alpha),$

$(i\alpha\ \ -i\alpha), (\alpha\ \ -\alpha),$

$(\alpha\ \ i\alpha)(-\alpha\ \ -i\alpha), (\alpha\ \ -i\alpha)(-\alpha\ \ i\alpha)\}$



Any perm inducing a field autom must preserve these "diagonals"

$E =$ s.f. of $x^4 - 4 = (x^2-2)(x^2+2)$

$\cong$ perms on $\pm\sqrt{2}, \pm\sqrt{2}\,i$

$\langle(\sqrt{2}\ \ -\sqrt{2})\rangle \times \langle(\sqrt{2}\,i\ \ -\sqrt{2}\,i)\rangle$

$C_2 \oplus C_2$

$E =$ s.f. of $x^2 - 1 = \mathbb{Q}$

$\mathrm{Gal} = \{e\}$

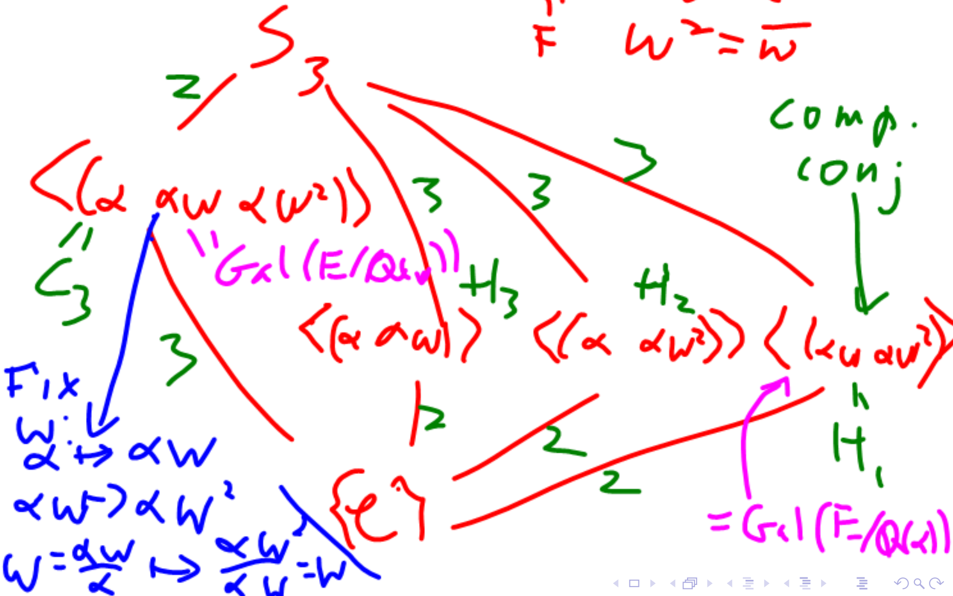
Subgroups of Gal(E/F)

$\alpha, \alpha\omega, \alpha\omega^2$ $\alpha = \sqrt[3]{7}$

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.

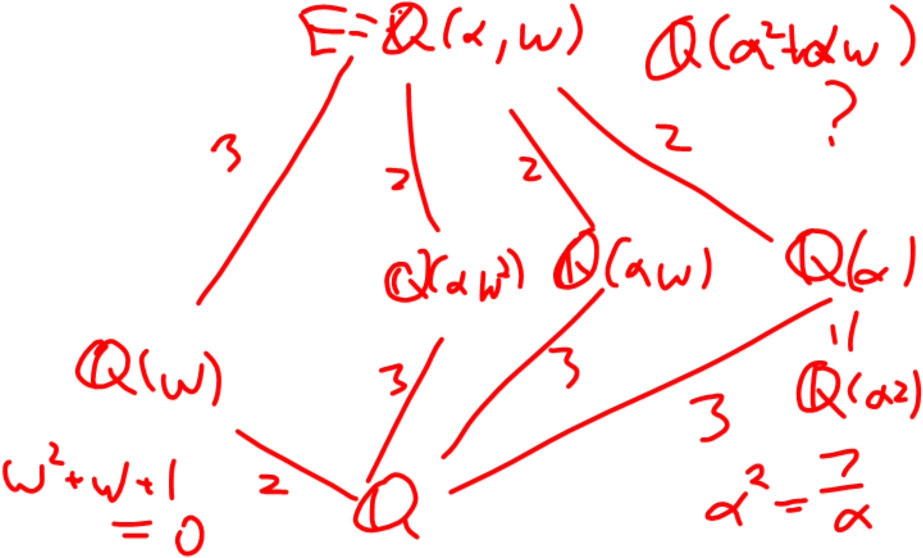
$\omega = e^{\frac{2\pi i}{3}}$

$\shortparallel$ F $\omega^2 = \overline{\omega}$

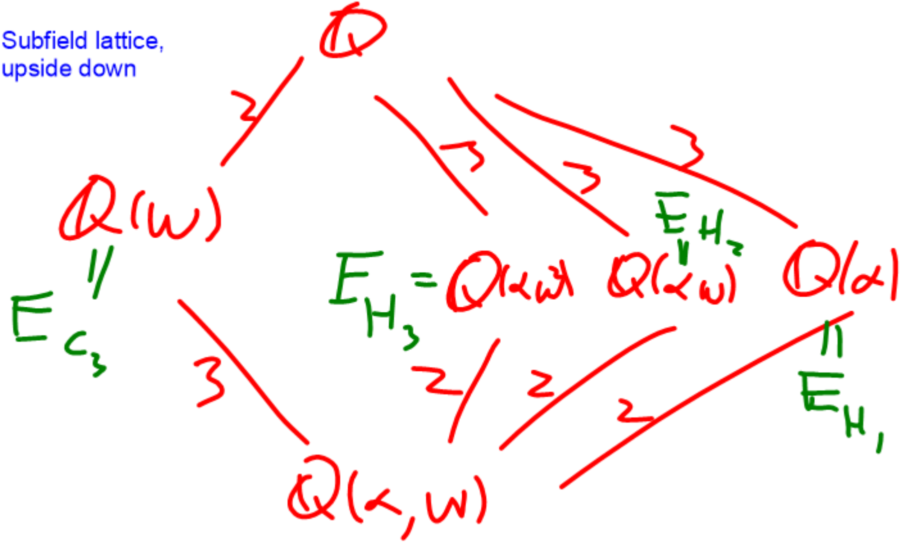


Subfields of E containing F

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.



Subfield lattice,
upside down



Fundamental Theorem of Galois Theory

See handout, not Gallian.

Let F be a field of characteristic 0 or a finite field, and let E be the splitting field of some $f(x) \in F[x]$. Let $\mathcal{S}$ be the set of all subgroups of $\mathrm{Gal}(E/F)$, and let $\mathcal{F}$ be the set of all subfields of E containing F.

Define $\Phi : \mathcal{S} \to \mathcal{F}$ and $\Psi : \mathcal{F} \to \mathcal{S}$ by

$H \leq G = \mathrm{Gal}(E/F)$

$\Phi(H) = E_H =$ the fixed field of H,

$\Psi(K) = \mathrm{Gal}(E/K) =$ the group of all automorphisms of E fixing K.

$K, L \subseteq E$

Then Φ and Ψ are inverses of each other, and therefore, bijections. Furthermore, if K, L subfields of E containing F, then

$$K \subseteq L \qquad \Leftrightarrow \qquad \mathrm{Gal}(E/K) \geq \mathrm{Gal}(E/L)$$

(I.e., Φ and Ψ are inclusion-reversing.)

If L is bigger than K, then fixing every element of L implies fixing every element of K.

Fundamental Theorem of Galois Theory, cont.

If K, L subfields of E containing F:

1. $[E : K] = |\mathrm{Gal}(E/K)|$, and therefore,

$$[K : F] = |\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)| = \frac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|}.$$

2. K is a splitting field of some $g(x) \in F[x]$ if and only if $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$. In that case,

$$\mathrm{Gal}(K/F) \approx \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K).$$

3. The group $\mathrm{Gal}(E/F)$ acts on (permutes) the set $X = \{a_1, \ldots, a_n\}$ of all zeros of $f(x)$ in E.
4. If $f(x)$ is irreducible over F, then $\mathrm{Gal}(E/F)$ acts transitively on $X = \{a_1, \ldots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a_i) = a_j$.

Picture of the Fundamental Theorem

Example: Splitting field of $x^3 - 7$

Example: Splitting field of $x^4 - 2$

Solvability by radicals

Definition

F a field, $f(x) \in F[x]$. To say $f(x)$ **solvable by radicals over** F means F splits in some $F(a_1, \ldots, a_n)$ such that $a_1^{k_1} \in F$, $a_2^{k_2} \in F(a_1)$, $a_3^{k_3} \in F(a_1, a_2)$, and so on.

Definition

To say a group G is **solvable** means there exist

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G,$$

where each H_i/H_{i-1} is abelian.

In general, a solvable group is made by "sticking together abelian pieces."

Solvable and non-solvable examples

Example: D_n is solvable because:

Example: A_n is non-solvable because:

Example: S_n is non-solvable because:

Extensions by roots are solvable

Theorem

F characteristic 0, $a \in F[x]$, E splitting field of $x^n - a$ over F. Then $\operatorname{Gal}(E/F)$ is solvable.

Why: Let $\alpha^n = a$, $\omega^n = 1$. Note that $F(\omega)$ is the splitting field of $x^n - 1$. Turns out that:

1. Each element of $\operatorname{Gal}(E/F(\omega))$ is defined by fixing ω and sending α to $\alpha\omega^k$ for some k. Those maps all commute, so $\operatorname{Gal}(E/F(\omega))$ is abelian.

2. $\operatorname{Gal}(F(\omega)/F)$ consists of maps sending ω to ω^j; those maps all commute, so $\operatorname{Gal}(F(\omega)/F)$ is abelian.

Then we have $\{e\} \lhd \operatorname{Gal}(E/F(\omega)) \lhd \operatorname{Gal}(E/F)$. Also $\operatorname{Gal}(E/F(\omega))$ is abelian, as is

$$\operatorname{Gal}(E/F)/\operatorname{Gal}(E/F(\omega)) \approx \operatorname{Gal}(F(\omega)/F).$$

Group-theoretic facts

Theorem

If G solvable, $N \lhd G$, then G/N is solvable.

Why: Take quotients of each step of solvable chain.

Theorem

If N and G/N solvable, then G solvable.

Why: Can "stick together" the solvable chains.

Theorem

Suppose F a field, $f(x) \in F[x]$; $F(a_1, \ldots, a_n)$ such that $a_1^{k_1} \in F$, $a_2^{k_2} \in F(a_1)$, $a_3^{k_3} \in F(a_1, a_2)$, and so on; and E splitting field for f in $F(a_1, \ldots, a_n)$. Then $\mathrm{Gal}(E/F)$ is solvable.

Why: Works for splitting one $x^{k_i} - a_i$ by previous result; then above group-theoretic results allow us to stick solvable pieces together to get a solvable group.

Insolvability of the quintic

Suppose $f(x) \in \mathbf{Q}[x]$ is irreducible over $\mathbf{Q}$ with 3 real roots.

- Can show that if E is the splitting field of f over $\mathbf{Q}$, then $\mathrm{Gal}(E/\mathbf{Q}) \approx S_5$.
- S_5 isn't solvable, so can't express zeros of f in terms of roots.

So no quintic formula!

Better proof: Show that almost every irreducible nth degree polynomial over $\mathbf{Q}$ has Galois group S_n. So **random** irreducible polynomial not solvable by roots — in fact, because of the A_n piece, best way to express zeros of polynomial is "the zeros of this polynomial".