# 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.
- PS11 due tonight.
- Final exam, **Tue May 25**. 9:45 am

Zoom link is same as class
Zoom link

# The Galois group of a field extension

$F$ 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:

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

all automorphisms of E that fix every element of 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 fixed by every element of H

# Fundamental Theorem of Galois Theory

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 $\text{Gal}(E/F)$, 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

$$\Phi(H) = E_H = \text{the fixed field of } H,$$
$$\Psi(K) = \text{Gal}(E/K) = \text{the group of all automorphisms of } E \text{ fixing } K.$$

Then $\Phi$ and $\Psi$ are inverses of each other, and therefore, bijections. Furthermore, if $K$, $L$ subfields of $E$ containing $F$, then

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

(I.e., $\Phi$ and $\Psi$ are inclusion-reversing.)

# Fundamental Theorem of Galois Theory, cont.

If $K$, $L$ subfields of $E$ containing $F$:

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

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

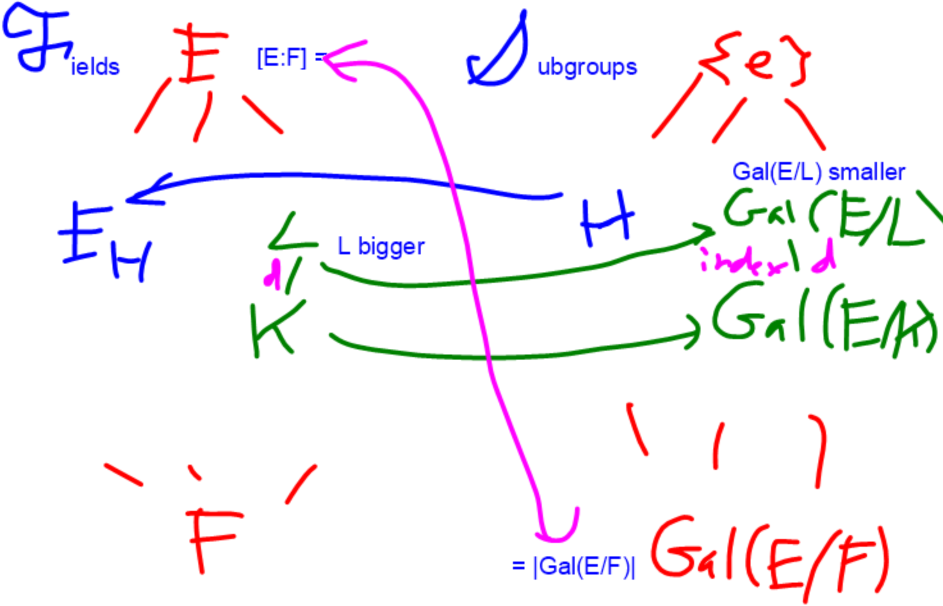
2. $K$ is a splitting field of some $g(x) \in F[x]$ if and only if $\text{Gal}(E/K)$ is normal in $\text{Gal}(E/F)$. In that case,

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

3. The group $\text{Gal}(E/F)$ 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 $\text{Gal}(E/F)$ acts transitively on $X = \{a_1, \ldots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \text{Gal}(E/F)$ such that $\sigma(a_i) = a_j$.

Galois groups are perm groups

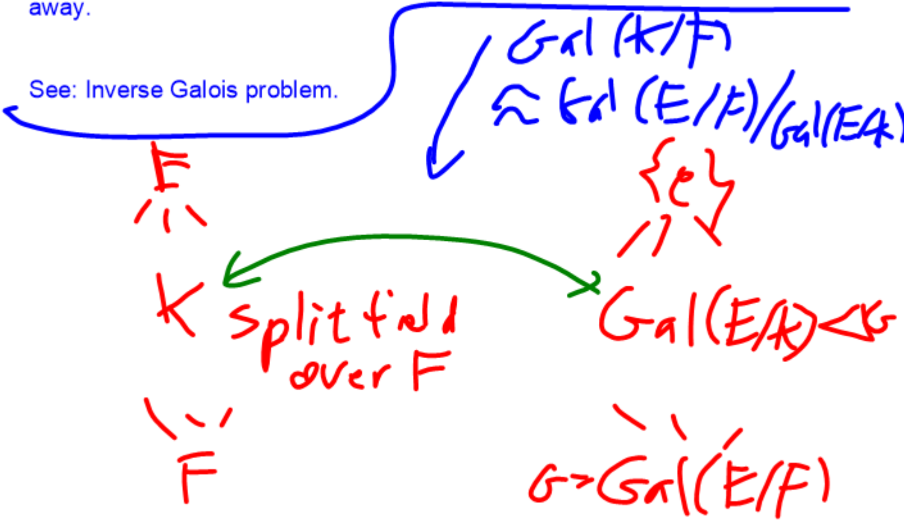
# Picture of the Fundamental Theorem



Q: Is every finite group a Galois group of some finite extension of Q?

A (2021): No one knows. Best guess is yet, but a proof seems pretty far away.

See: Inverse Galois problem.



E splitting field of f(x) over F

FTGT => If f(x) is irreducible, then Gal(E/F) permutes the roots of f transitively.

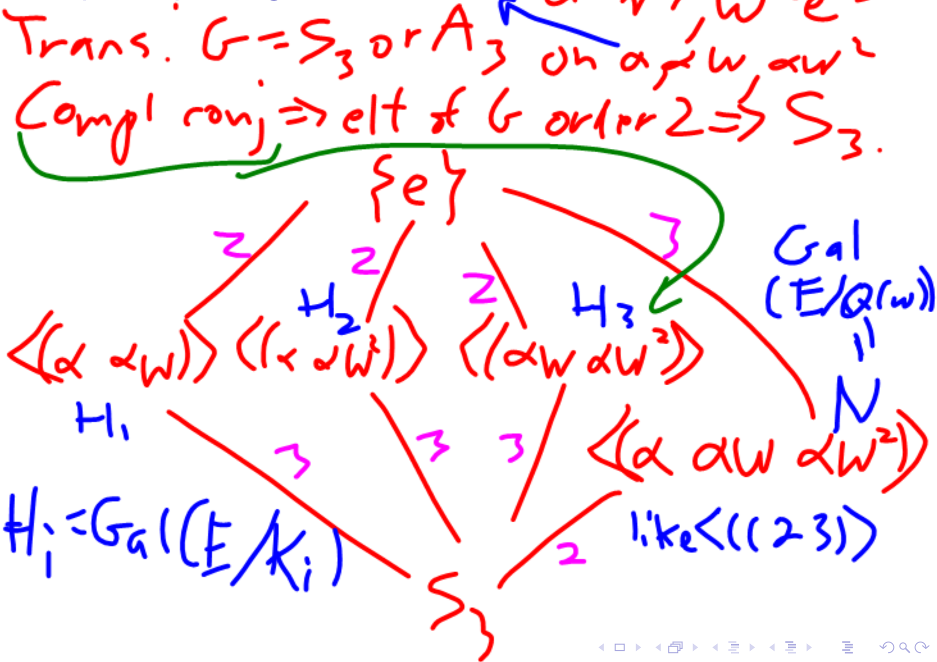
Ex. deg f = 4, E = split of f(x) over F

$G = \mathrm{Gal}(E/F) \leq S_4$

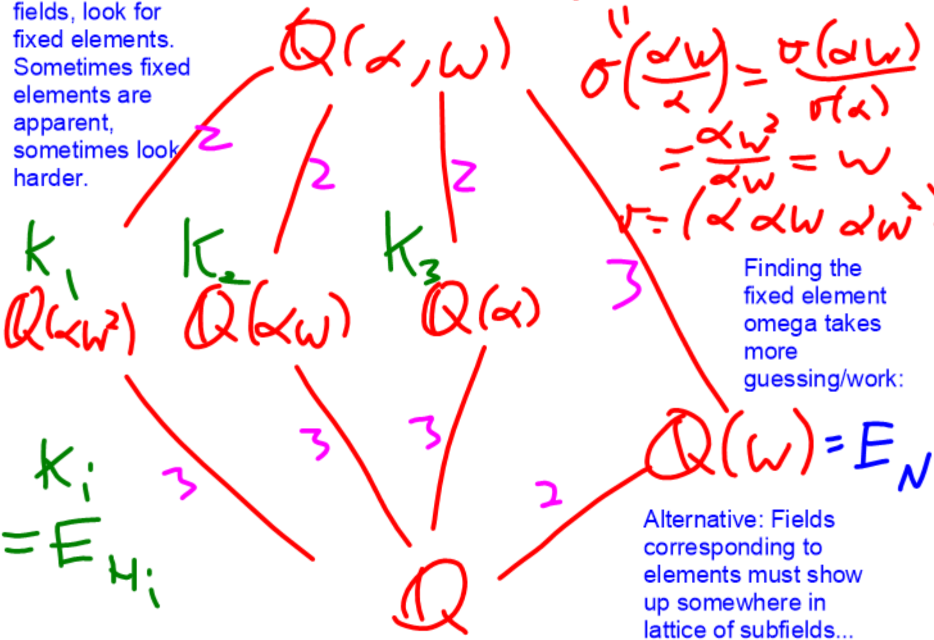
Trans $\Rightarrow G \cong S_4, A_4, D_4, C_4, V$

(These are the only transitive subgroups of S_4.)

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



To look for fixed fields, look for fixed elements. Sometimes fixed elements are apparent, sometimes look harder.




$$\sigma(\omega) = \sigma\left(\frac{\alpha\omega}{\alpha}\right) = \frac{\sigma(\alpha\omega)}{\sigma(\alpha)} = \frac{\alpha\omega^2}{\alpha\omega} = \omega$$

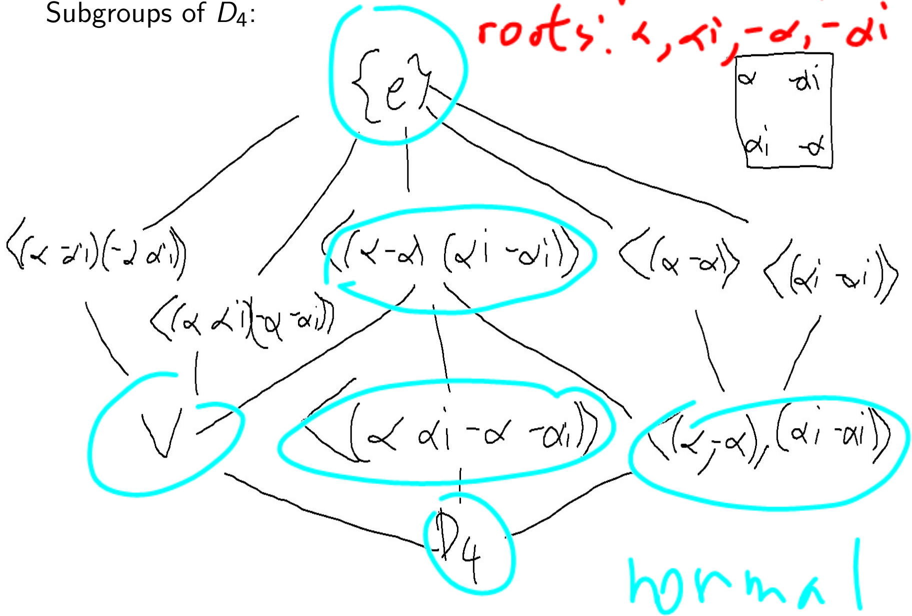
$$\sigma = (\alpha \;\; \alpha\omega \;\; \alpha\omega^2)$$

Finding the fixed element omega takes more guessing/work:

Alternative: Fields corresponding to elements must show up somewhere in lattice of subfields...

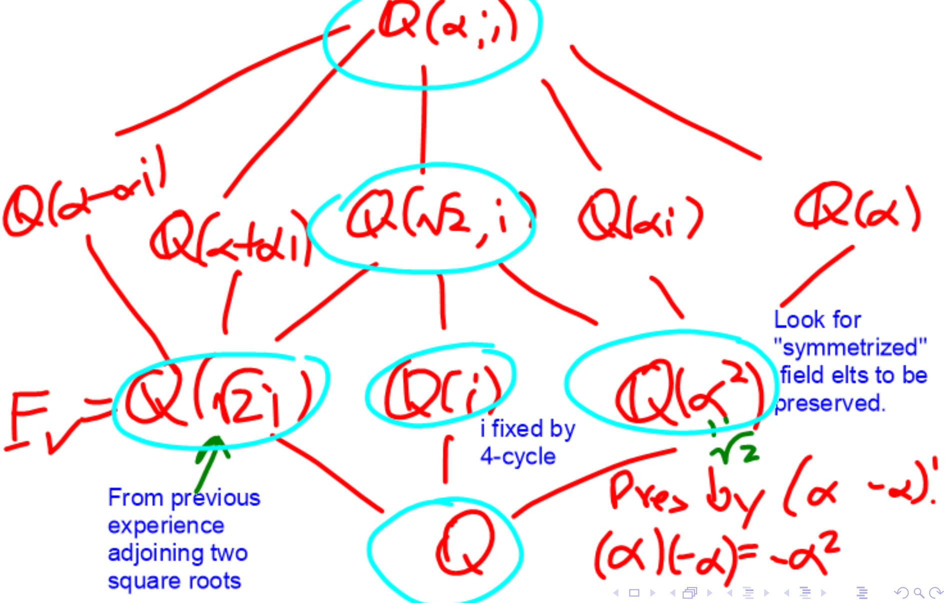
# Example: Splitting field of $x^4 - 2$

Subgroups of $D_4$:



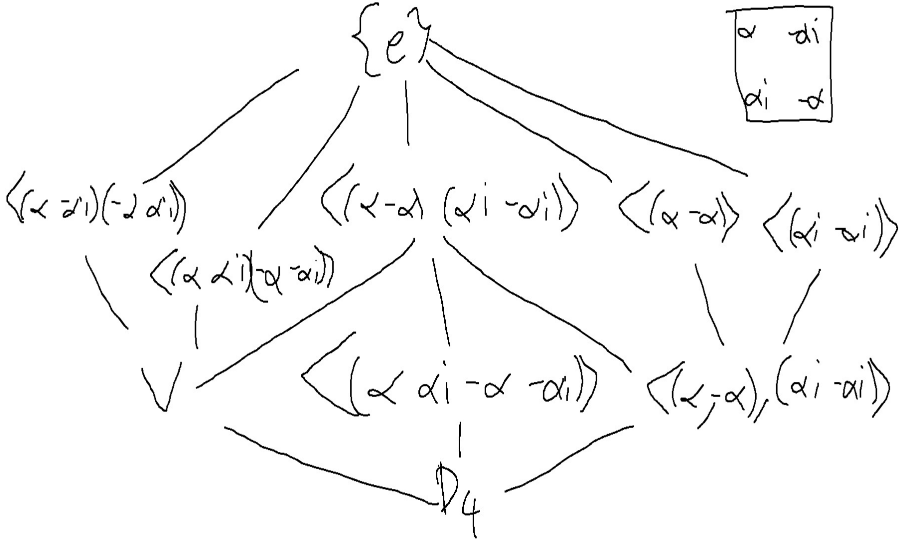
# Example: Splitting field of $x^4 - 2$

Subfields of $\mathbf{Q}(\alpha, i)$:



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

The two lattices, superimposed:



# 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 $F(a_1, \dots, a_n)$ 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

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

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: $A_5$ is non-solvable because:

Example: $S_5$ is non-solvable because:

# Extensions by roots are solvable

Long story short:

**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.*

# 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 $n$th 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".