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.
- Final reading for the course: 16.11 and 16.12.
- Take-home exam 3 due Wed. (But all deadlines are elastic.)
- Today's DJ: Meng-Ru.

Please submit exam on Gradescope!

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 $G(K/F)$. Computational
- Big finale: 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**. "Insolvability of the quintic" -- the only way to describe alpha_i is "the roots of f"

(Blue stuff is done; purple is today.)

Kummer extensions

So we can use linear algebra over C!

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 $\beta^p \in F$.

ζ in F assumed

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

polynomial

So elements of K are expressible in terms of radicals in elements of F (they are "solvable by radicals").

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).

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

For $\gamma, \delta \in K$, $c \in F$:

F-linear

$\sigma(\gamma+\delta)$ because sigma is a ring homom. $= \sigma(\gamma)+\sigma(\delta)$

$\sigma(c\gamma) = \sigma(c)\sigma(\gamma)$

b/c sigma is ring homom

sigma fixes F

$= c\,\sigma(\gamma)$

So sigma is a linear transformation from K to itself (as an F-vector space).

Proof of Kummer Thm, cont.

Sketch: Finite order elements preserve inner product, so (conj to) hermitian matrices.

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. $\lambda^p = 1$. (i.e. $\lambda = \zeta^k$, $k \not\equiv 0 \pmod p$)

So let $\beta \in K$ be an eigenvector of σ with eigenvalue $\lambda \neq 1$, and let $b = \beta^p$.

$$\sigma(b) = \sigma(\beta^p) = \sigma(\beta)^p$$
$$= (\lambda\beta)^p = \lambda^p \beta^p = \beta^p = b$$

I.e., b in fixed field of G.

So $b \in F$. Furthermore,

$$\sigma(\beta) = \lambda\beta \neq \beta \quad \text{b/c } \lambda \neq 1.$$

So beta is not in the fixed field of G.

yay Kummer!

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

Application: Cardano's Formula

Let $\omega = e^{2\pi i/3}$ and $F = \mathbb{Q}(\omega)$. Note that $[F : \mathbb{Q}] = 2$, since $1 + \omega + \omega^2 = 0$.

Suppose $f(x) = x^3 + 3px + 2q$ irreducible over F, with roots u_1, u_2, u_3 and discriminant $D = -2^2 3^2 (q^2 + p^3)$. Let K be the splitting field of f over F.

By Galois theory of the cubic, $[K : \mathbb{Q}] = 3$ or 6, so $[K : F] = 3$ and the permutation $\sigma = (u_1\ u_2\ u_3)$ is in $G(K/F)$. Furthermore,

$$z = u_1 + \omega u_2 + \omega^2 u_3, \qquad z' = u_1 + \omega^2 u_2 + \omega u_3$$

are both eigenvectors of σ, so by the proof of Kummer, $z^3, z'^3 \in F$.

But $z + z' =$

So $3u_1$ is the sum of two cube roots of elements of F. If done carefully, this gives Cardanos' formula for the cubic.

(details omitted)

Solvability

(Slightly different approach from Artin)

(so can use Kummer)

Suppose F subfield of $\mathbb{C}$, $\alpha \in F$.

Thm: TFAE:

1. There exists a chain of subfields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$ such that $\alpha \in K$ and for $1 \leq j \leq r$, $F_j = F_{j-1}(\beta_j)$ and $\beta_j^p \in F_{j-1}$. for some prime p. (So alpha expressed in radicals.)
2. There exists a chain of subfields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_s = K$ such that $\alpha \in K$ and for $1 \leq j \leq s$, F_j is a Galois extension of F_{j-1} with $[F_j : F_{j-1}] = p$. for some prime p.
3. There exists a chain of subfields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K$ such that $\alpha \in K$ and for $1 \leq j \leq t$, $G(K/F_j)$ is a normal subgroup of $G(K/F_{j-1})$ and $G(K/F_{j-1})/G(K/F_j) = C_p$.

Artin

Kummer

G solvable

If any (and therefore all) of these conditions hold, we say that α is solvable over F.

Proof: Kummer theory gives 1 implies 2.

$$G(K/F_0) \rhd G(K/F_1) \rhd G(K/F_2) \rhd \cdots \rhd G(K/F_t)$$

$$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad\qquad \|$$

$$G = H_0 \qquad H_1 \qquad H_2 \qquad\qquad H_t = \{1\}$$

$$H_j / H_{j-1} = C_{p_j} \qquad (K/F_t = K)$$

Subnormal series where each quotient is a finite cyclic group of prime order. We call a group that has such a subnormal series a finite *solvable* group. (For infinite solvable groups, we only require quotients to be abelian.)

(In case of finite G, we can take all quotients to be prime order because if we have an abelian group of nonprime order, we can cut it into prime order pieces.)

Proof of 2 implies 3

(Given 1 implies 3, if f(x)=0 solvable by radicals, then G(K/F) satisfies condition #3.)

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_s = K$$

F_j / F_{j-1} Galois extension

Normal subgroups part of Main Theorem of Galois Theory:

F_j / F_{j-1} Galois ← base

$\Leftrightarrow G(K/F_j) \triangleleft G(K/F_{j-1})$

Furthermore, in that case (also from normal part of Main Thm):

$$G(F_j/F_{j-1}) = G(K/F_{j-1})/G(K/F_j)$$

Extension has degree p, so this group has order p, therefore C_p.

Corollary

Facts.

- A_5 is simple (only proper normal subgroup is trivial).
- The only nontrivial proper normal subgroup of S_5 is A_5.

Corollary. If K is the splitting field of $f(x)$ over F, and $G(K/F) = A_5$ or S_5, then the roots of f are not solvable over F.

Proof:

A_5 not solv b/c only $1 \triangleleft A_5$.

S_5 not solv b/c $1 \triangleleft A_5 \triangleleft S_5$

The grand finale

(4 5)

Fact. If $G \leq S_5$ and G contains a 5-cycle and a transposition, then $G = S_5$.

Corollary. Suppose $f(x)$ irreducible, degree 5 over $\mathbb{Q}$, K is the splitting field of $f(x)$ over $\mathbb{Q}$. If f has exactly 3 real roots, $G(K/\mathbb{Q}) = S_5$.

Example: $f(x) = x^5 - 16x + 2$. 3 real roots by graphing, Irreducible by Eisenstein.

Proof:

Complex conjugation induces transposition on non-real roots.
G must include a 5-cycle because 5 divides order of G and 5-cycles are only elements of order 5 in S_5.