Midterm 3: Next week Thurs. (4/18)
7:00-8:30 Loomis Lab. 144

Topics: everything through Galois theory
Practice problems + policies: see email

Tuesday problem session cancelled
Instead: problem session will be Thurs. 10am-12pm, 3rd floor of Altgeld (345 or 347)

Def: $f(x) \in F[x]$ is <u>solvable by radicals</u> if $\exists$

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s \supseteq Sp_F f$$

where $K_{i+1} = K_i(\alpha_i)$ w/ α_i a root of $x^{n_i} - a_i$

We are proving

Thm (Galois):

a) $f(x)$ is solvable by radicals $\iff$ Gal f is a solvable gp

b) $\exists$ a degree 5 poly. which is not solvable by radicals.

Last time:

Lemma 1: If G is solvable, every subgp. and quotient of G is solvable.

Lemma 2: If $F \subseteq E \subseteq K$ w/ K/F, E/F Galois, then $\mathrm{Gal}(K/E)$, $\mathrm{Gal}(E/F)$ solvable $\Rightarrow$ $\mathrm{Gal}(K/F)$ solvable

Lemma 3: Let char $F = 0$. If $a \in F$, $K = Sp_F\, x^n - a$, then $\mathrm{Gal}(K/F)$ is solvable.

Lemma 4: K/F Galois w/ $\mathrm{Gal}(K/F) = C_n$. If $\zeta_n \in F$, then $K = F(\alpha)$ for some $\alpha \in K$ with $\alpha^n \in F$.

Pf sketch: Consider the Lagrange resolvent of $\alpha \in K$:

$$\beta := L(\alpha) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \qquad \zeta := \zeta_n$$

σ: gen.

Since $\sigma(\zeta) = \zeta$,

$$\sigma(\beta) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\alpha = \zeta^{-1}\beta$$

So $\sigma(\beta^n) = \beta^n$ i.e. $\beta^n \in F$.

Conversely, if $\beta \neq 0$, then $F(\beta) = K$ since $\sigma^i(\beta) = \zeta^{-i}\beta \neq \beta$ for all $1 \le i < n$, so $\mathrm{Aut}(K/F(\beta)) = \mathrm{id}$.

By D&F Thm 14.7, elts. of $\mathrm{Gal}(K/F)$ are linearly independent, so $\exists\, \alpha$ s.t. $L(\alpha) \neq 0$.

$\square$

Pf of Galois' Thm part a:

If $f \in F[x]$ is solvable by radicals, then

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s \supseteq K = Sp_F f$$

w/ $K_{i+1} = K_i(\alpha_i)$, with α_i a root of $x^{n_i} - a_i$, $a_i \in K_i$

Let

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L$$

where $L_{i+1} = Sp_{L_i}(x^{n_i} - a_i)$. Then $K_i \subseteq L_i$ $\forall i$, so $Sp_F f \subseteq K_s \subseteq L_s$. By Lemma 3, $\mathrm{Gal}(L_{i+1}/L_i)$ is solvable, so by Lemma 2, $\mathrm{Gal}(L/F)$ is solvable. Since K/F is Galois, by the Fun. Thm. prop. 4, $\mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$, So by Lemma 1, it is solvable

Conversely, if $G = Gal(K/F)$ is solvable

$$1 = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

cyclic quotients

Let $K_i = \text{Fix}\, G_i$, and

$$K = K_s \supseteq K_{s-1} \supseteq \cdots \supseteq K_0 = F$$

K_{i+1}/K_i is Galois by Fun. Thm. prop 4 w/

$$Gal(K_{i+1}/K_i) \cong Gal(K/K_i)/Gal(K/K_{i+1})$$
$$= G_i/G_{i+1} \cong C_{n_i} \text{ for some } i.$$

Let $F' = F(\zeta_{n_1}, \ldots, \zeta_{n_s})$, and set $K_i' = K_i F'$

We have

$$F \subseteq F' = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_s' \supseteq K$$

adjoin roots of 1

By Lemma 4, $K_{i+1}' = K_i'(\alpha)$, α a root of $x^{n_i} - a_i$, $a_i \in K_i'$, so f is solvable by radicals.

$\square$

Part b: Show that $\exists$ some poly. that is not solvable by radicals.

Fact: Let $\sigma, \tau \in S_5$, σ a 5-cycle, τ a 2-cycle. Then $\langle \sigma, \tau \rangle = S_5$.

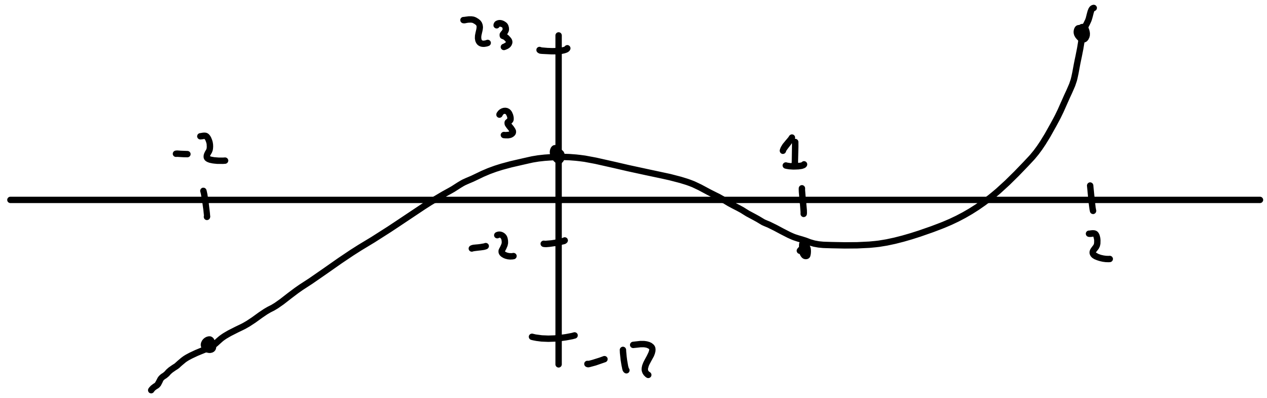
Pf: case check $\square$

Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. $K = Sp_{\mathbb{Q}} f$, $G = Gal(K/\mathbb{Q})$

Irred by Eis. @ $p=3$.

So $G \leq S_5$, G is transitive of order a mult. of 5.

The only order 5 elts. of S_5 are 5-cycles, so G contains a 5-cycle.



≥ 3 real roots by int. value thm. Can't have more since $f'(x) = 5x^4 - 6$ has only two real roots.

By the Fun. Thm. of Alg., $f(x)$ has 5 roots in $\mathbb{C}$, so two nonreal roots α and β.

Let $\tau \in \mathrm{Aut}(K/F)$ be complex conjugation. This fixes the real roots, so we must have $\overline{\alpha} = \beta$, and as an elt. of S_5, τ is a transposition.

Therefore, by part a of Galois' Theorem, it is impossible to express the roots of $f(x)$ by radicals! $\square$