

## Announcements

Midterm 3: Wed 4/23, 7:00-8:30pm, Sidney Lu 1043

Practice problems, topics: to come

Homework grading should be figured out

May take a little while to get through the back-log

---

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

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_s \supseteq \text{Sp}_F f$$

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

We are proving: Thm (Galois):

a)  $f(x)$  is solvable by radicals  $\iff \text{Gal } f$  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  $\text{Gal}(K/E), \text{Gal}(E/F)$  solvable  $\implies \text{Gal}(K/F)$  solvable

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

\* Missed this part last time. Kind of a converse of part b. If

$1 = G_s \triangleleft G_{s-1} \triangleleft \dots \triangleleft G_0 = G$  has cyclic quotients,

then so does

$$1 = G_s / (G_s \cap H) \triangleleft G_{s-1} / (G_{s-1} \cap H) \triangleleft G_0 / (G_0 \cap H) = G/H$$

$\downarrow$   
 $G_{s-1}H/H$

---

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

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

$$\beta := L(\alpha) := \alpha + \gamma \sigma(\alpha) + \gamma^2 \sigma^2(\alpha) + \dots + \gamma^{n-1} \sigma^{n-1}(\alpha) \quad \begin{array}{l} \gamma := \gamma_n \\ \sigma: \text{gen.} \end{array}$$

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

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

So  $\sigma(\beta^n) = \beta^n$  i.e.  $\beta^n \in F$ , and  $F(\beta) \subseteq K$ .

Conversely, if  $\beta \neq 0$ , then  $F(\beta) = K$  since

$\sigma^i(\beta) = \beta^{-i} \beta \neq \beta$  for all  $1 \leq i < n$ , so

$$\text{Aut}(K/F(\beta)) = \text{id}.$$

Therefore, we just need  $\alpha \in K$  with  $L(\alpha) \neq 0$ . This follows from D&F Thm 14.7: elts. of  $\text{Gal}(K/F)$  are linearly independent functions, so the function  $\alpha \mapsto L(\alpha)$  cannot be the zero function  $\square$

Pf of Galois' Thm part a:

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

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_s \supseteq K = \text{Sp}_F f$$

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

Let

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

where  $L_{i+1} = \text{Sp}_{L_i}(x^{n_i} - a_i)$ . Then  $K_i \subseteq L_i \forall i$ , so

$\text{Sp}_F f \subseteq K_s \subseteq L_s$ . By Lemma 3,  $\text{Gal}(L_{i+1}/L_i)$  is solvable, so by Lemma 2,  $\text{Gal}(L/F)$  is solvable. Since  $K/F$  is Galois, by the Fun. Thm. prop. 4,  $\text{Gal}(K/F)$  is a quotient of  $\text{Gal}(L/F)$ ,

So by Lemma 1, it is solvable

Conversely, if  $G = \text{Gal}(K/F)$  is solvable

$$1 = G_s \triangleleft G_{s-1} \triangleleft \dots \triangleleft G_0 = G$$

$\nwarrow \nearrow \searrow$   
cyclic quotients

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

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

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

$$\text{Gal}(K_{i+1}/K_i) \cong \text{Gal}(K/K_i) / \text{Gal}(K/K_{i+1})$$

$$= G_i / G_{i+1} \cong C_{n_i} \text{ for some } i.$$

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

We have

$$F \subseteq F' = K'_0 \subseteq K'_1 \subseteq \dots \subseteq K'_s \supseteq K$$

$\nwarrow$   
adjoin roots  
of 1

By Lemma 4,  $K_{i+1}' = K_i'(\alpha)$ ,  $\alpha$  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  $\sigma, \tau \in S_5$ ,  $\sigma$  a 5-cycle,  $\tau$  a 2-cycle.  
Then  $\langle \sigma, \tau \rangle = S_5$ .

Pf: Case check  $\square$

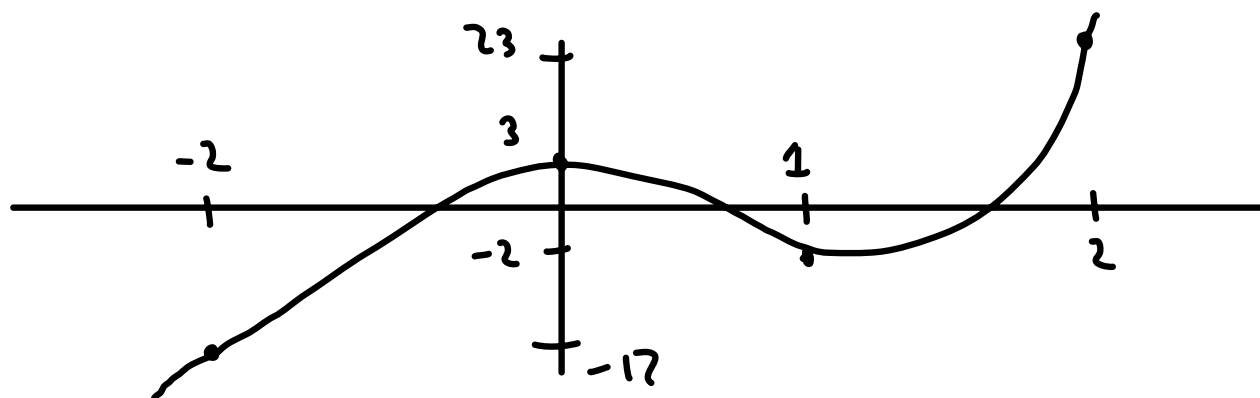
Let  $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ .  $K = S_{\mathbb{P}_{\mathbb{Q}} f}$ ,  $G = \text{Gal}(K/\mathbb{Q})$

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.



$\geq 3$  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  $\alpha$  and  $\beta$ .

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

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