# May 28: Galois's Criterion

Plan

Today & Wednesday: Galois's criterion

Friday: Discussion

No reflection

HW10:

## Galois's criterion:

Let $K$ char 0 field

Let $f \in K[x]$

Let $L$ be the splitting field

$f$ solvable by radicals $\iff$ $\mathrm{Gal}(L/K)$ solvable.

---

Recall that a group $G$ is solvable if

$\exists\ 0 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \cdots \trianglelefteq G_s = G$

s.t. $G_i/G_{i-1}$ abelian.

---

<u>Fact 1</u>: $S_n$ not solvable $n \geq 5$

<u>Fact 2</u> $\exists f \in \mathbb{Q}[x]$ of degree 5 s.t. $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$ where $L$ splitting field of $\mathbb{Q}$

<u>Cor</u> **Not all quintics are solvable!**

For any finite group $G$, can embed $G < S_n$ for some $n$

Use fact: $\exists\ \mathbb{Q} \subset L$ with $\mathrm{Gal}(L/\mathbb{Q}) = S_n$

$$G < S_n \longmapsto \mathbb{Q} < \underbrace{L^G < L}_{\text{Galois gp} = G}$$

Don't know normal

More generally, $\exists f$ of degree $n$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$

<u>Ques</u>:

(1) What is Galois group for a random $f$? Guess: $S_n$

(2) For any $G$ finite group, does $\exists f \in \mathbb{Q}[x]$ s.t. $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ Open!

## Galois's criterion:

Let $K$ char $0$ field

Let $f \in K[x]$

Let $L$ be the splitting field

$f$ solvable by radicals $\iff$ $\mathrm{Gal}(L/K)$ solvable.

---

We will prove $\Longrightarrow$.

(This direction gives us the cor that $\exists f \in \mathbb{Q}[x]$ not solvable)

Other direction $\Longleftarrow$ : Option for HW10

---

**Attempt:** (Where does this go wrong?)

Let $f \in K[x]$ be solvable by radicals. This means that

$$\exists\, K \subset L \subset E$$

$L$: splitting field of $f$

$E$: radical ext of $K$

Recall that $K \subset E$ is radical if $\exists\, K = E_0 \subset E_1 \subset \cdots \subset E_s = E$ s.t. $E_i = E_{i-1}(\alpha_i)$ where $a_i = \alpha_i^{n_i} \in E_{i-1}$ $\sim$ $\alpha_i = \sqrt[n_i]{a_i}$

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[5]{7})$ radical

Is $\mathrm{Gal}(E/K)$ solvable?

$$\cdots \subset \mathrm{Gal}(E/E_2) \subset \mathrm{Gal}(E/E_1) \subset \mathrm{Gal}(E/K)$$

Fund thm $\Longrightarrow$ (Not quite right!) because $E_i \subset E_{i+1}$ not nec. normal

$$\mathrm{Gal}(E/E_i)/\mathrm{Gal}(E/E_{i+1}) \cong \mathrm{Gal}(E_{i+1}/E_i)$$

~~abelian~~ solvable

$E_{i+1} = E_i(\sqrt[n_i]{a_i})$

$\Longrightarrow$ $\mathrm{Gal}(E/K)$ solvable!

But $\mathrm{Gal}(L/K) = \mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)$ $\Longrightarrow$ also solvable

Example

$K \subset K(\underbrace{\sqrt[n]{a}}_{\alpha})$ for $a \in K$

not nec. normal

$K \subset K(\sqrt[n]{a}) \Leftarrow K$ contains a prim. $n^{th}$ root of unity $\zeta$

Reason: If $\alpha$ is a root of $x^n - a \in K[x]$, then the other roots are

$$\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha$$

---

To fix the proof, we add in $n^{th}$ roots of unity.

**Lemma 1** $K$ char 0 field

Let $\rho$ be a prim. $n^{th}$ root of unity in some field ext.

Then $K \subset K(\rho)$ Galois and $Gal(K(\rho)/K)$ is abelian.

Could be case that $\rho \in K$. In which case $Gal(K(\rho)/K) = \{1\}$

PF: For $\sigma \in Gal(K(\rho)/K)$, we know $\sigma(\rho)$ determines $\sigma$

and $\sigma(\rho) = \rho^i$ for some $i$

Given $\tau \in Gal(K(\rho)/K)$, then $\tau(\rho) = \rho^j$ for some $j$

$$(\tau \circ \sigma)(\rho) = \rho^{i \cdot j} = (\sigma \circ \tau)(\rho)$$

$$\Longrightarrow \tau \circ \sigma = \sigma \circ \tau$$

**Lemma 2** $K$ char 0 field

- Assume $K$ has a prim $n^{th}$ root of unity $\rho \in K$.
- Suppose $\alpha$ is a root of $x^n - a \in K[x]$

Then $K \subset K(\alpha)$ Galois & $Gal(K(\alpha)/K)$ abelian.

PF: If $\alpha$ is a root, then so are $\alpha, \rho\alpha, \rho^2\alpha, \ldots, \rho^{n-1}\alpha$

$\Rightarrow K \subset K(\alpha)$ Galois

Any $\sigma \in Gal(K(\alpha)/K)$ is determined by $\sigma(\alpha) = \rho^i \alpha$ for some $i$.

Any $\tau$, $\tau(\alpha) = \rho^j \alpha$

$$(\tau \circ \sigma)(\alpha) = (\sigma \circ \tau)(\alpha)$$

$$\Longrightarrow \tau \circ \sigma = \sigma \circ \tau$$

$K \subset L$

splitting field of $x^n - a \in K[x]$

Let $\zeta$ prim $n^{th}$ root

$K \subset K(\zeta) \subset L = K(\alpha)$

normal w/ abelian Galois

$\Rightarrow$ Gal$(L/K)$ solvable

Ex: $x^p - 2 \in \mathbb{Q}[x]$