Math 100C — Lecture 24 — 6/2/2017

Last Time p-prime $\zeta = e^{2\pi i/p}$.

* If $F \subseteq \mathbb{C}$ is <u>any</u> subfield, then $F(\zeta)/F$ is cyc. <u>Galois</u> & $G(F(\zeta)/F)$ is <u>cyclic</u>.

---

§ 16.11 Kümmer Extensions

<u>Thm</u> Let $n \geq 1$ and let $F \subseteq \mathbb{C}$ be a subfield containing $\zeta = e^{2\pi i/n}$. Suppose $\alpha \in \mathbb{C}$ is s.t. $\alpha^n = a \in F$. Then $F(\alpha)/F$ is <u>Galois</u> and $G(F(\alpha)/F)$ is <u>cyclic</u>.

<u>Pf</u> <u>Ex</u> $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ not Galois $\qquad$ $\mathbb{Q}(2^{1/3}, e^{2\pi i/3})/\mathbb{Q}(e^{2\pi i/3})$ Galois, Galois gp $\approx C_3$.

<u>Pf</u> $F(\alpha)$ is the splitting field for $x^n - a \in F[x]$ (b/c $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha \in F(\alpha)$) so $F(\alpha)/F$ is Galois.

Given $\sigma \in G(F(\alpha)/F)$, σ is <u>determined</u> by $\sigma(\alpha) \in \{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$. If $\sigma_i(\alpha) = \zeta^i \alpha$ and

$\sigma(\alpha)$ is a root of $x^n - a$

$\sigma_j(\alpha) = \zeta^j \alpha$ then $\sigma_i\sigma_j(\alpha) = \sigma_i(\zeta^j \alpha) \overset{\sigma_i \text{ fixes } F}{=} \zeta^j \sigma_i(\alpha) = \zeta^j \zeta^i \alpha = \zeta^{i+j}\alpha$.

Thus we have an <u>embedding</u> $G(F(\alpha)/F) \subseteq \mathbb{Z}/n\mathbb{Z}$

$$\sigma \longmapsto i$$

$\sigma(\alpha) = \zeta^i \alpha$.

So $G(F(\alpha)/F)$ is cyclic. //

Solvable Groups

Def A finite gp G is <u>solvable</u> if $\exists$ a sequence of subgps

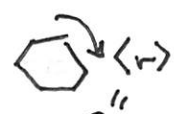
$$1 = G_0 < G_1 < \cdots < G_r = G$$

st
- $G_i \triangleleft G_{i+1}$ for all i,
- G_{i+1}/G_i is abelian for all i.

Ex ① G abelian $\Rightarrow$ G solvable.

② S_4 is <u>solvable</u>. $\{1, (12)(34), (13)(24), (14)(23)\}$

$$\underbrace{1 < V}_{\cong C_2 \times C_2} \underbrace{< A_4}_{\cong C_3} \underbrace{< S_4}_{\cong C_2}$$

③ D_n is <u>solvable</u>. 

$$\underbrace{1 < C_n}_{\cong C_n} \underbrace{< D_n}_{\cong C_2}$$

④ A_n is <u>not</u> solvable for $n \geq 5$. (non-ab., simple)

⑤ S_n ——— " ——— . (A_n <u>only</u> normal subgroup.)

Fact ~~Thm~~ Suppose $F \subseteq \mathbb{C}$ is a field & $f(x) = (x^{p_1} - a_1) \cdots (x^{p_n} - a_n)$ for some primes $p_1, \ldots, p_n$ & $a_1, \ldots, a_n \in F$. Let K/F be the spl. field of f/F. Then $G(K/F)$ is <u>solvable</u>.

<u>Pf</u> We have a chain:

$$F \subseteq F(\zeta_{p_1}) \subseteq F(\zeta_{p_1}, \zeta_{p_2}) \subseteq \cdots \subseteq F(\zeta_{p_1}, \ldots, \zeta_{p_n})$$
$$\subseteq F(\zeta_{p_1}, \ldots, \zeta_{p_n}, \alpha_1) \subseteq \cdots \subseteq \underbrace{F(\zeta_{p_1}, \ldots, \zeta_{p_n}, \alpha_1, \ldots, \alpha_n)}_{= K}$$

where $\zeta_{p_j} = e^{2\pi i / p_j}$ & $\alpha_i^{p_i} = a_i$. By Cyclotomic + Kümmer theory, this gives a chain:

$$G(K/F) \triangleright G(K/F(\zeta_{p_1})) \triangleright \cdots \triangleright G(K/F(\zeta_{p_1}, \ldots, \zeta_{p_n})) \triangleright \cdots \triangleright G(K/K) = 1$$

with cyclic factors. ▨

§ 16.12 <u>Insolubility of Quintic</u>

<u>Cardano Formula</u>

$$f(x) = x^3 + px + q \Rightarrow x \text{ "="} \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

<u>Def</u> Let $F \subseteq \mathbb{C}$ be a field. An <u>extension of F by radicals</u> is a chain of the form

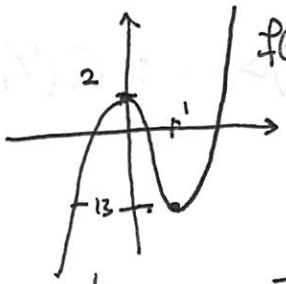
$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$$

where $F_{i+1} = F_i(\alpha_i)$ for some $\alpha_i \in \mathbb{C}$ with $\alpha_i^{n_i} \in F_i$ for some $n_i > 0$. $f(x) \in \mathbb{Q}[x]$ is <u>solvable by radicals</u> if $\exists$ an ext. K of $\mathbb{Q}$ by radicals st $f(x)$ splits in $K[x]$.

Theorem Suppose $f(x) \in \mathbb{Q}[x]$ is solvable by radicals. Let K be the splitting field of $f(x)/\mathbb{Q}$. Then $G(K/\mathbb{Q})$ is a solvable group.

Rmk Converse also true.

~~Cor~~ **Ex** Let $f(x) = x^5 - 16x + 2 \in \mathbb{Q}[x]$. We claim $f(x)$ is <u>not</u> solvable by radicals. By calculus, $f(x)$ has exactly 3 real roots. By



Eisenstein @ 2, $f(x)$ is irred. So if K is the spl. field of $f(x)/\mathbb{Q}$, then $5 \mid [K:\mathbb{Q}]$. $G(K/\mathbb{Q})$ embeds as a subgp of S_5 (it permutes the 5 roots of $f(x)$.) Since $5 \mid |G(K/\mathbb{Q})|$, $G(K/\mathbb{Q})$ contains a 5-cycle. Also, since f has 2 non-real roots, complex conjugation yields a 2-cycle in $G(K/\mathbb{Q})$. But any subgp of S_5 containing a 2-cycle & a 5-cycle is S_5 itself! So $G(K/\mathbb{Q}) \cong S_5$, which is not a solvable group. //

Ex $f(x) = x^5 - 2 \in \mathbb{Q}[x]$ is solvable by radicals

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_5, 2^{1/5}).$$

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_5, 2^{1/5})/\mathbb{Q}\right) \cong C_5 \rtimes \underset{\langle \sigma \rangle}{C_4}$$, which is solvable.

semidir. product