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

* If \( F \leq \mathbb{C} \) is any subfield, then \( F(\zeta)/F \) is cyclic Galois & \( G(F(\zeta)/F) \) is cyclic.

§ 16.11 Kümmer Extensions

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

\[
\text{Pf: } F(\alpha) = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\alpha^2, e^{2\pi i/n}) / \mathbb{Q}(e^{2\pi i/n})
\]

not Galois, not Galois, Galois, Galois, Galois, \( q \neq p, q \neq n \).

\[
\text{Pf: } F(\alpha) \text{ is the splitting field for } x^n - \alpha \in F[x] \text{ (\( \zeta, \alpha, \zeta \alpha, -\), \( \zeta \alpha \in F(\alpha) \)) so } F(\alpha)/F \text{ is Galois.}
\]

Given \( \sigma \in G(F(\alpha)/F) \), \( \sigma \) is determined by

\[
\sigma(\alpha) \in \{ \alpha, \zeta \alpha, \ldots, \zeta^{n-1} \alpha \}.
\]

If \( \sigma_i(\alpha) = \zeta^i \alpha \) and \( \sigma_i \) fixes \( F \)

\( \sigma(\alpha) = \zeta^j \alpha \) then \( \sigma_i \sigma_j(\alpha) = \sigma_i(\zeta^j \alpha) = \zeta^i \zeta^j \alpha = \zeta^{i+j} \alpha \).

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

\[
\sigma \mapsto i
\]

So \( G(F(\alpha)/F) \) is cyclic.
Solvable Groups

Def: A finite gp $G$ is solvable if $\exists$ a sequence of subgps

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

s.t. $G_i \triangleleft G_{i+1}$ for all $i$,

$G_{i+1}/G_i$ is abelian for all $i$.

Ex - ① $G$ abelian $\Rightarrow G$ solvable.

② $S_4$ is solvable.

$$1 < V < A_4 < S_4$$

$$\cong C_2 \times C_2 \cong C_3 \cong C_2$$

③ $D_n$ is solvable.

$$1 < C_n^r < D_n$$

$$\cong C_n \cong C_2$$

④ $A_n$ is not solvable for $n \geq 5$. (non-abelian, simple)

⑤ $S_n$ (An only normal subgroup.)

Fact: Suppose $F$ 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 solvable.
We have a chain:

\[ F \subseteq F(\xi_1) \subseteq F(\xi_1, \xi_2) \subseteq \cdots \subseteq F(\xi_1, \cdots, \xi_n) \]

where \( \xi_i = e^{2\pi i/p_i} \) and \( \alpha_i = \alpha_i \). By Cyclotomic + Kummer theory, this gives a chain:

\[ G(K_F) \supset G(K_{F(\xi_1)}) \supset \cdots \supset G(K_{F(\xi_1, \cdots, \xi_n)}) \supset \cdots \supset G(K_F) = 1 \]

with cyclic factors.

\[ \S 16.12 \text{ Insolubility of Quintic} \]

Cardano Formula

\[ f(x) = x^3 + px + q \Rightarrow z = \left( \frac{-9}{2} + \sqrt{\frac{9}{4} + \frac{p^3}{27}} \right) \]

Def Let \( F \subseteq C \) be a field. An extension of \( F \) by radicals 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 \( \alpha_i \in \sigma \) with \( \alpha_i^{n_i} \in F_i \) for some \( n_i > 0 \). \( f(x) \in \mathbb{Q}[x] \) is solvable by radicals if \( F \) 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.

Proof: Converse also true.

Let \( f(x) = x^5 - 16x + 2 \in \mathbb{Q}[x] \). We claim \( f(x) \) is not solvable by radicals. By calculus, \( f(x) \) has exactly 3 real roots. By Eisenstein @ 2, \( f(x) \) is irreducible. So if \( K \) is the splitting field of \( f(x) / \mathbb{Q} \), then \( 5 \mid [K: \mathbb{Q}] \). \( G(K/\mathbb{Q}) \) embeds as a subgroup 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 subgroup 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.

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

\( \text{Gal}(\mathbb{Q}(\zeta_5, 2^{1/5})/\mathbb{Q}) \cong C_5 \times C_4 \), which is solvable.