Lecture 40: Solving equations by radicals

§14.7 of [DF].

Last time: $f \in F[x]$ separable with roots $\alpha_i \in K$, a split. field.

Discriminant: $D = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F$

[Can be computed from the coeffs of $f(x)$.]

Thm: $\sqrt{D} \in F \iff \mathrm{Gal}(K/F) \leq A_n$, with $n = \deg(f)$.

- $x^2 + bx + c$ has solutions $\dfrac{-b \pm \sqrt{D}}{2}$.
- $x^3 + px + q$ so $D = -4p^3 - 27q^2$. Set

$$A = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \quad B = \sqrt[3]{\square - \square}$$

[So $(AB)^3 = -(3p)^2$]. The roots are

$$\alpha = \frac{A+B}{3} \quad \beta = \frac{\zeta_3^2 A + \zeta_3 B}{3} \quad \gamma = \frac{\zeta_3 A + \zeta_3^2 B}{3}$$

- For degree 4, there is an even worse formula.

Thm: There is no such formula for polys of degree ≥ 5, i.e. expressions of the roots in terms of the coefficients and the opperations: $+, -, \times, \div, \sqrt[k]{\cdot}$.

Def: $f(x) \in F[x]$ is *solvable by radicals* when there exist $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s$ where each $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - q_i \in K_i[x]$ and f splits completely in K_s.

Recall: A finite group is *solvable* where there exist

$$\{1\} = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$$

where each G_i/G_{i+1} is abelian.

Moreover, can choose G_i so that G_i/G_{i+1} is cyclic of prime order.

Thm: $f(x) \in F[x]$ is solvable by radicals $\iff$ $\mathrm{Gal}(K/F)$ is solvable, where K is a split field for f.

Cor: When $\mathrm{Gal}(K/F) = S_n$ for $n = \deg(f)$ and $n \geq 5$ then f is *not* solvable by radicals.

Pf: S_n is solvable $\iff$ $n \leq 4$. ▨

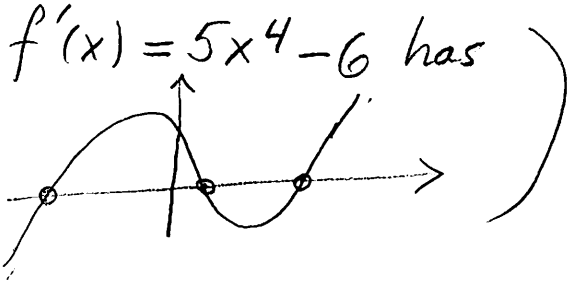
Thus there is no "quintic formula" as e.g.

$f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ has $G = \mathrm{Gal}(K/F) = S_5$
(K: split field.)

Reason: [Skip!] f is irred by Eisenstein with $p=3$.

As f is irreducible, $5 \mid [K:\mathbb{Q}] = |G|$. So G has an elt of order 5, which must be a 5-cycle.

Now f has 3 real roots $\alpha_1, \alpha_2, \alpha_3$ and 2 roots α_4, α_5 in $\mathbb{C} \setminus \mathbb{R}$ (Note that $f'(x) = 5x^4 - 6$ has only two real roots, and so:



Thus $\tau =$ restriction of $z \mapsto \bar{z}$ in G to K corresponds to (45). As G contains a 5 cycle and a transposition, it is S_5.

Examples where $\mathrm{Gal}(K/F)$ is solvable:

① $F(\sqrt{D})/F$

② Cyclotomic fields: $K = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ } degree $\phi(n)$

Pf: K is the splitting field of $x^n - 1$, hence Galois.

Consider

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

$$a \longmapsto (\sigma_a : \zeta_n \to \zeta_n^a)$$

This is a homomorphism as $\sigma_{ab}(\zeta_n) = \zeta_n^{ab}$

$= (S_n^{\,b})^a = \sigma_a(\sigma_b(S_n))$. This is injective and hence surjective as $|\mathrm{Gal}(K/\mathbb{Q})| = [K:\mathbb{Q}] = \phi(n)$ and so the groups have the same # of elts.

Note: $\mathrm{Gal}(\mathbb{Q}(S_n)/\mathbb{Q})$ is abelian but may not be cyclic, e.g. $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$.

Assumption: From now on, char $F = 0$.
[Not needed but makes proof simpler.]

Lemma: Suppose $F \subseteq L \subseteq K$ with K/F and L/F Galois. If $\mathrm{Gal}(K/L)$ and $\mathrm{Gal}(L/F)$ are solvable, then so is $\mathrm{Gal}(K/F)$.

Pf: As L/F is Galois, $\mathrm{Gal}(K/L) \trianglelefteq \mathrm{Gal}(K/F)$ with quotient $\mathrm{Gal}(L/F)$. So have $H \trianglelefteq G$ with H and G/H solvable $\Rightarrow$ G is solvable. ∎

Lemma: If K is the splitting field of $\underbrace{x^n - a}_{f(x)} \in F[x]$ then $\mathrm{Gal}(K/F)$ is solvable.

Pf: As $f'(x) = nx^{n-1}$ is coprime to f, have that f is separable. Let $\alpha_1, \ldots, \alpha_n \in K$ be the distinct roots.

Each $\alpha_i^n = a$, so $\left\{\frac{\alpha_i}{\alpha_1}\right\}$ are all n dist. roots of $X^n - 1$. So K contains a copy of $\mathbb{Q}(\zeta_n)$. and relabel so $\alpha_k = \zeta_n^k \alpha$ where $\alpha = \alpha_1$.

$$\begin{array}{c} K = F(\alpha, \zeta_n) \\ | \\ L = F(\zeta_n) \\ | \\ F \end{array}$$

Claim 1: $Gal(L/F)$ is abelian.

Claim 2: $Gal(K/L)$ is cyclic of order dividing n.

[These combine with the previous lemma to prove the current one.]

Pf of ①: Any two $\sigma, \tau \in Gal(L/F)$ have the form $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$. Then $\sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = \zeta_n^{ab} = \tau(\sigma(\zeta_n))$ and so σ and τ commute.

Pf of ②: Define $\rho : Gal(K/L) \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$(\alpha \mapsto \zeta_n^a \alpha) \longrightarrow a$$

This is clearly injective and is a homomorphism since $\forall \sigma, \tau \in Gal(K/L)$ we have $\sigma(\tau(\alpha)) = \sigma(\zeta_n^{\rho(\tau)}\alpha) = \zeta_n^{\rho(\tau)}\sigma(\alpha) = \zeta_n^{\rho(\tau)+\rho(\sigma)}\alpha$

$= \zeta_n^{\rho(\tau)+\rho(\sigma)}\alpha$ as $\sigma|_L = id_L$. ▨