Lecture 18: Solvability of Equations

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Part I: Solvability by Radicals

From the Quadratic Formula to the Quintic Question

Every root below is built from the coefficients by $+, -, \times, \div$ and extraction of roots.

- **Degree 2.** Over a field of characteristic $\neq 2$, the zeros of $ax^2 + bx + c$ ($a \neq 0$) are $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ — one square root.
- **Degrees 3 and 4.** Cardano's formula (1545) solves the cubic and Ferrari's method the quartic, by field operations and cube/square roots.
- **Degree 5.** After years of searching for a "quintic formula", Abel (1824–1826) proved that a quintic *need not* be solvable by radicals — there is no general formula.

Cardano's Formula (1545)

Depressed cubic. The substitution $x = y - \frac{a}{3}$ turns $x^3 + ax^2 + bx + c$ into $y^3 + py + q = 0$.

Cardano's trick. Write $y = u + v$. Then $(u+v)^3 + p(u+v) + q = u^3 + v^3 + q + (3uv + p)(u+v)$, so imposing $uv = -\frac{p}{3}$ gives $u^3 + v^3 = -q$ and $u^3v^3 = -\frac{p^3}{27}$; hence u^3, v^3 are the roots of $t^2 + qt - \frac{p^3}{27} = 0$.

The formula. With $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$,

$$y = \sqrt[3]{-\tfrac{q}{2} + \sqrt{\Delta}} \; + \; \sqrt[3]{-\tfrac{q}{2} - \sqrt{\Delta}} \qquad \text{(cube roots paired so the product is } -p/3\text{);}$$

the other two roots come from multiplying the pair by (ω, ω^2) and (ω^2, ω).

Casus irreducibilis. When $\Delta < 0$ the cubic has three real roots but the formula passes through $\mathbb{C}$ — the real radical tower over $\mathbb{Q}$ does not reach them.

Extensions by Radicals; Solvable by Radicals

Definition (Extension by Radicals).

K/F is an *extension by radicals* if there are $\alpha_1, \ldots, \alpha_r \in K$ and integers $n_1, \ldots, n_r \geq 1$ with

$$K = F(\alpha_1, \ldots, \alpha_r), \quad \alpha_1^{n_1} \in F, \quad \alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1}) \ \ (1 < i \leq r).$$

Equivalently: a tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$ with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$.

Definition (Solvable by Radicals).

$f \in F[x]$ is *solvable by radicals over F* if its splitting field E is contained in some extension of F by radicals — equivalently, every root of f is reached from the coefficients by finitely many $+, -, \times, \div$ and n_ith roots.

Examples: Some Quintics Are Solvable by Radicals

Insolvability does not mean that *no* quintic is solvable, as these examples show.

- $x^5 - 1$ is solvable by radicals over $\mathbb{Q}$: writing $\zeta_5 = e^{2\pi i/5}$ for a primitive 5th root of unity, its splitting field is $\mathbb{Q}(\zeta_5)$ with $\zeta_5^5 = 1 \in \mathbb{Q}$ — a one-step radical extension.
- $x^5 - 2$ is solvable by radicals over $\mathbb{Q}$: its splitting field is $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, where $(\sqrt[5]{2})^5 = 2 \in \mathbb{Q}$ and $\zeta_5^5 = 1$ — a two-step radical tower.

So the claim "the quintic is insolvable" means: **there exists** a degree-5 polynomial that is not solvable by radicals. We will exhibit one explicitly.

Galois's Criterion

Recall. A finite group G is *solvable* if it has a subnormal series $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$ with every quotient G_i/G_{i-1} abelian.

Theorem (Galois).

Let F have characteristic 0 and let $f \in F[x]$ have splitting field E. Then

$$f \text{ is solvable by radicals over } F \iff \mathrm{Gal}(E/F) \text{ is a solvable group.}$$

We prove the direction that yields impossibility:

$$f \text{ solvable by radicals} \implies \mathrm{Gal}(E/F) \text{ solvable,}$$

equivalently (contrapositive) a *non-solvable* Galois group forces f *not* solvable by radicals. The converse is also true (stated without proof).

Part II: Radical Towers Have Solvable Galois Groups

The Single-Radical Lemma: $x^n - a$

Lemma (Single-Radical).

Let F have characteristic 0, let $a \in F$, and let K be the splitting field of $x^n - a$ over F. Then $\mathrm{Gal}(K/F)$ is solvable.

Cyclotomic input (L17). For any field F of characteristic 0, $\mu_n = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ is cyclic, $F(\zeta_n)/F$ is Galois, and $\sigma \mapsto a$ $(\sigma(\zeta_n) = \zeta_n^a)$ embeds $\mathrm{Gal}(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$; in particular $\mathrm{Gal}(F(\zeta_n)/F)$ is **abelian**.

Two abelian layers. Pick any root β of $x^n - a$. The lemma rides on the tower

$$F \;\subseteq\; F(\zeta_n) \;\subseteq\; F(\zeta_n, \beta) = K,$$

whose bottom step is cyclotomic (abelian by the input above) and whose top step is a single radical $\beta^n \in F(\zeta_n)$ over a field already containing μ_n (abelian — proved next slide).

Proof of the Lemma

Case 1: $\mu_n \subseteq F$**.** Fix a generator ζ of μ_n. If β is one root of $x^n - a$, all roots are $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$, so $K = F(\beta)$. Each $\sigma \in \mathrm{Gal}(K/F)$ is determined by $\sigma(\beta) = \zeta^{i_\sigma}\beta$, and since $\zeta \in F$ the map $\sigma \mapsto i_\sigma \bmod n$ is a homomorphism $\mathrm{Gal}(K/F) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$. So $\mathrm{Gal}(K/F)$ is **cyclic** (a subgroup of $\mathbb{Z}/n\mathbb{Z}$).

Case 2: general F**.** Let $F' = F(\zeta_n)$, so $F \leq F' \leq K$. F'/F is Galois with $\mathrm{Gal}(F'/F)$ abelian by the cyclotomic Galois theorem (L17). Over F' we are in Case 1, so $\mathrm{Gal}(K/F')$ is cyclic. By the FTGT, $\mathrm{Gal}(K/F') \trianglelefteq \mathrm{Gal}(K/F)$ with

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/F') \;\cong\; \mathrm{Gal}(F'/F),$$

giving the subnormal series $\{e\} \trianglelefteq \mathrm{Gal}(K/F') \trianglelefteq \mathrm{Gal}(K/F)$ with abelian quotients. Hence $\mathrm{Gal}(K/F)$ is solvable. ∎

Radical Extension $\Rightarrow$ Solvable Galois Group

Theorem.

Let F have characteristic 0, E/F normal (hence Galois), and $E \subseteq K$ with K/F an extension by radicals. Then $\mathrm{Gal}(E/F)$ is solvable.

Group-theory input.

Solvable group (recall): admits a subnormal series $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$ with every quotient G_i/G_{i-1} abelian.
Solvable-by-solvable closure. If $N \trianglelefteq G$ with both N and G/N solvable, then G is solvable.

Proof. Build a normal radical extension $L \supseteq K$ over F in stages. From $K = F(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$, set $L_0 = F$ and let L_i be the splitting field over L_{i-1} of $\prod_{\sigma \in \mathrm{Gal}(L_{i-1}/F)}(x^{n_i} - \sigma(\alpha_i^{n_i})) \in F[x]$. Then L_i/L_{i-1} is a tower of $x^n - a$ extensions, so $\mathrm{Gal}(L_i/L_{i-1})$ is solvable (Lemma); $\mathrm{Gal}(L_{i-1}/F)$ is solvable by induction; the Closure gives $\mathrm{Gal}(L_i/F)$ solvable. Take $L = L_r \supseteq K$. Since E/F is normal, FTGT presents $\mathrm{Gal}(E/F)$ as a quotient of $\mathrm{Gal}(L/F)$, hence solvable. ■

Part III: Insolvability of Degree ≥ 5

The "General" Equation of Degree n

Question. For a degree-n equation $x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ with *independent* coefficients c_i, is there a formula expressing the roots in $c_0, \ldots, c_{n-1}$ using $+, -, \times, \div$ and radicals?

Model.

Take $y_1, \ldots, y_n$ independent transcendentals (the roots) and set $f(x) := \prod_{i=1}^{n}(x - y_i)$. By Vieta, $f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$, where the *elementary symmetric polynomials* are

$$s_k := \sum_{1 \le i_1 < \cdots < i_k \le n} y_{i_1} \cdots y_{i_k} \quad (k = 1, \ldots, n).$$

Two fields. $F := \mathbb{Q}(s_1, \ldots, s_n) \subseteq E := \mathbb{Q}(y_1, \ldots, y_n)$ —the latter the splitting field of f over the former.

Bridge. A radical formula for the y_i in the s_k exists $\iff$ f solvable by radicals over F $\iff$ $\mathrm{Gal}(E/F)$ solvable.

$\mathrm{Gal}(E/F) \cong S_n$

Theorem.

For the general degree-n equation, $\mathrm{Gal}(E/F) \cong S_n$, where $F = \mathbb{Q}(s_1, \ldots, s_n)$ and $E = \mathbb{Q}(y_1, \ldots, y_n)$.

$S_n \hookrightarrow \mathrm{Gal}(E/F)$. Each $\sigma \in S_n$ permutes the y_i, inducing $\bar{\sigma} \in \mathrm{Aut}(E)$ fixing $\mathbb{Q}$. Each s_k is invariant under index permutation, so $\bar{\sigma}$ fixes every s_k, hence fixes F. Thus $|\mathrm{Gal}(E/F)| \geq n!$.

$\mathrm{Gal}(E/F) \hookrightarrow S_n$. Every Galois automorphism permutes the roots of f and is determined by that permutation (since E is generated by the y_i over F). Thus $|\mathrm{Gal}(E/F)| \leq n!$.

Combining, $\mathrm{Gal}(E/F) \cong S_n$. ■

$$\begin{tikzcd}
E = \mathbb{Q}(y_1, \ldots, y_n) \arrow[d, dash, "S_n"] \\
F = \mathbb{Q}(s_1, \ldots, s_n) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

S_n Not Solvable for $n \geq 5 \Rightarrow$ General Equation Insolvable

S_n is not solvable for $n \geq 5$. A composition series of S_n is $\{e\} \trianglelefteq A_n \trianglelefteq S_n$, with quotients A_n and $\mathbb{Z}_2$. For $n \geq 5$, A_n is **non-abelian simple** (L09), so S_n has a non-abelian composition factor — not solvable.

Theorem (Abel–Galois).

The general equation of degree $n \geq 5$, $f(x) = \prod_{i=1}^{n}(x - y_i) \in F[x]$, is not solvable by radicals over $F = \mathbb{Q}(s_1, \ldots, s_n)$.

Proof. $\mathrm{Gal}(E/F) \cong S_n$ is not solvable; the radical theorem (contrapositive) gives f not solvable by radicals. ∎

What this rules out. *Any single* formula in the coefficients using $+, -, \times, \div$ and radicals that solves every degree-n equation. *Specific* equations may still be solvable — next we exhibit one over $\mathbb{Q}$ that is not.

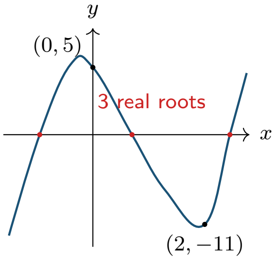
An Insolvable Quintic over $\mathbb{Q}$: $2x^5 - 5x^4 + 5$

Irreducible. $f(x) = 2x^5 - 5x^4 + 5$ is irreducible over $\mathbb{Q}$ by Eisenstein at $p = 5$: $5 \nmid 2$ (leading), $5 \mid -5, 0, 0, 0, 5$ (lower), and $5^2 = 25 \nmid 5$ (constant).

Exactly three real roots.
$f'(x) = 10x^4 - 20x^3 = 10x^3(x-2)$, so the critical points are $x = 0$ and $x = 2$, with

$$f(0) = 5 > 0 \text{ (max)}, \quad f(2) = -11 < 0 \text{ (min)}.$$

With $f \to -\infty$ as $x \to -\infty$ and $f \to +\infty$ as $x \to +\infty$, the graph crosses the axis exactly **three** times: three real roots and one conjugate pair of non-real roots.



Galois Group of $2x^5 - 5x^4 + 5$ is S_5

Let E be the splitting field of $f(x) = 2x^5 - 5x^4 + 5$ over $\mathbb{Q}$.

- **A 5-cycle.** f is irreducible of degree 5, so for a root α, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ divides $|\mathrm{Gal}(E/\mathbb{Q})|$; by Cauchy's theorem the group has an element of order 5, a 5-cycle on the five roots.
- **A transposition.** Complex conjugation restricts to an automorphism of E; it fixes the three real roots and swaps the conjugate pair, acting as a transposition.
- **Generation.** A standard fact: a subgroup of S_5 containing a 5-cycle and a transposition is all of S_5 (the transposition and the 5-cycle generate every transposition).

Hence $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$, which is not solvable, so

$$2x^5 - 5x^4 + 5 \text{ is not solvable by radicals over } \mathbb{Q}. \blacksquare$$

Part IV: Lagrange, Abel, Galois

Lagrange (1770): Resolvents

Resolvent for the cubic. For roots $\alpha_1, \alpha_2, \alpha_3$ and $\omega = e^{2\pi i/3}$, set

$$r = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3.$$

A 3-cycle of the roots sends $r \mapsto \omega^2 r$, so r^3 is fixed by A_3 and takes 2 **values** under S_3; hence r^3 satisfies a quadratic over $\mathbb{Q}(s_1, s_2, s_3)$ — this gives *Cardano's formula*. The analogous quartic resolvent takes 3 values, satisfying a cubic — *Ferrari's* resolvent cubic.

Why degree 5 stalls. For $n \geq 5$ no rational function of the roots takes a small enough number of values under S_n to reduce the problem. Lagrange identified this obstruction but could not prove impossibility.

Modern restatement. Lagrange's action $r \mapsto \omega^i r$ is precisely the Galois action on one radical step: *if $\mu_n \subseteq F$ and $\beta^n = a \in F$, then $\mathrm{Gal}(F(\beta)/F)$ is cyclic of order dividing n* — Case 1 of the Single-Radical Lemma. **Each radical step contributes a single cyclic, hence abelian, layer.**

Abel (1824–1826): Insolvability

Theorem (Abel).

The general equation of degree $n \geq 5$ is not solvable by radicals over $\mathbb{Q}(s_1, \ldots, s_n)$.

Strategy. Suppose a root lies in a radical tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r$ with $F_i = F_{i-1}(\alpha_i)$, $\alpha_i^{n_i} \in F_{i-1}$. By the Lagrange analysis applied at every step, the symmetry of the roots is built out of r stacked **abelian layers** (Single-Radical Lemma). Such an action is itself solvable as a group. But the general equation has S_n permuting its roots, and for $n \geq 5$ the group S_n has the non-abelian simple composition factor A_n, hence is *not* solvable — contradiction. In modern terms this is exactly the forward direction *radical* $\Rightarrow$ *solvable Galois group*.

Predecessor. Ruffini (1799) followed the same line, enumerating subgroups of S_5; the published proofs had gaps. Abel closed them.

Companion: abelian equations (Abel 1829). If the roots can be ordered so that each $\alpha_{i+1} = \theta_i(\alpha_1)$ for rational maps θ_i that pairwise commute, then f is solvable by radicals. This class is the origin of the term **abelian group**.

Galois (1831): The Criterion

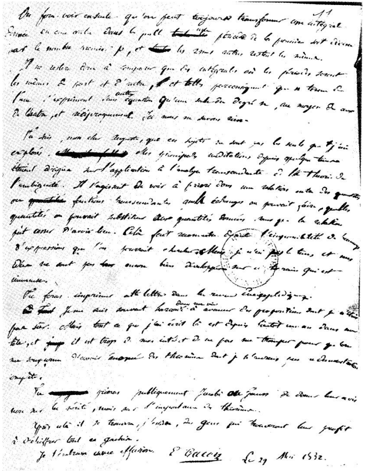
Galois recast the entire question group-theoretically, with the criterion (solvable by radicals $\iff$ Galois group solvable) stated in Part I and proved (forward direction) in Part II. To formulate it he introduced three concepts.

- **Group of an equation** — permutations of the roots compatible with every rational relation they satisfy; the modern $\mathrm{Gal}(E/F)$.
- **Normal subgroup** ($H \trianglelefteq G$ iff $gH = Hg$ for all $g \in G$) — expresses recursion: it splits the equation into one with group H and one with group G/H.
- **Solvable group** — a subnormal series with abelian quotients; one cyclic layer per radical step (Case 1 of the Single-Radical Lemma).

Subsumes the earlier results. Abelian Galois group $\Rightarrow$ solvable $\Rightarrow$ solvable by radicals (Abel's abelian equations); the general quintic has group S_5 with non-abelian simple composition factor A_5, so not solvable, hence not solvable by radicals (Abel's impossibility).

Galois (1832): The Last Letter

29 May 1832, to Auguste Chevalier — eve of the duel († 31 May, age 20). A mathematical testament summarising work Galois had been polishing in prison.



- Solvability by radicals — modern *Galois theory*.
- Modular equations and the exceptional $\mathrm{PSL}(2, p)$ for $p = 5, 7, 11$.
- Abelian integrals (algebraic differentials).

*"Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as to the **importance** of these theorems."*

Why we know it. Chevalier printed the letter (*Revue Encyclopédique*, Sept 1832); the manuscripts were rescued by **Liouville** and published in 1846 — Galois published nothing properly in his lifetime.