Solvability by Radicals

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Outline

In this file: : Solvability by radicals (§4.2 of Lecture Notes):

1. Formulation of solvability by radicals: radical extensions;
2. Galois' Great Theorem;
3. Examples.

Question. Is there a "formula" for roots of a polynomial $f(x)$ of degree n that involves only addition, subtraction, multiplication, division, and taking roots of coefficients of $f(x)$?

Simplest example: $x^2 + bx + c = 0$ if and only if

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}.$$

Precise formulation/definitions.

1. Let m be a positive integer. A field extension L of K is called a pure extension of type m if $L = K(a)$ for some $a \in L$ and if $a^m \in K$.

2. A tower of fields
$$K = L_0 \subset L_1 \subset \cdots \subset L_n$$
is called a radical tower if each L_{j+1} is a pure extension of L_j. In this case, we call L_n a radical extension of L_0.

3. Let K be a field. A polynomial $f(x) \in K[x]$ is said to be solvable by radicals over K if there exists a radical extension L over K in which f splits completely.

Example 2. For $f(x) = x^2 + bx + c \in \mathbb{C}[x]$, let

$$K = \mathbb{Q}(b, c),$$

so $f(x) \in K[x]$. Let

$$L_1 = K(\sqrt{b^2 - 4c}).$$

Then L_1 is a pure extension over K of type 2, and f completely splits in L_1. Therefore, $f(x)$ is solvable by radicals over K.

Example 3: For $f(x) = x^3 + px + q \in \mathbb{C}[x]$, the roots of $f(x)$ are

$$\alpha_1 = y_0 + z_0, \qquad \alpha_2 = \omega_3 y_0 + \omega_3^2 z_0, \qquad \alpha_3 = \omega_3^2 y_0 + \omega_3 z_0,$$

where $\omega_3 = e^{\frac{2\pi i}{3}}$, y_0 is one solution of

$$y_0^3 = \frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right),$$

and $y_0 z_0 = -p/3$. Let $K = \mathbb{Q}(p, q)$. Then $f \in K[x]$. Let

$$L_1 = K\left(\sqrt{q^2 + \frac{4p^3}{27}}\right), \qquad L_2 = L_1(y_0), \qquad L_3 = L_2(\omega_3).$$

Then

$$K \subset L_0 \subset L_2 \subset L_3 \ni \alpha_1, \alpha_2, \alpha_3.$$

Example 4. Quartic polynomials: let $r \neq 0$ and consider

$$f(x) = x^4 + qx^2 + rx + s \in \mathbb{C}[x].$$

Let $K = \mathbb{Q}(q, r, s)$, so $f(x) \in K[x]$. Is f solvable by radicals over K?

A method from the 16th century: Solve for $k, l, m \in \mathbb{C}$ from

$$x^4 + qx^2 + rx + s = (x^2 + kx + l)(x^2 - kx + m) \qquad (1)$$

and solve for x from $x^2 + kx + l = 0$ or $x^2 - kx + m = 0$.

$$(1) \quad \iff \begin{cases} l + m - k^2 = q \\ k(m - l) = r \\ lm = s \end{cases} \quad \iff \quad \begin{cases} 2m = k^2 + q + r/k \\ 2l = k^2 + q - r/k \\ 4lm = 4s \end{cases}$$

$$\implies k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0. \qquad (2)$$

Solve k^2 from (2) as a root of cubic $g(x) \in K[x]$! Thus $\exists$ radical tower

$$L_0 = K \subset L_1 \subset L_2 \subset L_3$$

with $k^2 \in L_3$.

Let $L_4 = L_3(k)$, so have the radical tower

$$L_0 = K \subset L_1 \subset L_2 \subset L_3 \subset L_4 \ni k, l, m..$$

Solve m and l from

$$2m = k^2 + q + \frac{r}{k}, \qquad 2l = k^2 + q - \frac{r}{k},$$

to get $l, m \in L_4$. Recall

$$f(x) = (x^2 + kx + l)(x^2 - kx + m).$$

Take $L_5 = L_4(\sqrt{k^2 - 4l})$ and $L_6 = L_5(\sqrt{k^2 - 4m})$. Have radical tower

$$L_0 = K \subset L_1 \subset L_2 \subset L_3 \subset L_4 \subset L_5 \subset L_6,$$

and f splits completely in L_6. Thus $f(x)$ is solvable by radicals over K.

Summary. Every non-zero

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{C}[x]$$

of degree $n \leq 4$ is solvable by radicals over $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$.

Theorem (Galois' Great Theorem)

For $f(x) \in K[x]$ non-constant and $\mathrm{Char}(K) = 0$,

$$f(x) \text{ is solvable by radicals over } K \iff \mathrm{Gal}_K(f) \text{ is a solvable group.}$$

On solvable groups.

1. A group is G is said to be solvable if there exists a finite sequence
$$\{e\} \subset G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$
such that each G_j is a normal subgroup of G_{j-1} and that G_{j-1}/G_j is abelian. Such a series is also called a normal series.

2. Abelian groups are solvable;

3. A subgroup of a solvable group is solvable; a quotient of a solvable group is solvable.

4. The permutation group S_n is solvable for $n \leq 4$.

5. The permutation group S_n is not solvable for $n \geq 5$.

A class of examples. Assume that an irreducible quintic (i.e., order 5) polynomial $f(x) \in \mathbb{Q}[x]$ has three distinct real roots and two non-real roots in $\mathbb{C}$. Then the Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$ of f is isomorphic to S_5, and thus f is not solvable by radicals over $\mathbb{Q}$.

Example. Let L be the splitting field of $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$.

- L is a Galois extension of $\mathbb{Q}$.
- As f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, f has no repeated roots L. Thus $\mathrm{Gal}_{\mathbb{Q}}(L)$ is isomorphic to a subgroup of S_5.
- Calculus shows that f has three real roots and two complex roots.

Example continued:

- The complex conjugation $z \to \overline{z}$ is one element of order 2 in $\mathrm{Gal}_{\mathbb{Q}}(L)$.
- A real root r of f gives $L_1 = \mathbb{Q}(r)$ with $[L_1 : \mathbb{Q}] = 5$. Thus $|\mathrm{Gal}_{\mathbb{Q}}(L)| = |L : Q|$ is divisible by 5.
- Cauchy's theorem implies that $\mathrm{Gal}_{\mathbb{Q}}(L)$ has an element of order 5.
- Conclude that $\mathrm{Gal}_{\mathbb{Q}}(L) \cong S_5$.
- There are 156 subgroups of S_5,so there are 156 fields M with $\mathbb{Q} \subset M \subset L$.

Prepare for the proof of Galois' Great Theorem.

Lemma

Let K be a subfield of $\mathbb{C}$, let $a \in K$, and let L be the splitting field of $x^n - a$ over K. Then $\mathrm{Gal}_K(L)$ is a solvable group.

Proof. Let $\beta \in \mathbb{C}$ be a solution of $x^n - a = 0$, and let

$$R = \{e^{2\pi ki/n} : 0 \le k \le n-1\},$$
$$R_0 = \{e^{2\pi ki/n} : 1 \le k \le n-1,\ (k,n) = 1\} \subset R.$$

Case 1. K contains some $\xi \in R_0$. Then $R \subset K$, so

$$L = K(\beta).$$

Then $\mathrm{Gal}_K(L)$ is abelian: any $\sigma, \tau \in \mathrm{Gal}_K(L)$ are of the form

$$\sigma(\beta) = \xi^j \beta, \qquad \tau(\beta) = \xi^k \beta$$

for some j, k, so

$$(\sigma\tau)(\beta) = \sigma(\xi^k \beta) = \xi^k \sigma(\beta) = \xi^{k+j}\beta = (\tau\sigma)(\beta).$$

Proof continued:

Case 2. K does not contain any element of R_0.

- Let $\xi \in R_0$. Then $K \subset K(\xi) \subset L = K(\beta, \xi)$. Thus have
$$\{e\} \subset \mathrm{Gal}_{K(\xi)}(L) \subset \mathrm{Gal}_K(L).$$
- Both extensions $K \subset L$ and $K \subset K(\xi)$ are Galois.
- By Fundamental Theorem of Galois Theory, $\mathrm{Gal}_{K(\xi)}(L)$ is a normal subgroup of $\mathrm{Gal}_K(L)$ and
$$\mathrm{Gal}_K(L)/\mathrm{Gal}_{K(\xi)}(L) \cong \mathrm{Gal}_K(K(\xi)).$$
- By Case 1, $\mathrm{Gal}_{K(\xi)}(L)$ is abelian.
- The group $\mathrm{Gal}_K(K(\xi))$ is also abelian: any $\sigma \in \mathrm{Gal}_K(K(\xi)$ is uniquely given by $\sigma(\xi) = \xi^k$ for some k.
- Conclude that $\mathrm{Gal}_K(L)$ is solvable.