Galois Theory: Polynomials of Degree 5 and Up

Tokuei Higashino

Union College

Quadratic Formula

$$ax^2 + bx + c = 0$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Cubic Formula

$$ax^3 + bx^2 + cx + d = 0$$

$$\begin{aligned}
x_1 = &- \frac{b}{3a} \\
&- \frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d + \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\
&- \frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d - \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\
x_2 = &- \frac{b}{3a} \\
&+ \frac{1 + i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d + \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\
&+ \frac{1 - i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d - \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\
x_3 = &- \frac{b}{3a} \\
&+ \frac{1 - i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d + \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\
&+ \frac{1 + i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d - \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]}
\end{aligned}$$

Question

Are there general solutions by radicals for polynomials of degree 5 and up?

Answer

No.

How do we prove this?

- translate into question about fields
- use Galois theory to translate into question about groups

Definition

A *field* is a set closed, associative, and commutative under $+$ and $\cdot$, contains 0, 1, negatives, and reciprocals, and satisfies the distributive laws of $\cdot$ over $+$.

Example

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Definition

A *field extension* of a field K is a field L that contains K.

Example

$\mathbb{R}$ is a field extension of $\mathbb{Q}$.

Example

$\mathbb{Q}(\sqrt{2})$ is a field extension of $\mathbb{Q}$.

Question

Given a polynomial $p(x)$ with coefficients in K and of degree 5 or up, is there a sequence of radical extensions $K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$ such that all of the roots of $p(x)$ are in K_n?

$$\begin{array}{ll}
K_n = K_{n-1}(\sqrt[r_n]{a_n}) & \\
\cup\!\mid & \\
\vdots & \\
\cup\!\mid & \\
K_2 = K_1(\sqrt[r_2]{a_2}) & \\
\cup\!\mid & \\
K_1 = K_0(\sqrt[r_1]{a_1}) & \\
\cup\!\mid & \qquad\qquad r_i \in \mathbb{N} \\
K_0 = K & \qquad\qquad a_{i+1} \in K_i
\end{array}$$

Definition

An *algebraic extension* L of K is a field extension such that for all $a \in L$, there exists a polynomial $p(x)$ with coefficients in K such that $p(a) = 0$.

Non-example

$\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$, since $\pi \in \mathbb{R}$.

Example

$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is an algebraic extension of $\mathbb{Q}$, since $a + b\sqrt{3}$ is a root of the polynomial $x^2 - 2ax + a^2 - 3b^2$.

All radical extensions are algebraic extensions.

Definition

A *normal extension* L of K is a field extension such that for every polynomial $p(x)$ with coefficients in K, if L contains one of its roots, then L contains all of its roots.

Example

$\mathbb{C}$ is a normal extension of $\mathbb{R}$, which follows from the Fundamental Theorem of Algebra.

Non-example

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ is not a normal extension of $\mathbb{Q}$, since the complex roots of $x^3 - 2$ are not in $\mathbb{Q}(\sqrt[3]{2})$.

Theorem

L is a normal extension of K iff for some polynomial $p(x)$ with coefficients in K, L contains all of p's roots.

Example

$\mathbb{Q}(\sqrt{6})$ contains $\sqrt{6}$ and $-\sqrt{6}$, which are roots of $x^2 - 6$, which is a polynomial with coefficients in $\mathbb{Q}$.

Definition

A *separable extension* L of K is a field extension such that for all $a \in L$, there exists an irreducible polynomial $m(x)$ with coefficients in K with distinct roots.

Example

Any algebraic extension of $\mathbb{Q}$, such as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a separable extension.

Definition

A *Galois extension* of K is a field extension that is algebraic, normal, and separable over K.

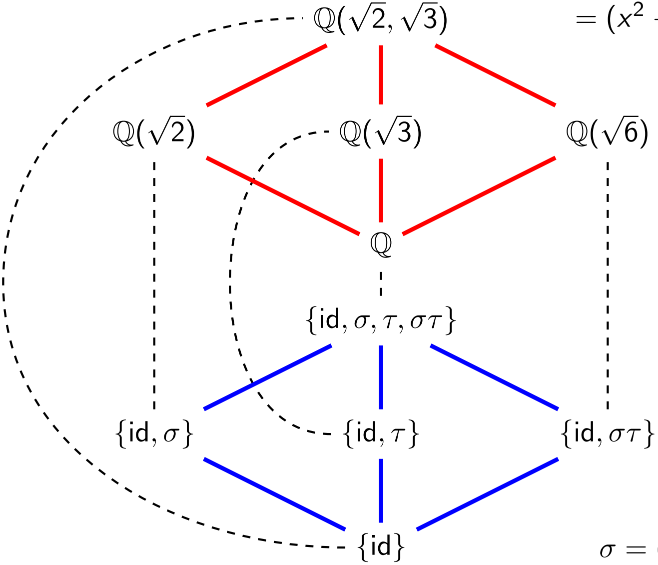
Definition

The *Galois group* of a field extension L over K is the set of automorphisms of L that preserve K. It is denoted $\mathrm{Gal}(L/K)$.

Fundamental Theorem of Galois Theory

If L is a finite Galois extension of K, then there is a one-to-one correspondence between the field extensions of K that are contained in L and the subgroups of $\mathrm{Gal}(L/K)$.

$$
\begin{aligned}
p(x) &= x^4 - 5x^2 + 6 \\
&= (x^2 - 2)(x^2 - 3)
\end{aligned}
$$



$$
\begin{aligned}
\sigma &= (\sqrt{3} \quad -\sqrt{3}) \\
\tau &= (\sqrt{2} \quad -\sqrt{2}) \\
\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) &= \{\mathrm{id}, \sigma, \tau, \sigma\tau\}
\end{aligned}
$$

Definition

A polynomial $p(x)$ with coefficients in K is *solvable by radicals* if there exists a sequence of radical extensions $K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$ such that all the roots of $p(x)$ are in K_n.

Definition

A group G is *solvable* if there exists a sequence of subgroups $\{id\} = G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m = G$, such that G_j is normal in G_{j+1} and $|G_{j+1}|/|G_j|$ is prime.

Theorem

$p(x)$ is solvable by radicals iff $\mathrm{Gal}(K_n/K)$ is solvable.

Abel-Ruffini Theorem

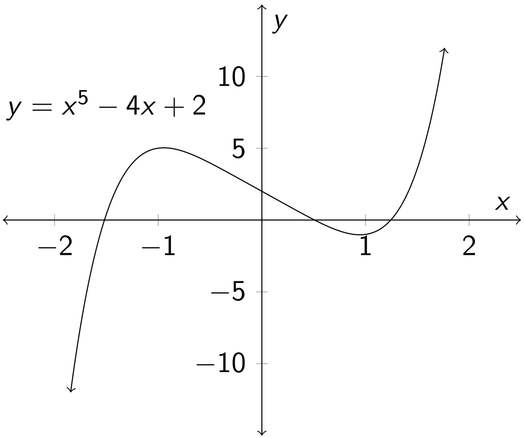
There exist polynomials of every degree ≥ 5 which are not solvable by radicals.

Lemma

If $f(x)$ is an irreducible polynomial over $\mathbb{Q}$, of prime degree p, and if f has exactly $p-2$ real roots, then its Galois group is S_p.

Lemma

If $n \geq 5$ and $\mathrm{Gal}(L/K) = S_n$, then $\mathrm{Gal}(L/K)$ is not solvable.



y
10
$y = x^5 - 4x + 2$
5
x
-2
-1
1
2
-5
-10