Solvability By Radicals

Robert Sweeney Blanco

Advisor: Brandon Williams

December 5, 2017

Linear and Quadratic Equations

Pretty straightforward...

$$ax + b = 0 \Rightarrow x = \frac{-b}{a}$$

$$ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Is there a cubic equation? What about a quartic equation? Is there a limit?

The answer for all these questions is yes. Both the cubic and quartic were eventually found and published by the 16th century mathematician Niccolo Tartaglia, although it is unclear if he was the first to do it. However, there does not exist a generalized formula for the quintic and polynomials of higher degrees.

Some definitions

Splitting Field

Let K be a subfield of $\mathbb{C}$ and $p \in K[x]$ be a nonzero polynomial. The splitting field over K of p is $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$ where $\{\alpha_i\}$ is the set of roots for p.

Galois Group

If L is a field extension of K,
$Gal(L/K) = \{g \in Aut(L) | g(k) = k \ \forall k \in K\}$

Fixed Field

If L is a field extension of K, a subfield of $\mathbb{C}$, and H is a subgroup of $Gal(L/K)$, $Fix(H) = \{l \in L | g(l) = l \ \forall g \in H\}$

Galois Correspondence

Correspondence 1

Subgroups of $Gal(L/K)$ and intermediate fields of L/K correspond in a one to one fashion.

Correspondence 2

The normal subgroup of $Gal(L/K)$ correspond to intermediate fields of L/K that are splitting fields.

Example

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr] & \mathbb{Q}(\sqrt{6}) \arrow[d] & \mathbb{Q}(\sqrt{2}) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & \{1\} \arrow[dl] \arrow[d] \arrow[dr] & \\
\{1,f\} \arrow[dr] & \{1,fg\} \arrow[d] & \{1,g\} \arrow[dl] \\
 & \{1,f,g,fg\} &
\end{tikzcd}$$

Solvability by Radicals

Radical Extension

A radical extension K of a field F is a field that may be written $K = F(a_1, ..., a_m)$ with $a_i^{n_i} \in F(a_1, ..., a_{i-1})$ for $1 \leq i \leq m$ and $n_i \in \mathbb{N}$

Solvable by Radicals

Let F be a subfield of $\mathbb{C}$ and $p \in F[x]$ an irreducible polynomial. Then p is solvable by radicals over F if each root a of p lies in a radical extension of F.

Tower of Field Extensions

Robert Sweeney Blanco

Suppose L is a splitting field and a radical extension of F with a particular representation as a radical extension using b_i for $i = 1, ..., m$ with corresponding exponents n_i. Let $n = lcm(\{n_i\})$ and ω be a primitive nth root of unity. Then $L(\omega)/F$ is a splitting field extension, which has the following tower of field extensions:

$$F \subset F(\omega) \subset F(\omega, b_1) \subset ... \subset F(\omega, b_1, ..., b_m) = L(\omega)$$

Solvable Subgroups

Define $G_i = Gal(L(\omega)/F(\omega, b_1, ..., b_i))$, which gives the following tower of subgroups:

$$Gal(L(\omega)/F(\omega)) \supset G_1 \supset ... \supset G_m = \{e\}$$

G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian.

Solvable Groups

A finite group is solvable if there exists a tower of subgroups such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian.

TFAE

Let F be a subfield of $\mathbb{C}$, and $p \in F[X]$ be an irreducible polynomial. Let L be the splitting field of p over F. The following are equivalent:

1. Some root of p lies in a radical extension of F
2. There is a radical extension of F containing all the roots of p
3. p is solvable by radicals
4. $Gal(L/F)$ is a solvable group

Insolvability of the Quintic

Let $p(x) = x^5 + 20x + 16$, if we can show that the galois group of the splitting field of p over $\mathbb{Q}$ is not solvable, then p is not solvable by radicals.

Lemma

Discriminant

Let p be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n$.

$$disc(p) = \Big(\prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)\Big)^2 = (-1)^{\frac{n(n-1)}{2}} Res_x(p, p')$$

Lemma: If $p \in K[x]$ has degree n, the following are equivalent:

1. $disc(p)$ is the square of an element in K
2. $x^2 - disc(p)$ has a linear factor over K
3. $Gal(p, K) \subset A_n$

Properties of Alternating Groups

1. A_n is abelian iff $n \leq 3$
2. A_n is simple iff $n = 3$ or $n \geq 5$
3. A_5 has order 60, making it the smallest non-abelian simple group

Proof

$(-1)^{10} Res_x(x^5 + 20x + 16, 5x^4 + 20) = 1,024,000,000 = (32,000)^2$, thus by the lemma $Gal(p, K) \subseteq A_5$. It can be shown that $|Gal(p, K)| = 60$, thus $Gal(p, K) = A_5$. Since A_5 is simple, $Gal(p, K)$ is not a solvable group. Thus p is not solvable by radicals.