ON THE INSOLVABILITY OF THE QUINTIC

DAKSH DHEER
(THIRD YEAR, HANSRAJ COLLEGE, 2023)

Abstract. In the 19th century, Évariste Galois proved that all algebraic equations of degree higher than 4 cannot always be solved by radicals, i.e., there does not exist a formula that relates the roots of the equations to their coefficients using the operations of addition, multiplication, subtraction, division, exponentiation and taking nth roots. This paper attempts to prove this result via a deep connection between field extensions and symmetric groups: an elegant amalgamation that manifests as the fundamental theorem of Galois theory.

1. Introduction

In algebra, an equation of the form $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ is called a quintic equation in one variable. The solutions of the equation are called its *roots*. By the Fundamental Theorem of Algebra and the fact that complex roots occur in conjugate pairs, there always exists a real root of every quintic equation. However, unlike the quadratic formula (which enables one to quickly find roots of a quadratic equation), a general **quintic formula** does not exist. We attempt to prove so in this article.

First, we need to understand what we mean when we say that a general quintic equation is not solvable by radicals and express this idea appropriately in the language of abstract algebra.
An equation (or rather, a polynomial) is solvable by radicals if its roots can be expressed via the operations of addition, subtraction, multiplication, division, and extraction of n-th roots.

We start with some prerequisite definitions from field theory that will prove useful for our discussions.

Definition 1. *A **field extension** is defined to be an inclusion of the field $L \hookrightarrow K$ of in a larger field K, denoted by K/L.*

For our purposes, the field extensions we will be interested in are adjunctions of algebraic elements to the field of rationals, i.e., $\mathbb{Q}[\alpha]$. These are known as *primitive* field extensions. Note that $\mathbb{Q}[\alpha]$ is the field generated by $\mathbb{Q}$ and
$alpha$, hence it must contain all sums, products, and powers of all algebraic expressions containing α.
For example, if we take $\alpha = \sqrt{2}$, then $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

Note that this is the smallest field containing both $\mathbb{Q}$ and $\sqrt{2}$.

Definition 2. *An element α is said to be **algebraic** over a field K if it is the root of some polynomial $p(x) \in K[x]$. Otherwise, the element is said to be **transcendental**.*

We call a field extension K/L an *algebraic extension* if every element of L is algebraic over K.

Remark 1. *If α is algebraic over a field K, then $\mathbb{K}[\alpha]$ is an algebraic extension. In general, if $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ are algebraic over K, then $K[\alpha_1, \alpha_2, ..., \alpha_n]$ is an algebraic extension.*

For example, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[1+\sqrt[3]{29}]$, $\mathbb{Q}[23+\sqrt[4]{1+56\sqrt[5]{7}}]$ are all algebraic extensions of $\mathbb{Q}$.

An interesting property of field extensions is that they may be regarded as vector fields over the base field. Hence, they must have a dimension over the base field.

Definition 3. *The degree of an algebraic extension $K[\alpha]/K$, denoted by $[K[\alpha] : K]$, is the dimension of $K[\alpha]$ as a vector space over K.*

We present two theorems without proof which are vital for our objective.

Theorem 1. *If finite, then $[K[\alpha] : K]$ is the same as the degree of the minimal polynomial of α, say n, and a basis of $K[\alpha]$ is given by $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.*

Theorem 2. *Let $B_1 = \{\beta_1, \beta_2, ..., \beta_n\}$ be a basis for for E over F and $B_2 = \{\gamma_1, \gamma_2, ..., \gamma_n\}$ be a basis for K over E. Then, $B = \{\beta_1\gamma_1, \beta_2\gamma_2, ..., \beta_n\gamma_n\}$ is a basis for K over F.*

These theorems allow us to construct a basis for any finite algebraic extension in the following way: let K be a field and consider the finite algebraic extension $E = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

We build up E by first adjoining α_1 to K, forming $K[\alpha_1]$, then we adjoin α_2 to get $K[\alpha_1][\alpha_2] = K[\alpha_1, \alpha_2]$, and iterate this process until α_n.
The first theorem gives us a basis for each intermediate field $K[\alpha_1, \alpha_2, \ldots, \alpha_i]$ over $K[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$, and the second theorem shows us how to construct a basis for the intermediate field over the base field, K.

Question. *Why do we need to do all this?*

Remember that our definition of 'solvable by radicals' included the operations of addition, subtraction, multiplication, division, and extraction of n-th roots. Everything here, except the extraction of n-th roots, may be done in a field. It is this last operation that we need to induce in our field, for which we need to introduce this additional structure of algebraic extensions.
The next definition is motivated by the same:

Definition 4. *A **simple radical extension** is a field extension that is generated by a single element α satisfying $\alpha^n = b$ for some a in the base field, i.e., extensions* *of the form $K[\alpha]$ where $\alpha^n \in K$ for some natural number n.*

We now can finally conclude this section by defining the field extensions that we'd be working with the most:

Definition 5. *A **splitting field** of a polynomial $p(x) \in K[x]$ is defined as the smallest field in which $p(x)$ factors into linear factors.*

Note: A splitting field of $p(x)$ contains the base field as well as all roots of $p(x)$.

For example, consider $p_1(x) = x^3 - 3$ over $\mathbb{Q}$, then its splitting field would be $\mathbb{Q}[\sqrt[3]{3}, \frac{1}{2}\left(-1 + \sqrt{3}i\right)]$. For $p_2(x) = x^2 - 2$, the splitting field would be $\mathbb{Q}[\sqrt{2}]$

2. Field Extensions and Galois Groups

Let L be a splitting field of some polynomial $p(x) \in K[x]$ and consider a field automorphism $\sigma : L \longrightarrow L$ such that σ preserves the base field K.

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and α be a root of $p(x)$.
We assume that $p(x)$ has no repeated roots. Then,

$$0 = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

$$\implies \sigma(0) = \sigma(a_n\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \ldots \sigma(a_1\alpha^1) + \sigma(a_0)$$

$$\implies 0 = a_n\sigma(\alpha^n) + a_{n-1}\sigma(\alpha^{n-1}) + \ldots \sigma a_1(\alpha^1) + a_0$$

(since σ fixes the base field K)

Hence, $\sigma(\alpha)$ is another root of $p(x)$. Thus, all such automorphisms simply permute the roots of $p(x)$ and we may take this to be the most vital property of automorphisms in this special case when L is a splitting field.
We call L a ***galois extension*** of K.
For example, one may consider the familiar automorphism: $\mathbb{C} \longrightarrow \mathbb{C}$ given by $z \rightsquigarrow \bar{z}$. This preserves the base field $\mathbb{R}$ conjugate of a real number is a real number.

One may show that all such automorphisms of L, that fix K, form a group, which we denote by $Aut(L/K)$, and this group is called the ***galois group*** of L. This is a subgroup of $Aut(L)$, the group of all automorphisms of L. It is usually denoted as $\text{Gal}(L/K)$.

Theorem 3. *If L is the splitting field of a polynomial over K, then $|Gal(L/K)| = [L : K]$.*

For example, $|\text{Gal}(\mathbb{Q}[i]/\mathbb{Q})| = [\mathbb{Q}[i] : \mathbb{Q}] = 2 \implies \text{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \cong \mathbb{Z}_2$.
To verify this, consider an arbitrary automorphism $\sigma : \mathbb{Q}[i] \longrightarrow \mathbb{Q}[i]$ such that $\sigma(p) = p \ \ \forall p \in \mathbb{Q}$. Then, for any arbitrary element $a + bi \in \mathbb{Q}[i]$, we have:
$\sigma(a + bi) = \sigma(a) + \sigma(b)\ \sigma(i) = a + b\ \sigma(i)$.

Since σ is an automorphism, it must preserve the order of i, so $\sigma(i) = i$ or $-i$, hence we only have two automorphisms.
Therefore, $\text{Gal}(\mathbb{Q}[i]/\mathbb{Q}) = \{\sigma_i, \sigma_{-i}\} \cong \mathbb{Z}_2$.

To a field extension L, we have associated a group above, i.e., the galois group. Thus, in other words, we have found an association from a subfield K of L to a subgroup of $Aut(L)$. There also exists an association from a given subgroup of $E = Aut(L)$ to a subfield of L as follows:

For any subgroup H of E, we define the fixed field E^H to be the set of elements in L that are fixed by all elements of H, that is, $E^H = \{a \in L : \sigma(a) = a, \ \ \forall \ \sigma \in H\}$. It is easy to see that E^H is a subfield of L, thus, we have established a map from subgroups of E to subfields of L.

This gives us a bijective correspondence between field extensions and subgroups of the galois group, which is the fundamental theorem of Galois theory. Here we have proved it in the specific case when L is splitting field, which makes the field extensions become galois extensions.

3. Solvable Groups

Let us now make the notion of solvability by radicals more precise.

Definition 6. *Let α be algebraic over L. Then α is solvable by radicals if $\alpha \in K$ that can be obtained from L by simple radical extensions successively, such that*

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$

where for $K_{i+1} := K_i\left(\sqrt[n_i]{a_i}\right)$ for some $a_i \in K_i$.

We call the field K a root extension of L, which is a Galois extension. We refer to the extensions K_{i+1}/K_i as the intermediate extensions of K. The motivation for $K_{i+1} := K_i\left(\sqrt[n_i]{a_i}\right)$ comes from the fact that by choosing this, our extensions automatically become galois extensions. Moreover, they give rise to galois groups that are abelian, which would prove to be useful. Finally, a polynomial $f(x) \in F[x]$ can be solved by radicals if all of its roots are solvable by radicals.

One can make sense of this definition by seeing that if we start with $\alpha \in K$, we can rewrite α in terms of elements of the field (via addition, subtraction, multiplication and division) one step down in the chain and radicals (taking nth roots) of these elements. We can repeat this process until we reach L and have α written in terms of elements of L and radicals, or multiple radicals, of elements in L. For example, suppose $L = \mathbb{Q}$ and $\alpha = \sqrt{5 + \sqrt[4]{51}}$. Then $K_0 = \mathbb{Q}$ and $K_1 = K_0\left(\sqrt[4]{a_0}\right)$, where $a_0 = 51$. We then let $K_2 = K_1\left(\sqrt{a_1}\right)$, where $a_1 = 5 + \sqrt[4]{51} \in K_1$. Since $\alpha \in K_2$, we have $K_2 = K$, so K_2 and we are done.

In a similar vein, we define the notion of solvability for groups:

Definition 7. *A finite group G is said to be solvable if $\exists K_i \lhd G, \ i = 0, 1, \ldots s$*

$$\{e\} = K_s \lhd K_{s-1} \lhd \cdots \lhd K_0 = G$$

such that K_i/K_{i+1} is cyclic.

The insolubility of the general quintic boils down to the equivalence between solvability of polynomials and solvability of their galois groups.

Lemma 1. *If extension K_{i+1}/K_i is a radical extension, then the quotient group G_{i+1}/G_i is a cyclic group for each i.*

Theorem 4. ***(Galois, 1830).*** *The separable polynomial $f(x) \in F[x]$ can be solved by radicals if and only if its Galois group is solvable.*

We only prove one direction: suppose we have a polynomial $f(x)$ of degree n that is solvable by radicals. This means that there exists a radical extension K of the field F containing the roots of $f(x)$, such that K/F is a Galois extension. We will show that its Galois group $G = \mathrm{Gal}(K/F)$ is solvable.
Since $f(x)$ is solvable by radicals, we can construct a tower of radical extensions $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_m = K$, such that each extension F_{i+1}/F_i is a radical extension. As a result, each intermediate field F_i is obtained by adjoining radicals to the previous field F_{i-1}. Thus, the intermediate fields F_i can be expressed by radicals.

Now, consider the Galois group $\mathrm{Gal}(K/F)$. Let G_i be the subgroup that fixes the field F_i, i.e., $G_i = \mathrm{Gal}(K/F_i)$. Since each extension F_{i+1}/F_i is a radical extension, the corresponding quotient groups G_i/G_{i+1} are cyclic (by Lemma).

Hence, we have

$$\{e\} = G_m/G_{m+1} \lhd G_{m-1} \lhd \cdots \lhd G_2/G_1 \lhd G_m/G_1/G_0 = \mathrm{Gal}(K/F)$$

Therefore, if the polynomial $f(x)$ is solvable by radicals, the Galois group G is a solvable group.

As an example to illustrate these ideas, consider the polynomial $f(x) = x^5 - 6x^3 - 6x^2 + 9x + 3$ over $\mathbb{Q}$. We will show that this polynomial is irreducible over $\mathbb{Q}$, and its Galois group over $\mathbb{Q}$ is not solvable.

First, we check that $f(x)$ has no rational roots. By the rational root theorem, any rational root of $f(x)$ must be of the form $\frac{p}{q}$, where p divides 3 and q divides 1. The only possible rational roots are $\pm 1, \pm 3$, and we can check that none of them are roots of $f(x)$.

Next, we show that $f(x)$ is irreducible over $\mathbb{Q}$. By Eisenstein's criterion with $p = 3$, we see that $f(x)$ is irreducible over $\mathbb{Q}$.

Since $f(x)$ is irreducible over $\mathbb{Q}$, its Galois group is the Galois group of the splitting field of $f(x)$, which is isomorphic to S_5.

Therefore, the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to S_5, which is not solvable because its only normal subgroup is A_5, which is not cyclic.

That is,

$$\{e\} \lhd A_5 \lhd S_5 = G$$

and $A_5/\{e\} \cong A_5$ is not cyclic. Hence, the general quintic is not solvable by radicals.

Moreover, in general, quadratics, cubics and quartics are solvable by radicals because S_n is solvable for $n \leq 4$ since:

$$\{e\} \lhd S_2$$

$$\{e\} \triangleleft Z_3 \triangleleft S_3$$
$$\{e\} \triangleleft Z_2 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

References

[1] Artin, Emil. *Galois Theory*. United States, Dover Publications, 1998. ISBN 9780486158259.
[2] Notes. Galois theory.
[3] Article. Galois Theory and the Insolvability of the Quintic Equation.
[4] Artin, Michael. *Algebra*. Germany, Pearson Education, 2011. ISBN 9780132413770.