Algebra II:
Application of Galois to solvability of equations

Ignacio Arroyo Rodrigo
Lucia Escudero Sartages
Daniel Alconchel Vázquez

December of 2022

Contents

1 Historical Context

Évariste Galois (1811-1832) was a French mathematician and political activist who produced a method of determining when a general equation could be solved by radicals and is famous for his development of early group theory.

He realized that the algebraic solution to a polynomial equation is related to the structure of a group of permutations associated with the roots of the polynomial.

This problem was tackled in 1770 by Lagrange, where he considering in terms of permutations of the roots, which yielded an auxiliary polynomial of lower degree, providing a unified understanding of the solutions and laying the groundwork for group theory and Galois' theory. However, Lagrange's method did not extend to quintic equations or higher.

It was in 1799 , where Paolo Ruffini attempted to prove the impossibility of solving the general quintic equation by radicals. Ruffini's effort was not wholly successful, and in 1824 Niels Abel gave a correct proof and published it that same year, establishing the Abel–Ruffini theorem.

While Ruffini and Abel established that the general quintic could not be solved, was Évariste Galois, who began searching for the necessary and sufficient conditions under which an algebraic equation of any degree can be solved by radicals. His method was to analyze the permutations of the roots of the equation.

His main discover was that solvability by radicals is possible if and only if the group of automorphisms is solvable, which means essentially that the group can be broken down into simple prime-order components that always have an easily understood structure. The term solvable is used because of this connection with solvability by radicals.

Thus, Galois perceived that solving equations of the quintic and beyond required a wholly different kind of treatment than that required for quadratic, cubic, and quartic equations. Although Galois used the concept of group and other associated concepts, such as coset and subgroup, but he did not actually define these concepts, and he did not construct a rigorous formal theory.

Galois's manuscripts, with annotations by Joseph Liouville, were published in 1846 in the 'Journal de Mathématiques Pures et Appliquées'. But it was not until 1870 that group theory became a fully established part of mathematics.

2 Galois Theory Notions

2.1 Basics definitions

In this section it will be explained the basic definitions for Galois theory.

We say that a field L is an extension of K, if there exists a monomorfism $f : K \to L$

There exists several types of extensions that are related amoung them.

A field extension L/K is normal if the following holds: every irreducible $f \in K[x]$ that has a root in L splits into linear factors over L[x]. In other words,

$$\text{f has one root in L} \Rightarrow \text{all roots of f are in L.}$$

It is said that a irreducible polynomial $P \in K[x]$ is separable over K is it does not have multiple roots. If L/K is an algebraic extension, it is said that $\alpha \in L$ is separable over K if its minimum polynomial is. Hence, it is said that the extension L/K is separable if $\forall \alpha \in L$ is over K. If it is not separable, we say it is inseparable.

An algebraic extension L/K of fields is Galois if it is not a finite degree and K is the fixed of the group of K -automorphism of L

For an extension L/K, the following statements are equivalent:

1. L is the splitting field of a separable polynomial $f \in F[X]$
2. L is Galois over K
3. $L = L^G$ for some finite group G of automorphism of L
4. L is normal, separable, and finite over L

Any one of this four conditions of the theorem can be used to define a Galois extension.

2.2 Galois Group

When L/K is Galois, it is said that $\sigma : L \to L$ is an K-automorphism if it is an automorphism that that fix the elements of K. The set of all K-automorphism it is called the Galois group of L over K, and it is denoted by Gal(L/K).

2.3 Galois group of a polynomial

If a polynomial $f \in F[x]$ is separable, then its splitting F_f is Galois over F, and we call $Gal(F/F_f)$ the Galois group G_f of f.

Let f(X) = $\prod_{i=1}^{n}(X - \alpha_i)$ in a splitting field F_f. We know that the elements of $Gal(F_f/F)$ map roots of f to roots of f. Being automorphisms, they act as permutations on $\alpha_1, \alpha_2, ..., \alpha_n$. As the α_i generate F_f over F, an element of $Gal(F_f/F)$ is uniquely determined it defines. Thus G_f can be identified with subset of $\alpha_1, \alpha_2, ..., \alpha_n$ is isomorfic to S_n (symmetric group on n symbols).

2.4 Teorems needed to demostrate the fundamental theorem of Galois Theory

Before demostrare the fundamental theorem of Galois Theory, we need to indicate the next and useful teorems and lemmas:

Theorem 2.1. *If K is a finite extension field of E and E is a finite extension of F. Then K is a finite extension field of F and [K : F] [K : E][E : F].*

Lemma 2.2. *Let E be an extension field of F, and K be the fixed field of Gal(E/F), then Gal(E/F) Gal(E/K).*

Lemma 2.3. *Let E be a normal extension of field F, and K be an intermediate extension of E/F. For* $Gal(E/K) = Gal(E/\phi(K)) = \phi Gal(E/K)\phi^{-1}$,

2.5 The fundamental theorem of Galois Theory

Let F be a field with characteristic 0, if E splits over F for some polynomial in F[x], then the mapping from the set of subfields of E containing F to the set of subgroups of Gal(E/F) from K $\rightarrow$ Gal(E/K) is one to one. For subfield K of E containing F,

1. $[E : K]$ = | Gal(E/K) | and [K : F] = |Gal(E/F)| / | Gal(E/K)|.
2. If K splits in F[x], we have that Gal(E/K) is a normal subgroup of Gal(E/F) and Gal(K/F) is isomorphic to Gal(E/F)/Gal(E/K)
3. The fixed field of Gal(E/K) is K
4. Let H be a subgroup of Gal(E/F), we have that H = $Gal(E/E_H)$

We will proof this 4 statements:

1. Assume E splits over F for some polynomial in F[x], and let $K \subseteq E$ be arbitrary with containing F, $H \leq Gal(E/F)$, we want to show that there is a bijection under the operation $K \longrightarrow Gal(E/K)$.

   We first show $K \longrightarrow Gal(E/K)$ is injective. Let $K_1, K_2 \subseteq E$ be arbitrary with containing F, and assume $Gal(E/K_1) = Gal(E/K_2)$, we want to show that $K_1 = K_2$.
   Since K_1, K_2 contains F, we can write that $K_1 = E_{H_1}$, $K_2 = E_{H_2}$, where $H_1, H_2 \leq Gal(E/F)$. Since $H_1 = Gal(E/E_{H_1})$ and $H_2 = Gal(E/E_{H_2})$, and $Gal(E/K_1) = Gal(E/K_2)$ by assumption, we have that $H_1 = H_2$, then we have that $K_1 = E_{H_1} = E_{H_2} = K_2$, as desired.

   Now we show that K $\rightarrow$ Gal(E/K) is surjective. Assume $H \leq Gal(E/F)$ be arbitrary, we want to show that there exists $K \subset E$ containing F such that Gal(E/K) = H. We choose K = E_H, then we have that H = Aut(E/K). Since E/F is Galois, and K is an intermediate field where $F \subset K \subset E$, we have that E/K is Galois as well, thus Gal(E/K) = H, as desired.

2. Since $K = E_{Gal(E/K)}$ is a fixed field of Gal(E/K) and |Gal(E/F)| = [E : F], we have that $[E : K] = |Gal(E/K)|$ and $[E : F] = |Gal(F/E)|$, with theorem 2.1 we know that $|Gal(E/F)|/|Gal(E/K)| = [E : F]/[E : K] = [K : F]$, as desired.

3. Assume K is a splitting field of some $f(x) \in F[x]$ over F, then we know that the zeros of f(x) in K are also the zeros of f(x) in E. We know that $Gal(E/K)$ generates the zeros of f(x) in E, thus the zeros of f(x) in K is also generated by Gal(E/K). Let $\phi \in Gal(E/F)$ be arbitrary, by the previous discussion, we know that $\phi(K) = K$. Then by lemma 2.3, we have that

   $$Gal(E/K) = Gal(E/\phi(K)) = \phi Gal(E/K)\phi^{-1},$$

   thus Gal(E/K) is normal in Gal(E/F). It now remains to show that $Gal(K/F) \cong Gal(E/F)/Gal(E/K)$.

   Since Gal(E/K) is normal in Gal(E/F), we have that for all $\phi \in Gal(E/F)$, $Gal(E/K) = \phi Gal(E/K)\phi^{-1}$.

Then by lemma 2.3, we know that $Gal(E/K) = Gal(E/\phi(K)$, thus ϕ is an automorphism of K. By the first isomorphism theorem, we have that Gal(E/F)/Gal(E/K) is isomorphic to a subgroup of Gal(K/F). By part 1 we proved, we have that $[K : F] = |Gal(E/F)|/|Gal(E/K)| \leq |Gal(K/F)|$

Since $|Gal(K/F) \leq [K : F] = |Gal(E/F)/Gal(E/K)|$. Then by simple algebraic calculation of the degrees, we know that this subgroup is Gal(K/F) itself, thus $Gal(K/F) \cong Gal(E/F)/Gal(E/K)$, as desired.

4. Suppose f(x) is monic irreducible polynomial over K. Since E splits on f(x) over K, let K' be the fixed field of Gal(E/K). We have that E is also the splitting field of $f(x) \in K'[x]$. By previous proof 1, we have that [E : K] = |Gal(E/K)| and [E : K'] = |Gal(E/K')|. By lemma 2.2, we have that Gal(E/K) = Gal(E/K'). Then [E : K] = [E : K']. By theorem 2.1, we have that [E : K] = [E : K'][K': K]. Thus [K': K] = 1, by our choice of K' , we know that K = K', that is ,K is the fixed field of Gal(E/K), as desired.

3 Solvability of Equations

3.1 Solvable Groups

Let's start with defining what it means to be a solvable for a group. and learn some properties of solvable group.

Definition 3.1. A group G is solvable if it has a finite series of subgroups

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

such that

- $G_i \lhd G_{i+1}$ for $i = 0, ..., n-1$
- G_{i+1}/G_i is abelian for $i = 0, ..., n-1$

Lemma 3.2. *Suppose G, H, A are groups, then*

1. *If $H \lhd G$ and $A \subseteq G$, then $H \cap A \lhd A$ and*

$$\frac{A}{H \cap A} \cong \frac{HA}{A}$$

2. *If $H \lhd G$ and $H \subseteq A \lhd G$, then $H \lhd A$, $A/H \lhd G/H$ and*

$$\frac{G/H}{A/H} \cong \frac{G}{A}$$

Theorem 3.3. *Let G be a finite group. The following statements are equivalent:*

1. *G is a solvable group.*
2. *G has a normal serie with abelian factors.*
3. *Factors of composition series are all cyclic group of prime order.*

4. *G has a normal serie with cycle factor*

Proof. • 1 $\implies$ 2) We just need to consider the derivative serie of G.

• 2 $\implies$ 3) Let $G = G_0 \rhd G_1 \rhd G_2 \rhd ... \rhd G_r = 1$ be a normal serie with abelian factors. Now, we just need to apply the Jordan-Holder theorem[1].

• 3 $\implies$ 4) Immediate.

• 4 $\implies$ 1) Let be $G = G_0 \rhd G_1 \rhd G_2 \rhd ... \rhd G_r = 1$ be a normal serie with cyclic factors $\implies$ factors are abelian $\implies$ G/G_1 is abelian $\implies$ $G' < G_2$ and we can see by induction that $G^{(i} < G_i$. Suppose it true $\forall i$, as G_i/G_{i+1} is abelian, we have that $G_i < G_{i+1}G^{i+1} = (G^i)' < G_i' < G_{i+1} \implies G^{(r} < G_r = 1 \implies$ the series are abelian and G is solvable.

Theorem 3.4. *Suppose G is a group, $H \leqslant G$, $N \lhd G$, then:*

1. *If G is solvable, then H is solvable.*
2. *If G is solvable, then G/N is solvable.*
3. *If N and G/N are solvable, then G is solvable.*

Proof. 1. Assume G is solvable, we want to show that H is solvable. Since G is solvable by assumption. Let $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ be a series for G where G_{i+1}/G_i, is abelian. Let $H_i = G_i < capH$. Then H has a series $1 = H_0 \lhd H_1 \lhd ... \lhd H_n = H$. We calculate

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

by 3.2, and, since $\frac{G_i(G_{i+1} \cap H)}{G_i} \leqslant \frac{G_{i+1}}{G_i}$ where G_{i+1}/G_i is abelian, hence H_{i+1}/H_i is abelian, thus we have that H is solvable.

2. Assume G is solvable, we want to show that G/N is solvable. Let $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ be a series for G where G_{i+1}/G_i is abelian. Then G/N has a series

$$1 = N/N = G_0N/N \lhd G_1N/N \lhd ... \lhd G_nN/N = G/N$$

it remains to show that $\frac{G_{i+1}N/N}{G_iN/N}$ is abelian,

$$\frac{G_{i+1}N/N}{G_iN/N} \cong \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

by 3.2 and is a quotient of G_{i+1}/G_i. which is abelian, hence $\frac{G_{i+1}N/N}{G_iN/N}$ is abelian, thus G/N is solvable.

3. Assume N and G/N are solvable, we want to show that G is solvable. Let $1 = N_0 \lhd N_1 \lhd ... \lhd N_m = N$, and $1 = G_0/N \lhd G_1/N \lhd ... \lhd G_n/N = G/N$ be series for N and G/N. Then we can combine the two series together and get $1 = N_0 \lhd N_1 \lhd ... \lhd N_m = G_0 \lhd G_1 \lhd ... \lhd G_n = G$, then we have that the quotients of the series are either in the form of N_{i+1}/N_i of G_{i+1}/G_i, which are both abelian by our assumption that N and G/N are solvable and $G_{i+1}/G_i \cong \frac{G_{i+1}/N}{G_i/N}$. Thus, we have that G is solvable.

[1]The Jordan-Holder theorem states that any two composition series of a given group are equivalent. That is, the have the same length and the same composition factors, up to permutation and isomorphism.

3.2 Solvability by radicals

Definition 3.5. A field extension $k \subset K$ is radical if there exists a chain $k = k_0 \subset k_1 \subset ... \subset k_r = K$ such that for each i, $k_{i+1} = k_i(\alpha_i)$ with $\alpha_i^{p_i} \in k_i$ for some prime p_i; that is, each step consists of adjoining a p^{th} root, ($x^{p_i} - a_i$ may be reducible). $k \subset K$ is solvable if there exists an extension $K \subset L$ such that $k \subset L$ is radical.

Proposition 3.6. *Let $k \subset K$ be a Galois extension with Galois group $G = Gal(K/k)$.*

1. *G is soluble if and only if there exists a chain of intermediate fields $k = k_0 \subset k_1 \subset ... \subset k_r = K$ such that each $k_i \subset k_{i+1}$ is Galois group with Z/p_i.*
2. *Suppose in addition that k contains p distinct pth roots of 1 for every prime p dividing $|G|$. Then G is solvable if and only if $k \subset K$ is radical.*

Theorem 3.7. *If $P(X)$ is an irreducible polynomial over a base field of characteristic zero, and P can be solved by radicals, then the Galois group of P is solvable.*

Proof. a finite group G is said to be a solvable if each of its Jordan-Holder simple quotients is abelian.

Proposition 3.8. *Let $n \in \mathbb{N}$ and K a field such that $char(K)$ not divide n and it contains $n-th$ roots of unity:*

1. *For $a \in K$, let $K = K(\sqrt[n]{a})$. The extension F/K is cyclic of degree d, a divisor of n.*
2. *Conversely, if F/K is cyclic of degree n, then $F = K(\sqrt[n]{a}$ for some $a \in K$.*

Lemma 3.9. *Let K be a field of characteristic 0.*

1. *If E and F are radical extensions of K then so are FE/F and FE/E, so that $K \leq F \leq FE$ and $K \leq E \leq FE$ are radical towers.*
2. *If F and E are root extensions of K then so is FE.*
3. *If F is a root extension K then so is the normal closure L of F over K.*

Proposition 3.10. *The group S_n is solvable if $n \leq 4$.*

Theorem 3.11. *Let K be a field of characteristic 0, and $f(x) \in K[x]$. Let F be the splitting of $f(x)$. The polynomial $f(x)$ is solvable by radicals if $Gal(F/K)$ is a solvable group.*

Theorem 3.12. ***[Abel]*** *The general equation degree n is not solvable by radicals for any $n \geq 5$.*

Proof. Since the Galois group of the polynomial $f(x) = x^5 - 20x + 6$ is S_5, then by Theorem 3.11 and Proposition 3.10, the roots of this polynomial cannot be expressed by radicals. Hence there is no formula to solve the general equation of degree 5 by radicals. For $n > 5$ the existence of a solution by radicals of the general polynomial o degree n yields a solution by radicals of the equation $f(x) \cdot x^{n-5} = 0$, contradicting the above.

4 Some Classical aplications

We will now tackle some classical problems

Proposition 4.1. *If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset R$ by a series of compass and straightedge constructions then*

$$[F(\alpha) : F] = 2^k$$

for some integer $k \geq 0$

4.1 Doubling the cube

We shall look at whether or not it is possible to construct a cube of volume twice that of a given cube using a straight edge and compass. A cube of volume 2 has sides of length $\sqrt[3]{2}$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ but

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

which is not a power of 2. So the construction is not possible.

4.2 Trisecting the Angle

Let angle θ be constructible. A point p at a unit distance from the origin and angle θ from the X-axis in $\mathbb{R}^2$, shows that $cos(\theta)$ and $sin\theta)$ can be constructed. Conversely if $cos(\theta)$ and $sin(\theta)$ can be constructed, then so can the point at an angle of θ from the X-axis. Certain angles like $180^{\underline{o}}$ can be trisected. But this is not always possible. We shall prove using a counter example. Let $\theta = 60^{\underline{o}}$. Then $cos(\theta) = \frac{1}{2}$. We have the formula,

$$cos(\theta) = 4cos^3(\frac{\theta}{3}) - 3cos(\frac{\theta}{3})$$

At $\theta = 60$

$$4(\beta)^3 - 3\beta - \frac{1}{2} = 0$$

where $\beta = cos(\frac{\theta}{3})$ Then,

$$8(\beta)^3 - 6\beta - 1 = 0$$

$$(2\beta)^3 - 3(2\beta) - 1 = 0$$

Then $\alpha = 2\beta$ is a real number between 0 and 2 satisfying the equation

$$\alpha^3 - 3\alpha - 1 = 0$$

As in the case with doubling the cube, since

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

the construction is not possible.

4.3 Squaring the Circle

We shall now determine whether it is possible to construct a square of area π. Consider a circle of radius 1. Then its area is π. To construct a square of the same area would require the construction of a line segment of length $\sqrt{\pi}$, which is transcendental over $\mathbb{Q}$. Thus since $\mathbb{Q}(\sqrt{\pi})$ is not algebraic over $\mathbb{Q}$ the degree of $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is not a power of 2, and the construction is not possible.

4.4 Fundamental theorem of Algebra

The field $\mathbb{C}$ is Algebraically closed
Proof:
Let us first take a look at the 2 results that will be used in the proof:

1. There are no nontrivial finite extensions of $\mathbb{R}$ of odd degree.
2. There are no quadratic extensions of $\mathbb{C}$

Let L be a finite extension of $\mathbb{C}$. Since characteristic of $\mathbb{R}$ is 0, the field L is separable over $\mathbb{R}$, and L is also a finite extension of $\mathbb{R}$. Let N be the normal closure of $\frac{L}{\mathbb{R}}$. To prove the theorem we prove $N = \mathbb{C}$. Let $G = Gal(\frac{N}{\mathbb{R})]}$. Then

$$|G| = [N : \mathbb{R} = [N : \mathbb{C}] * [\mathbb{C} : \mathbb{R}] = 2[N : \mathbb{C}]$$

is even. Let H be 2-sylow subgroup of G, and let E be the fixed field of H. Then $|G : H| = |E : \mathbb{R}|$ is odd. Since the only odd extension of $\mathbb{R}$ is $\mathbb{R}$ itself, $G = H$ is a 2-group. Then Gal$(\frac{N}{C})$ is also a 2-group. Since 2-groups have subgroups of all orders dividing it, if this group is non trivial, there would exist a quadratic extension of $\mathbb{C}$ which is not possible since $\mathbb{C}$ has no quadratic extensions. Hence $N = C$.

5 References

- Galois theory - Richard Koch
- Abstract Algebra, Theory and Applications - Thomas W.Judson
- Symmetries of Equations: An introduction to Galois Theory- Brent Everitt
- Galois Theory and the Quintic Equation-Yunye Jiang
- Galois Theory and Application-Abdulla Eid