

A Journey in the Mind of Galois

John Impagliazzo

Department of Computer Science
Hofstra University
Hempstead, New York 11549-1030 USA
<cscjzi@Hofstra.edu>

*Dedicated to my friend and colleague, Robert Bumcrot,
on the occasion of his retirement from
Hofstra University, 2001 spring.*

Abstract

The fascination surrounding the solubility of polynomials has challenged mathematicians for centuries. Until Galois, the subject remained largely an open question. Through his insight, Galois used a novel approach to resolve the question. This expository article attempts to retrace Galois' thoughts and illustrates in a small way the birth of modern group theory. The discussion should prove useful to professionals, and especially to students, who may use it to spark further study of the work of Galois.

Background

The solubility (or non-solubility) of polynomials has wreaked havoc in the minds of mathematicians for centuries. For any polynomial P , with real coefficients and real variable x , the polynomial is soluble if the zeros of the polynomial are formally determinable. The solubility of the quadratic polynomial had its roots in early algebra. From the times of the Babylonians circa 1600 BC through the time of the Hindus and the Arabs circa 1200 AD, people have shown various methods analogous to completing the square to show that the quadratic is soluble. We have adopted that formalism and we now call the method the quadratic formula.

Regarding the cubic polynomial, Scipio del Ferro and his pupil Fior allegedly solved the problem in the early part of the sixteenth century [Ste89]. Soon after, Niccolo Fontana (Tartaglia) published a solution to the cubic in 1535. Gerolamo Cardano (Jerome Cardan) published (1542-45) his *Ars Magna*, where he showed the solubility of the cubic using Fontana's method. Consequently, we have come to know this as Cardan's formula. Cardan also included his *Ars Magna* a method to show the solubility of the quartic or fourth-degree polynomial, a method due to Ludovico Ferrari. François Vieta, with his novel use of literal symbols, demonstrated the solutions of Cardan and Tartaglia in the latter part of the sixteenth century. Although many mathematicians tried, no one was able to determine a solution to the quintic or fifth-degree polynomial.

By 1771, Joseph-Louis Lagrange had serious doubts about the solubility of the quintic and higher degree polynomials. He even introduced the n^{th} roots of unity, also called the "Lagrange resolvent," in an effort to show formally, but without success, the non-solubility of polynomials of degree greater than four. About the year 1813, Paolo Ruffini showed in various ways that

polynomials of degree greater than four were not soluble, but his approach was not convincing. In 1824, Niels Abel showed convincingly that the fifth-degree polynomial was not soluble. Although the works of Ruffini and Abel were sound, they had led mathematicians to believe that their results were just special cases of a more encompassing theory. It was not until 1831 that Ivariste Galois developed the theory of solubility for any polynomial.

Unfortunately, Galois was never able to document clearly his theories, due to lost manuscripts and his political embroilment at the time. On the eve of his now infamous duel, he had written some notes outlining the relationship between groups and polynomial equations. He died two days later from a gunshot wound on 31 May 1832 at the age of twenty. It would take other mathematicians a century to place into order the truth of Galois' hidden revelations.

We will now embark on a journey in an attempt to see how Galois may have woven his thoughts in the quest of resolving polynomial solubility. In his pursuit to do this, he laid the foundation for one of the more beautiful and profound theories in mathematics—the Galois theory of groups. What was Galois thinking about when he did this? What were his thoughts and processes? What had possessed him in his passion to resolve the relationship between polynomials and groups? Let's step back in time and see how this development might have happened.

Some Preliminaries

Let us begin by considering a general polynomial of the form

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \dots + a_n$$

where $a_i \in \mathcal{F}$ where \mathcal{F} is a field (such as the complex, real, or rational numbers). Let $u_1, u_2, u_3, \dots, u_n$ be the zeros of P . Then there is a unique factorization of P given by

$$P(x) = (x - u_1) (x - u_2) (x - u_3) \dots (x - u_n)$$

where some u_i may equal other u_j .

The Vieta formulas give the relationship between the zeros of P and the coefficients of P . By the latter part of the eighteenth century, A.T. Vandermonde, among others, also showed the relationships, which are:

$$\begin{aligned} -a_1 &= u_1 + u_2 + u_3 + \dots + u_n \\ a_2 &= u_1u_2 + u_1u_3 + \dots + u_1u_n + u_2u_3 + \dots + u_{n-1}u_n \\ -a_3 &= u_1u_2u_3 + u_1u_2u_4 + \dots + u_{n-2}u_{n-1}u_n \\ &\dots \\ \pm a_n &= u_1u_2u_3 \dots u_n \end{aligned}$$

A symmetric function (polynomial) in n letters is a polynomial that does not change under any permutation of these letters. For example, Vieta's formulas are symmetric in u_1 through u_n . As

another example, the polynomial $x^2 + y^2 + 4xy$ is symmetric in x and y . The “theorem of symmetric polynomials” states the following.

Let u_i be the zeros of polynomial P . Then every symmetric polynomial in u_1, u_2, u_3, \dots with arbitrary coefficients A, B, C, \dots can be expressed integral rationally (+, −, *) in terms of A, B, C, \dots and the u_i .

We will see how this theorem becomes the basis for Galois’ approach to resolving the solubility of polynomials and the birth of group theory.

Galois’ Thinking from Former Results

The ideas of symmetric polynomials with their permutation of letters and integral rationality must have toiled in Galois’ mind. The basic question—Under which conditions is an equation soluble by radicals?—remained open. Galois must have suspected there were links between solutions by radicals, symmetric polynomials, and eventually groups.

Let’s return to the generalized polynomials. This time, however, remove the possibility of multiplicity of roots and allow only rational coefficients. That is, consider

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n = 0$$

where $a_i \in Q$ (rational numbers) and where $u_1, u_2, u_3, \dots, u_n$ are the *distinct* roots of P . As did Lagrange, Galois must have considered a first-degree expression V in the linearly independent u_i whose coefficients A, B, C, \dots are rational integers. Such an expression would take the form

$$V = Au_1 + Bu_2 + Cu_3 + \dots$$

By permuting the roots u_i of P , Galois must have thought about obtaining the $n!$ equations from V . These are

$$\begin{aligned} V_1 &= Au_1 + Bu_2 + Cu_3 + \dots \\ V_2 &= Au_2 + Bu_1 + Cu_3 + \dots \\ &\dots \\ &\dots \\ V_{n!} &= Au_n + Bu_{n-1} + Cu_{n-2} + \dots \end{aligned}$$

From this, Galois must of thought of constructing a new polynomial P' of degree $n!$ such that the V_i were its roots. Then we could write

$$P'(x) = (x - V_1)(x - V_2)(x - V_3) \dots (x - V_{n!})$$

By the theorem of symmetric polynomials, P' is a polynomial in $V_1, V_2, V_3, \dots, V_{n!}$ with coefficients from Q .

Galois' Inventive Thinking

Galois must have been on to something when he created the $n!$ -degree polynomial P' and realizing it had to have rational coefficients. He introduces the idea of irreducible polynomials over a given field; that is, polynomials that cannot be written as the product of two polynomials of smaller degree. Using the field \mathcal{Q} , it must have become clear to Galois that one could factor P' into irreducible polynomials. Letting Φ_j be one of these factors of degree r (where r depends on j), we could write

$$\Phi_j(x) = (x - V_{j1})(x - V_{j2})(x - V_{j3}) \dots (x - V_{jr})$$

The n zeros ($u_1, u_2, u_3, \dots, u_n$) of the original polynomial P can be taken in any order and given indices $1, 2, 3, \dots, n$. Hence, each V_i corresponds to all possible $n!$ permutations of the numbers $1, 2, 3, \dots, n$. Therefore, the $V_{j1}, V_{j2}, V_{j3}, \dots, V_{jr}$ correspond to only r of these permutations. The set of these r permutations of the numbers $1, 2, 3, \dots, n$ forms a group. We will come to call this the Galois group.

A Theoretical Viewpoint

Consider again the zeros of polynomial $P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n = 0$, where $a_i \in \mathcal{Q}$ and where the distinct zeros of P are $u_1, u_2, u_3, \dots, u_n$. We call the set of all quantities obtained from arithmetic operations on the a_i the ground field, K , of P . We call the set of all quantities obtainable from a finite number of operations on the u_i the splitting field, F , of P .

Example

$$P(x) = x^2 + \sqrt{2}x + 1;$$

$$K = \{a + \sqrt{2}b : a, b \in \mathcal{Q}\};$$

$$F = \{a + ib + \sqrt{2}c + i\sqrt{2}d : a, b, c, d \in \mathcal{Q}, i = \sqrt{-1}\}$$

Notice that by Vieta's formulas, we can always obtain the coefficients a_i from the roots u_i . Therefore, $K \subseteq F$. Galois must have realized this, which made him consider the possibility of using groups and extension fields to address the problem.

The question remains, how can one make permutations on the roots of P ? In more modern terminology, we can permute the roots of P by defining a function g such that $g(u_i) = u_j$. Now, since $u_i, u_j \in F$ (the splitting field), we observe that $g: F \rightarrow F$. Furthermore, suppose g has the following additional properties:

$$g(u_i + u_j) = g(u_i) + g(u_j), \quad \forall u_i, u_j \in F \text{ (the splitting field)}$$

$$g(u_i u_j) = g(u_i) g(u_j), \quad \forall u_i, u_j \in F$$

$$g(c) = c, \quad \forall c \in K \text{ (the ground field).}$$

In this case, g would be an automorphism over F . First evaluate $P(u_i)$ as

$$P(u_i) = u_i^n + a_1 u_i^{n-1} + a_2 u_i^{n-2} + \dots + a_n$$

Applying g to P does the following.

$$\begin{aligned} g(P(u_i)) &= g(u_i^n + a_1 u_i^{n-1} + a_2 u_i^{n-2} + \dots + a_n) \\ &= g(u_i^n) + g(a_1 u_i^{n-1}) + g(a_2 u_i^{n-2}) + \dots + g(a_n) \\ &= (g(u_i))^n + g(a_1) (g(u_i))^{n-1} + g(a_2) (g(u_i))^{n-2} + \dots + g(a_n) \\ &= u_j^n + a_1 u_j^{n-1} + a_2 u_j^{n-2} + \dots + a_n \\ &= P(u_j) \\ &= P(g(u_i)) \end{aligned}$$

Therefore, g transforms (permutes) the zero u_i into the zero u_j for the polynomial P . From this, we can now make the following conclusions.

1. Each g effects a definite permutation on the u_i .
2. When we know the permutations, we know all the automorphisms. This is because we can obtain all elements of F from the u_i .
3. Instead of automorphisms, we can think of permutations.
4. Every permutation gives rise to an automorphism g in a splitting field F .
5. In general, the group G for the general n^{th} -degree polynomial is the symmetric group of n letters, S_n .
6. Since $|S_n| < \infty$, then $|G| < \infty$.

Obviously, we cannot be sure if Galois reasoned in this precise way. However, we can surmise that he must have had clues following this same thought pattern to arrive at similar conclusions.

Once we find the Galois group G of any polynomial function, we look for the next largest subgroup; that is, $G_1 < G$ such that G_1 is maximal. Having found G_1 from group theory and having computed the index of G_1 in G , $[G:G_1]$, we seek to find a function h of the roots whose coefficients belong to the ground field K . The function h is fixed by substitutions in G_1 . However, h can change under all other substitutions in G . Hence, an equation in K has h as a root. We call such an equation the partial resolvent and the degree of such an equation is $[G:G_1]$. Then, by adjoining h to K , we form a new field $K(h)$ and the group of the original equation with respect to $K(h)$ is G_1 .

By repeating the process of finding the next largest subgroup G_k , finding index $[G_{k-1}:G_k]$, finding the resolvent equation, solving for the h_i , and adjoining it to the new ground field $K(h_1, h_2, \dots)(h_i)$, we reach a point where the next largest subgroup is the identity group. The process stops and the fully adjoined field $K(h_1, h_2, h_3, \dots, h_n)$ is the splitting field F .

Galois must have calculated that when the resolvent which reduces G_i to G_{i+1} is a binomial equation of the form $x^p - a = 0$, where p is prime, then G_{i+1} is a normal subgroup of G_i ; that is, $G_{i+1} \triangleleft G_i$. Conversely, if $G_{i+1} \triangleleft G_i$ and $[G_i:G_{i+1}] = p$, a prime, then the resolvent is a binomial of degree p . Thus, we can solve an equation by radicals if and only if the successive resolvents are binomial equations.

The series of normal subgroups

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_q = \{e\}$$

forms a composition series. Galois most certainly should have realized that if such a series has all prime indices (i.e. $[G_{i-1}:G_i] = p$, a prime), then G is soluble. He would naturally conclude that an equation is soluble if and only if the group G is soluble. See the appendix for an example describing the relationship between field extensions and permutation groups for a soluble polynomial.

A Special Case when Degree $n = 5$

The polynomial $P(x)$ becomes

$$P(x) = x^5 + a_1x^4 + a_2x^3 + \dots + a_5 = 0$$

where $a_i \in Q$ and a_i are indeterminate. The polynomial

$$P'(x) = (x - V_1)(x - V_2)(x - V_3) \dots (x - V_5!)$$

is irreducible over Q . The degree of P' is $5! = 120$. The group G is S_5 . A composition series for G is

$$S_5 \triangleright A_5 \triangleright \{e\}$$

Then $[S_5:A_5] = 2$, a prime. However $[A_5:\{e\}] = 60$, *not* a prime. Hence, G is not soluble and therefore, the polynomial P is not soluble by radicals.

Conclusion

It is only fitting that we honor Galois by calling the group in the composition series

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_q = \{e\}.$$

the *Galois group*. After all, Galois is the one who brought light and depth to the subject of group theory. Mathematicians also owe Galois a debt of gratitude for his insights that brought closure to polynomial solubility after centuries of intellectual toil.

We can only conjecture what new ideas and theories might have occurred had Galois not died at such an early age of twenty and one-half years. His ill-fated and untimely death was a deep loss to the development and evolution of mathematics.

References

- [Kli72] Kline, Morris; *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.
- [Ste89] Stewart, Ian; *Galois Theory*, Second Edition, Chapman-Hall/CRC, 1989, 1998.
- [Ver51] Verriest, G.; *Oeuvres mathématiques d'Évariste Galois* (1897 ed), 2nd edition, Gauthier-Villars, 1951.

Appendix

How Field Extensions Relate to Permutation Groups: An Example

[The following discussion parallels the one posed by Verriest [Ver51] to explain the work of Galois.]

We begin by considering the polynomial $P(x) = x^4 + px^2 + q$ where $p, q \in \mathcal{Q}$ are arbitrary rational numbers. Let $P(x) = 0$ and let K be the ground field. Then $K = \{\text{all rational expressions in } p \text{ and } q\}$. In this case, the distinct zeros of P are

$$\begin{aligned} u_1 &= +\sqrt{(-p + \sqrt{[p^2 - 4q]})/2} & u_2 &= -\sqrt{(-p + \sqrt{[p^2 - 4q]})/2} \\ u_3 &= +\sqrt{(-p - \sqrt{[p^2 - 4q]})/2} & u_4 &= -\sqrt{(-p - \sqrt{[p^2 - 4q]})/2} \end{aligned}$$

With reference to the ground field K , it is true that

$$\begin{aligned} u_1 + u_2 &= 0 \\ u_3 + u_4 &= 0 \end{aligned} \tag{1}$$

Since $\deg(P) = 4$, there are $4! = 24$ possible permutations of the u_i , the zeros of P . However, only eight of them will keep the relationship (1) true in K . The eight permutations are:

$$\begin{aligned} \sigma_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} & \sigma_2 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix} & \sigma_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} & \sigma_4 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \\ \sigma_5 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} & \sigma_6 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} & \sigma_7 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix} & \sigma_8 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} \end{aligned}$$

where each number corresponds to the u_i for $1 \leq i \leq 4$. These are the transpositions in S_4 . Let $G_0 = \{\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_8\}$. G_0 is a group and is a subgroup of S_4 . That is, $S_4 > G_0$.

Now consider another relationship between the roots, namely,

$$u_1^2 - u_3^2 = \sqrt{[p^2 - 4q]} = \alpha \tag{2}$$

Clearly, $\alpha \notin K$. If we adjoin this radical α to K , we form the field $K(\alpha)$. Then relation (2) is a relation in $K(\alpha)$. In view of the differences in two squares, $u_1^2 = u_2^2$ since $u_1 + u_2 = 0$, and $u_3^2 = u_4^2$ since $u_3 + u_4 = 0$. This means that neither u_1 nor u_2 can go to u_3 or u_4 . Hence, of the eight permutations of zeros, only $\sigma_1, \sigma_2, \sigma_3$, and σ_4 will leave the relation (2) true in $K(\alpha)$. The collection $G_1 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ forms a group and is a subgroup of G_0 . Hence, $S_4 > G_0 > G_1$.

Now consider a third relation among the roots, namely,

$$(u_3 - u_4)/2 = \sqrt{[(-p - \alpha)/2]} = \beta \tag{3}$$

Clearly, $\beta \notin K$ and $\beta \notin K(\alpha)$. If we adjoin this radical β to $K(\alpha)$, we form the field $K(\alpha)(\beta) = K(\alpha, \beta)$. Relationship (3) will remain invariant only if $u_3 \rightarrow u_3$ and $u_4 \rightarrow u_4$. Hence, of the eight permutations in G_0 , only σ_1 and σ_2 will keep relation (3) invariant. The collection $G_2 = \{\sigma_1, \sigma_2\}$ forms a group and is a subgroup of G_1 . Hence, $S_4 > G_0 > G_1 > G_2$.

Only one other relation is possible among the roots u_i . It is $u_1 - u_2$. Hence,

$$(u_1 - u_2)/2 = \sqrt{[-p + \alpha]/2} = \gamma \quad (4)$$

Clearly, $\gamma \notin K$, $\gamma \notin K(\alpha)$, and $\gamma \notin K(\alpha, \beta)$. Hence, we must adjoin γ to $K(\alpha, \beta)$ to form $K(\alpha, \beta, \gamma)$. Only σ_1 , the identity, will keep relation (4) invariant in $K(\alpha, \beta, \gamma)$. Let $G_3 = \{\sigma_1\} = \{e\}$. Hence, we have $S_4 > G_0 > G_1 > G_2 > G_3$.

The series $S_4 > G_0 > G_1 > G_2 > G_3$ is such that $|S_4| = 24$, $|G_0| = 8$, $|G_1| = 4$, $|G_2| = 2$, and $|G_3| = 1$. From this we know that $[S_4:G_0] = 3$, $[G_0:G_1] = 2$, $[G_1:G_2] = 2$, and $[G_2:G_3] = 2$. Clearly, all indices $[G_i:G_{i+1}] = 2$, a prime, for $0 \leq i \leq 2$. Furthermore, each subgroup was generated from a resolvent that is a binomial of prime degree 2. Since this means that radicals generate each subgroup, the series

$$S_4 > G_0 > G_1 > G_2 > G_3 = \{e\}$$

is a subnormal series. Furthermore, since each normal subgroup is maximal, the series is the composition series

$$S_4 \triangleright G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 = \{e\}$$

where each index is a prime number. Therefore, the equation $P(x) = x^4 + px^2 + q$ is soluble by radicals, a fact we already knew.