Undergraduate Review

Volume 7 | Article 7

2011

Analyzing the Galois Groups of Fifth-Degree and Fourth-Degree Polynomials

Jesse Berglund

Analyzing the Galois Groups of Fifth-Degree and Fourth-Degree Polynomials

JESSE BERGLUND

Jesse is a senior mathematics major. This research was conducted over the summer of 2010 as an Adrian Tinsley Program Summer Grant project under the mentorship of Dr. Ward Heilman. Upon graduating Jesse plans to attend graduate school and continue research in mathematics.

It is known that the general equations of fourth-degree or lower are solvable by formula and general equations of fifth-degree or higher are not. To get an understanding of the differences between these two types of equations, Galois theory and Field theory will be applied. The Galois groups of field extensions will be analyzed, and give the solution to the query "What is the difference between unsolvable fifth-degree equations and fourth-degree equations?"

Introduction

Babylonian society (2000-600B.C.) was rapidly evolving and required massive records of supplies and distribution of goods. Computational methods were also needed for business transactions, agricultural projects, and the making of wills. It was because of these demands that the Babylonians created the most advanced mathematics of their time. It is their hard work and dedication that created the linear formula as a solution to the linear equation.

$$\text{Linear equation: } ax + b = 0 \qquad \text{Linear formula: } x = -\frac{b}{a}$$

The ancient Babylonians, classical Greeks, and especially Hindu mathematicians of the seventh century knew how to solve quadratic equations of various types. It was not until five hundred years later that a complete solution comes to fruition. The solution appeared in a book in Europe only during the twelfth century. The author of the book was the Spanish Jewish mathematician Abraham Bar Hiyya Ha-nasi (1070-1136). The book was called Treatise on Measurement and Calculation. Abraham Bar Hiyya states, "Who wishes correctly to learn the ways to measure areas and to divide them, must necessarily thoroughly understand the general theorems of geometry and arithmetic, on which the teaching of measurement...rests. If he has completely mastered these ideas he…can never deviate from the truth" (Livio). It was this arduous train of thought that had taken the quadratic equation and transformed it into the quadratic formula.

$$\text{Quadratic equation: } ax^2 + bx + c = 0$$

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

The early Babylonians were able to solve specific cubic equations using tables. A geometric solution that solved a few more was invented by the Persian poet-mathematician Omar Khayyam during the twelfth century. Nevertheless, mathematicians were unable to break the code for the general cubic equation until the sixteenth century. In Italy during the 1500s, mathematical tournaments were a popular pastime. The people involved kept their methods secret. Niccolo of Brescia (1500-1557), commonly referred to as Tartagalia ("the stammerer"), owned the secret to the cubic equation. This gave him a distinct advantage in the tournaments. Girolamo Cardano (1501-1576) had discovered that Tartagalia had the secret, and asked him for the solution. Tartagalia refused to give him the solution for some time. Eventually Tartagalia reluctantly gave Cardano the solution, but swore him to secrecy. The solution was published in Cardano's work Ars Magna (1545) breaking his word which started a feud between the two mathematicians. After four hundred years the solution to the general cubic equation had come to light. Further contributions from Scipione del Ferro would lead to the complete cubic formula. The procedure for the extraction of the cubic solution is quite different than that of its smaller brethren. Without loss of generality, let a_0 of the general cubic equation

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0$$

equal one. Now, with the equation

$$x^3 + ax^2 + bx + c = 0$$

it is necessary to eliminate the x^2 term. To do this, substitute

$$x = z - \frac{a}{3}$$

into the equation. Executing this will yield

$$z^3 + pz + q = 0$$

$$\text{where } p = \frac{3b - a^2}{3} \text{ (1) and } q = \frac{2a^3 - 9ab + 27c}{27} \text{ (2)}$$

Next observe that if we substitute

$$z = u + v \text{ and } p = -3uv$$

into the expression, it produces

$$u^3 + v^3 + q = 0$$

From this point we get

$$v = -\frac{p}{3u}$$

to obtain

$$u^3 - \frac{p^3}{27u^3} + q = 0 .$$

Multiplying both sides by u^3 gives

$$u^6 + qu^3 - \frac{p^3}{27} = 0 ,$$

which is a quadratic equation for u^3. Completing the square and solving for u generates

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \text{ (3)} .$$

Amalgamating

$$x = z - \frac{a}{3},\ z = u + v \text{ and } v = -\frac{p}{3u}$$

solving for x we obtain

$$x = u - \frac{p}{3u} - \frac{a}{3} \text{ (4)} .$$

With equation one, two, three, and four in hand the complete cubic formula is realized.

Cubic Formula

$$p = \frac{3b - a^2}{3} \quad q = \frac{2a^3 - 9ab + 27c}{27} \quad u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$x = u - \frac{p}{3u} - \frac{a}{3}$$

Shortly after the contributions of the cubic formula by Del Ferro, Tartagalia, and Cardano; Ferrari, who was a student of Cardano, found the solutions to the general quartic equation. The quartic is even more complicated than the cubic, requiring more substitution and algebraic manipulation. Without loss of generality, let the leading coefficient be equal to one. With the equation

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

the x^3 must be eliminated. Letting $x = z - \frac{a}{4}$ in the expression produces

$$z^4 + pz^2 + qz + r = 0$$

where $p = \frac{8b - 3a^2}{8}$, $q = \frac{a^3 - 4ab + 8c}{8}$, and $r = \frac{16a^2b - 3a^4 - 64ac + 256d}{256}$.

For the next step add 2 pz^2 and p^2 to both sides completing the square to get

$$z^4 + 2pz^2 + p^2 + qz + r = pz^2 + p^2.$$

Factor $z^4 + 2pz^2 + p^2$ to obtain $(z^2 + p)^2 + qz + r = pz^2 + p^2$.
Add $2y(z^2 + p) + y^2$ to both sides of

$$(z^2 + p)^2 + qz + r = pz^2 = p^2$$

to get

$$(z^2 + p)^2 + 2y(z^2 + p)q + y^2 + qz + r = pz^2 + p^2 + 2y(z^2 + p) + y^2,$$

which simplifies to

$$(z^2 + p + y)^2 = (p + 2y)z^2 - qz + (y^2 + 2yp + p^2 - r).$$

We must now consider the discriminant

$$(-q^2) - 4(p + 2y)(y^2 + 2yp + p^2 - r)$$

– an expression which gives information about the polynomials roots – of the quadratic equation and because it is a perfect square it is equal to zero. Simplifying this expression gives the resolvent cubic – a quartic equation that has been algebraically broken down to a cubic – which is

$$y^3 + \frac{5}{2}py^2 + \left(2p^2 - r\right)y + \left(\frac{p^3}{2} - \frac{pr}{2} - \frac{q^2}{8}\right) = 0 .$$

This is a cubic which can be solved for by using the previous method. We are left with the quartic formula.

$$p = \frac{8b - 3a^2}{8} \qquad q = \frac{a^3 - 4ab + 8c}{8}$$

$$r = \frac{16a^2b - 3a^4 - 64ac + 256d}{256}$$

$$u = \sqrt[3]{-\frac{k}{2} \pm \sqrt{\frac{k^2}{4} + \frac{h^3}{27}}} \qquad y = u - \frac{h}{3u} - \frac{5}{6}p$$

$$h = \frac{-p^2 - 12r}{12} \qquad k = \frac{72pr - 2p^3 - 27q^2}{216}$$

$$x = -\frac{a}{4} + \frac{\pm\sqrt{p + 2y} \pm \sqrt{-\left(3p + 2y \pm \frac{2q}{\sqrt{p + 2y}}\right)}}{2}$$

The formulas involved in all of these general equations were solved using the four arithmetic operations and the extraction of roots. Paolo Ruffini (1765-1822) claimed to have proof that the general quintic equation could not be solved by these methods. Unfortunately, there was a critical gap in his proof. Not long after the failed proof by Ruffini, the mathematician Niels Henrik Abel (1802-1829) worked on the general quintic and tried to solve it with great vigor, but he could not. Even after his ineffective attempt to solve the quintic by formula, this subject did not leave Abel's relentless mind. After only a few months of vigorous work, the twenty-one year old Abel had solved this century old problem. He proved what is now called, "Abels Impossibility Theorem". This theorem shows that it is impossible to solve general polynomials of fifth-degree of higher, using the four arithmetic operations and the extraction of roots.

Not long after Abel's Theorem became known, Evariste Galois (1811-1832) would create a new branch of algebra known as Galois Theory. He would make a connection between the putative solutions and the permutations of these solutions. Galois was able to find the "key" of an equation – the Galois group of the equation – and determine from its properties whether it was solvable by formula or not.

Definitions:
To continue any further we will need some definitions to help clarify the following statements.

abelian A group, $(G,\circledast)$, is abelian (also known as commutative) if and only if $a \circledast b = b \circledast a$, for all elements $a,b \in G$.

automorphism A one-to-one correspondence mapping the elements of a set onto itself, so the domain and range of the function are the same. For example, $f(x) = x + 2$ is an automorphism on $\mathbb{R}$ but $g(x) = \cos x$ is not.

compostion series Given a group G, a sequence of groups $G_0,\ldots,G_r$, is called a composition series for G if

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \cdots G_{n-1} \lhd G_n = G,$$

where G_1 has no proper normal subgroup. The groups G_i / G_{i-1} are called quotient groups of G, their number n is the length of the series, and the integers $|G_i / G_{i-1}|$ are the quotient groups' orders.

Eisenstein irreducibility criterion Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where the coefficients are all integers. If there exists a prime p such that: (i) p divides each of $a_0, a_1, \ldots, a_{n-1}$; (ii) p does not divide a_n; and (iii) p^2 does not divide a_0; then f is irreducible over $\mathbb{Q}$.

Galois group The Galois group of a polynomial is the set of permutations on the solutions of that polynomial. So, to get a better idea of what a Galois group is, let's look at how Galois perceived it. As an example take $f(x) = x^2 - 2 = 0$. The solutions are $\alpha = \sqrt{2}$ and $\beta = -\sqrt{2}$.

The set of permutations on two objects includes the identity where α and β get mapped to themselves denoted by

$$1 : \alpha \mapsto \alpha \quad \beta \mapsto \beta$$

and where α and β get mapped to each other signified by

$$\sigma : \alpha \mapsto \beta \quad \beta \mapsto \alpha \quad .$$

These form the set of all automorphism's of 2 elements. This can be called the Galois group S_2.

general polynomial function An expression of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_n, a_{n-1},\ldots,a_1, a_0$ are rational numbers $(a_n \neq 0)$ and n is a nonnegative integer.

group A group is a nonempty set G together with a binary operation $*$ on the elements of G such that:

1) G is closed under $*$.

2) $*$ is associative.

3) G contains an identity element for $*$.

4) Each element in G has an inverse in G under $*$.

Examples of groups:

Addition mod n groups - Z_n where $n \in \mathbb{N}$

Alternating group - A_n where $n \in \mathbb{N}$

Dihedral group – D_4 where $n \in \mathbb{N}$

Klein four group - V

Symmetric group - S_n where $n \in \mathbb{N}$

identity A group that only contains the identity element.

identity element An element that is combined with another element with a particular binary operation that yields that element. Let $(G,*)$ be a group and $e, a \in G$. If $e * a = a$ the e is the identity.

homomorphism Let $(G,*)$ and $(H,\circ)$ be two groups. Let f be a function from G to H. f is a homomorphism (an operation preserving function) from $(G,*)$ to $(H,\circ)$ if and only if for every pair of elements, $a,b \in G$, $f(a*b) = f(a) \circ f(b)$.

irreducible polynomial The polynomial $x^2 - 5$ is irreducible over $\mathbb{Q}$. The roots of the polynomial are $\sqrt{5}$ and $-\sqrt{5}$.

These values are not within the field $\mathbb{Q}$. Therefore, the polynomial cannot be reduced to a factored form with values from the field $\mathbb{Q}$, but can be with the field $\mathbb{Q}(\sqrt{5})$.

isomorphic Two groups are said to be isomorphic (meaning they have the same structure and properties) if and only if there exists a 1-1, onto, homomorphism.

normal subgroup A subgroup H is normal in a group $(G,*)$ if and only if

$$\forall g \in G,\ g * H = H * g$$

denoted $H \lhd G$.

permutation A permutation is an arrangement or rearrangement of n objects. The number of permutations of n objects is $n!$.

quotient group If $H \lhd G$ then $G \mid H$ is the set of distinct cosets xH, where $x,y,\ldots$ range over G and we define an operation $*$ as follows: $(xH) * (yH) = (xyH)$. With this operation, $G \mid H$ is a group called the *factor* or *quotient group* of G by H.

rational number A number that can be written in the form $\frac{a}{b}$, where a and b are integers, with $b \neq 0$.

Rational Zeros Theorem Let f be a polynomial function of degree 1 or higher of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_n \neq 0, a_0 \neq 0$$

where each coefficient is an integer. If $\frac{p}{q}$, in lowest terms, is a rational zero of f, then p must be a factor of a_0, and q must be a factor of a_n.

reducible polynomial The polynomial x^2 -4 is reducible over $\mathbb{Q}$. The roots of the polynomial are 2 and -2. These values are within the field $\mathbb{Q}$. Therefore, the polynomial can be reduced to a factored form with the values from the field $\mathbb{Q}$.

Rolle's Theorem Let f be continuous on the closed interval $[a,b]$ and differentiable on the open interval (a,b). If $f(a) = f(b)$ then there is at least one number c in (a,b) such that $f'(c) = 0$.

splitting field If K is a subfield of C and f is a polynomial over K, then f splits over K if it can be expressed as a product of linear factors

$$f(t) = k(x-\alpha_1)\cdots(x-\alpha_n)$$

$$\text{where } k, \alpha_1, ..., \alpha_n \in K.$$

subgroup Let $(G,\circledast)$ be a group. If H is a subgroup of G then $H \subseteq G$ and H is a group under $\circledast$.

symbols

$\mathbb{C}$ - the complex numbers $\{a+bi \mid a,b \in \mathbb{R}\}$

$\mathbb{N}$ - the natural numbers $\{1,2,3,\ldots\}$

$\mathbb{Q}$ - the rational numbers $\left\{\frac{a}{b} \middle| a,b \in \mathbb{Z} \text{ and } b \neq 0\right\}$

Δ- the discriminant

symmetric group For any set X, a permutation of X is a one-to-one onto mapping from X to X. If X has n elements there are n! permutations of x and the set of all these, with composition of mappings as the operation, forms a group called the symmetric group of degree n, denoted by S_n.

trivial group A group that only contains the identity element.

What to do?

To find out what the difference is between fifth-degree and fourth-degree polynomials, there is some work to do. First, collect all the possible Galois groups of linear polynomials up to and including quartic polynomials. Next, find a quintic which is unsolvable by radicals and calculate its Galois group. Analyze both sets of groups using Group theory and compare their results.

Case 1:

Polynomials in $\mathbb{Q}$ with all solutions in $\mathbb{Q}$ have the Galois group S_1.

Let's look at $f(x) = x - 1$ and $f(x) = x^2 + 3x + 2$. Both have coefficients and solutions that lie in $\mathbb{Q}$. When these conditions are met the only possible permutation on the rational numbers is the identity. Therefore, the Galois group for these types of polynomials is the trivial group S_1.

Case 2:

A quadratic polynomial that is irreducible in $\mathbb{Q}$, has the Galois group S_2.

As an example, take the polynomial equation $f(x) = x_2 + 1 = 0$. This is irreducible in the rationals, and is of degree two. Since the splitting field is $\mathbb{Q}(i)$, there are two $\mathbb{Q}$-automorphisms defined by

$$1:\ i \mapsto i \quad -i \mapsto -i$$

$$\sigma:\ i \mapsto -i \quad -i \mapsto i$$

Notice that if the roots are irrational, we have the same Galois group. Let's examine $f(x) = x^2 - 3$. This is also irreducible in the rationals, and is of degree two. The splitting field is $\mathbb{Q}\left(\sqrt{3}\right)$, therefore, it has two $\mathbb{Q}$-automorphisms denoted by

$$1:\ \sqrt{3} \mapsto \sqrt{3} \quad -\sqrt{3} \mapsto -\sqrt{3}$$

$$\sigma:\ \sqrt{3} \mapsto -\sqrt{3} \quad -\sqrt{3} \mapsto \sqrt{3} \quad .$$

For that reason, the Galois group for both of these polynomials is S_2.

Case 3:

A cubic polynomial that is irreducible in $\mathbb{Q}$, has the Galois group S_3 or A_3.

Proposition: *Let*

$$f(x) = x^3 - ax^2 + bx - c \in \mathbb{Q}(x)$$

be irreducible over $\mathbb{Q}$. *Then its Galois group Is* A_3 *if the discriminant of,*

$$f\Delta = a^2b^2 + 18abc - 27c^2 - 4a^3c - 4b^3$$

is a perfect square in $\mathbb{Q}$, *and is* S_3 *otherwise.*

Let's take into account $f(x) = x^3 - 2$. This is irreducible by *Eisenstein's Criterion* and has the discriminant $\Delta = -108$, which is not a square. Hence, its Galois group is S_3. Another example is $f(x) = x^3 - 3x - 1$. This is irreducible by the *Rational Zeros Theory* and its discriminant is $\Delta = -81$, which is a square. Consequently, its Galois group is A_3.

Case 4:

A quartic polynomial that is irreducible in $\mathbb{Q}$, *has the Galois group* S_4, A_4, D_4, V, or Z_4. This chart will help to attain the group of a particular quartic.

Δ of f *in* $\mathbb{Q}$		Resolvent cubic *in* $\mathbb{Q}[x]$		Galois Group
$\neq \square$	+	*irreducible*	$\rightarrow$	S_4
$= \square$	+	*irreducible*	$\rightarrow$	A_4
$\neq \square$	+	*reducible*	$\rightarrow$	D_4 *or* Z_4
$= \square$	+	*reducible*	$\rightarrow$	V

To achieve these values, the discriminant of f is used along with the resolvent cubic of f. With this machinery, the groups of these quartics are realized. Consider the examples where Δ of

$$f(x) = x^4 + cx + d \text{ is } \Delta = -27c^4 + 256d^3$$

and the cubic resolvent of f is

$$R_3(x) = x^3 - 4dx - c^2.$$

$f(x)$	Δ of f	Resolvent cubic of f	Galois group
$x^4 + 2x + 2$	$101 \cdot 4^2$	$x^3 - 8x - 4$	S_4
$x^4 + 8x + 12$	576^2	$x^3 - 48x - 64$	A_4
$x^4 + 3x + 3$	$21 \cdot 15^2$	$(x+3)(x^2 - 3x - 3)$	D_4 *or* Z_4
$x^4 + 36x + 63$	4320^2	$(x-18)(x+6)(x+12)$	V

As a result, there are only five Galois groups that occur for any irreducible quartic.

Case 5:

Let p be a prime, and let f be an irreducible polynomial of degree p over $\mathbb{Q}$. *Suppose that f has precisely two nonreal zeros in* $\mathbb{C}$. *Then the Galois group of f over* $\mathbb{Q}$ *is isomorphic to the symmetric group* S_p.

Take the example $f(x) = x^5 - 4x + 2$. By *Eisenstein's Criterion f* is irreducible over the rationals. By *Rolle's Theorem* the zeros of f are separated by the zeros of the derivative of f. Since $5x^4 - 4$ has zeros at $\pm\sqrt{4/5}$, f has three real zeros each with multiplicity one, and as a consequence has two complex zeros. Also, f has degree five. Thus, the Galois group is isomorphic to S_5.

From the linear to the quartic

Now, let's take a look at the first four cases. In each case for the Galois groups that occur, there is a series of normal subgroups whose quotient groups are abelian.

Case 1:

$$1$$

$$1 \lhd 1 \text{ and } 1/1 = 1$$

Case 2:

$$S_2$$

$$1 \lhd S_2 \text{ and } S_2/1 = S_2$$

Case 3:

$$S_3 \text{ or } A_3$$

$$1 \lhd A_3 \lhd S_3,\ S_3/A_3 = Z_2, \text{ and } A_3/1 = A_3$$

Case 4:

$$S_4,\ A_4,\ D_4,\ V, \text{ or } Z_4$$

$$1 \lhd V \lhd A_4 \lhd S_4,\ S_4/A_4 = Z_2,\ A_4/V = Z_3, \text{ and } V/1 = V$$

$$1 \lhd V \lhd D_4 \text{ or } 1 \lhd Z_4 \lhd D_4, \text{ and } D_4/Z_4 = D_4/V = Z_2$$

The unsolvable quintic

Looking at the Galois group for the unsolvable quintic, there is a discrepancy when compared to the properties of the previous cases. All polynomials of fourth-degree or below have a series of normal subgroups in which their quotient groups are abelian.

Case 5:

$$S_5$$

$$1 \lhd A_5 \lhd S_5,\ S_5 / A_5 = Z_2$$

but $A_5 / 1 = A_5$ which is

not abelian

The unsolvable quintic does not have a series of normal subgroups in which all the quotient groups are abelian. This demonstrates the difference between an unsolvable quintic and equations of fourth-degree or lower. Therefore, a polynomial is solvable by radicals if it has a Galois group with a composition series containing quotient groups that are abelian.

References

Artin, Emil. *Galois Theory*. 3rd edition. Ed. Arthur N. Milgram. New York: Dover Publicatons, Inc., 1998.

Gaal, Lisl. *Classical Galois Theory*. 5th edition. Providence, Rhode Island: AMS Chelsea Publishing, 1988.

Gallian, Joseph A. *Contemporary Abstract Algebra*. 7th edition. Belmont, CA: Brooks/Cole Cengage Learning, 2010.

Garling, D.J.H. *A Course in Galois Theory*. 5th edition. New York: Cambridge University Press, 1995.

Hadlock, Charles R. *Field Theory and its Classical Problems*. Washington, DC: The Mathematical Association of America, 1978.

Herstein, I.N. *Abstract Algebra*. 3rd edition. Hoboken, NJ: John Wiley & Sons, Inc., 1999.

Jacobson, Nathan. *Basic Algebra I*. 2nd edition. New York: W.H. Freeman & Company, 1985.

Livio, Mario. *The Equation That Couldn't Be Solved*. New York: Simon & Schuster Paperbacks, 2005.

Stewart, Ian. *Galois Theory*. 3rd edition. New York: Chapman & Hall/ CRC Mathematics, 2004.

Tignol, Jean-Pierre. *Galois' Theory of Algebraic Equations*. 3rd edition. Toh Tuck Link, Singapore: World Scientific Publishing, 2001.

Conrad, Keith. Galois Groups of Cubic's and Quartic's (Not in Characteristic 2). *Expository papers*. 10 July. 2010 <http://www.math.uconn.edu/~kconrad/blurbs/