Galois Theory

Jacob Denson

January 18, 2016

Table Of Contents

Chapter 1

Quadratics, Cubics, and Quintics

> This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.
>
> Hermann Weyl (On Galois' theory)

The basic problem of Galois theory is to understand the structure of polynomials, in relation to the fields in which they are defined. In particular, the theory was invented as a tool to understand why the roots of some polynomials are difficult to solve, and how to find roots to polynomials in the easier cases.

Let us first consider the roots x of an arbitrary quadratic polynomial expression $X^2 + BX + C$. That is, the values of x such that

$$x^2 + Bx = -C \tag{1.1}$$

Considering any particular x, we let $y = x + B/2$, obtaining that

$$y^2 = \left(y - \frac{B}{2}\right)^2 + B\left(y - \frac{B}{2}\right) + \frac{B^2}{4} = x^2 + Bx + \frac{B^2}{4} = \frac{B^2}{4} - C$$

The polynomials $P = Y^2 - (C - B^2/4)$ and $Q = X^2 + BX + C$ are equivalent, in the sense that x is a root for Q if and only if the corresponding y is a root for P. Hence x satisfies the equation

$$x = -\frac{B}{2} \pm \sqrt{\frac{B^2}{4} - C} = \frac{-B \pm \sqrt{B^2 - 4C}}{2}$$

And by brute force, one verifies that every solution to the equation above is a root of the formula.

First, note that the method of solving quadratics above determines the geometric structure of quadratic polynomials[1]. Our calculation shows that every quadratic polynomial with real coefficients can be graphed in the plane as a parabola: completing the square corresponds to choosing a coordinate system where the graph is a convex parabola whose node rests at the origin. Thus solving polynomials corresponds to understanding the structure of geometric shapes. We shall see that Galois theory also has applications to an understanding of some varieties of geometry.

Second, we see that the quadratic formula is expressed using five basic operations: addition, subtraction, multiplication, division, and taking radicals ('powers of $1/n$') – we say that all quadratic polynomials are 'solvable in radicals'. In more precise terms, the aim of Galois theory is to determine which polynomials are solvable in radicals – the earliest deep result being that it is impossible to find a general formula for the roots of polynomials of degree five or higher. Galois theory has many applications to other areas of mathematics, since a great many problems may be reduced to finding the solution of some polynomial over a field.

1.1 The Cubic Formula

We shall begin our journey to the insolvability of the quintic by deriving the solutions of the cubic. Consider an arbitrary cubic $X^3 + BX^2 + CX + D$. Substitute $X = Y - \frac{B}{3}$ (geometrically, shift the graph of the polynomial to the right by $B/3$ units). We obtain the polynomial

$$\begin{aligned}\left(Y - \frac{B}{3}\right)^3 + B\left(Y - \frac{B}{3}\right)^2 + C\left(Y - \frac{B}{3}\right) + D \\ = Y^3 + Y\left(C - \frac{B^2}{3}\right) + \left(\frac{4B^3}{27} - \frac{CB}{3} + D\right)\end{aligned}$$

we have moved the polynomial so the point of inflection lies at the origin, hence the quadratic coefficient vanishes. By the equivalence of roots, it follows that we need only analyze cubics of the form $X^3 - 3PX - 2Q$. If

[1] the quadratic 'formula' was known to the Babylonians and Greeks only in this geometric form

$P = 0$, then we have a 'degenerate' polynomial $X^3 - 2Q$, which is a just the canonical cubic expression shifted down by $2Q$ units, and its zeroes can be easily solved. Otherwise, make the substitution $X = Y + Z$, obtaining the multivariate polynomial

$$(Y+Z)^3 - 3P(Y+Z) - 2Q = Y^3 + Z^3 + 3YZ(Y+Z) - 3P(Y+Z) - 2Q$$

Provided that y is an instance of Y, and z of Z, such that $yz = P$ and $y^3 + z^3 = 2Q$, then $y + z$ solves the cubic equation. Letting $z = P/y$ in this formula, we find that

$$y^3 + P^3/y^3 = 2Q$$

So we must find the roots of the equation $Y^6 + P^3 = 2QY^3$, which is a quadratic equation in Y^3 known as the *cubic resolvent*, and we know how to solve quadratic polynomials. It only remains to be seen that all solutions can be described in the form $Y + Z$ for Y and Z satisfying the constraints above, and we shall not discuss this in detail, since it requires a rather vast calculation.

Cubic equation occupied a vast amount of mathematical effort, from the medieval ages to the rennaissance. Challenges and contests were used to test an algebraists aptitude. Early in the 16th century, Scipio del Ferro found a solution to cubics of the form $X^3 + BX = C$, where B and C are positive[2], who used it to great success in contests (without sharing the solution). Ferro told the solution to his student Florido, who challenged the mathematician Niccoló Tartaglia. In preparation, Tartaglia found the general solution to the cubic, and with it, beat Florido. Tartaglia also wanted to keep the solution secret, so he could stay competitive, but the solution was revealed after an exchange with Girolamo Cardano, who published it in his book, the Ars Magna, in 1545. Without complex and positive numbers, the solution requires a total of thirteen cases. The book also included a solution to the quartic equation (a degree four polynomial), using methods of Lodovico Ferrari. We shall not discuss his method here, since the formulas are inconvenient (to say the least), but as with the method of the cubic, Ferrari's method results from reducing quartic polynomials to simpler and simpler forms, until we can reduce the problem to solutions of the cubic.

Thus, after almost 2000 years of work, the problem of polynomial roots had begun to crack. It was hoped, after a century of success, that one

[2]Negative numbers were not regarded as rigorous tools at the time

could expand the technique to quintic equations, and to general polynomials of arbitrary degree. From the 16th century to the 18th, mathematicians as prominent as Euler and Lagrange attempted to crack the equation, to little success. Lagrange attempted to generalize existing techniques, and showed that they had no such extension to the quintic formula. He was the first to come to believe that there may be no solution. In 1813, Paolo Ruffini provided the impossibility proof. Nonetheless, the proof was messy, and had multiple gaps in rigour. By 1827, the gaps in the proof had been filled by Henrik Abel. However, in 1832, Everiste Galois found a much more elegant approach to insolvability. His scheme has been generalized to what is now known as Galois theory – the insolvability of the quintic reduces to the unsolvability of a certain group. The gist of this approach is as follows, executed on a particular equation.

Consider a polynomial equation $P = X^4 - 4X^2 - 5$, viewed as a rational polynomial, which can be factored as

$$P = (X^2 + 1)(X^2 - 5)$$

The rational numbers may be extended to the complex numbers, which, by the fundamental theorem of arithmetic, splits P into linear factors,

$$P = (X - i)(X + i)(X - \sqrt{5})(X + \sqrt{5})$$

In fact, we do not even need all of the complex numbers, for we may consider a subfield $\mathbf{K}$, which is the smallest subfield to contain i, $-i$, $\sqrt{5}$, and $-\sqrt{5}$. If we abstractly denote i by α, $-i$ by β, δ by $\sqrt{5}$, and γ for $-\sqrt{5}$, (for we will not know their exact values for general polynomials). In general, we shall denote a field by $\mathbf{Q}(\alpha, \beta, \gamma, \lambda)$.

Now each abstract (polynomial) expression in $\mathbf{K}$ represents an actual value of $\mathbf{K}$, by evaluation. By the properties of α, β, γ, and λ, some expressions shall be naturally equivalent. For instance

$$\alpha + \beta = 0 \qquad \delta\gamma = -5 \qquad \alpha\beta = 1$$

Some such expressions remain to be true under permutations of the variables. In fact, there are some permutations which maintain the truth of all such expressions. As an example, the permutation $(\alpha\beta)$, swapping α and β, or $(\delta\gamma)$, swapping δ and γ, maintains the truth of all formulae. The set of permutations which preserve the truth of expressions forms a group,

known as the Galois group $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$. In our particular case, the galois group can be shown to be $G = \{e, (\alpha\beta), (\delta\gamma), (\alpha\beta)(\delta\gamma)\}$.

Assume that we have no knowledge of the zeroes of a polynomial Q, but we have determined that it has four distinct zeroes $\alpha, \beta, \gamma, \lambda$ in $\mathbf{C}$, and that $\mathbf{Q}[\alpha, \beta, \lambda, \gamma]$ has the same Galois group G as P. Consider $\mathbf{Q}[\lambda, \gamma]$, defined analogously to $\mathbf{Q}[\alpha, \beta, \lambda, \gamma]$, so that

$$\mathbf{Q} \subset \mathbf{Q}[\lambda, \gamma] \subset \mathbf{Q}[\alpha, \beta, \lambda, \gamma]$$

Assume that $H = \{e, (\alpha\beta)\}$ is the galois group of $\mathbf{Q}[\lambda, \gamma]$. Also, assume that H only fixes elements of $\mathbf{Q}[\lambda, \gamma]$, and G only fixes rational numbers. We may find a radical solution to Q as follows: $\alpha\beta$ and $\alpha + \beta$ are both fixed by H, so that $\alpha\beta$ and $\alpha + \beta$ can both be expressed as expressions in $\mathbf{Q}[\lambda, \gamma]$. Since the polynomial $(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$ has coefficents in $\mathbf{Q}[\lambda, \gamma]$, so that α and β can be expressed as a radical expressions in λ and γ. But we may apply the same trick for λ and γ, since $\lambda\gamma$ and $\lambda + \gamma$ are fixed by the whole of G, so that λ and γ are expressed as radical expressions in $\mathbf{Q}$. Therefore, we may also express α and β as radical expressions in $\mathbf{Q}$.

What we see above is the importance of the Galois group sat work. In turns out that the reason the quintic cannot be solved by a formula is that there are certain quintic formulas which have the wrong type of Galois group. But how can we determine the structure of the galois group without knowing the roots? We shall find that a detailed study of field extensions will reveal this to us, and the elegance of results is only improved not only by analyzing $\mathbf{Q}$, but also arbitrary fields, as was introduced by Emil Artin in the 20th century.

Chapter 2

Fields, and their Extensions

The primary numbers systems that we wish to study are the fields $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$, as well as the finite fields $\mathbf{F}_p$, which are the integers modulo a prime. Nonetheless, we must consider more general number systems obtained by adding additional 'numbers' into the systems, so it is useful to define exactly what we mean by a 'number system'.

Definition. A **field** is a commutative ring in which every non-zero element is invertible. That is, in a field we have two distinguished elements 0 and 1, as well as operations of addition and multiplication, which are both associative, commutative and distributive, and satisfy, for all field elements x,

$$0 + x = x + 0 = x \qquad 1 \cdot x = x \cdot 1 = x$$

We are to understand fields by embedding them in higher dimensional systems, so it is worth it to note which fields are contained in the field we are working with.

Definition. The **prime field** in a field $\mathbf{F}$ is the smallest subfield. The **prime ring** is the smallest ring.

Lemma 2.1. *The prime field of any field* $\mathbf{F}$ *is isomorphic either to* $\mathbf{Q}$ *or* $\mathbf{F}_p$*, where* p *is prime. In the first case, the prime ring is* $\mathbf{Z}$*, and in the first, it is* $\mathbf{F}_p$*.*

Proof. Consider the map $f : \mathbf{Z} \to \mathbf{F}$ defined by

$$f(0) = 0 \qquad f(n+1) = f(n) + 1 \qquad f(-n) = -f(n)$$

Then this is verified by induction to be a ring homomorphism. The kernel of this map is an ideal, and since $\mathbf{Z}$ is a principal ideal domain may be written as (p). This must be a prime ideal, since $\mathbf{F}$ is an integral domain. If $p \neq 0$, then (p) is a maximal ideal, then by the first isomorphism theorem $\mathbf{Z}/(p) = \mathbf{F}_p \cong f(\mathbf{Z})$. Thus $f(\mathbf{Z})$ is a field, and any other subfield of $\mathbf{F}$ must contain it, so it is the prime field of $\mathbf{F}$. If $p = 0$, then f is an injective function, and we may extend f to $\mathbf{Q}$ by defining

$$f\left(\frac{m}{n}\right) = f(m)f(n)^{-1}$$

(which is well defined exactly because $f(n) \neq 0$). The extension is also injective, for if $f(m)f(n)^{-1} = f(p)f(q)^{-1}$, then $f(mq) = f(pn)$, so $mq = pn$, hence $m/n = p/q$. Thus $\mathbf{Q} \cong f(\mathbf{Q})$. As we have seen, every field must contain $f(\mathbf{Z})$, but then it must also contain $f(\mathbf{Q})$, for a field must be closed under inverses. Hence $f(\mathbf{Q})$ is the prime subfield. □

This shows that the most interesting fields to extend are the rational and prime fields, since any other field may be obtained by extension. If the prime field of a field $\mathbf{F}$ is isomorphic to $\mathbf{F}_p$, we shall say $\mathbf{F}$ has **characteristic** p. If the prime field is $\mathbf{Q}$ instead, then we shall say $\mathbf{F}$ has **characteristic** 0.

To introduce some further notation, if $\mathbf{F} \subset \mathbf{E}$ are fields, we rewrite this relationship as $\mathbf{E}/\mathbf{F}$ (read '$\mathbf{E}$ over $\mathbf{F}$'), and say $\mathbf{E}$ **extends** $\mathbf{F}$. Artin's most notable contribution to the foundations of Galois theory was that we may view $\mathbf{E}$ as an algebra over $\mathbf{F}$, and therefore use techniques of linear algebra to understand the extension. For instance, we may talk of independent bases of $\mathbf{F}$ over $\mathbf{E}$, and the dimension of $\mathbf{E}$ over $\mathbf{F}$, denoted $\dim_{\mathbf{F}} \mathbf{E}$, or $[\mathbf{E} : \mathbf{F}]$.

Lemma 2.2. *If* $\dim_{\mathbf{F}} \mathbf{E} = 1$*,* $\mathbf{F} = \mathbf{E}$*.*

Proof. For then $1 \in \mathbf{F}$ is a non-zero element of $\mathbf{E}$, and therefore spans $\mathbf{E}$. Every element of $\mathbf{E}$ can be expressed $\alpha \cdot 1 = \alpha$, for $\alpha \in \mathbf{F}$. □

Lemma 2.3. *If* $\mathbf{F} \subset \mathbf{E} \subset \mathbf{K}$*, then* $\dim_{\mathbf{F}} \mathbf{K} = (\dim_{\mathbf{E}} \mathbf{K})(\dim_{\mathbf{F}} \mathbf{E})$*, which can be written* $[\mathbf{K} : \mathbf{F}] = [\mathbf{K} : \mathbf{E}][\mathbf{E} : \mathbf{F}]$*.*

Proof. Let $\{u_i\}$ be a basis for $\mathbf{K}$ over $\mathbf{E}$, and let $\{v_i\}$ be a basis for $\mathbf{E}$ over $\mathbf{F}$. We contend $\{u_i v_j\}$ is a basis for $\mathbf{K}$ over $\mathbf{F}$. First, independence. If

$$\sum c_{(\alpha,\beta)} v_\alpha u_\beta = \sum_\beta \left(\sum_\alpha c_{(\alpha,\beta)} u_\alpha \right) v_\beta = 0$$

then, by independance of the v_β, $\sum_\alpha c_{(\alpha,\beta)} u_\alpha = 0$ for each β. But then, by independance of the u_α, $c_{(\alpha,\beta)} = 0$ for all α and β. Now we prove that the basis spans all of $\mathbf{K}$. If $k \in \mathbf{K}$, we may write $k = \sum e_\alpha u_\alpha$, with $e_\alpha \in \mathbf{E}$. But then $e_\alpha = \sum c_{(\alpha,\beta)} v_\beta$, and then

$$k = \sum_{(\alpha,\beta)} u_\alpha v_\beta$$

So the $u_\alpha v_\beta$ forms a basis. □

Corollary 2.4. *If* $\mathbf{F} \subset \mathbf{E} \subset \mathbf{K}$ *is a tower of field extensions, and* $[\mathbf{K} : \mathbf{F}]$ *is prime, then* $\mathbf{E} = \mathbf{K}$ *or* $\mathbf{E} = \mathbf{F}$.

Proof. Since $[\mathbf{K} : \mathbf{F}] = [\mathbf{K} : \mathbf{E}][\mathbf{E} : \mathbf{F}]$, either $[\mathbf{K} : \mathbf{E}]$ or $[\mathbf{E} : \mathbf{F}]$ is equal to one, since one is the only positive unit integer. But then $\mathbf{K} = \mathbf{E}$ or $\mathbf{E} = \mathbf{F}$. □