Galois Theory

Jacob Denson

February 5, 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' Notes)

The basic problem of Galois theory is to understand the structure of polynomials with coefficients in a field. In particular, we wish to understand why the roots of some polynomials are difficult to solve, and how to find roots to polynomials in easier cases.

1.1 Quadratic Polynomials

The quadratic case is the easiest polynomial to solve. We wish to find x such that

$$X^2 + bX + c = 0$$

Considering any particular X, we let $Y = X + B/2$, so

$$Y^2 = X^2 + BX + \frac{B^2}{4} = \frac{B^2}{4} - C$$

which implies that

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

Note that the method of solving quadratics is geometric in nature. Our calculation shows that every quadratic polynomial 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 deeper applications to geometry. Also, note 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, Galois theory determines which polynomials are solvable in radicals. 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.

1.2 The Cubic Formula

Let's up the difficulty a notch. 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). Then

$$Y^3 + Y\left(C - \frac{B^2}{3}\right) + \left(\frac{4B^3}{27} - \frac{CB}{3} + D\right) = X^3 + BX^2 + CX + D$$

the polynomial is translated so the point of inflection lies at the origin, hence the quadratic coefficient vanishes. This is known as the Tschirnhasu transformation. It follows that we need only consider cubics of the form

$$X^3 - 3PX - Q$$

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

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

Provided that $YZ = P$ and $Y^3 + Z^3 = Q$, then X solves the cubic equation. Letting $Z = P/Y$, we find

$$Y^3 + P^3/Y^3 = Q$$

So we must find the roots of the equation $Y^6 + P^3 = QY^3$, which is a quadratic equation in Y^3 known as the *cubic resolvent*, and we know how to solve quadratic polynomials. Hence if $\omega \neq 1$ is a cube root of unity, then for some $i, j \in \mathbf{Z}_3$,

$$Y = \omega^i \sqrt[3]{\frac{Q + \sqrt{Q^2 - 4P^3}}{2}} \qquad Z = \omega^j \sqrt[3]{\frac{Q - \sqrt{Q^2 - 4P^3}}{2}}$$

$$X = \omega^i \sqrt[3]{\frac{Q + \sqrt{Q^2 - P^3}}{2}} + \omega^j \sqrt[3]{\frac{Q - \sqrt{Q^2 - P^3}}{2}}$$

We have a little bit of a problem. These choices of cube roots leads to nine possible solutions! Note that these solutions do not always satisfy $YZ = P$, so that

$$\left(\omega^i \sqrt[3]{\frac{Q + \sqrt{Q^2 - 4P^3}}{2}}\right)\left(\omega^j \sqrt[3]{\frac{Q - \sqrt{Q^2 - 4P^3}}{2}}\right)$$
$$= \omega^{i+j} \sqrt[3]{\frac{Q^2 - (Q^2 - 4P^3)}{4}} = \omega^{i+j} P$$

So $i = 2 - j$, and we obtain three solutions, as we wanted.

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 numbers[1], who used it to great success in contests, of course, 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, winning the mathematical duel. 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.

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

1.3 Quartic Equations

Since we've solved the cubic, why not solve the quartic, by a method of Lodovico Ferrari? Consider

$$X^4 + AX^2 - BX - C$$

Any polynomial can be reduced to this form, by a Tschirnhaus transformation. Introduce a new term Y, and consider

$$(X^2 + A/2 + Y)^2 = 2YX^2 + BX + C + A^2/4 + AY/2 + Y^2$$

Choose Y so that the right side is a perfect square, i.e.

$$B^2 = 8Y(C + A^2/4 + AY/2 + Y^2) = 8Y^3 + 4AY^2 + (8C + 4A^2)Y$$

Then

$$X^2 + A/2 + Y = \pm\frac{B}{2Y}$$

And this is an ordinary quadratic to solve.

After almost 2000 years of work, the problem of polynomial roots had begun to crack. After a century of success, mathematicans hoped to expand the technique to quintic equations and higher. From the 16th century to the 18th, mathematicians as prominent as Euler and Lagrange tried their hand at 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 prominant mathematician to believe that there may be no solution. In 1813, Paolo Ruffini almost gave an impossibility proof – 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.

Chapter 2

Fields, and their Extensions

Galois theory was invented to study polynomials over the number systems

$$\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

Nonetheless, the methods of the theory can be extended with little added effort to arbitrary fields. In number theory and cryptography, we are interested in studying finite fields, or in fields of functions, and Galois theory applies in exactly the same way as it does in the ordinary number systems. This modern approach was advanced by Emil Artin in the early 20th century. To understand polynomials over a field, we must first understand the fields themselves, which this chapter provides the background for.

Definition. The **prime field** in a field F is the smallest subfield. The **prime ring** is the smallest ring.

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

Proof. Consider the map $f : \mathbf{Z} \to F$ 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 F is an integral domain. If $p \neq 0$, then (p) is a maximal ideal, then by the first isomorphism theorem $\mathbf{Z}/(p) = F_p \cong f(\mathbf{Z})$. Thus $f(\mathbf{Z})$ is a field, and any other subfield of F must contain it, so it is the prime field of 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. □

If we are to understand field extensions, we may as well understand extensions of $\mathbf{Q}$ and F_p, since every field is an extension of these fields.If the prime field of a field F is isomorphic to F_p, we shall say F has **characteristic** p. If the prime field is $\mathbf{Q}$ instead, then we shall say F has **characteristic** 0.

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

Example. *All complex numbers can be written $a + bi$, so $[\mathbf{C} : \mathbf{R}] = 2$.*

Example. *Since $\mathbf{R}$ is uncountable, $[\mathbf{R} : \mathbf{Q}] = \infty$.*

Example. *The set $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$ for a field, and $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$, with basis $\{1, \sqrt{2}\}$.*

Theorem 2.2 (Tower Formula). *If $F \subset E \subset K$, then $[K : F] = [K : E][E : F]$.*

Proof. Let $\{u_i\}$ be a basis for K over E, and let $\{v_i\}$ be a basis for E over F. We contend $\{u_i v_j\}$ is a basis for K over 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 K. If $k \in K$, we may write $k = \sum e_\alpha u_\alpha$, with $e_\alpha \in E$. 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. □

Example. *Consider* $\mathbf{R}[i]$*, which is the smallest field to contain* i*. But* $\mathbf{C}$ *is just the set of all* $a + bi$*, where* $a, b \in \mathbf{R}$*, so* $\mathbf{R}[i] = \mathbf{C}$*. Once can also see this by the tower formula, since* $[\mathbf{C} : \mathbf{R}] = 2$*, so there are no fields between* $\mathbf{R}$ *and* $\mathbf{C}$*.*

If $\{u_i\}$ is a basis for E over F, then E is the smallest field containing both F and $\{u_i\}$. If $S \subset E$, then $F(S)$ will denote the smallest subfield of E to contain both F and S, and $F[S]$ the smallest subring. Notationally, this parallels the use of the polynomial rings and fields $F[X]$ and $F(X)$. This is no mistake, for if we take the free commutative monoid G on S, and take the ring $F[G]$, then we obtain the map from $F[G]$ onto $F(S)$ defined by

$$\sum c_i (s_{i_1} \dots s_{i_{n_i}}) \mapsto \sum c_i (s_{i_1} \dots s_{i_{n_i}})$$

where on the right we actually multiply elements of S together. When $F[G]$ is localized, we obtain the field $F(G)$, and the corresponding evaluation is surjective onto $F(S)$.

Lemma 2.3. *If* E/F*,* K/F *are extensions of* F*, and there exists an isomorphism* $\phi : E \to K$ *which fixes* F*, then* $[E : F] = [K : F]$*.*

Proof. Then ϕ is a linear map. □

2.1 Algebraic Extensions

The most important case to analyze is the case when S consists of a single element, $F(a)$, known as a **simple extension**. In this case we have a natural surjective evaluation map

$$\text{ev}_a : F[X] \to F[a]$$

If the map is injective, a is known as **trancendental**. Otherwise, the map generates an ideal (P) such that $F[X]/(P) \cong F[a]$. Since $F[a]$ is an integral domain, (P) is prime. But by unique factorization, (P) is maximal, so $F[X]/(P)$ is a field, which implies $F[a]$ is a field, thus $F[a] = F(a)$. The polynomial P is unique if we require that it is monic, and is called the **minimal polynomial** of a. If

$$P = a_n X^n + \cdots + a_0$$

then $a, a^2, \dots, a^{n-1}$ is a basis of $F(a)$ over F, so that $[F(a) : F] = \deg(P)$. If a is trancendental, then $[F(a) : F] = \infty$. One corrolary of this discussion is that every finite extension is algebraic. Also, if two elements a and b in an extension E/F have the same minimal polynomial P, then $F(a) \cong F(b)$, since both are isomorphic to $F[X]/(P)$. We have a partial converse to our discussion.

Lemma 2.4. *If $F[a] = F(a)$, then a is algebraic over F.*

Proof. Every element in $F[a]$ may be written $P(a)$ for some $P \in F[X]$. If $a = 0$, the theorem is trivial. Otherwise, there is $Q(a)$ for which $aQ(a) = 1$. But then $(XQ - 1)(a) = 0$. □

Example. *Every element of a field is algebraic over that field. $\sqrt{2}$ is algebraic over $\mathbf{Q}$, since $X^2 - 2$ is the minimal polynomial. e and π are trancendental, though it takes a lot of analysis to determine this.*

An extension E/F is **algebraic** if every element of E is algebraic over F.

Theorem 2.5. *The field extension $F(u_1, \dots, u_n)$ is algebraic over F if and only if each u_i is algebraic over F. Then $F(u_1, \dots, u_n) = F[u_1, \dots, u_n]$.*

Proof. One way is trivial. We prove the other case by induction. The case $n = 0$ is trivial. Since u_{n+1} is algebraic over F, u_{n+1} is algebraic over $F(u_1, \dots, u_n)(u_{n+1})$, so

$$\begin{aligned} F(u_1, \dots, u_n) &= F(u_1, \dots, u_n)(u_{n+1}) = F[u_1, \dots, u_n](u_{n+1}) \\ &= F[u_1, \dots, u_n][u_{n+1}] = F[u_1, \dots, u_{n+1}] \end{aligned}$$

and by the tower formula,

$$[F(u_1, \dots, u_n) : F] = \prod_{i=1}^{n} [F(u_1, \dots, u_i) : F(u_1, \dots, u_{i-1})] < \infty$$

so every element is algebraic. □

Corollary 2.6. *If $F \subset E \subset K$, then K is algebraic over F if and only if K is algebraic over E and E is algebraic over F.*

Example. *$\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbf{Q}$, so $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is algebraic over $\mathbf{Q}$.*

Theorem 2.7. *If F/E is an extension, then the set of algebraic elements in F form an algebraic field over E.*

Proof. If a and b are algebraic, then $E(a, b)$ is algebraic, so $a + b$, ab, and if $a \neq 0$, a^{-1} are all algebraic over E. The fact that the field generated is algebraic is obvious by construction. □

2.2 Splitting Fields

The structure of field extensions is intricately connected to polynomials over the base field. Here we use polynomials to designate specific fields. A field extension F/E **splits** $P \in E[X]$ if P splits into linear factors in $F[X]$. The **splitting field** of P in F/E is then the smallest subfield of F to contain all the roots of P. If $r_1, \dots, r_n$ are the roots of P in F, then the splitting field is $E[r_1, \dots, r_n]$.

Theorem 2.8. *If $P \in E[X]$, then there is a field extension which splits P.*

Proof. We prove by induction on the degree of P. If $\deg(P) = 1$, then P is already split. In general, we may write $P = QR$, where Q is irreducible in $E[X]$. Then (Q) is maximal, and $K = E[X]/(Q)$ is a field, and we may naturally consider K as an extension of E. Q has a root in K, so P splits into a linear factor, and a polynomial of smaller degree. By induction, we may extend K to a field which splits P. □

In particular, since $\deg Q \leqslant n$, there is a field extension with degree at most $n!$.

Example. *$\mathbf{R}$ splits $X^2 - 2$ over $\mathbf{Q}$. The splitting field is $\mathbf{Q}(\sqrt{2})$.*

We wish to show that any two splitting fields are isomorphic, even if we begin with two fields E/F and K/F which split the polynomial in different ways. Let E/F, K/F be a pair of extensions. $\phi : E \to K$ is an F-**homomorphism** if it fixes F. It is a field homomorphism that is also a linear map. To avoid overuse of brackets, we shall write x^ϕ for $\phi(x)$.

Lemma 2.9. *Let $\phi : E \to F$ be an isomorphism of fields, K/E and L/F field extensions. If $x \in K$ is algebraic, with minimal polynomial $P \in E[X]$, then ϕ extends to a homomorphism $\tilde{\phi}$ from $E(x)$ to L if and only if $\phi(P) \in F[X]$ has a root in L. The number of distinct extensions is the number of distinct roots of $\phi(P)$ in L.*

Proof. It is a trivial verification that for each $x \in K$,

$$P^{\phi}(x^{\phi}) = P(x)^{\phi}$$

Therefore if $\tilde{\phi}$ exists, then

$$P^{\phi}(x^{\tilde{\phi}}) = P(x)^{\phi} = 0^{\phi} = 0$$

Conversely, let y be a root of P^{ϕ} in L. We will define a morphism $\tilde{\phi}$ mapping x to y. First, begin with the induced morphisms

$$E[X] \xrightarrow{\phi} F[X] \xrightarrow{\mathrm{ev}_y} L$$

The kernel of the morphism includes P, so we obtain an induced map

$$E[x] \cong E[X]/(P) \xrightarrow{[\phi]} F[X]/(P^{\phi}) \xrightarrow{[\mathrm{ev}_y]} L$$

This map maps x onto y, and is an injective morphism, since $E[X]/(P)$ is a field. The number of distinct morphisms is found to be the number of distinct roots, since every morphism is uniquely defined by its action on x, and x is mapped onto a root of P^{ϕ}. □

Theorem 2.10. *Let $\phi : E \to F$ be a field isomorphism. If K/E is a splitting field of $P \in E[X]$, and L/F a splitting field of P^{ϕ}, then $F \cong E$.*

Proof. We prove by induction on $[K : E]$. If $[K : E] = 1$, then

$$K = E \cong F = L$$

Now suppose $[K : E] > 1$. Then P has an irreducible monic factor Q. ϕ extends to a map from $E[X]$ to $F[X]$. Since K is a spltting field of P, then we may write

$$P =_{i=1}^{n} (X - u_i) \qquad Q =_{i=1}^{m} (X - u_i)$$

$$P^{\phi} =_{i=1}^{n} (X - v_i) \qquad Q =_{i=1}^{m} (X - v_i)$$

The irreducibility of Q ensures it is the minimal polynomial of u_1, so $[E(u_1) : E] = m$. If $k \leqslant n$ is the unique number of roots v_i, then ϕ extends to k injective morphisms ψ_i from $E(u_1)$ to L. Now K is a splitting field of $E(u_1)$, and

$$[K : E(u_1)] = [F : E]/[E(u_1) : E] < [F : E]$$

So induction tells us each ψ_i extends to an isomorphism from K to L, and the number of extensions is less than or equal to $[F : E(u_1)]$, with equality if and only if P^{ϕ} has distinct roots. All such extensions are constructed in this manner, for if Φ extends ϕ, then Φ embeds $E(u_1)$ in L, so $\Phi_{E(u_1)} = \psi_i$ for some i. □

Corollary 2.11. *If $P \in E[X]$ is non-constant, then any two splitting fields of P are E-isomorphic.*

Corollary 2.12. *If F/E is an extension, then the identity map on E extends to E-automorphisms on F, and the number of such automorphisms is less than or equal to $[F : E]$.*

2.3 Normal Extensions

An extension F/E is **normal** if every irreducible polynomial in $E[X]$ that has a root in F splits over F.