Galois Theory

Jacob Denson

February 10, 2016

Table Of Contents

1 Quadratics, Cubics, and Quartics **1**
1.1 Quadratic Polynomials 1
1.2 The Cubic Formula 2
1.3 Quartic Equations 4
1.4 The Quintic 4

2 Fields, and their Extensions **5**
2.1 Algebraic Extensions 8
2.2 Splitting Fields and Normal Extensions 12
2.3 Separability 15
2.4 Application to Finite Fields 18

3 Galois Theory **21**

Chapter 1

Quadratics, Cubics, and Quartics

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 easiest. We wish to find values for 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

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

Note that our solution has a geometric meaning. 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. We shall see that Galois theory has much deeper geometric applications.

Every root of a quadratic polynomial is expressed in terms of the coefficients using five basic operations: addition, subtraction, multiplication, division, and taking radicals ('powers of $1/n$') – we say all quadratic polynomials are 'solvable in radicals'. It is the job of Galois theory to classify which polynomials are solvable in radicals. A great many problems may be reduced to finding the solution of some polynomial over a field, hence Galois theory has many applications outside algebra.

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 to the right $B/3$ 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 quadratric coefficient vanishes because the point of inflection of the equation now lies at the origin. This is known as the Tschirnhaus 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 $YZ = P$ and $Y^3 + Z^3 = Q$, 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 cubic resolvent

$$Y^6 + P^3 = QY^3$$

which is a quadratic equation in Y^3, and we know how to solve quadratic polynomials. Hence if $\omega \neq 1$ is a cube root of unity, then for some $i, j \in \mathbf{Z}_3$,

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

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

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 $YZ = P$. Performing a calculation,

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

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

So $j = 3 - i$, and we obtain three solutions.

Cubic equation occupied a vast amount of mathematical effort. Challenges and contests were formed to test algebraic aptitude. Early in the 16th century, italian mathematician 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, he did not share his solution to the general public. 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, 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

The Arns Magna also included a solution to the quartic equation, 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.

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

After solving a cubic equation, we need only solve solve

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

And this is an ordinary quadratic to solve. Since Y can be solved in radicals, so can X.

1.4 The Quintic

After almost 2000 years of work, polynomials had begun to crack. After a century of success, mathematicans hoped to expand techniques to quintic equations. From the beginning of the 16th century to the end of 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 found they had no 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 rings

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

Without much added effort, the methods can be extended to arbitrary fields. This is not generalization for generalization's sake; in number theory and cryptography, we are interested in studying finite fields. In algebraic geometry, we are interested in fields of functions – Galois theory applies unperturbed in both cases. Our modern approach was advanced by the 20th century mathematician Emil Artin. In Artin's formulation, the main object of study is an **extension**, a pair (F, E) of fields, the first contained within the latter[1]. We write the extension E/F, read "E over F". Artin's main contribution was to view E as an algebra over F, through which we may apply the robust techniques of linear algebra. Most importantly, we may talk of basis of F over E. The dimension of E over F will be denoted $[E : F]$, and called the **degree** of the extension. E/F is a **finite** extension if E is a finite dimensional vector space over F.

Example. *The complex numbers are a field extension of the real numbers. Any complex number can be written uniquely in the form $a + bi$, where a and b are real numbers, so $[\mathbf{C} : \mathbf{R}] = 2$.*

Example. *Since $\mathbf{R}$ is uncountable, and $\mathbf{Q}$ is countable, $[\mathbf{R} : \mathbf{Q}]$ is infinite.*

[1] Category theoretically, an extension is (F, E, i) where i is an epimorphism from F to E. It is cleaner to just consider subsets, for then we do not explicitly need to write out the embedding, but keep in mind that the theory does not change if we allow arbitrary embeddings.

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

Theorem 2.1 (Tower Formula)**.** *If* $F \subset E \subset K$, *then* $[K : F] = [K : E][E : F]$.

Proof. Let $\{u_i\}$ be a basis for K/E, and $\{v_i\}$ a basis for E/F. We contend $\{u_i v_j\}$ is a basis for K/F. If

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

then, since the v_β are independent, we conclude for each β,

$$\sum_\alpha c_{(\alpha,\beta)} u_\alpha = 0$$

But then, by independance of the u_α, we conclude $c_{(\alpha,\beta)} = 0$ for all α and β. Thus the $\{u_i v_j\}$ are independent. If $k \in K$, we may write $k = \sum e_\alpha u_\alpha$, with $e_\alpha \in E$. But then $e_\alpha = \sum c_{(\alpha,\beta)} v_\beta$ for some $c_{(\alpha,\beta)}$, and so

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

Thus $u_\alpha v_\beta$ is an independent spanning set. □

Example. *Let* F/E *be an extension of prime degree. Then there is no field between* E *and* F. *Indeed, if* F/K *and* K/E *are extensions, then*

$$[F : E] = [F : K][K : E]$$

The left side is prime, which implies either $[F : K] = 1$, *or* $[K : E] = 1$. *We conclude* $K = F$ *or* $K = E$. *In particular, there is no field between* $\mathbf{R}$ *and* $\mathbf{C}$.

If $\{u_i\}$ is a basis for E/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 $F(X)$. If we take the free commutative monoid G generated by the set S, and consider the monoid ring $F[G]$, then we obtain a surjective map from $F[G]$ onto $F[S]$, defined by

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

The left is an abstract sum, whereas on the right we multiply elements of S together. When $F[G]$ is localized, we obtain the field $F(G)$, and the corresponding evaluation is surjective onto $F(S)$.

On vector spaces, the natural maps are linear maps. On groups, the natural maps are homomorphisms. The most natural map between field extensions E/F and K/F is an F-**morphism** – a field morphism which is the identity when restricted to F. Viewing E and K as F-algebras, this is simply an algebra homomorphism, a ring homomorphism which is also linear.

Lemma 2.2. *If $E/F \cong K/F$, then $[E : F] = [K : F]$.*

Proof. If ϕ is an F-isomorphism between E and K, then ϕ is an F-linear isomorphism, which maps bases to bases, preserving dimension. □

Fields are powerful objects, but in some sense the category of fields is too rigid. We cannot take normal set-theoretic products in the category of fields, for then the set has zero divisors,

$$(1,0)(0,1) = (0,0)$$

Category theoretic products also don't work, for $\mathbf{F}_p \times \mathbf{F}_q$ must then be a field which contains copies of $\mathbf{F}_p$ and $\mathbf{F}_q$ are subfields, which is impossible. Even if we restrict ourselves to fields of the same characteristic, we have trouble. Let K be a field with a non-trivial automorphism ζ. Suppose we had a product $K \times K$, with projections $\pi : K \times K \to K$ and $\psi : K \times K \to K$. By the universal property of products, there must be $f : K \to K \times K$ with

$$\pi \circ f = \psi \circ f = \mathrm{id}_K$$

Since every morphism of fields is injective, this implies f is an isomorphism, and $\pi = \psi$. But this is impossible, for if we then take $\zeta \neq \mathrm{id}_K$, there must exist $g : K \to K \times K$, for which

$$\psi = \pi \circ g = \psi \circ g = \mathrm{id}_K$$

And this is clearly impossible. A similar argument shows coproducts do not exist. The reason this fails is because the definition of fields are not homogenous. In the field of universal algebra, one studies arbitrary objects endowed with arbitrary operations. One shows that in the category

of such objects, one has products, coproducts, etc. In fields, addition and multiplication are defined on all elements of the field, but multiplicative inverses are only defined on non-zero elements, a fundamental asymmetry.

We have to make do with what we've got. A useful, but non-general construction is the **compositum** of two fields E and F, denoted EF, which is the smallest field containing both E and F. This only makes sense if E and F are both contained in a larger field. Then

$$EF = \{xy : x \in E, y \in F\}$$

so EF coincides with the normal way of taking products of sets. In general, we can consider products of arbitrary fields, which are all contained within a larger field.

2.1 Algebraic Extensions

The most important fields to analyze are the **simple extensions** $F(a)$. a is known as the **primitive element** of the extension. In this case we have a natural surjective evaluation map

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

If this map is a bijection, a is known as **trancendental** over F. Otherwise, a is the root of some polynomial, and is known as **algebraic**, and the map has a non-trivial kernel (P), and

$$F[X]/(P) \cong F[a]$$

Since $F[a]$ is an integral domain, (P) is prime. But then (P) is maximal, since $F[X]$ is a P.I.D. We conclude $F[X]/(P)$ is a field, which implies $F[a]$ is a field, so $F[a] = F(a)$. The polynomial P is unique if we require it to be monic, and ones calls P the **minimal polynomial** of a. If

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

then $1, a, a^2, \ldots, a^{n-1}$ form a basis of $F(a)$ over F, so that $[F(a) : F] = \deg(P)$. One corollary is that if two elements a and b in an extension E/F have the same minimal polynomial P, then $F(a)/F \cong F(b)/F$, since both are isomorphic to the extension constructed as the quotient field of the polynomial

ring. What's more, this isomorphism maps a onto b. We have a partial corollary.

Lemma 2.3. *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, which we leave for another time.*

An extension E/F is **algebraic** if every element of E is algebraic over F. One can have algebraic extensions which are not finite dimensional, but we have shown every finite extension is algebraic. This is because if a is trancendental, then $[F(a) : a] = \infty$.

Theorem 2.4. *$F(u_1, \ldots, u_n)/F$ is algebraic if and only if each u_i is algebraic.*

Proof. One way is trivial. We prove the other case by induction by showing $F[u_1, \ldots, u_n] = F(u_1, \ldots, u_n)$. The case $n = 1$ has already been argued. Since u_{n+1} is algebraic over F, u_{n+1} is algebraic over $F(u_1, \ldots, u_n)(u_{n+1})$, so

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

and by the tower formula,

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

so every element is algebraic. □

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

Theorem 2.5. *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. □

Example. $\mathbf{C}$ *is an extension of* $\mathbf{Q}$*, such that every polynomial in* $\mathbf{Q}[X]$ *splits into linear factors in* $\mathbf{C}[X]$*. We may then consider the algebraic closure* $\mathbf{Q}^{\mathfrak{a}}$*, which is the set of algebraic elements in* $\mathbf{C}$*.*

We shall say a class $\mathcal{C}$ of field extensions satisfies the **three standard properties**, or is a **distinguished property**,

1. When $E \subset K \subset F$, $F/E \in \mathcal{C}$ iff $F/K, K/E \in \mathcal{C}$.
2. If $E/K \in \mathcal{C}$, and F/K is another extension, then $EF/F \in \mathcal{C}$.
3. If $E/K, F/K \in \mathcal{C}$, then $EF/K \in \mathcal{C}$

One summarizes the properties using standard Hasse diagrams. Note that (3) follows from (1) and (2).

Theorem 2.6. *The class of algebraic extensions is distinguished.*

Proof. Let us first verify the tower property. If F/E is algebraic, then K/E and F/K must be algebraic, by inclusion properties. On the other hand, let K/E and F/K be algebraic. Let $x \in F$ be given. Then there is an irreducible polynomial $P \in K[X]$ for x. Let $P = \sum a_i X^i$. Then $[F(x) : F(a_0, \ldots, a_n)] < \infty$. But also $[F(a_0, \ldots, a_n) : K] < \infty$, since each a_i is algebraic over K. By the tower formula, we conclude that x is algebraic over E.

Now let us verify the lifting property. Let E/K be an algebraic extension, and consider $xy \in EF$, with $x \in E$, $y \in F$. Then $F(xy) = F(x)$, and x is surely algebraic over F, so

$$[F(xy) : F] = [F(x) : F] < \infty$$

But this implies that xy is algebraic over F. □

The best kinds of fields are **algebraically closed** – K is algebraically closed if every non-constant polynomial in $K[X]$ has a root. This is a natural place for Galois theory, which was built to study the algebraically closed field $\mathbf{C}$. We shall show that every field has an algebraic extension which is algebrically closed, known as the algebraic closure.

Lemma 2.7. *For* $P \in K[X]$*,* K *can be algebraically extended so* P *has a root.*

Proof. Assume, without loss of generality, that P doesn't have a root. Then we may write $P = QR$, where Q is irreducible, and has no root. Then (Q) is maximal, and $L = K[X]/(Q)$ forms a field. Technically, this is not a set-theoretic extension of K, but by replacing elements where needed, we may pretend it is. It follows that $Q(X) = 0$ in L, so Q has a root in L. □

Theorem 2.8. *Every field has an algebraic closure.*

Proof. Let K be a field, and consider the set $\mathcal{C}$ of all fields which are algebraic over K. Then they are partially ordered by inclusion, and the union of a chain of fields is also a field. By Zorn's lemma, there is a maximal extension L. If E/L is an algebraic extension, then E/K is an algebraic extension, so $E = L$. Thus, if $P \in L[X]$, then P has a root in $L[X]$, by the lemma above. □

Technically, $\mathcal{C}$ is too big to be a set. One instead considers $\mathcal{C}$ to be a class, in which we may apply a stronger axiom of choice. Those suspicious may restrict $\mathbf{C}$ to all fields whose elements are contained in a set S, chosen with a large enough cardinality to contain all algebraic extensions needed. One usually takes S to be the polynomial ring $K[X]$.

We will show the algebraic closure of a field is unique. Notationally, it will help to write an application of a morphism $f(x)$ as x^f, to avoid bracket overuse.

Lemma 2.9. *Let $f : K \to L$ be a field morphism, and E/K and F/L extensions. Let $P \in K[X]$ be the minimal polynomial of $a \in K$. Then f extends to a map $f : K[a] \to L$ if and only if P^f has a root in L. The number of extensions is the number of unique roots of P^f in L.*

Proof. It is clear that any extension maps a root of P onto a root of P^f, proving the existence of a root. Conversely, let b be a root of P^f in L. Consider the sequence

$$E[X] \xrightarrow{f} F[X] \xrightarrow{\mathrm{ev}_b} L$$

The kernel of f includes P, and the kernel of ev_b include (P^f) so we obtain an induced sequence

$$E[a] \cong E[X]/(P) \xrightarrow{[f]} F[X]/(P^f) \xrightarrow{[\mathrm{ev}_b]} L$$

Which is exactly the map required. □

Theorem 2.10. *Let K/E be an algebraic extension. If $f : K \to L$ is an embedding in an algebraically closed field, then f extends to an embedding of E. If E is an algebraic closure, and L is algebraic over E, then the map is an isomorphism.*

Proof. Consider all (F, g), where $K \subset F \subset E$ extends K and g extends f. We may take unions of chains, so Zorn's lemma applies to give us a maximal field $(J, \tilde{f})$. The last lemma says we may extend maps on any proper subfield of E, so $J = E$. To verify the second fact, suppose $L/\tilde{f}(E)$ is algebraic, and E is algebraically closed. When $x \in J$, then $P(x) = 0$ for some $P \in \tilde{f}(E)[X]$, where

$$P = (x - \tilde{f}(a_1)) \dots (x - \tilde{f}(a_n))$$

This implies $x = \tilde{f}(a_i)$ for some $a_i \in E$. □

Corollary 2.11. *Any two algebraic closures of a field are isomorphic.*

2.2 Splitting Fields and Normal Extensions

The structure of field extensions is intricately connected to polynomials defined over the base field. 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 an extension which splits P, such that no proper subextension of F splits P. If $r_1, \dots, r_n$ are the roots of P in F, then $F = E[r_1, \dots, r_n]$. If the t_i are not multiple roots, then the degree of F/E is $n!$. A splitting field always exists, since we may always take a subfield of the algebraic closure. The degree of this extension is at most $n!$, as one verifies by induction on the minimal polynomials of the roots.

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

Theorem 2.12. *Let $f : E \to F$ be a field isomorphism. If K/E is a splitting field of $P \in E[X]$, and L/F a splitting field of P^f, 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. f extends to an isomorphism between $E[X]$ and $F[X]$. Since K is a splting field of P, then we may write, for $u_i \in K$, $v_i = f(u_i)$,

$$P = (X - u_1)\dots(X - u_n) \qquad Q = (X - u_1)\dots(X - u_m)$$

$$P^f = (X - v_1)\dots(X - v_m) \qquad Q^f = (X - v_1)\dots(X - v_m)$$

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 f 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^f has distinct roots. All such extensions are constructed in this manner, for if g extends f, then g embeds $E(u_1)$ in L, so $g|_{E(u_1)} = \psi_i$ for some i. □

Corollary 2.13. *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 $[F : E]$.*

It is also important to consider splitting fields over families of polynomials. If this family is finite, then the splitting field is the same as the splitting field of the product of the polynomials.

Theorem 2.14. *Any splitting fields of a family of polynomials are isomorphic.*

Proof. Let K/E and F/E be splitting fields of a family $\mathcal{F}$. Extend F to an algebraic closure $F^{\mathfrak{a}}$. Then there is an embedding $f : K/E \to F^{\mathfrak{a}}/E$. We know that $f(K)$ splits $\mathcal{F}$, so $f(K) \supset F$. But we may pull F back to conclude that $f^{-1}(F)$ splits $\mathcal{F}$, so $f(K) = F$. □

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

Lemma 2.15. *If F/E is normal, then every embedding $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$.*

Proof. Let $x \in F$ be given, and pick $P \in E[X]$ for which $P(x) = 0$. In $F^{\mathfrak{a}}[X]$, We may write

$$P = (X - a_1) \dots (X - a_n)$$

Now $P^\sigma = P$, and $P(x^\sigma) = 0$, which implies $x^\sigma \in F$. □

Theorem 2.16. *If F/E is an extension for which every embedding $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$, then F/E is normal.*

Proof. Let $P(x) = 0$, for $P \in E[X]$, $x \in F$. Let y be a root of P in $F^{\mathfrak{a}}$. Then there is a morphism $\sigma : F/E \to F^{\mathfrak{a}}/E$ for which $\sigma(x) = y$. This implies $y \in F$, so that P splits into linear factors. □

Corollary 2.17. *Every splitting field is normal, and every normal extension is a splitting field.*

Proof. Let F/E be a splitting field for a family $\mathcal{F}$, and let $\sigma : F/E \to F^{\mathfrak{a}}/E$ be a morphism. Then $\sigma(F) \subset F$, for if x is a root of $P \in \mathcal{F}$, then x^σ is a root of P, so $x^\sigma \in F$. The relation follows since F is generated by these roots. Hence the splitting field is normal.

Conversely, let F/E be normal. For each $x \in F$, consider the minimal polynomial $P_x \in E[X]$. Then $P_x(x) = 0$, so F splits P_x. But this implies exactly that F is the splitting field of $\{P_x : x \in F\}$. □

Example. *Every extension of degree 2 is normal, for if $\{1, x\}$ is the basis for F/E, then $F = E[x]$ is the splitting field for the minimal polynomial of x. This shows that normal extensions are not distinguished, for $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is normal, and $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})$ is normal, yet $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ is not normal.*

Some properties do preserve normality, however.

Theorem 2.18. *If $K \subset E \subset F$, then if F/K is normal, then F/E is normal.*

Proof. For if F is a splitting field for a family of polynomials in $K[X]$, then F is a splitting field for a family of polynomials in $E[X]$. □

Theorem 2.19. *If K/E and F/E are normal, then KF/E and $K \cap F/E$ are normal.*

Proof. If K is a splitting field for $\mathcal{F}$, and F a splitting field for $\mathcal{G}$, then KF is a splitting field for $\mathcal{F} \cup \mathcal{G}$, and $K \cap F$ is a splitting field for $\mathcal{F} \cap \mathcal{G}$. □

2.3 Separability

Let F/E be an algebraic extension, and consider an algebraic closure $F^{\mathfrak{a}}$. We shall let $[F:E]_s$ denote the number of different embeddings of F in $F^{\mathfrak{a}}$. The number of different embeddings is invariant of which algebraic closure we choose, since any two closures are isomorphic. A finite extension is **separable** if $[F:E]_s = [F:E]$.

Example. *Consider a simple extension $E[a]$, with minimal polynomial P. In $F^{\mathfrak{a}}$, write*

$$P = (X - b_1)\dots(X - b_n)$$

Then $E[a]/E$ is separable if and only if the b_i are distinct. This shows that $\mathbf{C}/\mathbf{R}$ is separable. a is called separable if $E[a]$ is separable.

Theorem 2.20. *If $F \subset K \subset L$ is a tower, then*

$$[L:K]_s[K:F]_s = [L:F]_s$$

If $[L:F]$ is finite, $[L:F]_s \leqslant [L:F]$.

Proof. Let $\{\pi_i\}$ be all F embeddings of K into L. Then each π_i can be extended to a family of embeddings $\{\psi_{ij}\}$, and these are all such embeddings. If $[L:F]$ is finite, we may consider a tower

$$F \subset F(a_1) \subset \cdots \subset F(a_1,\dots,a_n) = L$$

And we know that

$$[F(a_1,\dots,a_n) : F(a_1,\dots,a_{n-1})]_s \leqslant [F(a_1,\dots,a_n) : F(a_1,\dots,a_{n-1})]$$

Because every embedding must embed into the splitting field of the minimal polynomial of

$$F(a_1,\dots,a_n)/F(a_1,\dots,a_{n-1})$$

And the number of extensions is the number of distinct roots. □

Corollary 2.21. *If E/F is finite, and $F \subset K \subset E$, then E/F is separable if and only if K/F and E/K are separable.*

A polynomial is separable if it has no multiple roots. It is clear from the corollary that the splitting field of a separable polynomial is separable. A finite extension is separable if and only if each element of the extension is separable. We shall define a general algebraic extension E/F to be separable if each finite subextension is separable, or if each element of a is separable over F. With this definition it follows that the class of separable extensions is distinguished, and even allows for infinite compositums of fields.

Example. *Let K be a field. There is a unique maximal separable extension of K in $K^{\mathfrak{a}}$, since the compositum of separable extensions is separable. We call this maximal extension the separable closure, denoted $K^{\mathfrak{s}}$.*

Let E/K be a finite extension. The intersection of all normal extensions of E in $E^{\mathfrak{a}}$ is normal, and is the smallest normal extension. If $\sigma_1, \ldots, \sigma_n$ are all the embeddings of E in $E^{\mathfrak{a}}$, then $L = \sigma_1(E) \ldots \sigma_n(E)$ is a field, which we contend to be the smallest normal field. Let $\pi : L \to E^{\mathfrak{a}}$ be an embedding. Then $\pi \circ \sigma_i$ embeds E in $E^{\mathfrak{a}}$, so π induces a permutation of the σ_i, each E_i maps into some E_j, and thus L maps into itself. If E is separable, then $\sigma_i(E)$ is separable, which implies K is separable. Similar results hold for infinite extensions, where we require an infinite compositum to be taken. We call each $\sigma_i(E)$ a conjugate of E, and $\sigma_i(a)$ a conjugate of a.

Example. $\mathbf{C}/\mathbf{R}$ *is a separable extension, for we have two automorphisms, the identity map $z \mapsto z$, and the conjugation map $z \mapsto \overline{z}$. This also follows because $\mathbf{C} = \mathbf{R}(i)$, and the minimal polynomial of i is $X^2 + 1 = (X + i)(X - i)$, which has distinct roots. Thus every element of $\mathbf{C}$ has two conjugates over $\mathbf{R}$, z and $\overline{z}$.*

Example. *The minimal polynomial of $\mathbf{Q}(\sqrt[3]{2})$ is*

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2})$$

where ω is a cubic root of unity. Thus $\mathbf{Q}(\sqrt[3]{2})$ is separable. The two embeddings in $\mathbf{Q}^{\mathfrak{a}}$ are

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{4}$$
$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\omega^2\sqrt[3]{2} + c\omega\sqrt[3]{4}$$

which are obtained from the lemma established for algebraic embeddings. Thus $\sqrt[3]{2}$ is conjugate with $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$., and $\sqrt[3]{4}$ is conjugate with $\omega\sqrt[3]{4}$ and $\omega^2\sqrt[3]{4}$.

Theorem 2.22. *A finite extension E/K is simple if and only if there are a finite number of fields between K and E.*

Proof. If E is finite, then the theorem is trivial, since we know that the multiplicative group of a finite field is cyclic. Therefore, without loss of generality, we may assume we are working in a field of characteristic zero. Suppose we can write $E = K(\alpha, \beta)$. Then we have an infinite number of fields of the form $K(\alpha + a\beta)$, lying between K and E. Thus

$$K(\alpha + a\beta) = K(\alpha + b\beta)$$

for some a and b, which implies $(a - b)\beta \in K(\alpha + a\beta)$. Since $a \neq b$, $\beta \in K(\alpha + a\beta)$, and so $K(\alpha + a\beta) = K(\alpha, \beta)$. We may thus proceed inductively to consider all finite extensions.

Conversely, consider a finite extension $E = K(\alpha)$. Let P be the minimal polynomial of α. If $K \subset L \subset E$, then the minimal polynomial of α over L divides P. In $E^{\mathfrak{a}}$, we have unique factorization into linear coefficients, so if P has degree n, we can only have at most 2^n unique monic polynomials dividing the polynomial. If the minimal polynomial of α in L is $\sum_{i=1}^{m} c_i X^i$, then the degree of α over $F(c_1, \ldots, c_m)$ is the same as the degree over L, which implies that $F(c_1, \ldots, c_m) = L$. Thus a subfield is uniquely identified by the minimal polynomial of α. □

The next theorem uses the following bit of ingenuity – to prove a subfield of a separable field is equal to the entire field, we need only show that it has the same number of embeddings into its algebraic closure..

Corollary 2.23 (Primitive Element Theorem)**.** *If E/K is finite and separable, then E is a simple extension.*

Proof. Without loss of generality, we may suppose $E = K(\alpha, \beta)$, where α and β are separable over K. Let $\sigma_1, \ldots, \sigma_n$ be all embeddings of K into $E^{\mathfrak{a}}$. Consider the polynomial

$$P = \prod_{i \neq j} ([\alpha^{\sigma_i} + X\beta^{\sigma_i}] - [\alpha^{\sigma_j} + X\beta^{\sigma_j}])$$

$P \neq 0$, so there is $c \in K$ with $P(c) \neq 0$, so the $\sigma_i(\alpha + c\beta)$ are distinct, and we have at least n distinct extensions in $K(\alpha + c\beta)$. This implies that

$$[K(\alpha + c\beta) : K] \geqslant [K(\alpha + c\beta) : K]_s = n$$

and from this, we conclude that $K(\alpha + c\beta) = K(\alpha, \beta)$, since

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K]_s = n$$

By induction, the theorem follows. □

It shall also be convinient to discuss **perfect fields**, which are fields in which every irreducible polynomial is separable. This is equivalent to saying every extension is separable.

Example. *Every field of characteristic zero is perfect, for if f was irreducible and inseparable, then $gcd(f, f') \neq 0$, which would imply $f|f'$, hence $f' = 0$, which would imply f was constant.*

Example. *Consider the polynomial*

$$X^2 - T$$

in the field $\mathbf{F}_2(T)$. The polynomial is irreducible and separable, for it is the product $(X + \sqrt{T})(X + \sqrt{T})$ in $\mathbf{F}_2(T)^{\mathfrak{a}}$.

Theorem 2.24. *Every finite field is perfect*

Proof. For every finite field extension of a finite field is separable. □

Corollary 2.25. *Every finite, separable extension is simple.*

2.4 Application to Finite Fields

We shall use our current knowledge of Galois theory to understand the structure of finite fields. If K is an arbitrary finite field, then it has a certain prime characteristic $p > 0$. Then we may view K as a finite dimensional vector space over $\mathbf{F}_p$. If the degree of $K/\mathbf{F}_p$ is n, then K has cardinality p^n, since K is (by elementary linear algebra), linearly isomorphic to $\mathbf{F}_p^n$. Every element of K is a root of the polynomial

$$X^{p^n} - X = X(X^{p^n - 1} - 1)$$

this follows from Lagrange's theorem, since there are $p^n - 1$ elements in the group of units of K. But this implies K is a splitting field of $X^{p^n} - X$. But we

now have a characterization of K, which is then shown to be any other field of order p^n, since splitting fields are isomorphic. In particular, there exists a field of order p^n for each n, since the splitting field of $X^{p^n} - X$ has order p^n. This follows from the aptly named 'freshman's dream theorem', in a field of characteristic $p > 0$, $(x+y)^{p^k} = x^{p^k} + y^{p^k}$. By taking the binomial expansion

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

And p divides all coefficients except when $k = 0$ or p. By induction, we prove the theorem in general by induction. But then the collection of all roots in $\mathbf{F}_p^{\mathfrak{a}}$ form a field, since if $x^{p^n} = x$, $y^{p^n} = y$, then

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$$

$$(xy)^{p^n} = x^{p^n} y^{p^n} = xy$$

$$(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1}$$

and thus has order p^n, since the polynomial $X^{p^n} - X$ has distinct roots, found by taking the derivative. This also shows that $\mathbf{F}_p^{\mathfrak{a}}$ contains a unique field of order p^n, since this field must be the splitting field of $X^{p^n} - X$. We denote this unique field $\mathbf{F}_{p^n}$.

We consider the Frobenius mapping φ from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^n}$, defined by $x \mapsto x^p$. Then this map is a field homomorphism, by Freshman's dream. In fact, the map is actually an $\mathbf{F}_p$-isomorphism, since $x^p = x$ for all $x \in \mathbf{F}_p$ (Lagrange's theorem again). We shall show that φ generates all $\mathbf{F}_p$ automorphisms of $\mathbf{F}_{p^n}$. If d is the order of φ, then $\varphi^d(x) = x^{p^d} = x$ for all x, so every $x \in \mathbf{F}_{p^n}$ is a root of

$$X^{p^d} - X$$

so $d \geqslant n$, and in fact must be equal, for n is an exponent of $\mathbf{F}_{p^n}^*$. Thus $\mathbf{F}_{p^n}$ is a separable and normal extension of $\mathbf{F}_{p^m}$, for $m < n$, of order $n - m$.

We know that the multiplicative group of non-zero elements in a finite field is cyclic. The proof may be generalized for interesting consequences.

Theorem 2.26. *A finite multiplicative subgroup of a field is cyclic.*

Proof. Let G be a subgroup of $F^\times$, where F is a field. Let x be an element of G of maximal order m. Then $y^m = 1$ for all $y \in G$. But this implies that G contains all roots of $X^m - 1$, and in particular, G has only m elements, since roots are distinct factors of the polynomial. Thus $G = \langle x \rangle$. □

Example. *The only finite subgroups of* $\mathbf{C}^\times$ *are the n'th roots of unity. The only finite subgroup of* $\mathbf{R}$ *is tbe trivial group and* $\{-1, 1\}$. *The only finite subgroups of* $\mathbf{F}_p$ *is* $\mathbf{F}_p$ *itself.*

Corollary 2.27. *Every extension F/K where F is finite is simple.*

Corollary 2.28. *s*

Chapter 3

Galois Theory

> 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)