Galois Theory

Jacob Denson

August 12, 2020

Table Of Contents

Chapter 1

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 rational functions. Under a general formulation, Galois theory applies unperturbed. This modern approach was advanced by the 20th century mathematician Emil Artin. In Artin's formulation, the main object of study is a *field extension*, a pair of fields E and F, with $F \subset E$. We write the extension as E/F. Artin's main contribution to the foundations of Galois theory was then to view E as an algebra over F, through which we can apply the robust techniques of linear algebra. In particular, we can talk about bases and dimension. The dimension of E as a F vector space will be denoted $[E : F]$ and called the *degree* of the extension. If the dimension is finite, we say E/F is a *finite* extension. Note that this is different from a *finitely generated* extension, which occurs when E is a finite dimensional algebra over F.

Remark. Categorically speaking, a field extension E/F is a morphism $i : F \to E$. But it is notationally simpler to view F as a subset of E, since F can be identified with $i(F) \subset E$.

Example. *The field* $\mathbf{C}$ *of complex numbers is a field extension of the real numbers* $\mathbf{R}$*. This is because any complex number can be written uniquely as* $a + bi$*,*

where a and b are real numbers, so that $\{1, i\}$ is a basis for $\mathbf{C}$ as a $\mathbf{R}$ vector space, and so $[\mathbf{C} : \mathbf{R}] = 2$.

Example. *The set $\mathbf{Q}[\sqrt{2}]$ of all real numbers expressed as $a + b\sqrt{2}$, with $a, b \in \mathbf{Q}$, forms a field, because*

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

which is well defined if a or b is nonzero since the equation $a^2 - 2b^2 = 0$ has no rational solutions. To emphasize the field structure of this ring we also denote it by $\mathbf{Q}(\sqrt{2})$. Any element of $\mathbf{Q}(\sqrt{2})$ can be uniquely *written as $a + b\sqrt{2}$ for $a, b \in \mathbf{Q}$, so $\{1, \sqrt{2}\}$ is a basis for $\mathbf{Q}(\sqrt{2})$. Thus $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.*

Example. *Even in the classical situation, a field extension need not have a finite degree. Since $\mathbf{R}$ is uncountable, and $\mathbf{Q}$ countable, $[\mathbf{R} : \mathbf{Q}]$ has the same cardinality of $\mathbf{R}$, namely $\mathfrak{c}$. If K is any field, then the field $K(X)$ of rational functions over K is an infinite field extension of K; a basis is given by taking partial fractions. In particular, if K is algebraically closed, then a basis is given by*

$$\{1, X, X^2, \dots\} \cup \left\{ \frac{1}{(X - a)^n} : a \in K, n \geqslant 0 \right\}$$

Over $\mathbf{R}$, we must also add elements of the form

$$\frac{1}{(X^2 + aX + b)^n} \quad \textit{and} \quad \frac{X}{(X^2 + aX + b)^n}$$

for any irreducible quadratic polynomial $X^2 + aX + b$ and $n \geqslant 0$.

Example. *Every field K is the extension of its prime subfield, the smallest field contained in K. This field is characterized by the characteristic of p. If K has characteristic $p > 0$, then the prime subfield is $\mathbf{F}_p$, and if K has characteristic 0, then the prime subfield is isomorphic to $\mathbf{Q}$. It follows that $\mathbf{F}_p$ and $\mathbf{Q}$ are the only fields that contain no proper subfields.*

The notation $[E : F]$ should remind you of the notation $[G : H]$ for a subgroup H of G. Like for groups, field extensions satisfy a 'Lagrange theorem' type result, known as the tower formula. One of the main principles of Galois theory is that there is a deep correspondence between the theory of groups and the theory of fields, which appears once we analyze the symmetry of a field extension.

Theorem 1.1 (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 $x \in K$, we may write $x = \sum e_\alpha u_\alpha$, with $e_\alpha \in E$. But then $e_\alpha = \sum c_{\alpha\beta} v_\beta$ for some $c_{\alpha\beta}$, and so

$$k = \sum_{\alpha\beta} c_{\alpha\beta} u_\alpha v_\beta$$

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

We note that this argument works even if the field extensions K/E and E/F are infinite, in which case we view the tower formula as an equation interpreted in the theory of infinite cardinals.

Example. *Let F/E be an extension whose degree is prime. 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 $K = E$. As a particular case of this argument, we conclude there is no proper field between **R** *and* **C**.

If E is a subfield of F, and $S \subset F$, we will denote by $E(S)$ the smallest subfield of F to contain both E and S, and $E[S]$ the smallest subring. In particular, if $\mathcal{B}$ is a basis for an extension E/F, then $F = E(\mathcal{B})$. Notationally, this parallels 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 $F[G]$ (which is really just the polynomial ring with the elements of S interpreted as variables), 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 a formal 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 $F(S)$ since the image is a subfield of $F(S)$ containing F and S.

The category of fields is suprisingly restrictive. No products exist, nor coproducts. The most natural construction which occur systematically in Galois theory are the *compositums* and *intersections*. If E and F are both subfields of a field K, we let EF denote the smallest subfield of K containing E and F, and $E \cap F$ the largest subfield contained in E and F. More generally, we can form the compositum and intersection of infinite families of fields. When we relate field extensions to groups, these operations correspond to intersections of subgroups and the smallest subgroup generated by two subgroups.

1.1 Algebraic and Simple Extensions

The most basic extensions are the *simple extensions* $F(a)$, where a lies in some extension E of F. a is known as a *primitive element* of the extension. In this case we have a natural surjective evaluation map

$$\mathrm{ev}_a : F[X] \to E \qquad f \mapsto f(a)$$

The element $a \in E$ is *algebraic* over F if it is the root of some polynomial in $F[X]$. Then ev_a has a non-trivial kernel $\mathfrak{a}$, and $F[X]/\mathfrak{a} \cong F[a]$. Since $F[a]$ is entire, $\mathfrak{a}$ is a prime ideal, hence it is maximal. Thus we conclude $F[X]/\mathfrak{a}$ is a field, which implies $F[a]$ is a field, so $F[a] = F(a)$. Note that the converse of this statement, that if $F[a] = F(a)$, then a is algebraic over F, is also true, since then a has an inverse $f(a)$, hence $af(a) = 1$, and so $Xf(X) - 1$ vanishes at a. Because $F[X]$ is a principal ideal domain, $\mathfrak{a}$ can be uniquely written as (f), for some monic polynomial f. One calls f the *minimal polynomial* of a, sometimes denoted by $\mathrm{Irr}(F, a)$. If f is the minimal polynomial of a and has degree n, then $\{1, a, \dots, a^{n-1}\}$ is a basis

for $F(a)$, which implies $[F(a) : F]$ is equal to the degree of the minimal polynomial of a over F.

Example. *The number $\sqrt{2}$ is algebraic over $\mathbf{Q}$, since $X^2 - 2$ is the minimal polynomial. We have already seen that $\{1, \sqrt{2}\}$ form a basis for $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, which corresponds to the result of the more general arguments here.*

Example. *Let $F(a)/F$ be an extension of odd degree n. Then $F(a) = F(a^2)$. Certainly $F(a^2) \subset F(a)$, so we can apply the Tower formula to write*

$$n = [F(a) : F] = [F(a) : F(a^2)][F(a^2) : F].$$

Note that $F(a^2)/F(a)$ is a simple algebraic extension. Since $f(x) = x - a^2$ certainly satisfies $f(a^2) = 0$, it follows that the minimal polynomial of a^2 is less than or equal to two, and so $[F(a^2) : F(a)] \leqslant 2$. Since $[F(a^2) : F(a)]$ divides n, it follows that $[F(a^2) : F(a)] \neq 2$, and so $[F(a^2) : F(a)] = 1$. Thus $F(a^2) = F(a)$.

Remark. The opposite of an algebraic number is a *trancendental* number, i.e. an element $a \in E$, where E/F is an extension, such that for any $f \in F[x]$, $f(a) \neq 0$. Examples of algebraic numbers include e and π, which are trancendental over $\mathbf{Q}$, though these are difficult statements to prove without significant analytical techniques. If a is trancendental, then $F(a)$ is isomorphic to the field of rational functions $F(x)$. For obvious reasons, non-algebraic extensions are harder to analyze than algebraic extensions, and we leave their analysis till later on in these notes.

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. if $a \in E$ is trancendental, then $[F(a) : F]$ is infinite, so

$$[E : F] = [E : F(a)][F(a) : F]$$

is infinite. In particular, we conclude all finite extensions are algebraic. On the other hand, there are algebraic extensions that are not finite; however, one trick often used in the theory of algebraic fields is a kind of 'compactness'; statements about algebraic extensions can often be reduced to the study of their finite extensions. In particular any element of an algebraic extension is contained in a finite subextension.

Theorem 1.2. *If E/F is an extension, and $\{u_i\}$ is a basis for E over F, and each u_i is algebraic over F, then E/F is algebraic.*

Proof. Given any $a \in E$, there exists $u_{i_1}, \ldots, u_{i_n}$ in the basis such that $a \in F(u_{i_1}, \ldots, u_{i_n})$. But by induction one can verify that $[F(u_{i_1}, \ldots, u_{i_n}) : F]$ is finite (if u_{i_j} has degree m_j for each $j \in \{1, \ldots, n\}$, then the tower formula verifies that $F(u_{i_1}, \ldots, u_{i_n})$ has degree at most $m_1 \ldots m_n$). Thus a is contained in a finite extension and is therefore algebraic. □

Example. *$\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbf{Q}$, so every element of the form*

$$1 + a\sqrt{2} + b\sqrt{3} + c\sqrt{6}$$

for $a, b, c \in \mathbf{Q}$ is algebraic over $\mathbf{Q}$, because $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$ is algebraic.

Theorem 1.3. *If E/F is an extension, then the set of algebraic elements in E forms an algebraic subextension of E/F.*

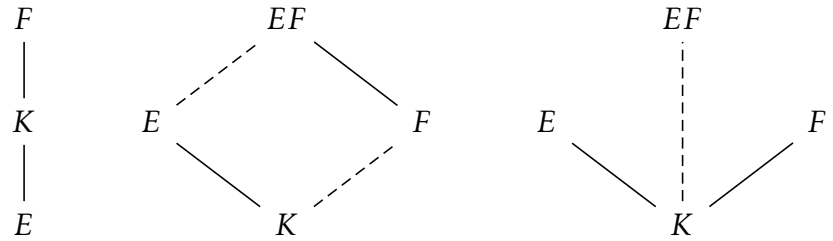
Proof. If a and b are algebraic, then $F(a, b)/F$ is a finite extension, hence algebraic, so $a + b$, ab, and if $a \neq 0$, a^{-1} are all algebraic over E. □

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

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

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

One summarizes the properties using Hasse diagrams.



Note that (3) follows from (1) and (2). It is easy to see that the class of finite extensions is distinguished. So too is the class of algebraic extensions.

Theorem 1.4. *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 F/K and K/E 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's verify the lifting property. Let E/K be an algebraic extension. The set of elements in EF algebraic over F is a field containing E and F, since $F \subset K$, which implies that every element of EF is algebraic over F. □

1.2 Constructible Numbers

TODO

1.3 Homomorphisms of Extensions

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 over the same field F is a morphism of extensions – a ring homomorphism $f : E \to K$ such that $f(a) = a$ for all $a \in F$. Such a map is a F-linear map, so that $[E : F]$ is an isomorphism invariant of these families of homomorphisms.

The existence of certain morphisms of extensions is incredibly important to Galois theory, for they begin to unveil the symmetries of certain fields, in particular, relating the symmetries of roots of a polynomial. Given a morphism of fields $F : K \to L$ and a polynomial $f \in K[X]$, we let $F_* f \in L[X]$ be the polynomial obtained by swapping all coefficients in f with their image under F. This is a ring morphism from $K[X]$ to $L[X]$.

Lemma 1.5. *Let $F : K \to L$ be a field morphism, and consider a simple algebraic extension $K(a)$, where a has minimal polynomial f. Then F extends to a map from $K(a)$ to L if and only if $F_* f$ has a root in L. The number of possible extensions is equal to the number of unique roots of $F_* f$.*

Proof. It is clear that any extension of F must map a root of f onto a root of F_*f. Given any root b of F_*f in L. Consider the sequence

$$K[x] \to L[x] \to L$$

where the first map is induced by F, and the second induced by evaluation at b. Since the kernel of evaluation at b contains F_*f, we obtain an induced sequence

$$K(a) \cong K[x]/(f) \to L[x]/(F_*f) \to L$$

and following through this sequence shows that a is mapped to b under this morphism. □

Corollary 1.6. *Suppose $F(a)/F$ and $F(b)/F$ are two simple extensions. If a and b have the same minimal polynomial over F, then $F(a)/F \cong F(b)/F$.*

We view adding $\sqrt[3]{2}$ to $\mathbf{Q}$ to solve the equation $X^3 - 2$ as more natural than adding $\omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$, where ω is a third root of unity. However, $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\omega\sqrt[3]{2})$ are isomorphic. Thus adding a root is independant of *which* root we add.

Corollary 1.7. *Every endomorphism $f : E/K \to E/K$ of algebraic extensions is automatically an automorphism.*

Proof. We know every field morphism is injective. Furthermore, we know every K morphism maps roots of a polynomial onto itself. Since this set of roots is finite, this morphism just permutes the roots of the polynomial. In particular, if $x \in E$ is algebraic, it is the root of some polynomial g, and is therefore $f(y)$ for some other root y of g. □

Remark. This argument fails for trancendental extensions. For instance, the endomorphism of $K(x)$ fixing K and mapping x to x^2 is not surjective.

1.4 Algebraic Closure

In terms of looking at polynomial equations, the nicest fields are *algebraically closed*, that is, if every non-constant polynomial 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 K has a unique algebrically closed algebraic, known as the *algebraic closure* of K.

Lemma 1.8. *For any polynomial $f \in K[X]$, there is an algebraic extension L/K in which f has a root.*

Proof. Assume, without loss of generality, that f doesn't have a root in K. Then we may write $f = gh$, where g is irreducible, and has no root. Then (g) is maximal, and $L = K[X]/(g)$ 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 $g(X) = 0$ in L, so g has a root in L. □

Theorem 1.9. *Every field has an algebraic closure.*

Proof. We shall apply the elementary theory of first order logic. The theory of fields is a first-order theory. A field is simply a normal model of this theory. Given a field F, enlarge the language of the theory of fields to contain all elements of F as constants, and to add the additional axioms which force the constants to behave exactly like they behave in F. That is, we add the axioms $a + b = c$ and $ab = c$ whenever these equations hold in F. This new theory is still consistant, for it has a model. For each $a_1, \ldots, a_n \in F$, consider the statement

$$(\exists x : a_1 x + a_2 x^2 + \cdots + a_n x^n = 0)$$

We have verified that, if we add a single one of these statements to the theory of fields, the theory remains consistant, for we may find an extension of F in which such an x exists. By induction, we may find a field such that any finite subset of these statements holds. Applying the compactness theorem of first order logic, we find a field F_1, with $F \subset F_1$, such that for any polynomial $f \in F[X]$, there is $a \in F_1$ with $f(a) = 0$. We may clearly shrink F_1 so that it is also algebraic. Now proceed inductively, forming

$$F \subset F_1 \subset F_2 \subset \ldots$$

If $F^{(k+1)} = F^{(k)}$ for any k, then $F^{(k)}$ is an algebraic closure of F. Otherwise, we take the union of all $F^{(k)}$. It is certainly a field, for it is closed under finitary operations, and any polynomial over the union has only finitely many coefficients, hence lies in some $F^{(k)}[X]$ and hence has a root. □

Remark. It turns out that F_1 is always equal to the algebraic closure of F, but it is much more simple to pretend it isn't, and consider the argument above, even though it is technically redundant. It requires some rather advanced Galois theory to show that algebraic extensions F/E which contain all roots of $E[X]$ are algebraically closed.

An alternative proof might be to consider the class of all algebraic extensions of some field, and then take some maximal element, i.e. by Zorn's lemma. The obvious application of this lemma fails, because to apply the lemma you would have to work over the class of all fields, and Zorn's lemma cannot apply to classes (For instance, we could then apply Zorn's lemma on the class of all sets to conclude that there is a largest set X, which would have to be the universe, and it is impossible for this to be a set). Nonetheless, it is a simple cardinality argument to verify that, if the algebraic closure of a field F existed, then it's cardinality would be the same as $F[X]$, so that we could instead apply Zorn's lemma to fields whose elements are contained in $F[X]$, and this application would be logical.

Theorem 1.10. *Let K/E be an algebraic extension. If $f : E \to L$ is an embedding of E in an algebraically closed field, then f extends to an embedding of K. If E is an algebraic closure, and L is algebraic over $f(E)$, then the extension 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 1.11. *Any two algebraic closures of a field are isomorphic.*

1.5 Splitting Fields and Normal Extensions

A field extension F/E *splits* a polynomial $f \in E[X]$ if f splits into linear factors in $F[X]$. The *splitting field* of f in F/E is the smallest subextension which splits f. That is, if we write

$$f = (X - t_1) \dots (X - t_n),$$

then $F = E(t_1, \dots, t_n)$. The degree of $[F : E]$ is less than or equal to $n!$, for the first root adds degree n to the polynomial the second a degree of at

most $n-1$, the second $n-2$, and so on. A splitting field always exists, since we may always take a subfield of the algebraic closure generated by the roots in the closure.

Example. $\mathbf{R}$ *splits* X^2-2 *over* $\mathbf{Q}$. *A splitting field is* $\mathbf{Q}(\sqrt{2})$, *which is a degree two extension over* $\mathbf{Q}$.

Example. *Consider* $X^3+X+1 \in \mathbf{Z}_2[X]$. *We have a degree 3 extension* $\mathbf{Z}_2(i)$ *of* $\mathbf{Z}_2$, *where* i *is a formal number satisfying*

$$i^3+i+1=0.$$

We may then write

$$X^3+X+1=(X+i)(X+i^2)(X+i+i^2)$$

Thus $\mathbf{Z}_2(i)$ *splits* X^3+X+1 *and so the splitting field has degree three.*

Example. *Let* n *be an integer, let* K *be a field, and consider the polynomial* X^n-1 *in* $K[X]$. K *always contains one root to this polynomial, namely* 1, *so*

$$X^n-1=(X-1)(1+X+\cdots+X^{n-1}).$$

The set of roots to this polynomial form a group $\mu_n[K]$ *of roots of unity. There can be at most* n *such roots, so* $\mu_n[K]$ *is a finite subgroup of* K^*, *hence* $\mu_n[K]$ *is cyclic. if* K *splits* X^p-1, *then a generator for* $\mu_n[K]$ *is known as a* primitive n'th root of unity. *If* $1+X+\cdots+X^{n-1}$ *is irreducible in* $K[X]$, *then it's splitting field has degree* $n-1$. *This is the case, for instance, when* n *is a prime, and* $K=\mathbf{Q}$, *since one can apply Eisenstein's criterion to verify irreducibility.*

Example. *The field* $\mathbf{C}$ *splits* X^5-2. *If* ω *is a 5th root of unit, then the roots of* X^5-2 *are*

$$\sqrt[5]{2}, \omega\sqrt[5]{2}, \omega^2\sqrt[5]{2}, \omega^3\sqrt[5]{2}, \omega^4\sqrt[5]{2}$$

And therefore a splitting field of the polynomial is

$$\mathbf{Q}(\sqrt[5]{2}, \omega\sqrt[5]{2}, \omega^2\sqrt[5]{2}, \omega^3\sqrt[5]{2}, \omega^4\sqrt[5]{2}) = \mathbf{Q}(\sqrt[5]{2}, \omega).$$

Now $[\mathbf{Q}(\sqrt[5]{2}):\mathbf{Q}]=5$ *since* X^5-2 *is an irreducible polynomial by Eisenstein's criterion. And* $[\mathbf{Q}(\sqrt[5]{2},\omega):\mathbf{Q}(\sqrt[5]{2})]=4$ *since the minimal polynomial of* ω *is*

$X^4 + X^3 + X^2 + X + 1$; *there are certainly no linear factors of this polynomial in* $\mathbf{Q}(\sqrt[5]{2})$. *Suppose we had quadratic factors, and we could write*

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d).$$

Then

$$a + c = b + ac + d = ad + bc = bd = 1$$

Let us eliminate c using the equation $c = 1 - a$. *Thus we obtain the equivalent set of equations*

$$a + b + d = 1 + a^2, \quad ad + b = 1 + ab, \quad \text{and} \quad bd = 1.$$

Eliminate d with the equation $bd = 1$, *obtaining the equations*

$$(1 + a^2)b = (a + b)b + 1 \quad \text{and} \quad b(b - 1) = a(b - 1)(b + 1).$$

From the second equation, we conclude that either $b = 1$, *or* $b = a(b + 1)$. *If* $b = 1$, *the first equation reads* $a^2 - a - 1 = 0$, *and* $\mathbf{Q}$ *contains no solutions to this equation, giving a contradiction. Conversely, if* $b = a(b + 1)$, *then we can eliminate a from the first equation, so that it reads*

$$b^4 - 3b^2 - 2b - 1 = 0.$$

The rational root test applied to this equation implies $b \in \{\pm 1\}$. *But neither* $+1$ *nor* -1 *satisfy this equation, which completes the proof that the equation is irreducible. Thus we have*

$$\left[\mathbf{Q}\left(\sqrt[5]{2}, \omega\right) : \mathbf{Q}\right] = \left[\mathbf{Q}\left(\sqrt[5]{2}, \omega\right) : \mathbf{Q}\left(\sqrt[5]{2}\right)\right]\left[\mathbf{Q}\left(\sqrt[5]{2} : \mathbf{Q}\right)\right] = 5 \cdot 4 = 20$$

and this is the degree of the splitting field of the polynomial.

The next theorem is simple to show from the fact that algebraic closures of a field are isomorphic, but it is nice to approach things from a finitary perspective to obtain a new perspective.

Theorem 1.12. *Let* $F : E \to F$ *be an isomorphism. If* K/E *is a splitting field of* $f \in E[X]$, *and* L/F *a splitting field of* $F_* f$, *then* $K \cong L$.

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

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

Now suppose $[K : E] > 1$. Then f has an irreducible monic factor g. The morphism F extends to an isomorphism F_* between $E[X]$ and $F[X]$. Since K is a splting field of f, then we may write, for $u_i \in K$, $v_i = F(u_i)$,

$$f = (X - u_1)\dots(X - u_n) \qquad g = (X - u_1)\dots(X - u_m)$$

and

$$F_*f = (X - v_1)\dots(X - v_m) \qquad F_*g = (X - v_1)\dots(X - v_m).$$

The irreducibility of g 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

$$[K : E(u_1)] = \frac{[F : E]}{[E(u_1) : E]} < [F : E].$$

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 F_*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 1.13. *If F/E is a finite 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 1.14. *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^{a}. Then there is an embedding $f : K/E \to F^{\mathrm{a}}/E$. 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 1.15. *If F/E is normal, every morphism $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$.*

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

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

where $a_i \in F$. Now $F_* f = f$, and $f(\sigma(x)) = 0$, which implies $\sigma(x) \in F$. □

Theorem 1.16. *If F/E is an extension for which every $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$, then F/E is normal.*

Proof. Let $f(x) = 0$, for $f \in E[X]$, $x \in F$. 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 f splits into linear factors. □

Corollary 1.17. *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 $\sigma(x)$ is a root of P, so $\sigma(x) \in F$. 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 $f_x \in E[X]$. Then $f_x(x) = 0$, so F splits f_x. But this implies exactly that F is the splitting field of $\{f_x : x \in F\}$. □

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.*

Normality is not distinguished, yet it is preserved over some relations.

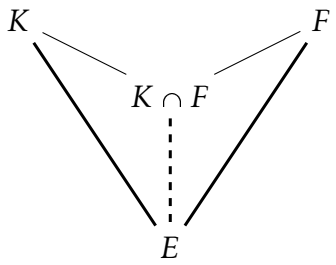
Theorem 1.18. *If $K \subset E \subset F$, and if F/K is normal, then F/E is normal.*

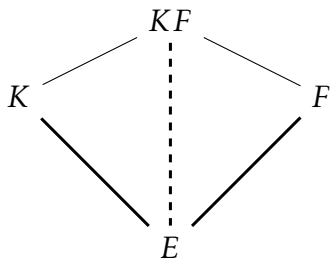
Proof. For if F is a splitting field for a family of polynomials in $K[X]$, then F is a splitting field for a family of polynomials in $E[X]$. □

Theorem 1.19. *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 $\mathcal{F} \cup \mathcal{G}$. Let f embed $K \cap F$ in $E^{\mathfrak{a}}$. Then f extends to isomorphisms from K and F into $E^{\mathfrak{a}}$. Since K and F are normal, $f(K \cap F) \subset f(K) \subset K$, and $f(K \cap F) \subset f(F) \subset F$, hence $f(K \cap F) \subset K \cap F$. □

This theorem can be summed up in diagrams, if we let bold lines stand for normal extensions.





These diagrams will become more and more useful when we analyze Galois groups of extensions.

1.6 Separability

When we analyze the splitting field of a polynomial, we shall find that it is nice to assume that the polynomial has no multiple roots. The reason for this is simple – we have seen that roots of polynomials give rise to automorphisms of the field, and so multiple roots in a polynomial remove the amount of automorphisms a field can have.

Of course, if we may split a polynomial f into linear factors

$$f = (X - r_1)\dots(X - r_n)$$

it is a rather simple procedure to check whether the polynomial has multiple roots. But there is a more simple procedure that does not require the algebraic closure at all. Consider the ring $K[X, dX]$ of formal equations in X and dX. The correspondence $X \mapsto X + dX$ gives a homomorphism from $K[X]$ to $K[X, dX]$. Given any $f \in K[X]$ we may write

$$f(X + dX) = \sum_{i=0}^{n} f_i(X) dX^i.$$

for some polynomials $f_i \in k[X]$. If we work 'to a first approximation' (Rigorously, we switch to the quotient by the ideal generated by dX^2, so that '$dX^2 = 0$'), then

$$f(X + dX) = f(X) + f'(X)dX.$$

We define the derivative of f to be f'. By working to first approximations, it is easy to see that this map is linear, and satisfies the Leibnitz rule

$$(fg)' = f'g + fg'.$$

Since modulo dX^2,

$$\begin{aligned}(fg)(X + dX) = (f(X) + f'(X)dX)(g(X) + g'(X)dX) = (fg)(X) \\ + [(f'g)(X) + (fg')(X)]dX.\end{aligned}$$

We call a linear map $D : R \to R$ between rings a **derivation** if it satisfies the Leibnitz rule. There is an explicit formula for this derivation, which should already be very familiar. If $f = \sum a_i X^i$, then

$$f(X + dX) = \sum_{i=0}^{n} a_i (X + dX)^i = \sum_{j \leqslant i} a_i \binom{i}{j} X^j dX^{i-j}.$$

So in turn,

$$f'(X) = \sum_{i=0}^{n} a_i \binom{i}{i-1} X^{i-1} = \sum_{i=0}^{n} i a_i X^{i-1}.$$

Thus analytic differentiation in $\mathbf{R}[X]$ is extended to algebraic differentiation in general rings. We shall use this method as a test of whether a polynomial has multiple roots.

Proposition 1.20. *A polynomial $f \in K[X]$ has a multiple root a if and only if a is a common root of both f and f'.*

Proof. Suppose that

$$f = (X - a)^2 g$$

Then $f(a) = 0$ and $f'(a) = 0$. Conversely, suppose that $f'(a) = f(a) = 0$. Then we may write

$$f = a_1(X - a) + a_2(X - a)^2 + \cdots + a_n(X - a)^n$$

which implies

$$f'(X) = a_1 + 2a_2(X-a) + \cdots + na_n(X-a)^{n-1}$$

Since $f'(X) = 0$, $a_1 = 0$, so

$$f(X) = (X-a)^2 \left(\sum_{k=2}^{n} a_k (X-k)^{k-2} \right)$$

so a is a multiple root of f. □

Theorem 1.21. *If $f \in K[X]$ satisfies $f' = 0$, then*

1. *If K is a field of characteristic zero, then f is constant.*
2. *If K has characteristic $p > 0$, then $f = \sum_{n \geqslant 0} a_n X^{np}$*

Proof. The characteristic case is obvious. If $P = \sum a_n X^n$, then $na_n = 0$ for all n. If $p \nmid n$, and $a_n \neq 0$, then $na_n \neq 0$, so we must have $a_n = 0$. This shows that P has the form required. □

Corollary 1.22. *All irreducible polynomials in a field of characteristic zero do not have multiple roots.*

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 $F^{\mathfrak{a}}$ which fix E. 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 $[F:E]_s = [F:E]$. This is well defined regardless of which closure we pick, for if $K/F \cong E/F$, and L/F is a particular extension, then $\mathrm{Mor}(L/F, K/F)$ is bijective with $\mathrm{Mor}(L/F, E/F)$.

Example. *Consider a simple extension $E(a)$, with minimal polynomial f. In $F^{\mathfrak{a}}$, write*

$$f = (X-b_1)\ldots(X-b_n)$$

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

Theorem 1.23. *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 the set of all embeddings of K into $L^{\mathfrak{a}}$ which fix F. Then, for each π_i, generate embeddings ψ_{ij} which extend π_i. We contend these are all such embeddings of L in $L^{\mathfrak{a}}$ which fix F, because if γ is any embedding of L which fixes F, then $\gamma|_K$ embeds K and fixes F, so γ is an extension of some π_i. We claim that for each i, there are $[L:K]_s$ extensions ψ_{ij} of π_i. This is certainly true of the identity map, which we will assume to be π_1. But then if γ is any particular extension of π_i, then $\psi_{1j} \circ \gamma$ is a family of $[L:K]_s$ extensions of π_i. These are all such extensions, for if λ is any extension of ψ_i, then $\lambda \circ \gamma^{-1}$ fixes F, and hence is one of ψ_{1j}.

If $[L:F]$ is finite, we may consider a tower

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

And we know that

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

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

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

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

Corollary 1.24. *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 extension of E. 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 $K^{\mathfrak{s}}$. It can also be described as all $a \in K^{\mathfrak{a}}$ whose minimal polynomials over K are separable.*

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 of E. 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 L 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 1.25. *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 a finite field, then the theorem is trivial, since we know that the multiplicative group of a finite field is cyclic. Thus we may assume E is an infinite field.

Suppose $E = K(\alpha, \beta)$, and there are finitely many fields between K and E. Then we have an infinite number of fields of the form $K(\alpha + a\beta)$, for $a \in E$. Thus

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

for some $a, b \in E$. But then

$$(a - b)\beta \in K(\alpha + a\beta)$$

Hence $\beta \in K(\alpha + a\beta)$, and thus α is as well. We may then proceed inductively to prove the theorem for any finite extension.

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, and the number of fields between K and E is finite. □

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

Proof. We address the characteristic zero case, for the cyclicity of units in other characteristics makes the theorem trivial. 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 $P(c) \neq 0$, and thus 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 convenient to discuss *perfect fields*, which are fields in which every irreducible polynomial is separable. This is equivalent to saying every finite extension is separable, or that every irreducible polynomial in the field is separable.

Example. *Every field of characteristic zero is perfect.*

Example. *Consider the polynomial $X^2 + T$ in the field $\mathbf{F}_2(T)$. Let $S \in \mathbf{F}_2(T)^{\mathfrak{a}}$ be such that $S^2 = T$. Then $X^2 + T = (X + S)^2$. Thus $\mathbf{F}_2(T)$ is not a perfect field, since the extension $\mathbf{F}_2(S)/\mathbf{F}_2(T)$ is not a separable extension.*

Thus we conclude that there are some non perfect fields, but they must have nonzero characteristic. The fundamental problem which causes inseparable extensions is the 'freshman's dream' property of fields of finite characteristic. Let $p > 0$ be the characteristic of a field K. Then

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Since p is prime, p divides $\binom{p}{k}$ for $k \neq 0, p$. Thus

$$(a + b)^p = a^p + b^p$$

Similarily, $(ab)^p = a^p b^p$, and $1^p = 1$. Thus the map $a \mapsto a^p$ is a field endomorphism, known as the *Frobenius Endomorphism*. A fundamental question of a field is whether this endomorphism is surjective. It certainly is in the case in $\mathbf{F}_p$, or in general any finite field, since every injective map is surjective. Fix a field K of characteristic p.

Lemma 1.27. *The polynomial $X^p - a$ is either irreducible, or $X^p - a = (X - b)^p$ for some $b \in K$ with $b^p = a$.*

Proof. If $X^p - a$ has a root b in the splitting field $X^p - 1$, then $b^p = a$, and

$$X^p - a = X^p - b^p = (X - b)^p$$

Therefore, if we can write $X^p - a = fg$, where f and g are non-trivial, then for some k,

$$f = (X - b)^k \qquad g = (X - b)^{p-k}$$

and we find that $b^k \in K$. But since $b^p = a \in K$, there are integers n and m such that $nk + mp = 1$, and then

$$(b^k)^n (b^p)^m = b^{nk+mp} = b \in K$$

so K splits $X^p - a$. □

Proposition 1.28. *K is perfect if and only if $K^p = K$.*

Proof. Suppose $K^p = K$. Let $f \in K[X]$ be an irreducible polynomial. Then there exists n and an irreducible polynomial $g \in K[X]$ such that $f(X) = g(X^{p^n})$ with $g' \neq 0$. Write $g = a_0 + a_1 X^{p^n} + \cdots + a_m X^{p^n m}$. For each $i \in \{0, \ldots, m\}$, we can find $b_i \in K$ such that $b_i^{p^n} = a_i$. Then

$$f = b_0^{p^n} + b_1^{p^n} X^{p^n} + \cdots + b_m^{p^n} X^{p^n m} = (b_0 + b_1 X + \cdots + b_m X^m)^{p^n}.$$

Since f is irreducible in $K[X]$, it follows that $n = 0$. Thus $f = g$, so $f' \neq 0$, and this implies all roots of f are distinct.

Conversely, suppose $K^p \neq K$. Pick $a \in K - K^p$. Then $X^p - a$ has only a single root in it's splitting field; if α is any root, then $X^p - a = (X - \alpha)^p$. Whatmore, $X^p - a$ is an irreducible polynomial in $K[X]$, since any proper factor must be of the form $(X - \alpha)^k$ for some $k \leqslant p$, which implies $\alpha \in K$. Thus K is not perfect. □

Remark. In particular, by trivial combinatorics it follows that every finite field is perfect.

1.7 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 easily generalized.

Theorem 1.29. *A finite multiplicative subgroup of a field is cyclic.*

Proof. Let G be a subgroup of F^*, 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* $\mathbf{C}^*$ *are the n'th roots of unity. The only finite subgroup of* $\mathbf{R}^*$ *is the trivial group and* $\{-1, 1\}$. *The only finite subgroup of* $\mathbf{F}_p^*$ *is* $\mathbf{F}_p$ *itself.*

Corollary 1.30. *Every extension* F/K *where* F *is finite and* K *is a finite field is simple.*

Corollary 1.31. *Every finite extension of a finite field is normal and separable.*

1.8 Inseparability

We shall now investigate the ways that inseparability can occur in fields of positive characteristic.

Theorem 1.32. *The roots of an irreducible polynomials all have the same multiplicity (in the characteristic zero case, we know the multiplicity is one).*

Proof. Let $P \in K[X]$ be an irreducible polynomial, which is, without loss of generality, monic. Factor P in $K^{\mathfrak{a}}$,

$$P = (X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r}$$

There are embeddings σ_j of $K(\alpha_1)$ in $K^{\mathfrak{a}}$ which map α_1 to α_j for each j. But then $P^{\sigma_j} = P$, and we see that $m_1 = m_2 = \cdots = m_r$. □

The next theorem shows, in fact, that each multiplicity must be a power of the characteristic of the field. Over $\mathbf{Q}$, coefficients tend to accumulate because we cannot quotient out coefficients which eventually contain a prime number. Thus inseparability is a direct result of working over a field with characteristic p, because

$$(X - a)^p = X^p - a^p$$

so taking a polynomial to a power of the field causes many coefficients to vanish, so a single root may be taken to such a power that it becomes an element of the base field. This is both a boon and a curse when working with fields of positive characteristic.

Theorem 1.33. *If* $K(\alpha)$ *is inseparable over* K *with characteristic* $p > 0$, *then*

$$[K(\alpha) : K] = p^{\mu}[K(\alpha) : K]_s$$

for some non-negative integer μ.

Proof. Let $P = \mathrm{Irr}(K, \alpha)$. If P is inseparable, then $\gcd(P, P')$ is not a unit, implying $P \mid P'$, which is only possible if $P' = 0$. Thus we may write $P = Q_0(X^p)$, where

$$Q_0 = a_0 + a_1 X + \cdots + a_n X^n$$

Thus α^p is a root of Q_0, a polynomial whose degree is smaller than P. If Q_0 is not separable, then we find α^{p^2} is a root of some Q_1 whose degree is smaller than Q_0. By infinite descent, we must be able to find a smallest μ such that α^{p^μ} is a root of a separable polynomial Q. Then $P = Q(X^{p^\mu})$, so

$$\deg(Q) = \deg(P)/p^\mu = np^{1-\mu}$$

and we find, since Q and P are irreducible polynomials, that

$$[K(\alpha) : K(\alpha^\mu)] = \frac{[K(\alpha) : K]}{[K(\alpha^\mu) : K]} = \frac{np}{np^{1-\mu}} = p^\mu$$

Since Q is separable, we know $[K(\alpha^{p^\mu}) : K]_s = [K(\alpha^{p^\mu}) : K]$. Furthermore, since Q has as many roots as P, we see $[K(\alpha) : K]_s = [K(\alpha^{p^\mu}) : K]_s$. But then, by the tower formulas,

$$[K(\alpha) : K] = [K(\alpha) : K(\alpha^{p^\mu})][K(\alpha^{p^\mu}) : K] = p^\mu [K(\alpha^{p^\mu}) : K]_s = p^\mu [K(\alpha) : K]_s$$

And we have found the p^μ we wanted. □

By induction, if K/E is a finite extension, then we may write

$$[K : E] = [K : E]_i [K : E]_s$$

For some integer $[K : E]_i$, which is a power of the characteristic of E. We call $[K : E]_i$ the **degree of inseparability**. Since the degree and the separable degree are multiplicative, we have

$$[K : E]_i = \frac{[K : E]}{[K : E]_s} = \frac{[K : F][F : E]}{[K : F]_s [F : E]_s} = [K : F]_i [F : E]_i$$

so the inseparable degree is multiplicative.

We now introduce the gnarliest inseparable fields.

Theorem 1.34. *Let K/E be an algebraic extension of fields of characteristic $p > 0$. The following are equivalent.*

1. $[K : E]_s = 1$.
2. *For any* $a \in K$, *there is* n *such that* $a^{p^n} \in E$.
3. *For any* $a \in K$, $Irr(E, a) = X^{p^n} - y$ *for some integer* n, *and* $y \in E$.
4. K *has a basis* $\{\alpha_i\}$, *where each* α_i *has* n_i *such that* $\alpha_i^{n_i} \in E$.

If K/E *satisfies these properties, it is known as a* **purely separable extension**.

Proof. $(1 \Rightarrow 2)$: If $[K : E]_s = 1$, then $[E(\alpha) : E]_s = 1$ by multiplicative properties. In $K^{\mathfrak{a}}$, we may write

$$\mathrm{Irr}(E, \alpha) = (X - a)^{rp^n}$$

for some non-negative n, and r such that p does not divide r. If $r = 1$, we find $a^{p^n} \in E$. If $r \neq 1$, take the second lowest coefficient in the expansion, from which we conclude that $ra^{p^n} \in E$, hence $a^{p^n} \in E$, contradicting the fact that k is the smallest integer for which $(X - a)^k$ is a polynomial in $E[X]$.

$(2 \Rightarrow 3)$: The irreducible polynomial of each $a \in K$ must divide a polynomial of the form

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

and is therefore of the form $(X - a)^k$ for some integer k. Write $k = rp^n$, where r does not contain any factor of p. Then

$$(X - a)^k = (X - a)^{rp^n} = (X^{p^n} - a^{p^n})^r = \sum_{k=0}^{r} \binom{r}{k} a^{r-k} X^k$$

If $r \neq 1$, take the second lowest coefficient in the expansion, from which we conclude that $ra^{p^n} \in E$, hence $a^{p^n} \in E$, contradicting the fact that k is the smallest integer for which $(X - a)^k$ is a polynomial in $E[X]$.

$(4 \Rightarrow 1)$: We know $[E(\alpha_i) : E]_s = 1$, since the minimal polynomial has only a single root, so there is a unique way to embed α_1 into $E^{\mathfrak{a}}$. If two embeddings ψ and π are different, they must differ at some α_i. But this is clearly impossible. □

Corollary 1.35. *If* K/E *is a finite, purely inseparable extension, then* $[K : E]$ *is a power of the characteristic.*

A purely inseparable extension is the perfect intersection of primehood. We are working over a characteristic p, in a field whose degree is a power of p, which is obtained by adding roots from polynomials all have roots whose power is the same multiplicity. This perfect intersection of primes is what causes the rigidity of embeddings into the algebraic closure of the field.

Lemma 1.36. *The class of purely inseparable extensions is distinguished.*

Proof. The tower property is clear from the multiplicative property of the degree of inseparability. The lifting property is clear from property four which defines a purely inseparable extension. If E/K is a purely inseparable extension, then $E = K(\alpha_1, \ldots, \alpha_n)$, where each α_i is purely inseparable. Then $EF = F(\alpha_1, \ldots, \alpha_n)$, and each α_i is purely inseparable over F. □

Theorem 1.37. *If E/K is an algebraic extension, let F be the largest separable extension of E between K and E (the compositum of all separable extensions). Then E/F is a purely inseparable.*

Proof. If α in an inseparable element of E with respect to F, then for some n, α^{p^n} is separable. But then α is purely inseparable over K. Hence E is purely inseparable over K. □

Corollary 1.38. *A separable and purely inseparable extension K/E is only possible if $K = E$.*

Proof. For then $1 = [K : E]_s = [K : E]$. □

Theorem 1.39. *If K/E is normal, and F is the maximal separable subextension, then F/E is normal.*

Proof. Every embedding σ of K into $K^{\mathfrak{a}}$ satisfies $\sigma(K) \subset K$. If π embeds F in $K^{\mathfrak{a}}$, then π extends to a unique embedding of K in $K^{\mathfrak{a}}$. Since $\pi(F)$ is separable, hence $\pi(F) \subset F$. □

Chapter 2

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)

Here we introduce the fundamental trick to Galois theory. Given a field extension F/E, we study the automorphism group $\mathrm{Aut}(F/E)$. Understanding the structure of these groups corresponds to understanding the relations between elements of the extension. If F/E is a normal, separable extension, then we say the extension is *Galois*, in which case the automorphism group is even more closely connected to the space, denoted by $\mathrm{Gal}(F/E)$. The separability condition of the space ensures we have enough automorphisms into the algebraic closure, and the normality condition ensures that these actually are automorphisms into the space we are studying.

Example. *$Gal(\mathbf{C}/\mathbf{R}) \cong \mathbf{Z}_2$, because there are two automorphisms of $\mathbf{C}$ over $\mathbf{R}$, the identity $z \mapsto z$, and the conjugation $z \mapsto \overline{z}$. One may argue explicitly that conjugation is an automorphism, or instead use the fact that i and $-i$ both have the same minimal polynomial over $\mathbf{R}$. That these are all automorphisms follows because $\mathbf{C}$ is the splitting field of $X^2 + 1$ in $\mathbf{R}$. Every automorphism of $\mathbf{C}$ which fixes $\mathbf{R}$ is determined by how it maps i, and we must map i either to itself or to $-i$.*

Example. *The Galois group might not behave how you think it will.* $\mathbf{R}/\mathbf{Q}$ *is an infinite dimensional extension, yet* $Gal(\mathbf{R}/\mathbf{Q})$ *is trivial. Let* σ *be an automorphism of* $\mathbf{R}$*. If* $x \in \mathbf{R}$ *is positive, then* $x = y^2$ *for some* $y \in \mathbf{R}$*, and then this implies* $\sigma(x) = \sigma(y)^2$ *is positive. Thus* σ *is order preserving, hence continuous, and thus fixes all of* $\mathbf{R}$ *since* $\mathbf{Q}$ *is dense in* $\mathbf{R}$*.*

Example. *Consider the field* $F(X)$ *of rational expressions.* $GL_2(F)$ *acts on* $F(X)$ *via the expression*

$$MP = \frac{M_{11}P + M_{12}}{M_{21}P + M_{22}} \in F(P)$$

This implies MX *generates* $F(X)$ *for each* $M \in GL_2(F)$*, because*

$$X = M^{-1}MX \in F(MX)$$

Let $U \in F(X)$*, and write* $U = P/Q$*, where* P *and* Q *are relatively prime. We contend the polynomial*

$$P - YQ \in F[X, Y]$$

is irreducible, for if it can be written as RS*, then we can assume without loss of generality that* $R \in F[X]$*, and* $S = S_1 + S_2Y$ *with* $S_1, S_2 \in F[X]$*. Then* $RS_1 = P$*, and* $RS_2 = Q$*, which implies* $R \in F$*, for it divides both* P *and* Q*. Thus* $P - YQ$ *cannot be decomposed into proper factors.*

Now $F(X)$ *is algebraic over* $F(U)$*, for* X *is a zero of the polynomial*

$$P(Y) - UQ(Y) \in F(U)[Y]$$

and this polynomial is irreducible, and is thus differs from the minimal polynomial by a non-zero constant. Thus the degree $[F(X) : F(U)]$ *is the maximum of the degrees of* P *and* Q*, and we find* $[F(X) : F(U)] = 1$ *if and only if*

$$U = \frac{aX + b}{cX + d}$$

and $ad - bc \neq 0$ *expresses exactly that the numerator and denominator are relatively prime. Thus the generators of* $F(X)$ *are exactly the* U *of the form above.*

Why did we do all this work? The answer is to calculate Gal $F(X)/F$*. Certainly any automorphism is determined by where it maps* X*, and for any polynomial* $P \neq 0$*, the map* $X \mapsto P$ *extends to an endomorphism* f *of* $F(X)$*. Thus*

we need only find the surjective endomorphisms, and that occurs if and only if P is a generator, because $f(F(X)) = F(f(X))$. Now we switch back to the matrix notation used above. If f_M maps X to MX, then we find $f(P) = P(MX)$, so

$$(f_N \circ f_M)(P) = f_N(P(MX)) = P(MNX)$$

so that the map $M \mapsto f_M$ is a surjective antihomomorphism, whose kernel is the set of matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

with $a \neq 0$, for these are exactly the matrices which fix X. Thus the map

$$M \mapsto f_{M^{-1}}$$

is a surjective homomorphism, establishing an isomorphism of Gal $F(X)/F$ and the projective linear group

$$PGL_2(F) = GL_2(F)/F^*$$

where F^* is seen as the matrices defined above, which are isomorphic to F^*.

Given a G-action on F, we let F^G denote the fixed points of the action,

$$F^G = \{x \in F : (\forall g \in G : gx = x)\}$$

We want to study fields for which $F^{\mathrm{Gal}(F/E)} = E$, so as many elements as possible are 'jigged around'. This is why we restrict ourselves to the Galois extensions.

Theorem 2.1. *Every Galois extension satisfies $F^{Gal(F/E)} = E$.*

Proof. Suppose F/E is normal and separable. Let $x \in F - E$, and let P be the minimal polynomial of x. We know P splits over F, since F/E is normal. We also know $\deg P \geqslant 2$, and since F/E is separable, P has a root $y \neq x$ in F. Thus there is a homomorphism $f : E(x) \to E(y)$ which maps x to y. This extends to a homomorphism $\tilde{f} : F \to E^{\mathfrak{a}}$, and since F/E is normal, $\tilde{f}$ is actually an automorphism of F. □

Given a tower $K \leqslant E \leqslant F$ of fields, $\mathrm{Gal}(F/E)$ can naturally be realized as a subgroup of $\mathrm{Gal}(F/K)$, since every automorphism of F which fixes E must also necessarily fix K.

Lemma 2.2. *If F/K is Galois, then the mapping*

$$E \mapsto Gal(F/E)$$

is injective, from fields between K and F into subgroups of $Gal(F/K)$.

Proof. Let $K \subset E \subset F$ be a tower of fields. Then F/E is a normal, separable extension, so $F^{\mathrm{Gal}(F/E)} = E$. Thus, if E and L have the same Galois group, then

$$E = F^{\mathrm{Gal}(F/E)} = F^{\mathrm{Gal}(F/L)} = L$$

So $\mathrm{Gal}(F/-)$ is injective. □

We denote the map in the proof by $\mathrm{Gal}(F/-)$. In the case of a Galois extension, this map is injective. We shall soon find out that, in the finite dimensional case, the map is surjective.

Proposition 2.3. *Let K/F be a finite separable extension, and let E be the normal closure. Then E/F is finite and separable.*

Proof. Write $K = F[x_1, \ldots, x_n]$. Then K is separable if and only if the polynomials $\mathrm{Irr}(F, x_i)$ are separable. Let $y_i^1, \ldots y_i^{k_i}$ be the roots of $\mathrm{Irr}(F, x_i)$. Then

$$E = F[y_1^1, \ldots, y_1^{k_1}, y_2^1, \ldots, y_2^{k_2}, \ldots, y_n^1, \ldots, y_n^{k_n}]$$

is a splitting field for a family of polynomials, hence normal. It is clearly also separable. Any normal field containing K must contain all the roots of $\mathrm{Irr}(F, x_i)$, so E is clearly the smallest normal extension. Since the order of the Galois group of E/F is equal to $[E : F]$, there are finitely many subgroups of $\mathrm{Gal}(E/F)$, and since each subgroup corresponds to a subfield between F and E, there are only finitely many subfields. □

Corollary 2.4. *There are finitely many fields between a finite, separable extension.*

Proof. For there are finitely fields between the normal closure, since there are finitely many subgroups of the Galois group. □

We already know this is true, as we proved in the course of the primitive element theorem, but it is nice to see another proof.

Lemma 2.5. *If the order of every element of a separable extension E/K is less than or equal to n, then E/K is finite, and $[E:K] \leqslant n$.*

Proof. Let x_1 be an element of E. Inductively find x_i, for $i \in \{1,\dots,n\}$, such that $x_{i+1} \notin K(x_1,\dots,x_i)$. If this is impossible, then E/K is finite, as was required. Otherwise, we find that the degree of $K(x_1,\dots,x_n)$ over K is greater than n. Yet $K(x_1,\dots,x_n)/K$ is separable, and therefore can be written $K(y)/K$ for some element y. But then y has order greater than n. Thus the extension is finite, and $[E:K] \leqslant n$. □

Theorem 2.6 (Artin)**.** *Let K be a field, and G a finite group of automorphisms of K. If $F = K^G$, then K/F is a finite, Galois extension, such that $Gal(K/F) = G$.*

Proof. Fix $x \in K$, and let $\sigma_1,\dots,\sigma_n \in G$ be a maximal set such that $\sigma_i(x)$ are distinct. Then x is certainly a root of

$$\prod_{k=1}^{n} (X - \sigma_i(x))$$

and for all $\tau \in G$, $\tau(\sigma_1(x)),\dots,\tau(\sigma_n(x))$ must be a permutation of the roots, for if the set does not contain some root, we may enlarge this set, meaning our original set was not maximal. Thus all coefficients of the polynomial are fixed by G, and therefore the polynomial lies in $F[X]$. Since the $\sigma_i(x)$ are distinct, x is separable over F. What's more, K therefore contains all roots of $\mathrm{Irr}(F,x)$. Since x was arbitrary, we find K/F is separable and normal, and therefore Galois. Since G is finite, and $[K:F]$ is equal to the order of G, K/F is finite. □

Corollary 2.7. *On a finite Galois extension, $Gal(K/-)$ is a surjective map.*

Proof. The proof above essentially verifies that, in the finite case, the map $G \mapsto K^G$ is the inverse of $\mathrm{Gal}(K/-)$. □

The set of intermediate fields between K and F form a partially ordered set under the $\subset$ relation. Similarily, the set of subgroups of $\mathrm{Gal}(F/K)$ is partially ordered under the subgroup operation $<$. These partially ordered sets form a lattice, since if G and H are groups

$$G \vee H = \langle G, H \rangle = \langle k : k \in G \text{ or } k \in H \rangle \qquad G \wedge H = G \cap H$$

If E and L are fields between K and F, then

$$E \vee L = EL \quad E \wedge L = E \cap L$$

In this manner, the map associating E with $\mathrm{Gal}(K/E)$ is found to be an order-reversing isomorphism. This makes the following proposition obvious.

Proposition 2.8. *If K/F is a Galois extension, and $F \subset E, L \subset K$, then*

$$Gal(K/E \cap L) = \langle Gal(K/E), Gal(K/L) \rangle$$

$$Gal(K/EL) = Gal(K/E) \cap Gal(K/L)$$

The 'Galois' map $\mathrm{Gal}(K/-)$ acts functorially with respect to isomorphisms, in the case that K/L is originally a Galois extension. Let $f : E \to E'$ be an isomorphism in the category of fields, restricted only to those fields which lie between L and K. Then f induces an automorphism from

Theorem 2.9 (The Fundamental Theorem of Galois Theory)**.** *Let E/F be a finite Galois extension. Then the map $L \mapsto Gal(E/L)$ is a order reversing isomorphism between subfields between F and E and subgroups of $Gal(E/F)$, whose inverse is $G \mapsto E^G$, such that*

$$[E : L] = |Gal(E/L)|$$

A group G is normal if and only if its corresponding field extension L is normal, and in this case

$$Gal(L/F) \cong Gal(E/F)/Gal(E/L)$$

Proof. We need only prove the last few tidbits of the proof. Let L/F be a normal extension. Then any $\sigma \in \mathrm{Gal}(E/F)$ satisfies $\sigma(L) = L$, so if $\tau \in \mathrm{Gal}(E/L)$, then $\sigma\tau\sigma^{-1}$ fixes F, and maps L to itself, and is thus an element of $\mathrm{Gal}(E/L)$. so $\mathrm{Gal}(E/L)$ is normal in $\mathrm{Gal}(E/F)$. Conversely, let G be a normal subgroup of $\mathrm{Gal}(E/F)$. Let $\sigma \in \mathrm{Gal}(E/L)$. If there is $x \in L$ such that $\sigma(x) \notin L$, then there is $\tau \in \mathrm{Gal}(E/L)$ such that $\tau(\sigma(x)) \neq \sigma(x)$ (for the extension is Galois), which implies that

$$(\sigma^{-1} \circ \tau \circ \sigma)(x) \neq x$$

contradicting the fact that $\sigma^{-1} \circ \tau \circ \sigma \in \mathrm{Gal}(E/L)$. Thus $\sigma(x) \in L$ for all $x \in L$, and if f is any embedding of L in L^{a} which fixes F, then f extends

to an embedding of E in L^a, which must map E to itself and hence is in $\mathrm{Gal}(E/F)$, so maps L to itself by the above discussion.

The map $\sigma \mapsto \sigma_L$ is a homomorphism from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(L/F)$ when L is normal, and it is surjective by the extension property of automorphisms, so that

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/L)$$

and this concludes the proof of the fundamental theorem. □

Example. *Consider the field $F(X_1,\ldots,X_n)$ of rational functions in n indeterminates, and let S_n act on $F(X_1,\ldots,X_n)/F$ by permuting the indeterminates. This is an embedding of S_n in $Gal(F(X_1,\ldots,X_n)/F)$, which thus corresponds to a finite subgroup G of the Galois group. Let us determine the fixed field $L = F(X_1,\ldots,X_n)^G$, which corresponds to a finite, Galois extension $F(X_1,\ldots,X_n)/L$. Consider the polynomial*

$$Q = (Y - X_1)(Y - X_2)\ldots(Y - X_n) \in F(X_1,\ldots,X_n)[Y]$$

Expand Q to the form

$$Y^n - S_1 Y^{n-1} + S_2 Y^{n-2} + \cdots + (-1)^k S_k Y^{n-k} + \cdots + (-1)^n P_0$$

with $S_i \in F(X_1,\ldots,X_n)$. This polynomial is fixed by G, so

$$F(S_1,\ldots,S_n) \subset L$$

It is clear that $F(X_1,\ldots,X_n)$ is the splitting field of Q over $F(S_1,\ldots,S_n)$, and is a separable extension of $F(S_1,\ldots,S_n)$, since the X_i are distinct. If

$$\sigma \in Gal(F(X_1,\ldots,X_n)/F(S_1,\ldots,S_n))$$

Then $Q^\sigma = Q$, and since $Q^\sigma(X_i^\sigma) = Q(X_i) = 0$, we see σ just permutes the X_i, and is thus in G. But by the Galois correspondence, since $F(S_1,\ldots,S_n) \subset L$, we have $Gal(F(X_1,\ldots,X_n)/L) \subset Gal(F(X_1,\ldots,X_n)/F(S_1,\ldots,S_n))$, so that the two Galois groups are equal. But this implies that $L = F(S_1,\ldots,S_n)$ by the Galois correspondence. Thus every P fixed under permutations of the X_i can be expressed as a rational functions of the S_i.

By a similar technique, suppose we take the subgroup of G corresponding to A_n, and consider the corresponding subfield L. Certainly $F(S_1,\ldots,S_n) \subset L$. Consider the descriminant

$$\Delta = \prod_{i<j} (X_j - X_i)$$

Then $(ij)\Delta = -\Delta$, *so* $\Delta \notin F(S_1,\dots,S_n)$, *but* $\Delta \in L$, *for* $--\Delta = \Delta$. *What's more,* $\Delta^2 \in F(S_1,\dots,S_n)$, *so*

$$L = F(S_1,\dots,S_n,\Delta)$$

For

$$\begin{aligned}[F(S_1,\dots,S_n,\Delta) : F(S_1,\dots,S_n)] &= [F(X_1,\dots,X_n) : F(S_1,\dots,S_n,\Delta)]^{-1} \\ &\quad [F(X_1,\dots,X_n) : F(S_1,\dots,S_n)] \\ &= |S_n|/|A_n| = [S_n : A_n] = 2\end{aligned}$$

so the extension must have degree 2. Thus Δ *somehow corresponds to* A_n.

2.1 Solvability of Radicals

We almost have enough theory to determine the main result of our study of Galois theory. The solutions of the quintic cannot be 'solved by radicals'. Formally, what does it mean to 'solve by radicals'. Before formal mathematics developed the various algebraists used various assumptions of what this means, but with all the theory we've discussed, formal definitions can be explicitly stated. Our definition is of course the one chosen by Galois, for it connects the nicest to Galois theory. A polynomial $P \in K[X]$ is **solvable by radicals** if there is a sequence of fields

$$K \subset K(a_1) \subset K(a_1,a_2) \subset \cdots \subset K(a_1,\dots,a_n)$$

together with $n_i \geqslant 2$ such that $a_i^{n_i} \in K(a_1,\dots,a_{i-1})$, and $K(a_1,\dots,a_n)$ is the splitting field of P. Thus every root of P can be expressed as sums and products of n'th roots of P. The size of the tower details the 'recursion depth' of the formula for the roots. If we have a tower of degree 1, then every root can be expressed $\sum b_i a_1^i$, with $b_i \in K$, and $a_1^{n_i} = c_1 \in K$, then the roots can be expressed 'in radicals' as

$$X = \sum b_i \sqrt[n_1]{c_1}^i$$

conversely, if we have an additional a_2, then every root is of the form $\sum b_{i,j} a_1^i a_2^j$, and if $a_2^{n_2} = \sum d_i a_1^i$, then every root is of the form

$$X = \sum b_{i,j} \sqrt[n_1]{c_1}^i \sqrt[n_2]{\sum d_k \sqrt[n_1]{c_1}^k}^j$$

we notice that working with fields is *much* simpler than working with the formulas themselves, which have as many coefficients as the degree of the splitting field. In the worst case, 5th degree polynomials has degree 120.

Now given a polynomial $P \in K[X]$, define the Galois group of the polynomial to be $\mathrm{Gal}(L/K)$, where L is the splitting field of K.

Chapter 3

Solutions by Radicals

The basic problem of Galois theory is to understand the structure of polynomials via the symmetries of their roots. In particular, we wish to understand why the roots of some polynomials are difficult to find, and how to find roots to polynomials in the easier cases. Primarily, we want to discuss when the roots of polynomials can be solved 'by radicals', i.e. they can be obtained from expressions involving rational numbers and the operations of addition, multiplication, subtraction, division, and most importantly, taking n'th roots. We say such numbers can be 'expressed in radicals'.

One might expect that all algebraic numbers might be expressed by equations of this form; this is true for solutions to polynomials of degree four or less, but there are solutions to polynomial equations of degree five or more which cannot be expressed in radicals, a simple example being the solutions to the polynomial equation $x^5 - x - 1 = 0$. Of course, because of this, there cannot be a general formula in radicals which expresses the roots of a degree five polynomial equation in terms of the coefficients of the polynomial (such equations do exist for degree two, three, and four polynomials).

We begin this chapter by discussing the ad hoc techniques which were discovered around the 16th century to find the roots of quadratic, cubic, and quartic polynomials. We list them here. Later on, Galois theory gives reasons to explain why these techniques work, and why we cannot generalize these techniques to find roots of higher degree polynomials.

3.1 Quadratic Polynomials

Finding the roots of a quadratic polynomial should be familiar from high school algebra. We wish to find values for x such that $x^2 + Bx + C = 0$. In this case, the standard technique is to 'complete the square', reexpressing the polynomial as $(x + B/2)^2 = B^2/4 - C$. Geometrically, this means that applying a translation in the plane, the locus of points in the plane satisfying the equation $y = x^2 + Bx + C$ are translated into the locus of points satisfying $y = x^2$. In other words, every locus of this form is affinely equivalent to the standard convex parabola whose node lies at the origin. Provided that the *discriminant* $\Delta = B^2 - 4C$ is non-negative, we can take the square root of the equation on both sides, and we find

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

If $\Delta > 0$, then we obtain two, distinct real solutions to the equation. If $\Delta < 0$, then the square root will be a complex number, and we obtain two complex solutions which are complex conjugates of one another. If $\Delta = 0$, we get a single, repeated real root.

3.2 The Cubic Formula

Let's up the difficulty a notch. Consider a cubic equation $x^3 + Bx^2 + Cx + D = 0$. Begin by substituting $x = y - B/3$ into the equation (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 a *Tschirnhaus transformation*, which is a general technique to shifting a polynomial equation so that the coefficient corresponding to the term one less than the degree of the polynomial vanishes.

It follows that we need only consider cubics of the form $x^3 + Px + Q = 0$. We proceed in an ad-hoc manner. Consider variables y and z, and write $x = \sqrt[3]{y} + \sqrt[3]{z}$. Then $x^3 = y + z + 3\sqrt[3]{y}\sqrt[3]{z}(\sqrt[3]{y} + \sqrt[3]{z})$. Thus the values of y and

z which result in a solution of the original equation for x are exactly those satisfying $(Q+Y+Z)+(3\sqrt[3]{y}\sqrt[3]{z}+P)(\sqrt[3]{y}+\sqrt[3]{z})=0$. In particular, we may find solutions for y and z by choosing y and z such that $Q+y+z=0$ and $\sqrt[3]{y}\sqrt[3]{z}=-P/3$. A necessary condition for these equations to be satisfied is that $y+z=-Q$, and $yz=-P^3/27$. Thus $y^2=y(y+x)-yz=P^3/27-Qy$, which can be arranged into the quadratic equation $y^2+Qy-P^3/27=0$, so

$$y=\frac{-Q}{2}\pm\sqrt{\frac{Q^2}{4}+\frac{P^3}{27}} \qquad z=\frac{-Q}{2}\mp\sqrt{\frac{Q^2}{4}+\frac{P^3}{27}}$$

and so we obtain *Cardano's formula*

$$x=\sqrt[3]{\frac{-Q}{2}+\sqrt{\frac{Q^2}{4}+\frac{P^3}{27}}}+\sqrt[3]{\frac{-Q}{2}-\sqrt{\frac{Q^2}{4}+\frac{P^3}{27}}}$$

Notice that over the complex numbers, we have 9 choices of cubic roots, which leads to 9 different solutions to the equation! Since we know we can only have three roots, what did we miss? Notice that $3\sqrt[3]{y}\sqrt[3]{z}+P=0$ implies $yz=-P^3/27$, but the converse need not necessarily hold. If α and β are choices of $\sqrt[3]{y}$ and $\sqrt[3]{z}$, then we require that $3\alpha\beta+P=0$. If α and β are chosen with this property, then the other two roots can then be given as $\omega\alpha+\omega^2\beta$ and $\omega^2\alpha+\omega\beta$, where ω is a root of unity. That these are the three solutions can be verified by computing the product

$$(x-(\alpha+\beta))(x-(\omega\alpha+\omega^2\beta))(x-(\omega^2\alpha+\omega\beta))=x^3-3\alpha\beta x-(\alpha^3+\beta^3)$$

and the relations $P+3\alpha\beta=0$ and $\alpha^3+\beta^3+Q=0$ give back the original polynomial. This means that Cardano's formula always give all roots to the cubic equation, though one must be careful to choose the cubic roots carefully in the formula.

Cardano's formula is not nearly as useful as the quadratic formula. For one, simplification of the radical equation is often nontrivial; the polynomial $x^3+3x-36$ has an integer root of $x=3$, but Cardano's formula gives solutions of the form

$$x=\sqrt[3]{18+\sqrt{325}}+\sqrt[3]{18-\sqrt{325}}.$$

Even more weirdly, the polynomial $x^3-15x-4$ has a root of 4, yet Cardano's formula gives roots of the form

$$x=\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}},$$

Rafael Bobelli noticed that $(2\pm i)^3 = 2\pm 11i$, from which we can recover the solution $x = 4$, but this is a strange method of finding roots, and must have looked even stranger to the renaissance mathematicians who had trouble reconciling the use of negative numbers, let alone complex numbers. One can use Galois theory to show that this is unavoidable. There does not exist a formula which expresses the real and imaginary parts of an irreducible cubic in terms of real radicals.

3.3 Viete's Formula For the Cubic

The traditional escape in the case of three real roots is to use trigonometric functions to express the real roots of a cubic polynomial, as discovered by François Viéte, which finds three real roots to the nondegenerate cubic equation $x^3 - Px + Q = 0$ when the *discriminant* $\Delta = 4P^3 - 27Q^2$ is positive. Note that this forces P to be a positive number. For each angle θ,

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

Given a real root x to the equation $x^3 - Px + Q = 0$, set $x = r\cos(\theta)$. We then expand the equation to obtain that $r^3\cos^3(\theta) - rP\cos(\theta) + Q = 0$. The idea is to change coordinates such that we can substitute in the trigonometric identity. If we can find y such that $r^3 = 4y$, and $rP = 3y$, then the equation can be written as

$$y\cos(3\theta) + Q = y(4\cos^3(\theta) - 3\cos(\theta)) + Q = 0.$$

Thus the equation becomes $\cos(3\theta) = -Q/y$, and we can take an arccosine to obtain θ. We note that if $r^3 = 4y$, then $rP = -3y$ is satisfied precisely when

$$rP = 3y = (3/4)r^3.$$

In particular, this implies that, since $r = 0$ does not give a solution since the equation is not reducible, then $r = 2\sqrt{P/3}$. Thus

$$y = r^3/4 = 2\sqrt{P^3/27},$$

and we conclude that

$$\cos(3\theta) = -(Q/2)\sqrt{27/P^3}.$$

The condition that $27Q^2 < 4P^3$ guarantees that the right hand side is less than one, so we can take the arccosine. Thus we conclude that if $k \in \{0, 1, 2\}$, then the quantities

$$2\sqrt{P/3} \cdot \cos\left(\frac{1}{3}\arccos\left(\frac{Q}{2}\sqrt{\frac{27}{P^3}}\right) + \frac{2\pi k}{3}\right).$$

give three distinct real roots to the equation $x^3 - Px + Q = 0$, since the condition $27Q^2 < 4P^3$ implies degenerate cases of this equation cannot occur.

Remark. The discriminant $\Delta = 4P^3 - 27Q^2$ again characterizes the behaviour of the roots of the equation $x^3 - Px + Q$. If $\Delta > 0$, we have seen there are three real solutions. If $\Delta = 0$, then there are three real roots, with one root repeated twice. If $\Delta < 0$, then there is one real root and two complex roots, which are conjugates of one another.

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 (Negative numbers were not commonly accepted at the time), 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 using complex or negative numbers, the solution requires a total of thirteen cases, a testament to the utility of the modern 'formal' approach to arithmetic, confidently applying the complex numbers as if they were real numbers after all.

3.4 Quartic Equations

The Arns Magna also included a solution to the quartic equation, a method of Lodovico Ferrari which enables one to reduce the case to solving a cubic equation. Applying a Tschirnhaus transformation, it suffices to consider roots to the equation $x^4 + Px^2 + Qx + R = 0$. We can write this as

$\left(x^2 + P/2\right)^2 =$. Introduce a new term y, and consider the equation

$$(x^2 + P/2 + y)^2 = 2yx^2 - Qx + P^2/4 - R + y^2$$

Choose y so that the right side is a polynomial in x with a repeated root, which occurs precisely when the discriminant vanishes, i.e.

$$Q^2 = 8y(P^2/4 + y^2 - R)$$

Cardano's formula enables us to find y be an expression in radicals, i.e.

$$y = \sqrt[3]{\frac{Q^2}{16} + \sqrt{\frac{Q^4}{64} + \frac{(P^2/4 - R)^3}{27}}} + \sqrt[3]{\frac{Q^2}{16} - \sqrt{\frac{Q^4}{64} + \frac{(P^2/4 - R)^3}{27}}}$$

But if the expression $2yx^2 - Qx - R + P^2/4$ is a perfect square, then it must be the square of

$$\sqrt{2y}x - \frac{Q}{2\sqrt{2y}}$$

Now we have the equation

$$(x^2 + P/2 + y)^2 = \left(\sqrt{2y}x - \sqrt{2x}\right)^2.$$

Thus

$$x^2 + P/2 + y = \pm(\sqrt{2y}x - \sqrt{2y}).$$

This is a quadratic equation, and so we may write

$$x = \frac{\pm\sqrt{2y}x \pm \sqrt{2y - 4(P/2 + y \pm \sqrt{2y})}}{2}.$$

Substituting in the expression for y completes the expression for x in radicals, albeit resulting in an incredibly complicated expression.

3.5 The Quintic

After almost 2000 years of work, the 16th century had developed techniques to begin to crack finding solutions to polynomials beyond the quadratic. 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; his proof was messy, and had multiple gaps in rigour. By 1827, the gaps in the proof had been filled by Henrik Abel, giving a proof that there is no 'general' equation in radicals to solve a quintic equation. In 1832, Evariste Galois discovered a much more elegant and flexible approach to the question of insolvability, enabling us to determine whether roots to *particular* equations can be solved in radicals.

The abstract formulation to the problem involves the field theory we have developed. Let E/F be a field extension. Then E is a *Ruffini extension*. If there exists a sequence of fields $K_0 \subset \cdots \subset K_n$ with $K_0 = F$ and $K_n = E$, and there also exists a sequence $\alpha_1, \ldots, \alpha_n$ with $K_i = K_{i-1}(\alpha_i)$ for each $i \in \{1, \ldots, n\}$, and such that for each i, there exists n_i with

$$\alpha_i^{n_i} \in K_{i-1}.$$

We say a polynomial $f \in F[X]$ is solvable in Ruffini radicals if it's splitting field is a Ruffini extension. It is simple to see that if E/F and K/E are Ruffini extensions, then K/F is a Ruffini extension.

This problem seems unrelated to the problem of finding a *general formula* for the roots of a polynomial f of a fixed degree, but this problem can be reduced to the study of Ruffini radicals. For any field K and integer n, we can consider the field $E = K(t_1, \ldots, t_n)$ of rational expressions in n indeterminates $t_1, \ldots, t_n$. We let $s_1, \ldots, s_n \in K(t_1, \ldots, t_n)$ be elements such that in $K(t_1, \ldots, t_n)$ such that in $E[X]$,

$$(X - t_1) \cdots (X - t_n) = X^n + \sum_{k=1}^{n} (-1)^k s_k X^{n-k}.$$

In the elementary study of polynomials it is preserved that $s_1, \ldots, s_n$ are algebraically independant over K, and $K[s_1, \ldots, s_n]$ is precisely the ring of symmetric polynomials in $K[t_1, \ldots, t_n]$. If we write $f = (X - t_1) \cdots (X - t_n)$ and $F = K[t_1, \ldots, t_n]$, then f is solvable in Ruffini radicals precisely when there is a general formula for the n'th roots of a degree n polynomial over

f in radicals. It then follows that any degree n polynomial in K is solvable in Ruffini radicals.

Remark. Ruffini and Abel worked out a general proof that there is no general formula for the quintic over $\mathbf{C}$. Of course, this does not rule out that there exists any *particular* degree five polynomial $f \in \mathbf{C}[X]$ which cannot be solved in Ruffini radicals. It was the work of Galois which pushed the tools to the point where we could address the solvability of any particular quintic polynomial.

It turns out the core problem to obtain solutions to polynomial equations is a certain 'symmetry' in the roots of this equation. We shall see that any 'generically' symmetric equation in the roots of a polynomial equation can be expressed as a rational function in the coefficients of the polynomial. If there are enough symmetries in the roots, then we can obtain enough equations in the roots to obtain a formula for these roots in radicals. As we will now see, we exploited these symmetries in the construction of the various formulae obtained above.

Example. *Consider the general quadratic equation*

$$X^2 - bX + c = (X - t_1)(X - t_2).$$

If $v = t_1 - t_2$, then v^2 is a symmetric polynomial, so $v^2 \in K[b,c]$. In fact, $v^2 = b^2 - 4c$. Since $b = t_1 + t_2$,

$$t_1 = \frac{b+v}{2} \quad \textit{and} \quad t_2 = \frac{b-v}{2}.$$

Thus $\mathbf{C}(t_1,t_2) = \mathbf{C}(a,b)(v)$, where $v^2 \in \mathbf{C}(a,b)$. Of course, one can see from this calculation the quadratic formula in disguise. In particular, if we write $v = \sqrt{b^2-4c}$, then

$$t_1 = \frac{b+\sqrt{b^2-4c}}{2} \quad \textit{and} \quad t_2 = \frac{b-\sqrt{b^2-4c}}{2}$$

which gives back the quadratic formula.

Example. *Consider the general cubic equation*

$$X^3 - bX^2 + cX + d = (X - t_1)(X - t_2)(X - t_3).$$

over $\mathbf{C}$. *The values* $u = (t_1 + \omega t_2 + \omega^2 t_3)^3$ *and* $v = (t_1 + \omega^2 t_2 + \omega t_3)^3$ *are almost symmetric under permutations of roots, but not completely. Namely, odd permutations map* u *to* v, *and* v *to* u *(it is easy to see the elements are preserved by cycles but inverted by transpositions). In particular, this means* $u + v$ *and* uv *are symmetric polynomials. Thus* $u + v, uv \in \mathbf{C}(b, c, d)$. *But this means that*

$$(X - u)(X - v) = X^2 - (u + v)X + uv \in \mathbf{C}(b, c, d)[X],$$

This is a quadratic equation. The last example shows $\mathbf{C}(u, v)$ *is a Ruffini extension of* $\mathbf{C}(b, c, d)$. *But if* $\alpha = t_1 + \omega t_2 + \omega^2 t_3$ *and* $\beta = t_1 + \omega^2 t_2 + \omega t_3$, *then* $\alpha^3, \beta^3 \in \mathbf{C}(b, c, d, u, v)$, *and thus* $\mathbf{C}(b, c, d, u, v, \alpha, \beta)$ *is a Ruffini extension of* $\mathbf{C}(b, c, d, u, v)$. *But since*

$$\begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \\ 1 & 1 & 1 \end{pmatrix}$$

is an invertible matrix, we can use α, β, *and* $t_1 + t_2 + t_3 \in \mathbf{C}(s_1, s_2)$ *to linearly solve for* t_1, t_2, *and* t_3. *In particular,* $\mathbf{C}(b, c, d, u, v, \alpha, \beta) = \mathbf{C}(t_1, t_2, t_3)$. *Calculating all the formulas here gives precisely Cardano's formula.*

Remark. Note that unlike for the quadratic, we explicitly needed to use complex radicals by introducing the third roots of unity ω. Using Galois theory (for instance, in Isaacs, Algebra: A Graduate Course TODO LOOK AT PROOF), one can show that this is unavoidable; the general cubic over $\mathbf{R}$ is *not* solvable in Ruffini radicals.

Example. *Let us now consider the general quartic equation*

$$(X - t_1)(X - t_2)(X - t_3)(X - t_4) = X^4 - bX^3 + cX^2 - dX + e.$$

Consider the three expressions

$$u = (t_1 + t_2 - t_3 - t_4)^2,$$

$$v = (t_1 - t_2 + t_3 - t_4)^2,$$

and

$$w = (t_1 - t_2 - t_3 + t_4)^2.$$

Then permutations of roots permute u, v, *and* w. *Thus* $u+v+w$, $uv+uw+vw$, *and* uvw *all lie in* $\mathbf{C}(b, c, d, e)$. *But this means* u, v, *and* w *are roots of the cubic*

$$(X - u)(X - v)(X - w) = X^3 - (u + v + w)X^2 + (uv + uw + vw)X - uvw$$

Thus applying the formula for the cubic shows $\mathbf{C}(b,c,d,e,u,v,w)$ *is a Ruffini extension of* $\mathbf{C}(b,c,d,e)$. *But if* $\alpha = t_1 + t_2 - t_3 - t_4$, $\beta = t_1 - t_2 + t_3 - t_4$ *and* $\lambda = t_1 - t_2 - t_3 + t_4$, *then* $\alpha^3 = u$, $\beta^3 = v$, *and* $\lambda^3 = w$. *Thus* $\mathbf{C}(b,c,d,e,u,v,w,\alpha,\beta,\lambda)$ *is a Ruffini extension of* $\mathbf{C}(b,c,d,e,u,v,w)$. *But using the invertible matrix*

$$\begin{pmatrix} +1 & +1 & -1 & -1 \\ +1 & -1 & +1 & -1 \\ +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 \end{pmatrix},$$

we have $\mathbf{C}(b,c,d,e,u,v,w,\alpha,\beta,\lambda) = \mathbf{C}(t_1,t_2,t_3,t_4)$. *Thus the quartic can be solved in Ruffini radicals.*

Let us now consider the case of degree five polynomials. The previous techniques for constructing symmetric parts completely fails here. To begin with, in $\mathbf{C}(t_1,\ldots,t_5)$ a natural symmetric quantity to consider is

$$(t_1 + \xi t_2 + \cdots + \xi^4 t_5)^5$$

where ξ is a primitive fifth root of unity. The similar quantity $(t_1 + \omega t_2 + \omega^2 t_3)^3$ get transferred to two separate values which enables us to reduce the cubic equation to a quadratic. However, permutations give 24 possible representatives. This gives a degree 24 equation which is certainly not a simplification. In fact, the best thing we can do is consider the expression

$$(t_1t_2 + t_2t_3 + t_3t_4 + t_4t_5 + t_5t_1 - t_1t_2 - t_2t_4 - t_3t_5 - t_4t_1 - t_5t_2)^2.$$

This takes on six different values. A degree six equation is still harder to solve than the degree five equation, but is better than a degree twenty four equation. Thus we are at an impasse. This does not show that the quintic equation is not solvable in radicals, but it does suggest that the symmetries of the quintic have drastically different behaviour to the lower degree equations. The goal of Galois theory is to form a sharp connection of these symmetries to the underlying roots to show that the problems of symmetry does manifest in an insolvability of the quintic.

Remark. If we work with a particular degree five solution with the property that the degree six equation constructed has a root whose square is rational, in which case the degree six equation reduces to a degree four equation once we remove the root and its conjugate. In fact, one can show that this is the only case in which all roots of a degree five equation can be solved by radicals.