# Galois Theory

Jacob Denson

April 7, 2016

# Table Of Contents

# Chapter 1

# Quadratics, Cubics, and Quartics

The basic problem of Galois theory is to understand the structure of polynomials. 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.

## 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 more deep applications to geometry.

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; his 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. It is his beautiful ideas that are the main focus of Galois theory.

# Chapter 2

# Polynomials

In a ring, we can add and multiply. It is natural then, to 'solve' equations of the form

$$5X^2 + 1 = 2 \qquad XYZ + 2Y = Z$$

in mathematics, objectification has been key to an understanding of certain objects. A polynomial is the static object representing an equation, which we can pin down and understand. Polynomials over abstract fields are the modern way to understand Galois theory, and thus an understanding is crucial.

## 2.1 Univariate Polynomials

Let $A$ be a ring. A **univariate polynomial** in $A$ is an abstract expression of the form

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

where the $a_i \in A$. Really, we can view a polynomial as an infinite sequence of elements $(a_0, a_1, \dots)$ in $A$ which are zero except on a finite subset. The set of all polynomials is denoted $A[X]$. We define a ring structure on $A[X]$ by letting

$$\left(\sum_{k=0}^{n} a_k X^k\right) + \left(\sum_{k=0}^{m} b_k X^k\right) = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$$

$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j X^{i+j} = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k$$

Then $A[X]$ is an algebra over $A$, since $A$ embeds into $A[X]$.

Terminology for univariate polynomials is repeated. If $A \subset B$, then each polynomial $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ gives rise to a function $P : B \to B$, defined by

$$P(b) = a_0 + a_1 b + \cdots + a_n b^n$$

correspondingly, each $b \in B$ gives rise to an **evaluation homomorphism**

$$\mathrm{ev}_b : A[X] \to B \qquad P \mapsto P(b)$$

If the evaluation is injective, $b$ is known as trancendental over $A$. $\pi$ and $e$ are trancendental over $\mathbf{Q}$, but it is a difficult analytical argument to show this.

Each homomorphism $f : A \to B$ gives rise to a homomorphism $\tilde{f} : A[X] \to B[X]$, such that for each $a \in A$, the diagram below commutes.

$$\begin{array}{ccc} A[X] & \xrightarrow{\tilde{f}} & B[X] \\ \downarrow{\scriptstyle \mathrm{ev}_a} & & \downarrow{\scriptstyle \mathrm{ev}_{f(a)}} \\ A & \xrightarrow{f} & B \end{array}$$

The diagrams effectively force us to define the mapping as

$$a_0 + a_1 X + \cdots + a_n X^n \mapsto f(a_0) + f(a_1)X + \cdots + f(a_n)X^n$$

Thus if $f : A \to B$ is a homomorphism, and $b \in B$, there is a unique homomorphism $\tilde{f} : A[X] \to B$ extending $f$ for which $\tilde{f}(X) = b$. It follows that $A[X]$ is the free $A$-algebra generated by $X$. The most important case occurs when we consider the projection $\pi : A \to A/\mathfrak{a}$, so that we can 'reduce' polynomials modulo $\mathfrak{a}$. We will use this tool when understanding factorization in the ring of integer valued polynomials.

## 2.2 Multivariate Polynomials

Univariate polynomials have their problems, but the fun really begins with multivariate polynomials. We consider polynomials in $n$ variables

$X_1, \ldots, X_n$, expressions of the form

$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

such that only finitely many $a_{i_1,\ldots,i_n}$ are non-zero.

Given $f : A \to B$, there is $\tilde{f} : A[X_1, \ldots, X_n] \to B[X_1, \ldots, X_n]$ causing the standard diagram to commute. If $A \subset B$, each polynomial $P \in A[X]$ gives rise to $P_A : B^n \to A$. Each $(b_1, \ldots, b_n) \in B^n$ gives rise to an evaluation function

$$\mathrm{ev}_{(b_1,\ldots,b_n)} : A[X_1, \ldots, X_n] \to B$$

The tuple $(b_1, \ldots, b_n)$ is **algebraically independent** over $A$ if $\mathrm{ev}_{(b_1,\ldots,b_n)}$ is injective. Trancendentality is an incredibly difficult criterion to determine. Algebraic independence is even more impossible. It is still an open question whether $(e, \pi)$ is algebraically independant over $\mathbf{Q}$.

The polynomials $X_1^{i_1} \ldots X_n^{i_n}$ are **primitive**. We define the degree of this primitive polynomial to be $i_1 + i_2 + \cdots + i_n$, and we define the degree of a general polynomial to be the maximal degree of the primitive polynomials which have non-zero coefficients in the evalutation. The set of polynomials over a ring $A$ is denoted $A[X_1, \ldots, X_n]$. We may also write any such polynomial $P$ as

$$P = \sum_{k=0}^{n} P_k X_n^k$$

with $P_k \in A[X_1, \ldots, X_{n-1}]$, so $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$. We define the degree of $P$ with respect to $X_n$ to be the degree of $P$ viewed as an element of $A[X_1, \ldots, X_{n-1}][X_n]$. A polynomial $P \in A[X_1, \ldots, X_n]$ is **homogenous** of degree $m$ if

$$P = \sum_{i_1+i_2+\cdots+i_n=m} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

In a commutative ring, this implies that for any $u, t_1, \ldots, t_n \in B$,

$$P(ut_1, \ldots, ut_n) = u^m P(t_1, \ldots, t_n)$$

Homogenous polynomials are precisely those satisfying this equation, provided that there exists algebraically independent $u, t_1, \ldots, t_n \in B$ over $A$.

## 2.3 Monoid and Group Rings

Let $M$ be a monoid, and $A$ a ring. We shall define a ring $A[M]$ which is similar to that of the polynomial ring over a variable. The ring consists of all sums

$$\sum_{m \in M} a_m m$$

such that $a_m = 0$ for all but finitely many $a_m$. The addition and multiplication structures will be defined

$$\left( \sum_{m \in M} a_m m \right) + \left( \sum_{m \in M} b_m m \right) = \sum_{m \in M} (a_m + b_m) m$$

$$\left( \sum_{m \in M} a_m m \right) \left( \sum_{n \in M} b_n n \right) = \sum_{m,n \in M} a_m b_n mn$$

This ring is commutative if and only if $M$ is. This is the **monoid ring** over $M$ with coefficients in $A$. If we instead start with a group $G$ instead of a monoid $M$, we obtain the **group ring** $A[G]$, studied extensively in the representation theory of finite groups.

**Example.** $\mathbf{N}$ *is a monoid. We have already encountered this monoid, for* $A[\mathbf{N}]$ *is effectively the ring of univariate polynomials. If we take the free abelian monoid* $\mathbf{N}^k$ *on* $k$ *generators, we obtain the monoid ring* $A[\mathbf{N}^k]$*, which is effectively the ring of polynomials in* $k$ *variables. If we consider the set of all elements*

$$X_1^{i_1} X_2^{i_2} X_3^{i_2} \dots X_k^{i_k} \dots$$

*such that* $\sum i_k < \infty$*, then we obtain a polynomial ring with 'infinitely many variables'.*

## 2.4 The Euclidean Algorithm

The **degree** of a univariate polynomial is the largest index of a non-zero coefficient in the polynomial. If $P$ is a polynomial, we denote the degree by $\deg(P)$. We have

$$\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$$

$$\deg(PQ) \leqslant \deg(P) + \deg(Q)$$

If we are working over an integral domain, the second equation is an equality. This is key to multiple theorems for univariate polynomials.

**Theorem 2.1.** *Given $P, Q \in R$, if the leading coefficient of $Q$ is a unit, then*

$$P = MQ + L$$

*where $deg(L) < deg(Q)$.*

*Proof.* We prove the theorem by induction. If $\deg(P) < \deg(Q)$, the theorem is trivial. Otherwise, write

$$P = a_0 + a_1 X + \cdots + a_n X^n \qquad Q = b_0 + b_1 X + \cdots + b_m X^m$$

Then

$$\deg(P - a_n b_m^{-1} X^{n-m} Q) < \deg(P)$$

so by induction,

$$P - a_n b_m^{-1} X^{n-m} Q = MQ + L$$

where $\deg(L) < \deg(\mathrm{Q})$. But this implies

$$P = (M + a_n b_m^{-1} X^{n-m})Q + L$$

so we have found a polynomial for $P$. □

**Corollary 2.2.** *If $F$ is a field, then $F[X]$ is a principal ideal domain.*

*Proof.* Let $\mathfrak{a}$ be an ideal in $F[X]$. Then there is a polynomial $P \neq 0$ in $\mathfrak{a}$ for which any nonzero $Q \in \mathfrak{a}$ satisfies $\deg(Q) \geqslant \deg(P)$. If $P$ is a constant, then $\mathfrak{a} = F[X] = (1)$. Otherwise, we may write $Q = MP + L$, where $\deg(L) < \deg(P)$. But $L \in \mathfrak{a}$, implying $L = 0$. Thus $P \mid Q$ for any non-zero $Q \in \mathfrak{a}$, so $\mathfrak{a} = (P)$. □

If we require $P$ to be **monic**, such that the coefficient of highest coefficient is 1, then $P$ is a unique generator, for if $(P) = (Q)$, then $P$ and $Q$ must have the same degree, and since they are monic, $\deg(P - Q) < \deg(P)$. Since $P - Q \in (P)$, $P - Q = 0$.

**Corollary 2.3.** *If $F$ is a field, $F[X]$ is factorial.*

**Theorem 2.4.** *Given $P \in F[X]$. If $P(a) = 0$, then $X - a \mid P$. If $P$ is degree $n$, then $P$ can have at most $n$ roots in $F$.*

*Proof.* We may write

$$P = M(X - a) + L$$

where $L$ is a constant. Then

$$L = P(a) = 0$$

thus $P = M(X-a)$. If we have $n$ roots $a_1, \ldots, a_n$, we may write, by induction,

$$P = M(X - a_1) \ldots (X - a_n)$$

The degree of the left hand side is $n$, and the degree of the right hand side is $n + \deg(M)$, hence $\deg(M) = 0$, so $M$ is a non-zero coefficient of $F$. If $b \neq a_i$ for any $i$, then because a field is an integral domain,

$$P(b) = M(b - a_1) \ldots (b - a_n) \neq 0$$

Thus $P$ can only have $n$ roots. □

**Corollary 2.5.** *Consider any polynomial $P \in K[X]$. If $P(k) = 0$ for infinitely many $k \in K$, then $P = 0$.*

**Corollary 2.6.** *Let $P \in K[X_1, \ldots, X_n]$, where $K$ is an infinite field. If $P(k_1, \ldots, k_n) = 0$ for all $(k_1, \ldots, k_n) \in K^n$, then $P = 0$.*

*Proof.* We prove by induction. We have already shown this for univariate polynomials. Fix $k_n$. Then consider the polynomial $P(X_1, \ldots, X_{n-1}, k_n)$ is a polynomial in $K[X_1, \ldots, X_{n-1}]$ which induces the zero function on $K^{n-1}$, so $P(X_1, \ldots, X_{n-1}, k_n) = 0$. If

$$P(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$$

Then

$$P(X_1, \ldots, X_{n-1}, k_n) = \sum_{i_1, \ldots, i_{n-1}} \left( \sum_{i_n} a_{i_1, \ldots, i_n} k_n^{i_n} \right) X_1^{i_1} \ldots X_{n-1}^{i_{n-1}} = 0$$

So $\sum_{i_n} a_{i_1, \ldots, i_n} k_n^{i_n} = 0$ for all $k_n \in K$. Since we may view this as a univariate polynomial in $K[X]$, we have $a_{i_1, \ldots, i_n} = 0$ for all $i_1, \ldots, i_n$. Hence $P = 0$. □

Note that non-zero polynomials may induce the zero function in finite fields. For instance, if $p$ is prime, then in $\mathbf{F}_p$, we have $x^p = x$ for all $x \in \mathbf{F}_p$. Thus the function induced by the polynomial

$$X^p - X$$

is the zero function, yet $X^p - X \neq 0$.

**Lemma 2.7.** *Let $F$ be a finite field with $n$ elements. If $P \in F[X]$ induces the zero function on $F$, and $\deg(P) < n$, then $P = 0$.*

*Proof.* If $P \neq 0$, and we factorize enough, then we obtain a contradiction by the degree and the number of roots. □

Now suppose $P = \sum a_i X^i$. A polynomial $P$ is reduced to $Q$ in a finite field $F$ in $n$ elements if $\deg(Q) < n$, and $P(x) = Q(x)$ for all $x \in F$. In $F$, $x^n = x$, by Lagrange's theorem, since $F^*$ has $n - 1$ elements. Then reductions always exist, for if we let

$$Q = \sum_{i=0}^{n-1} \left( \sum_j a_{i+nj} \right) X^i$$

Then $Q(x) = P(x)$ for all $x$. What's more, reductions are unique, for if $Q(x) = R(x)$ for all $x \in F$, and both have degree less than $n$, then $(Q - R)(x) = 0$ for all $x \in F$, so $Q - R = 0$, hence $Q = R$.

## 2.5 The Polynomial Differential Calculus

Later, we shall need to test whether a polynomial has roots of multiplicity greater than one, without actually factorizing the polynomial. Consider the correspondence $X \mapsto X + h$, which gives us a homomorphism $f : K[X] \to K[X, h]$. Since $K[X, h] = K[X][h]$, for any $P \in K[X]$,

$$P^f(X, h) = P(X + h) = \sum_{i=0}^{n} P_i(X) h^i$$

Thus 'to a first approximation', $P(X + h) = P_0(X) + P_1(X)h$. We define $P_1(X)$ to be the derivative of $P$, denoted $P'(X)$. By the binomial theorem,

if $P = \sum a_i X^i$, then it follows that

$$P(X+h) = \sum a_n (X+h)^n = \sum_{m \leqslant n} a_n \binom{n}{m} X^m h^{n-m}$$

So in turn,

$$P'(X) = \sum a_n \binom{n}{n-1} X^{n-1} = \sum_i n a_n X^{n-1}$$

Which implies (by pure computation) that the differentiation operator $D : K[X] \to K[X]$ which sends $P$ to $P'$ is a linear map, which is a **derivation**,

$$D(PQ) = PD(Q) + QD(P)$$

We use differentiation to determine whether a polynomial has multiple roots. Suppose that

$$P = (X-k)^2 Q$$

Then

$$P'(k) = [2(X-k)Q + (X-k)^2 Q'](k) = 0 + 0 = 0$$

Conversely, suppose that $P'(k) = P(k) = 0$. Then we may write

$$P(X) = a_1(X-k) + a_2(X-k)^2 + \cdots + a_n(X-k)^n$$

which implies

$$P'(X) = a_1 + 2a_2(X-k) + \cdots + n a_n (X-k)^{n-1}$$

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

$$P(X) = (X-k)^2 \left( \sum_{k=2}^{n} a_2 (X-k)^{k-2} \right)$$

This gives us a method for determining whether a polynomial is a multiple root in any field.

**Theorem 2.8.** *If $P \in K[X]$ satisfies $P' = 0$, then*

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

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

## 2.6 Polynomials over a Factorial Ring

Let $A$ be a factorial ring. Since $A$ is an integral domain, we may consider the field of fractions $F$. We shall show that $P \in A[X]$ is irreducible over $F[X]$ if and only if $P$ is irreducible over $A[X]$. For each prime $p \in A$, and a non-zero $x \in F$, we may uniquely write $x = p^r u$, where $r \in \mathbf{Z}$, and $p \nmid u$. We define the **order** of $x$ at $p$ to be $r$, and denote it by $\mathrm{ord}_p(x)$. We have

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$$

If $x = 0$, we define $\mathrm{ord}_p(x) = \infty$. Now given a polynomial $P = \sum a_i X^i \in K[X]$, we define

$$\mathrm{ord}_p(P) = \min_{a_i} \mathrm{ord}_p(a_i)$$

For each $a \in A$, we have $\mathrm{ord}_p(aP) = \mathrm{ord}_p(a) + \mathrm{ord}_p(P)$, and if $\mathrm{ord}_p(P) = n$, then $P = p^n Q$, where $\mathrm{ord}_p(Q) = 0$.

Now pick an irreducible $p$ from each equivalence class of those which differ by a unit. We define the content of a non-zero $P \in A[X]$, to be

$$\mathrm{cont}(P) = \prod_p p^{\mathrm{ord}_p(P)}$$

If $P = 0$, define $\mathrm{cont}(P) = 0$. Then the content is unique up to a unit in $A$. We may factorize $P = \mathrm{Cont}(P)Q$, where $Q$ is a polynomial in $A[X]$ such that $\mathrm{cont}(Q)$ is a unit.

**Lemma 2.9** (Gauss)**.** *For $P, Q \in K[X]$, $cont(PQ) = cont(P)cont(Q)$.*

*Proof.* Assume, without loss of generality, that $P, Q \neq 0$. If $\mathrm{cont}(P) = a$, $\mathrm{cont}(Q) = b$, then we may write $P = aP_1$, $Q = bQ_1$, where

$$\mathrm{cont}(P_1) = \mathrm{cont}(Q_1) = 1$$

We have

$$\mathrm{cont}(PQ) = ab\ \mathrm{cont}(P_1 Q_1)$$

so we need only prove that when $P$ and $Q$ have content 1, then $PQ$ has content 1. This relies on a simple trick. Fix a prime $p$. Consider reduction modulo $(p)$. Then $\tilde{P}$, $\tilde{Q}$ do not equal zero modulo $p$. But this implies that

$$\widetilde{P}\widetilde{Q} = \widetilde{PQ} \neq 0$$

since $(p)$ is prime. But since $\widetilde{PQ} \neq 0$, $\mathrm{ord}_p(PQ) = 1$. Since we have shown this for general $p$, $\mathrm{cont}(PQ) = 1$. □

**Corollary 2.10.** *A polynomial in $A[X]$ is irreducible over $A[X]$ if and only if it is irreducible in $F[X]$ and has unit content.*

*Proof.* Let $P \in A[X]$ be reducible over $F[X]$, with $P = QR$, and $Q$ and $R$ are both not units. Write $P = aP_1$, $Q = bQ_1$, $R = cR_1$, where $P_1, Q_1$, and $R_1$ all have unit content, and are therefore elements of $F[X]$. We may assume $a = bc$, by the Gauss lemma. But then $bc \in A$, and we may write $P = (bc)Q_1R_1$, a product of polynomials in $A[X]$. Thus if $P$ is irreducible over $A[X]$, $P$ is irreducible over $K[X]$.

Now suppose $P$ is irreducible over $K[X]$. Suppose $P = QR$, where $Q, R \in A[X]$. Then either $Q$ or $R$ is a unit in $K[X]$ (without loss of generality, let $Q$ be a unit), which implies $Q$ is an element of $A$. Since

$$\text{cont}(P) = \text{cont}(Q)\text{cont}(R)$$

since $Q = \text{cont}(Q)$,

$$\text{cont}(Q)\text{cont}(R)\text{cont}(P)^{-1} = 1$$

So $Q$ is a unit in $A[X]$. □

**Corollary 2.11.** *If $A$ is factorial, then $A[X_1, \ldots, X_n]$ is factorial.*

*Proof.* We just prove that $A[X]$ is factorial if $A$ is, from which the general theorem holds by induction. The existence of a factorization is quite easy to show, for if $P \in A[X]$, we may write

$$P = Q_1 \ldots Q_n$$

where $Q_n$ are irreducible elements of $K[X]$. Now write $Q_i = a_i Q_i'$, where $a_i = \text{cont}(Q_i)$. Thus

$$P = (a_1 \ldots a_n) Q_1' \ldots Q_n'$$

Each $Q_i'$ is an element of $A[X]$ which is irreducible over $K[X]$ and has unit content, so it is irreducible over $A[X]$. We may write

$$a_1 \ldots a_n = p_1^{k_1} \ldots p_m^{k_m}$$

where each $p_i$ is irreducible elements of $A$ (and thus irreducible over $A[X]$), so

$$P = p_1^{k_1} \ldots p_m^{k_m} Q_1' \ldots Q_n'$$

has been written as a product of irreducible elements in $A[X]$. If we have two different factorizations

$$p_1^{k_1} \dots p_m^{k_m} Q_1' \dots Q_n' = q_1^{l_1} \dots q_r^{l_r} R_1 \dots R_t$$

Then by unique factorization in $F[X]$, we must have $t = n$, and after some rearranging, $Q_i = u_i R_i$, for some unit $u_i$. Yet $u_i$ must also be a unit of $A$, for it has unit content. Cancelling out, we find that

$$p_1^{k_1} \dots p_m^{k_m} = (u_1 q_1^{l_1}) \dots (u_r q_r^{l_r})$$

unique factorization in $A$ then tells us that these are the same up to a rearrangement. □

Note that for $n \geqslant 2$, the ring $F[X_1, \dots, X_n]$ is not principal. Indeed $(X, Y)$ is an ideal in $F[X, Y]$ which cannot be principal, for no non unital element divides both $X$ and $Y$.

## 2.7 Criterion for Irreducibility

It is actually quite tricky to determine whether a given polynomial $P \in A[X]$ is irreducible. For instance, $X^4 + 4$ does not have any roots in $\mathbf{Q}$, yet $X^4 + 4$ is reducible,

$$X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$$

Some techniques can be used to determine when a polynomial is irreducible.

**Theorem 2.12** (Eisenstein)**.** *Let $A$ be a factorial ring. Let $P \in A[X]$ be a polynomial, where we write*

$$P = a_0 + a_1 X + \dots + a_n X^n$$

*Let $p$ be a prime in $A$. If $p \mid a_i$ for $i < n$, $p \nmid a_n$, and $p^2 \nmid a_0$, then $P$ is irreducible in $K[X]$.*

*Proof.* Suppose, without loss of generality, that $P$ has content 1. Then we need only show $P$ is irreducible in $A[X]$. Suppose we can write $P = QR$, with $Q, R \in A[X]$. Write

$$Q = b_0 + b_1 X + \dots + b_m X^m \qquad R = r_0 + r_1 X + \dots + r_l X^l$$

Then $b_m r_l = a_n$. Since $p$ does not divide $a_n$, $p$ does not divide $b_m$ and $r_l$. Furthermore, since $p^2$ does not divide $a_0$, $p$ does not divide $b_0$, or $p$ does not divide $r_0$. Assume $p$ does not divide $b_0$. Then $p$ divides $r_0$. For each $i$, we have

$$a_i = r_0 b_i + \cdots + r_i b_0$$

By induction, $p$ divides $r_0, \ldots, r_{i-1}$. If $i < n$, then $p$ divides $i$, so $p$ divides $r_i b_0$. It follows that $p$ divides $r_i$. But this contradicts that $l < i$, since $p$ does not divide $r_l$. □

**Example.** *Consider the polynomial $X^n - a$ in $\mathbf{Q}[X]$. Suppose $n \geqslant 1$, and $a$ is not a perfect square. Then some prime $p \in \mathbf{Z}$ divides $a$, but $p^2$ does not divide $a$. We may apply Eisenstein's criterion to conclude $X^n - a$ is irreducible in $\mathbf{Q}[X]$.*

**Example.** *The polynomial $X^{p-1} + \cdots + X + 1$ is irreducible in $\mathbf{Q}$ if $p$ is prime. Consider the transformation $X = Y + 1$. The transformation preserve irreducibility, since it is really an isomorphism of $\mathbf{Q}[X]$. Then*

$$(Y+1)^{p-1} + \cdots + (Y+1) + 1 = \frac{(Y+1)^p - 1}{Y} = \sum_{k=0}^{n} \binom{p}{k+1} Y^k$$

*The highest coefficient is 1, and all other coefficients divide $p$, and $p^2$ does not divide $\binom{p}{1} = p$, so Eisenstein's criterion tells us that the polynomial is irreducible.*

**Example.** *Let $F$ be a field, and consider the field of rational functions $F(T)$. The polynomial*

$$X^n - T$$

*is irreducible in $F(T)[X]$, for $T$ is irreducible in $F[T]$, $T$ does not divide $X^n$, and $T^2$ does not divide $T$. We may apply Eisenstein's criterion because $F[T]$ is factorial.*

**Theorem 2.13** (Reduction Criterion)**.** *Let $A$ and $B$ be integral domains, and consider a homomorphism $\varphi : A \to B$. Let $K$ and $L$ be the respective quotient fields of $A$ and $B$. Let $P \in A[X]$ be a polynomial such that $\varphi(P) \neq 0$, and $deg(\varphi(P)) = deg(P)$. If $\varphi(P)$ is irreducible in $L[X]$, then we cannot write $P = QR$, with $deg(Q), deg(R) \geqslant 1$.*

*Proof.* Suppose $P = QR$. Then $\varphi(P) = \varphi(Q)\varphi(R)$. We have

$$\deg(\varphi(Q)) \leqslant \deg(Q) \quad \deg(\varphi(R)) \leqslant \deg(R)$$

But these inequalities must be equalities, since

$$\deg(\varphi(Q)) = \deg(Q) + \deg(R) = \deg(\varphi(Q)) + \deg(\varphi(R))$$

Since $\varphi(P)$ is irreducible, $\varphi(Q)$ or $\varphi(R)$ is a unit in $B[X]$, so either $\varphi(Q)$ or $\varphi(R)$ is in $B$. Let $\varphi(Q)$ be in $B$. Then $Q$ must also be in $A$, so $Q$ is a unit in $K$. □

**Theorem 2.14** (Integral Root Test)**.** *Let $A$ be a factorial ring, and $K$ its quotient field. Let*

$$P = a_0 + a_1X + \cdots + a_nX^n$$

*Suppose $P(b/d) = 0$, where $b$ and $d$ are relatively prime. Then $b$ divides $a_0$, and $d$ divides $a_n$. In particular, if $a_n = 1$, then $b/d \in A$, and $b/d$ divides $a_0$.*

*Proof.* We have

$$a_0 + a_1(b/d) + \cdots + a_n(b/d)^n = 0$$

Then

$$d^n a_0 + a_1 b d^{n-1} + \cdots + a_n b^n = 0$$

which implies

$$b(a_1 d^{n-1} + \cdots + a_n b^{n-1}) = -d^n a_0$$

since $b$ does not divide $d$, $b$ does not divide $d^n$, and thus $b$ divides $a_0$. Similarily, by factoring out $d$, we find $d$ divides $a_n$. □

## 2.8 Partial Fractions

**Theorem 2.15.** *Let $A$ be a factorial ring, and let $K$ be its quotient field. Choose a representation $\{p_i\}$ of primes. Then for each $a/b \in K$ there is $a_i \in A$ and $j_i \in \mathbf{N}$ for each $p_i$ such that almost all $a_i$ are zero, and*

$$a/b = \sum_i \frac{a_i}{p^{j_i}}$$

*Proof.* First we show existence. Let $a, b \in A$ be relatively prime. Then we may write $ma + nb = 1$, so

$$\frac{1}{ab} = \frac{m}{b} + \frac{n}{a}$$

Thus for any $c \in A$,

$$\frac{c}{ab} = \frac{cm}{b} + \frac{cn}{a}$$

By induction, we may write

$$\frac{1}{p_1^{k_1} \dots p_{n+1}^{k_{n+1}}} = \sum \frac{a_i}{p_i^{k_i}}$$

Hence

$$\frac{c}{p_1^{k_1} \dots p_{n+1}^{k_{n+1}}} = \sum \frac{ca_i}{p_i^{k_i}}$$

□

# Chapter 3

# 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 an **extension**, a pair $F \subset E$ 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 $F$. Note that this is different from a **finitely generated** extension, when $E$ is a finite dimensional algebra 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 $[\mathbf{C} : \mathbf{R}] = 2$.*

[1] Categorically speaking, an extension is $(F, E, i)$ where $i$ is an epimorphism from $F$ to $E$. Nonetheless, it is cleaner to consider only subsets, for it is notationally speaking. The theory does not change, and proofs carry through with some rewording in the general case.

**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* $\{1, \sqrt{2}\}$*.*

**Example.** *Field extensions need not have a finite degree. Since* $\mathbf{R}$ *is uncountable, and* $\mathbf{Q}$ *is countable,* $[\mathbf{R} : \mathbf{Q}] = \mathfrak{c}$*. If* $\mathbf{F}$ *is any field, then the field of rational functions* $\mathbf{F}(X)$ *is an extension, and the degree of the extension is* $[\mathbf{F}(X) : \mathbf{F}] = \aleph_0$*.*

**Example.** *Every field* $F$ *is the extension of its* **prime subfield***, the smallest field contained in* $F$*. If* $F$ *is characteristic* $p$*, then the prime subfield is* $\mathbf{F}_p$*, and if the field is characteristic 0, then the prime subfield is isomorphic to* $\mathbf{Q}$*.* $\mathbf{F}_p$ *and* $\mathbf{Q}$ *are the fundamental base fields from which to study field extensions.*

**Example.** *If* $[F : K] = 1$*, then* $F = K$*, for* $\{1\}$ *is an independent set of* $F$ *over* $K$*, and therefore every* $x \in F$ *can be written as* $y \cdot 1 = y$*, for some* $y \in K$*.*

**Theorem 3.1** (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 $v_\beta$ are independent, we conclude for each $\beta$,

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

But then, by independance of the $u_\alpha$, we conclude $c_{(\alpha,\beta)} = 0$ for all $\alpha$ and $\beta$. 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

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

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 a particular case of this argument, there is no proper field between* $\mathbf{R}$ *and* $\mathbf{C}$.

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 $F[G]$, 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 $F(S)$.

More notation can be used when two fields $E$ and $F$ are both contained in a larger field $K$. We define the **compositum** $EF$ to be the smallest field containing both $E$ and $F$. In general, we can consider the compositum of an arbitrary number of fields, provided they all lie in some common larger field.

## 3.1 Algebraic and Simple Extensions

The most basic extensions 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

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

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**. Then $\mathrm{ev}_a$ has a non-trivial kernel $(P)$, and

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

Since $F[a]$ is a principal ideal domain, $(P)$ is prime, hence maximal. Then 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 one calls $P$ the **minimal polynomial** of $a$, sometimes denoted $\mathrm{Irr}(F, a)$. If $\deg(\mathrm{Irr}(F, a)) = n$, then $1, a, a^2, \ldots, a^{n-1}$ form a basis of $F(a)/F$, which imples the degree of the extension is the same as the degree of the minimal polynomial. We have a partial corollary.

**Lemma 3.2.** *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 $\pi$ are trancendental, though it takes a lot of analysis to determine this.*

An extension $E/F$ is **algebraic** if every element of $E$ is algebraic over $F$. 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 $[F(a) : F] = \aleph_0$, so

$$[E : F] = [E : F(a)][F(a) : F] > \aleph_0$$

Hence $a$ must be algebraic if $[E : F]$ is finite.

One trick to Galois theory is to utilize the 'compactness' of field extensions. In first order logic, if a statement holds for every finite subset of statements, it can be usually extended to all statements, since every proof using statements necessarily only holds for a finite number. For fields, if we can prove things for finite subextensions, we can usually extend the theorem to the entire extension.

**Theorem 3.3.** *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.* Suppose each $u_i$ is algebraic over $F$. Pick $x \in E$. Then $x = a_1 u_{i_1} + \cdots + a_n u_{i_n}$ for some $a_i \in F$, so $x \in F(u_{i_1}, \ldots, u_{i_n})$. Since each $u_{i_k}$ is algebraic,

each $\mathrm{Irr}(F(u_{i_1},\ldots,u_{i_{n-1}}),u_{i_n})$ exists, so

$$\begin{aligned}[F(u_{i_1},\ldots,u_{i_n}):F] &= \sum_{k=1}^{n}\Big[F(u_{i_1},\ldots,u_{i_k}):F(u_{i_1},\ldots,u_{i_{k-1}})\Big]\\ &= \sum_{k=1}^{n}\deg\Big(\mathrm{Irr}\Big(F(u_{i_1},\ldots,u_{i_{k-1}})\Big),u_{i_k})\Big) < \infty\end{aligned}$$

so $F(u_{i_1},\ldots,u_{i_n})$ is algebraic, and thus $x$ is also 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 3.4.** *If $F/E$ is an extension, then the set of algebraic elements in $F$ form an algebraic field over $E$.*

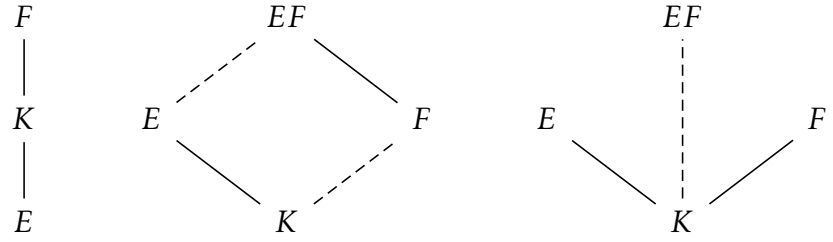
*Proof.* If $a$ and $b$ are algebraic, then $E(a,b)/E$ is an algebraic extension, so $a+b$, $ab$, and if $a\neq 0$, $a^{-1}$ are all algebraic over $E$. □

**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 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).

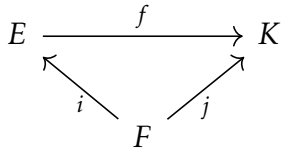
**Theorem 3.5.** *The class of algebraic extensions is distinguished.*

*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 us 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 $F$. □

## 3.2 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 an $F$-**morphism** – a field morphism which is the identity when restricted to $F$. One may view an $F$-**morphism** as a ring homomorphism satisfying the commutative diagram below.



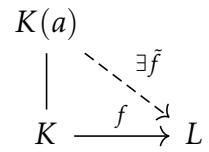

Viewing $E$ and $K$ as $F$-algebras, this is simply an algebra homomorphism, a ring homomorphism which is also linear.

**Lemma 3.6.** *If $E/F \cong K/F$, then $[E : F] = [K : F]$.*

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

The existence of certain $F$-morphisms is incredibly important to the theory of Galois, for they are a way to relate different roots of polynomials. Notationally, it will help to write an application of a morphism $f(x)$ as $x^f$, to avoid being suffocated by brackets.

**Lemma 3.7.** *Let $f : K \to L$ be a field morphism, and let $P = Irr(K, a)$. Then $f$ extends to a map $\tilde{f} : K(a) \to L$ 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 $\mathrm{ev}_b$ 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. We have found all such maps, for any map is determined by its action on $a$. □

**Corollary 3.8.** *If $Irr(E, a) = Irr(E, b)$, then $E(a) \cong E(b)$, by the map*

$$\sum \lambda_i a^k \mapsto \sum \lambda b^k$$

*Proof.* Extend the identity map on $E$. □

When we add $\sqrt[3]{2}$ to $\mathbf{Q}$ to solve the equation $X^3 - 2$, we view this as more natural to the complex numbers $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Yet we have showed that the fields introduced are algebraically isomorphic. This theorem shows that adding a root of a polynomial to a field is independent of *which* root we add up to an isomorphism, in the cases where the polynomial is irreducible over the base field.

**Corollary 3.9.** *If $f : E/K \to E/K$ is a morphism, then $f$ is an automorphism.*

*Proof.* As a field morphism, $f$ must be injective. Conversely, let $a \in E$, and take $P = \mathrm{Irr}(K, a)$. Consider the set of all roots $\{x_1, \ldots, x_n\}$ of $P$ in $E$. Then, $f$ maps $K(x_1, \ldots, x_n)$ into itself. Since $f$ is an injective $E$-linear map from a finite dimensional vector space to itself, it must be surjective, and since $a \in K(x_1, \ldots, x_n)$, $a$ is in the image of $f$, so $f$ is surjective. □

## 3.3 Algebraic Closure

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 a unique (up to isomorphism) algebraic extension which is algebrically closed, known as the **algebraic closure**.

**Lemma 3.10.** *For any polynomial $P \in K[X]$, there is an algebraic extension $L/K$ in which $P$ has a root.*

*Proof.* Assume, without loss of generality, that $P$ doesn't have a root in $K$. 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 3.11.** *Every field has an algebraic closure.*

*Proof.* We shall begin with a fallacious 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 $L[X]$.

Why is this proof wrong? Technically, $\mathcal{C}$ is too big to be a set, and Zorn's lemma doesn't apply. To fix the proof, we 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. One can prove that if $K$ is a field, and $E$ is an algebraic extension, then the cardinality of $E$ is bounded by $K[X]$. Thus we pick $S$ with $\#(S) > \#(K[X])$. Then consider the set of all algebraic extensions with elements in $S$. Such a set is partially ordered, and we can take unions, so there is a maximal field $E$ in this family of fields. Since this field is algebraic over $K$, we know that it is algebraically closed, for we may surely extend $E$ to add another root if such a root existed. □

**Theorem 3.12.** *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 3.13.** *Any two algebraic closures of a field are isomorphic.*

## 3.4 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 $r_i$ are not multiple roots, then the degree of $[F : E] = n!$, and in general, $[F : E] \leqslant n!$, for the first root of $P$ adds degree $n$ to the polynomial, the second has a polynomial of degree at most $n-1$ over the new field, adding at most $n-1$ factors, and so on. A splitting field always exists, since we may always take a subfield of the algebraic closure.

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

**Theorem 3.14.** *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 $K \cong L$.*

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

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

Now suppose $[K : E] > 1$. Then $P$ 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 $\psi_i$ 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 $\psi_i$ 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 3.15.** *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 3.16.** *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 3.17.** *If $F/E$ is normal, every $\sigma : F/E \to F^{\mathfrak{a}}/E$ 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

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

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

**Theorem 3.18.** *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 $P(x) = 0$, 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 3.19.** *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 $x^{\sigma}$ 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.*

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

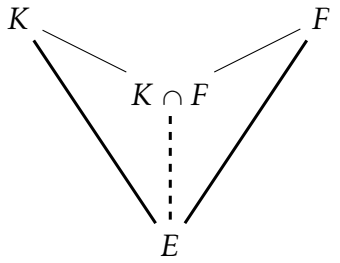
**Theorem 3.20.** *If $K \subset E \subset F$, and if $F/K$ is normal, then $F/E$ is normal.*

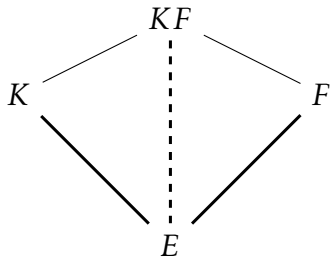
*Proof.* For if $F$ is a splitting field for a family of polynomials in $K[X]$, then $F$ is a splitting field for a family of polynomials in $E[X]$. □

**Theorem 3.21.** *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.

## 3.5 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 $F^{\mathfrak{a}}$ 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 $P$. 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. An element $a$ is called separable if $E(a)$ is separable.*

**Theorem 3.22.** *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 $\pi_i$, generate embeddings $\psi_{ij}$ which extend $\pi_i$. We contend these are all such embeddings of $L$ in $L^{\mathfrak{a}}$ which fix $F$, because if $\gamma$ is any embedding of $L$ which fixes $F$, then $\gamma|_K$ embeds $K$ and fixes $F$, so $\gamma$ is an extension of some $\pi_i$. We claim that for each $i$, there are $[L:K]_s$ extensions $\psi_{ij}$ of $\pi_i$. This is certainly true of the identity map, which we will assume to be $\pi_1$. But then if $\gamma$ is any particular extension of $\pi_i$, then $\psi_{1j} \circ \gamma$ is a family of $[L:K]_s$ extensions of $\pi_i$. These are all such extensions, for if $\lambda$ is any extension of $\psi_i$, then $\lambda \circ \gamma^{-1}$ fixes $F$, and hence is one of $\psi_{1j}$.

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

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

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 3.23.** *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 $a \in K^{\mathfrak{a}}$ such that $Irr(E,a)$ is 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 $\pi$ induces a permutation of the $\sigma_i$, 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* $\omega$ *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 3.24.** *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 $\alpha$. If $K \subset L \subset E$, then the minimal polynomial of $\alpha$ 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 $\alpha$ in $L$ is $\sum_{i=1}^{m} c_i X^i$, then the degree of $\alpha$ 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 $\alpha$. □

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 3.25** (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 $\alpha$ and $\beta$ 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, and thus 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, an impossibility.*

**Example.** *Consider the polynomial $X^2 + T$ in the field $\mathbf{F}_2(T)$. The polynomial is irreducible and inseparable, for it is the product $(X + \sqrt{T})(X + \sqrt{T})$ in $\mathbf{F}_2(T)^{\mathfrak{a}}$.*

Thus we conclude that there are some non perfect fields, but they must have nonzero characteristic.

## 3.6 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 $\varphi$ 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 $\varphi$ generates all $\mathbf{F}_p$ automorphisms of $\mathbf{F}_{p^n}$. If $d$ is the order of $\varphi$, 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 3.26.** *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 3.27.** *Every extension $F/K$ where $F$ is finite and $K$ is a finite field is simple.*

**Corollary 3.28.** *Every finite extension of a finite field is normal and separable.*

## 3.7 Inseparability

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

**Theorem 3.29.** *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 $\sigma_j$ of $K(\alpha_1)$ in $K^{\mathfrak{a}}$ which map $\alpha_1$ to $\alpha_j$ 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 3.30.** *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 $\mu$.*

*Proof.* Let $P = \operatorname{Irr}(K,\alpha)$. 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 $\alpha^p$ is a root of $Q_0$, a polynomial whose degree is smaller than $P$. If $Q_0$ is not separable, then we find $\alpha^{p^2}$ 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 $\mu$ such that $\alpha^{p^\mu}$ 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 $p^\mu$ 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 3.31.** *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 $\alpha_i$ 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 $K^{\mathrm{a}}$, 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 $\alpha_1$ into $E^{\mathfrak{a}}$. If two embeddings $\psi$ and $\pi$ are different, they must differ at some $\alpha_i$. But this is clearly impossible. □

**Corollary 3.32.** *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 3.33.** *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 $\alpha_i$ is purely inseparable. Then $EF = F(\alpha_1, \ldots, \alpha_n)$, and each $\alpha_i$ is purely inseparable over $F$. □

**Theorem 3.34.** *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 $\alpha$ in an inseparable element of $E$ with respect to $F$, then for some $n$, $\alpha^{p^n}$ is separable. But then $\alpha$ is purely inseparable over $K$. Hence $E$ is purely inseparable over $K$. □

**Corollary 3.35.** *A separable and purely inseparable extension $K/E$ is only possible if $K = E$.*

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

**Theorem 3.36.** *If $K/E$ is normal, and $F$ is the maximal separable subextension, then $F/E$ is normal.*

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

# Chapter 4

# 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 automorphisms $\mathrm{Gal}(F/E)$ over the category of field extensions. 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**, and denote the automorphism group as $\mathrm{Gal}(F/E)$.

**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 $z \mapsto \overline{z}$. 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 $i$ 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, since every automorphism of $\mathbf{R}$ which fixes $\mathbf{Q}$ is order preserving, hence continous, and thus fixed $\mathbf{R}$.*

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'

**Theorem 4.1.** *Every normal, separable extension is Galois.*

*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 $\tilde{f} : F \to E^{\mathrm{a}}$, 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 4.2.** *If $F/K$ is Galois, then the mapping*

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

*is an injective map from fields between $K$ and $F$ into the set of subgroups of $Gal(F/K)$.*

*Proof.* Let $K \subset E \subset F$ be a tower of fields. If $F/E$ is a normal extension, then $F^{\mathrm{Gal}(F/E)} = E$. Thus, if $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/L)$, and $F/E$ and $F/L$ are normal, then

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

Since $F/K$ is normal and separable, we know $F/E$ is normal and separable, so this argument applies to all immediate fields. □

We denote the map in the proof by $\mathrm{Gal}(F/-)$. In the Galois case, this map is injective. Soon we shall find out that the map is also surjective.

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

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

In this manner, the map associating $E$ with $\mathrm{Gal}(K/E)$ is found to be an injective order-reversing map. We shall in fact find that this map is also surjective, so it is an order-reversing isomorphism. This isomorphism makes the next two theorems obvious.

**Proposition 4.3.** *If $K/F$ is a Galois extension, and $F \subset E, L \subset K$, then*

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

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

*Proof.* We calculate the fixed field of $\langle \mathrm{Gal}(K/E), \mathrm{Gal}(K/L) \rangle$. Certainly $E \cap L$ is contained within this field. If $x$ is not in $E$, then it is moved by an element of $\mathrm{Gal}(K/E)$, and if $x$ is not in $L$, then it is moved by an element of $\mathrm{Gal}(K/L)$, so we find that $E \cap L$ contains all fixed elements. Similarily, any automorphism of $K$ which fixes $E$ and $L$ certainly fixes $EL$. Conversely, if an automorphism fixes $EL$, then it fixes $E$ and $L$. □

**Proposition 4.4.** *Let $K/F$ be a finite separable extension, and let $E$ be the smallest field in $K^{\mathfrak{a}}$ containing $K$ such that $E/F$ is normal. Then $E/F$ is finite and separable. There are finitely many fields between $F$ and $K$.*

*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. But this implies there are only finitely many subfields between $K$ and $F$. □

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.

**Proposition 4.5.** *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, $[E : K] \leqslant n$, shown again by applying the primitive element method. □

**Theorem 4.6.** *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 above 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 4.7.** *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 $\mathrm{Gal}(K/-)$. □