Galois Theory

Jacob Denson

May 22, 2017

Table Of Contents

Chapter 1

Quadratics, Cubics, and Quartics

The basic problem which gave rise to Galois theory was 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. We begin 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. We shall find that Galois theory explains the general reason why these techniques work.

1.1 Quadratic Polynomials

Finding the roots of a quadratic polynomial is the simplest case, and 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 $B^2 - 4C \geqslant 0$, we can take the square root of the equation on both sides, and we find that

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

If $B^2 - 4C < 0$, then the square root will be a complex number, and we obtain two complex solutions.

The sign of the *discriminant* $\Delta = B^2 - 4C$ thus tells us how many solutions there are to the original equation over the real numbers. If the discriminant is positive, we obtain two distinct square roots, and so the quadratic has two distinct roots. If $\Delta = 0$, then we find that the polynomial has a single root, where the node of the corresponding parabola lies directly on the X axis. If $\Delta < 0$, then the polynomial has no solutions over the real numbers. This makes sense, because if the polynomial has two roots z and w, then

$$(X - z)(X - w) = X^2 - (z + w)X + zw$$

so

$$\Delta = B^2 - 4C = (z + w)^2 - 4zw = z^2 + w^2 - 2zw = (z - w)^2$$

If $z = w$, then $\Delta = 0$. If $z \neq w$, but z and w are both real numbers, then $\Delta = (z - w)^2 > 0$. If we have no real solutions, but instead two distinct complex solutions, then the basic algebra of complex numbers tells us they must occur as complex conjugates of one another, with $w = \overline{z}$, so that $\Delta = (z-w)^2 = (z-\overline{z})^2 = (2i\mathfrak{Im}(z))^2 = -4\mathfrak{Im}(z)^2 < 0$. The main reason why the technique of forming the discriminant works is that it is a *symmetric function* of the roots. That is, if we swap z and w in the equation $(z - w)^2$, the value of the equation doesn't change. There is a general argument showing that any equation of the roots of a polynomial invariant under permutations of the roots is expressible as a rational function of the coefficients of the polynomial, and this is why we may write $\Delta = B^2 - 4C$.

1.2 The Cubic Formula

Let's up the difficulty a notch. Consider an arbitrary cubic

$$X^3 + BX^2 + CX + D$$

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 the 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 $X^3 + PX + Q$. To solve this, we introduce new variables. 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 roots for Y and Z by choosing Y and Z such that $Q + Y + Z$ and $3\sqrt[3]{Y}\sqrt[3]{Z}$ both vanish. To make these values vanish, we must choose Y and Z which satisfy $Y + Z = -Q$ and $YZ = -P^3/27$, and so $Y^2 = Y(Y + Z) - YZ = P^3/27 - QY$, 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! So 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 $3\alpha\beta + P = 0$. If this holds, then we obtain three other solutions by multiplying by third roots of unity, which are $\alpha + \beta$, $\omega\alpha + \omega^2\beta$, and $\omega^2\alpha + \omega\beta$. These are the three solutions to the cubic which are obtained from, as 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.

Cardano's equation (as the solution is known) is not nearly as useful as the quadratic formula. If a polynomial has three real roots, the equation gives bewildering equations. For instance, the polynomial $X^3 + 3Y - 36$ has an integer root $X = 3$, but Cardano's formula gives solutions of the form

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

The real cubic roots give the solution $X = 3$, but this is certainly not immediately obvious. As another example, the polynomial $X^3 - 15X - 4$ has a root of 4, yet Cardano's formula gives roots of the form

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

The mathematician Rafael Bombelli noticed that we have an algebraic expansion $(2 \pm i)^3 = 2 \pm 11i$, and using this expansion we can recover the solution $X = 4$ from Cardano's equation. But determining these roots in this way isn't exactly satisfying. Thus Cardano's formula does not avoid the use of complex numbers even when finding the real solutions to a polynomial. In fact, one can prove using Galois theory that a general formula for the roots of a cubic polynomial must use the complex numbers.

The traditional escape to this approach is to use trigonometric functions to express the roots of the polynomial, as discovered by François Viéte. Consider the equation $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$. Given a formula $X^3 + PX + Q = 0$, 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 choose Y such that we can substitute in the trigonometric identity. If we set $R^3 = 4Y$, and $RP = -3Y$, then the equation can be written as $Y\cos 3\theta + Q = Y(4\cos^3\theta - 3\cos\theta) + Q = 0$. For each R, there is a unique Y satisfying $R^3 = 4Y$, and the second equation can be satisfied when $RP = -3Y = (-3/4)R^3$, so we can choose values of R such that $4RP + 3R^3 = 0$, and this gives $R = 0$ and $R = \sqrt{-4P/3} = 2\sqrt{-P/3}$. This gives $\cos 3\theta = (3Q/2P)\sqrt{-3/P}$, hence we find that we can find a family of real roots to the cubic by

$$2\sqrt{\frac{-P}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{3Q}{2P}\sqrt{\frac{-3}{P}}\right) + \frac{2\pi k}{3}\right)$$

which are distinct for $k \in \{0,1,2\}$. If $P < 0$, then all terms in the equation above are real, and the condition for the arccos to exist is that the argument is between -1 and 1, which means exactly that $0 \leqslant (3Q/2P)^2(-3/P) \leqslant 1$, which occurs exactly when $27Q^2 + 4P^3 \leqslant 0$. A fairly brutal calculation shows that these are all the roots of the equation.

Note that again, we can characterize the solution set of a cubic equation by a quantity $\Delta = -27Q^2 - 4P^3$. If $X^3 + PX + Q = (X-z)(X-w)(X-u)$, then we find that $\Delta = (z-w)^2(z-u)^2(w-u)^2$, and so we find that if $\Delta < 0$, then the cubic has two real solutions and one complex solution (because complex solutions to a cubic cannot come in pairs), if $\Delta > 0$, we have seen there are three real solutions, and if $\Delta < 0$, then we obtain two complex solutions and a real solution.

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 regarded as rigorous tools 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 complex or positive numbers, the solution requires a total of thirteen cases, a testament to the utility of the modern 'formal' approach, employing the complex numbers in full confidence.

1.3 Quartic Equations

The Arns Magna also included a solution to the quartic equation, a method of Lodovico Ferrari. Consider

$$X^4 + PX^2 + QX + R$$

Any polynomial can be reduced to this form, by a Tschirnhaus transformation similar to the cubic case. We can write this as

$$(X^2 + \frac{P}{2})^2 = -QX - R + \frac{P^2}{4}$$

Introduce a new term Y, and consider

$$(X^2 + P/2 + Y)^2 = 2YX^2 - QX - R + \frac{P^2}{4} + Y^2$$

Choose Y so that the right side is a perfect square. If it is, it must be the square of

$$\sqrt{2Y}X - \frac{Q}{2\sqrt{2Y}}$$

Thus we require

$$-R + \frac{P^2}{4} + PY + Y^2 = \frac{Q^2}{8Y}$$

Provided $Y \neq 0$, we are reduced to solving a cubic equation. Now we have the equation

$$(X^2 + \frac{P}{2} + Y)^2 = (\sqrt{2Y}X - \sqrt{2Y})^2$$

So

$$X^2 + \frac{P}{2} + Y = \pm(\sqrt{2Y}X - \sqrt{2Y})$$

which are two quadratics, giving us the solutions to the entire equation.

1.4 The Quintic

Every root of quadratic, cube, and quartic polynomials can be expressed in terms of the coefficients of the polynomial using five basic operations: addition, subtraction, multiplication, division, and taking radicals ('powers of $1/n$') – we say all quadratic polynomials are 'solvable in radicals'. This is the key problem of Galois theory. 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.

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 a thorough understanding of polynomials is crucial to the rest of our discourse.

2.1 Univariate Polynomials

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

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

with $a_0, \dots, a_n \in A$. 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, and this is the set theoretic way to construct the polynomial ring, though once this is done we tend to forget the construction. The set of all polynomials is denoted $A[X]$. We define a ring structure on $A[X]$ by letting

$$\sum a_k X^k + \sum b_k X^k = \sum (a_k + b_k) X^k$$

$$\left(\sum a_i X^i\right)\left(\sum b_j X^j\right) = \sum a_i b_j X^{i+j} = \sum_k \left(\sum a_i b_{k-i}\right) X^k$$

Then $A[X]$ is an algebra over A, since A embeds into $A[X]$. If $A \subset B$, then each polynomial $f = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ gives rise to a function $f : B \to B$, defined by $f(b) = a_0 + a_1 b + \cdots + a_n b^n$. Correspondingly, each $b \in B$ gives rise to an **evaluation homomorphism** $\text{ev}_b : A[X] \to B$, which maps a polynomial f to $f(b)$. If the evaluation is injective, b is known as a **trancendental element** over A. π and e are trancendental over $\mathbf{Q}$, but it is a difficult analytical argument to show this, and we still do not know whether other numbers, like $\pi + e$, or π/e are trancendental (it is not even known whether they are irrational or not).

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

$$\begin{tikzcd} A[X] \arrow[r, "\tilde{T}"] \arrow[d, "\text{ev}_a"] & B[X] \arrow[d, "\text{ev}_{T(a)}"] \\ A \arrow[r, "T"] & B \end{tikzcd}$$

The diagrams effectively force us to define the mapping as

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

Though there need not be a unique such map for general rings.

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 're-duce' 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 $X_1, \dots, X_n$, expressions of the form

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

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

Given $f : A \to B$, there is $\tilde{f} : A[X_1,\dots,X_n] \to B[X_1,\dots,X_n]$ 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 $(b_1,\dots,b_n) \in B^n$ gives rise to an evaluation function

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

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

The polynomials $X_1^{i_1}\dots X_n^{i_n}$ are **primitive**. We define the degree of this primitive polynomial to be $i_1 + i_2 + \dots + i_n$, 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 $A[X_1,\dots,X_n]$. We may also write any such polynomial P as

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

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

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

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

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

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

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 $\mathfrak{a} = (P)$. $\square$

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. $\square$

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 $P = 0$. $\square$

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. $\square$

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 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 $\text{ord}_p(aP) = \text{ord}_p(a) + \text{ord}_p(P)$, and if $\text{ord}_p(P) = n$, then $P = p^n Q$, where $\text{ord}_p(Q) = 0$.

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

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

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

Lemma 2.8 (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 $\text{cont}(P) = a$, $\text{cont}(Q) = b$, then we may write $P = aP_1$, $Q = bQ_1$, where

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

We have

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

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

Corollary 2.9. *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 $A[X]$. $\square$

Corollary 2.10. *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

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

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

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

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

Note that for $n \geqslant 2$, the ring $F[X_1, \ldots, X_n]$ 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.

2.6 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 2.11 (Eisenstein). *Let A be a factorial ring. Let $P \in A[X]$ be a polynomial, where we write*

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

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

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

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 2.12 (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 2.13 (Integral Root Test)**.** *Let* A *be a factorial ring, and* K *its quotient field. Let*

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

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. □

2.7 Partial Fractions

Theorem 2.14. *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

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

□

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 to problems in field theory. 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, which occurs when E is a finite dimensional algebra over F.

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

[1]Categorically speaking, an extension is a morphism $i : E \to F$ of fields, in which we view E as being contained in F. Nonetheless, it is cleaner to consider only subsets, for it is notationally simpler. The theory does not change in this simplification.

and b are real numbers, so $[\mathbf{C} : \mathbf{R}] = 2$. *Galois theory was built to study* $\mathbf{C}$ *and its subfields, but its method can be extended to cover much more complicated situations.*

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_β are independent, we conclude for each β,

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

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

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

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 $F(S)$.

The category of fields is suprisingly restrictive. No products exist, nor coproducts. The only construction which is systematic in Galois theory is the **compositum** EF of two fields E and F, which is defined to be the smallest field containing both E and F (we must assume E and F lie in some common larger field). In general, we can consider the compositum of an arbitrary number of fields, being the smallest field which contains every other field. We have equations like

$$F(x)F(y)=F(x,y)$$

which in the sequel will turn out to be useful.

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 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 $\text{Irr}(F,a)$. If $\deg(\text{Irr}(F,a)) = n$, then $1, a, a^2, \dots, a^{n-1}$ 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 $(XQ - 1)(a) = 0$. $\square$

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

An extension E/F is **algebraic** if every element of E is algebraic over F. 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 $x \in F(u_{i_1}, \dots, u_{i_n})$. Since each u_{i_k} is algebraic, each $\text{Irr}(F(u_{i_1}, \dots, u_{i_{n-1}}), u_{i_n})$ exists, so

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

so $F(u_{i_1}, \dots, u_{i_n})$ is algebraic, and thus x is also algebraic. $\square$

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. $\square$

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

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.

$$\begin{tikzcd}
F \arrow[d, dash] \\
K \arrow[d, dash] \\
E
\end{tikzcd}
\qquad
\begin{tikzcd}
 & EF \arrow[dl, dash, dashed] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & F \arrow[dl, dash, dashed] \\
 & K &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & EF \arrow[dd, dash, dashed] & \\
E \arrow[dr, dash] & & F \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

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. $\square$

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.

$$\begin{tikzcd} E \arrow[rr, "f"] & & K \\ & F \arrow[ul, "i"] \arrow[ur, "j"'] & \end{tikzcd}$$

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 ϕ is an F-isomorphism between E and K, then ϕ is an F-linear isomorphism, which maps bases to bases, preserving dimension. $\square$

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.*

$$\begin{tikzcd}
K(a) \arrow[d, no head] \arrow[dr, dashed, "\exists \tilde{f}"] & \\
K \arrow[r, "f"] & L
\end{tikzcd}$$

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

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

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

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

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

Proof. As a field morphism, f must be injective. To verify surjectivity, let $a \in E$, and take $P = \text{Irr}(K, a)$. Consider the set of all roots $\{x_1, \dots, x_n\}$ of P in E. Then, f maps $K(x_1, \dots, x_n)$ into itself, for each x_i must be mapped onto an $x_j \in K(x_1, \dots, x_n)$. The restriction is an injective E-linear map from a finite dimensional vector space to itself, and it therefore must be surjective, and since $a \in K(x_1, \dots, x_n)$, 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 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

$$a + b = c \quad ab = c$$

exactly when they hold in F. This new theory is still consistant, for it has a model. For each $a_1, \dots, a_n \in F$, consider the statement

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

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', with $F \subset F'$, such that for any polynomial $P \in F[X]$, there is $a \in F'$ with $P(a) = 0$. We may clearly shrink F' so that it is algebraic. Now proceed inductively, forming

$$F \subset F' \subset F'' \subset \dots$$

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[2]. $\square$

The obvious Zorn's lemma argument is tricky to apply in this situation, 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 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 $a_i \in E$. $\square$

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

[2]It turns out that F' is always an 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.

3.4 Splitting Fields and Normal Extensions

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, and is the smallest field with this property. That is, if we write

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

in F, then $F = E(r_1, \dots, r_n)$. 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 $\mathbf{Q}(\sqrt{2})$.*

Example. *A splitting field of $X^2 + aX + b \in \mathbf{Q}(X)$ has either degree 1 or degree 2. This follows from our discussion above, since if F is a splitting field, then $[F : \mathbf{Q}] \leqslant 2! = 2$. But we may approach this theorem more practically here. If the polynomial splits in $\mathbf{Q}$, then we need not extend the field at all. Otherwise, we need to add the numbers*

$$\frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

which is equivalent to just adding $\sqrt{a^2 - 4b}$, an element of degree 2 over $\mathbf{Q}$. This method works for any field, but care needs to be taken in fields of characteristic 2, where the quadratic formula need not apply.

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 satisfies*

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

Then we may write

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

Thus $\mathbf{Z}_2(i)$ splits $X^3 + X + 1$.

Example. *Consider the polynomial $X^p - 1$ in $\mathbf{Q}$. We see that, on the real axis, $X^p - 1$ has only a single inflection point which occurs at the axis, so $\mathbf{Q}$ cannot* *contain all roots of the polynomial for $p > 2$. If $a^p = 1$ and $b^p = 1$, then $(ab)^p = 1$, so the set of roots to this polynomial form a finite, multiplicative subgroup of* $\mathbf{Q}^*$*, which therefore must be cyclic. This implies that the splitting field of $X^p - 1$ is* $\mathbf{Q}(\omega)$*, where ω is a generator of this cyclic group (known as a* **primitive p'th root of unity***). In general, a field always contains roots to $X^2 - 1$ (namely, ± 1). If the field does not contain the roots to $X^p - 1$, then the splitting field has degree p, by the same argument as above.*

Example. $\mathbf{C}$ *splits $X^5 - 2$. If ω is a 5'th 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

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

We have

$$Irr(\sqrt[5]{2}, \mathbf{Q}) = X^5 - 2 \qquad Irr(\omega, \mathbf{Q}(\sqrt[5]{2})) = X^4 + X^3 + X^2 + X + 1$$

The first is irreducible by Eisenstein's criterion. To verify that the second is irreducible, we note that it has no linear factors in $\mathbf{Q}(\sqrt[5]{2})$*, for all roots are complex. 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 we have the equalities

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

Using the fourth equality, we may remove d from all future equations, so

$$a + c = 1 \qquad b^2 + bac + 1 = a + b^2c = b$$

But then

$$b - 1 = (b^2 - 1)c = (b - 1)(b + 1)c$$

so either $b = 1$, or $(b + 1)c = 1$. However, it is impossible for $b = 1$, for then

$$ac = -1 \qquad a + c = 1$$

hence we would have the equation

$$a^2 - a - 1 = 0$$

and then by using the quadratic equation,

$$a = \frac{1 \pm \sqrt{5}}{2}$$

which implies $\sqrt{5} \in \mathbf{Q}(\sqrt[5]{2})$*, which is impossible, for*

$$[\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = 2 \quad [\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}] = 5$$

Thus we must have $(b+1)c = 1$ *instead. Now we may use this to remove* c *from our equations*

$$ab + a = a(b+1) = b \quad b^3 + ab + 1 = 0$$

Finally, multiplying by $b+1$ *on the right equation gives us*

$$b^4 + b^3 + b^2 + b + 1 = 0$$

which implies that the polynomial has a linear factor in $\mathbf{Q}(\sqrt[5]{2})$*, which we have previously verified to be impossible. Thus we have*

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

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 viewpoint.

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 spltting field of P, then we may write, for $u_i \in K$, $v_i = f(u_i)$,

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

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

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

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

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

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 $f(K) = F$. $\square$

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 $x^\sigma \in F$. $\square$

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. $\square$

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^σ is a root of P, so $x^\sigma \in F$. The relation follows since F is generated by these roots. Hence the splitting field is normal. Conversely, let F/E be normal. For each $x \in F$, consider the minimal polynomial $P_x \in E[X]$. Then $P_x(x) = 0$, so F splits P_x. But this implies exactly that F is the splitting field of $\{P_x : x \in F\}$. $\square$

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.

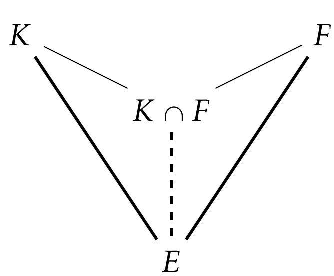
Theorem 3.20. *If $K \subset E \subset F$, and if F/K is normal, then F/E is normal.*

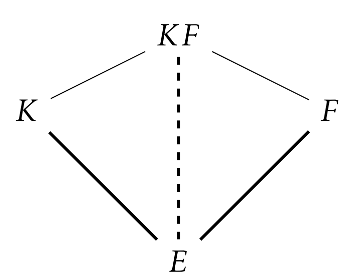
Proof. For if F is a splitting field for a family of polynomials in $K[X]$, then F is a splitting field for a family of polynomials in $E[X]$. $\square$

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 $f(K \cap F) \subset K \cap F$. $\square$

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

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 P into linear factors

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

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. Consider the correspondence $X \mapsto X + dX$, which gives us a homomorphism $K[X] \to K[X, dX]$. Since $K[X, dX] = K[X][dX]$, for any polynomial P, we may write

$$P(X + dX) = \sum P_i(X) dX^i$$

for some polynomials P_i. If we work 'to a first approximation'[3], then

$$P(X + dX) = P(X) + P'(X) dX$$

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

$$(PQ)' = P'Q + PQ'$$

Since

$$\begin{aligned}(PQ)(X + dX) = (P(X) + P'(X)dX)(Q(X) + Q'(X)dX) &= (PQ)(X) \\ + [(P'Q)(X) + (PQ')(X)]dX + (P'Q')(X)dX^2\end{aligned}$$

[3]Rigorously, we switch to the quotient by the ideal generated by dX^2, so '$dX^2 = 0$'

and $dX^2 = 0$. We call a linear map $D : R \to R$ between rings a **derivation** if it satisfies the Leibniz rule. There is an explicit formula for this derivation, which should already be very familiar. If $P = \sum a_i X^i$, then

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

So in turn,

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

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

Proposition 3.22. *A polynomial P has a multiple root k if and only if*

$$P(k) = P'(k) = 0$$

Proof. Suppose that

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

Then $P(k) = 0$, and

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

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

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

so derivatives imply multiple roots. $\square$

Theorem 3.23. *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 $na_n = 0$ 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 3.24. *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^a. We shall let $[F : E]_s$ denote the number of different embeddings of F in F^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 $\text{Mor}(L/F, K/F)$ is bijective with $\text{Mor}(L/F, E/F)$.

Example. *Consider a simple extension $E(a)$, with minimal polynomial P. In F^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 3.25. *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^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^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

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

And we know that

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

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

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

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

Corollary 3.26. *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 $\sigma_1, \dots, \sigma_n$ are all the embeddings of E in $E^{\mathfrak{a}}$, then $L = \sigma_1(E) \dots \sigma_n(E)$ 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 3.27. *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 $F(c_1, \dots, c_m)$ is the same as the degree over L, which implies that $F(c_1, \dots, c_m) = L$. Thus a subfield is uniquely identified by the minimal polynomial of α, and the number of fields between K and E is finite. $\square$

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 3.28 (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 $\sigma_1, \dots, \sigma_n$ 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. $\square$

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, for if P was irreducible and inseparable, then $gcd(P, P') \neq 0$, which would imply $P|P'$, hence $P' = 0$, which would imply P 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.

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 of a field with characteristic p, known as the **Frobenius Endomorphism**. A fundamental question of a field is whether the 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 3.29. *$X^p - a$ is either irreducible or is a p'th power in $K[X]$ for $a \in K$.*

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 $X^p - a = PQ$, where P and Q are non-trivial, then for some k,

$$P = (X-b)^k \qquad Q = (X-b)^{p-k}$$

and we find that $b^k \in K$. But since $b^p = a \in K.$, there are inters 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 3.30. *K is perfect if and only if $K^p = K$.*

Proof. Let P be a polynomial in $K[X]$. □

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 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 3.31. *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 $G = \langle x \rangle$. $\square$

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

Corollary 3.33. *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 3.34. *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 $m_1 = m_2 = \cdots = m_r$. $\square$

The next theorem shows, in fact, that each multiplicity must be a power of the characteristic of the field. Over **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 3.35. *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 $P = \text{Irr}(K, \alpha)$. 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. $\square$

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 3.36. *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

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

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 3.37. *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 3.38. *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 $E = K(\alpha_1, \dots, \alpha_n)$, where each α_i is purely inseparable. Then $EF = F(\alpha_1, \dots, \alpha_n)$, and each α_i is purely inseparable over F. □

Theorem 3.39. *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 3.40. *A separable and purely inseparable extension K/E is only possible if $K = E$.*

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

Theorem 3.41. *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 $\pi(F) \subset F$. $\square$

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 automorphism group $\text{Gal}(F/E)$ 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**, in which case the automorphism group is even more closely connected to the space. 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 4.1. *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 4.2. *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 4.3. *Let K/F be a finite separable extension, and let E be the normal closure. Then E/F is finite and separable.*

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

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

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 4.4. *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 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, and $[E : K] \leqslant n$. $\square$

Theorem 4.6 (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. $\square$

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 $\mathrm{Gal}(K/-)$. $\square$

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 $\text{Gal}(K/E)$ is found to be an order-reversing isomorphism. This makes the following proposition obvious.

Proposition 4.8. *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 $\text{Gal}(K/-)$ 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 4.9 (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 $\sigma \in \text{Gal}(E/F)$ satisfies $\sigma(L) = L$, so if $\tau \in \text{Gal}(E/L)$, then $\sigma\tau\sigma^{-1}$ fixes F, and maps L to itself, and is thus an element of $\text{Gal}(E/L)$. so $\text{Gal}(E/L)$ is normal in $\text{Gal}(E/F)$. Conversely, let G be a normal subgroup of $\text{Gal}(E/F)$. Let $\sigma \in \text{Gal}(E/L)$. If there is $x \in L$ such that $\sigma(x) \notin L$, then there is $\tau \in \text{Gal}(E/L)$ 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 $\sigma^{-1} \circ \tau \circ \sigma \in \text{Gal}(E/L)$. Thus $\sigma(x) \in L$ for all $x \in L$, and if f is any embedding of L in $L^{\mathfrak{a}}$ which fixes F, then f extends to an embedding of E in $L^{\mathfrak{a}}$, 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.

4.1 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

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

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.