Galois Theory

Jacob Denson

July 8, 2020

Table Of Contents

Chapter 1

Quadratics, Cubics, and Quartics

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

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

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

1.1 Quadratic Polynomials

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

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

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

1.2 The Cubic Formula

Let's up the difficulty a notch. Consider a cubic equation $x^3 + Bx^2 + Cx + D = 0$. Begin by substituting $x = y - B/3$ into the equation (geometrically, shift the graph to the right $B/3$ units). Then

$$y^3 + y\left(C - \frac{B^2}{3}\right) + \left(\frac{4B^3}{27} - \frac{CB}{3} + D\right) = x^3 + Bx^2 + Cx + D$$

The quadratric coefficient vanishes because the point of inflection of the equation now lies at the origin. This is known as a *Tschirnhaus transformation*, which is a general technique to shifting a polynomial equation so that the coefficient corresponding to the term one less than the degree of the polynomial vanishes.

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

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

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

and so we obtain *Cardano's formula*

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

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

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

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

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

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

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

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

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

1.3 Viete's Formula For the Cubic

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

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

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

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

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

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

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

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

and we conclude that

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

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

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

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

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

Cubic equation occupied a vast amount of mathematical effort. Challenges and contests were formed to test algebraic aptitude. Early in the 16th century, italian mathematician Scipio del Ferro found a solution to cubics of the form $x^3 + Bx = C$, where B and C are positive numbers (Negative numbers were not commonly accepted at the time), who used it to great success in contests. Of course, he did not share his solution to the general public. Ferro told the solution to his student Florido, who challenged the mathematician Niccoló Tartaglia. In preparation, Tartaglia found the general solution to the cubic, winning the mathematical duel. Tartaglia also wanted to keep the solution secret, but the solution was revealed after an exchange with Girolamo Cardano, who published it in his book, the Ars Magna, in 1545. Without using complex or negative numbers, the solution requires a total of thirteen cases, a testament to the utility of the modern 'formal' approach to arithmetic, confidently applying the complex numbers as if they were real numbers after all.

1.4 Quartic Equations

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

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

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

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

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

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

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

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

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

Now we have the equation

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

Thus

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

This is a quadratic equation, and so we may write

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

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

1.5 The Quintic

After almost 2000 years of work, the 16th century had developed techniques to begin to crack finding solutions to polynomials beyond the quadratic. After a century of success, mathematicans hoped to expand techniques to quintic equations. From the beginning of the 16th century to the end of the 18th, mathematicians as prominent as Euler and Lagrange tried their hand at the equation, to little success. Lagrange attempted to generalize existing techniques, and found they had no extension to the quintic formula. He was the first prominant mathematician to believe that there may be no solution. In 1813, Paolo Ruffini almost gave an impossibility proof; his proof was messy, and had multiple gaps in rigour. By 1827, the gaps in the proof had been filled by Henrik Abel, giving a proof that there is no 'general' equation in radicals to solve a quintic equation. In 1832, Evariste Galois discovered a much more elegant and flexible approach to the question of insolvability, enabling us to determine whether roots to *particular* equations can be solved in radicals.

It turns out the core problem to obtain solutions to polynomial equations is a certain 'symmetry' in the roots of this equation. We shall see that any 'generically' symmetric equation in the roots of a polynomial equation can be expressed as a rational function in the coefficients of the polynomial. If there are enough symmetries in the roots, then we can obtain enough equations in the roots to obtain a formula for these roots in radicals. As we will not see, we exploited these symmetries in the construction of the various formulae obtained above.

For instance, suppose the polynomial $x^2 + Bx + C$ has roots x_1 and x_2. Then the quantities $x_1 + x_2$ and x_1x_2 are invariant under permutations of the roots, so they are expressed as polynomials in the coefficients. In particular, $x_1 + x_2 = -B$, and $x_1x_2 = C$. But these two equations enable us to find the roots; since

$$(x_1 + x_2)^2 - (x_1 - x_2)^2 = 4x_1x_2$$

we conclude that $(x_1 - x_2)^2 = B^2 - 4C$. Thus $x_1 - x_2 = \sqrt{B^2 - 4C}$, and so combining this with the equation for $x_1 + x_2$ gives the quadratic formula.

Obtaining Cardano's formula for the cubic requires stronger techniques, since there is a higher degree of freedom. If ω is a third root of unity, then

$$y = (x_1 + \omega x_2 + \omega^2 x_3)^3$$

is *almost* fixed by permutations of roots. Even permutations fix the roots, whereas odd roots change the quantity to

$$z = (x_1 + \omega^2 x_2 + \omega x_3)^3.$$

This implies $y + z$ and yz is fixed by all permutations, so it must be expressed as a rational equation in B and C. Thus we write $y + z = G_1(B, C)$ and $yz = G_2(B, C)$. But then y and z are both roots of the polynomial $x^2 - G_1(B, C)x + G_2(B, C)$. Thus the quadratic formula enables us to express y and z as radical expressions in $G_1(B, C)$ and $G_2(B, C)$. But now taking cube roots shows that $\sqrt[3]{y} = x_1 + \omega x_2 + \omega^2 x_3$ and $\sqrt[3]{z} = x_1 + \omega^2 x_2 + \omega x_3$ are expressible using radicals in B and C. But then this means that

$$\sqrt[3]{y} - \sqrt[3]{z} = i\sqrt{3}(x_2 - x_1)$$

is expressible using radicals, as is

$$\sqrt[3]{y} + \sqrt[3]{z} = 2x_1 - x_2 - x_3.$$

Since $x_1 + x_2 + x_3 = 0$, we can now combine these three independent linear equations to solve for x_1, x_2, and x_3 in radicals. This is essentially the approach which lead to Cardano's formula.

Finally, for the quartic equation $x^4 + Px^2 + Qx + R = 0$, with roots x_1, x_2, x_3 and x_4. If we set

$$u = (x_1+x_2-x_3-x_4)^2, \quad v = (x_1-x_2+x_3-x_4)^2, \quad \text{and} \quad w = (x_1-x_2-x_3+x_4)^2,$$

then $u+v+w$, $uv+uw+vw$, and uvw are all invariant under permutations under roots, and so can be written as rational coefficients in the equations of the polynomials, denoted respectively as $G_1(P, Q, R)$, $G_2(P, Q, R)$, and $G_3(P, Q, R)$. But then, as in the cubic case, we find u, v, and w are roots of the polynomial $x^3 - G_1(P, Q, R)x^2 + G_2(P, Q, R)x - G_1(P, Q, R)$, and can thus be solved in radicals by Cardano's formula. But this implies that $\sqrt{u}$, $\sqrt{v}$, and $\sqrt{w}$ can be expressed as radicals. The fact that $x_1 + x_2 + x_3 + x_4$, together with the square roots, gives four linearly independent equations in x_1, x_2, x_3, and x_4 which solves the equation in radicals.

These techniques completely fail in the case of the quintic. To begin with, given roots $x_1, \ldots, x_5$, considering a fifth root of unity ξ and considering the quantity

$$(x_1 + \xi x_2 + \cdots + \xi^4 x_5)^5$$

Unfortunately, the permutations of the roots give 24 possible different representatives, leading to a degree twenty four equation which is obviously not a simplification of the equation. In fact, the best thing that can be done is to consider the expression

$$(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_2 - x_2x_4 - x_3x_5 - x_4x_1 - x_5x_2)^2$$

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

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

Chapter 2

Polynomials

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

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

Making an abstract concept into a precise mathematical object is often the key method to study mathematical phenomena. A polynomial is the static object representing the equations we can construct in a ring, which we can pin down and understand. In this Chapter, all rings will be assumed to be commutative unless stated otherwise.

2.1 Univariate Polynomials

We now provide a brief introduction to the ring of polynomials with coefficients in a ring. If A is a commutative ring, a *univariate polynomial* in the indeterminate X with coefficients in A is an abstract expression of the form $f(X) = a_0 + a_1 X + \dots + a_n X^n$, with $a_0, \dots, a_n \in A$. The set of all univariate polynomials in X is denoted $A[X]$. We define a ring structure on $A[X]$ by letting

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

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

Since A embeds itself in $A[X]$ as the set of terms with no occurence of X, we can view $A[X]$ as an algebra over A.

If A is a subring of a ring B, then each polynomial

$$f = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$$

gives rise to a function from B to itself, mapping $x \in B$ to

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in B.$$

This gives a homomorphism from $A[X]$ to the ring A^A. The dual of this is the *evaluation homomorphism*. Given $x \in B$, we obtain a homomorphism $\text{ev}_x : A[X] \to B$ mapping f to $f(x)$. Thus we can interpret $A[X]$ as the *free commutative A-algebra* generated by X, i.e. the 'most general' way of adding an additional element to the ring A.

Remark. If A is *not* a commutative ring, we may still define $A[X]$ as in the commutative case. But the evaluation maps are now *not* necessarily homomorphisms. For instance, over the Hamiltonian ring $\mathbf{H}$, in $\mathbf{H}[X]$ we find

$$(x+i)(x-i) = x^2 + 1$$

yet

$$(j+i)(j-i) = 2k \quad \text{and} \quad j^2 + 1 = 0.$$

In fact, for $x \in A$, $\text{ev}_x : A[X] \to A$ is a homomorphism if and only if $x \in Z(A)$, since if ev_x is a homomorphism, then for any $a \in A$, the polynomial X, times the constant a, is equal to aX. Thus

$$\text{ev}_x(Xa) = \text{ev}_x(aX) = ax$$

whereas

$$\text{ev}_x(X)\text{ev}_x(a) = xa.$$

Thus $ax = xa$ for any $a \in A$.

If A and B are rings, then each homomorphism $\varphi : A \to B$ extends uniquely to a *reduction* homomorphism from $A[X]$ to $B[X]$ such that for each $a \in A$, the diagram below commutes

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

The diagram forces us to define the mapping as

$$a_0 + a_1 X + \dots + a_n X^N \mapsto \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$$

The most important case of the reduction homomorphism we will consider is when we consider an ideal $\mathfrak{a}$ in A, and then obtain the reduction homomorphism $A[X] \to (A/\mathfrak{a})[X]$; for instance, we can reduce an integer polynomial in $\mathbf{Z}[X]$ modulo some prime p to obtain a polynomial in $\mathbf{Z}_p[X]$. If we abuse notation, also writing $\mathfrak{a}$ for the ideal in $A[X]$ generated by $\mathfrak{a}$, then $A[X]/\mathfrak{a}$ is actually isomorphic to $(A/\mathfrak{a})[X]$. This is because a polynomial $a_0 + \dots + a_n X^n$ is in the kernel of the reduction map if and only if $a_0, \dots, a_n \in \mathfrak{a}$, which occurs if and only if $a_0 + \dots + a_n X^n \in \mathfrak{a}$.

Corollary 2.1. *If $\mathfrak{a} \subset A$ is a prime ideal, then $\mathfrak{a} \subset A[X]$ is a prime ideal.*

2.2 The Euclidean Algorithm

If $f = a_0 + \dots + a_n X^n \in A[X]$ is a non-zero polynomial with $a_n \neq 0$, we define the *degree* of f, denoted $\deg(f)$, to be n - the largest index with a nonzero coefficient in A. If $f = 0$, we define the degree of f to be $-\infty$. One can think of the degree of a polynomial as a measure of complexity of the corresponding arithmetic structure. The simplest polynomials are the *linear* polynomials, which have degree one. Upping the difficulty gives us the *quadratic* polynomials of degree two, the *cubic* polynomials of degree three, and so on and so forth. Looking at the operations defining polynomial addition and multiplication, it is easy to see that for any $f, g \in A[X]$,

$$\deg(f + g) \leqslant \max(\deg(f), \deg(g)),$$

and provided one of the leading coefficients of f or g is not a zero divisor,

$$\deg(fg) = \deg(f) + \deg(g)$$

thus multiplication of two polynomials always bilinearly magnifies the complexity of the polynomial. The multiplicative identity shows that the degree gives a *filtration* turning $A[X]$ into a *graded algebra*.

Remark. Note that the reason why we define $\deg(0) = -\infty$ is precisely so that these equations continuous to hold even if we do not assume the polynomials involved are nonzero.

Lemma 2.2. *If A is an integral domain, then $A[X]$ is an integral domain, and the units of $A[X]$ are precisely the units of A.*

Proof. The degree formula guarantees that if $fg = 0$, then $\deg(fg) = \deg(f) + \deg(g) = -\infty$, so either $\deg(f) = -\infty$, or $\deg(g) = -\infty$, which implies either $f = 0$ or $g = 0$. Thus $A[X]$ is an integral domain. Now suppose $f, g \in A[X]$ and $fg = 1$. Then $\deg(fg) = \deg(f) + \deg(g) = 0$. Thus $\deg(f) = \deg(g) = 0$, so $f, g \in A$. Thus $U(A[X]) = U(A)$. □

One of the most important facts about the degree of a univariate polynomial is that we can perform the Euclidean algorithm on them, which gives the ring $A[X]$ properties analogous to the ring of integers.

Theorem 2.3. *If $f, g \in A[X]$ and the leading coefficient of g is a unit, then there exists polynomials $h, r \in A[X]$ such that*

$$f = gh + r,$$

and deg$(r) <$ deg(g).

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

$$f = a_0 + a_1 X + \dots + a_n X^n \qquad g = b_0 + b_1 X + \dots + b_m X^m$$

Then

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

so by induction,

$$f - a_n b_m^{-1} X^{n-m} g = hg + r$$

where $\deg(r) < \deg(g)$. But this implies

$$f = (h + a_n b_m^{-1} X^{n-m}) g + r$$

so we have found an expansion for f. □

We have found that every polynomial ring is 'almost' a Euclidean domain, except that the expansion properties of the domain only hold for polynomials whose leading term is invertible. In particular, this means that if A is a field K, then *any* nonzero polynomial $A[X] = K[X]$ satisfies this property, and so the general argument for Euclidean domains gives the following corollary.

Corollary 2.4. *If K is a field, then $K[X]$ is a principal ideal domain.*

Proof. Let $\mathfrak{a}$ be a nonzero ideal of $K[X]$, and let g be a nonzero element of $\mathfrak{a}$ with smallest degree. Given any $f \in \mathfrak{a}$, the Euclidean algorithm enables us to find h and r with $f = gh + r$, where $\deg(r) < \deg(g)$. Since $r = f - gh \in \mathfrak{a}$, we conclude that $r = 0$. Thus we conclude that $\mathfrak{a} = (f)$. □

Corollary 2.5. *If K is a field, then $K[X]$ is factorial.*

Remark. For any nonzero ideal $\mathfrak{a}$ in $K[X]$, then $\mathfrak{a}$ is a generated by any f in $\mathfrak{a}$ where f is nonzero and has the smallest possible degree in $\mathfrak{a}$. But we can choose a unique generator by requiring $\mathfrak{a}$ to be monic, since if f and g are monic polynomials of smallest degree in $\mathfrak{a}$, then $\deg(f - g) < \deg(f)$, so we conclude $f - g = 0$, hence $f = g$.

Theorem 2.6. *Let A be an integral domain, and fix $f \in A[X]$.*

- *If $f(a) = 0$, then $X - a$ divides f.*
- *If $f \neq 0$, then f can have at most* $\deg(f)$ *roots in F.*

Proof. Since $X - a$ has degree 1, we may use the Euclidean alogrithm to find a polynomial $g \in A[X]$ and $r \in A$ such that we may write $f = g(X - a) + r$. Since $f(a) = r$, we conclude $r = 0$. If we have n distinct roots $a_1, \dots, a_n$, we may apply induction to write $f = r(X - a_1)\dots(X - a_n)$. The degree of the left hand side is n, and the degree of the right hand side is $n + \deg(r)$, hence $\deg(r) = 0$, so r is a nonzero constant. If $b \neq a_i$ for any i, then

$$f(b) = r \cdot (b - a_1)\dots(b - a_n) \neq 0$$

Thus f can have at most n roots. □

Corollary 2.7. *If A is an integral domain, $f \in A[X]$, and $f(a) = 0$ for infinitely many $a \in A$, then $f = 0$.*

For finite integral domains, non-zero polynomials may still induce the zero function. For instance, if K is a finite field of order n, then $x^n = x$ for all $x \in K$. Thus the polynomial $X^n - X$ induces the zero function on K, yet $X^n - X$ is not formally the zero polynomial. This causes problems in certain problems where we must find a nonzero polynomial of low degree vanishing over a set of points in some K^n in an interesting way. Fortunately, the next lemma shows that these techniques generalize provided we can bound the degree of the nonzero terms.

Lemma 2.8. *Let K be a finite field with n elements. If $f \in K[X]$ induces the zero function on K, and deg$(f) < n$, then $f = 0$.*

Proof. If f is nonzero but induces the zero function on K, then we obtain a contradiction by factoring out the linear terms corresponding to each element of K, which contradicts the degree of f. □

Now suppose K is a finite field with n elements, and $f \in K[X]$. Given f, the *reduced form* of f is a polynomial $g \in K[X]$ with $\deg(g) < n$ and $f(x) = g(x)$ for all $x \in K$. Repeatedly using the identity $x^n - x = 0$ in K shows that reduced forms always exist, and the above lemma shows they are unique.

Theorem 2.9. *If A is an integral domain, every finite subgroup of A^* is cyclic.*

Proof. Let G be such a subgroup. Since G is abelian, we can write it as the product of p groups, and so it suffices to prove the theorem by proving that a p-subgroup of A^* is abelian. Let x be an element of G of maximal period p^r. Then all elements of G are roots of the polynomial $X^{p^r} - 1$. But we know that there can only be at most p^r roots, and so G consists precisely of these roots, which are $x, x^2, \dots, x^{p^r}$. □

Example. *If K is a finite field, then K^* is cyclic. In particular, $\mathbf{Z}_p^*$ is cyclic for each prime p; however, the proof above is not constructive, so we do not actually have efficient ways of* finding *generators for $\mathbf{Z}_p^*$ when p is a large prime.*

Example. *For each n, the set μ_n of n'th roots of unity, i.e. solutions to the equation $X^n - 1$ over $\mathbf{C}$, forms a finite subgroup of $\mathbf{C}^*$, and is therefore cyclic. The set $\mu = \bigcup_{n=1}^\infty \mu_n$ is a group, the group of all roots of unity. More generally, over any algebraically complete field K, we can conisder the groups $\mu_n(K)$ and $\mu(K)$. If K is a finite field with n elements, then $K^* = \mu(K)$, since all elements of K^* are roots of the polynomial $X^{n-1} - 1$.*

2.3 Algebraic

Given a ring B with a subring A, we say $b \in B$ is *algebraic* over A if there is a nonzero polynomial $f \in A[X]$ such that $f(b) = 0$. Otherwise, b is called *trancendental*. It is fairly easy to show a particular element of a ring is algebraic (e.g. $\sqrt{2}$ is algebraic over $\mathbf{Q}$, since we can set $f(X) = X^2 - 2$), but it is often very difficult to show that an element of a ring is trancendental. We know that π and e are trancendental over $\mathbf{Q}$, but the proof is a difficult analytical argument. It is still an open question whether $\pi + e$ and π/e are trancendental; it is not even known whether they are irrational! For multivariate polynomial rings, the situation is even less understood. We say $b_1,\dots,b_n \in B$, we say these elements are *algebraically independent* over A if there is no polynomial $f \in A[X_1,\dots,X_n]$ with $f(b_1,\dots,b_n) = 0$.

2.4 Multivariate Polynomials

We can study multivariate expressions in a commutative ring by using multivariate polynomials. Given n variables $X_1,\dots,X_n$, we can consider 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. The set of all such expressions forms a ring over A, denoted $A[X_1,\dots,X_n]$. Let us list some commonly used properties of this ring.

- One can reduce multi-dimensional polynomial rings to univariate polynomial rings by noticing that

  $$A[X_1,\dots,X_n] = A[X_1,\dots,X_{n-1}][X_n],$$

  because every polynomial can be uniquely written as $\sum f_k X_n^k$ for some $f_k \in A[X_1,\dots,X_{n-1}]$, formed by factoring out the right powers of f_k.

- Given a tuple $b = (b_1,\dots,b_n) \in B^n$, where A is a subring of a ring B, we can consider an evaluation morphism $\text{ev}_b : A[X_1,\dots,X_n] \to B$, as in the one-dimensional case.

- Given a homomorphism $f : A \to B$, there is a unique homomorphism from $A[X_1,\dots,X_n]$ to $B[X_1,\dots,X_n]$ causing the evaluation diagrams to commute.

- The polynomials $X_1^{i_1} \dots X_n^{i_n}$ are known as *primitive monomials*. 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 in the expansion of the polynomial which have non-zero coefficients.

- Alternatively, if we want to focus on a particular variable, we define the degree of f with respect to X_n to be the degree of f viewed as an element of $A[X_1,\dots,X_{n-1}][X_n]$.

- A polynomial $f \in A[X_1,\dots,X_n]$ is *homogenous* of degree m if the only monomials $X^{i_1}\dots X^{i_n}$ occuring in f satisfy $i_1 + \dots + i_n = m$. If A is a subring of B, and $u, t_1,\dots,t_n \in B$, then we find

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

  Homogenous polynomials are precisely those polynomials satisfying this equation, provided that there exists algebraically independent $u, t_1,\dots,t_n$ in B over A, because then the fact that $f(ut_1,\dots,ut_n) = u^m f(t_1,\dots,t_n)$ implies

  $$f(YX_1,\dots,YX_n) = Y^m f(X_1,\dots,X_n)$$

  and looking at the terms in this expansion shows all monomials must have the same degree.

Just as in the univariate case, a nonzero multivariate polynomial cannot have too many zeroes.

Corollary 2.10. *Let $f \in A[X_1,\dots,X_n]$, where A is an integral domain. If there exists infinite sets $S_1,\dots,S_n \subset A$ such that $f(a_1,\dots,a_n) = 0$ for each $a_1 \in S_1,\dots,a_n \in S_n$, then $f = 0$.*

Proof. We prove by induction on n, the case $n = 1$ having already been proven. For each $a \in A$, we have an evaluation homomorphism

$$\text{ev}_a : A[X_1,\dots,X_n] \to A[X_1,\dots,X_{n-1}]$$

obtained by setting $X_n = a$. By induction, we know $\text{ev}_a(f) = 0$ for each $a \in S_n$. Now write

$$f = \sum_{i_1,\dots,i_{n-1}} \left(\sum_{i_n} a_{i_1\dots i_n} X_n^{i_n} \right) X_1^{i_1} \dots X_{n-1}^{i_{n-1}}$$

Since $\mathrm{ev}_a(f) = 0$ for each $a \in S_n$, then for each $i_1,\dots,i_{n-1}$, the polynomial $\sum_{i_n} a_{i_1\dots i_n} X_n^{i_n}$ has infinitely may zeroes, and thus vanishes identically. Thus $f = 0$, completing the induction. □

For finite fields we obtain a similar result after applying a reduction.

Lemma 2.11. *Suppose K is a finite field with m elements. If $f \in K[X_1,\dots,X_n]$ induces the zero function on K^n and has degree less than m in each variable $\{X_1,\dots,X_n\}$, then $f = 0$. The ideal of functions vanishing on K^n is precisely*

$$(X_1^m - X_1,\dots,X_n^m - X_n).$$

Proof. We proceed by induction. Write

$$\mathfrak{a} = (X_1^m - X_1,\dots,X_n^m - 1).$$

Suppose $f \in K[X_1,\dots,X_n]$ has degree less than m in each variable and induces the zero function on K^n. Write

$$f = \sum_{i_1,\dots,i_{n-1}} \left(\sum_{i_n} a_{i_1\dots i_n} X_n^{i_n} \right) X_1^{i_1} \dots X_{n-1}^{i_{n-1}}$$

The inductive case applies that for each $i_1,\dots,i_{n-1}$, the polynomial $\sum_{i_n} a_{i_1\dots i_n} X^{i_n}$ induces the zero function on K. Since the degree in i_n is less than m, $a_{i_1\dots i_n} = 0$ for all $i_1,\dots,i_n$. This completes the proof of the first property of this lemma.

Now write

$$\mathfrak{a} = (X_1^m - X_1,\dots,X_n^m - X_m)$$

If $f \in K[X_1,\dots,X_n]$ induces the zero function on K^n, then it is certainly equivalent modulo $\mathfrak{a}$ to a polynomial $g \in K[X_1,\dots,X_n]$ with degree less than m in each variable. But then g induces the zero function on K^n, hence $g = 0$, so $f \in \mathfrak{a}$. □

2.5 Polynomials over a Factorial Ring

Let A be an integral domain. If K is the field of fractions of A, then $K[X]$ is a principal ideal domain, hence factorial. One might naturally ask what the relation is between the divisibility theory of $A[X]$ and the divisibility theory of $K[X]$. Normally this can be obtained by 'cancelling denominators' of equations in $K[X]$ to obtain equations in $A[X]$. Clearly we cannot use this fact to conclude $A[X]$ is factorial in general, since if $A[X]$ is factorial, A is factorial.

However, we can use this technique to prove $A[X]$ is factorial if A is factorial, a process we now carry out. Let A be a factorial ring. Since A is an integral domain, we may consider the field of fractions K. We shall show that $f \in A[X]$ is irreducible over $K[X]$ if and only if f is irreducible over $A[X]$, and if the greatest common denominator of the coefficients of f is equal to zero. For each prime $p \in A$, and non-zero $x \in K$, 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 $\text{ord}_p(x)$. Just as with polynomials, we have

$$\text{ord}_p(x+y) \geqslant \min\left(\text{ord}_p(x), \text{ord}_p(y)\right) \qquad \text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$$

If $x = 0$, we define $\text{ord}_p(x) = \infty$ so that these identities continue to hold. Any prime $p \in A$ is also a prime in $A[X]$, so we can define $\text{ord}_p(f)$ for each $f \in A[X]$; if $f = a_0 + \dots + a_n X^n$, then

$$\text{ord}_p(f) = \min\left(\text{ord}_p(a_0), \dots, \text{ord}_p(a_n)\right).$$

If A is a factorial ring, we define the *content* $\text{cont}(f) \in A$ of a non-zero $f \in A[X]$ to be the greatest common denominator of the coefficients of f (technically, we must interpret $\text{cont}(f)$ as a coset of A modulo it's units, but we abuse notation here). If we pick a prime p from each coset of primes identified up to units, then

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

If $f = 0$, define $\text{cont}(f) = 0$. Then the content is unique up to a unit in A. We may always write $f = \text{cont}(f) g$, where g is a polynomial in $A[X]$ with unit content (such polynomials are known as *primitive*.

Lemma 2.12 (Gauss). *Let A be a factorial ring, and K it's field of fractions. Then for $f, g \in K[X]$, $cont(fg) = cont(f) \cdot cont(g)$.*

Proof. Assume without loss of generality that f and g have unit content. Then it suffices to prove fg has unit content. Let $p \in A$ be a prime, denote $A/(p)$ by B, and consider the reduction homomorphism $\varphi : A \to B$, which extends to a map $\varphi : A[X] \to B[X]$. Since $\varphi(f)$ and $\varphi(g)$ are nonzero polynomials, and p is prime, $\varphi(fg)$ is a nonzero polynomial. □

Corollary 2.13. *Suppose A is a factorial ring, let $f \in A[X]$ be primitive, and let K be the field of fractions of A. Then f is irreducible in $A[X]$ if and only if it is irreducible in $K[X]$.*

Proof. Suppose $f \in A[X]$ is primitive and irreducible over $A[X]$, and suppose $f = gh$, where $g, h \in K[X]$. Then we can find primitive polynomials $g_0, h_0 \in A[X]$ and $a_0, b_0 \in A$ such that $a_0 g = g_0$, $b_0 h = h_0$. If $c = a_0 b_0$, then $cf = g_0 h_0$. But then since g_0 and h_0 is primitive, we conclude by Gauss' lemma that c is a unit in A. Thus $f = (g_0/c)h_0$, where $g_0/c, h_0 \in A[X]$, and so we conclude that either g_0 or h_0 is a unit in $A[X]$, and thus either g or h is a unit in $K[X]$.

Conversely, if $f \in A[X]$ is primitive and irreducible over $K[X]$, and if $f = gh$ for $g, h \in A[X]$, then either g or h is a unit in $K[X]$,which implies that either g or h is a constant. Since $\text{cont}(g)\text{cont}(h) = 1$, this implies that either g or h is a unit in A. □

Corollary 2.14. *If A is factorial, then $A[X_1, \dots, X_n]$ 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. Let K be the field of fractions of A. If $f \in A[X]$, we may write

$$f = g_1 \cdots g_n$$

where g_n are irreducible elements of $K[X]$. Now write $g_i = a_i g_i'$, where g_i' is a primitive polynomial in $A[X]$. Thus $f = (a_1 \dots a_n) g_1' \dots g_n'$. Each g_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

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

where each p_i is an irreducible element of A (and thus irreducible over $A[X]$). Thus

$$f = p_1^{k_1} \dots p_m^{k_m} g_1' \cdots g_n'$$

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

$$p_1^{k_1} \dots p_m^{k_m} g_1 \dots g_n = q_1^{l_1} \dots q_r^{l_r} h_1 \dots h_t$$

Then by unique factorization in $K[X]$, we must have $t = n$, and after some rearranging, $f_i = u_i g_i$, for some nonzero $u_i \in K$. But since f_i and g_i are primitive, we may assume without loss of generality that u_i is a unit in A. Cancelling out appropriate factors, we conclude that

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

and we may now apply unique factorization in A. □

Note that for $n \geqslant 2$, the ring $K[X_1, \dots, X_n]$ is not principal. Indeed (X, Y) is an ideal in $K[X, Y]$ which cannot be principal, for no non unital element divides both X and Y. Thus the fact that these rings are factorial is truly a novel part of the proof above.

2.6 Criterion for Irreducibility

It is actually quite tricky to determine whether a given polynomial 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. We begin with a powerful result for polynomials over factorial rings.

Theorem 2.15 (Integral Root Test). *Let A be a factorial ring, and K its quotient field. Let*

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

Suppose $f(b/d) = 0$, where b and d are relatively prime. Then b divides a_0, and d divides a_n. In particular, if $a_n = 1$, then the only roots of f are in A.

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. □

Example. *The polynomial X^3-3X-1 is irreducible in $\mathbf{Z}[X]$. If the polynomial was reducible, it would have an integer root. But the integral root test implies that the only possible roots are either $+1$ or -1. Neither gives a root, completing the proof.*

Example. *For any prime $p \in \mathbf{Z}$, the polynomials $X^2 - p$ and $X^3 - p$ are irreducible in $\mathbf{Z}[X]$. To see this, they would only be reducible if they had an integer root. But the only possible integer roots are either p or $-p$ by the integral root test, completing the proof.*

Another way to prove a polynomial is irreducible is to reduce the polynomial's coefficients modulo an ideal, detailed in the next proposition. In the case $\mathbf{Z}[X]$, we reduce modulo a prime to obtain an element of $\mathbf{F}_p[X]$, and we can easily check this polynomial's properties since $\mathbf{F}_p$ is finite.

Theorem 2.16 (Reduction Criterion)**.** *Let A and B be integral domains and consider a surjective homomorphism $\varphi : A \to B$. If $f \in A[X]$, $\varphi(f)$ has the same degree in f, and $\varphi(f)$ cannot be factored into two polynomials of smaller degree in B, then f is irreducible.*

Example. *Consider the polynomial $X^2 + XY + 1 \in \mathbf{Z}[X,Y]$. View $\mathbf{Z}[X,Y]$ as $\mathbf{Z}[Y][X]$. Let $\phi : \mathbf{Z}[X,Y] \to \mathbf{Z}[X]$ be the homomorphism obtained by setting $Y = 0$. Then $\phi(X^2 + XY + 1) = X^2 + 1$ has the same degree in X. Moreover, $X^2 + 1$ is irreducible in $\mathbf{Z}[X]$, and so $X^2 + XY + 1$ is irreducible in $\mathbf{Z}[X,Y]$ by the reduction criterion.*

Theorem 2.17 (Eisenstein)**.** *Let A be an integral domain, and let $\mathfrak{a}$ be a prime ideal. Consider a polynomial*

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[X],$$

with $a_0,\dots,a_{n-1} \in \mathfrak{a}$, but $a_0 \notin \mathfrak{a}^2$. Then f is irreducible in $A[X]$.

Proof. Let $\phi : A \to A/\mathfrak{a}$ denote the reduction homomorphism. If $f = gh$ for $g,h \in A[X]$, then $X^n = \phi(f) = \phi(g)\phi(h)$. Since $(A/\mathfrak{a})$ is an integral domain, the only divisors of X^n in $(A/\mathfrak{a})[X]$ are powers of X^n multiplied by a unit, so $\phi(g) = tX^m$, $\phi(h) = t^{-1}X^l$ for some $t \in U(A/\mathfrak{a})$, where $m + l = n$. If $m,l > 0$, this gives a contradiction, for it implies $g(0),h(0) \in \mathfrak{a}$, and thus $a_0 = g(0)h(0) \in \mathfrak{a}^2$. This we may assume without loss of generality that $m = 0$. But then $\deg(h) = n$, $\deg(g) = 0$. Thus g is a constant, and since f is monic, this implies that g is actually an element of $U(A)$. □

Example. *Eisenstein's criterion's can often be used to determine when the polynomial $X^n - a \in \mathbf{Z}[X]$ is irreducible, i.e. when some prime p divides a, but p^2 does not. This shows $X^n - 6$ and $X^n - 4$ are irreducible. On the other hand, this cannot detect that $X^3 - 8 = (X-2)(X^2+2X+4)$ is irreducible.*

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

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

All coefficients of this polynomial are divisible by p except for the higher order term, which is equal to one, and the lowest term is $\binom{p}{1} = p$, so Eisenstein's criterion tells us the polynomial is irreducible.

Example. *Let K be a field, and consider the field of rational functions $K(X)$. The polynomial $Y^n - X$ is irreducible in $K(X)[Y]$. Note first that $Y^n - X$ has content one with respect to $K[X]$, so $Y^n - X$ is irreducible over $K(X)[Y]$ if and only if it is irreducible over $K[X][Y]$. But over $K[X][Y]$ we may apply Eisenstein's criterion, since X is a prime in $K[X]$, to conclude that $Y^n - X$ is irreducible.*

2.7 Partial Fractions

Theorem 2.18. *Let A be a factorial ring, and let K be its quotient field. Choose a representation $\{p_i\}$ of primes. Then for each $a/b \in K$ there is $a_i \in A$ and $j_i \in \mathbf{N}$ for each p_i such that almost all a_i are zero, and*

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

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

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

Thus for any $c \in A$,

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

By induction, we may write

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

Hence

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

□

Chapter 3

Fields, and their Extensions

Galois theory was invented to study polynomials over the rings

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

Without much added effort, the methods can be extended to arbitrary fields. This is not generalization for generalization's sake; in number theory and cryptography, we are interested in studying finite fields. In algebraic geometry, we are interested in fields of rational functions. Under a general formulation, Galois theory applies unperturbed. This modern approach was advanced by the 20th century mathematician Emil Artin. In Artin's formulation, the main object of study is a *field extension*, a pair $F \subset E$ of fields, the first contained within the latter. We write the extension as E/F, read "E over F". Artin's main contribution to the foundations of Galois theory was to view E as an algebra over F, through which we can apply the robust techniques of linear algebra. Most importantly, at least in the basic theory, we can talk of a basis of F over E. The dimension of E as an F vector space will be denoted $[E : F]$, and called the *degree* of the extension. If the dimension is finite, we say E/F is a *finite* extension. Note that this is different from a *finitely generated* extension, which occurs when E is a finite dimensional algebra over F.

Remark. Categorically speaking, 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, since in the morphism scenario we may consider F as extending $i(E)$ rather than E.

Example. *The field* $\mathbf{C}$ *of complex numbers is a field extension of the real numbers* $\mathbf{R}$*. This is because any complex number can be written uniquely as* $a + bi$*, where* a *and* b *are real numbers, so that* $\{1, i\}$ *is a basis for* $\mathbf{C}$ *as a* $\mathbf{R}$ *vector space, and so* $[\mathbf{C} : \mathbf{R}] = 2$*.*

Example. *It turns out that the set of real numbers which can be expressed as* $a + b\sqrt{2}$*, where* a *and* b *range over rational numbers, forms a field, which we denote by* $\mathbf{Q}(\sqrt{2})$*, which extends* $\mathbf{Q}$*. Since* $\sqrt{2}$ *is an irrational number, the expansion* $a + b\sqrt{2}$ *is unique for each element of* $\mathbf{Q}(\sqrt{2})$*, so that* $\{1, \sqrt{2}\}$ *is a basis for* $\mathbf{Q}(\sqrt{2})$*, an so* $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$*.*

Example. *Even in the classical situation, a field extension need not have a finite degree. Since* $\mathbf{R}$ *is uncountable, and* $\mathbf{Q}$ *countable,* $[\mathbf{R} : \mathbf{Q}]$ *has the same cardinality of* $\mathbf{R}$*, namely* $\mathfrak{c}$*. If* K *is any field, then the field* $K(X)$ *of rational functions over* K *is an infinite field extension of* K*, since the set* $\{1, X, X^2, \dots\}$ *is linearly independant over this field.*

Example. *Every field* K *is the extension of its prime subfield, the smallest field contained in* K*. This field is characterized by the characteristic of* p*. If* K *has characteristic* $p > 0$*, then the prime subfield is* $\mathbf{F}_p$*, and if* K *has characteristic 0, then the prime subfield is isomorphic to* $\mathbf{Q}$*. It follows that* $\mathbf{F}_p$ *and* $\mathbf{Q}$ *are the fundamental base fields with which to study field extensions.*

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

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

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

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

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

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

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

The left side is prime, which implies either $[F : K] = 1$, or $[K : E] = 1$. We conclude $K = F$ or $K = E$. As a particular case of this argument, we conclude there is no proper field between **R** *and* **C**.

If E is a subfield of F, and $S \subset F$, we will denote by $E(S)$ the smallest subfield of F to contain both E and S, and $E[S]$ the smallest subring. In particular, if $\mathcal{B}$ is a basis for an extension E/F, then $F = E(\mathcal{B})$. Notationally, this parallels the polynomial rings and fields $F[X]$ and $F(X)$. If we take the free commutative monoid G generated by the set S (which is really just the polynomial ring with the elements of S interpreted as variables), 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 a formal sum, whereas on the right we multiply elements of S together. When $F[G]$ is localized, we obtain the field $F(G)$, and the corresponding evaluation is surjective onto $F(S)$.

The category of fields is suprisingly restrictive. No products exist, nor coproducts. The only construction which is used systematically 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. If K is a field, then we find equations like $K(x)K(y) = K(x,y)$, which often turn out to be useful.

3.1 Algebraic and Simple Extensions

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

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

a is *algebraic* over F if it is the root of some polynomial in $F[X]$. Then ev_a has a non-trivial kernel $\mathfrak{a}$, and $F[X]/\mathfrak{a} \cong F[a]$. Since $F[a]$ is entire, $\mathfrak{a}$ is a prime ideal, hence it is maximal. Thus we conclude $F[X]/\mathfrak{a}$ is a field, which implies $F[a]$ is a field, so $F[a] = F(a)$. Note that the converse of this statement, that if $F[a] = F(a)$, then a is algebraic over F, is also true, since then a has an inverse $f(a)$, hence $af(a) = 1$, and so $Xf(X) - 1$ vanishes at a. Because $F[X]$ is a principal ideal domain, $\mathfrak{a}$ can be uniquely written as (f), for some monic polynomial f. One calls f the *minimal polynomial* of a, sometimes denoted by $\text{Irr}(F,a)$. If $\deg(\text{Irr}(F,a)) = n$, then $\{1, a, a^2, \dots, a^{n-1}\}$ form a basis for $F(a)$, which implies the degree of the extension is the same as the degree of the minimal polynomial.

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, and we have already seen that $\{1, \sqrt{2}\}$ form a basis for $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$.*

Example. *Let $F(\alpha)/F$ be an extension of odd degree n. Then we have*

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$$

If $f = Irr(F, \alpha^2)$ and $g = Irr(F, \alpha)$, then $f(\alpha^2) = 0$, implying $g(X)$ divides $f(X^2)$, hence $[F(\alpha^2) : F] \leqslant 2[F(\alpha) : F].w111$

Then $F(\alpha) = F(\alpha^2)$. To see this, let f denote the irreducible polynomial of α. Then

Remark. The opposite of an algebraic number is being *trancendental*, that is, an element a is trancendental over F if no polynomial f has $f(a) = 0$. For instance, the numbers e and π are trancendental over $\mathbf{Q}$, though this is incredibly difficult to prove. From this, it follows that $F(a)$ is isomorphic to the field $F(X)$ of rational functions in a single variable. For obvious reasons, non-algebraic extensions are harder to analyze than algebraic extensions, and we leave their analysis till later.

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

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

It follows tht if $[E : F]$ is finite, it cannot contain any trancendental elements.

One trick to the theory of algebraic field extensions is that because of the discrete equations which define the extensions, they act in a 'compact' manner, so almost all statements about finite fields can be extended to statements about algebraic fields. 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 3.2. *If E/F is an extension, and $\{u_i\}$ is a basis for E over F, and each u_i is algebraic over F, then E/F is algebraic.*

Proof. Since each u_{i_k} is algebraic, each $\text{Irr}(F(u_{i_1}, \dots, u_{i_{n-1}}), u_{i_n})$ exists, so

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

so $F(u_{i_1}, \dots, u_{i_n})/F$ is a finite extension, hence algebraic. □

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

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

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

Theorem 3.3. *If F/E is an extension, then the set of algebraic elements in F form an algebraic field over E.*

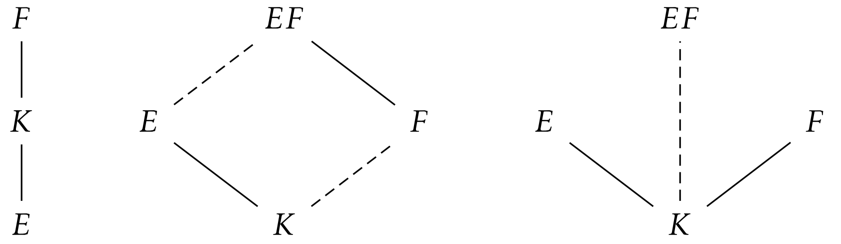
Proof. If a and b are algebraic, then $E(a,b)/E$ is an algebraic extension, so $a+b$, ab, and if $a \neq 0$, a^{-1} are all algebraic over E. □

Example. $\mathbf{C}$ *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.



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

Theorem 3.4. *The class of algebraic extensions is distinguished.*

Proof. Let us first verify the tower property. If F/E is algebraic, then K/E and F/K must be algebraic, by inclusion properties. On the other hand, let F/K and K/E be algebraic. Let $x \in F$ be given. Then there is an irreducible polynomial $P \in K[X]$ for x. Let $P = \sum a_i X^i$. Then $[F(x) : F(a_0, \dots, a_n)] < \infty$. But also $[F(a_0, \dots, a_n) : K] < \infty$, since each a_i is algebraic over K. By the tower formula, we conclude that x is algebraic over E. Now let's verify the lifting property. Let E/K be an algebraic extension. The set of elements in EF algebraic over F is a field containing E and F, since $F \subset K$, which implies that every element of EF is algebraic over F. □

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 3.5. *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. □

The existence of certain F-morphisms is incredibly important to Galois theory, for they begin to unveil the symmetries of certain fields, in particular, relating the symmetries of roots of a polynomial. Notationally, it will help to write an application of a morphism $f(x)$ as x^f, to avoid being suffocated by brackets.

Lemma 3.6. *Let $F : K \to L$ be a field morphism, and let $f = Irr(K, a)$. Then F extends to a map on $K(a)$ if and only if f^F has a root in L. The number of extensions is the number of unique roots of P^f in L.*

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

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

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

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

Which is exactly the map required. We have found all such maps, for any map is determined by its action on a. □

Corollary 3.7. *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 more naturally than adding $\omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$. Yet we have shown that the resulting fields introduced are algebraically isomorphic, so, without adding any additional numbers, there is no way to distinguish $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$ over the rational numbers. 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 3.8. *Every endomorphism $f : E/K \to E/K$ of algebraic extensions is an automorphism.*

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

3.3 Algebraic Closure

In terms of looking at polynomial equations, the nicest fields are *algebraically closed*, that is, if every non-constant polynomial has a root. This is a natural place for Galois theory, which was built to study the algebraically closed field **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 3.9. *For any polynomial $f \in K[X]$, there is an algebraic extension L/K in which f has a root.*

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

Theorem 3.10. *Every field has an algebraic closure.*

Proof. We shall apply the elementary theory of first order logic. The theory of fields is a first-order theory. A field is simply a normal model of this theory. Given a field F, enlarge the language of the theory of fields to contain all elements of F as constants, and to add the additional axioms which force the constants to behave exactly like they behave in F. That is, we add the axioms $a + b = c$ and $ab = c$ whenever these equations hold in F. This new theory is still consistant, for it has a model. For each $a_1, \dots, a_n \in F$, 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_1, with $F \subset F_1$, such that for any polynomial $f \in F[X]$, there is $a \in F_1$ with $f(a) = 0$. We may clearly shrink F_1 so that it is algebraic. Now proceed inductively, forming

$$F \subset F_1 \subset F_2 \subset \dots$$

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. □

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

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

Theorem 3.11. *Let K/E be an algebraic extension. If $f : E \to L$ is an embedding of E in an algebraically closed field, then f extends to an embedding of K. If E is an algebraic closure, and L is algebraic over $f(E)$, then the extension is an isomorphism.*

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

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

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

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

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. **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

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

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

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

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

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

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 3.13. *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 $u_i \in K$, $v_i = f(u_i)$,

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

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

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

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

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

Corollary 3.14. *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 3.15. *Any splitting fields of a family of polynomials are isomorphic.*

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

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

Lemma 3.16. *If F/E is normal, every $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$.*

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

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

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

Theorem 3.17. *If F/E is an extension for which every $\sigma : F/E \to F^{\mathfrak{a}}/E$ satisfies $\sigma(F) = F$, then F/E is normal.*

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

Corollary 3.18. *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 $\sigma : F/E \to F^{\mathrm{a}}/E$ be a morphism. Then $\sigma(F) \subset F$, for if x is a root of $P \in \mathcal{F}$, then x^σ is a root of P, so $x^\sigma \in F$. The relation follows since F is generated by these roots. Hence the splitting field is normal. Conversely, let F/E be normal. For each $x \in F$, consider the minimal polynomial $P_x \in E[X]$. Then $P_x(x) = 0$, so F splits P_x. But this implies exactly that F is the splitting field of $\{P_x : x \in F\}$. □

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

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

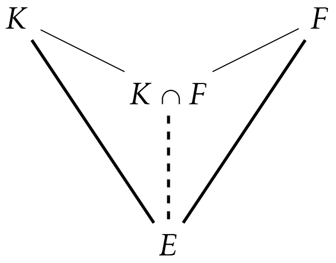
Theorem 3.19. *If $K \subset E \subset F$, and if F/K is normal, then F/E is normal.*

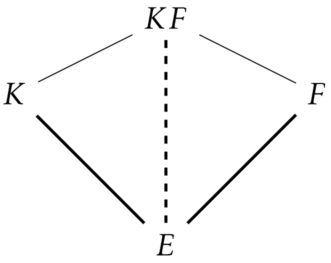
Proof. For if F is a splitting field for a family of polynomials in $K[X]$, then F is a splitting field for a family of polynomials in $E[X]$. □

Theorem 3.20. *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^{a}. Then f extends to isomorphisms from K and F into E^{a}. Since K and F are normal, $f(K \cap F) \subset f(K) \subset K$, and $f(K \cap F) \subset f(F) \subset F$, hence $f(K \cap F) \subset K \cap F$. □

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





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

3.5 Separability

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'[1], 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

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

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

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

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

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 3.21. *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

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

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. □

Theorem 3.22. *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 3.23. *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 3.24. *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

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

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 3.25. *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 $\mathbf{Q}^a$ 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 3.26. *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^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. □

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 3.27 (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. □

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 3.28. *$X^p - a$ 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 3.29. *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 $\mathbf{F}_p^a$ 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 $\mathbf{F}_p^a$ 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 3.30. *A finite multiplicative subgroup of a field is cyclic.*

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

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

Corollary 3.31. *Every extension F/K where F is finite and K is a finite field is simple.*

Corollary 3.32. *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 3.33. *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^a,

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

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

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

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

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

Theorem 3.34. *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. □

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 3.35. *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

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

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 3.36. *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 3.37. *The class of purely inseparable extensions is distinguished.*

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

Theorem 3.38. *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 3.39. *A separable and purely inseparable extension K/E is only possible if $K = E$.*

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

Theorem 3.40. *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^a satisfies $\sigma(K) \subset K$. If π embeds F in K^a, then π extends to a unique embedding of K in K^a. Since $\pi(F)$ is separable, hence $\pi(F) \subset F$. □

Chapter 4

Galois Theory

> This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.
>
> Hermann Weyl (On Galois' Notes)

Here we introduce the fundamental trick to Galois theory. Given a field extension F/E, we study the 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 $F^{\text{Gal}(F/E)} = E$, 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, $\text{Gal}(F/E)$ can naturally be realized as a subgroup of $\text{Gal}(F/K)$, 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 $K = F[x_1, \ldots, x_n]$. Then K is separable if and only if the polynomials $\mathrm{Irr}(F, x_i)$ are separable. Let $y_i^1, \ldots y_i^{k_i}$ be the roots of $\mathrm{Irr}(F, x_i)$. Then

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

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

Corollary 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 $[E:K] \leqslant n$. □

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 $\operatorname{Irr}(F,x)$. Since x was arbitrary, we find K/F is separable and normal, and therefore Galois. Since G is finite, and $[K:F]$ is equal to the order of G, K/F is finite. □

Corollary 4.7. *On a finite Galois extension, $Gal(K/-)$ is a surjective map.*

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

The set of intermediate fields between K and F form a partially ordered set under the $\subset$ relation. Similarily, the set of subgroups of $\operatorname{Gal}(F/K)$ 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 $F(X_1,\dots,X_n)$ of rational functions in n indeterminates, and let S_n act on $F(X_1,\dots,X_n)/F$ by permuting the indeterminates. This is an embedding of S_n in $Gal(F(X_1,\dots,X_n)/F)$, which thus corresponds to a finite subgroup G of the Galois group. Let us determine the fixed field $L = F(X_1,\dots,X_n)^G$, which corresponds to a finite, Galois extension $F(X_1,\dots,X_n)/L$. Consider the polynomial*

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

Expand Q to the form

$$Y^n - S_1Y^{n-1} + S_2Y^{n-2} + \dots + (-1)^k S_k Y^{n-k} + \dots + (-1)^n P_0$$

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

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

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

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

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 $F(S_1,\dots,S_n) \subset L$, we have $Gal(F(X_1,\dots,X_n)/L) \subset Gal(F(X_1,\dots,X_n)/F(S_1,\dots,S_n))$, so that the two Galois groups are equal. But this implies that $L = F(S_1,\dots,S_n)$ 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 $F(S_1,\dots,S_n) \subset L$. 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

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

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.