Galois Theory

Arnau Mas

2019

These are notes gathered during the subject *Teoria de Galois* as taught by Francesc Perera between September 2019 and January 2020.

Chapter 1

Preliminaries

1.1 The solution of low degree polynomial equations

It is surely well-known to any aspiring mathematician that there exist no general formulas for the solutions of polynomial equations of degree five and higher. This implies, of course, that such formulas exist for equations of degree fourth and lower. Indeed, the solution of linear equations is trivial and the quadratic formula should be more than well-known by this point. In this section we present a derivation of the solutions of both the quadratic and cubic equations.

1.1.1 The quadratic equation

First, note that we can, without loss of generality, assume that we are working with a monic equation since we may always divide through by the leading coefficient to obtain an equation with the same solutions and with leading coefficient 1. Thus, we are trying to solve $x^2 + bx + c = 0$. The standard method is completing the square, that is to write $x^2 + bx + c$ as a square, and one achieves so by adding and substracting $\frac{b^2}{4}$:

$$x^2 + bx + c = x^2 + bx + \frac{b^2}{4} - \frac{b^2}{4} + c = \left(x + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c.$$

Then the solutions to the original equation must satisfy

$$\left(x + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c.$$

If the term on the right is not a square in the field we are working over then there are no solutions in that field. On the other hand, if it is a square then it has two

square roots and the solutions to the original equation are

$$x = -\frac{b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c},$$

which is the well known quadratic formula.

1.1.2 The cubic equation

Less well-known is the formula for the solutions of the cubic equation. Whereas the quadratic formula had been known to the greeks and babylonians, the cubic formula was discovered later during the fifteenth century. There were several italian mathematicians involved in its discovery: Cardano, Ferrari and del Ferro among others. The question of the original discoverer is a contemptious matter.

The first step in the solution is a change of variables to eliminate the quadratic term. If $x = y - \frac{1}{3}b$ then the original (monic) polynomial becomes

$$\begin{aligned} x^3 + bx^2 + cx + d &= y^3 - by^2 + \frac{1}{3}b^2y - \frac{1}{27}b^3 + by^2 - \frac{2}{3}b^2y + \frac{1}{9}b^3 + cy - \frac{1}{3}bc + d \\ &= y^3 + \left(c - \frac{1}{3}b^2\right)y + \frac{2}{27}b^3 - \frac{1}{3}bc + d. \end{aligned}$$

Therefore we only need to be able to solve cubics of the form $x^3 + px + q = 0$.

The basic trick is similar to completing the square. We have the identity

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + 3uv(u+v) + v^3,$$

and rearranging we obtain $(u+v)^3 - 3uv(u+v) - u^3 - v^3 = 0$. One then notices that there are cubic and linear terms in $u+v$ but no quadratic terms. Then one tries to solve for u and v to then obtain x as $u+v$. u and v must satisfy $-3uv = p$ and $-u^3 - v^3 = q$. Multiplying this second condition by u^3 we get

$$u^6 + qu^3 + u^3v^3 = 0,$$

and using the fact that $uv = -\frac{1}{3}p$ we arrive at

$$u^6 + qu^3 - \frac{p^3}{27} = 0,$$

which is quadratic in u^3. If we instead had multiplied through by v^3 we would have arrived to the same equation for v^3 instead.

Up to now nothing we have done relied on any additional assumption on the field have been working over. From this point, however, the nature of the solutions

will depend on the behaviour of radicals in the field in question. We will assume we are working in $\mathbb{C}$. We can then solve for u^3 and v^3 to find

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
$$v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

The ambiguity with the signs is eliminated due to the fact that $u^3 + v^3 = -q$ so we find the only good options are those in which the signs of the square root terms are opposite, so that they will cancel when added. Since we only care about the sum of u and v we might as well choose

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

There are three possibilities for u and three for v. Indeed, every complex number has three roots and if a is one of them then so are ωa and $\omega^2 a$ where $\omega = e^{\frac{2\pi}{3}i}$. Not every combination of them leads to a solution of the cubic —if it were so we would have more than three roots and a cubic polynomial can only have three roots— since they are constrained by the relation $3uv = -p$. So, once we find u and v that satisfy this then so will ωu and $\omega^2 v$, as well as $\omega^2 u$ and ωv since $\omega^3 = 1$.

All together, one of the solutions to the cubic $x^3 + px + q = 0$ is given by

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

which is known as Cardano's formula. If we undo the change of variable to eliminate the quadratic term and use $p = c - \frac{1}{3}b^2$ and $q = \frac{2}{27}b^3 - \frac{1}{3}bc + d$ then we obtain the cubic formula in all of its glory:

$$x = -\frac{b}{3} + \sqrt[3]{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right) + \sqrt{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right)^2 + \left(\frac{c}{3} - \frac{b^2}{9}\right)^3}}$$
$$+ \sqrt[3]{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right) - \sqrt{\left(-\frac{b^3}{27} + \frac{bc}{6} - \frac{d}{2}\right)^2 + \left(\frac{c}{3} - \frac{b^2}{9}\right)^3}}.$$

1.2 Polynomial rings

The study of polynomial rings is particularly important in Galois theory since they play an important role in many of the constructions and definitions of the theory. Of special relevance is the study of their quotient rings.

1.2.1 The universal property of polynomial rings

Given a ring[1] R its polynomial ring $R[x]$ can be defined in various ways. Most commonly, the elements of $R[x]$ are said to be "formal sums" of the form

$$\sum_{k=1}^{n} a_k x^k$$

where the a_k are elements of R and x is refered to as an "indeterminate" or some other similarly ambiguous term. This definition may feel imprecise to the more technically inclined reader. A more exact definition of $R[x]$ is as the set of sequences of elements of R with finite suport. The sum is defined pointwise and the product is defined in a convoluted manner which correspond to the way one would multiply polynomials with repeated application of the distribuitive law. Then there is a canonical inclusion $R \hookrightarrow R[x]$ by way of $a \mapsto (a, 0, \cdots)$. And if we define x to be the sequence $(0, 1, \cdots)$ then we recover the more standard presentation of $R[x]$.

This discussion, however, is about what a programmer would call the implementation details and it misses the bigger picture. How $R[x]$ is constructed is not really what is relevant here. It is much more illuminating to think about what we want out of $R[x]$ instead. For one, $R[x]$ should contain R. We could require $R \subseteq R[x]$, but let's be more general and allow for an injective morphism $\iota\colon R \hookrightarrow R[x]$ that picks out a copy of R inside $R[x]$. The other important aspect of $R[x]$ is the indeterminate. The way to formalize it is with what is known as a universal property: for any morphism $\phi\colon R \to S$ and distinguished element $s \in S$ there is a unique morphism $\tilde{\phi}\colon R[x] \to S$ such that $\tilde{\phi} \circ \iota = \phi$ and $\tilde{\phi}(x) = s$. That is, $\tilde{\phi}$ must agree with ϕ on R and it must send x to s. This does indeed uniquely determine $\tilde{\phi}$. It can be shown that this determines $R[x]$ up to unique isomorphism, meaning there is a unique isomorphism between any two rings that satisfy the universal property. So you can construct $R[x]$ in whatever way you like so long as the result satisfies the universal property.

[1] We will always assume that we are dealing with commutative rings with identity unless otherwise stated.

One last remark about polynomial rings in many variables: once we have defined the polynomial ring of a ring $\mathbb{R}$, we can then proceed inductively to define the polynomial ring on n variables as $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$. Polynomial rings in more than one variables also satisfy a universal property, which is essentially the same as before except now we have to specify where $\tilde{\phi}$ sends all of the x_i.

This universal property is not just of theoretical importance, it is also extermely practical. Indeed, it provides a very quick way of specifying morphisms on a polynomial ring. All you need is to specify how it acts on the coeficients and where it sends the indeterminate and you're done.

Example 1.1. These are various examples of morphisms defined on a polynomial ring making use of the universal property.

(*i*) For any element $\alpha \in R$ we can define the evaluation morphism $\mathrm{ev}_\alpha \colon R[x] \to R$ such that $\mathrm{ev}_\alpha|_R = \mathrm{id}_R$ and $\mathrm{ev}_\alpha(x) = \alpha$. That is, simply evaluate a polynomial on the element $\alpha \in R$. The element we evaluate at need not be an element of R, in fact it can be an element of any ring which contains R.

(*ii*) A trick that is often used when working with polynomials is a change of variable. This idea can be made formal in terms of an automorphism of $R[x]$. Say we wanted to make the change $y = x + 1$, or $x = y - 1$. This amounts to defining a morphism $\phi \colon R[x] \to R[x]$ such that $\phi|_R = \mathrm{id}_R$ and $\phi(x) = y - 1$. ϕ does not move the coeficients and changes x to $y - 1$. More generally, we could perform a change of the form $\phi(x) = ay + b$. In order for ϕ to be an isomorphism, a must be invertible. Indeed, ϕ^{-1} sends x to $a^{-1}(x - b)$. Then, when showing that a certain polynomial is irreducible, for instance, we can do any change of variable we please and rest assured that the resulting polynomial will be irreducible if and only if the original one was irreducible, for irreducibility is preserved under isomorphism.

(*iii*) Any permutation $\sigma \in \mathfrak{S}_n$ induces an isomorphism on $R[x, \ldots, x_n]$ by permuting the variables according to σ. Indeed, let ϕ_σ be the unique morphism that is the identity on R and such that $\phi_\sigma(x_i) = x_{\sigma(i)}$. You can check that $\phi_\sigma \circ \phi_\tau = \phi_{\sigma\circ\tau}$. And as a corollary $\phi_\sigma^{-1} = \phi_{\sigma^{-1}}$. This is in fact an action of the symmetric group $\mathfrak{S}_n$ on $R[x_1, \cdots, x_n]$. The polynomials invariant under this action, $R[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ are known as the *symmetric polynomials*.

$\triangledown$

Chapter 2

Field extensions

2.1 Definition and examples

Definition 2.1 (Field extension)**.** We say a field F is an *extension* of a field K if K is a subfield of F. More generally, given any field K and an injective morphism $\iota\colon K \hookrightarrow F$ we will refer to the situation as a field extension and often identify K with $\iota(K)$ and simply write $K \subseteq F$. △

There are some immediate examples of field extensions such as $\mathbb{R} \subseteq \mathbb{C}$ and $\mathbb{Q} \subseteq \mathbb{R}$. In the following examples we detail the construction of three related kinds of extensions.

2.1.1 Simple extensions

Say we already have an extension $K \subseteq F$ and an element $\alpha \in F$. Then α induces an evaluation morphism, $\mathrm{ev}_\alpha\colon K[x] \to F$. Since $K[x]$ is a PID there must exist a polynomial $p(x) \in K[x]$ such that $\ker(\mathrm{ev}_\alpha) = \langle p(x)\rangle$. If we denote $\mathrm{im}(\mathrm{ev}_\alpha)$ by $K[\alpha]$ we have, by the Isomorphism Theorem

$$K[\alpha] \cong K[x]/\langle p(x)\rangle\,.$$

We also have $K \subseteq K[\alpha]$. Indeed, the image of a constant by ev_α is itself, so $K \subseteq \mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha]$. We can then consider the set $K(\alpha)$ which is the union of $K[\alpha]$ and the inverses of all of its nonzero elements —they exist since $K[\alpha] \subseteq F$—. This is isomorphic to the field of fractions of $K[\alpha]$. Thus we have $K \subseteq K[\alpha] \subseteq K(\alpha)$, meaning $K(\alpha)$ is a field extension of K. From the

Various things can happen with $K(\alpha)$. For one, if $\alpha \in K$ then $\mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha] = K$, which is to be expected since α was already in α. In this case then

$\ker(\mathrm{ev}_\alpha) = \langle x - \alpha) \rangle$, which is essentially the fact that a polynomial has α as a root if and only if it is divisible by $(x - \alpha)$.

If ev_α has a nontrivial kernel then it follows that its generator is irreducible. Indeed, since $K[x]/\langle p(x) \rangle \cong K[\alpha]$ and $K[\alpha]$ is a domain then $p(x)$ is prime, and therefore irreducible. This means that $\langle p(x) \rangle$ is a maximal ideal and $K[\alpha]$ is a field, so in this case $K[\alpha] = K(\alpha)$. If this is the case we say the element α is *algebraic* over K. The generator of $\ker(\mathrm{ev}_\alpha)$ is not unique, since any scalar multiple of a generator is also a generator. However, there is always a unique *monic* generator, which is called the *minimal polynomial of* α *over* K, written $m_{\alpha,K}(x)$ or simply $m_\alpha(x)$ if the base field is understood.

If, instead, ev_α has a trivial kernel then $K[\alpha] \cong K[x]/\{0\} \cong K[x]$ and so $K(\alpha) \cong K(x)$. This means that adding α to K is essentially like adding a free variable. We say α is *transcendental* over K. We will analyse the difference between this two cases later on.

Extensions of this sort are called *simple extensions* and α is called a *primitive element* of the extension.

2.1.2 Quotient of a polynomial ring by a maximal ideal

This is a way of constructing what are essentially simple extensions without requiring the prior existence of a primitive element in a larger extension.

The polynomial ring $K[x]$ is a PID which means that the ideal generated by an irreducible polynomial $p(x)$, $\langle p(x) \rangle$ is a maximal ideal. This in turn means that the quotient $F = K[x]/\langle p(x) \rangle$ is a field. Not only that, F is in fact a field extension of K. Let's see how we can construct an inclusion $F \hookrightarrow K$.

We have at our disposal an inclusion $\iota \colon K \hookrightarrow K[x]$ and a projection $\pi \colon K[x] \twoheadrightarrow F$. Since any two elements of K belong to different equivalence classes the restriction of π to K is injective, which means the composition $\pi \circ \iota \colon K \to F$ is also injective. Thus F is an extension of K.

We may summarise this in the following lemma.

Lemma 2.1. *Let K be a field and $p(x) \in K[x]$ an irreducible polynomial. Then the quotient $K[x]/\langle p(x) \rangle$ is a field extension of K.*

A number of extensions are of this form. Indeed, we have that $\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$ and the class of x is written i. There is also the extension $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$, which is typically written $\mathbb{Q}(\sqrt{2})$. More generally, if b is not a square in $\mathbb{Q}$ then $x^2 - b$ is irreducible and we have the extension $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}[x]/\langle x^2 - b \rangle$.

By this process we have enlarged the field K by "artificially" adding a primitive element. Indeed, if $p(x) = \sum_{k=0}^{n} a_k x^k$ in the quotient we have

$$0 = \overline{p(x)} = \overline{\sum_{k=0}^{n} a_k x^k} = \sum_{k=0}^{n} a_k \overline{x}^k \tag{2.1.1}$$

so $\bar{x}$, the class of x, is a root of $p(x)$. Note that in eq. (2.1.1) we abused notation and wrote what should have been $\overline{a_k}$ simply as a_k. As we mentioned, the equivalence class of a constant does not contain any other constant so we can, and will, get away with this abuse of notation.

Conversely, a simple extension $K(\alpha)$ is isomorphic to $K[x]/\langle m_\alpha \rangle$ if α is algebraic, essentially by definition.

2.1.3 Subfield generated by a set

Given an existing extension $K \subseteq F$ and a set $S \subseteq F$ we define $K[S]$ to be the smallest subring of F containing K and X, and then $K(S)$ as the result of adding to $K[S]$ the inverses of all its nonzero elements. This is, by construction, the smallest subfield of F that contains both K and S. Notice that $K(\{\alpha\})$ coincides with the simple extension $K(\alpha)$ we described in the previous section. Indeed, $K(\alpha)$ is a subfield of F and it contains K and α, so it contains, by definition $K(\{\alpha\})$. On the other hand, it is clear that $\mathrm{im}(\mathrm{ev}_\alpha) = K[\alpha] \subseteq K(\{\alpha\})$ since they are linear combinations of powers of α with coefficients in K. And since $K(\{\alpha\})$ is a field it contains the inverses of nonzero $K[\alpha]$, that is, it contains $K(\alpha)$.

If the set S is finite, say $S = \{\alpha_1, \ldots, \alpha_n\}$ then we will drop the brackets and simply write $K(\alpha_1, \ldots, \alpha_n)$ instead of $K(\{\alpha_1, \ldots, \alpha_n\})$. Furthermore, we have

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

Indeed, $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ is, by definition, the smallest field which contains $K(\alpha_1, \ldots, \alpha_{n-1})$ and α_n. This means it contains K and $\alpha_1, \ldots, \alpha_n$, so, by definition

$$K(\alpha_1, \ldots, \alpha_n) \subseteq K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

For the other inclusion, $K(\alpha_1, \ldots, \alpha_n)$ contains, K and $\alpha_1, \ldots, \alpha_{n-1}$, which means that, by definition

$$K(\alpha_1, \ldots, \alpha_{n-1}) \subseteq K(\alpha_1, \ldots, \alpha_n).$$

And since $\alpha_n \in K(\alpha_1, \ldots, \alpha_n)$, again by definition

$$K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \subseteq K(\alpha_1, \ldots, \alpha_n).$$

This means that extensions of this kind are simply iterated simple extensions.

2.2 Algebraic and Transcendental Extensions

We already encountered the concept of an algebraic element and a transcendental element when discussing simple extensions in section 2.1.1. We will formalise these ideas in this section.

Definition 2.2 (Algebraic and transcendental elements)**.** Given an extension $K \subseteq F$ we say an element $\alpha \in F$ is *algebraic over* K or simply *algebraic* if it is the root of some (nonzero) polynomial in $K[x]$. On the other hand, we say α is *transcendental over* K or simply *transcendental* if it is not algebraic, i.e. if there is no polynomial in $K[x]$ that has α as a root. △

In section 2.1.1 we said an element was algebraic when the evaluation morphism it induced had a nontrivial kernel. This is equivalent to the definition we just gave. Indeed, if the kernel of ev_α is nontrivial there exists a nonzero polynomial that has it as a root, so α is algebraic in the sense of Definition 2.2. Conversely, if α is the root of some nonzero polynomial then this polynomial is in $\ker(\mathrm{ev}_\alpha)$, thus α is algebraic in the sense of section 2.1.1. Similarly we can show that an element is transcendental in the sense of Definition 2.2 if and only if $\ker(\mathrm{ev}_\alpha) = \langle 0 \rangle$.

An important object associated to an algebraic element is its minimal polynomial, which we have already encountered. We state its definition here for completeness' sake.

Definition 2.3 (Minimal polynomial)**.** The *minimal polynomial* of an element $\alpha \in F$ over a field K, where F is an extension K is the unique monic generator of $\ker(\mathrm{ev}_\alpha)$. It is written $m_{\alpha,K}(x)$ or simply $m_\alpha(x)$ if the base field K is understood. It is sometimes also refered to as the *irreducible polynomial* of α. △

The following gives a characterisation of the minimal polynomial

Proposition 2.2 (Characterisation of the minimal polynomial)**.** *Let $K \subseteq F$ be a field extension and $\alpha \in F$. If there is a monic polynomial $p(x) \in K[x]$ such that $p(\alpha) = 0$ —so α is algebraic— then the following are equivalent*

(i) $p(x) = m_\alpha(x)$,

(ii) $p(x)$ *is irreducible,*

(iii) $p(x)$ *divides any polinomial* $q(x) \in K[x]$ *that has* α *as a root,*

(iv) $p(x)$ *has degree smaller than that of any polinomial* $q(x) \in K[x]$ *that has* α *as a root.*

Proof. The implication (*i*) $\implies$ (*ii*) is the definition of the minimal polynomial. For the converse, note that $p(x) \in \ker(\text{ev}_\alpha)$, which means $\langle p(x)\rangle \subseteq \ker(\text{ev}_\alpha)$. Since $p(x)$ is irreducible, $\langle p(x)\rangle$ is maximal, which means either $\ker(\text{ev}_\alpha) = \langle p(x)\rangle$ or $\ker(\text{ev}_\alpha) = K[x]$. No evaluation map can ever be the zero map, since the constants always evaluate to themselves. This means it must be the case that

$$\langle p(x)\rangle = \ker(\text{ev}_\alpha)$$

and since $p(x)$ is, by hypothesis, monic, it follows $p(x) = m_\alpha(x)$.

Let's show (*ii*) $\implies$ (*iii*). We know that $p(x)$ is the minimal polynomial of α, thus $\langle p(x)\rangle = \ker(\text{ev}_\alpha)$. If $q(\alpha) = 0$ we have that $q(x) \in \ker(\text{ev}_\alpha) = \langle p(x)\rangle$ which means $p(x)$ divides $q(x)$.

The implication (*ii*) $\implies$ (*iv*) follows from the fact that if a polynomial divides another polynomial then it must have a smaller degree.

Let's now show (*iv*) $\implies$ (*ii*). Suppose we can factor $p(x)$ as

$$p(x) = s(x)r(x).$$

Then

$$0 = p(\alpha) = r(\alpha)s(\alpha).$$

This means that one of $r(\alpha)$ or $s(\alpha)$ must be zero. Say $r(\alpha) = 0$. Then, by hypothesis $\deg(p(x)) \leq \deg(r(x))$. On the other hand we also have $\deg(r(x)) \leq \deg(p(x))$ since $r(x)$ divides $p(x)$. Therefore $\deg(p(x)) = \deg(r(x))$ and so $\deg(s(x)) = 0$, which means it is a unit. If it had been $s(\alpha)$ we would have wound up showing that $r(x)$ was a unit. This implies that $p(x)$ is irreducible.

This concludes the proof. □

— ∗ —

The notions of algebraic and transcendental serve to make a distinction between two classes of extensions.

Definition 2.4 (Algebraic and transcendental extensions)**.** We say an extension $K \subseteq F$ is *algebraic* if every element of F is algebraic over K. On the other hand, if the extension is not algebraic —i.e. there exists a transcendental element of F— we say it is *transcendental*. △

2.3 Degree of an extension

2.3.1 Definition and properties

If we have a field extension $K \subseteq F$ then F is a K-vector space. Indeed, the addition is the addition defined on F by virtue of being a field, as is the multiplication by elements of K. All of the vector space axioms follow immediately from the fact that F is a field. This leads to the following definition

Definition 2.5 (Degree of an extension)**.** The *degree* of a field extension $K \subseteq F$ is the dimension of F as a vector space. We write it $[F\colon K]$. An extension of finite degree is called *finite*, otherwise it is called *infinite*. △

We can calculate the degree of any simple extension directly from the definition.

Proposition 2.3 (Degree of a simple extension)**.** *The simple extension* $[K(\alpha) : K]$ *is finite if and only if* α *is algebraic over* K[1]*. If it is finite then its degree is the degree of the minimal polynomial of* α *over* K*. That is,*

$$[K(\alpha)\colon K] = \deg(m_{\alpha,K}(x)).$$

Proof. Let's assume α is algebraic. We will show that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $K(\alpha)$, where n is the degree of $m_\alpha(x)$.

Since α is algebraic we know $K[\alpha] = K(\alpha)$. And since $K[\alpha]$ is, by definition, $\mathrm{im}(\mathrm{ev}_\alpha)$ every element of $K(\alpha)$ is a polyomial expression in α with coefficients in K. Say

$$m_\alpha(x) = x^n + \sum_{k=0}^{n-1} a_k x^k.$$

Then, since $m_\alpha(\alpha) = 0$ then

$$\alpha^n = -\sum_{k=0}^{n-1} a_k x^k. \tag{2.3.1}$$

Using eq. (2.3.1) we can rewrite any linear combination of powers of α as a linear combination of powers of α less than n. This means that $1, \alpha, \ldots, \alpha^{n-1}$ span $K(\alpha)$.

Let's now show that they are linearly independent. Say there were $a_0, \ldots a_{n-1} \in K$ such that

$$\sum_{k=0}^{n-1} a_k \alpha^k = 0.$$

[1] α is understood to lie in some extension of K.

This would translate to a polynomial $q(x) = \sum_{k=0}^{n-1} a_k x^k$ that evaluates to 0 at α. Thus it would be divisible by $m_\alpha(x)$, but since $q(x)$ is of degree at most $n-1$ the only possibility is that $q(x)$ is actually the zero polynomial. That means $a_0 = \cdots = a_{n-1} = 0$, which shows that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent.

On the other hand, if α is transcendental then $K(\alpha)$ has infinite degree over K. Indeed, since $K(\alpha) \cong K(x)$ it contains a copy of $K[x]$ which has infinite dimension as a K-vector space. □

A very similar argument shows that the degree of an extension of the form $K[x]/\langle p(x)\rangle$ where $p(x)$ is irreducible is $\deg p(x)$. Indeed, extensions of this form are essentially simple extensions constructed without the need for the primitive element to exist in a prior extension, the class of x, $\bar{x}$ plays its role.

Example 2.1. With proposition 2.3 we can calculate the degree of various extensions.

(*i*) We have $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. Indeed, the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ given that it is irreducible over $\mathbb{Q}$ since it has no roots. Similarly, the minimal polynomial of $\sqrt{3}$ is $x^2 - 3$.

(*ii*) Since the complex numbers have dimension 2 as a $\mathbb{R}$-vector space then $[\mathbb{C}\colon \mathbb{R}] = 2$. Another way to show this is by noting that the minimal polynomial of i over $\mathbb{R}$ is $x^2 + 1$ and $\mathbb{C} = \mathbb{R}(i)$. By the same argument, $[\mathbb{Q}(i)\colon \mathbb{Q}] = 2$ since $x^2 + 1$ is also the minimal polynomial of i over $\mathbb{Q}$.

(*iii*) It is known that π and e are transcendental over the rationals, with proofs due to Lindemann and Hermite respectively. This means that both $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are infinite. Consequently, since both extensions are contained within the reals it follows that $\mathbb{R}$ is also infinite over $\mathbb{Q}$.

(*iv*) Let's calculate $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$. We have

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}.$$

Therefore

$$24 = [(\sqrt{2} + \sqrt{3})^2 - 5]^2 = (\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 25.$$

Thus we have found that $\sqrt{2}+\sqrt{3}$ is a root of $p(x) = x^4 - 10x^2 + 1$. The only possible rational roots of this polynomial are 1 and -1, and it is easily checked that they are not. However this does not prove that $p(x)$ is irreducible, since its degree is higher

than 3. However this is a biquadratic polynomial (a polynomial that is quadratic in x^2), meaning its real roots can be computed, and so it can be factored over $\mathbb{R}$. With this factorisation, one would compute all four possible degree 2 factors of $p(x)$ and find that none of them are rational, thus concluding that $p(x)$ is irreducible over the rationals —if $p(x)$ factored as the product of a degree 3 and a degree 1 polynomial it would have a rational root, which is not the case, so it can only factor as two degree 2 polynomials—. All of this means that

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4.$$

$\triangledown$

2.3.2 The Tower Formula

One of the fundamental ideas in Galois Theory is to study field extensions in relation to other extensions, in a setup that is called a *tower of extensions* or *tower of fields*.

Definition 2.6 (Tower of extensions)**.** A *tower of fields* is a sequence of extensions

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n.$$

$\triangle$

Theorem 2.4 (Tower Formula)**.** *For a tower $K \subseteq F \subseteq$ it is true that*

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

Proof. If $[F:K]$ is infinite then so is $[E:K]$ since E contains F which is, as a K-vector space, infinite dimensional, then so mut be E. Similarly, if $[E:F]$ then E is infinite dimensional as a F-vector space which means it could not possibly be finite dimensional as a K-vector space. Certainly, if it were there would exist a finite K-basis for E, which would serve as a finite F-basis, a contradiction. Thus, let's now focus on the case were all degrees are finite.

Say $[E:F] = n$ and $[F:K] = m$. This means there exists an F-basis of E, $e_1, \ldots, e_n$ and a K-basis of F, $f_1, \ldots, f_m$. We will show that the vectors $e_i f_j$ with $1 \leq i \leq n$ and $1 \leq j \leq m$ are a K-basis of E therefore proving

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

Expand any $e \in E$ in the e_i basis,

$$e = \sum_{i=1}^{n} \lambda_i e_i$$

Since the $\lambda_i \in F$ we expand them in the f_j basis:

$$e = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \mu_{ij} f_j \right) e_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} f_j e_i$$

therefore E is spanned by the $e_i f_j$ as a K-vector space.

Let's now show that the $e_i f_j$ are linearly independent. We need to show that if there exist $\mu_{ij} \in K$ such that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} f_j e_i = 0$$

then it must be the case that all of the μ_{ij} are zero. Let $\lambda_i = \sum_{j=1}^{m} \mu_{ij} f_j \in F$. Then we have

$$\sum_{i=1}^{n} \lambda_i e_i = 0$$

which implies, by the linear independence of the e_i over F, that $\lambda_i = 0$ for $1 \leq i \leq n$. And if $\lambda_i = \sum_{j=1}^{m} \mu_{ij} f_j = 0$, then by the lienar independence of the f_j over K it follows that $\mu_{ij} = 0$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$, as we wanted. □

Corollary 2.5. *For a tower $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ one has*

$$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0].$$

Proof. Simply apply the Tower Formula and induction. □

— ∗ —

The following result, which is an immediate consequence of the Tower Formula, clarifies the relationship between finite and algebraic extensions.

Proposition 2.6. *Every finite extension is algebraic.*

Proof. Consider an extension $K \subseteq F$. We wish to show that this extension is algebraic, which amounts to proving that every element of F is algebraic. For any $\alpha \in F$ we have the tower $K \subseteq K(\alpha)F$, and applying the Tower Formula we find

$$[F : K] = [F : K(\alpha)][K(\alpha) : K].$$

Now, $[F : F]$ is finite by hypothesis, which means $[K(\alpha) : K]$ must also be finite. By proposition 2.3, it follows α is algebraic. □

Corollary 2.7. *No transcendental extension is finite.*

Proof. This is just the contrapositive of the previous proposition. □

Note, however, that the converse of proposition 2.6 is not true. There exist algebraic extensions which are not finite. For example, the algebraic closure of the rationals is, by construction, algebraic but it can be shown it is not finite.

We can, however, give a weaker converse to the previous result.

Proposition 2.8. *For an extension $F \subseteq K$ it is equivalent*

(i) the extension is finite,

(ii) $F = K(\alpha_1, \ldots, \alpha_n)$ where the α_i are algebraic over K,

(iii) $F = K(\alpha_1, \ldots, \alpha_n)$ where each α_i is algebraic over $K(\alpha_1, \ldots, \alpha_{i-1})$.

Proof. Let's show *(i)* $\implies$ *(ii)*. If $F = K$ then $F = K(\emptyset)$ and we are done. Let's assume, then, that $K \subset F$. This means there exist $\alpha_1 \in F - K$. Then we have the tower

$$K \subset K(\alpha_1) \subseteq F$$

If it happens that $F = K(\alpha_1)$ we are done. If not, we do the same thing, find $\alpha_2 \in F - K(\alpha_1)$ and construct the tower

$$K \subset K(\alpha_1) \subset K(\alpha_2, \alpha_1) \subseteq F.$$

This process must end at some point. Ideed, at step n we have the tower

$$K \subset K(\alpha_1) \subset K(\alpha_2, \alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) \subseteq F. \tag{2.3.2}$$

Therefore, by the Tower Formula

$$[F : K] = [F : K(\alpha_1, \ldots, \alpha_n)] \cdots [K(\alpha_1) : K] \tag{2.3.3}$$

and every factor is strictly greater than 1 by construction. Thus we must be finished in at most $[F : K]$ steps. Additionally, by Proposition 2.6 F is algebraic over K, meaning every one of the α_i is algebraic over K.

We now show *(ii)* $\implies$ *(iii)*. If α_i is algebraic over K then it is also algebraic over $K(\alpha_1, \ldots, \alpha_{i-1})$. Indeed, α_i is a root of a polynomial with coeficients in K, which are in particular also in $K(\alpha_1, \ldots, \alpha_{i-1})$ thus α_i is also algebraic over $K(\alpha_1, \ldots, \alpha_{i-1})$.

Lastly we prove *(iii)* $\implies$ *(i)*. Construct the tower in eq. (2.3.2) which gives us eq. (2.3.3). By hypothesis, every extension

$$K(\alpha_1, \ldots, \alpha_{i-1}) \subseteq K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$$

is algebraic, therefore finite. This means every factor in eq. (2.3.3) is finite, therefore $[F : K]$ is finite as well, as we wanted. □

— ∗ —

With Tower Formula, together with Proposition 2.3 and Proposition 2.8 we can now, in principle, compute the degree of any finite extension. Indeed, we just showed that any finite extension is a tower of simple algebraic extensions. We can calculate the degree of each step with Proposition 2.3 and then put them together with Tower Formula.

Thus the calculation reduces to the computation of the degree of simple extensions[2], i.e. finding the minimal polynomial of a number. This is entirely dependent on the field we are working over. In $\mathbb{C}$ it is trivial by virtue of the Fundamental Theorem of Algebra. Over $\mathbb{R}$ we know that irreducible polynomials can only be of degree 1 or 2, and we have an explicit way of determining whether or not a certain degree 2 polynomial is irreducible. Over $\mathbb{Q}$ there exist irreducible polynomials of any degree so the task becomes harder. On the flipside we have a number of useful tools, such as Eisenstein's criterion, the modular criterion or Gauß's lemma. As we climb the tower the fields can become more exotic. The following example illustrates these ideas.

Example 2.2. Let's calculate $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}]$ where p and q are different primes. We will make use of the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{q})(\sqrt{p}).$$

Thus, by the Tower Formula

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{q})(\sqrt{p}) : \mathbb{Q}(\sqrt{q})][\mathbb{Q}(\sqrt{q}) : \mathbb{Q}].$$

We can easily see that $[\mathbb{Q}(\sqrt{q}) : \mathbb{Q}] = 2$ since

$$m_{\sqrt{q},\mathbb{Q}}(x) = x^2 - q.$$

To determine $[\mathbb{Q}(\sqrt{q})(\sqrt{p}) : \mathbb{Q}(\sqrt{q})]$ we need to find $m_{\sqrt{p},\mathbb{Q}(\sqrt{q})}(x)$, which we will simply write as $r(x)$ for brevity's sake. It is not immediately clear that $r(x)$ should equal $x^2 - p$, however it does. Indeed, we have that $\sqrt{p}$ is a root of $x^2 - p \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{q})[x]$. Thus, by Proposition 2.2 $x^2 - p$ must be divisible by $r(x)$. Therefore $r(x)$ must be of degree either 1 or 2. If it were of degree 1 it would have to be $x - \sqrt{p}$, since it is the only monic linear polynomial that has $\sqrt{p}$ as a root. This would

[2]Of course, we are glossing over the problem of determining the primitive elements of the extension.

mean, however, that $\sqrt{p} \in \mathbb{Q}(\sqrt{q})$ given that $r(x)$ is, by definition, a polynomial with coefficients in the field $\mathbb{Q}(\sqrt{q})$. Therefore there would exist $a, b \in \mathbb{Q}$ such that

$$\sqrt{p} = a + b\sqrt{q}. \tag{2.3.4}$$

Squaring eq. (2.3.4) we find

$$p = a^2 + b^2 q + 2ab\sqrt{q}.$$

Since $\sqrt{q} \neq 0$ this forces $ab = 0$, or otherwise we would deduce $\sqrt{q} \in \mathbb{Q}$, which we know is not the case. If $b = 0$ then we would find $p = a^2$, which cannot be true since no prime is a square in $\mathbb{Q}$. And if $a = 0$ we would have $p = b^2 q$ which is not possible either, by similar reasons.

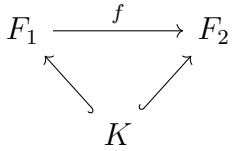
We conclude, therefore, that a and b cannot exist and so $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$, or equivalently, $r(x)$ must have degree 2. Therefore $r(x) = x^2 + p$ and $[\mathbb{Q}(\sqrt{q})(\sqrt{p}) : \mathbb{Q}(\sqrt{q})] = 2$. Finally we obtain the result we set out to calculate

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

▽

2.4 Morphisms of Field Extensions

Another recurring question in Galois theory is the extension of a morphism on a field to a morphism on an extension of said field. We will in general not be interested on any morphism, but rather on morphisms which preserve the base field. This is because what we are actually thinking about are maps between extensions. So, if we have two extensions of the same field, $K \subseteq F_1$ and $K \subseteq F_2$ really what we want is a map between F_1 and F_2 which preserves the structure relevant to the extension, so a morphism $f\colon F_1 \to F_2$ which makes the following diagram commute



If K is an honest to goodness subfield of F this means that the restriction of f to K, $f|_K$ must be the identity on K since the composition $f \circ \iota$ is precisely $f|_K$. This means, among other things, that this sort of morphisms, which we will call K-*morphisms*, play nice with polynomials of $K[x]$ since they preserve their coefficients.

Notice as well that a K-morphism is linear, meaning the map $f\colon F_1 \to F_2$ is linear when thinking of F_1 and F_2 as K-vector spaces. The converse, however, is not true: a linear map from F_1 to F_2 need not be a K-morphism.

More generally, given two extensions $K_1 \subseteq F_1$ and $K_2 \subseteq F_2$ then we define an extension morphism between the two to be a pair of morphisms $f\colon K_1 \to K_2$ and $g\colon F_1 \to F_2$ such that the following square commutes

$$\begin{array}{ccc} F_1 & \xrightarrow{g} & F_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow{f} & K_2 \end{array}$$

It is easy to see that the composition of two extension morphisms is also an extension morphism and that they compose associatively. In addition, the identity is always an extension morphisms. What this means is that field extensions form a category.

— ∗ —

We will mainly deal with K-automorphisms of an extension $K \subseteq F$, that is, automorphisms $\sigma\colon F \to F$ that fix K. These form a group (check it!) which plays a central role in Galois theory, the *Galois group* of the extension, typically denoted $\mathrm{Gal}_K(F)$. For a finite extension, if σ is a K-endomorphism it is automatically a K-automorphism. Indeed, if the extension $K \subseteq F$ is finite then F has finite dimension as a K-vector space. σ is a nonzero field morphism since it fixes K, so it must be injective. We have then an injective linear endomorphism of a finite dimensional vector space, which implies it is actually a linear automorphism and therefore bijective.

2.5 The Morphism Extension Lemmas

We now turn to the question of the existence and uniqueness of morphisms between extensions. We start with a simple enough result

Proposition 2.9. *Let $K \subseteq F_1$ and $K \subset F_2$ be extensions and $\sigma\colon F_1 \to F_2$ a K-morphism between them. Then, if $\alpha \in F_1$ is a root of a polynomial $p(x) \in K[x]$ so is $\sigma(\alpha) \in F_2$.*

Proof. Let $p(x) = \sum_{k=0}^{n} a_k x^k$ with $a_k \in K$. Then, since α is a root of $p(x)$

$$0 = p(\alpha) = \sum_{k=0}^{n} a_k \alpha^k.$$

Applying σ we find

$$\begin{aligned} 0 = \sigma(0) = \sigma(p(\alpha)) &= \sigma\left(\sum_{k=0}^{n} a_k \alpha^k\right) \\ &= \sum_{k=0}^{n} \sigma(a_k)\sigma(\alpha)^k = \sum_{k=0}^{n} a_k \sigma(\alpha)^k && \text{since } \sigma \text{ fixes } K \\ &= p(\sigma(\alpha)) \end{aligned}$$

so $\sigma(\alpha)$ is a root of $p(x)$. □

A special case of this proposition is the well known fact that if a polynomial with real coefficients has a complex root it also has its complex conjugate. This is because complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

Corollary 2.10. *K-morphisms preserve minimal polynomials.*

Proof. Let F_1 and F_2 be extensions of a field K and $f\colon F_1 \to F_2$ a K-morphism between them. Suppose $\alpha \in F_1$ is algebraic with minimal polynomial $m_{\alpha,K}(x)$. By Proposition 2.9 $f(\alpha)$ is also a root of $m_{\alpha,K}(x)$. Additionally $m_{\alpha,K}(x)$ is irreducible, so it follows

$$m_{\alpha,K}(x) = m_{f(\alpha),K}(x).$$

□

— ∗ —

We now establish the existence and uniqueness of K-morphisms from a simple algebraic extension K to another extension $K \subseteq F$. Note that any such K-morphism is solely determined by the image of a primitive element of the extension. Indeed, we know that a simple extension of degree n, $K(\alpha)$, has $1, \alpha, \ldots, \alpha^{n-1}$ as a basis. Thus we would have to specify the image of each of these elements. However, since a K-morphism is also a field morphism, it preserves 1 and once we know the image of α we know the image of all its powers. That is to say, if we have a K-morphism from $K(\alpha)$ to another extension it is sufficient to know where it sends α.

Lemma 2.11 (Morphism Extension Lemma I)**.** *Let K be a field, $K(\alpha)$ a simple algebraic extension of K and F another extension of K. Then for any $\beta \in F$ there exists a unique K-morphism $f\colon K(\alpha) \to F$ such that $f(\alpha) = \beta$ if an only if β is a root of $m_{\alpha,K}(x)$.*

Proof. ($\implies$) Suppose there exists one such $f\colon K(\alpha) \to F$ such that $f(\alpha) = \beta$. We have that α is a root of its minimal polynomial. Thus, by Proposition 2.9 we have that $\beta = f(\alpha)$ must also be a root of the minimal polynomial of α.

($\impliedby$) Consider the evaluation at β morphism, $\mathrm{ev}_\beta\colon K[x] \to F_2$. By hypothesis β is a root of $m_{\alpha,K}(x)$ thus

$$\langle m_{\alpha,K}(x)\rangle \subseteq \ker(\mathrm{ev}_\beta).$$

But since $m_{\alpha,K}(x)$ is irreducible and ev_β is not the zero map it follows that we have equality,

$$\langle m_{\alpha,K}(x)\rangle = \ker(\mathrm{ev}_\beta).$$

Thus, by the Isomorphism Theorem

$$K(\beta) = \mathrm{im}(\mathrm{ev}_\beta) \cong K[x]/\langle m_{\alpha,K}(x)\rangle \cong K(\alpha)$$

which means we have an isomorphism between $K(\alpha)$ and $K(\beta)$. Let's try to determine this isomorphism explicitly. In general, given a morphism $f\colon A \to B$, the Isomorphism Theorem shows there is an induced isomorphism $\bar{f}\colon A/\ker f \to \mathrm{im}\, f$ given by $\bar{f}(\bar{a}) = f(a)$, where $\bar{a}$ is the equivalence class of $a \in A$ in $A/\ker f$.

Thus, we have the isomorphism

$$\overline{\mathrm{ev}_\beta}\colon K[x]/\langle m_{\alpha,K}(x)\rangle \to K(\beta)$$

specified by $\overline{\mathrm{ev}_\beta}(\bar{x}) = \beta$. It is easy to see that it is a K-morphism. By the same token, $\overline{\mathrm{ev}_\alpha}\colon K[x]/\langle m_{\alpha,K}(x)\rangle \to K(\alpha)$ is also a K-morphism.

Therefore $\overline{\mathrm{ev}_\beta} \circ \overline{\mathrm{ev}_\beta}^{-1}\colon K(\alpha) \to K(\beta)$ is a K-isomorphism from $K(\alpha)$ to $K(\beta)$ which simply sends α to β. This should be no surprise at all, since we argued before that if a K-morphism between $K(\alpha)$ and $K(\beta)$ which sends α to β were to exist then it can only possibly be what you expect: send α to β and extend to $K(\alpha)$ in the only possible manner. The real substance of what we have shown is that this morphism actually *exists* when α and β are roots of the same irreducible polynomial over K.

Finally, precompose with the natural inclusion $\iota\colon K(\beta) \hookrightarrow F$ to obtain a K-morphism from $K(\alpha)$ to F. □

— ∗ —

Given a field morphism $f\colon K_1 \to K_2$ we can lift it to a ring morphism between the corresponding polynomial rings, $K_1[x]$ and $K_2[x]$ by acting on the coefficients with f and sending x to x. We will write this lift as $\hat{f}\colon K_1[x] \to K_2[x]$. With this we can give a generalisation version of Lemma 2.11.

Lemma 2.12 (Morphism Extension Lemma II)**.** *Let K be a field and $K(\alpha)$ a simple algebraic extension of K. Then for any field morphism $f\colon K \to F$ and $\beta \in F$ there is a unique morphism $\tilde{f}\colon K(\alpha) \to F$ such that $\tilde{f}(\alpha) = \beta$ and which makes the following diagram commute*

$$\begin{array}{ccc} K(\alpha) & \overset{\tilde{f}}{\dashrightarrow} & F \\ \uparrow & \nearrow_{f} & \\ K & & \end{array}$$

if and only if β is a root of $\hat{f}(m_{\alpha,K}(x))$.

Proof. ($\implies$) For the forward implication, suppose $\tilde{f}\colon K(\alpha) \to F$ exists. Say

$$m_{\alpha,K}(x) = \sum_{k=0}^{n} a_k x^k$$

then

$$(\mathrm{ev}_\beta \circ \hat{f})(m_{\alpha,K}(x)) = \sum_{k=0}^{n} f(a_k)\beta^k = \sum_{k=0}^{n} \tilde{f}(a_k)\tilde{f}(\alpha) = \tilde{f}\left(\sum_{k=0}^{n} a_k \alpha^k\right) = \tilde{f}(0) = 0.$$

So β is a root of $\hat{f}(m_{\alpha,K}(x))$, as we wanted.

($\impliedby$) The argument is basically the same as the proof of Lemma 2.11. However, rather than directly using ev_β we will first apply $\hat{f}$ to get a "pseudoevaluation morphism", $\phi_\beta = \mathrm{ev}_\beta \circ \hat{f}$. Since, by hypothesis, β is a root of $\hat{f}(m_{\alpha,K}(x)$ we have

$$\langle m_{\alpha,K}(x)\rangle \subseteq \ker(\phi_\beta)$$

and by the irreducibility of $m_{\alpha,K}(x)$ we actually have equality. We have the situation

$$K(\alpha) \cong K[x]/\langle m_{\alpha,K}(x)\rangle \cong \mathrm{im}(\phi_\beta)$$

where the explicit isomorphisms are $\overline{\mathrm{ev}_\alpha}^{-1}$ and $\overline{\phi_\beta}$.

Let's show that $\mathrm{im}(\phi_\beta) = f(K)(\beta) \subseteq F$. By hypothesis, β is algebraic over $f(K)$ since it is a root of $\hat{f}(m_{\alpha,K}(x)) \in f(K)[x]$. Therefore

$$f(K)(\beta) = \mathrm{ev}_\beta(f(K)[x]) = \mathrm{ev}_\beta(\hat{f}(K[x])) = \phi_\beta(K[x]) = \mathrm{im}(\phi_\beta).$$

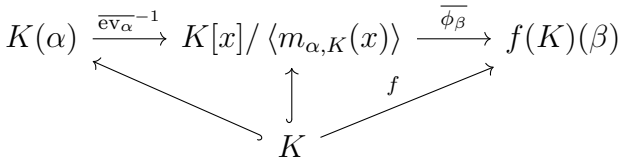
Additionally, the following diagram commutes

$$\begin{array}{ccc} K[x]/\langle m_{\alpha,K}(x)\rangle & \xrightarrow{\overline{\phi_\beta}} & f(K)(\beta) \\ \uparrow & \nearrow_{f} & \\ K & & \end{array}$$

Indeed, if $\lambda \in K$ then $f(\lambda) \in f(K) \subseteq f(K)(\beta)$. On the other hand, we identify λ with its equivalence class in $K[x]/\langle m_{\alpha,K}(x)\rangle$, thus

$$(\bar{\lambda}) = \phi_\beta(\lambda) = (\mathrm{ev}_\beta \circ f)(\lambda) = f(\lambda).$$

From this we build the diagram



Thus we get an isomorphism from $K(\alpha)$ to $f(K)(\beta)$, which can be extended to F.

The uniqueness comes from the fact that a morphism from $K(\alpha)$ is completely determined by where it sends α, in this case to β. □

Chapter 3

The Galois Group of an Extension

3.1 Definition

Galois Theory has two main ingredients. One of them are field extensions, which we discussed in the previous chapter. The other are their Galois groups. It turns out there is a correspondence between field extensions and their Galois groups.

Definition 3.1 (Galois Group of an Extension)**.** The *Galois group* of a field extension $K \subseteq F$ is the group of K-automorphisms of F, i.e. the group of field automorphisms of F which fix K. We write it $\mathrm{Gal}_K(F)$. △

Example 3.1. Let's calculate the Galois group of the field $\mathbb{Q}(\sqrt{2})$. If $\sigma \in \mathrm{Gal}_K(F)$ then, by definition, σ makes the following diagram commute,

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{2}) \\ \uparrow & \nearrow & \\ \mathbb{Q} & & \end{array} .$$

Conversely, if σ is a K-morphism such that the previous diagram then, as we have argued before, it is actually a K-automorphism and thus $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$. There are, then, only two possibilities for σ, since, by Lemma 2.11, it must send $\sqrt{2}$ to one of the two roots of $m_{\sqrt{2}}(x) = x^2 - 2$, which are $\sqrt{2}$ and $-\sqrt{2}$. The first possibility means σ is in fact the identity, and the second one is akin to complex conjugation. This means $\left|\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))\right| = 2$. Therefore

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}.$$

▽

Example 3.2. We will compute the Galois group of the field $\mathbb{Q}(\xi)$ where ξ is a p-th root of unity different from 1 and p a prime. For the sake of concreteness, say

$$\xi = e^{\frac{2\pi i}{p}}.$$

We need to determine the minimal polynomial of ξ over $\mathbb{Q}$. For one, ξ is a root of $x^p - 1$, but this is not irreducible. Indeed, since 1 is also a root, we have the factorisation

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1).$$

The polynomial $x^{p-1} + \cdots + 1$, which is known as a cyclotomic polynomial, is irreducible. One uses a standard trick to show it. In the fraction field, $\mathbb{Q}(x)$ we have

$$x^{p-1} + \cdots + 1 = \frac{x^p - 1}{x - 1}.$$

Now aply the change of variable $x = y + 1$:

$$\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \left(\frac{1}{y}\sum_{k=0}^{p}\binom{p}{k}y^k\right) - \frac{1}{y} = \sum_{k=1}^{p}\binom{p}{k}y^{k-1}.$$

The leading term of this polynomial is y^{p-1} while its last term is p. Every other term is divisible by p. We apply Eisenstein's Criterion and readily conclude that it is irreducible (note the importance of p being prime). A change of variables, as we discussed, can be thought of as an automorphism of $\mathbb{Q}[x]$ meaning our original polynomial is also irreducible.

All this goes to show that

$$m_{\xi,\mathbb{Q}}(x) = x^{p-1} + \cdots + 1.$$

This means $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$. As we argued in the previous example, the elements of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ are in bijection with the roots of $m_{\xi,\mathbb{Q}}(x)$ in $\mathbb{Q}(\xi)$. It is easy to check that its roots are every power of ξ, except for 1, of which there are $p - 1$. Thus, we have $p - 1$ elements in $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi))$, given by

$$\sigma_i(\xi) = x^i.$$

Consider the map

$$\begin{aligned} \Phi \colon \mathbb{F}_p^{\times} &\to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) \\ i &\mapsto \sigma_i \end{aligned}$$

where $\mathbb{F}_p$ is the finite field of order p and $\mathbb{F}_p^*$ its multiplicative group. Φ is surjective and since its domain and codomain have the same number of elements, it is bijective. It is also a group homomorphism since

$$\Phi(i_1 i_2)(\xi) = f_{i_1 i_2}(\xi) = \xi^{i_1 i_2} = (\xi^{i_1})^{i_2} = (f_{i_1} \circ f_{i_2})(\xi) = (\Phi(i_1) \circ \Phi(i_2))(\xi).$$

So it follows that $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) \cong \mathbb{F}_p^{\times}$, and, by the Primitive Element Theorem, $\mathbb{F}_p^{\times}$ is cyclic of order $p-1$.

More generally, for the extension generated by the n-th roots of unity, where n may or may not be a prime, one has the result

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) \cong \mathbb{Z}/n\mathbb{Z}^{\times}$$

$\bigtriangledown$

3.2 Galois Groups of Finite Extensions

3.3 The Discriminant

There is a quantity that is very useful in the calculation of Galois groups of polynomials, known as the *discirminant*. It is a generalisation of the quadratic disriminant, $b^2 - 4ac$, which, hence its name, discriminates between different situtations for the existence of roots of the polynomial.

Definition 3.2 (Discriminant)**.** The *discriminant* of a polynomial $p(x) \in K[x]$ with roots $\alpha_1, \ldots, \alpha_n$ in its splitting field is

$$\Delta(p(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

We also define the quantity

$$\delta(p(x)) = \prod_{i<j} (\alpha_i - \alpha_j).$$

$\bigtriangleup$

Chapter 4

Normal and Separable Extensions

4.1 Normal Extensions

Definition 4.1 (Normal Extension)**.** We say a field extension $K \subseteq F$ is *normal* if it is algebraic and if every irreducible polynomial of $k[x]$ which has a root in F splits in F. △

This definition suggests a certain relationship between normal extensions and splitting fields, since both have to do with the property of a polynomial automatically splitting if it has a root. The following result clarifies this relationship.

Theorem 4.1. *A finite extension is normal if and only if it is the splitting field of a polynomial.*

Proof. ($\Longrightarrow$) Suppose $K \subseteq F$ is a finite normal extension. By Proposition 2.8, F is of the form $F = K(\alpha_1, \ldots, \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in F$ algebraic over K. We will show that F is the splitting field of

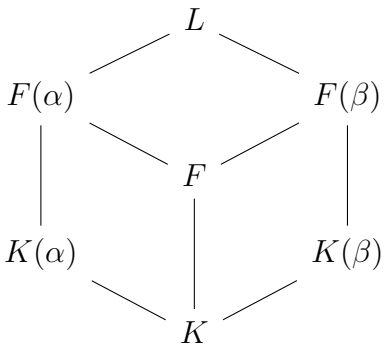
$$p(x) = m_{\alpha_1}(x) \cdots m_{\alpha_n}(x).$$

Every $m_{\alpha_i}(x)$ is irreducible and has a root in F, namely α_i. By normality they all split in F which means $p(x)$ splits in F. Let's show that F is the minimal field in which $p(x)$ splits, thus its splitting field. Consider an extension F' in which $p(x)$ splits and such that $K \subset F' \subset F$. Then F' contains every root of $p(x)$, in particular $\alpha_1, \ldots, \alpha_n$. Thus $F = K(\alpha_1, \ldots, \alpha_n) \subseteq F'$, therefore $F = F'$. Then it follwos F is the splitting field of $p(x)$.

($\Longleftarrow$) Let's now assume F is the splitting field of a polynomial $q(x) \in K[x]$. Let $p(x) \in K[x]$ be an irreducible polynomial with a root in F. If we can show that in fact any root of $p(x)$ is in F then we can conclude that F is normal. We will

show that in fact the extension that results from adjoining a root of $p(x)$ to F has the same degree no matter which root we choose. Thus, if $p(x)$ has a root in F then the adjunction of that root gives an extension of degree 1. It follows that any other such extension has degree 1 and therefore any other root of $p(x)$ is in F, proving normality.

Let $L \supseteq K$ be the splitting field of $p(x)$ over F. Then L contains every root of $p(x)$. Let α and β be any two of these roots. We can construct the following diagram, where every line simply represents an inclusion.



We will show that $F(\alpha)$ and $F(\beta)$ have the same degree over F, which means that if one of the roots of $p(x)$ is in F Now, using the Tower Formula we have

$$[F(\alpha) : K] = [F(\alpha) : K(\alpha)][K(\alpha) : K]. \tag{4.1.1}$$

Since $p(x)$ is irreducible over K and it has α as a root it is actually the minimal polynomial of α, thus

$$[K(\alpha) : K] = \deg p(x),$$

which, when substituted in eq. (4.1.1) yields $[F(\alpha) : K] = [F(\alpha) : K(\alpha)] \deg p(x)$. By going down through F instead of $K(\alpha)$ we find

$$[F(\alpha) : K] = [F(\alpha) : F][F : K].$$

Thus

$$[F(\alpha) : F][F : K] = [F(\alpha) : K(\alpha)] \deg p(x). \tag{4.1.2}$$

The exact same calculations hold substituting α by β and so we also have

$$[F(\beta) : F][F : K] = [F(\beta) : K(\beta)] \deg p(x). \tag{4.1.3}$$

Now, since F is the splitting field of $q(x)$ over K it follows $F(\alpha)$ is a splitting field of $q(x)$ over $K(\alpha)$. Indeed, if $q(x)$ were to split in a field inbetween, Q, then Q would contain K, α and every root of $q(x)$. Thus it would contain F and α, by

virtue of F being a splitting field, which means $F(\alpha) \subseteq Q$. For the same reason $F(\beta)$ is the splitting field of $q(x)$ over $K(\beta)$.

We can show $K(\alpha)$ and $K(\beta)$ are isomorphic. Indeed, $p(x)$ is irreducible over K and has α as a root in $K(\alpha)$ and β as a root in $K(\beta)$. Thus, using the Morphism Extension Lemma I there is a K-morphism from $K(\alpha)$ to $K(\beta)$ which sends α to β, and conversely, a morphism from $K(\beta)$ to $K(\alpha)$ which sends β to α. These are, therefore, inverses of each other. What this means is that $K(\alpha)$ and $K(\beta)$ are essentially the same field, meaning, by the uniqueness up to isomorphism of the splitting field, that $F(\alpha)$ and $F(\beta)$ must also be isomorphic. We thus have the diagram

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\sim} & F(\beta) \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\sim} & K(\beta) \\ & \nwarrow \quad \nearrow & \\ & K & \end{array}$$

from which one deduces that

$$[F(\alpha) : K(\alpha)] = [F(\beta) : K(\beta)].$$

And from this follows

$$[F(\alpha) : K] = [F(\alpha) : K(\alpha)] \deg p(x) = [F(\beta) : K(\beta)] \deg p(x) = [F(\beta) : K].$$

Finally, combining this with eqs. (4.1.2) and (4.1.2) we find

$$[F(\alpha) : F] = \frac{[F(\alpha) : K]}{[F : K]} = \frac{[F(\beta) : K]}{[F : K]} = [F(\beta) : F].$$

Thus, as we previously argued, if $p(x)$ has a root in F, say α then we have $[F(\alpha)(F) : F(\alpha)] = 1$ since $F(\alpha) = F$. Therefore, for any other root of $p(x)$ we have $[F(\beta) : F] = 1$ which implies $F(\beta) = F$ and $\beta \in F$. Thus $p(x)$ splits in F and we conclude F is normal. □

From this result it follows that every splitting field is a normal extension, since a splitting field is finite. The converse, however, need note be true, meaning there exist normal extensions which are not the splitting field of any polynomial —although they can't of course be finite—.

Example 4.1. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is finite but it is not normal. Indeed, $x^3 - 2$ is irreducible over $\mathbb{Q}$ and it has a root in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$. However, the

other two roots of $x^3 - 2$ are not in $\mathbb{Q}(\sqrt[3]{2})$ since they are not real and $\mathbb{Q}(\sqrt[3]{2})$ is contained in $\mathbb{R}$. However, if $\omega = e^{\frac{2\pi i}{3}}$ then $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2$. By what we have just shown it must be a normal extension.

Incidentally, this example shows that if we have a normal extension $K \subseteq F$ it is not in general true that an extension sandwiched inbetween, $K \subseteq E \subseteq F$ is also normal over K. ▽

Theorem 4.1 is helpful in discussing the normality of simple extensions. We know a simple extension is finite if and only if it is algebraic. Therefore, a simple algebraic extension will be normal if and only if it is a splitting field. A natural candidate for the extension $K(\alpha)$ to be the splitting field of is $m_\alpha(x)$. We have the following result.

Proposition 4.2. *A simple algebraic extension $K(\alpha)$ is normal if and only if it is the splitting field of $m_\alpha(x)$.*

Proof. If $K(\alpha)$ is normal then, since $m_\alpha(x)$ has a root in $K(\alpha)$, namely α, $m_\alpha(x)$ must split in $K(\alpha)$. And if $m_\alpha(x)$ splits in any other field K' then K' must contain every root of $m_\alpha(x)$, in particular α. Therefore K' must contain $K(\alpha)$ which shows $K(\alpha)$ is the splitting field of $m_\alpha(x)$.

Conversely, if $K(\alpha)$ is the splitting field of $m_\alpha(x)$ then it must be normal by Theorem 4.1. □

4.2 Separable Extensions

Definition 4.2 (Separable Polynomial)**.** We say an irreducible polynomial is *separable* over a field K if it has no repeated roots in its splitting field over K. And more generally, a polynomial, irreducible or not, is said to be *separable* over a field K if all of its irreducible factors are separable. △

Definition 4.3 (Separable Extension)**.** An extension $K \subseteq F$ is said to be *separable* if it is algebraic and if the minimal polynomial of every element of F is separable over K. △

As it turns out, for extensions over a field of zero characteristic, being algebraic is equivalent to being separable, as for extensions over finite fields. To see this we need to introduce some results related to the existence of repeated roots of a polynomial.

4.2.1 The Formal Derivative

It makes no sense to speak of the derivative of a polynomial in the context of a general polynomial ring since we don't even have a topology on this space. What we can do is define, in purely algebraic terms, a map which mimics a number of the properties of the derivative from Analysis, which turns out to also have useful algebraic properties.

Definition 4.4 (Formal Derivative)**.** The *formal derivative* or simply *derivative* is the linear map $D\colon K[x] \to K[x]$ defined by

$$\begin{aligned} D(1) &= 0 \\ D(x^n) &= nx^{n-1} \text{ for } n \geq 1. \end{aligned}$$

△

The derivative has a number of familiar properties

Proposition 4.3. *Let $K[x]$ be a polynomial ring and $D\colon K[x] \to K[x]$ the formal derivative operator. Then*

(i) D is linear,

(ii) D satisfies the Leibniz Product Rule, that is, for any $p(x), q(x) \in K[x]$

$$D(p(x)q(x)) = D(p(x))q(x) + p(x)D(q(x)).$$

Proof. (i) follows immediately from the definition of D.

If $p(x)$ or $q(x)$ are 0 then (ii) is clearly true. It is also clearly true if $q(x) = 1$. Let's show it for the case $q(x) = x^n$ with $n \geq 1$. Let $p(x) = \sum_{k=1}^{m} a_k x^k$. Then

$$\begin{aligned} D(p(x)x^n) = D\left(\sum_{k=0}^{n} a_k x^{k+n}\right) &= \sum_{k=0}^{n} (k+n) a_k x^{k+n-1} \\ &= x^n \sum_{k=1}^{n} k a_k x^{k-1} + n x^{n-1} \sum_{k=1}^{n} a_k x^k \\ x^n D(p(x)) + n x^{n-1} p(x) &= x^n D(p(x)) + D(x^n) p(x). \end{aligned}$$

Now, if $q(x) = \sum_{k=0}^{n} b_k x^k$ we have

$$\begin{aligned} D(p(x)q(x)) &= D\left(\sum_{k=0}^{n} p(x)a_k x^k\right) = \sum_{k=0}^{n} a_k D(p(x)x^k) \\ &= \sum_{k=0}^{n} a_k \left(D(p(x))x^k + kp(x)x^{k-1}\right) \\ &= D(p(x)) \sum_{k=0}^{n} a_k x^k + p(x) \sum_{k=1}^{n} k a_k x^{k-1} \\ &= D(p(x))q(x) + p(x)D(q(x)), \end{aligned}$$

as we wanted. □

If the field we are working over has characteristic 0 then the derivative of any polinomial with degree greater than or equal to 1 is nonzero. On the other hand, if our base field has finite characteristic p then $D(x^p) = px^{p-1} = 0$.

4.2.2 Greatest Commmon Divisor in a PID

Recall that a greatest common divisor of two elements is a divisor of both that is maximal with respect to the the divisibility relation. That is, d is said to be a greatest common divisor of a and b if $d \mid a$ and $d \mid b$, and if d' is such that $d' \mid a$ and $d' \mid b$ then $d' \mid d$. This means that in an integral domain, if a greatest common divisor exists then it is unique up to units, meaning that any other greatest common divisor is related to it by multiplication by a unit.

The question of existence of the greatest common divisor is somewhat more complicated. However, in a PID the existence of a greatest common divisor is guaranteed. Indeed, given $a, b \in R$ where R is a PID then the ideal generated by a and b, which is the sum of the ideals generated by each one, must be principal. So there must exist $d \in R$ such that

$$\langle d \rangle = \langle a \rangle + \langle b \rangle .$$

Then d is a greatest common divisor of a and b. Indeed, since $\langle a \rangle , \langle b \rangle \subseteq \langle a \rangle + \langle b \rangle = \langle d \rangle$ then $d \mid a$ and $d \mid b$. And if d' is such that $d' \mid a$ and $d' \mid b$ then $\langle d \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle d' \rangle$, which means $d' \mid d$.

In fact, in a PID R one has that a common divisor d of a and b is a greatest common divisor if and only if it satisfies a Bézout identity, meaning there exist $r, s \in R$ such that

$$d = ra + sb.$$

If d is known to be a greatest common divisor then this is trivial since $d \in \langle d \rangle = \langle a \rangle + \langle b \rangle$. On the other hand, since d divides a and b then $\langle a \rangle + \langle b \rangle \subseteq \langle d \rangle$. But since $d = ra + sb$ we have $d \in \langle a \rangle + \langle b \rangle$ meaning $\langle d \rangle \subseteq \langle a \rangle + \langle b \rangle$.

Lemma 4.4. *Let R and S be PIDs and $f\colon R \to S$ be an injective ring morphism. If $d \in R$ is a greatest common divisor of $a, b \in R$ then $f(d)$ is a greatest common divisor of $f(a)$ and $f(b)$ in S.*

Proof. If either a or b are 0 then the result is true. Indeed, the greatest common divisor of 0 and any other element a is a since everyone divides 0. Suppose, then, a and b are both nonzero. Since f is injective then $f(a)$ and $f(b)$ are also both nonzero. Let d be a greatest common divisor of a and b. Since R is a PID then this is equivalent to d satisfying a Bézout identity, meaning there exist $r, s \in R$ such that

$$f(d) = f(r)f(a) + f(s)f(b)$$

thus $f(d)$ satisfies a Bézout identity for $f(a)$ and $f(b)$.

By hypothesis, d is a divisor of both a and b, meaning there exist nonzero $\alpha, \beta \in R$ such that $a = \alpha d$ and $b = \beta d$. Thus $f(a) = f(\alpha)f(d)$ and $f(b) = f(\beta)f(d)$. This means $f(d)$ divides both $f(a)$ and $f(b)$, since none of the terms are 0 by the injectivity of f. Therefore $f(d)$ is a common divisor of $f(a)$ and $f(b)$ and satisfies a Bézout identity, which means it must be a greatest common divisor of $f(a)$ and $f(b)$. □

— ∗ —

All of this will be useful to us in the context of polynomial rings over a field, which are PIDs. In these rings we will simply speak of *the* greatest common divisor, and not just *a* greatest common divisor, and take it to be a monic greatest common divisor, which guarantees uniqueness. If $p(x), q(x) \in K[x]$ then we will write their greatest common divisor in $K[x]$ by $\gcd_K(p(x), q(x))$. Recall that a field morphism $f\colon K \to L$, which must be injective, lifts to a ring morphism $\hat{f}\colon K[x] \to L[x]$ which is also injective. In particular, since the image of a monic polynomial by a morphism of this kind is also monic, we have the identity

$$\hat{f}\Big(\gcd_K(p(x), q(x))\Big) = \gcd_L\Big(\hat{f}(p(x)), \hat{f}(q(x))\Big).$$

In particular, if f is simply an inclusion then this means that the greatest common divisor over an extension is the same as the greatest common divisor over the base field, which means we can dispense with the subindexes altogether.

4.2.3 Separable Extensions and Algebraic Extensions

Lemma 4.5. *A nonconstant polynomial $p(x) \in K[x]$ does not have repeated roots in its splitting field over K if and only if*

$$\gcd(p(x), D(p(x)) = 1.$$

Proof. ($\implies$) Assume $p(x)$ has no repeated roots in its splitting field over K, L. Let $d(x) = \gcd(p(x), D(p(x)))$. If $d(x) \neq 1$ then $d(x)$ has degree at least 1[1] so it must share one of the irreducible factors of $p(x)$, which in L are all of degree 1. Let $(x - \alpha) \mid d(x) \mid p(x)$. Since $d(x) \mid D(p(x))$ then $(x - \alpha) \mid D(p(x))$. Say $p(x) = (x - \alpha)q(x)$. Then

$$D(p(x)) = q(x) + (x - \alpha)D(q(x))$$

and since $(x - \alpha) \mid D(p(x))$ it must be that $(x - \alpha) \mid q(x)$. But this would mean $(x - \alpha)^2 \mid p(x)$ which cannot be the case since α is a root of $p(x)$ and therefore assumed to be simple. Thus $d(x) = 1$.

($\impliedby$) Suppose $p(x)$ has at least a repeated root. This means there exists $\alpha \in L$ such that

$$p(x) = (x - \alpha)^n q(x)$$

for $n > 1$. It is easy to show by induction on n and using Leibniz's rule, that $D((x - \alpha)^n) = n(x - \alpha)^{n-1}$, therefore

$$D(p(x)) = n(x - \alpha)^{n-1}q(x) + (x - \alpha)^n D(q(x)).$$

It follows $(x - \alpha)$ also divides $D(p(x))$ thus

$$(x - \alpha) \mid \gcd_(p(x), D(p(x)))$$

which means $\gcd_(p(x), D(p(x)))$ can't be 1. □

Corollary 4.6. *If $p(x) \in K[x]$ is irreducible and $\mathrm{ch}(K) = 0$ then $p(x)$ has no repeated roots in its splitting field over K.*

Proof. Since $p(x)$ is irreducible then $\gcd(p(x), D(p(x)))$ can only be 1 or $p(x)$. If it were $p(x)$ then $p(x) \mid D(p(x))$ but since $\deg(D(p(x))) \leq \deg(p(x))$ it must be $D(p(x)) = 0$. But, since $\mathrm{ch}(K) = 0$, this could only happen if $p(x)$ were 0, which it is not since it is irreducible. Therefore it must be 1 and by Lemma 4.5 it follows that $p(x)$ does not have repeated roots. □

[1] The greatest common divisor of any two elements can never be 0 since 0 divides no element other than itself

From this it follows that when a field has zero characteristic then any extension of it is algebraic if and only if it is separable. Indeed, a separable extension is algebraic by definition. And over a field of characteristic zero any irreducible polynomial is separable, by the last corollary. Thus the minimal polynomial of any element of an algebraic extensino is separable and so the extension is separable.

What happens then over fields of nonzero characteristic? Lemma 4.5 is not true, meaning there exist irreducible polynomials over a field of nonzero characteristic with repeated roots. Indeed, consider the fraction field $\mathbb{F}_p(t)$ and the polynomial $x^p - t \in \mathbb{F}_p(t)[x]$. We can show it is irreducible. Indeed, $\mathbb{F}_p(t)$ is the fraction field of $\mathbb{F}_p[t]$. $x^p - t$ is irreducible over $\mathbb{F}_p[t]$. Indeed, t is irreducible in $\mathbb{F}_p[t]$ since it is of degree 1 and $t^2 \nmid t$. Therefore, using Eisenstein's criterion, we conclude it is irreducible. Then, by Gauss' Lemma it is irreducible in $\mathbb{F}_p(t)[x]$.

Now, when working over a field K of finite characteristic p then

$$\begin{aligned} \phi_p \colon K &\to K \\ a &\mapsto a^p \end{aligned}$$

is a morphism, known as the Frobenius morphism. The only difficulty is showing that $\phi_p(a+b) = \phi_p(a) + \phi_p(b)$. But if we expand $(a+b)^p$ using the binomial formula then, since the binomial coefficients will all be divisible by p, every term vanishes except for a^p and b^p therefore $(a+b)^p = a^p + b^p$. Thus, if $t^{1/p}$ is a root of $x^p - t$ in its splitting field then

$$(x - t^{1/p})^p = x^p - t$$

which means $x^p - t$ has one single root repeated p times.

— ∗ —

Let's try to find some version of Corollary 4.6 for fields of finite characteristic. It is still true that if $p(x)$ is irreducible then $\gcd(p(x), D(p(x)))$ must either be 1 or $p(x)$. If it is 1 then it follows $p(x)$ is separable. The problem, therefore, is if it is $p(x)$. It is still true, independent of characteristic, that D lowers the degree, so that if $\gcd(p(x), D(p(x))) = p(x)$ it must mean $D(p(x))$. The issue is we cannot conclude from this that $p(x) = 0$. What we can say, however, is that $p(x)$ must only contain terms of degree a multiple of p, so that all of them vanish when differentiated. So

$$p(x) = \sum_{k=0}^{n} a_k x^{pk}.$$

If it just so happened that every one of the a_k were a p-th power of some other b_k, meaning $a_k = b_k^p$ then

$$p(x) = \sum_{k=0}^{n} b_k^p x^{pk} = \left(\sum_{k=0}^{n} b_k x^k \right)^p$$

which cannot be the case if $p(x)$ is irreducible. What this means is that the only possible offenders must be polynomials whose terms are all of degree a multiple of p and such that at least one of their coefficients is *not* a p-th power of something.

The Frobenius morphism is injective, so if we are in a finite field it is actually an automorphism. Thus, in a finite field of characteristic p, every single element has a p-th root. This means there are no possible irreducible polynomials with 0 derivative and therefore they must all be separable. We summarise all of this in the following theorem

Theorem 4.7. *An irreducible polynomial over a finite field or a field of zero characteristic has no repeated roots in its splitting field and is therefore separable.*

This implies the following

Theorem 4.8. *An extension of a finite field or a field of characteristic 0 is separable if and only if it is algebraic.*

Chapter 5

The Galois Correspondence

Definition 5.1 (Intermediate field)**.** We say L is an *intermediate field* of the extension $K \subseteq F$ if L is a field such that $K \subseteq L \subseteq F$. The set of all intermediate fields of an extension $K \subseteq F$ is denoted $\mathcal{L}_K(F)$ and is generally called the *lattice of intermediate fields* of the extension. △

Definition 5.2 (Field fixed by a group)**.** Given a subgroup $H \leq \mathrm{Gal}_K(F)$ we write F^H for the set of elements of F which are fixed by the action of H, i.e.

$$F^H := \{x \in F \mid \forall f \in H \colon f(x) = x\}.$$

△

It turns out F^H is actually a field and thus an intermediate field of the extension. All that needs to be shown is that the sum, product and inverse of elements fixed by H is again fixed by H. So if $x, y \in F^H$ then for all $f \in H$ we have

$$f(x+y) = f(x) + f(y) = x + y$$
$$f(xy) = f(x)f(y) = xy$$

and provided $x \neq 0$ then $f(x <^{-1}) = f(x)^{-1} = x^{-1}$. Thus F^H is a subfield of F. And since, by definition, any element of $\mathrm{Gal}_K(F)$ fixes K then we have K is a subfield of F^H and so $F^H \in \mathcal{L}_K(F)$.

Lemma 5.1. *If L is an intermediate field of an extension $K \subseteq F$ then* $\mathrm{Gal}_L(F) \subseteq \mathrm{Gal}_K(F)$.

Proof. Let $\sigma \in \mathrm{Gal}_L(F)$. Then σ is a field automorphism of F which fixes L. But since $K \subseteq L$ it also fixes K, thus $\sigma \in \mathrm{Gal}_K(F)$. Since $\mathrm{Gal}_L(F)$ is by itself a group with composition it follows it is a subgroup of $\mathrm{Gal}_K(F)$. □

Definition 5.3 (Subgroup lattice)**.** We write $\mathcal{L}(G)$ for the set of all subgroups of a group G, called the *subgroup lattice* of G. △

Definition 5.4 (Galois correspondence)**.** Given a field extension $K \subseteq F$, the pair of maps

$$\begin{aligned} \mathcal{F}\colon \mathcal{L}(\mathrm{Gal}_K(F)) &\longrightarrow \mathcal{L}_K(F) \\ H &\longmapsto F^H \end{aligned}$$

$$\begin{aligned} \mathcal{G}\colon \mathcal{L}_K(F) &\longrightarrow \mathcal{L}(\mathrm{Gal}_K(F)) \\ K &\longmapsto \mathrm{Gal}_L(F) \end{aligned}$$

are called the *Galois correspondence* of the extension. △

Notice that both $\mathcal{L}(\mathrm{Gal}_K(F))$ and $\mathcal{L}_K(F)$ are partially ordered by inclusion.

Proposition 5.2. *The Galois correspondence of an extension $K \subseteq F$ satisfies*

(i) if $L \in \mathcal{L}_K(F)$ then $L \subseteq \mathcal{F}(\mathcal{G}(L)) = F^{\mathrm{Gal}_L(F)}$

(ii) if $H \in \mathcal{L}(\mathrm{Gal}_K(F))$ then $H \leq \mathcal{G}(\mathcal{F}(H)) = \mathrm{Gal}_{F^H}(F)$

(iii) both $\mathcal{F}$ and $\mathcal{G}$ are decreasing, meaning if $H_1 \leq H_2$ then $\mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$ and if $L_1 \subseteq L_2$ then $\mathcal{G}(L_1) \geq \mathcal{G}(L_2)$

(iv) $\mathcal{F} \circ \mathcal{G} \circ \mathcal{F} = \mathcal{F}$ and $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G} = \mathcal{G}$.

Proof. *(i)* Let $x \in L$. Then, for any $\sigma \in \mathrm{Gal}_L(F)$ one has, by definition, $\sigma(x) = x$. Thus $x \in F^{\mathrm{Gal}_L(F)}$, which means $L \subseteq F^{\mathrm{Gal}_L(F)}$.

(ii) Let $h \in H$. Then, by definition, h is a field automorphism of F which fixes F^H. Thus $h \in \mathrm{Gal}_{F^H}(F)$ and $H \subseteq \mathrm{Gal}_{F^H}(F)$.

(iii) Let $H_1 \leq H_2 \leq \mathrm{Gal}_K(F)$. Then, any element of $\mathcal{F}(H_2) = F^{H_2}$ is fixed by every element of H_2, which means it is in particular fixed by any element of H_1. Thus $F^{H_2} \subseteq F^{H_1}$. This shows $\mathcal{F}$ is decreasing.

Similarly, if L_1 and L_2 are intermediate fields and $L_1 \subseteq L_2$ then any field automorphism of F which fixes L_2 must fix L_1, which means $\mathrm{Gal}_{L_2}(F) \leq \mathrm{Gal}_{L_1}(F)$. This shows $\mathcal{G}$ is decreasing.

(iv) Let $H \leq \mathrm{Gal}_K(F)$. Then we need to show

$$(\mathcal{F} \circ \mathcal{G} \circ \mathcal{F})(H) = F^{\mathrm{Gal}_{F^H}(F)} = F^H.$$

Using (i) we have

$$(\mathcal{F} \circ \mathcal{G} \circ \mathcal{F})(H) = (\mathcal{F} \circ \mathcal{G})(\mathcal{F}(H)) \supseteq \mathcal{F}(H).$$

The other inclusion remains to be shown. We need to see that if $x \in F^{\mathrm{Gal}_{F^H}(F)}$ then $x \in F^H$. From (ii) follows that $\mathrm{Gal}_{F^H}(F) = (\mathcal{G} \circ \mathcal{F})(H) \geq H$. Therefore, from (iii) we conclude

$$(\mathcal{F} \circ \mathcal{G} \circ \mathcal{F})(H) = \mathcal{F}((\mathcal{G} \circ \mathcal{F})(H)) \subseteq \mathcal{F}(H),$$

as we wanted.

Since $\mathcal{F}$ and $\mathcal{G}$ have the same properties, the exact same argument shows $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G} = \mathcal{G}$ simply by interchanging $\mathcal{F}$ and $\mathcal{G}$. □