Galois Theory - Week 4 - Field Extensions

Antonio León Villares

January 2023

Contents

Based on the notes by Tom Leinster, Chapter 4

1 Introducing Field Extensions

1.1 Definition: Field Extension

*Let K be a **field**.*
*An **extension** of K is:*

- *a **field** M*
- *alongisde a **homomorphism**:*

$$\iota : K \to M$$

*We write $M : K$ (read "M over K") to mean that M is an **extension** of K, whereby ι is typically the **inclusion homomorphism**.*
(Definition 4.1.1)

1.1.1 Clash Between Intuition and Definition

*This definition might seem **counterintuitive**. We should think of an **extension** as something that **extends** our **field** K.*
For example, we defined:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

*We have been considering these extensions as **fields**, which have K as a **subfield** - or at least a **subset** ($\mathbb{Q}$ is a **subfield** of $\mathbb{Q}(\sqrt{2})$).*
*However, this isn't **formally** the case: for example, it is simple to argue that $\mathbb{R}$ isn't a subset/subfield of $\mathbb{C}$. This is rather simple: $\mathbb{R}$ contains objects like $6, -2, \pi^2$; but these objects aren't part of $\mathbb{C}$. However, $\mathbb{C}$ **does** have $6 + 0i$, $-2 + 0i$ or $\pi^2 + 0i$.*
*What we are doing under the hood is using a **homomorphism** $\iota : \mathbb{R} \to \mathbb{C}$:*

$$x \mapsto x + 0i$$

1.1.2 Examples of Field Extensions

- $\mathbb{C}$ alongside the inclusion $\iota : \mathbb{Q} \to \mathbb{C}$ is an **extension** of $\mathbb{Q}$, so $\mathbb{C} : \mathbb{Q}$. Similarly, $\mathbb{C} : \mathbb{R}$ and $\mathbb{R} : \mathbb{Q}$
- consider:

  $$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

  Clearly, $\mathbb{Q}(\sqrt{2})$ is a **subring** of $\mathbb{C}$, since:
  - it contains the identity of $\mathbb{C}$
  - it is clearly closed under subtraction (the $\sqrt{2}$ doesn't "mix" with the rationals)

– similarly, we have closure under multiplication

Moreover, it is a **subfield**, since the inverse of $a + b\sqrt{2}$ (with a, b non-zero) is:

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

where the denominator is non-zero, since $\sqrt{2}$ is irrational. Hence, we have an extension:

$$\mathbb{C} : \mathbb{Q}(\sqrt{2})$$

(again using inclusion). Moreover, again with inclusion we get that:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \implies \mathbb{Q}(\sqrt{2}) : \mathbb{Q}$$

- we can see that we get a field:

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}$$

which extends the rationals:

$$\mathbb{Q}(\sqrt{2}, i) \ : \ \mathbb{Q}$$

but which extends to the complex numbers:

$$\mathbb{C} : \mathbb{Q}(\sqrt{2}, i)$$

- the field of **rational expressions** $K(t)$ over K with homomorphism $\iota : K \to K(t)$:

$$\iota(a) = \frac{a}{1}$$

leads to a field extension:

$$K(t) : K$$

- **complex conjugation** is a homomorphism, and so we see that $\mathbb{C} : \mathbb{C}$

1.1.3 Exercises

1.2 Generating Fields from Sets

1.2.1 Definition: Subfield Generated by a Subset

> *Let K be a **field**, and $X \subseteq K$. The **subfield** of K **generated by** X is the **intersection** of all the **subfields** of K containing X.*
> *By definition, it is the **smallest** subfield of K containing X, in the sense that any subfield of K containing X must contain F.*
> *(Definition 4.1.4)*

1.2.2 Definition: Subfield Generated by Adjoining Subsets

We now formalise and generalise what we have been using, with examples like $\mathbb{Q}(\sqrt{2})$.

*Let $M : K$ be a **field extension**, and consider $Y \subseteq M$.*
*We write $K(Y)$ to denote the **subfield** of M generated by $K \cup Y$.*
$K(Y)$ is:

- *K **with** Y **adjoined***
- *or **the subfield of** M **generated by** Y **over** K*

*In particular, $K(Y)$ is the **smallest subfield** of M containing both K and Y.*

---

*If Y is **finite**:*

$$Y = \{\alpha_1, \ldots, \alpha_n\}$$

we write:

$$K(Y) = K(\alpha_1, \ldots, \alpha_n)$$

(Definition 4.1.8)

1.2.3 Examples of Generated Fields

- the subfield of K generated by $\emptyset$ is the **prime subfield**: every subfield contains $\emptyset$, so $\emptyset$ must generate the smallest possible subfield of K
- $L = \{a + bi \mid a, b \in \mathbb{Q}\}$ is nothing but the subfield of $\mathbb{C}$ generated by $\{i\}$. It is clearly a subfield, and if L' is any other subfield of $\mathbb{C}$, it must contain $\mathbb{Q}$ (since it is the prime subfield). Thus, L' must contain all the rationals, alongside i, so:

$$a, b, i \in L' \implies a + bi \in L' \implies L \subseteq L'$$

- in fact, $L = \mathbb{Q}(i)$: since $\mathbb{Q}$ is the prime subfield of $\mathbb{C}$, the subfield generated by $\mathbb{Q} \cup \{i\}$ is simply the smallest subfield of $\mathbb{C}$ containing i (since any subfield will automatically include $\mathbb{Q}$). The same reasoning works with $\mathbb{Q}(\sqrt{2})$: it is the subfield of $\mathbb{C}$ generated by $\{\sqrt{2}\}$
- when we use $K(t)$ to denote the field of rational expressions over K, we aren't abusing notation: it also corresponds to the smallest subfield of $K(t)$ containing both K and t. To this end, let L be any such subfield. Any polynomial over K is:

$$f(t) = \sum a_i t^i$$

Clearly, $f(t) \in L$, since $a_i, t \in L$, and L is a field (so there's closure). Hence, if $f(t), g(t)$ are polynomials over K, then:

$$f(t), g(t) \in L \implies f(t)/g(t) \in L$$

since where $f(t)/g(t)$ is a polynomial $h(t)$ satisfying:

$$g(t)h(t) = f(t)$$

Thus, it follows that $L = K(t)$!

1.2.4 Warning: On Adjoining to Create Subfields

In general, it is not the case that:

$$K(\alpha) = \{a + b\alpha \mid a, b \in K\}$$

In fact, we have that:

$$K(\alpha) = \left\{ \sum_{i=1}^{n-1} c_i \alpha^i \mid c_i \in K \right\}$$

*where n is the degree of the **minimal polynomial** of α (we will see this later on).*
For example, we have just seen that $K(t)$, the field of rational expressions is bigger than $\{a + bt \mid a, b \in K\}$, which isn't even a field (it isn't closed under multiplication)!
*Another more concrete example: let ζ be the **real** cube root of 2. It can be shown that ζ^2 can't be expressed as $a + b\zeta$, but clearly:*

$$\zeta \in \mathbb{Q}(\zeta) \implies \zeta^2 \in \mathbb{Q}(\zeta)$$

by closure, so we must have:

$$\mathbb{Q}(\zeta) = \{a + b\zeta + c\zeta^2 \mid a, b, c \in \mathbb{Q}\}$$

2 Algebraic and Transcendental Numbers ~~Over a Field~~

2.1 Definition: Algebraic and Transcendental Numbers

*Let $M : K$ be a **field extension**, and consider $\alpha \in M$. α is **algebraic over** K if:*

$$\exists f \neq 0_K \in K[t] \ : \ f(\alpha) = 0$$

*If no such f exists, α is **transcendental over** K.*
(Definition 4.2.1)

2.1.1 Examples of Algebraics and Transcendentals

- trivially, any $k \in K$ is algebraic over K, since $f(t) = t - k$ has k as a root
- classically, we know that π, e are **transcendental over** $\mathbb{Q}$ (given the extension $\mathbb{C} : \mathbb{Q}$), which also gives us that all transcendentals over $\mathbb{Q}$ must also be irrational
- however, π, e are **algebraic over** $\mathbb{R}$, since $e, \pi \in \mathbb{R}$
- $t \in K(t)$ is transcendental over K, since:

$$f(t) = 0 \iff f = 0$$

by definition of f

- the set of **complex numbers algebraic over** $\mathbb{Q}$ is denoted $\overline{\mathbb{Q}}$, which is a **subfield** of $\mathbb{C}$ - this is extremely non-trivial (try showing that it is even closed under addition)
- if $n \geq 1$, then $e^{2\pi i/n}$ is algebraic over $\mathbb{Q}$, since $f(t) = t^n - 1$ satisfies $f(\omega) = 0$

2.2 The Minimal Polynomial

2.2.1 Definition: Annihilating Polynomial

*Let $M : K$ be a **field extension**, and let $\alpha \in M$. An **annihilating polynomial** of α is a polynomial:*

$$f \in K[t] \ : \ f(\alpha) = 0$$

Thus:

$$\alpha \text{ is } \textbf{algebraic} \iff \alpha \text{ has a } \textbf{non-zero annihilating polynomial}$$

2.2.2 Lemma: The Minimal Polynomial Generates Annhiliating Polynomials

*Let $M : K$ be a **field extension**, and let $\alpha \in M$. Then:*

$$\exists m(t) \in K[t] \ : \ \langle m \rangle = \{\text{annihilating polynomials of } \alpha \text{ over } K\}$$

In particular:

- *if α is **transcendental over** K, then $m = 0$*
- *if α is **algebraic over** K, then m is a **unique, monic** polynomial called the **minimal polynomial of** α*

(Lemma 4.2.6)

Proof. Recall the **Universal Property of Polynomial Rings**:

*Let R, B be **rings**. Consider **any** homomorphism:*

$$\varphi : R \to B$$

*and **any** $b \in B$.*
*Then, there exists a **unique** homomorphism:*

$$\theta : R[t] \to B$$

such that:

$$\forall a \in R, \theta(a) = \varphi(a)$$
$$\theta(t) = b$$

(Proposition 3.1.6)

In particular, this implies that (using φ to be the inclusion $K \to M$) there is a unique homomorphism:

$$\theta : K[t] \to M$$

satisfying:

$$\forall a \in K,\ \theta(a) = a \qquad \theta(t) = \alpha$$

Explicitly:

$$\theta\left(\sum a_i t^i\right) = \sum a_i \alpha^i$$

In particular, the kernel $ker(\theta)$ corresponds to all polynomial $f \in K[t]$, such that $f(\alpha) = 0$, so:

$$ker(\theta) = \{\text{annihilating polynomials of } \alpha \text{ over } K\}$$

But a property of the kernel is that it is an ideal of $K[t]$, and since K is a field, $K[t]$ is a principal ideal domain, it follows that:

$$\exists m \in K[t]\ :\ ker(\theta) = \langle m \rangle$$

Then:

- if α is transcendental, $ker(\theta) = 0 \implies m = 0$
- if α is algebraic, then $m \neq 0$. We can freely multiply m by some non-zero constant, and this won't change the ideal, so we may assume that m is monic.

Now we just need to show that m is unique. To this end, consider any other $\tilde{m}$ such that:

$$ker(\theta) = \langle \tilde{m} \rangle$$

In particular this means that $\tilde{m} = cm$ for some non-zero constant c. But since $m, \tilde{m}$ are both monic, we must have that $c = 1$, so $m = \tilde{m}$, as required.

□

2.2.3 Lemma: Equivalent Conditions for Minimal Polynomials

*Let $M : K$ be a **field extension**, let $\alpha \in M$ be **algebraic over** K, and let $m \in K[t]$ be a **monic polynomial**. Then, the following are equivalent:*

1. *m is the **minimal polynomial** of α over K*
2. *$m(\alpha) = 0_K$, and for any **annihilating polynomial** f of α over K:*
$$m \mid f$$
3. *$m(\alpha) = 0_K$, and for any **non-zero annihilating polynomial** f of α over K:*
$$deg(m) \leq deg(f)$$
*That is, the **minimal polynomial** is the monic, annihilating polynomial of least degree.*
4. *$m(\alpha) = 0_K$ and m is **irreducible** over K*

Proof.

- (1) $\implies$ (2): this is immediate from the definition of a minimal polynomial ($f \in \langle m \rangle \iff m \mid f$)
- (2) $\implies$ (3): since $m \mid f$, it is immediate that $deg(m) \leq deg(f)$
- (3) $\implies$ (4): firstly, m can't be constant (unit), since m is monic, so we'd have $m = 1_K$, and clearly $m(\alpha) = 1_K \neq 0_K$. Thus, we must have:
$$\exists f, g \in K[t] \ : \ m(t) = f(t)g(t)$$
By (3):
$$m(\alpha) = 0_K \implies f(\alpha)g(\alpha) = 0_K$$
WLOG assume that $f(\alpha) = 0$, so f must be an annihilating polynomial. Thus, $deg(f) \geq deg(m)$ by (3). However, since f is a factor of g, we also have $deg(m) \geq deg(f)$, which implies that $deg(f) = deg(m)$, and so, $deg(g) = 0$, which implies that g is a unit. Hence, m is irreducible over K.
- (4) $\implies$ (1): let m_α denote the minimal polynomial of α. Assuming (4), we know that $m(\alpha) = 0$, and m is irreducible over K, so:
$$m_\alpha \mid m$$
by definition of the minimal polynomial. But since m is irreducible, and m_α can't be constant (a unit), it follows that m is a non-zero, constant multiple of m_α. Since both m, m_α are monic by assumption, it must be the case that $m = m_\alpha$.

□

2.2.4 Examples of Minimal Polynomials

- $t^2 - 2$ is the **minimal polynomial** of $\sqrt{2}$ over $\mathbb{Q}$. To see why, we can first note that it is clearly annihilating and monic:
  - since $\sqrt{2}$ is irrational, there is no polynomial with $deg(f) \leq 1$ which is annihilating, so by (3) $t^2 - 2$ must be minimal
  - recalling

> *Let K be a **field** and $f \in K[t]$. Then:*
>
> *1.*
> $$deg(f) \leq 0 \implies f \text{ is } \textbf{not irreducible}$$
> *2.*
> $$deg(f) = 1 \implies f \text{ is } \textbf{irreducible}$$
> *3.*
> $$deg(f) \geq 2 \text{ and } f \text{ has a } \textbf{root} \implies f \text{ is } \textbf{reducible}$$
> *4.*
> $$deg(f) \in \{2, 3\} \text{ and } f \text{ has } \textbf{no root} \implies f \text{ is } \textbf{irreducible}$$
> *(Lemma 3.3.1)*

    we can see that $t^2 - 2$ has no root in $\mathbb{Q}$, and is of degree 2, so it is irreducible, so by (4), $t^2 - 2$ must be minimal

- the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $t^3 - 2$. This can be shown by noting that it has no root in $\mathbb{Q}$ and degree 3 (or using Eisenstein with $p = 2$). However, notice it isn't trivial to show that $t^3 - 2$ is the annihilating polynomial of least degree
- if $\omega = e^{2\pi i/p}$, ω is a root of $t^p - 1$, but this isn't the minimal polynomial, as it is reducible:

$$t^p - 1 = (t - 1)m(t) = (t - 1)(t^{p-1} + \ldots + t + 1)$$

  Since $\omega - 1 \neq 0$, we must have that $m(\omega) = 0$, and m is irreducible over $\mathbb{Q}$ (it is the pth **cyclotomic polynomial**), so it must be the minimal polynomial

3 Simple Extensions

3.1 Motivation

3.1.1 Extending the Rationals to Contain Roots

Suppose we want to find a field K, such that for any non-constant polynomial over $\mathbb{Q}$, K contains the roots of the polynomial. For $\mathbb{Q}$ this is trivial: by the ***Fundamental Theorem of Algebra****, we know that any root of a polynomial in $\mathbb{Q}$ will lie in $\mathbb{C}$, so we take $K = \mathbb{C}$, and we are done!*

Now, lets try to be a bit more economical. Say we have an ***irreducible, monic*** *polynomial m over $\mathbb{Q}$. Say that $\alpha \in \mathbb{C}$ is a root of m. We know that $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing α.*

However, we can look at this from a different perspective. Say we want to find an extension for $\mathbb{Q}$ containing some $\alpha \in \mathbb{C}$. By the ***Universal Property****, we know that there's a homomorphism:*

$$\theta : \mathbb{Q}[t] \to \mathbb{C}$$
$$\sum a_i t^i \mapsto \sum a_i \alpha^i$$

We know that the ***kernel*** *$ker(\theta)$ is the ideal containing all the annihilating polynomials of α over $\mathbb{Q}$, which is generated by the* ***minimal polynomial****:*

$$ker(\theta) = \langle m \rangle$$

Moreover, by the ***First Isomorphism Theorem*** *we have that:*

$$im(\theta) \cong \mathbb{Q}[t]/\langle m \rangle$$

We know that $\mathbb{Q}[t]/\langle m \rangle$ will be a subfield of $\mathbb{C}$ ($im(\theta)$ is a subring, and the quotient of an integral domain by an ideal of an irreducible element is a field). Moreover, we know that $\alpha = \theta(t) \in im(\theta)$. In other words, $im(\theta)$ ***is a subfield of $\mathbb{C}$ containing α****!*

In fact, we have that:

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[t]/\langle m \rangle$$

That is, we can start with a root or a minimal polynomial, and we arrive at the same subfield of $\mathbb{C}$! To see why, as we discussed above $\mathbb{Q}(\alpha)$ must contain any polynomial in α, $f(\alpha)$. But any such polynomial must be in $\mathbb{Q}[t]$, so $f(\alpha) \in im(\theta)$.

3.1.2 Extending Arbitrary Fields to Contain Roots

Unfortunately, we don't always get to work with nice fields like $\mathbb{Q}$ and $\mathbb{C}$. However, it is easy to adapt what we've done above to an abstract field K.

Generally, given a field K and an irreducible polynomial $m \in K[t]$, we can adjoin a root α of m to K by considering:

$$K[t]/\langle m \rangle$$

where α will be the equivalence class of t in $K[t]/\langle m \rangle$.

More concretely, we know that $K[t]/\langle m \rangle$ is a field, and we have a homomorphism:

$$K \to K[t]/\langle m \rangle$$

which can be constructed by chaining homomorphisms:

$$K \xrightarrow{\phi} K[t] \xrightarrow{\pi} K[t]/\langle m \rangle$$

*(ϕ is the inclusion $a \mapsto a$, and π is the canonical homomorphism). In particular, this means that we have a **field extension** $K[t]/\langle m \rangle : K$, given by the homomorphism $\phi \circ \pi$. If we call $\pi(t) = \alpha$, then:*

$$\pi\left(\sum a_i t^i\right) = \sum a_i \alpha^i$$

*Below, we formalise our discussion above for K, involving how α is a root of m, and how this extension is actually **economical**: it is as small as can be.*

3.1.3 Example

Example from this video

Consider the field $F = \mathbb{Z}_2$ and the polynomial $m = t^3 + t + 1$ (you can see that this is irreducible, since it has degree 3 and no roots in F). What field is the field $F[t]/\langle m \rangle$?

From Honours Algebra, we can intuitively think of it as the set of equivalence classes, such that 2 elements are equal if subtracting one from the other leads to a polynomial with a factor of m. This immediately allows us to discard polynomials of degree 3 or more, since we can always write such polynomials as $p = mq + r$, which reduces to r over $F[t]/\langle m \rangle$, and $deg(r) \leq 2$. Hence, we immediately get:

$$F[t]/\langle m \rangle = \{0, 1, t, 1+t, t^2, 1+t^2, t+t^2, 1+t+t^2\}$$

Notice, this extends our base field F, and contains a root t, such that $m(t) = 0$.

3.2 Lemma: Formalising the Motivation

*Let K be a **field**. Then:*

1. *Let $m \in K[t]$ be **monic** and **irreducible**. Let:*

$$\pi(t) = \alpha \in K[t]/\langle m \rangle$$

*be the **image** of t under the **canonical homomorphism**:*

$$\pi : K[t] \to K[t]/\langle m \rangle$$

*Then, α has a **minimal polynomial** m over K, and $K[t]/\langle m \rangle$ is **generated** by α over K ($K[t]/\langle m \rangle = K(\alpha)$).*

2. *The element t of the field $K(t)$ is **transcendental** over K, and $K(t)$ is **generated** by t over K.*

(Lemma 4.3.1)

Proof.

(1)

Write:

$$M = K[t]/\langle m \rangle$$

We have that:

$$\pi\left(\sum a_i t^i\right) = \sum a_i \alpha^i$$

which implies that $ker(\pi) = \langle m \rangle$ contains the set of annihilating polynomials of α over K. By definition, m must be the minimal polynomial of α over K.

Now, any subfield L of M which contains K and α must contain every polynomial in α over K ($1 + \alpha^2, 2 + 3\alpha^3, \ldots$), so $L = M$. In other words, $M = K(\alpha)$.

(2)

We already showed above that t is transcendental in $K(t)$. Let L be a subfield of $K(t)$ which contains both K and t. If $f, g \in K[t]$ are in L, then by properties of fields $f/g \in L$, so $L = M$, and $M = K(t)$.

□

3.3 Morphisms Over Fields

3.3.1 Definition: Homomorphisms Over Fields

Let K be a field, and let:

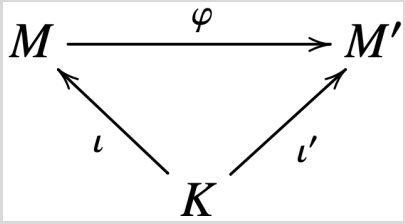
$$\iota_1 : K \to M_1$$

$$\iota_2 : K \to M_2$$

define extensions of K.
*A **homomorphism**:*

$$\varphi : M_1 \to M_2$$

*is said to be an **homomorphism over** K if the following commutes:*



(Here $M = M_1$ and $M' = M_2$)
Explicitly, we must have:

$$\forall a \in K,\ \varphi(\iota_1(a)) = \iota_2(a)$$

If ι_1, ι_2 are just inclusions, we can shorten notation, and just require:

$$\forall a \in K,\ \varphi(a) = a$$

(Definition 4.3.3)

- **Is complex conjugation a homomorphism over $\mathbb{R}$?**
  - yes, since clearly it defines a homomorphism, and:

$$\forall a \in \mathbb{R},\ \bar{a} = a$$

3.3.2 Lemma: Homomorphisms Over Fields are Determined by Value on Subsets

Let M_1, M_2 be extensions of a field K, and let:

$$\varphi, \psi : M_1 \to M_2$$

*be **homomorphisms over** K.*
Let Y be a subset of M_1, such that $M_1 = K(Y)$. Then:

$$\forall a \in Y,\ \varphi(a) = \psi(a) \implies \varphi = \psi$$

In other words, knowing the behaviour of φ, ψ on Y is sufficient to understand φ, ψ on all of M_1.
(Lemma 4.3.6)

Proof. Recall the **equalizer**:

Let X, Y be sets, and let S be a subset of all functions of the form $X \to Y$.
*The **equalizer** of S is:*

$$Eq(S) = \{x \mid x \in X, \forall f, g \in S : f(x) = g(x)\}$$

*That is, the **equalizer** is the set of all $x \in X$ which are equal under all functions in S.*
(Definition 2.3.7)

alongside the fact that:

*Let K, L be **fields**, and let S be a subset of all **homomorphisms** of the form $K \to L$.*
*Then, the **equalizer** $Eq(S)$ is a **subfield** of K.*
(Lemma 2.3.8)

Now, since φ, ψ are homomorphisms over K, we have that:

$$\forall a \in K,\ \varphi(a) = a = \psi(a)$$

Moreover, by assumption:

$$\forall a \in Y,\ \varphi(a) = \psi(a)$$

Hence, it follows that $K \cup Y$ is a subset of $Eq\{\varphi, \psi\}$. But then, $Eq\{\varphi, \psi\}$ is a subfield of M_1, which contains $K \cup Y$, so it must be the case that:

$$Eq\{\varphi, \psi\} = K(Y)$$

but by assumption $K(Y) = M_1$, so:

$$Eq\{\varphi, \psi\} = M \implies \varphi = \psi$$

as required.

□

3.3.3 Proposition: Universal Properties of $K[t]/\langle m \rangle$ and $K(t)$

*Let K be a **field**. Then:*

1. *Let:*

   - *$m \in K[t]$ be **monic** and **irreducible***
   - *$L : K$ be an **extension** of K*
   - *$\beta \in L$ have **minimal polynomial** m*

   *If we write $\alpha = \pi(t)$ (where π is the **canonical homomorphism** $\pi : K[t] \to K[t]/\langle m \rangle$), then there is **exactly one** homomorphism:*

   $$\varphi : K[t]/\langle m \rangle \to L$$

   over K, such that $\varphi(\alpha) = \beta$.

2. *Let:*

   - *$L : K$ be an **extension** of K*
   - *$\beta \in L$ be **transcendental***

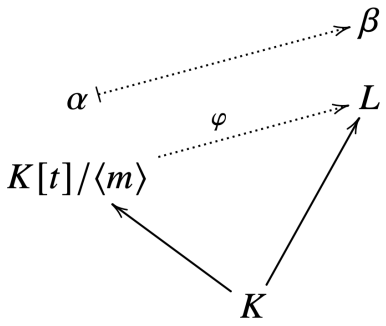
   *Then, there is **exactly one** homomorphism:*

   $$\varphi : K(t) \to L$$

   over K, such that $\varphi(t) = \beta$

(Propostion 4.3.7)

The first universal property can be described with a diagram:



*Notice, L is drawn higher than $K[t]/\langle m\rangle$ to convey that L may be bigger. This says that if m is a **monic, irreducible** polynomial over K, the **extension** $K[t]/\langle m\rangle$ contains a root of m, and said root generates the extension. In fact, we will show that this is the **only** such extension (up to isomorphism).*

For instance, if:

- $K = \mathbb{Q}$
- $m(t) = t^2 - 2$
- $L = \mathbb{C}$
- $\beta = -\sqrt{2} \in \mathbb{C}$

Then the universal property says that there exists a unique homomomorphism:

$$\varphi : \mathbb{Q}[t]/\left\langle t^2 - 2\right\rangle \to \mathbb{C}$$

which maps the equivalence class of t (namely $\pi(t)$) to $-\sqrt{2}$.

Proof.

(1)

We begin by showing that there is **at least** one homomorphism:

$$\varphi : K[t]/\langle m\rangle \to L$$

over K, such that $\varphi(a) = \beta$.

To this end, by the Universal property of Rings, there is exactly one homomorphism:

$$\theta : K[t] \to L$$

such that:

- $\forall a \in K,\ \theta(a) = a$
- $\theta(t) = \beta$

Then:

$$\theta(m(t)) = m(\beta) = 0 \implies \langle m\rangle \subseteq ker(\theta)$$

But now, recall the Universal Property of Factor/Quotient Rings:

*Let I be an **ideal** of the **ring** R. Define the **canonical homomorphism**:*

$$\pi_I : R \to R/I$$

Then:

1. *π_I is **surjective**, and:*

$$ker(\pi_I) = I$$

2. *If:*

$$\varphi : R \to S$$

*is a **ring homomorphism**, and:*

$$\varphi(I) = \{0_S\}$$

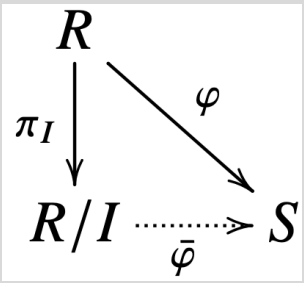
*(so that $I \subseteq ker(\varphi)$), then there exists a **unique ring homomorphism***

$$\bar{\varphi} : R/I \to S$$

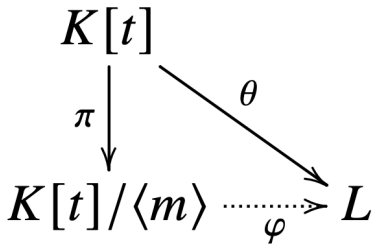
such that:

$$\varphi = \bar{\varphi} \circ \pi_I$$

Diagrammatically, we have:



Here, identifying $R = K[t]$, $I = \langle m \rangle$, $S = L$, it follows that there exists a unique homomorphism $\varphi : K[t]/\langle m \rangle \to L$ such that:



Moreover, φ will be a homomorphism over K:

$$\forall a \in K,\ \varphi(a) = \varphi(\pi(a)) = \theta(a) = a$$

and also:

$$\varphi(\alpha) = \varphi(\pi(t)) = \theta(t) = \beta$$

so we must have $\varphi(\alpha) = \beta$. Thus, we have demonstrated existence.

Next, we show that there is at most one homomorphism $K[t]/\langle m\rangle \to L$ over K such that $\alpha \mapsto \beta$. Assume that φ_1, φ_2 are 2 such homomorphism. Then:

$$\varphi_1(\alpha) = \varphi_2(\alpha)$$

and by Lemma 4.3.1:

> *Let K be a **field**. Then:*
>
> 1. *Let $m \in K[t]$ be **monic** and **irreducible**. Let:*
>
> $$\pi(t) = \alpha \in K[t]/\langle m\rangle$$
>
> *be the **image** of t under the **canonical homomorphism**:*
>
> $$\pi : K[t] \to K[t]/\langle m\rangle$$
>
> *Then, α has a **minimal polynomial** m over K, and $K[t]/\langle m\rangle$ is **generated** by α over K ($K[t]/\langle m\rangle = K(\alpha)$).*
>
> 2. *The element t of the field $K(t)$ is **transcendental** over K, and $K(t)$ is **generated** by t over K.*
>
> *(Lemma 4.3.1)*

α generates $K[t]/\langle m\rangle$ over K so by:

> *Let M_1, M_2 be extensions of a field K, and let:*
>
> $$\varphi, \psi : M_1 \to M_2$$
>
> *be **homomorphisms over** K.*
> *Let Y be a subset of M_1, such that $M_1 = K(Y)$. Then:*
>
> $$\forall a \in Y,\ \varphi(a) = \psi(a) \implies \varphi = \psi$$
>
> *In other words, knowing the behaviour of φ, ψ on Y is sufficient to understand φ, ψ on all of M_1.*
> *(Lemma 4.3.6)*

with $Y = \{\alpha\}$, we must have that $\varphi_1 = \varphi_2$, as required.

---

(2)

We begin by showing that there is at least one homomorphism $\varphi : K(t) \to L$ over K such that $\varphi(t) = \beta$. Recall, every element of $K(t)$ is given by f/g, with $f, g \in K[t]$ and $g \neq 0$. Since by assumption β is

transcendental over K, we have that $g(\beta) \neq 0$, so $f(\beta)/g(\beta) \in L$ is well-defined. In particular:

$$\varphi : K(t) \to L$$

defined by:

$$\frac{f(t)}{g(t)} \mapsto \frac{f(\beta)}{g(\beta)}$$

is a well-defined homomorphism. Moreover, it is clearly a homomorphism over K:

$$\forall a \in K,\ \varphi(a) = a \qquad \varphi(t) = \beta$$

proving the "at most" one case is similar to part (1). Consider 2 homomorphism $\varphi_1, \varphi_2 : K(t) \to L$ over K satisfying:

$$\varphi_1(t) = \beta = \varphi_2(t)$$

Since t generates $K(t)$ (again by 4.3.1), it follows (again by 4.3.6) that $\varphi_1 = \varphi_2$ on all $K(t)$.

□

3.3.4 Definition: Isomorphisms Over Fields

*Let M_1, M_2 be extensions of a field K. Then, a **homomophism**:*

$$\varphi : M_1 \to M_2$$

*is an **isomorphism over** K, if:*

- *it is a **homomorphism over** K*
- *it is an **isomorphism** of **fields***

*If such a φ exists, then M_1, M_2 are **isomorphic over** K.*

---

*It is important to remark that even if M_1, M_2 are **isomorphic**, this need not mean that they are **isomorphic over** K.*

3.3.5 Corollary to the Universal Property

Let K be a ***field****.*

1. *Let:*

   - $m \in K[t]$ *be* ***monic*** *and* ***irreducible***
   - $L : K$ *be an* ***extension*** *of* K
   - $\beta \in L$ *have* ***minimal polynomial*** m ***and*** $L = K(\beta)$

   If $\alpha = \pi(t)$ *(where* π *is the* ***canonical homomorphism*** $K[t] \to K[t]/\langle m \rangle$*), then there is* ***exactly one isomorphism****:*

   $$\varphi : K[t]/\langle m \rangle \to L$$

   over K*, such that* $\varphi(\alpha) = \beta$*.*

2. *Let:*

   - $L : K$ *be an* ***extension*** *of* K
   - $\beta \in L$ *be* ***transcendental*** *with* $L = K(\beta)$

   Then, there is ***exactly one isomorphism****:*

   $$\varphi : K(t) \to L$$

   over K*, such that* $\varphi(t) = \beta$*.*

Notice, this differs from the ***Universal Property*** *in the sense that* $L = K(\beta)$*.*
(Corollary 4.3.11)

Proof.

(1)

The Universal Property tells us that there is a unique homomorphism:

$$\varphi : K[t]/\langle m \rangle \to L$$

over K, such that $\varphi(\alpha) = \beta$. We just need to show that this is an isomorphim under the assumption that $L = K(\beta)$.

Homomorphism of fileds are automatically injective, so it is sufficient to show that φ is surjective. We know that $im(\varphi)$ is a subfield of L. Moreover:

- $K \in im(\varphi)$ (φ is a homomorphism over K, so $\forall a \in K,\ \varphi(a) = a$)

- $\beta \in L$ (since $\varphi(\alpha) = \beta$)

But then, since $im(\varphi)$ is a subfield containing K and β, it must be $K(\beta)$. But by assumption, $L = K(\beta)$, so $L = im(\varphi)$, so φ is surjective.

---

(2)

Again, this involves showing that $\varphi : K(t) \to L$ is surjective, which it is by following identical reasoning as above for (1).

□

3.3.6 Examples

- let m be a **monic, irreducible** polynomial over $\mathbb{Q}$, with complex root $\beta \in \mathbb{C}$. We know that the subfield $\mathbb{Q}(\beta)$ of $\mathbb{C}$ is an extension of $\mathbb{Q}$, generated by β. By the Corollary of the Universal Property, it follows that we have an isomorphism:

  $$\mathbb{Q}[t]/\langle m \rangle \cong \mathbb{Q}(\beta)$$

  over $\mathbb{Q}$.

- if β is a transcendental complex number, by the Corollay of the Universal Property, the field $\mathbb{Q}(t)$ is isomorphic to $\mathbb{Q}(\beta) \subseteq \mathbb{C}$.

3.4 Simple Field Extensions

3.4.1 Definition: Simple Field Extension

> *A **field extension** $M : K$ is **simple** if:*
>
> $$\exists \alpha \in M \ : \ M = K(\alpha)$$
>
> *(Definition 4.3.13)*

3.4.2 Examples

- the field extension:

  $$\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$$

  is simple, since:

  $$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

  To see why, notice that $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$. Thus:

  $$\sqrt{2} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \frac{(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3}))}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

  $$\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \frac{(\sqrt{2} + \sqrt{3})^3 - 11(\sqrt{2} + \sqrt{3}))}{-2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

  so:

  $$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

- $K(t) : K$ is **simple**

3.4.3 Theorem: Classification of Simple Extensions

Let K be a ***field****.*

1. *Let $m \in K[t]$ be a* ***monic, irreducible*** *polynomial. Then:*

$$\exists M : K,\ \exists \alpha \in M\ :\ M = K(\alpha)$$

where α is ***algebraic****, and has a* ***minimal polynomial*** *m over K. Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is* ***exactly one isomorphism****:*

$$\varphi : M_1 \to M_2$$

over K, such that $\varphi(\alpha_1) = \alpha_2$.

2. *There exists an* ***extension*** *$M : K$ and a* ***transcendental*** *$\alpha \in M$, such that:*

$$M = K(\alpha)$$

Moreover, if (M_1, α_1) and (M_2, α_2) are 2 such pairs, there is ***exactly one isomorphism****:*

$$\varphi : M_1 \to M_2$$

over K, such that $\varphi(\alpha_1) = \alpha_2$.

(Theorem 4.3.16)

This theorem simply states that by adjoining a root α of some monic, irreducible polynomial m to ***any*** *field K, we obtain an extension $K(\alpha) : K$. Similarly, we can obtain an extension by adjoining a transcendental.*

Proof.

(1)

We can easily construct an extension $M = K[t]/\langle m \rangle$, and pick $\alpha = \pi(t)$. Again by Lemma 4.3.1, we have that $M = K(\alpha)$. Moreover, by the Corollary to the Universal Property, we get the unique homomorphism φ, with $\beta = \alpha_1$, and $\alpha = \alpha_2$.

(2)

This part follows similarly, but by using the second parts of Lemma 4.3.1 and the Corollary of the Universal Property.

□

3.4.4 Examples

- if K is a field without a square root of 2 (i.e for any $\alpha \in K$, we never have $\alpha^2 = 2 \in K$), then $t^2 - 2$ is irreducible over K (and clearly monic). Hence, by the classification of simple extensions, we can adjoin to K a root of $t^2 - 2$ to give an extension $K(\sqrt{2}) : K$

  This might not seem "revolutionary", since we have seen this done when $K = \mathbb{Q}$, where $\mathbb{Q}(\sqrt{2})$ is regarded as a subfield of $\mathbb{C}$. What makes it remarkable is that it works for **any** field with this property. For example, in $\mathbb{Z}_3$, 2 has no square root, so $\mathbb{Z}_3(\sqrt{2})$ defines an extension of $\mathbb{Z}_3$. To construct it, we consider:

$$\mathbb{Z}_3[t]/\left\langle t^2 - 2 \right\rangle = \{0, \}$$