Galois Theory - Week 6 - Homomorphism Extensions, Splitting Fields and the Galois Group

Antonio León Villares

February 2023

Contents

Based on the notes by Tom Leinster, Chapter 6

1 Extending Homomorphisms

1.1 Definition: Homomorphism Extension

Homomorphism extensions allow us to go between field extensions.

Let:

- ι_1 *be a* ***field extension****:*

$$\iota_1 : K_1 \to M_1$$

- ι_2 *be a* ***field extension****:*

$$\iota_2 : K_2 \to M_2$$

- ψ *be a* ***field homomorphism****:*

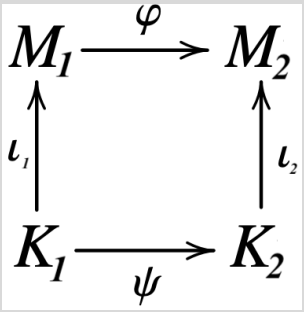
$$\psi : K_1 \to K_2$$

Then, a ***field homomorphism****:*

$$\varphi : M_1 \to M_2$$

extends ψ *if:*

$$\varphi \circ \iota_1 = \iota_2 \circ \psi$$



If we think of K_1 *as a* ***subset*** *of* M_1 *(and similarly with* K_2, M_2*), and view* ι_1, ι_2 *as* ***inclusions****, then* φ ***extends*** ψ *if:*

$$\forall a \in K_1, \quad \varphi(\iota_1(a)) = \iota_2(\psi(a)) \implies \varphi(a) = \psi(a)$$

(Definition 6.1.1)

1.1.1 Examples: Homomorphism Extensions

- let M_1, M_2 be extensions of K. If $\varphi : M_1 \to M_2$ extends $\psi = \mathrm{id}_K$, then φ must be a homomorphism over K:
$$\forall a \in K, \quad \varphi(a) = \psi(a) = a$$
- let $\kappa : \mathbb{C} \to \mathbb{C}$ denote complex conjugation. Then, κ extends the conjugation homomorphism over the subfield $\mathbb{Q}(i)$, $\gamma : \mathbb{Q}(i) \to \mathbb{Q}(i)$. This is trivial:
$$\forall p, q \in \mathbb{Q}, \quad \kappa(p + iq) = p - iq = \gamma(p + iq)$$

1.2 Lemma: Homomorphism Extension Preserves Roots

Consider ***field extensions****:*

$$M_1 : K_1 \qquad M_2 : K_2$$

and consider:

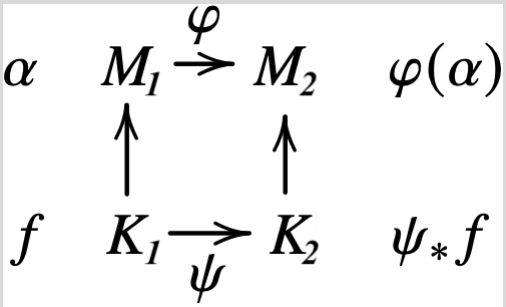
- ψ*, the* ***homomorphism****:*
$$\psi : K_1 \to K_2$$
- φ*, the* ***homomorphism*** *which* ***extends*** ψ*:*
$$\varphi : M_1 \to M_2$$
- ψ_**, the* ***homomorphism*** *induced by* ψ*, which maps between polynomial rings:*
$$\psi_* : K_1[t] \to K_2[t]$$

If:

$$\alpha \in M_1 \qquad f(t) \in K_1[t]$$

then, if we denote $\psi_* f = \psi_*(f)$*:*

$$f(\alpha) = 0_{K_1} \iff (\psi_* f)(\varphi(\alpha)) = 0_{K_2}$$



(Lemma 6.1.3)

Proof. We can write:

$$f(t) = \sum_i a_i t^i \in K_1[t], \quad a_i \in K_1$$

Then:

$$\psi_* f = \sum_i \psi(a_i) t^i \in K_2[t]$$

so:

$$\begin{aligned}(\psi_* f)(\varphi(\alpha)) &= \sum_i \psi(a_i)\varphi(\alpha)^i \\ &= \sum_i \varphi(a_i)\varphi(\alpha)^i, \quad \text{(since } \varphi \text{ extends } \psi\text{, so they are equal on } K_1\text{)} \\ &= \varphi\left(\sum_i a_i \alpha^i\right) \\ &= \varphi(f(\alpha))\end{aligned}$$

Since φ is a field homomorphism, in particular it is injective, so:

$$f(\alpha) = 0 \iff \varphi(f(\alpha)) = (\psi_* f)(\varphi(\alpha)) = 0$$

as required.

□

1.2.1 Corollary: Annihilating Polynomial

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

$$\varphi : M_1 \to M_2$$

*be a **homomorphism over** K:*

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

*Then, the **annihilating polynomials** of $\alpha \in M_1$ are the **same** as the **annihilating polynomials** of $\varphi(\alpha)$.*
(Example 6.1.4)

Proof. If φ is a homomorphism over K, then it is an extension of the trivial homomorphism $\psi = \mathrm{id}_K$ (this was the example above). Thus, by the above Lemma, if $\alpha \in M$ and $f(t) \in K[t]$:

$$f(\alpha) = 0 \iff (\psi_* f)(\varphi(a)) = 0 \iff f(\varphi(a)) = 0$$

where we have used the fact that ψ_* maps any polynomial to itself, since ψ is the identity mapping.

□

1.2.2 Exercises

1. *[Exercise 6.1.5]* **Show that if a ring homomorphism ψ is injective, then so is ψ_*; and if ψ is an isomorphism, then so is ψ_*.**

1.3 Lemma: Unique Isomorphism Extension

We now see that if 2 base fields are isomorphic, we can find a unique isomorphism between their corresponding extensions.

Let:

- ψ *be a* ***field isomorphism****:*

$$\psi : K_1 \to K_2$$

- $K_1(\alpha_1) : K_1$ *be a* ***simple extension****, where* α_1 *has* ***minimal polynomial*** $m \in K_1[t]$
- $K_2(\alpha_2) : K_2$ *be a* ***simple extension****, where* α_2 *has* ***minimal polynomial*** $\psi_* m \in K_2[t]$

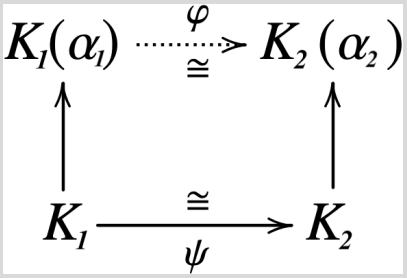
Then, there is ***exactly one isomorphism****:*

$$\varphi : K_1(\alpha_1) \to K_2(\alpha_2)$$

that:

1. ***extends*** ψ
2. *satisfies:*

$$\varphi(\alpha_1) = \alpha_2$$



(Proposition 6.1.6)

Proof. We can think of $K_2(\alpha_2)$ as an extension of K_1, by considering the homomorphism:

$$K_1 \xrightarrow{\psi} K_2 \longrightarrow K_2(\alpha_2)$$

Now, say that α_1 has a minimal polynomial $m \in K_1[t]$, and α_2 has a minimal polynomial $\psi_* m \in K_2[t]$. Then, since ψ, ψ_* will be isomorphism, we will have that $m \in K_1[t]$ is a minimal polynomial for α_2 over K_1 (since m and $\psi_* m$ are isomorphic, we are just "renaming" the coefficients in m when defining $\psi_* m$).

But now recall the Theorem on 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)*

Since m is minimal, it is monic and irreducible. We have the pairs (M_1, α_1) and (M_2, α_2), where α_1, α_2 both have m as a minimal polynomial over K_1. Hence, it follows that there exists a unique isomorphism:

$$\varphi : K_1(\alpha_1) \to K_2(\alpha_2)$$

over K_1, such that:

$$\varphi(\alpha_1) = \alpha_2$$

as required

□

2 The Existence and Uniqueness of Splitting Fields

2.1 Definition: Polynomial Splits in a Field

*Let f be a **polynomial** over a **field** M. Then, f **splits** in M if:*

$$f(t) = \beta(t - \alpha_1) \dots (t - \alpha_n)$$

where:

$$n \geq 0 \qquad \beta, \alpha_1, \dots, \alpha_n \in M$$

(Definition 6.2.2)

2.1.1 Examples: Fields over Which Polynomials Split

- a field M is **algebraically closed** if and only if every polynomial over M splits in M.
- let $f(t) = t^4 - 4t^2 - 5$. Then, f splits in $\mathbb{Q}(i, \sqrt{5})$, since:

  $$f(t) = (t^2 + 1)(t^2 - 5) = (t - i)(t + i)(t - \sqrt{5})(t + \sqrt{5})$$

  However, f doesn't split in $\mathbb{Q}(i)$, since its factorisation into irreducibles in $\mathbb{Q}(i)[t]$ is:

  $$f(t) = (t - i)(t + i)(t^2 - 5)$$

  which contains a non-linear factor.
- let $M = \mathbb{Z}_2(\alpha)$, where α is a root of:

  $$f(t) = 1 + t + t^2$$

  Then:

  $$f(a + \alpha) = 1 + (1 + \alpha) + (1 + 2\alpha + \alpha^2) = 1 + \alpha + \alpha^2 = 0$$

  Hence, f has distinct roots $\alpha, 1 + \alpha$:

  $$f(t) = (t - \alpha)(t - (1 + \alpha))$$

  so f splits in M, since $\alpha \in M \implies 1 + \alpha \in M$. However, it is not always the case (as we saw above), that adjoining a root will give us a field containing **all** roots.

2.2 Definition: Splitting Field of a Polynomial

Intuitively, a splitting field for a polynomial is the smallest field which contains all the roots of the polynomial.

*Let f be a **non-zero polynomial** over a **field** K. A **splitting field** of f over K is an **extension** $M : K$, such that:*

1. *f **splits** in M*
2. *if $\alpha_1, \dots, \alpha_n$ are roots of f in M, then:*

   $$M = K(\alpha_1, \dots, \alpha_n)$$

(Definition 6.2.6)

2.2.1 Examples: Splitting Fields

- since $\mathbb{C}$ is an algebraically closed field containing $\mathbb{Q}$, $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is the splitting field of $f \in \mathbb{Q}[t]$ with roots $\alpha_1, \ldots, \alpha_n$
- let:
$$f(t) = t^3 - 2 \in \mathbb{Q}[t]$$
which has complex roots:
$$\eta, \omega\eta, \omega^2\eta$$
where:
  - η is the **real** cube root of 2
  - $\omega = e^{2\pi i/3}$

  Then, the splitting field of f over $\mathbb{Q}$ is:
$$\mathbb{Q}(\eta, \omega\eta, \omega^2\eta) = \mathbb{Q}(\eta, \omega)$$
To see that adjoining just η isn't sufficient to get a splitting field, note that:
  - f is irreducible, so:
$$\deg_{\mathbb{Q}}(\eta) = 3$$
  - ω has minimal polynomial $1 + t + t^2$, so:
$$\deg \mathbb{Q}(\omega) = 2$$

  Thus, and applying the Tower Law:
$$[\mathbb{Q}(\eta, \omega) : \mathbb{Q}] = [\mathbb{Q}(\eta, \omega) : \mathbb{Q}(\eta)][\mathbb{Q}(\eta) : \mathbb{Q}] = 3[\mathbb{Q}(\eta, \omega) : \mathbb{Q}(\eta)]$$
$$[\mathbb{Q}(\eta, \omega) : \mathbb{Q}] = [\mathbb{Q}(\eta, \omega) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 2[\mathbb{Q}(\eta, \omega) : \mathbb{Q}(\omega)]$$
  Hence, $[\mathbb{Q}(\eta, \omega) : \mathbb{Q}]$ is divisible by 3 and 2. Moreover, by the Corollary:

> *Let $M : K$ be a **field extension** and:*
> $$\alpha_1, \ldots, \alpha_n \in M$$
> *Then:*
> $$[K(\alpha_1, \ldots, \alpha_n) : K] \leq [K(\alpha_1) : K] \ldots [K(\alpha_n) : K]$$
> *(Corollary 5.1.21)*

  It follows that $[\mathbb{Q}(\eta, \omega) : \mathbb{Q}] \leq 6$. Since 2 and 3 are coprime, we must thus have that $[\mathbb{Q}(\eta, \omega) : \mathbb{Q}] = 6$. On the other hand, as we've seen:
$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \qquad [\mathbb{Q}(\eta) : \mathbb{Q}] = 3$$
  Hence, we sometimes need to adjoin **all** roots to obtain the splitting field.
- let $f(t) = 1 + t + t^2 \in \mathbb{Z}_2[t]$. Since f is the minimal polynomial of α (by definition), and $\{1, \alpha\}$ is a linearly independent set in $\mathbb{Z}_2(\alpha)$, it follows that it forms a basis over $\mathbb{Z}_2$, so:
$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, 1 + \alpha\} = \mathbb{Z}_2 \cup \{\text{roots of } f \text{ in } \mathbb{Z}_2(\alpha)\}$$
  so by definition $\mathbb{Z}_2(\alpha)$ is a splitting field of f over $\mathbb{Z}_2$

2.3 Uniqueness of Polynomial Splitting Fields

We now seek to show that every non-zero polynomial f has exactly one splitting field. To do so, we first show existence (easy), and then uniqueness (hard).

2.3.1 Lemma: Bounding Degree of Splitting Field of a Polynomial

We begin by showing not only existence, but a bound on the degree of the splitting field.

> *Let $f \neq 0$ be a **polynomial** over a **field** K. Then, there exists a **splitting field** M of f over K, such that:*
>
> $$[M : K] \leq \deg(f)!$$
>
> *(Lemma 6.2.10)*

Proof. We prove by induction on $deg(f)$, for an arbitrary field K.

(1) **Base Case:** $n = 0$

If $deg(f) = 0$, then we have a constant polynomial. But then, $M = K$ will be a splitting field (since it has no roots, and f will trivially split), so:

$$[M : K] = 1 \leq 1 = 0!$$

(2) **Inductive Hypothesis:** $n = k$

Assume that the claim is true when $deg(f) \leq k$. That is, for such f, there exists a splitting field M of f over K, such that:

$$[M : K] \leq \deg(f)! = k!$$

(3) **Inductive Step:** $n = k + 1$

Consider some polynomial $f \in K[t]$, such that $\deg(f) = k + 1$. We can factorise f with some irreducible factor m. By the Theorem on 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)

we know that if α is some root of m ($m(\alpha) = 0$), there exists an extension:

$$K(\alpha) : K$$

In particular, we know that in $K(\alpha)[t]$:

$$(t - \alpha) \mid f(t)$$

so define:

$$g(t) = f(t)/(t - \alpha) \in K(\alpha)[t]$$

Then, it follows that $deg(g) = deg(f) - 1 = k$, so by the inductive hypothesis, there exists a splitting field M of g over $K(\alpha)$, such that:

$$[M : K(\alpha)] \leq \deg(g)! = k!$$

Notice, M will be a splitting field of f over K. We can write:

$$f(t) = (t - \alpha)g(t)$$

and g splits over M, so f will also split over M. Moreover, by the Tower Law:

$$[M : K] = [M : K(\alpha)][K(\alpha) : K] \leq \deg(g)! \deg(m) = k! \deg(m) \leq k! \deg(f) = (k + 1)!$$

which completes the induction.

□

2.3.2 Proposition: Isomorphisms Between Splitting Fields

The following result is useful in proving the uniqueness of splitting fields for polynomials.

Let:

- ψ *be an* ***isomorphism of fields****:*

$$\psi : K_1 \to K_2$$

-

$$0_{K_1} \neq f \in K_1[t]$$

- M_1 *be a* ***splitting field*** *of* f *over* K_1
- M_2 *be a* ***splitting field*** *of* $\psi_* f$ *over* K_2

Then:

1. *there exists an* ***isomorphism****:*

$$\varphi : M_1 \to M_2$$

   which ***extends*** ψ

2. *there are* ***at most*** $[M : K]$ *such* ***extensions*** φ

(Proposition 6.2.11)

Proof. Again, we prove this by induction on $\deg(f)$, for arbitrary K_1, K_2.

(1) **Base Case:** $n = 0$

If $\deg(f) = 0$, then we have a constant polynomial, so $M_1 = K_1$ and $M_2 = K_2$. In particular, by:

Let:

- ψ *be a* ***field isomorphism****:*

$$\psi : K_1 \to K_2$$

- $K_1(\alpha_1) : K_1$ *be a* ***simple extension****, where* α_1 *has* ***minimal polynomial*** $m \in K_1[t]$
- $K_2(\alpha_2) : K_2$ *be a* ***simple extension****, where* α_2 *has* ***minimal polynomial*** $\psi_* m \in K_2[t]$

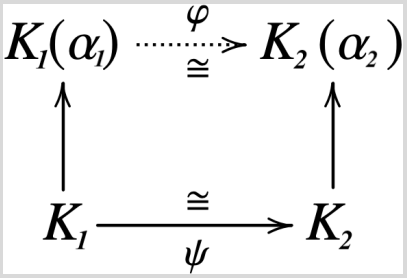
Then, there is ***exactly one isomorphism****:*

$$\varphi : K_1(\alpha_1) \to K_2(\alpha_2)$$

that:

1. ***extends*** ψ
2. *satisfies:*

$$\varphi(\alpha_1) = \alpha_2$$



(Proposition 6.1.6)

it follows that there is a unique isomorphism:

$$\varphi : M_1 \to M_2$$

which extends ψ. Hence, there is a single extension, and $[M : K] = 1$, so both parts follow.

(2) **Inductive Hypothesis:** $n = k$

Assume that if $\deg(f) \leq k$, the result follows: there are at most $[M : K]$ isomorphisms $\varphi : M_1 \to M_2$ extending ψ.

(3) **Inductive Step:** $n = k + 1$

□

2.3.3 Theorem: Non-Zero Polynomials Have a Unique Splitting Field

> *Let f be a* ***non-zero polynomial*** *over a* ***field*** *K. Then:*
>
> 1. *there exists a* ***splitting field*** *of f over K*
> 2. *any 2* ***splitting fields*** *of f are* ***isomorphic*** *over K*
> 3. *if M is a* ***splitting field*** *of f over K:*
>
> $$\#\ \textit{of}\ \textbf{\textit{automorphisms}}\ \textit{of}\ M\ \textit{over}\ K \leq [M : K] \leq \deg(f)!$$
>
> *(Theorem 6.2.13)*

Proof.

(1)

This is immediate from Lemma 6.2.10:

> *Let $f \neq 0$ be a* ***polynomial*** *over a* ***field*** *K. Then, there exists a* ***splitting field*** *M of f over K, such that:*
>
> $$[M : K] \leq \deg(f)!$$
>
> *(Lemma 6.2.10)*

(2)

This follows from Proposition 6.2.11:

Let:

- ψ *be an* ***isomorphism of fields****:*

$$\psi : K_1 \to K_2$$

-

$$0_K \neq f \in K_1[t]$$

- M_1 *be a* ***splitting field*** *of* f *over* K_1
- M_2 *be a* ***splitting field*** *of* $\psi_* f$ *over* K_2

Then:

1. *there exists an* ***isomorphism****:*

$$\varphi : M_1 \to M_2$$

   which ***extends*** ψ

2. *there are* ***at most*** $[M : K]$ *such* ***extensions*** φ

(Proposition 6.2.11)

by letting $K_1 = K_2$ and $\psi = \mathrm{id}_{K_1}$.

(3)

The first inequality follows from Proposition 6.2.11 again, with $K_1 = K_2, M_1 = M_2, \psi = \mathrm{id}_{K_1}$, and the second follows from Lemma 6.2.10.

□

2.3.4 Definition: THE Splitting Field

The above theorem allows us to talk about ***the splitting field*** *of* f ***unambiguously****. We denote the* ***splitting field*** *of* f *over a* ***field*** K *via* $SF_K(f)$.

2.4 Lemma: Splitting Field From Subset

1. *Let:*
   - $M : S : K$ *be a* ***field extension***
   - $$0_K \neq f \in K[t]$$
   - $Y \subseteq M$

   Let S *be the* ***splitting field*** *of* f *over* K*. Then,* $S(Y)$ *is the* ***splitting field*** *of* f *over* $K(Y)$*:*

   $$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$

2. *Let:*
   - $$0_K \neq f \in K[t]$$
   - L *be a* ***subfield*** *of* $SF_K(f)$ *containing* K*, such that:*

   $$SF_K(f) : L : K$$

   Then, $SF_K(f)$ *is the* ***splitting field*** *of* f *over* L*:*

   $$SF_K(f) = SF_L(f)$$

(Lemma 6.2.14)

Proof.

(1)

Since S is the splitting field of f, f splits in S. $S(Y)$ contains S, so f splits in $S(Y)$.

Now, let X be the set of roots of f in S. By definition of the splitting field:

$$S = K(X)$$

so:

$$S(Y) = (K(X))(Y) = K(X \cup Y) = (K(Y))(X)$$

In other words, $S(Y)$ will be the splitting field of f over $K(Y)$, by definition.

(2)

We have:

$$S = SF_K(f) : L : K$$

Let $Y = L$. Then by (1), $S(L) = S$ is the splitting field of f over $K(L) = L$. That is:

$$SF_K(f) = SF_L(f)$$

as required.

□

3 Galois Groups Revamped

One of the things that makes Galois Theory special is that we can leverage groups to study fields and polynomials. We explore this relationship in this section, where we redefine the ***Galois Group****.*

3.1 Motivating a New Definition for Galois Group

At the start of the course, we defined the ***Galois Group*** *in terms of the* ***subset*** *of S_k such that the* ***roots*** *of a* ***polynomial*** *were* ***conjugate*** *under the application of the symmetry. This made computing the* ***Galois Group*** *extremely difficult.*
We now present an alternative view of the ***Galois Group****: it can be defined by using the* ***symmetry group*** *of the* ***splitting field*** *of a* ***polynomial****.*
Why is this more convenient?

- *this generalise to* ***every*** *field, not just $\mathbb{Q}$ (before we needed to consider "conjugacy over $\mathbb{Q}$")*
- *some field extensions don't arise from* ***polynomials****, but have nonetheless interesting symmetry groups*
- *by leveraging* ***abstract algebra****, we don't require as much* ***explicit*** *computations involving* ***polynomials***

3.2 Redefining Galois Groups

3.2.1 Definition: Galois Group of Field Extension

*Let $M : K$ be a **field extension**. The **Galois Group** of $M : K$, denoted $Gal(M : K)$, is the **group of automorphisms** of M over K, where **composition** is the **group operation**.*

---

*Explicitly, an element of $Gal(M : K)$ is an **automorphism**:*

$$\theta : M \to M$$

such that:

$$\forall a \in K, \quad \theta(a) = a$$

(Definition 6.3.1)

3.2.2 Definition: Galois Group of a Polynomial

*Let $f \in K[t]$ be a **non-zero polynomial**. The **Galois Group** of f over K, denoted $Gal_K(f)$, is the **Galois Group** of the **splitting field** of f over K:*

$$Gal(SF_K(f) : K)$$

(Definition 6.3.5)

- **Is the Galois Group always finite?**
  - recall Theorem 6.2.13:

*Let f be a **non-zero polynomial** over a **field** K. Then:*

1. *there exists a **splitting field** of f over K*
2. *any 2 **splitting fields** of f are **isomorphic** over K*
3. *if M is a **splitting field** of f over K:*

$$\#\ of\ \textbf{automorphisms}\ of\ M\ over\ K \leq [M : K] \leq \deg(f)!$$

(Theorem 6.2.13)

– in particular, (3) implies that:

$$|Gal_K(f)| \leq [SF_K(f) : K] \leq \deg(f)!$$

so $Gal_K(f)$ is **always** a **finite group**

3.2.3 Examples: Galois Group for Field Extensions

- consider the extension $\mathbb{C} : \mathbb{R}$. Both the identity mapping id and complex conjugation κ are automorphisms of $\mathbb{C}$ over $\mathbb{R}$, so:

$$\{\text{id}, \kappa\} \subseteq Gal(\mathbb{C} : \mathbb{R})$$

Are there any other elements? Assume this is the case, and let $\theta \in Gal(\mathbb{C} : \mathbb{R})$. Then, in particular:

$$(\theta(i))^2 = \theta(i^2) = \theta(-1) = -\theta(1) = -1$$

This implies that $\theta(i) = \pm i$. But then:

– if $\theta(i) = i$, $\theta = \text{id}$ by the fact that $\mathbb{C} = \mathbb{R}(i)$ and using:

> *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 $M_1 = M_2 = \mathbb{C}, K = \mathbb{R}, Y = \{i\}$

– applying similar logic, if $\theta(i) = -i$, then $\theta = \kappa$

Hence:

$$Gal(\mathbb{C} : \mathbb{R}) = \{\text{id}, \kappa\} \cong C_2$$

- let η be the real cube root of 2. If $\theta \in Gal(\mathbb{Q}(\eta 9 : \mathbb{Q})$:

$$(\theta(\eta))^3 = \theta(\eta^3) = \theta(2) = 2$$

Hence:

$$\theta(\eta) \in \mathbb{Q}(\eta) \subseteq \mathbb{R}$$

Thus, $\theta(\eta)$ is a real cube root of 2, so $\theta(\eta) = \eta$. using Lemma 4.3.6, we must have that $\theta = \text{id}$, so $Gal(\mathbb{Q}(\eta) : \mathbb{Q})$ is trivial.

3.2.4 Exercises

1. *[Exercise 6.3.4]* **Prove that:**

$$Gal(\mathbb{Q}(e^{2\pi i/3} : \mathbb{Q}) = \{\text{id}, \kappa\}$$

where κ denotes complex conjugation.

3.2.5 Examples: Galois Group for Polynomials

- if $f \in K[t]$ splits in K, we have that $SF_K(f) = K$, so:

$$|Gal_K(f)| \leq [SF_K(f) : K] = 1 \implies |GaL_K(f)| = 1$$

  so $Gal_K(f)$ is trivial.

- the above example shows that any polynomial over an algebraically closed field has a trivial Galois group
- if $f = t^2 + 1 \in \mathbb{Q}[t]$, then:

$$SF_{\mathbb{Q}}(f) = \mathbb{Q}(i)$$

  Using similar arguments as above (where we considered $\mathbb{C} : \mathbb{R}$) it can be shown that:

$$Gal_{\mathbb{Q}}(f) = Gal(\mathbb{Q}(i) : \mathbb{Q}) = \{\text{id}, \kappa\} \cong C_2$$

- let:

$$f(t) = (t^2 + 1)(t^2 - 2)$$

  Then, $Gal_{\mathbb{Q}}(f)$ is the group of automorphisms of $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}$. Using similar arguments to the ones in the examples above, it can be shown that:

$$\theta \in Gal_{\mathbb{Q}}(f) \implies \theta(i) = \pm i, \quad \theta(\sqrt{2}) = \pm\sqrt{2}$$

  The choice of sign determines θ, so:

$$|Gal_{\mathbb{Q}}(f)| = 4$$

  There are 2 groups of order 4 (C_4 and $C_2 \times C_2$), but any $\theta \in Gal_K(f)$ has order 1 or 2 (since if θ isn't the identity map for both $i, \sqrt{2}$, we have that $\theta^2 = \text{id}$). Thus, $Gal_{\mathbb{Q}}(f) \ncong C_4$, so $Gal_{\mathbb{Q}}(f) \cong C_2 \times C_2$

- notice, all these examples show a rather interesting property: when $Gal_{\mathbb{Q}}(f)$ acts on the set of roots, it always returns a root. In particular, if X is the set of roots of f:

$$\alpha \in SF_K(f) \cap X,\ \theta \in Gal_K(f)\ :\ (\theta, \alpha) \mapsto \theta(a) \in X$$

  This turns out to be true in general: the action of $Gal_K(f)$ on $SF_K(f)$ restricts to an **action** on the **set of roots**; in other words, the Galois Group permutes the roots of f

3.3 Connecting Definitions for Galois Groups

3.3.1 Lemma: Action of Galois Groups Defined by Effect on Polynomial Roots

> *Let f be a **non-zero polynomial** over a **field** K. Then, the **action** of $Gal_K(f)$ on $SF_K(f)$ **restricts** to an **action** on the set of **roots** of f in $SF_K(f)$.*
> *(Lemma 6.3.7)*

---

*Given a group G acting on X, and a **subset** $A \subseteq X$, the action **restricts** to A if:*

$$\forall g \in G, \forall a \in A, \qquad ga \in A$$

That is, the action of G on X is completely determined by how G acts on A.

Proof. We need to show that if $\theta \in Gal_K(f)$ and $\alpha \in SF_K(f)$ is a root of f. Then $\theta(\alpha)$ is also a root. But this is immediate from Example 6.1.4:

> *Let M_1, M_2 be **extensions** of a **field** K. Let:*
>
> $$\varphi : M_1 \to M_2$$
>
> *be a **homomorphism over** K:*
>
> $$\forall a \in K, \quad \varphi(a) = a$$
>
> *Then, the **annihilating polynomials** of $\alpha \in M_1$ are the **same** as the **annihilating polynomials** of $\varphi(\alpha)$.*
> *(Example 6.1.4)*

where $M_1 = M_2 = SF_K(f)$, and $\varphi = \theta \in Gal_K(f)$.

□

3.3.2 Lemma: Galois Group Acts Faithfully

> *Let f be a **non-zero polynomial** over a **field** K. Then, the **action** of $Gal_K(f)$ on the **roots** of f is **faithful**.*
>
> ---
>
> *Recall, G acts faithfully on X if:*
>
> $$\forall g, h \in G, \forall x \in X \ : \ gx = hx \implies g = h$$
>
> *Equivalently, G acts faithfully if:*
>
> $$\forall g \in G \ : \ gx = x \implies g = e_G$$
>
> *(Lemma 6.3.8)*

Proof. Let X be the set of roots of f in $SF_K(f)$. By definition, we have that:

$$SF_K(f) = K(X)$$

By Lemma 4.3.6:

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)

Hence, assume that $\theta \in Gal_K(f)$ is such that $\forall x \in X,\ \theta(x) = x$. Then, by Lemma 4.3.6, it follows that $\theta = \text{id}$ on all of $SF_K(f)$. Hence, θ must act faithfully.

□

- **What does this Lemma imply about the elements of the Galois Groups?**
  - let $\theta \in Gal_K(f)$
  - the above Lemma tells us that θ acts **faithfully**
  - in other words, it is entirely determined by how it permutes the roots of f
  - hence, we can view θ as a **permutation of roots**
- **Is the Galois Group a subgroup of S_k?**
  - suppose $f \in K[t]$ has k distinct roots:

    $$\alpha_1, \ldots, \alpha_k \in SF_K(f)$$

  - since we can identify each $\theta \in Gal_K(f)$ with a permutation of the roots, we know that:

    $$\exists \sigma_\theta \in S_k\ :\ \theta(\alpha_i) = \alpha_{\sigma_\theta(i)}$$

  - since the action is faithful, in particular, we have an **isomorphism**:

    $$\theta \mapsto \sigma_\theta$$

    such that:

    $$Gal_K(f) \cong \{\sigma_\theta \mid \theta \in Gal_K(f)\} \subseteq S_k$$

3.3.3 Definition: Conjugates Over Field Extensions

*We first defined conjugate tuples in terms of elements in $\mathbb{C}$ or $\mathbb{R}$ which were **indistinguishable** when viewed by polynomials over $\mathbb{Q}$. Notice, we were actually working over **field extensions**: $\mathbb{C} : \mathbb{Q}$ and $\mathbb{R} : \mathbb{Q}$. We now formalise the notion of conjugacy for arbitrary extensions.*

*Let $M : K$ be a **field extension**, and consider k-tuples of elements of M:*

$$k \geq 0 \qquad (\alpha_1, \ldots, \alpha_k) \qquad (\alpha'_1, \ldots, \alpha'_k)$$

*These tuples are **conjugate over** K if:*

$$\forall p \in K[t_1, \ldots, t_k],\ p(\alpha_1, \ldots, \alpha_k) = 0 \iff p(\alpha'_1, \ldots, \alpha'_k)$$

(Definition 6.3.9)

3.3.4 Proposition: Equivalence of Galois Group Definitions

*Let f be a **non-zero polynomial** over a **field** K, with k **distinct roots**:*

$$\alpha_1, \ldots, \alpha_k \in SF_K(f)$$

Then:

$$\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate over } K\}$$

*is a **subgroup** of S_k, **isomorphic** to $Gal_K(f)$.*
(Proposition 6.3.10)

Proof. Let $\sigma \in S_k$ be "good" if it belongs to the set:

$$\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate over } K\}$$

We want to show that σ is good **if and only if** $\sigma = \sigma_\theta$ for some $\theta \in Gal_K(f)$.

Firstly, assume that there is some $\theta \in Gal_K(f)$, such that:

$$\sigma = \sigma_\theta$$

In other words:

$$\theta(\alpha_i) = \alpha_{\sigma(i)}$$

Notice:

$$\begin{aligned} & p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \\ = {} & p(\theta(\alpha_1), \ldots, \theta(\alpha_k)) \\ = {} & \theta(p(\alpha_1, \ldots, \alpha_k)) \end{aligned}$$

where the last step follows from the fact that p is a polynomial over K, and θ is an isomorphism over K. Moreover, this further implies that:

$$p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) = 0 \iff \theta(p(\alpha_1, \ldots, \alpha_k)) = 0 \iff p(\alpha_1, \ldots, \alpha_k) = 0$$

so σ is good.

On the other hand, assume that σ is good. Since $\alpha_1, \ldots, \alpha_k$ are algebraic over $SF_K(f)$, they form a basis (Corollary 5.1.14) for $SF_K(f)$ over K, so in particular, any element of $SF_K(f)$ can be expressed as $p(\alpha_1, \ldots, \alpha_k)$ for some $p \in K[t_1, \ldots, t_k]$.

Define a function:

$$\theta : SF_K(f) \to SF_K(f)$$

via:

$$\theta(p(\alpha_1, \ldots, \alpha_k)) = p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)})$$

We claim that $\theta \in Gal_K(f)$. For this, we need to show it is both injective and surjective (it is clear it is an endomorphism).

Since σ is good, let $q, P \in K[t_1, \ldots, t_k]$, such that $P = p - q$. Applying the definition of conjugacy to P implies that:

$$P(\alpha_1, \ldots, \alpha_k) = 0 \iff P(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)})$$

so:

$$\begin{aligned} & p(\alpha_1, \ldots, \alpha_k) = q(\alpha_1, \ldots, \alpha_k) \\ \iff & p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) = q(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \\ \iff & \theta(p(\alpha_1, \ldots, \alpha_k)) = \theta(q(\alpha_1, \ldots, \alpha_k)) \end{aligned}$$

and thus, θ is an injective mapping.

Moreover, it is surjective. Let:

$$\alpha = \sum_{i=1}^{k} a_i \alpha_i \in SF_K(f)$$

Then:

$$\theta(\alpha) = \sum_{i=1}^{k} a_i \theta(\alpha_i) = \sum_{i=1}^{k} a_i \alpha_{\sigma(i)} \in SF_K(f)$$

Now, for any other $\alpha' \in SF_K(f)$, the difference between α', α will purely be based on the coefficients of the linear combination, and by applying σ to an appropriate α, we can always ensure that:

$$\theta(\alpha) = \alpha'$$

Thus, we have that θ is an automorphism of $SF_K(f)$, so $\theta \in Gal_K(f)$ and $\sigma = \sigma_\theta$, as required.

□

3.3.5 Corollary: Galois Subgroups from Extensions

We know see how the Galois Groups of polynomials vary over different extensions.

> *Let $L : K$ be a **field extension** and:*
>
> $$0 \neq f \in K[t]$$
>
> *Then, $Gal_L(f)$ is **isomorphic** to a **subgroup** of $Gal_K(f)$.*
> *(Corollary 6.3.12)*

---

*This might seem **counterintuitive** at first: after all, L is "larger" so we might expect that more automorphisms are possible, so we'd expect $Gal_K(f) \leq Gal_L(f)$. The key is to notice that precisely since L is larger, it is more likely that the roots of f lie in L, which then makes it so that any automorphism must fix said roots. For example, we saw that $Gal(\mathbb{C} : \mathbb{Q}) \cong C_2 \times C_2$, whilst, since $\mathbb{C}$ is **algebraically closed**, $Gal(\mathbb{C} : \mathbb{C})$ is trivial (since $|Gal(\mathbb{C})| \leq [\mathbb{C} : \mathbb{C}] = 1$).*

Proof. Say we have an extension $M : L : K$, and consider a set of k-tuples in M, which are conjugate over L. Then, they must also be conjugate over K. Intuitively, this follows by the fact that if a k-tuple is "indistinguishable" from L, it must be "indistinguishable" from K, since L contains K. In particular, this implies that:

$$\begin{aligned} &\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate over } L\} \\ \subseteq &\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate over } K\} \end{aligned}$$

which implies that:

$$Gal_L(f) \subseteq Gal_K(f)$$

Since Galois Groups are subgroups, this thus implies that:

$$Gal_L(f) \leq Gal_K(f)$$

as required. □

3.3.6 Example: Galois Subgroups

Consider the polynomial:

$$f(t) = (t^2 + 1)(t^2 - 2)$$

We'll consider its Galois Group over different fields.

(1) $\mathbb{Q}$

We already saw above that:

$$Gal_{\mathbb{Q}}(f) \cong C_2 \times C_2$$

since any automorphism of $SF_{\mathbb{Q}}(f)$ led to:

$$\theta(i) = \pm i \qquad \theta(\sqrt{2}) = \pm\sqrt{2}$$

(2) $\mathbb{R}$

Both roots of $t^2 - 2$ are real, so the splitting field of f over $\mathbb{R}$ will only have to adjoin i. In particular:

$$SF_{\mathbb{R}}(f) = SF_{\mathbb{R}}(t^2 + 1) = \mathbb{R}(i) = \mathbb{C}$$

Hence:

$$Gal_{\mathbb{R}}(f) = Gal(\mathbb{C} : \mathbb{R}) \cong C_2$$

as we showed in examples above.

(3) $\mathbb{C}$

As discussed, $Gal_{\mathbb{C}}(f)$ is the trivial subgroup, since $\mathbb{C}$ is algebraically closed, so $SF_{\mathbb{C}}(f) = \mathbb{C}$.

Hence, as predicted:

- $Gal_{\mathbb{C}}(f)$ is isomorphic to a subgroup of $Gal_{\mathbb{R}}(f)$
- $Gal_{\mathbb{R}}(f)$ is isomorphic to a subgroup of $Gal_{\mathbb{Q}}(f)$
- $Gal_{\mathbb{C}}(f)$ is isomorphic to a subgroup of $Gal_{\mathbb{Q}}(f)$

3.3.7 Corollary: Order of Galois Group Divides Order of Symmetric Group

*Let f be a **non-zero polynomial** over a **field** K, with k **distinct** roots in $SF_K(f)$. Then:*

$$|Gal_K(f)| \mid k!$$

(Corollary 6.3.14)

---

*This is important for 2 reasons. Firstly, it gives us a **tighter bound** on the order of a Galois Group:*

$$|Gal_K(f)| \leq k! \leq \deg(f)!$$

*Secondly, not only do we have a bound, but it limits the set of possible values to **divisors** of $k!$.*

Proof. This follows immediately, by applying Lagrange's Theorem and using the fact that $Gal_K(f)$ is isomorphic to a subgroup of S_k.

□