Galois Theory - Week 8 - The Fundamental Theorem of Galois Theory

Antonio León Villares

April 2023

Contents

Based on the notes by Tom Leinster, Chapter 8

1 The Galois Correspondence

1.1 Terminology for Galois Correspondence

1.1.1 Definition: Intermediate Fields

*Let $M : K$ be a **field extension**, where we view K as a **subfield** of M. An **intermediate field** of $M : K$ is a **subfield** of M containing K. We write:*

$$\mathscr{F} = \{\textit{intermediate fields of } M : K\}$$

*If $L \in \mathscr{F}$, we can draw such fields by placing **bigger fields** higher up:*

$$\begin{tikzcd}
M \arrow[d, dash] \\
L \arrow[d, dash] \\
K
\end{tikzcd}$$

1.1.2 Definition: Subgroups of the Galois Group

*Let $M : K$ be a **field extension**, where we view K as a **subfield** of M. We write:*

$$\mathscr{G} = \{\textit{subgroups of } Gal(M : K)\}$$

*If $H \in \mathscr{G}$, we can draw such subgroups by placing **bigger subgroups** lower down:*

$$\begin{tikzcd}
\{\iota\} \arrow[d, dash] \\
H \arrow[d, dash] \\
Gal(M : K)
\end{tikzcd}$$

1.1.3 Definition: The Fix Function

Define a function:

$$\begin{aligned} Fix : \mathscr{G} &\to \mathscr{F} \\ H &\mapsto Fix(H) \end{aligned}$$

- **Why does the Fix function define an intermediate field of $M : K$?**
  - since $H \in \mathscr{G}$, this implies that:
    $$H \subseteq Gal(M : K)$$
  - every element of $Gal(M : K)$ fixes every element of K, so:
    $$K \subseteq Fix(H)$$
  - since $Fix(H)$ is automatically a subfield of M, by definition, it is an **intermediate field**:
    $$Fix(H) \in \mathscr{F}$$

1.1.4 Definition: The Gal Function

Define a function:

$$\begin{aligned} Gal(M : -) : \mathscr{F} &\to \mathscr{G} \\ L &\mapsto Gal(M : L) \end{aligned}$$

- **Why does the Gal function define a subgroup of $Gal(M : K)$?**
  - if $L \in \mathscr{F}$, then $Gal(M : L)$ contains all automorphisms φ of M that fix each element of L
  - since $K \subseteq L$, any such φ will fix K, so:
    $$Gal(M : L) \leq Gal(M : K)$$
    so clearly:
    $$Gal(M : L) \in \mathscr{G}$$

1.1.5 Definition: The Galois Correspondence

Let $M : K$ be an extension. The ***Galois Correspondence*** *for $M : K$ is given by:*

$$\begin{tikzcd} \mathscr{F} \arrow[r, shift left, "Fix"] & \mathscr{G} \arrow[l, shift left, "Gal(M:-)"] \end{tikzcd}$$

when these functions are ***mutually inverse****, such that for all $L \in \mathscr{F}, H \in \mathscr{G}$:*

$$L = Fix(Gal(M : L)) \qquad H = Gal(M : Fix(H))$$

- **When will the Galois Correspondence fail? That is, when will *Gal* and *Fix* not be mutual inverses?**
  - consider the extension:
    $$\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$$
  - by the Tower Law, since $[M : K] = 3$, this extension has no non-trivial intermediate fields, so:
    $$\mathscr{F} = \{M, K\}$$
  - we have seen that $Gal(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ is trivial (since an element of the Galois Group can only send $\sqrt[3]{2}$ to itself)
  - hence, $|\mathscr{G}| = 1$, whereas $|\mathscr{F}| = 2$, so no correspondence can exist
- **Where does the Galois Correspondence fail above?**
  - if we compute:
    $$Fix(Gal(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}))$$
    since $Gal(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ is trivial, this is nothing but:
    $$Fix(Gal(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})) = Fix(\{id_{\mathbb{Q}(\sqrt[3]{2})}\}) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$$
- **What is the consequence of having a correct Galois Correspondence?**
  - if the **Galois Correspondence** is correct (i.e *Gal* and *Fix* are mutually inverse), then there is a **one-to-one** correspondence between **subgroups** of the **Galois Group** $Gal(M : K)$, and **intermediate fields** of the **extension** $M : K$
  - the **Fundamental Theorem of Galois Theory** gives us conditions under which they are mutually inverse

1.1.6 Lemma: Gal and Fix for All Extensions

Let $M : K$ be a ***field extension****. Then:*

1. *For $L_1, L_2 \in \mathscr{F}$:*

$$L_1 \subseteq L_2 \implies Gal(M : L_2) \subseteq Gal(M : L_1)$$

Similarly, for $H_1, H_2 \in \mathscr{G}$:

$$H_1 \subseteq H_2 \implies Fix(H_2) \subseteq Fix(H_1)$$

2. *For $L \in \mathscr{F}, H \in \mathscr{G}$:*

$$L \subseteq Fix(H) \iff H \subseteq Gal(M : L)$$

3. *For all $L \in \mathscr{F}$:*

$$L \subseteq Fix(Gal(M : L))$$

Similarly, for all $H \in \mathscr{G}$:

$$H \subseteq Gal(M : Fix(H))$$

(Lemma 8.1.2)

Proof.

①

Notice, this makes intuitive sense: if L_1 is a smaller subfield than L_2, then it is easier to find automorphisms of M which fix all of L_1, instead of fixing all of L_2. Similarly, if H_1 is a smaller subgroup than H_2, it is more likely that all of its elements fix “stuff” in M. Diagrammatically:

$$\begin{tikzcd}
M \arrow[d, dash] & \{\iota\} \arrow[d, dash] \\
L_2 \arrow[d, dash] & Gal(M : L_2) \arrow[d, dash] \\
L_1 \arrow[d, dash] & Gal(M : L_1) \arrow[d, dash] \\
K & Gal(M : K)
\end{tikzcd}$$

To be more explicit, assume that $L_1, L_2 \in \mathscr{F}$. Let $\varphi \in Gal(M : L_2)$. Since φ is an automorphism of M over L_2, it fixes L_2. But since $L_1 \subseteq L_2$, φ also fixes L_1. Hence, $\varphi \in Gal(M : L_1)$, so:

$$Gal(M : L_2) \subseteq Gal(M : L_1)$$

as required.

Similarly, assume that $H_1 \subseteq H_2$, and let $\alpha \in Fix(H_2)$. Then, by definition, for any $\theta \in H_2$:

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

But $H_1 \subseteq H_2$, so for any $\theta \in H_1$:

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

so $\alpha \in Fix(H_1)$ and:

$$Fix(H_2) \subseteq Fix(H_1)$$

as required.

②

Notice, $L \subseteq Fix(H)$ if and only if:

$$\forall \alpha \in L, \forall \theta \in H,\ \theta(\alpha) = \alpha$$

Similarly, $H \subseteq Gal(M : L)$ if and only if:

$$\forall \theta \in H, \forall \alpha \in L,\ \theta(\alpha) = \alpha$$

Thus, both statements are equivalent.

③

This follows immediately from 2. For the first statement, let $H = Gal(M : L)$, and for the second statement take $L = Fix(H)$.

□

1.1.7 Exercises

1. *[Exercise 8.1.8]* **Let p be a prime number, let $K = \mathbb{F}_p(u)$ and let M be the splitting field of $t^p - u$ over K. Prove that $Gal(M : -)$ and Fix are not mutually inverse.**

2 The Fundamental Theorem of Galois Theory

2.1 Theorem: Fundamental Theorem of Galois Theory

Let $M : K$ be a ***finite, normal, separable*** *extension. Write:*

$$\mathscr{F} = \{\textit{intermediate fields of } M : K\}$$

$$\mathscr{G} = \{\textit{subgroups of } Gal(M : K)\}$$

1. *The functions:*

   $$Gal(M : -) : \mathscr{F} \to \mathscr{G} \quad Fix : \mathscr{G} \to \mathscr{F}$$

   are ***mutually inverse****.*

2. $$\forall L \in \mathscr{F}, \quad |Gal(M : L)| = [M : L]$$
   $$\forall H \in \mathscr{G}, \quad [M : Fix(H)] = |H|$$

3. *Let $L \in \mathscr{F}$. Then:*

   $$L \textit{ is a } \textbf{\textit{normal extension}} \textit{ of } K$$
   $$\iff$$
   $$Gal(M : L) \textit{ is a } \textbf{\textit{normal subgroup}} \textit{ of } Gal(M : K)$$

   Moreover, in that case:

   $$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$

(Theorem 8.2.1)

- **What sort of extensions does the Fundamental Theorem of Galois Theory talk about?**
  - we require that $M : K$ be **finite**, **normal** and **separable**
  - we know that all **finite** and **normal** extensions are **splitting fields**
  - for **separability**, we operate either over fields of **characteristic** 0, or **finite** fields
  - thus, this theorem is about **splitting fields** which are either **finite**, or have **characteristic** 0

Proof. Note the following:

- Since $M : K$ is finite, normal and separable, for every $L \in \mathscr{F}$, the extension $M : L$ is finite and normal, as:

> *Let $M : L : K$ be **field extensions**. If $M : K$ is **finite** and **normal**, then so is $M : L$.*
> *(Corollary 7.1.6)*

  Moreover, it is separable:

> *Let $M : L : K$ be **field extensions**, and let $M : K$ be **algebraic**. Then:*
>
> $$M : K \text{ is } \textbf{separable} \implies M : L,\ L : K \text{ are } \textbf{separable}$$
>
> *(Lemma 7.2.16)*

- $Gal(M : K)$ is a finite group by

> *For every **finite**, **normal**, **separable** extension $M : K$:*
>
> $$|Gal(M : K)| = [M : K]$$
>
> *(Theorem 7.2.18)*

  so in particular any subgroup $H \in \mathscr{G}$ is finite too.

① & ②

Let $H \in \mathscr{G}$. Then:

- by Lemma 8.1.2 above (part 3):

$$H \subseteq Gal(M : Fix(H)) \implies |H| \leq |Gal(M : Fix(H))|$$

- by the preamble above, since $Fix(H) \in \mathscr{F}$, $M : Fix(H)$ is a finite, normal and separable extension, and

> *For every **finite**, **normal**, **separable** extension $M : K$:*
>
> $$|Gal(M : K)| = [M : K]$$
>
> *(Theorem 7.2.18)*

  we have that:

$$|Gal(M : Fix(H))| = [M : Fix(H)]$$

- lastly, since H is finite (as $Gal(M : K)$ is), and using

> *Let M be a **field** and H a **finite subgroup** of $Aut(M)$. Then:*
>
> $$[M : Fix(H)] \leq |H|$$
>
> *(Theorem 7.3.3)*

  it follows that:

$$[M : Fix(H)] \leq |H|$$

But then, we have the following chain of inequalities:

$$|H| \leq |Gal(M : Fix(H))| = [M : Fix(H)] \leq |H|$$

But certainly $|H| = |H|$, so in fact:

$$|H| = |Gal(M : Fix(H))| = [M : Fix(H)]$$

Since we have that $H \subseteq Gal(M : Fix(H))$, it also follows that:

$$H = Gal(M : Fix(H))$$

which shows that Gal inverts Fix.

Now, consider $L \in \mathscr{F}$.

- if we take $H = Gal(M : L)$ the equality $|H| = [M : Fix(H)]$ above becomes:

$$[M : Fix(Gal(M : L))] = |Gal(M : L)|$$

- using

> *For every **finite**, **normal**, **separable** extension $M : K$:*
>
> $$|Gal(M : K)| = [M : K]$$
>
> *(Theorem 7.2.18)*

  we have that:

$$|Gal(M : L)| = [M : L]$$

Thus, we have the following chained equality:

$$[M : Fix(Gal(M : L))] = |Gal(M : L)| = [M : L]$$

Notice, by using Lemma 8.1.2 (part 3) above, we have that:

$$L \subseteq Fix(Gal(M : L))$$

By the Tower Law:

$$[M : Fix(Gal(M : L))] = [M : L] = [M : Fix(Gal(M : L))][Fix(Gal(M : L)) : L]$$

This is true if and only if:

$$[Fix(Gal(M : L)) : L] = 1 \iff L = Fix(Gal(M : L))$$

which shows that Fix inverts Gal.

Thus, we have shown that Gal and Fix are mutually inverse, and that:

$$\forall L \in \mathscr{F}, \quad |Gal(M : L)| = [M : L]$$
$$\forall H \in \mathscr{G}, \quad [M : Fix(H)] = |H|$$

as required.

③

We already did most of the work for this when proving part 2 of:

> *Let $M : L : K$ be a **field extension**, with $M : K$ **finite** and **normal**. Then:*
>
> 1. *let*
>
> $$\varphi L = \{\varphi(\alpha) \mid \alpha \in L\}$$
>
>   *then*
>
> $$L : K \textit{ is a } \textbf{\textit{normal}} \textit{ extension} \iff \forall \varphi \in Gal(M : K),\ \varphi L = L$$
>
> 2. *if $L : K$ is a **normal** extension, then:*
>   - *$Gal(M : L)$ is a **normal subgroup** of $Gal(M : K)$*
>   - $$\frac{Gal(M : K)}{Gal(M : L)} \cong Gal(L : K)$$
>
> *(Theorem 7.1.15)*

We just need to show that if $L \in \mathscr{F}$, and $Gal(M : L)$ is a normal subgroup of $Gal(M : K)$, then L is a normal extension of K (Theorem 7.1.15 already gives us the $\implies$ direction *and* the statement on quotients).

Assume that $H = Gal(M : L)$ is a normal subgroup of $Gal(M : K)$. Then from:

> *Let $M : K$ be a **finite normal extension**, and let H be a **normal subgroup** of $Gal(M : K)$. Then, $Fix(H) : K$ is **normal**.*
> *(Proposition 7.3.7)*

it follows that $Fix(Gal(M : L)) : K$ is a normal extension. But from ①, we know that $Fix(Gal(M : L)) = L$, so $L : K$ is normal, which is what we wanted to show.

$\square$

2.2 Using the Fundamental Theorem

2.2.1 Useful Remarks

1. The **Galois Group permutes the roots of polynomials**

   - the **action** of $Gal_K(f)$ on $SF_K(f)$ is completely determined by how it operates on the roots of f in $SF_K(f)$:

> *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)*

   - the **action** is **faithful**:

> *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)*

2. If k is the number of **distinct roots** of f in $SF_K(f)$, then:

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

   - $Gal_K(f)$ is isomorphic to a subgroup of S_k:

> *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)*

- by **Lagrange's Theorem**, the order of the **Galois Group** divides $k!$:

> *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)*

3. The **Galois Group** maps **conjugates** to **conjugates** (over the base field)

- this is immediate from:

> *Let $M : K$ be a* ***finite normal*** *extension, and $\alpha_1, \alpha_2 \in M$. Then:*
>
> $$\alpha_1, \alpha_2 \text{ are } \textbf{\textit{conjugate}} \text{ over } K \iff \exists \varphi \in Gal(M : K) \; : \; \alpha_2 = \varphi(\alpha_1)$$
>
> *In other words, 2 elements are conjugate over K if there is an element of the* ***Galois Group*** *which maps between them.*
> *(Proposition 7.1.9)*

- moreover, 2 elements of M are **conjugate** if they share the same **minimal 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)*

4. If f is **irreducible**, then $Gal_K(f)$ acts **transitively** on the **roots**, so if α, β are roots of f, we can always find φ which satisfies $\varphi(\alpha) = \beta$

- this is immediate from:

Let f be an ***irreducible polynomial*** *over a field K. Then, the action of $Gal_K(f)$ on the* ***roots*** *of f is* ***transitive****.*
In other words, the action of the Galois Group on the set of roots generates ***one orbit****, so from one root, we can always reach all other roots through an element of the Galois Group; thus, if X denotes the set of roots of f:*

$$\forall \alpha_1, \alpha_2 \in X, \exists \varphi \in Gal_K(f) \ : \ \varphi(\alpha_1) = \alpha_2$$

(Corollary 7.1.11)

2.2.2 Finding Fixed Fields for a Subgroup

- **For a given subgroup, how can you compute its corresponding fixed field explictly?**
  - let H be a subgroup of $Gal(M : K)$
  - then:
    1. Find elements $\alpha_1, \ldots, \alpha_r$ fixed by H. Then:
       $$K(\alpha_1, \ldots, \alpha_r) \subseteq Fix(H)$$
    2. Ensure that:
       $$[M : K(\alpha_1, \ldots, \alpha_r)] = |H|$$
    3. Then, using the Fundamental Theorem, we know that:
       $$[M : Fix(H)] = |H|$$
       so by the Tower Law:
       $$[M : K(\alpha_1, \ldots, \alpha_r)] = [M : Fix(H)] \iff K(\alpha_1, \ldots, \alpha_r) = Fix(H)$$
  - this is similar to how in **linear algebra**, we prove that 2 subspaces are **equal** by showing that one is a **subset** of the other, and they have the same **dimension**

2.2.3 Corollary: Corollary to the FTGT

Let $M : K$ be a ***finite****,* ***normal****,* ***separable*** *extension. Then:*

$$\forall \alpha \in M \setminus K, \exists \varphi : \varphi(\alpha) \neq \alpha$$

where φ is an ***automorphism*** *of M over K.*
(Corollary 8.2.7)

Proof. By the Fundamental Theorem, we have that:

$$K = Fix(Gal(M : K))$$

Let $\alpha \in M \setminus K$. Since $\alpha \notin K$, then:

$$\alpha \notin Fix(Gal(M : K))$$

Thus, none of the elements of the Galois Group fix α, as required.

□

2.2.4 Example: Galois Group of Extensions of Prime Degree

Let $M : K$ be a normal, separable extension of prime degree p.

- by the **Fundamental Theorem of Galois Theory**, it follows that:

$$|Gal(M : K)| = [M : K] = p$$

- every group of prime order is **cyclic**, so:

$$Gal(M : K) \cong C_p$$

- by **Lagrange's Theorem**, $Gal(M : K)$ won't have any (non-trivial) subgroups; similarly, by the **Tower Law**, $M : K$ won't have any (non-trivial) intermediate fields
- hence, we obtain the following correspondence structure:

$$\mathscr{F} = \{M, K\} \qquad \mathscr{G} = \{\{\iota\}, Gal(M : K)\}$$

$$\begin{tikzcd}
M \arrow[d, dash] & & \{\iota\} \arrow[d, dash] \\
K & & Gal(M : K)
\end{tikzcd}$$

- M is a **normal** extension of K by construction, and K is a **normal** extension of K (since if f is an irreducible polynomial, and f has a root in K, then f must be linear, and this trivially splits in K)
- the trivial subgroup and the group itself are always normal subgroups

2.2.5 Example: Verifying a Known Galois Group

Back in Week 6, we considered the Galois Group of:

$$f(t) = (t^2 + 1)(t^2 - 2) \in \mathbb{Q}[t]$$

and showed that:

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

However, this was rather "hacky", and we now have tools which allow us to better explore the group structure.

Let:

- $M = SF_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt{2}, i)$
- $G = Gal(M : K) = Gal_{\mathbb{Q}}(f)$

M is, by construction, finite and normal (since it is a splitting field). It is also separable, since it has characteristic 0. Hence, the **Fundamental Theorem of Galois Theory** applies, so:

$$|G| = [M : K] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$, so:

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

Similarly, since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, i has minimal polynomial t^2+1 over $\mathbb{Q}(\sqrt{2})$, so:

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

Hence:

$$|G| = 4$$

The roots of f are $\pm\sqrt{2}, \pm i$, so the action of G on $SF_{\mathbb{Q}}(f)$ restricts to an action on these roots. Moreover, $\pm\sqrt{2}$ are conjugate, whereas $\pm i$ are conjugate. Thus, for any $\varphi \in G$, we must have that:

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

The choice of sign for where $i, \sqrt{2}$ get sent to thus determine φ entirely, and since $|G| = 4$, all 4 possibilities must occur. Thus, define:

$$G = \{\iota, \varphi_{+-}, \varphi_{-+}, \varphi_{--}\}$$

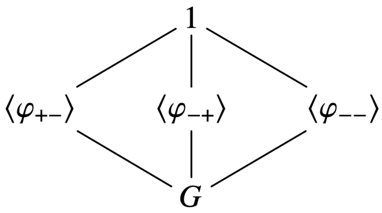
where:

$$\varphi_{+-}(\sqrt{2}) = \sqrt{2} \quad \varphi_{+-}(i) = -i$$
$$\varphi_{-+}(\sqrt{2}) = -\sqrt{2} \quad \varphi_{-+}(i) = i$$
$$\varphi_{--}(\sqrt{2}) = -\sqrt{2} \quad \varphi_{--}(i) = -i$$

Each element of G has order 2, and the only group of order 4 with all elements of order 2 is $C_2 \times C_2$, so:

$$G \cong C_2 \times C_2$$

and we have the following subgroup structure:


1
$\langle\varphi_{+-}\rangle$
$\langle\varphi_{-+}\rangle$
$\langle\varphi_{--}\rangle$
G

For the Galois Correspondence, we now have to find the corresponding intermediate subfields associated with these subgrouops. To this end, we follow the strategy outlined above: we find elements in M which get fixed by the subgroups, and adjoin these elements to $\mathbb{Q}$ until we have an extension whose degree agrees with the order of the subgroup. For this case, this is relatively easy:

- by construction:
$$\varphi_{+-}(\sqrt{2}) = \sqrt{2}$$
so it follows that $\mathbb{Q}(\sqrt{2}) \subseteq Fix(\langle\varphi_{+-}\rangle)$. Moreover, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. By the Fundamental Theorem, we also have that $[\mathbb{Q}(\sqrt{2}, i) : Fix(\langle\varphi_{+-}\rangle] = |\,\langle\varphi_{+-}\rangle\,| = 2$. Hence, using the Tower Law, it is clear that:
$$\mathbb{Q}(\sqrt{2}) = Fix(\langle\varphi_{+-}\rangle)$$

- similar logic then gives:
$$\varphi_{-+}(i) = i \implies Fix(\langle\varphi_{-+}\rangle) = \mathbb{Q}(i)$$
$$\varphi_{--}(\sqrt{2}i) = \sqrt{2}i \implies Fix(\langle\varphi_{--}\rangle) = \mathbb{Q}(\sqrt{2}i)$$

which then gives us the intermediate field structure:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}i) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The Galois Correspondence then tells us that, for example:

$$Gal(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)) = \langle \varphi_{-+} \rangle$$

Every subgroup of an abelian group is normal, so in particular all the intermediate fields lead to normal extensions.

2.2.6 Example: Working Out the Galois Correspondence for a New Polynomial

We now work with an example that is "big enough": smaller examples are easy/boring from the perspective of using the fundamental theorem (as we saw above), whilst larger examples are too complex and would require too much time. In particular, we want to work out all the details pertaining to the Galois Correspondence of:

$$t^4 - 2 \in \mathbb{Q}[t]$$

Using Eisenstein's Criterion with $p = 2$ shows that this is an irreducible polynomial. Finally, let:

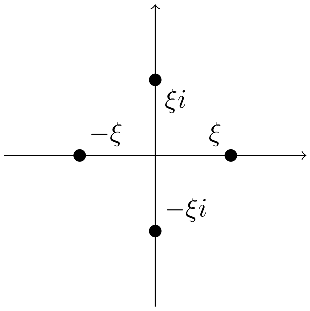
$$G = Gal_{\mathbb{Q}}(f)$$

① **The Splitting Field**

Let ξ denote the real, positive root of f. It is easy to check that the 4 roots of f are then:

$$\pm\xi, \pm\xi i$$

It helps to build intuition if we plot these 4 roots on the complex plane:



The splitting field of f over $\mathbb{Q}$ is:

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

② **The Galois Group**

For the Galois Group, we first determine the number of elements it contains, by using the **Fundamental Theorem of Galois Theory**. Indeed:

$$|G| = [\mathbb{Q}(\xi, i) : \mathbb{Q}] = [\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}]$$

Since $t^4 - 2$ is an irreducible, annihilating polynomial for ξ over $\mathbb{Q}$, it is it's minimal polynomial, so:

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg_{\mathbb{Q}}(\xi) = 4$$

Moreover, $\mathbb{Q}(\xi) \subseteq \mathbb{R}$, so certainly $i \notin \mathbb{Q}(\xi)$. $t^2 + 1$ is an irreducible, annihilating polynomial for i over $\mathbb{Q}(\xi)$, so:

$$[\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] = \deg_{\mathbb{Q}(\xi)}(i) = 2$$

Overall, it follows that:

$$|G| = [\mathbb{Q}(\xi, i) : \mathbb{Q}] = 2 \times 4 = 8$$

To find its elements, we first note that complex conjugation is certainly a non-trivial automorphism of $\mathbb{Q}(\xi, i)$ over $\mathbb{Q}$; denote it with κ.

We now claim that there exists $\rho \in G$ satisfying:

$$\rho(\xi) = \xi i \qquad \rho(i) = i$$

This is motivated by the fact that the roots $\pm\xi, \pm\xi i$ are conjugate. Since f is irreducible, G acts transitively on these roots, thus mapping each root to one of the other roots. In particular, $\exists \varphi \in G$ such that:

$$\varphi(\xi) = \xi i$$

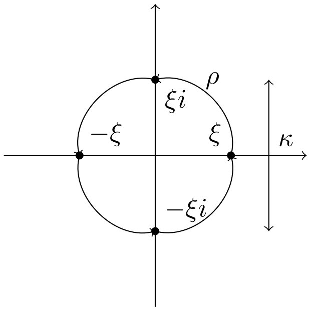
Now, $t^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$, so $\pm i$ are conjugate. In particular, since φ is an automorphism over $\mathbb{Q}$, we must have that:

$$\varphi(i) = \pm i$$

If $\varphi(i) = i$, then we can set $\rho = \varphi$, and the claim is true. Otherwise, $\varphi(i) = -i$. Then, we can define $\rho = \varphi \circ \kappa$, and then:

$$(\varphi \circ \kappa)(\xi) = \varphi(\xi) = \xi i \qquad (\varphi \circ \kappa)(i) = \varphi(-i) = -\varphi(i) = i$$

The action of ρ, κ on the roots can be visualised:



This action structure is strangely familiar: it highly ressembles that of D_4, the set of symmetries of the square. Notice, κ is an element of order 2, whereas ρ is an element of order 4 (see the diagram). If G is really the dihedral group, then we should have that:

$$\kappa\rho = \rho^{-1}\kappa$$

It is sufficient to check the effect of ρ, κ on ξ, i. Notice, 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)

if $\varphi, \theta \in G$ and:

$$\varphi(\xi) = \theta(\xi) \qquad \varphi(i) = \theta(i)$$

then $\varphi = \theta$.

$\varphi \in G$	$\varphi(\xi)$	$\varphi(i)$
ι	ξ	i
ρ	ξi	i
ρ^2	$-\xi$	i
$\rho^3 = \rho^{-1}$	$-\xi i$	i
κ	ξ	$-i$
$\kappa\rho$	$-\xi i$	$-i$
$\kappa\rho^2$	$-\xi$	$-i$
$\kappa\rho^3 = \kappa\rho^{-1}$	ξi	$-i$

Notice, we have defined 8 elements, each of which act differently on ξ, i, so these 8 elements must be the 8 elements of G. Moreover, computing:

$$\kappa\rho(\xi) = \kappa(\xi i) = -\xi i \qquad \kappa\rho(i) = \kappa(i) = -i$$
$$\rho^{-1}\kappa(\xi) = \rho^{-1}(\xi) = -\xi i \qquad \rho^{-1}\kappa(i) = \rho^{-1}(-i) = -i$$

Thus, we have that $\kappa\rho = \rho^{-1}\kappa$, so $G \cong D_4$, as required.

③ Galois Subgroups

We now look at the subgroup structure of G. By Lagrnage's Theorem, it follows that any non-trivial subgroup of G will have order 2 or 4.

The subgroups of order 2 are easy: these are the subgroups generated by elements of order 2, namely:

$$\langle \rho^2 \rangle, \langle \kappa \rangle, \langle \kappa\rho \rangle, \langle \kappa\rho^2 \rangle, \langle \kappa\rho^3 \rangle$$

Notice, ρ^2 (trivially) commutes with any ρ^r, and furthermore:

$$\kappa\rho^2 = \rho^2\kappa$$

by properties of the dihedral group. In other words, ρ^2 commutes with every element of G, so $\left\langle \rho^2 \right\rangle$ will be a normal subgroup of G. On the other hand, for $r \in \mathbb{Z}$, the subgroup $\langle \kappa\rho^r \rangle$ won't be 2 normal, since:

$$\begin{aligned}
\rho(\kappa\rho^r)\rho^{-1} &= (\rho\kappa)\rho^{r-1} \\
&= (\kappa\rho^{-1})\rho^{r-1} \\
&= \kappa\rho^{r-2} \notin \langle \kappa\rho^r \rangle
\end{aligned}$$

where for the last step, we use the fact that $\kappa\rho^{r-2}$ is never the identity, and:

$$\kappa\rho^{r-2} = \kappa\rho^r \iff \iota = \rho^2$$

which is false, since ρ has order 4. Hence, G has 5 subgroups of order 2 (isomorphic to C_2), but only one of these is a normal subgroup.

Since ρ has order 4, it generates a subgroup of order 4. In fact, it is the only element of order 4 alongside $\rho^3 = \rho^{-1}$, and ρ generates ρ^3. Hence, there is a single subgroup of order 4 isomorphic to C_4, namely:

$$\langle \rho \rangle = \{\iota, \rho, \rho^2, \rho^3\}$$

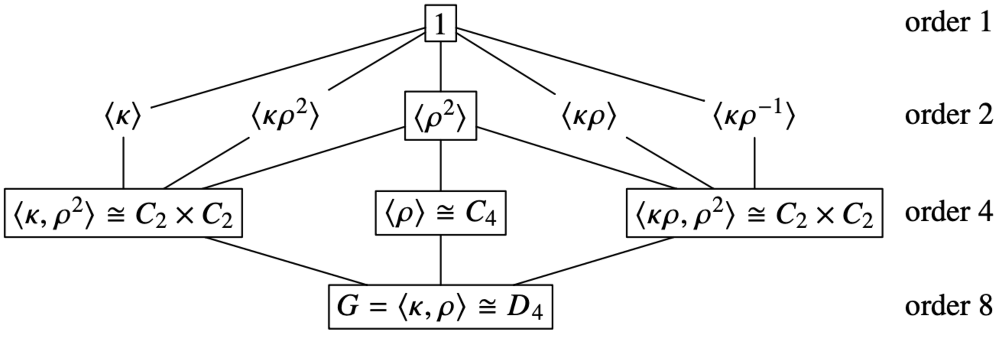
The other group of order 4 that exists is $C_2 \times C_2$. This group is characterised by all of its elements being its own inverses (it is isomorphic to the Klein 4 group). Any such group must contain ρ^2: it must contain elements of the form $\kappa\rho^r$, and none of the powers of ρ (aprt from ρ^2 are their own inverses). Knowing this, and using the fact that $\kappa, \kappa\rho$ are their own inverses, it follows that:

$$\left\langle \kappa, \rho^2 \right\rangle = \{\iota, \kappa, \rho^2, \kappa\rho^2\} \cong C_2 \times C_2$$

$$\left\langle \kappa\rho, \rho^2 \right\rangle = \{\iota, \kappa\rho, \rho^2, \kappa\rho^3\} \cong C_2 \times C_2$$

are the remaining subgroups of order 4.

Finally, notice that if $|H| = 4$, then $|G/H| = 2$, which immediately implies that H is a normal subgroup. Thus, the subgroup structure of G looks like:


1
order 1
$\langle\kappa\rangle$
$\langle\kappa\rho^2\rangle$
$\langle\rho^2\rangle$
$\langle\kappa\rho\rangle$
$\langle\kappa\rho^{-1}\rangle$
order 2
$\langle\kappa,\rho^2\rangle \cong C_2 \times C_2$
$\langle\rho\rangle \cong C_4$
$\langle\kappa\rho,\rho^2\rangle \cong C_2 \times C_2$
order 4
$G = \langle\kappa,\rho\rangle \cong D_4$
order 8

④ Intermediate Fields

This is perhaps where most ingenuity is required, as for each subgroup we need to find an element which gets fixed by its elements. For this, it is sufficient to look at which elements of $\mathbb{Q}(\xi, i)$ get fixed by the generators of the subgroup.

We can start looking at the subgroups of order 2:

$$\left\langle \rho^2 \right\rangle, \langle \kappa \rangle, \langle \kappa\rho \rangle, \left\langle \kappa\rho^2 \right\rangle, \left\langle \kappa\rho^3 \right\rangle$$

For convenience, let $M = \mathbb{Q}(\xi, i)$.

- since ρ fixes i, clearly ρ^2 fixes it too. However, this isn't enough, since by the Fundamental Theorem:

  $$[M : Fix(\rho^2)] = |\left\langle \rho^2 \right\rangle| = 2$$

  but

  $$[M : \mathbb{Q}(i)] = 4$$

  so we need more elements. One example is:

  $$\rho^2(\xi^2) = (\rho^2(\xi))^2 = (-\xi)^2 = \xi^2$$

  Then, we have that $\mathbb{Q}(\xi^2, i) \subseteq Fix(\rho^2)$:

  $$[M : \mathbb{Q}(\xi^2, i)] = 2$$

  To see why, we can think of M as $(\mathbb{Q}(\xi^2, i))(\xi)$. If we look at the minimal polynomial of ξ over $\mathbb{Q}(\xi^2, i)$, it will no longer be $t^4 - 2$, but rather:

  $$t^2 - \xi^2$$

  from which the above degree follows. Thus, by the Tower Law:

  $$Fix(\rho^2) = \mathbb{Q}(\xi^2, i)$$

- now consider κ. It is easy to see that $\kappa(\xi) = \xi$, so $\mathbb{Q}(\xi) \subseteq Fix(\kappa)$. Moreover, we saw above that:

  $$[M : \mathbb{Q}(\xi)] = 2$$

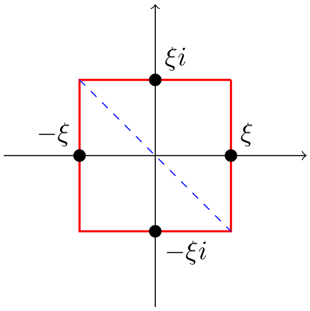
  and by the Fundamental Theorem:

  $$[M : Fix(\kappa)] = |\langle \kappa \rangle| = 2$$

  Thus, by the Tower Law:

  $$Fix(\kappa) = \mathbb{Q}(\xi)$$

- for $\kappa\rho$, finding a fixed element isn't as simple. However, if we think about it geometrically, we might get an idea. $\kappa\rho$ represents a rotation by 90º, followed by a reflection. This can be thought of as a reflection through the diagonals (from top left to bottom right) of a square.

  Thinking like this, we can pick any element along this diagonal, and it should get fixed by $\kappa\rho$. We have 2 easy choices for this:

  $$\xi - \xi i = \xi(1 - i) \qquad -\xi + \xi i = \xi(i - 1)$$

  We can check that indeed these get fixed (we only check the first one):

  $$\kappa\rho(\xi(1 - i)) = \kappa(\xi i(1 - i)) = \kappa(\xi(1 + i)) = \xi(1 - i)$$

Thus, $\mathbb{Q}(\xi(1-i)) \subseteq Fix(\kappa\rho)$. Now we just need to find:

$$[M : \mathbb{Q}(\xi(1-i))]$$

Now, $\xi(1-i)$ can't be the root of a quadratic over $\mathbb{Q}$, since:

$$(\xi(1-i))^2 = \xi^2(1-i)^2 = \xi^2(1-2i-1) = -2\xi^2 i \notin \mathbb{Q}$$

Moreover, we must have that $[\mathbb{Q}(\xi(1-i)) : \mathbb{Q}]$ divides 8 (the degree of $[M : \mathbb{Q}]$), which implies that:

$$[\mathbb{Q}(\xi(1-i)) : \mathbb{Q}] \geq 4 \iff [M : \mathbb{Q}(\xi(1-i))] \leq 8/4 = 2$$

$[M : \mathbb{Q}(\xi(1-i))] \neq 1$ as $M \neq \mathbb{Q}(\xi(1-i))$ (ξ isn't an element of $\mathbb{Q}(\xi(1-i))$). Hence, we must have that $[M : \mathbb{Q}(\xi(1-i))] = 2$, so again by the Fundamental Theorem and the Tower Law:

$$[M : Fix(\kappa\rho)] = |\langle\kappa\rho\rangle| = 2 \implies Fix(\kappa\rho) = \mathbb{Q}(\xi(1-i))$$

- for the remaining cases, similar arguments can be followed to see that:
  - $Fix(\kappa\rho^2) = \mathbb{Q}(\xi i)$
  - $Fix(\kappa\rho^3) = \mathbb{Q}(\xi(1+i))$

Now, we look at the subgroups of order 4:

$$\langle\rho\rangle, \langle\kappa, \rho^2\rangle, \langle\kappa\rho, \rho^2\rangle$$

- ρ fixes i by definition, so:

  $$\mathbb{Q}(i) \subseteq Fix(\rho)$$

  By the Fundamental Theorem:

  $$[M : Fix(\rho)] = |\langle\rho\rangle| = 4$$

  Since $i \notin \mathbb{Q}$, the minimal polynomial of ξ over $\mathbb{Q}(i)$ is still $t^4 - 2$, so:

  $$[M : \mathbb{Q}(i)] = 4$$

  and by the Tower Law:

  $$Fix(\rho) = \mathbb{Q}(i)$$

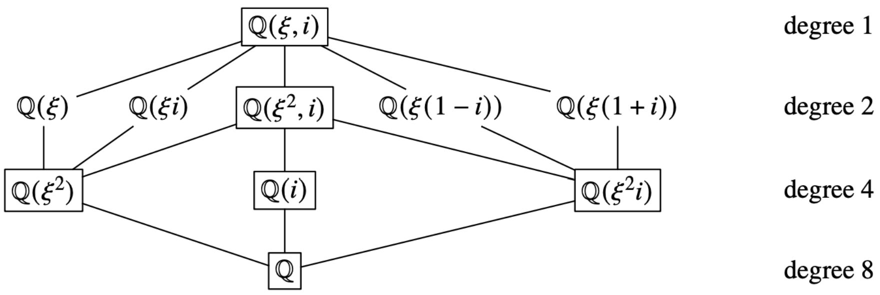
- with identical arguments, one can see that:
  - ξ^2 is fixed by both κ and ρ^2, so:

    $$Fix(\langle\kappa, \rho^2\rangle) = \mathbb{Q}(\xi^2)$$

  - $\xi^2 i$ is fixed by both $\kappa\rho$ and ρ^2, so:

    $$Fix(\langle\kappa\rho, \rho^2\rangle) = \mathbb{Q}(\xi^2 i)$$

Overall, this results in the following subfield structure:



⑤ **Normality**

The last step in using the Fundamental Theorem is in computing quotients. In particular, the Fundamental Theorem tells us that:

$$\frac{Gal(M:\mathbb{Q})}{Gal(M:L)} \cong Gal(L:\mathbb{Q})$$

Considering non-trivial normal intermediate fields L:

- if $L = \mathbb{Q}(\xi^2, i)$, then:

  $$G/\left\langle \rho^2 \right\rangle \cong Gal(\mathbb{Q}(\xi^2, i):\mathbb{Q})$$

  Using Lagrange's Theorem, we see that $Gal(\mathbb{Q}(\xi^2, i):\mathbb{Q}) = 8/2 = 4$. But this group contains no elements of order 4 (only ρ, ρ^3 have order 4 in G, but their images have order 2 in $G/\left\langle \rho^2 \right\rangle$). Thus:

  $$Gal(\mathbb{Q}(\xi^2, i):\mathbb{Q}) \cong C_2 \times C_2$$

  This is easy to see if we notice that $\mathbb{Q}(\xi^2, i)$ is the splitting field of $(t^2-2)(t^2+1)$, which we already saw has Galois Group isomorphic to $C_2 \times C_2$

- if L is any of the subfields of degree 4, then:

  $$\left| \frac{Gal(M:\mathbb{Q})}{Gal(M:L)} \right| = 8/4 = 2$$

  so it follows that:

  $$Gal(\mathbb{Q}(\xi^2):\mathbb{Q}) \cong Gal(\mathbb{Q}(i):\mathbb{Q}) \cong Gal(\mathbb{Q}(\xi^2 i):\mathbb{Q}) \cong C_2$$