The Galois Correspondence

Logan Gilbert
lagmath13@gmail.com

June 2022

What is Galois Theory?

Galois Theory is an area of mathematics created by French mathematician Évariste Galois. It is interested in connecting field and group theory, and in studying roots of polynomials.
The Galois Correspondence, or the Fundamental Theorem of Galois Theory, is an important result in the field that connects groups to fields.

Some Basic Definitions

To start off, let's define a few helpful terms. An example of a *group* would be the rational numbers $\mathbb{Q}$ or real numbers $\mathbb{R}$, with the operation of addition. If we look at some properties of $\mathbb{Q}$, we see that for all $a, b \in \mathbb{Q}$:

- $a + b \in \mathbb{Q}$;
- $a + 0 = 0 + a = a$;
- $a + (-a) = (-a) + a = 0$;
- $a + (b + c) = (a + b) + c$;
- $a + b = b + a$.

The first three properties of closure, identity (0), inverses and associativity are needed for a set and operation to be a group, with commutativity making $\mathbb{Q}$ an *abelian* group.

Some Basic Definitions

If we add another operation, multiplication, to our previous example, more behaviour emerges:

- $a \cdot b \in \mathbb{Q}$;
- $a \cdot b = b \cdot a$;
- $a \cdot 1 = 1 \cdot a = a$;
- If $a \neq 0$, $a \cdot (a^{-1}) = a^{-1} \cdot a = 1$;
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- $a \cdot (b + c) = a \cdot b + a \cdot c$.

With an extra operator, multiplication, and these extra conditions, we call $\mathbb{Q}$ a *field*.

Typical Groups and Applications

Some examples of groups include:

- Many typical sets form groups on addition, and fields on addition and multiplication. $\mathbb{Z}$ and $\mathbb{R}$ are groups on addition, and $\mathbb{R}$ and $\mathbb{C}$ are fields.
- Symmetry groups are groups on composition, and many exist such as cyclic (rotation) and dihedral groups in two dimensions.

With groups, we can define another useful term:

Definition (Homomorphisms)

A homomorphism is any function $f : G \to H$ *between groups* $(G, \cdot)$ *and* $(H, *)$ *such that* $\forall g_1, g_2 \in G$,

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2).$$

Isomorphisms and Automorphisms

Homomorphisms on their own can be useful, but often it is more useful to look at derivative ideas such as isomorphisms and automorphisms.

Definition (Isomorphisms)

An isomorphism is a bijective (one-to-one) homomorphism.

Definition (Automorphisms)

An automorphism is an isomorphism from a group to itself. In other words, any isomorphism $f : G \to G$ is an automorphism.

An example of an automorphism is complex conjugation ($\mathbb{C} \to \mathbb{C}$), as $(z_1 \cdot z_2)^* = z_1^* \cdot z_2^*$.
The set of all possible automorphisms of a group G is referred to as $Aut(G)$.

Field Extensions and Splitting Fields

Definition (Field Extensions)

A field extension K of a field F, also denoted K/F, is the smallest field containing the elements and operations of F, as well as other elements α. (This is also denoted as $F(\alpha)$.)

Often, a field extension will contain much more than the original field and added elements, as it must be closed. For example, $\mathbb{Q}(\sqrt{2})$ contains rational numbers and $\sqrt{2}$, but due to additive closure, it must also contain all $a + b\sqrt{2}$.

Definition (Splitting Field)

Given a field F and an irreducible, nonzero polynomial $f(x)$ with coefficients in F, the splitting field of $f(x)$ on F is the field extension of F containing all the roots of $f(x)$.

Fixed Fields

A fixed field is also a useful concept, and simple to understand.
Say that we have a field or field extension such as $K = \mathbb{Q}(\sqrt{2})$, and an automorphism such as one where $f(\sqrt{2}) = -\sqrt{2}$. Then, there exist some elements in the field that are left unchanged by the automorphism. We call these elements, which form a field, the *fixed field* of f on K. For a set of automorphisms S, we can also write the fixed field as K^S.
It is also useful to know what the dimension of a field extension is. Similarly to how it is defined for a vector field, we define it as the size of the smalest linearly independent spanning set of elements. It is typically written as $\dim_F(K)$, or $[K : F]$.

Galois Groups

Finally, we can define...

Definition (Galois Extensions and Groups)

A Galois Extension is a field extension E/F such that

1. *Every irreducible polynomial over F with a root in E factorizes linearly in E. (E/F is normal.)*
2. *For any $\alpha \in E$, the minimal polynomial of α over F has no repeated roots. (E/F is separable.)*

A Galois Group $Gal(E/F)$ is the same as $Aut(E/F)$ for any Galois field extension.

Alternatively, any Galois group $\mathrm{Gal}(K/F)$ must fix all the elements in F, and also $|Aut(K/F)| = [K : F]$ for a finite field extension.

An Example

Let's see if $\mathbb{Q}(\sqrt{2})$ is a Galois extension. To show this, we need to confirm that it is both normal and separable.
For it to be separable, the minimal polynomial of any $\alpha \in \mathbb{Q}(\sqrt{2})$ cannot have any repeated roots. We only need to look at $\sqrt{2}$. It has the minimal polynomial $x^2 - 2$, which factors into $(x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})$.
For it to be normal, the only noteworthy irreducible polynomial with a coefficient in $\mathbb{Q}(\sqrt{2})$ is $x^2 - 2$; this again factors linearly, so $\mathbb{Q}(\sqrt{2})$ is normal.

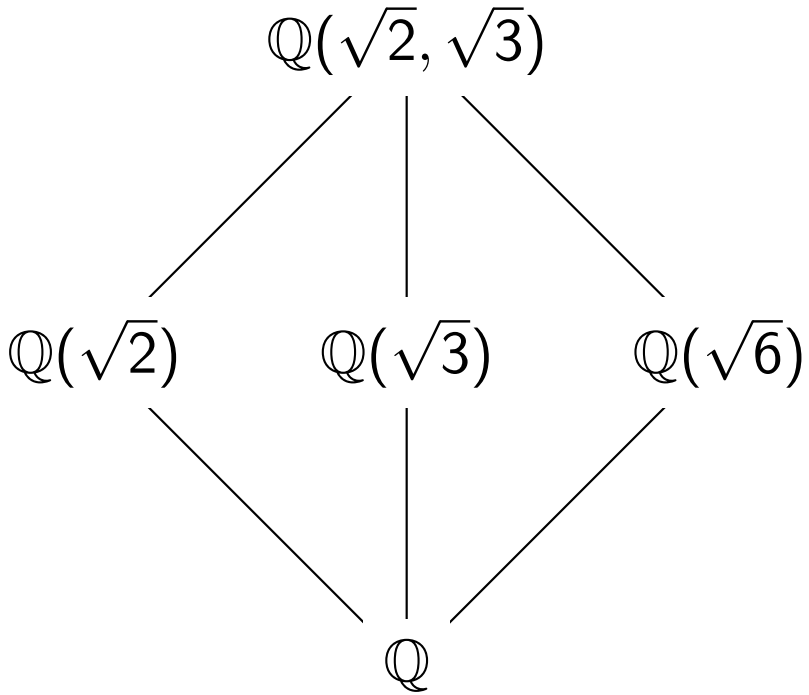
Intermediate Fields

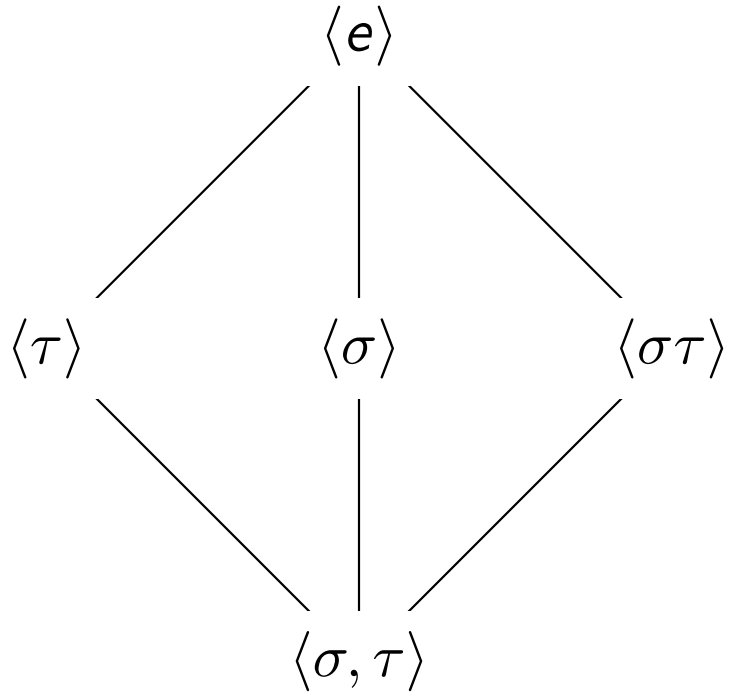
To start, let's look at the Galois extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. Its Galois group has four elements, as each automorphism must send $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. We can define two of these, σ and τ, that generate the rest of the group as follows:

$$\sigma(\sqrt{2}) = -\sqrt{2} \quad \sigma(\sqrt{3}) = \sqrt{3}$$
$$\tau(\sqrt{2}) = \sqrt{2} \quad \tau(\sqrt{3}) = -\sqrt{3}$$

From there, the other two members of the Galois group are e and $\sigma\tau$. In total, there are three intermediate fields between $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}$, those being $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$. It turns out that each of these is generated by a specific member of the full Galois group, and we can show this correspondence in a simple diagram.

Intermediate Fields





The Galois Correspondence

This leads us to the Galois Correspondence, also known as the Fundamental Theorem of Galois Theory.

Theorem (Galois Correspondence)

The Galois Correspondence, also known as the Fundamental Theorem of Galois theory, states that:

1. *There exists a bijection between intermediate fields K between fields L and F, and subgroups of $Gal(L/F)$. This bijection is given by the function $\Phi : K \mapsto Gal(L/K)$, with its inverse being $\Psi : H \mapsto L^H$.*
2. *Ψ and Φ reverse inclusion, so if K_1 and K_2 are intermediate fields so that $K_1 \subseteq K_2$, $\Phi(K_2) \leq \Phi(K_1)$; and if H_1 and H_2 are subgroups of $Gal(L/F)$ and $H_1 \leq H_2$, then $L^{H_2} \subseteq L^{H_1}$.*
3. *For any intermediate field K, $|\Phi(K)| = [L : K]$; if $H \leq Gal(L/K)$, then $|H| = [L : \Psi(H)]$.*

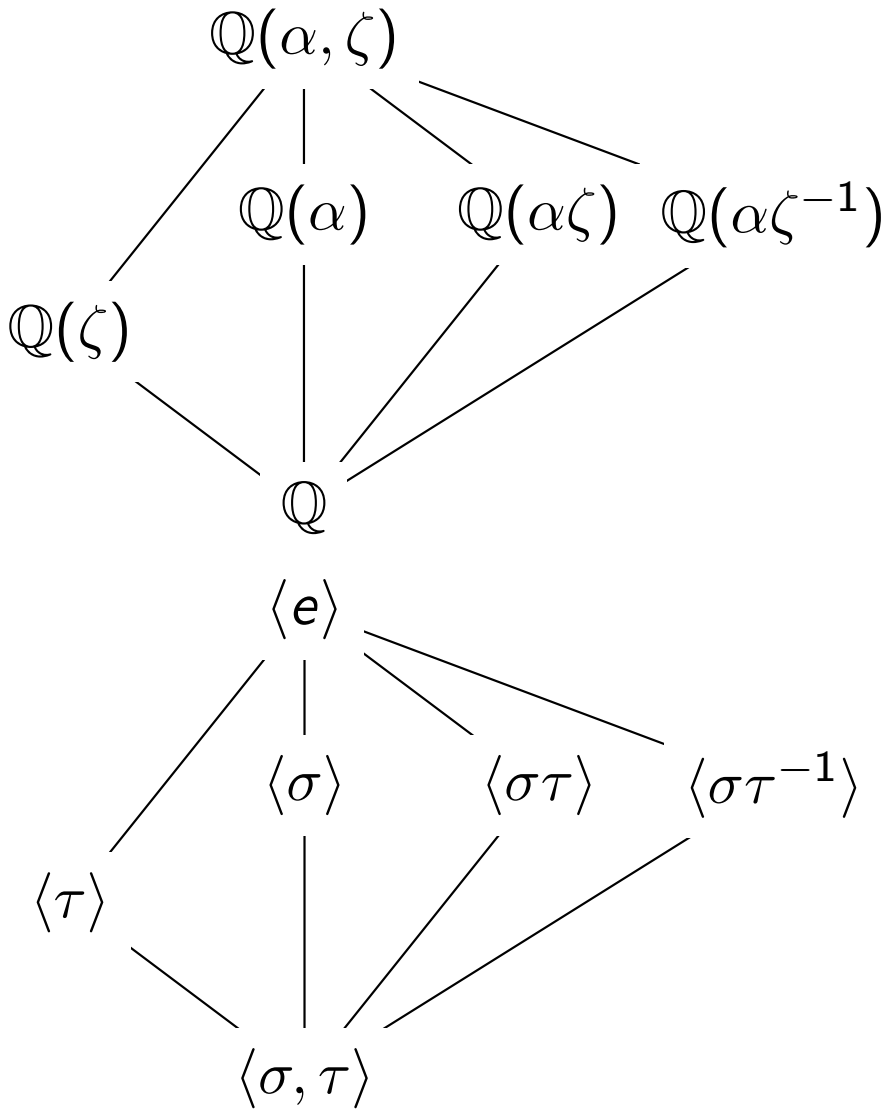
The Galois Correspondence

Let's see what the function Φ does with another example, this time of $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}/\mathbb{Q}$. This is the splitting field of $x^3 - 2$, so it is Galois. We can define $\alpha = \sqrt[3]{2}$ and $\zeta = e^{2\pi i/3}$ for conciseness. Then, out of six total automorphisms, the Galois group is generated by two:

$$\begin{aligned} \sigma(\alpha) &= \alpha \quad & \sigma(\zeta) &= \zeta^{-1} \\ \tau(\alpha) &= \zeta\alpha \quad & \tau(\zeta) &= \zeta. \end{aligned}$$

Since Φ maps intermediate fields between $\mathbb{Q}(\alpha, \zeta)$ and $\mathbb{Q}$ to subgroups of $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q})$, we can create the diagram on the next slide.

The Galois Correspondence



Applications of the Correspondence

Some applications of the Galois Correspondence include:

- A proof of the nonexistence of a quintic (or higher) equation
- Information about the roots of polynomials
- Solvability of groups of polynomials of higher degree