The Galois Correspondence

Logan Gilbert
lagmath13@gmail.com

July 10, 2022

Galois Theory is a field of mathematics related to abstract algebra. Originally started by French mathematician Évariste Galois, it is used to connect group and field theory, as well as study roots of polynomials. The Galois Correspondence, or Fundamental Theorem of Galois Theory, is arguably its most important result.

1 Group Theory

It will help to start by defining some terms from group theory, which will help us understand a Galois group.

Definition 1 (Groups and Fields)**.** *A group is a set G and a binary operation $\cdot$ (typically denoted as $(G,\cdot)$) acting on elements of G. $\cdot$ follows three properties:*

- *There is an element e in G such that for any g in G, $e \cdot g = g \cdot e = g$.*
- *For any $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.*
- *For all $g, h, k \in G$, $g \cdot (h \cdot k) = (g \cdot h) \cdot k$.*

A group G is abelian if $a \cdot b = b \cdot a$, i.e. it is commutative.

A field is similar. It is a set F and two binary operations $+$ and $\cdot$ such that $(F, +)$ is a group, $(F \backslash \{0\}, \cdot)$ is a group, and $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

A typical example of a group would be a symmetry group of a geometric object, such as a tetrahedron the graph K_4. Here, different permutations of vertices form a group over composition. We know that any two permutations will form another permutation; there is an identity element, which is to leave the vertices as they are; and associativity holds for permutations.

An example of a non-abelian group would be the group of nonzero invertible matrices over multiplication. While there is an identity matrix, an inverse for every matrix and associativity of multiplication, matrix multiplication is *not* commutative.

As for fields, an example would be $\mathbb{Q}$. It is a group over addition; $\mathbb{Q}\backslash\{0\}$ is a group over multiplication, and distribution holds.
Interestingly, the intersection of two or more fields will always be another field.

Definition 2 (Homomorphisms and Isomorphisms)**.** *Define two groups,* $(G, \cdot)$ *and* $(G', *)$*. Then a function* $f : G \to G'$ *is a homomorphism if it satisfies*

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

An isomorphism is simply a bijective homomorphism.

Example. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+, \times)$.
Proof. To find an isomorphism f between these two groups, notice that

$$e^{(x+y)} = e^x \times e^y.$$

Then, by letting $f(x) = e^x$, we have that

$$f(x+y) = e^{x+y} = e^x \times e^y = f(x) \times f(y).$$

Since $f(x) = e^x$ is a bijective function, $f(x)$ is an isomorphism, so $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+, \times)$.

Automorphisms, a subclass of isomorphisms, are notable for this paper:

Definition 3 (Automorphism)**.** *An automorphism is any function* $f : G \to G$ *that maps a group to itself. This includes the identity function, but there are nontrivial examples as well.*

The set of all automorphisms, which is a group itself, is called $Aut(K)$.
One example of a nontrivial automorphism would be $f(g) = 2 \cdot g$ on $(\mathbb{Z}, \cdot)$, where $\cdot$ is standard multiplication.
From an automorphism, the concept of a fixed field follows naturally.

Definition 4 (Fixed Field)**.** *Given a field* K *and an automorphism* $\sigma \in Aut(K)$*, the elements of* K *that are fixed by* σ*, i.e.* $\sigma(x) = x$*, forms a field. With a set of automorphisms* S*, then the field of all elements fixed by all members of* S *is called the fixed field of* S*, and it is denoted* K^S*.*

Definition 5 (Field Extentions)**.** *A field extension, typically denoted* K/F *or* $F(\alpha)$*, is the smallest possible field containing the elements and operations of* F*, as well as* α*. There are also instances where more* α *are needed; this is denoted* $F(\alpha_1, \alpha_2, \ldots)$*.*

An example of a field extension would be $\mathbb{Q}(\sqrt{2})$. This field contains $\mathbb{Q}$, but must also contain $\sqrt{2}$; adding this extra element also implies that all $a + b\sqrt{2}$ must be in the field as well.

We should also define fixed fields here, as they will be useful later.

Definition 6 (Vector Space). *For any field F, a vector space over F is defined to be any abelian group V, with binary operation $\cdot : F \times V \to V$, or scalar multiplication, such that for all $a, b \in F$ and $v, w \in V$,*

- $0_F \cdot v = 0_V$*, where* 0_F *and* 0_V *are 0 in* F *and* V *respectively;*
- $1v = v$*;*
- $a \cdot (v + w) = av + aw$*;*
- $(ab)v = a(bv)$*;*
- $(a + b)v = av + bv$*.*

Given a vector space V over a field K, we call the smallest linearly independent collection of elements $v_k \subseteq V$ a basis of V; we then define the *dimension* of V, or $dim_F(V)$, to be $|v_k|$. Interestingly, no matter what basis is chosen, $dim_F(V)$ remains constant, and is a notable invariant of a vector field.

In many ways, field extensions are similar to vector spaces, and the axioms for a vector space are satisfied by field extensions. As such, we define $[K : F]$ to be the dimension of a field extension in much the same way as we do a vector field.

2 Galois Theory

Definition 7 (Splitting Fields). *Given a field F and a nonzero irreducible polynomial $f(x)$ with coefficients in F and roots $\{\alpha_k\}$, we say that an extension L/F is a splitting field for $f(x)$ if $\{\alpha_k\} \subseteq L$, but $\{\alpha_k\}$ do not lie in any smaller extension of F. In other words, the splitting field for $f(x)$ is $F(\alpha_1, \alpha_2, \ldots)$*

For example, the splitting field for $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$.

Definition 8 (Galois Extentions and Groups). *A Galois Extension is a field extension E/F in which*

- *E/F is normal, i.e. every irreducible polynomial over F with a root in E splits into linear factors in E*
- *E/F is separable, i.e. for every $\alpha \in E$, the minimal polynomial of α over F has no repeated roots in any extension field.*

If an extension K/F is Galois, Gal(K/F) is the same as $Aut(K/F)$, and we call it the Galois Group of K/F.

Alternatively, any Galois extension of a field F must fix all of the elements in F, and $|Aut(K/F)| = [K : F]$ if the field extension is finite.

Example. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois Extension.
Proof. For $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ to be a Galois Extension of $\mathbb{Q}$, it must be normal and separable. For it to be separable, we need only look at the minimal polynomial of $\sqrt{2}$, as the minimal polynomial of any $a \in \mathbb{Q}$ is trivial. This minimal polynomial, $x^2 - 2$, is $(x - \sqrt{2})(x + \sqrt{2})$, which has no repeated roots; hence, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable. For it to be normal, we need to show that any irreducible polynomial with a root in $\mathbb{Q}(\sqrt{2})$ factors linearly. For most polynomials, this is trivial, as they factor linearly in $\mathbb{Q}$, so they must also in $\mathbb{Q}(\sqrt{2})$. The only exceptions are those that reduce to $x^2 - 2$; this factors linearly, as shown above, so $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal. Hence, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension. ■

To find the Galois group of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, we need to find the automorphism group of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Since $\mathbb{Q}$ must remain fixed, we need only show where each automorphism sends $\sqrt{2}$. Since the roots of the minimal polynomial $x^2 - 2$ are $\sqrt{2}, -\sqrt{2}$, we are left with two automorphisms, σ_0 and σ_1.

$$\sigma_0(\sqrt{2}) = \sqrt{2}$$
$$\sigma_1(\sqrt{2}) = -\sqrt{2}.$$

Example. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is a Galois extension.
Proof. To show that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is a Galois extension, we need to show that it is normal and separable.
As with the previous example, we need only look at irreducible polynomials with roots in $\mathbb{Q}(\sqrt[4]{2})$ and minimal polynomials of elements only in $\mathbb{Q}(\sqrt[4]{2})$ and not $\mathbb{Q}(\sqrt{2})$; this means we need only look at $\pm\sqrt[4]{2}$.
The minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - \sqrt{2}$, which factors into $(x - \sqrt[4]{2})(x + \sqrt[4]{2})$. Since there are no repeated roots and it factors linearly, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is both a normal and separable extension; hence, it is Galois.

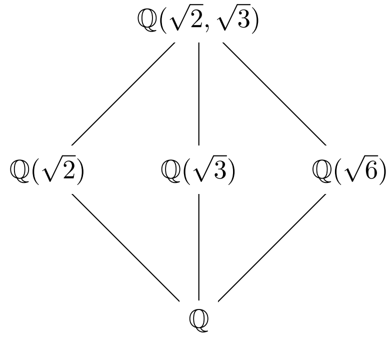
3 The Galois Correspondence

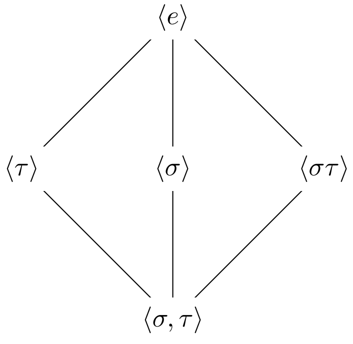
Before getting to the Galois correspondence, let's start with a helpful example.
Example. Consider the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. In between $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}$, there are three intermediate fields: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$. For each of these subfields K, we can consider $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/K)$. This is a subgroup of the full Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, as some elements of the full Galois group must also fix every element of K.
Let us give names to the automorphisms the full Galois group. As each one must send $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$, there are four possible automorphisms in the group. We can choose

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

Then, the other two elements of the Galois group are the identity automorphism, e, and $\sigma\tau$, which sends $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$. Next, we can work out $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/K)$, which we can call Γ_K, in terms of σ and τ.

Obviously, e is present in all of these subgroups. If $K = \mathbb{Q}(\sqrt{2})$, then $\tau \in \Gamma_K$; if $K = \mathbb{Q}(\sqrt{3})$, then $\sigma \in \Gamma_K$; and if $K = \mathbb{Q}(\sqrt{6})$, then $\sigma\tau \in \Gamma_K$. For conciseness, we can call the subgroup generated by an element γ $\langle\gamma\rangle$.





For each field K in the left diagram, we have the subgroup $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/K)$, which is kept track of in the right diagram.
Interestingly, if we start with any intermediate field K, then look at its Galois group Γ_K, and find the fixed field $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\Gamma_K}$, we are left with K; this can also be done the opposite direction, where if we start with any subgroup $H \leq \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, take its fixed field, and find the Galois group of the resulting field, we are left with H.

Theorem 1 (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 $\text{Gal}(L/F)$. 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 $\text{Gal}(L/F)$ 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 $H \leq \text{Gal}(L/K)$, then $|H| = [L : \Psi(H)]$.

Proof. We'll start with the proof of statement (3).
(3) Earlier, we said that for any L/K to be Galois, $[L : K] = |Aut(L/K)|$. As for the second part, we know that $H \leq \text{Gal}(L/K)$ fixes L^H, so $H \leq \text{Gal}(L/L^H)$, or $H \leq [L : \Psi(H)]$. To prove equality, we must now prove that $H \geq [L : \Psi(H)]$. It turns out that we can always find $\alpha \in L$ such that $L = L^H(\alpha)$ for a finite Galois extension.
Consider the polynomial

$$h(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

For any $\tau \in H$, the coefficients of $h(x)$ are fixed by τ, as τ simply permutes the order of factors in the product for $h(x)$. Hence, the coefficients of $h(x)$ lie in L^H. Thus, if $p(x)$ is the minimal polynomial of α, $p(x)|h(x)$, so

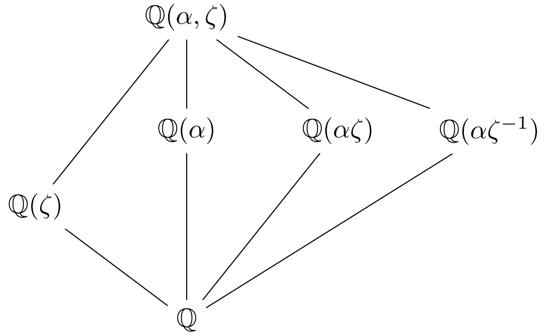
$$|H| = \deg(h) \geq \deg(p) = [L^H(\alpha) : L^H] = [L : L^H].$$

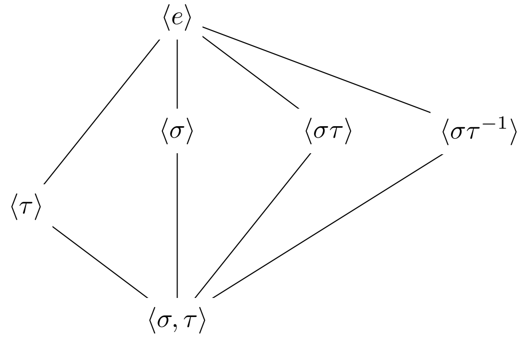
Hence, $|H| \geq [L : L^H]$, so $|H| = [L : L^H] = [L : \Psi(H)]$.
(1) Starting with an intermediate field K, let's look at $L^{\mathrm{Gal}(L/K)}$. $\mathrm{Gal}(L/K)$ is the subgroup of $\mathrm{Gal}(L/F)$ that fixes K, so by definition $L^{\mathrm{Gal}(L/K)}$ *must* contain K, so $K \subseteq L^{\mathrm{Gal}(L/K)}$. By part (3), this means that $[L : L^{\mathrm{Gal}(L/K)}] = |\mathrm{Gal}(L/K)| = [L : K]$. Hence, $L^{\mathrm{Gal}(L/K)} = K$.
As for the other direction, we start with $H \leq \mathrm{Gal}(L/F)$, and look at $\mathrm{Gal}(L/L^H)$. By part (3), $|\mathrm{Gal}(L/L^H)| = [L : L^H] = |H|$, so $H = \mathrm{Gal}(L/L^H)$.
(2) Suppose that $L/K_2/K_1/F$ is a tower of fields, and that $\sigma \in \Phi(K_2) = \mathrm{Gal}(L/K_2)$. This means that σ fixes every element of K_2, and since $K_1 \subseteq K_2$, it fixes K_1 as well, so $\sigma \in \Phi(K_1) = \mathrm{Gal}(L/K_1)$. Thus, $\Phi(K_1) \leq \Phi(K_2)$.
Now suppose that $H_1 \leq H_2 \leq \mathrm{Gal}(L/F)$. Suppose that $\alpha \in L^{H_2}$, so α is fixed by every element of H_2. Then $\alpha \in L^{H_1}$, so $L^{H_1} \subseteq L^{H_2}$. □

Example. Consider the splitting field of $x^3 - 2$, $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}/\mathbb{Q}$. As each automorphism fixes $\mathbb{Q}$, we need only look at where each root is sent, which gives six automorphisms. Let us write $\alpha = \sqrt[3]{2}$ and $\zeta = e^{2\pi i/3}$, for conciseness. The Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q})$ is generated by two elements, σ and τ where

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

From the Galois Correspondence, we know that there must exist a bijection Φ mapping intermediate fields between $\mathbb{Q}(\alpha, \zeta)$ and $\mathbb{Q}$ to subgroups of $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q})$; this is shown in the diagram below.


$\mathbb{Q}(\alpha, \zeta)$
$\mathbb{Q}(\alpha)$
$\mathbb{Q}(\alpha\zeta)$
$\mathbb{Q}(\alpha\zeta^{-1})$
$\mathbb{Q}(\zeta)$
$\mathbb{Q}$


$\langle e \rangle$
$\langle \sigma \rangle$
$\langle \sigma\tau \rangle$
$\langle \sigma\tau^{-1} \rangle$
$\langle \tau \rangle$
$\langle \sigma, \tau \rangle$

References

[1] Emil Artin. *Galois Theory.* Courier Corporation, 2012.

[2] David A. Cox. *Galois Theory.* John Wiley & Sons, 2012.

[3] Joseph Rotman. *Galois Theory.* Springer New York, 2012.