

3 Galois Theory

3.1 Definitions and Examples

This section of notes roughly follows Section 14.1 in Dummit and Foote.

Let F be a field and let $f(x) \in F[x]$. In the previous chapter, we proved that there always exists a finite extension K of F that contains the roots of $f(x)$. The big idea of Galois Theory (named after Évariste Galois, 1811–1832) is to consider the relationship between the group of permutations of the roots of $f(x)$ and the algebraic structure of its splitting field. The explicit connection is given by the Fundamental Theorem of Galois Theory, which we will prove in the next section.

In this section, we introduce all of the necessary terminology.

Definition 3.1. Let K be a field. The collection of all automorphisms of K is denoted $\text{Aut}(K)$. An automorphism $\sigma \in \text{Aut}(K)$ is said to **fix** $\alpha \in K$ if $\sigma(\alpha) = \alpha$. If $S \subseteq K$, then σ is said to **fix** S if it fixes all the elements of S (i.e., $\sigma(\alpha) = \alpha$ for all $\alpha \in S$).

Note that $\text{Aut}(K) \neq \emptyset$ since the identity map is an automorphism, called the **trivial automorphism**.

Recall that the prime subfield of K is generated by 1. Moreover, every $\sigma \in \text{Aut}(K)$ satisfies $\sigma(0) = 0$ and $\sigma(1) = 1$. It follows that σ fixes the prime subfield of K . In particular, $\text{Aut}(\mathbb{Q})$ and $\text{Aut}(\mathbb{Z}_p)$ only contain the trivial automorphism.

Definition 3.2. Let K/F be an extension of fields and let $\text{Aut}(K/F)$ be the collection of automorphisms of K that fix F .

Note that if F is the prime subfield of K , then $\text{Aut}(K/F) = \text{Aut}(K)$ since every automorphism of K fixes its prime subfield.

Theorem 3.3. For every field K , the set $\text{Aut}(K)$ is a group under function composition. If K/F is an extension of fields, then $\text{Aut}(K/F)$ is a subgroup of $\text{Aut}(K)$.

Theorem 3.4. Let K/F be an extension of fields and let $\alpha \in K$ be algebraic over F . Then for any $\sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ is a root of the minimal polynomial for α over F (i.e., $\text{Aut}(K/F)$ permutes the roots of irreducible polynomials). Equivalently, any polynomial with coefficients in F having α as a root has $\sigma(\alpha)$ as a root.

Example 3.5. Here are two examples.

- (1) Consider $\mathbb{Q}(\sqrt{2})$. If $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\sigma(\sqrt{2})$ is either $\sqrt{2}$ or $-\sqrt{2}$ since these are the only two roots of the minimal polynomial for $\sqrt{2}$. It follows that for $a, b \in \mathbb{Q}$, $\sigma(a+b\sqrt{2})$ is equal to either $a+b\sqrt{2}$ or $a-b\sqrt{2}$ (since σ fixes \mathbb{Q}). The map determined by $\sqrt{2} \mapsto \sqrt{2}$ is the identity automorphism. The map determined by $\sqrt{2} \mapsto -\sqrt{2}$ is the only other map in $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. This implies that $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is a cyclic group of order 2.

- (2) Now, consider $K = \mathbb{Q}(\sqrt[3]{2})$. Let $\tau \in \text{Aut}(K/\mathbb{Q})$. Then τ is completely determined by its action on $\sqrt[3]{2}$:

$$\tau(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\tau(\sqrt[3]{2}) + c\tau(\sqrt[3]{2})^2.$$

Recall that the other two roots of $x^3 - 2$ are not elements of K . However, $\tau(\sqrt[3]{2}) \in K$ and must be a root of $x^3 - 2$. It follows that $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore, τ must be the identity map, and so $\text{Aut}(K/\mathbb{Q})$ is the trivial group.

In general, if K is generated over F by some collection of elements, then any automorphism $\sigma \in \text{Aut}(K/F)$ is uniquely determined by what it does to the generators. If K/F is finite, then K is finitely generated over F by algebraic elements, so by the previous theorem, the number of automorphisms of K that fix F is finite. That is, $\text{Aut}(K/F)$ is a finite group. In particular, the automorphisms of a finite extension can be considered as permutations of the roots of a finite number of equations, but not every permutation of the roots gives rise to an automorphism (as in the previous example).

We can also associate to each group of automorphisms a field extension.

Theorem 3.6. Let $H \leq \text{Aut}(K)$, where K is a field. Then the collection F of elements of K fixed by all the elements of H is a subfield of K .

Remark 3.7. In the previous theorem, H need not be a subgroup.

Definition 3.8. If $H \leq \text{Aut}(K)$, then the subfield fixed by H is called the **fixed field** of H .

Theorem 3.9. The association of groups to fields and fields to groups defined above is inclusion reversing, namely

- (1) If $F_1 \subseteq F_2 \subseteq K$ are two subfields of K , then $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$, and
- (2) If $H_1 \leq H_2 \leq \text{Aut}(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2 , respectively, then $F_2 \subseteq F_1$.

Example 3.10. Let's return to the previous examples.

- (1) The fixed field of $\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is just \mathbb{Q} .
- (2) Since $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group, every element of $\mathbb{Q}(\sqrt[3]{2})$ is fixed by $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, and so the fixed field of $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$.

Here's the current summary of the big picture. Given a subfield F of K , the associated group is the collection of automorphisms of K that fix F . On the other hand, given a group of automorphisms of K , the associated extension is defined by taking F to be the fixed field of the automorphisms.

In Example 3.5(1), starting with the subfield \mathbb{Q} of $\mathbb{Q}(\sqrt{2})$ one obtains the group $\{1, \sigma\}$ (where $\sigma : \sqrt{2} \mapsto -\sqrt{2}$) and starting with the group $\{1, \sigma\}$ one obtains the subfield \mathbb{Q} . In this case, we get a “duality” between the two concepts.

In Example 3.5(2), starting with the subfield \mathbb{Q} of $\mathbb{Q}(\sqrt[3]{2})$, we only get the trivial group. Starting with the trivial group, we can't “drop down” from $\mathbb{Q}(\sqrt[3]{2})$ to obtain \mathbb{Q} . The shortcoming in this example is that there are not enough automorphisms to force the fixed field to be \mathbb{Q} .

The next theorem provides us with a bound on the size of the automorphism groups associated to a splitting field of a single polynomial.

Theorem 3.11. Let E be the splitting field of the polynomial $f(x) \in F[x]$. Then

$$|\text{Aut}(K/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F .

More generally, it is true that $|\text{Aut}(K/F)| \leq [E : F]$ for any finite extension. We will prove this later.

Definition 3.12. Let K/F be a finite extension. Then K is said to be **Galois** over F and K/F is called a **Galois extension** if $|\text{Aut}(K/F)| = [K : F]$. If K/F is Galois, $\text{Aut}(K/F)$ is called the **Galois group** of K/F , denoted $\text{Gal}(K/F)$.

The next result follows immediately from Theorem 3.11 and the definition of Galois extension. In the next section, we will see that the converse is also true.

Corollary 3.13. If K is the splitting field over F of a separable polynomial $f(x)$, then K/F is Galois.

Note that the splitting field of any polynomial $f(x)$ is the same as the splitting field of the product of irreducible factors of $f(x)$ (i.e., remove any repeated factors of $f(x)$). The latter polynomial is separable by Corollary 2.70. Corollary 3.13 implies that the splitting field of any polynomial over \mathbb{Q} is Galois.

Definition 3.14. If $f(x)$ is a separable polynomial over F , then the **Galois group of $f(x)$ over F** is the Galois group of the splitting field of $f(x)$ over F .

Example 3.15. Let's play with a few examples.

- (1) Previous calculations showed us that $|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Thus, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension. In this case, the Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is isomorphic to \mathbb{Z}_2 . Moreover, the Galois group of the separable polynomial $f(x) = x^2 - 2$ is $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.
- (2) Any quadratic extension K of any field F of characteristic different from 2 is Galois.
- (3) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since its group of automorphisms does not have order equal to $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
- (4) Let's tinker with $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, where $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$.
- (5) Let's play the same game with the splitting field of $x^3 - 2$ over \mathbb{Q} .
- (6) As in (3), the field $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over \mathbb{Q} since any automorphism is determined by where it sends $\sqrt[4]{2}$ and of the four possibilities $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, only two are in the field $\mathbb{Q}(\sqrt[4]{2})$ (the two real roots). Note that the degree 2 extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are both Galois extensions (since both are quadratic extensions; see (2)). This shows that a Galois extension of a Galois extension need not be Galois.