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 $\mathrm{Aut}(K)$. An automorphism $\sigma \in \mathrm{Aut}(K)$ 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 $\mathrm{Aut}(K) \neq \emptyset$ since the identity map is an automorphism, called the **trivial automorphism**.

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

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

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

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

Theorem 3.4. Let K/F be an extension of fields and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is a root of the minimal polynomial for α over F (i.e., $\mathrm{Aut}(K/F)$ 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 $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, 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 $a, \in \mathbb{Q}, \sigma(a+b\sqrt{2})$ 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 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. This implies that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is a cyclic group of order. 2

(2) Now, consider $K = \mathbb{Q}(\sqrt[3]{2})$. Let $\tau \in \mathrm{Aut}(K/\mathbb{Q})$. 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 $\mathrm{Aut}(K/\mathbb{Q})$ is the trivial group.

In general, if K is generated over F by some collection of elements, then any automorphism $\sigma \in \mathrm{Aut}(K/F)$ 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, $\mathrm{Aut}(K/F)$ 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 $H \leq \mathrm{Aut}(K)$, 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 $H \leq \mathrm{Aut}(K)$, 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 $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$, and

(2) If $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ 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 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is just $\mathbb{Q}$.

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

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

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

More generally, it is true that $|\mathrm{Aut}(K/F)| \leq [E : F]$ 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 $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, $\mathrm{Aut}(K/F)$ is called the **Galois group** of K/F, denoted $\mathrm{Gal}(K/F)$.

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 $|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Thus, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension. In this case, the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2$. Moreover, the Galois group of the separable polynomial $f(x) = x^2 - 2$ is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

(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.

3.2 The Fundamental Theorem of Galois Theory

This section of notes roughly follows Section 14.2 in Dummit and Foote.

In the examples we've looked at so far, every time we've had a Galois extension, there was a nice 1-1 correspondence between the subgroups of the Galois group and the lattice of fixed subfields of the extension. Moreover, the correspondence has been inclusion reversing. It turns out that we always have this correspondence whenever we have a Galois extension. This is exactly the content of the Fundamental Theorem of Galois Theory. In order to prove this amazing theorem, we need to develop some more tools.

Definition 3.16. A (linear) **character** χ of a group G with values in the field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^\times.$$

That is, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g) \neq 0$ for all $g \in G$. A collection of characters $\chi_1, \ldots, \chi_n$ of G are said to be **linearly independent** over L if they are linearly independent as functions on G, i.e., if there is no nontrivial relation

$$a_1\chi_1 + \cdots + a_n\chi_n = 0$$

with $a_1, \ldots, a_n \in L$ not all 0 as a function on G.

Theorem 3.17. If $\chi_1, \ldots, \chi_n$ are distinct characters of G with values in L, then they are linearly independent over L.

Consider an injective homomorphism σ of a field K into a field L, called an **embedding** of K into L. Then σ is an injective group homomorphism from $G = K^\times$ into $L^\times$, and so σ is a character of $G = K^\times$ with values in $L^\times$. Since we know that $\sigma(0) = 0$, σ viewed as a character contains all of the information about σ as an injective field homomorphism on K.

Corollary 3.18. If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular, distinct automorphisms of K are linearly independent as functions on K.

Theorem 3.19. Let K be a field, $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\} \leq \mathrm{Aut}(K)$, and F be the field fixed by G. Then

$$[K : F] = n = |G|.$$

Recall that Theorem 3.11 tells us that if K is the splitting field over F of the polynomial $f(x) \in F[x]$, then $|\mathrm{Aut}(K/F)|$ is bounded by $[K : F]$ (with equality if $f(x)$ is separable). The next result tells us that we have the same bound for any finite extension K/F.

Corollary 3.20. Let K/F be any finite extension. Then

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

with equality iff F is the fixed field of $\mathrm{Aut}(K/F)$. That is, K/F is Galois iff F is the fixed field of $\mathrm{Aut}(K/F)$.

Corollary 3.21. Let G be a finite subgroup of automorphisms of a field K and let F be the corresponding fixed field. Then every automorphism of K fixing F is contained in G, i.e., $\mathrm{Aut}(K/F) = G$, so that K/F is Galois with Galois group G.

Corollary 3.22. If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K, then their fixed fields are also distinct.

By the corollaries above, we see that taking the fixed fields for distinct finite subgroups of $\mathrm{Aut}(K)$ gives distinct subfields of K over which K is Galois. Moreover, the degrees of the extensions are given by the orders of the subgroups. A portion of the Fundamental Theorem of Galois Theory states that these are all of the subfields of K.

The next theorem provides the converse for Theorem 3.11.

Theorem 3.23. The extension K/F is Galois iff K is the splitting field of a separable polynomial over F. Furthermore, if this is the case, then every irreducible polynomial in $F[x]$ that has a root in K is separable and has all of its roots in K (so in particular, K/F is a separable extension).

Definition 3.24. Let K/F be a Galois extension. If $\alpha \in K$, the elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the **conjugates** (or **Galois conjugates** of $\alpha \in K$. If E is a subfield of K containing F, the field $\sigma(E)$ is called the **conjugate field** of E over F.

The proof of Theorem 3.23 shows us that in a Galois extension K/F, the other roots of the minimal polynomial over F of any element $\alpha \in K$ are precisely the conjugates of α under the Galois group of K/F.

The second statement in Theorem 3.23 tells us that K is not Galois over F if we can find an irreducible polynomial in $F[x]$ having a root in K but not all of its roots in K. Loosely speaking, Galois extensions are extensions with just enough distinct roots of irreducible polynomials.

For convenience, let's put all of our characterizations of Galois extensions K/F in one place.

(1) Fields with $[K : F] = |\mathrm{Aut}(K/F)|$ (Definition 3.12)

(2) Splitting fields of separable polynomials over F (Corollary 3.13/Theorem 3.23)

(3) Fields where F is precisely the set of elements fixed by $\mathrm{Aut}(K/F)$ (Corollary 3.20)

(4) Finite, normal, and separable extensions (Theorem 3.23)

We are finally ready to tackle the Fundamental Theorem of Galois Theory.

Theorem 3.25 (Fundamental Theorem of Galois Theory)**.** Let K/F be a Galois extension. Then there is a bijection

$$\{\text{subfields } E \text{ of } K \text{ containing } F\} \leftrightarrow \{\text{subgroups } H \text{ of } \mathrm{Gal}(K/F)\}$$

Given by the correspondences

$$E \mapsto \{\text{the elements of } G \text{ fixing } E\}$$
$$\{\text{the fixed field of } H\} \mapsto H$$

which are inverses of each other. Under this correspondence, we have the following:

(1) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ iff $H_2 \leq H_1$

(2) $[K : E] = |H|$ and $[E : F] = [\mathrm{Gal}(K/F) : H]$.

(3) K/E is always Galois with Galois group $\mathrm{Gal}(K/E) = H$.

(4) E is Galois over F iff H is a normal subgroup in $\mathrm{Gal}(K/F)$. If this is the case, then the Galois group is isomorphic to the quotient group:

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/H$$

More generally, even if H is not necessarily normal in $\mathrm{Gal}(K/F)$, the isomorphisms of E (into a fixed algebraic closure of F containing K) that fix F are in one-to-one correspondence with the cosets $\{\sigma(H)\}$ of H in $\mathrm{Gal}(K/F)$.

(5) If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ and the composite subfield E_1E_2 corresponds to $H_1 \cap H_2$. Hence the lattice of subfields of K containing F and the lattice of subgroups of $\mathrm{Gal}(K/F)$ are dual.

Example 3.26. We conclude this section by tinkering with three examples.

(1) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

(2) $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

(3) Splitting field of $x^8 - 2$ over $\mathbb{Q}$