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 which 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 $\sigma(a + b\sqrt{2})$ 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) 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 $\mathbb{Q}(\sqrt[3]{2})$.

More coming soon...