Legend: Everything in *green* is from the Bergman's Companion to Lang's Algebra.

In this chapter we will study the core of Galois theory, the group of automorphisms of a finite (and sometimes infinite) Galois extension at length.

1 Galois extensions

Definition 1.1. Let K be a field and let G be a group of automorphisms of K. We let

$$K^G = \{x \in K \mid x^\sigma = x \text{ for all } \sigma \in G\}$$

We call this the **fixed field** of G.

Definition 1.2. An algebraic extension K of a field k is called **Galois** if it is normal and seperable.

The group of automorphisms of K over k is called the **Galois group** of K over k, and is denoted $G(K/k)$, $G_{K/k}$, $\mathrm{Gal}(K/k)$ or simply G.

This is the main theorem of the Galois theory or finite Galois extensions.

Theorem 1. *Let K be a finite Galois extension of k, with Galois group G. There is a bijection between the set of subfields E of K, containing K and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the map $\sigma \to \sigma|_E$ induces an isomorphism of G/H onto the Galois group of E over k.*

Theorem 2. *Let K be a Galois extension of k. Let G be its Galois group. Then $k = K^G$. If F is an intermediate field, $k \subseteq F \subseteq K$, then K is Galois over F. The map*

$$F \to Gal(K/F)$$

from the set of intermediate fields into the set of subgroups of G is injective.

Proof. Let $\alpha \in K^G$. Let σ be any embedding of $k(\alpha)$ in K^a, inducing the identity on k. Extend σ to an embedding of K into K^a, we also call this extension σ. Note since K is normal, σ is an automorphisms of K over k it is an element of G. Since $\alpha \in K^G$, σ leaves α fixed. Therefore there is actually only one extension of σ to an embedding of K in K^a (the identity). So:

$$[k(\alpha) \colon k]_s = 1$$

Since α is seperable over k, $[k(\alpha) \colon k] = [k(\alpha) \colon k]_s = 1$, so $\alpha \in k$. This proves the first assertion.

Let F be an intermediate field. Then K is normal and seperable over F by previous theorems from chapter five. Hence K is Galois over F. If $H = \mathrm{Gal}(K/F)$ then by what we have proved above we conclude that $F = K^H$. Now we will show that the map defined in our statement is injective. Let F, F' be intermediate fields such that $F \to \mathrm{Gal} K/F = H$ and $F' \to \mathrm{Gal} K/F' = H'$.

Assume that $H = H'$, then:

$$F = K^H = K^{H'} = F'$$

□

Definition 1.3. We shall call the group $\mathrm{Gal}(K/F)$ of an intermediate field the group **associated** with F. We say that a subgroup H of G **belongs** to an intermediate field F if $H = \mathrm{Gal}(K/F)$

Bergman 1. *Note this does not mean that H is the Galois group of F. For example the Galois group of the whole extension K is $Gal(K/F)$, $\{1\}$ is the subgroup belonging to K, since $\{1\} = Gal(K/K)$.*

Corollary 2.1. *Let K/k be Galois with group G. Let F, F' be two intermediate fields, and let H, H' be the subgroups of G belonging to F, F' respectively. Then $H \cap H'$ belongs to FF'.*

Proof. Note every element of $H \cap H'$ leaves FF' fixed (basically from how FF' is constructed), and every element of G which also leaves FF' fixed also leaves F and F' fixed so lies in $H \cap H'$. □

Corollary 2.2. *The fixed field of the smallest subgroup of G containing H and H' is $F \cap F'$.*

Proof. Let E be the smallest subgroup of G containing H and H'. Note this means that $E = \langle H \cup H' \rangle$.

Let $x \in K^E$. This means that

$$\sigma(x) = x \text{ for all } \sigma \in E$$

Since $H, H' \subseteq E$ we see that $x \in K^H = F$ and $x \in K^{H'} = F'$. So $x \in F \cap F'$. On the other hand, if $x \in F \cap F'$, then for $\sigma \in E$ we have $\sigma = \tau_1 \cdots \tau_n$, where $\tau_i \in H \cup H'$.

So

$$\sigma(x) = \tau_1 \circ \cdots \circ \tau_{n-1} \circ \tau_n(x) = \tau_1 \circ \cdots \circ \tau_{n-1}(x) = x$$

Since $\tau_i(x) = x$ for all i,

Therefore we indeed see that $F \cap F' = K^E$.

$\square$