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

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

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

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

Corollary 2.3. *$F \subseteq F'$ if and only if $H' \subseteq H$*

Proof. If $F \subseteq F'$ and $\sigma \in H'$ leaves F' fixed, then σ leaves F fixed, so $\sigma \in H$. So $H' \subseteq H$.

Conversely if $H' \subseteq H$, then $F = K^H \subseteq K^{H'} = F'$. □

Corollary 2.4. *Let E be a finite seperable extension of a field k. Let K be the smallest normal extension of k containing E. Then K is finite Galois over k. There is only a finite number of intermediate fields F such that $k \subseteq F \subseteq E$.*

Proof. Note K is the compositum of a the finite number of conjugates of E, i.e

$$K = (\sigma_1 E) \cdots (\sigma_n E) \text{ where } \sigma_i \text{ are the distinct embeddings of } E \text{ into } E^a$$

Therefore it is normal(by definition), seperable(since E is) and it is finite over k.

The Galois group K/k has only a finite number of subgroups. So there is only a finite number of subfields of K containing k, so a finite number of subfields of E containing k. □

Lemma 3. *Let E be an algebraic seperable extension of k. Assume that there is an integer $n \geq 1$ such that every element $\alpha \in E$ is of degree $\leq n$ over k. Then E is finite over k and $[E\colon k] \leq n$.*

Proof. Let $\alpha \in E$ be such that $m = [k(\alpha)\colon k] \leq n$ is maximal. Assume that, there exists $\beta \in E \setminus k(\alpha)$, then since $k(\alpha, \beta)$ is seperable and finite over k by the primitive element theorem there is a $\gamma \in k(\alpha, \beta) \subseteq E$ such that:

$$[k(\gamma)\colon k] = [k(\alpha, \beta)\colon k] > m$$

Which contradicts our assumption that α had maximal degree in E. Therefore $E \setminus k(\alpha) = \emptyset \Rightarrow E = k(\alpha)$,

So it is finite over k and $[E\colon k] \leq n$. □

Theorem 4. ***Artin*** *Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k, and its Galois group is G. We have $[K\colon k] = n$,*

Proof. Let $\alpha \in K$ and let $\sigma_1, \ldots, \sigma_r$ be a maximal set of elements of G such that $\sigma_1\alpha, \ldots, \sigma_r\alpha$ are distinct. If $\tau \in G$ then for all i, there is a $\xi \in S_r$ such that

$$\tau\sigma_i\alpha = \sigma_{\xi(i)}\alpha$$

Indeed $\tau\sigma_i\alpha \in \{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$, by maximality. And since τ is injective, $\tau\sigma_i\alpha = \tau\sigma_j\alpha \iff \sigma_i\alpha = \sigma_j\alpha$.

So not only is α the root of a polynomial

$$f(X) = \prod_{i=1}^{r}(X - \sigma_i\alpha) \text{ and } \forall\tau \in G,\ f^\tau = f$$

So the coefficients of f are in $K^G = k$. Furthermore, f is seperable since all the $\sigma_i\alpha$ are distinct. So every element $\alpha \in K$ is the root of a seperable polynomial of degree $\leq n$ with coeffs in k. We also see that this polynomial splits into linear factors in K, so K is seperable and normal (hence Galois) over k.

By lemma 3 we see that $[K\colon k] \leq n$. But recall from chapter 5, the Galois group of K over k has order $\leq [K\colon k]$. Since $G \subseteq \mathrm{Gal}(K/k)$, but $n = |G| \leq |\mathrm{Gal}(K/k)| \leq [K\colon k] \leq n$, we see that $G = \mathrm{Gal}(K/k)$, and $[K\colon k] = n$. □

Index