THE GALOIS GROUP OF $K \subseteq L$ WHEN K IS INFINITE

ARNAB SAHA

Let $K \subseteq L$ be a finite extension and assume that K is infinite. Then there exists a minimal set of generators $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$. Let $f_i \in K[x]$ be the minimal polynomials for each α_i respectively.

Claim. We can choose α_i such that $f_i \neq f_j$ when $i \neq j$.

Proof. We will prove by induction on n. Clearly it is true for $n = 1$. Assume true for $n-1$. Consider $K(\alpha_1, \dots, \alpha_{n-1}) \subset K(\alpha_1, \dots, \alpha_n)$. If $f_n \neq f_i$ for all $i = 1, \dots, n-1$, then we are done. Otherwise, $f_n = f_i$ for some $i = 1, \dots, n-1$. Let S denote the set of the union of all the roots of $f_1, \dots, f_{n-1}$ that lie in L. Clearly, $|S|$ if finite and $\alpha_n \in S$ by assumption. Now consider the set $H = \{\lambda\alpha_n \mid \lambda \in K^\times\}$. H is infinte because the field K is. Therefore there exists $\beta_n \in H$ such that $\beta_n \notin S$. Consider the minimal polynomial g_n of β, then $g_n \neq f_i$ for all $i = 1, \dots, n-1$. Replace α_n by β_n and we have $L = K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \beta_n)$ and we are done. $\square$

Lemma 1.1. *For any $\sigma \in Gal(L/K)$, $f_i(\sigma(\alpha_i)) = 0$.*

Proof. Let $f_i(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$. Since α_i is a root of f_i, we have

$$a_m \alpha_i^m + \cdots + a_0 = 0.$$

By applying σ to both sides, we get

$$\sigma(a_m)\sigma(\alpha_i)^m + \cdots + \sigma(a_0) = 0.$$

Since σ is identity on K, we have $\sigma(a_i) = a_i$ for all i and this proves the claim. $\square$

Lemma 1.2. *Let $\sigma \in Gal(L/K)$. Then $\sigma(\alpha_i)$ is not a root for any f_j, $j \neq i$.*

Proof. Suppose $\sigma(\alpha_i)$ satisfies $f_j(\sigma_i)$ for some $j \neq i$. Let $f_j(x) = a_m x^m + \cdots + a_0$ with $a_i \in K$. Then $f(\sigma(\alpha_i)) = 0$ implies $a_m\sigma(\alpha_i)^m + \cdots + a_0 = 0$. Applying σ^{-1}, we get $a_m\alpha_i^m + \cdots + a_0 = 0$ which implies $f_j(\alpha_i) = 0$. But that is a contradiction to our choices of α_i since f_j is not the minimal polynomial of α_i. $\square$

For each $i = 1, \dots, n$, let S_i denote the set of distinct roots of f_i that are in L. Set $m_i = |S_i| \leq \deg f_i$. Clearly, $\prod_{i=1}^n m_i \leq \prod_{i=1}^n \deg f_i = [L : K]$. Consider $S = S_1 \times \cdots \times S_n$ and let $\alpha = (\alpha_1, \dots, \alpha_n) \in S$.

Define the map

$$\theta : Gal(L/K) \to S$$
$$\sigma \mapsto (\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

We will also write $\sigma(\alpha) := (\sigma(\alpha_1), \dots, \sigma(\alpha_n))$. With this notation, $\theta(\sigma) = \sigma(\alpha)$. By lemma 1.1 and 1.2, this map is well defined.

Lemma 1.3. *Let $\beta = (\beta_1, \dots, \beta_n) \in S$. Then there exists $\sigma \in Gal(L/K)$ such that $\sigma(\alpha) = \beta$.*

Proof. We can write the field L as a quotient $L = K[x_1, \dots, x_n]/(f_1, \dots, f_n)$ where α_i is the image of x_i in L for each i. Here each $f_i(x_i)$ is considered as a polnomial in the variable x_i. Define a ring homomorphism

$$\begin{aligned}\Psi : K[x_1, \dots, x_n] &\to K[x_1, \dots, x_n]/(f_1, \dots, f_n) = L \\ g(x_1, \dots, x_n) &\mapsto g(\beta_1, \dots, \beta_n)\end{aligned}$$

Note that $\Psi(x_i) = \beta_i$ for each $i = 1, \dots, n$ and that $\Psi(c) = c$ for $c \in K$. We want to show that Ψ induces a homomorphism $\overline{\Psi} : L \to L$. By the first isomorphism theorem, it is enough to show that $\Psi(f_i(x_i)) = 0$ for all $i = 1, ..., n$. But then $\Psi(f_i(x_i)) = f_i(\beta_i) = 0$ since β_i is a root of f_i and we are done. □

Proposition 1.4. *The map θ induces a bijection between $Gal(L/K)$ and S.*

Proof. Let $\sigma, \sigma' \in Gal(L/K)$ such that $\sigma(\alpha) = \sigma'(\alpha)$. Then $\sigma(\sigma')^{-1}(\alpha) = \alpha$. But then $\sigma(\sigma')^{-1}(\alpha_i) = \alpha_i$ for all i, that is, it fixes the whole of L and therefore must be identity. Hence we have $\sigma = \sigma'$. This proves the injectivity of θ.

Surjectivity follows from lemma 1.3. □

Corollary 1.5. *If K is infinite, then $|Gal(L/K)| \leq [L : K]$.*

Proof. It follows from the fact that $|Gal(L/K)| = |S| = |S_1| \times \cdots |S_n| = \prod_{i=1}^n m_i \leq \prod_{i=1}^n \deg f_i = [L : K]$. □

Corollary 1.6. *Let K is infinite, then $|Gal(L/K)| = [L : K]$ if and only if $K \subseteq L$ is normal and separable.*

Proof. If $K \subseteq L$ is normal and separable, then $|S_i| = \deg f_i$. Hence $|S| = [L : K]$ and therefore $|Gal(L/K)| = [L : K]$.

Conversely, if $|Gal(L/K)| = [L : K]$, then $|S| = \prod m_i = \prod \deg f_i = [L : K]$. This is possible if $m_i = \deg f_i$. This means that all the roots of f_i lie in L, that is, L is the splitting field for all f_is and therefore L is normal.

Also, the roots of f_is are all distinct and therefore $\alpha_1, \dots, \alpha_n$ are all separable which implies $L = K(\alpha_1, \dots, \alpha_n)$ is separable. □

Definition 1.7. *A finite extension $K \subseteq L$ is called* **Galois** *if it is both normal and separable over K.*