I GALOIS GROUPS I 1

1 Galois Groups I

Definition 1 (Galois group of polynomial). Let $L = K(\alpha_1, ..., \alpha_n)$ and let $P(\alpha_1, ..., \alpha_n)$ where $P \in K[\alpha_1, ..., \alpha_n]$ is an element of L. Then we define

$$\operatorname{Gal}_K(f) = \{ \sigma \in S_n \mid \forall P \in K[\alpha_1, \dots, \alpha_n], \text{ if } P(\alpha_1, \dots, \alpha_n) = 0 \text{ then } P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) \}$$

Lemma 1.1. 1. $Gal_K(f) \leq S_n$;

2. If $K_1: K$, then $Gal_{K_1}(f) \leq Gal_K(f)$.

Definition 2. Let L:K be a field extension. Then

$$\operatorname{Gal}_K(L) = \operatorname{Gal}(L:K) = \{ \varphi \in \operatorname{Aut}(L) : \varphi \text{ is a K-homomorphism} \}$$

Definition 3 (Galois automorphism on splitting field). Let $\sigma \in \operatorname{Gal}_K f$ where L is a splitting field for f over K, and define $\widehat{\sigma} \in \operatorname{Aut}_K(L)$ such that $\widehat{\sigma}(P(\alpha_1, \ldots, \alpha_n)) = P(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

Lemma 1.2. The map $\psi(\sigma) = \widehat{\sigma}$ is a group isomorphism.

Theorem 1.3. If L: K is an algebraic extension and $\sigma: L \to L$ is a K-homomorphism, then $\sigma \in Aut(L)$

Lemma 1.4. Suppose that M:K is a normal extension. Then:

- (a) for any $\sigma \in Gal(M:K)$ and $\alpha \in M$, we have $\mu_{\sigma(\alpha)}^K = \mu_{\alpha}^K$;
- (b) for any $\alpha, \beta \in M$ with $\mu_{\alpha}^K = \mu_{\beta}^K$, there exists $\tau \in \operatorname{Gal}(M:K)$ having the property that $\tau(\alpha) = \beta$.