1 Galois Groups I

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

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

Lemma 1.1. *1.* $\mathrm{Gal}_K(f) \leqslant S_n$*;*

2. If $K_1 : K$*, then* $\mathrm{Gal}_{K_1}(f) \leqslant \mathrm{Gal}_K(f)$*.*

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

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

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

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* $\sigma \in \mathrm{Aut}(L)$

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

(a) for any $\sigma \in \mathrm{Gal}(M : K)$ *and* $\alpha \in M$*, we have* $\mu^K_{\sigma(\alpha)} = \mu^K_\alpha$*;*

(b) for any $\alpha, \beta \in M$ *with* $\mu^K_\alpha = \mu^K_\beta$*, there exists* $\tau \in \mathrm{Gal}(M : K)$ *having the property that* $\tau(\alpha) = \beta$*.*