Galois, Fields and Algebras

Naveensurya V
naveen24@iisertvm.ac.in

January 19, 2025

Contents

1 First half of Galois Theory

1.1 Basic Definitions

Definition 1.1. *Let L/K be a field extension and* ***Automorphism*** *of L/K is defined as*

$$Aut(L/K) := \{\phi : L \to L|\ \phi(k) = k,\ \forall k \in K\}$$

Definition 1.2. *Let $U \subseteq Aut(L/K)$ then $\mathscr{F}(U)$ is defined as*

$$\mathscr{F}(U) := \{x \in L|\ \Psi(x) = x,\ \forall \Psi \in U\}$$

Definition 1.3. *Let $Z \subset L$ be a intermediate field between L and K then $\mathscr{G}(Z)$ is defined as*

$$\mathscr{G}(Z) := Aut(L/Z)$$

Lemma 1.1. *Let $U \subseteq Aut(L/K)$ and $Z \subset L$ be a intermediate field between L and K*

(a) $U \subseteq \mathscr{G} \circ \mathscr{F}(U) := Aut(L/\mathscr{F}(U))$

(b) $Z \subseteq \mathscr{F} \circ \mathscr{G}(Z)$

(c) *$\mathscr{F}$ is inclusion reversing. i.e,* $U_1 \subseteq U_2 \implies \mathscr{F}(U_2) \subseteq \mathscr{F}(U_1)$

(d) *$\mathscr{G}$ is inclusion reversing. i.e,* $Z_1 \subseteq Z_2 \implies \mathscr{G}(Z_2) \subseteq \mathscr{G}(Z_1)$

(e) $\mathscr{G} = \mathscr{G} \circ \mathscr{F} \circ \mathscr{G}$

(f) $\mathscr{F} = \mathscr{F} \circ \mathscr{G} \circ \mathscr{F}$

Proof. Isn't it obvious ♡ □

1.2 Dedekind Theorem

Theorem 1.1. ***[Dedekind's theorem on linear independence of characters.]*** *Distinct field automorphims $\sigma_1, \ldots, \sigma_n$ from $L \to L$ are linearly independent on the L-vector space of all mappings from $L \to L$*

Proof. □

Definition 1.4. *Let L/K be a field extension. we can view L as vector space over K and* ***degree of extension*** *is defined as*

$$[L : K] := dim_K(L)$$

Lemma 1.2. *Suppose $[V_1 : K] = n$ and $[V_2 : K] = m$, then*

$$dim_K\big(Hom_K(V_1, V_2)\big) = mn$$

Lemma 1.3. *Let L/K be a finite field extension. Then $Aut(L/K) \leq [L : K]$*

1.3 Artin Theorem

Definition 1.5. *Let $U \subseteq Aut(L/K)$ be a finite subgroup. Then the* ***U-trace*** *of $\alpha \in L$ is defined as*

$$tr_U(\alpha) := \sum_{\sigma \in U} \sigma(\alpha)$$

Lemma 1.4. *$tr_U : L \to \mathscr{F}(U)$ is a K-linear map. If $char(K) \nmid |U|$, then $tr_U : L \to \mathscr{F}(U)$ is surjective*

Lemma 1.5. *tr_U is not identitically zero.*

Theorem 1.2. ***[Artin]*** *Let $U \subseteq Aut(L/K)$ be a finite subgroup. Then $[L : \mathscr{F}(U)] = |U|$ and $\mathscr{G} \circ \mathscr{F}(U) = U$*

Proof. Exercise. □

Corollary 1. *If L/K is a finite field extension , then $\mathscr{G} \circ \mathscr{F} \equiv id$*

1.4 Galois extension

Definition 1.6. *An extension L/K is* ***Galois extension*** *if*

$$\mathscr{F} \circ \mathscr{G}(K) = K$$

Equivalently, $\mathscr{F}(Aut(L/(K))) = K$

Corollary 2. *Let $G \subseteq Aut(L)$ be a finite subgroup and let $K := \mathscr{F}(G)$. Then L/K is a galois extension and $Aut(L/K) = G$*

Proof. □

Corollary 3. *Let L/K be a finite extension . Then L/K is Galois $\iff |Aut(L/K)| = [L : K]$*

2 Results from Ring Theory