Galois Theory

IKHAN CHOI

1. Elementary field theory

1.1. Finite extensions.

Theorem 1.1. *Let E/F be a field extension. Then, E is a vector space over F.*

Definition 1.1. A *degree* of a field extension E/F is the dimension of the vector space E over F and denoted by $[E : F]$.

Definition 1.2. A field extension is called *finite* if its degree is finite.

Theorem 1.2 (Multiplicity of degree)**.** *If K is an intermediate field in a field extension E/F, then*

$$[E : F] = [E : K][K : F].$$

Proof. Boring basis counting. □

Corollary 1.3. *Finite extension of finite extension is finite.*

Theorem 1.4. *Let E/F be a finite extension. There is a finite tower of simple extensions.*

Proposition 1.5. *A nontrivial field homomorphism is injective.*

Definition 1.3. A nontrivial field homomorphism is called *embedding* of *isomorphism onto a subfield of codomain.*

2. Algebraic extension

2.1. Finite simple extensions.

We will discuss minimal polynomial and conjugates

Definition 2.1. A field extension E/F is called *simple* if there is an element $\alpha \in E$ such that E is the smallest field containing α and F. In this case, we write $E = F(\alpha)$.

Definition 2.2. Let E/F be a field extension. An element $\alpha \in E$ is *algebraic over F* if $F(\alpha)/F$ is finite.

Proposition 2.1. *Let α be algebraic over F. Then, $F(\alpha) = F[\alpha]$.*

Theorem 2.2. *Let E/F be a field extension and $\alpha \in E$. Then, α is algebraic over F iff there is a polynomial $f \in F[x]$ such that $f(\alpha) = 0$.*

Proof. Since $d = [F(\alpha) : F] < \infty$, we can find linearly dependent finite subset of $\{1, \alpha, \alpha^2, \cdots\}$. The coefficients construct the polynomial.

Conversely, if there is such f, every element of $F(\alpha)$ is represented as a linear combination of $\{1, \alpha, \cdots, \alpha^{\deg f - 1}\}$. □

Theorem 2.3. *Let E/F be a field extension and $\alpha \in E$is algebraic over F. Then there is a unique monic irreducible polynomial $\mu_{\alpha,F} \in F[x]$ such that $\mu_{\alpha,F}(\alpha) = 0$.*

Proof. The polynomials satisfying α form an ideal of $F[x]$. Since $F[x]$ is a PID, there is a generator which can be taken to be monic. Since the ideal is prime, the generator is prime(=irreducible), and it is the only irreducible in the ideal. □

Definition 2.3. Let E/F be a field extension and $\alpha \in E$ is algebraic. A monic irreducible polynomial $\mu_{\alpha,F} \in F[x]$ satisfying $\mu_{\alpha,F}(\alpha) = 0$ is called the *minimal polynomial* of α over F.

Theorem 2.4. *Let E/F be a field extension and $\alpha \in E$ is algebraic. Then, $F(\alpha) \cong F[x]/\mu_{\alpha,F}$, and $[F(\alpha) : F] = \deg \mu_{\alpha,F}$.*

Proof. Consider $\mathrm{eval}_\alpha : F[x] \to F(\alpha)$. The kernel is characterized as the principal ideal generated by $\mu_{\alpha,F}$. Since $\mu_{\alpha,F}$ is irreducible, $F[x]/(\mu_{\alpha,F})$ is a field, which implies the isomorphism $F[x]/(\mu_{\alpha,F}) \cong F(\alpha)$.

Now we claim the dimension of $F[x]/(f)$ is the degree of f. □

Definition 2.4. Let E/F be a field extension and $\alpha, \beta \in E$ be algebraic over F They are said to be *conjugate over F* if they have a common minimal polynomial over F.

Theorem 2.5. *Let ϕ be a nontrivial field homomorphism. Then, α and $\phi(\alpha)$ are conjugates.*

2.2. **Algebraic extensions and isomorphism extension.**

Definition 2.5. A field extension E/F is called *algebraic* if all elements $\alpha \in E$ is algebraic over F.

Equivalently,

Definition 2.6. A field extension is called *algebraic* if it is a direct limit of finite extensions.

Theorem 2.6. *Let K be an intermediate field of a field extension E/F. Then, E/F is algebraic iff E/K and K/F are algebraic.*

Proof. One direction is clear. Suppose E/K and K/F are algebraic. Take $\alpha \in E$ and $\mu_{\alpha,K}$ be the minimal polynomial of α over K. Let L be a field generated by F and the coefficients of $\mu_{\alpha,K}$. Then, $F(\alpha)/L$ and L/F are finite. □

Proposition 2.7. *A simple extension is finite iff it is algebraic.*

Proof. Trivial. □

Theorem 2.8 (Isomorphism extension theorem)**.** *Let E/F be an algebraic extension. Let $\phi : F \cong F'$ be a field isomorphism. Let $\overline{F}'$ be an algebraic closure of F'. Then, there is an embedding $\widetilde{\phi} : E \to \overline{F}'$ which extends ϕ.*

Proof. □

2.3. Algebraic closure.

Theorem 2.9. *Let E/F be a field extension. The set of all algebraic elements in E over F forms a field.*

Proof. □

Definition 2.7. A field F is called *algebraically closed* if it has no proper algebraic extension.

Definition 2.8. A field $\overline{F}$ is called an *algebraic closure* if $\overline{F}$ is algebraically closed field and $\overline{F}/F$ is algebraic.

Theorem 2.10. *Every field has an algebraic closure.*

Proof. □

Theorem 2.11. *Algebraic closure is unique up to isomorphism.*

Proof. □

Proposition 2.12. *Let E/F be a field extension with algebraically closed field E. Then the set of all algebraic elements in E over F is the only algebraic closure of F contained in E.*

Proof. The set of algebraic elements is algebraically closed. □

3. Separable extension

4. Normal extension

5. Computation of Galois groups

* reducible case, irreducible¡=¿transitivity * resolvent polynomial1: discriminant * resolvent polynomial2: cubic resolvent * ,   * =2n: composition of n transpositions * x- Jacobson-Velez * reduction modulo p (over F)

5.1. Quartic.

In this section, we assume the following setting:

- F is a perfect field,
- f is an irreducible quartic over F,
- E is the splitting of f over F,
- $G = \mathrm{Gal}(E/F)$,
- $H = G \cap V_4$.

Theorem 5.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4.*

Corollary 5.2. $G \cong S_4,\ A_4,\ D_4,\ V_4,$ *or* C_4.

Proposition 5.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4.*

Now we define our resolvent polynomial.

Proposition 5.4. *Let K be the fixed field of H. Then,*

$$K = F(\alpha_1\alpha_2 + \alpha_3\alpha_4,\ \alpha_1\alpha_3 + \alpha_2\alpha_4,\ \alpha_1\alpha_4 + \alpha_2\alpha_3).$$

Definition 5.1. Let K be the fixed field of H. A *resolvent cubic* is a cubic R_3 that has K as the splitting field over F.

Theorem 5.5. *We have*

(1) $G \cong S_4$ *if* R_3 *is irreducible and ,*
(2) $G \cong A_4$ *if* R_3 *is irreducible and ,*
(3) $G \cong D_4$ *if* R_3 *has only one root in* K *and* f *is irreducible over* K*,*
(4) $G \cong C_4$ *if* R_3 *has only one root in* K *and* f *is reducible over* K*,*
(5) $G \cong V_4$ *if* R_3 *splits in* K*.*

Proof. There are five possible cases:

$$(G, H) = (S_4, V_4),\ (A_4, V_4),\ (D_4, V_4),\ (V_4, V_4),\ (C_4, C_2).$$

We have

$$[K : F] = |G/H|, \qquad [E : K] = |H|.$$

If f is reducible over K, then $\mathrm{Gal}(E/K)$ is no more a transitive subgroup of S_4 so that $H \neq V_4$ and $G \cong C_4$. □

$$\begin{tikzcd}
E \arrow[rrrr] & & & & 1 \arrow[d, dashed, "2"] & \\
& & & & C_2 \arrow[dl, dashed, "2"'] \arrow[dr, dashed, "2"] & \\
K = F_{V_4 \cap G} \arrow[uu, dashed] & & & V_4 \arrow[dl, dashed, "3"'] \arrow[dr, dashed, "2"] & & C_4 \arrow[dl, dashed, "2"] \\
F \arrow[u, dashed] \arrow[r] & ? & A_4 \arrow[dr, dashed, "2"'] & & D_4 \arrow[dl, dashed, "3"] & \\
& & & S_4 & &
\end{tikzcd}$$