ALGEBRA

TIANJIAO NIE

1. Fields

1.1. Splitting Fields.

Lemma 1.1.1. Let F be a field. Let $f \in F[X]$ be a non-constant polynomial. There exists a smallest field extension E/F such that f splits completely over E. Moreover, the extension E/F is normal and unique up to (non-unique) isomorphisms.

Definition 1.1.2. Let F be a field. Let $f \in F[X]$ be a non-constant polynomial. The field extension E/F in Lemma 1.1.1 is called a splitting field of f over F.

2. Galois Theory

2.1. **Even Permutations.** Let F be a field. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be a monic polynomial in $F[X]$. Let F_f be a splitting field for f. Suppose $f(X) = \prod_{i=1}^n (X - \alpha_i)$ in F_f. Set

$$\Delta(f) = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j).$$

Note that $\Delta(f)$ depends on the ordering of the roots $(\alpha_i)_i$. The discriminant of f is defined to be $D(f) = \Delta(f)^2$, which is independent on the ordering. Note that $D(f)$ is non-zero if and only if f has only simple roots, i.e. f is separable. In the following we assume that f is separable. Let $G_f = \mathrm{Gal}(F_f/F)$ be the Galois group of f, and identify it with a subgroup of $\mathrm{Perm}(\{\alpha_1, \dots, \alpha_n\}) \simeq S_n$.

Lemma 2.1.1. Let $\sigma \in G_f$. Then

(1) $\sigma(\Delta(f)) = \mathrm{sign}(\sigma)\Delta(f)$.
(2) $\sigma(D(f)) = D(f)$.

Therefore $D(f) \in F$.

Lemma 2.1.2. Suppose $\mathrm{char}(F) \neq 2$. The subextension of F_f/F corresponding to the subgroup $A_n \cap G_f$ is $F[\Delta(f)]/F$. Therefore $G_f \subset A_n$ if and only if $D(f)$ is a square in F.

Lemma 2.1.3. (1) $D(X^2 + bX + c) = b^2 - 4c$.
(2) $D(X^3 + bX + c) = -4b^3 - 27c^2$.

Remark 2.1.4. Suppose $\mathrm{char}(F) = 2$. In this case, $\sigma(\Delta(f)) = \Delta(f)$ and thus $D(f)$ is always a square. In order to compare G_f and A_n, we need to use the Berlekamp discriminant

$$D(f) = \sum_{i<j} \frac{\alpha_i\alpha_j}{\alpha_i^2 + \alpha_j^2}.$$

2.2. Transitive Action.

Lemma 2.2.1. Let $f \in F[X]$ be separable. Then f is irreducible if and only if G_f permutes the roots of f transitively.

Email address: `nietianjiao@outlook.com`