

1 Galois Fields I

Definition 1 (Formal derivative). We define the *derivative operator* $\mathcal{D} : K[t] \rightarrow K[t]$ by

$$\mathcal{D} \left(\sum_{k=0}^n a_k t^k \right) = \sum_{k=1}^n k a_k t^{k-1}.$$

Theorem 1.1. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f with $K \subseteq L$. Then the following are equivalent:

- (i) f has a repeated root over L ;
- (ii) There exists $\alpha \in L$ such that $f(\alpha) = 0 = (\mathcal{D}f)(\alpha)$;
- (iii) There exists $g \in K[t]$ with $\deg g \geq 1$ such that $g \mid f$ and $g \mid \mathcal{D}f$.

Definition 2 (Inseparable). A polynomial $f \in K[t]$ is *inseparable over* K if f is not separable over K , i.e. f has an irreducible factor $g \in K[t]$ having the property that g has fewer than $\deg g$ distinct roots in K .

Theorem 1.2. Suppose $f \in K[t]$ is irreducible over K . Then f is inseparable over $K \iff \text{char } K = p > 0$ and $f \in K[t^p]$.

Definition 3 (Frobenius map). Suppose that $\text{char } K = p > 0$. The *Frobenius map* $\varphi : K \rightarrow K$ is defined by $\varphi(\alpha) = \alpha^p$.

Theorem 1.3. Suppose that $\text{char } K = p > 0$, and put $F = \{c \cdot 1_K : c \in \mathbb{Z}\}$. Then F is a subfield (called the prime subfield) of K , and $F \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 4 (Fixed field). Let $L : K$ be a field extension and $G \leq \text{Aut}(L)$. We define the *fixed field* of G as

$$\text{Fix}_L(G) = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Theorem 1.4. Suppose that $\text{char } K = p > 0$, and let F be the prime subfield of K . Let $\varphi : K \rightarrow K$ denote the Frobenius map. Then φ is an injective homomorphism, and $\text{Fix}_\varphi(K) = F$.

Corollary 1. Suppose that $\text{char } K = p > 0$ and K is algebraic over its prime subfield. Then the Frobenius map is an automorphism of K .

Corollary 2. Suppose that $\text{char } K = p > 0$ and K is algebraic over its prime subfield. Then all polynomials in $K[t]$ are separable over K .

Corollary 3 (**). Suppose that $\text{char } K = 0$. Then all polynomials in $K[t]$ are separable over K .

Theorem 1.5. Suppose that $\text{char } K = p > 0$. Let

$$f(t) = g(t^p) = a_0 + a_1 t^p + \cdots + a_{n-1} t^{(n-1)p} + t^{np}$$

be a non-constant monic polynomial over K . Then $f(t)$ is irreducible in $K[t]$ if and only if $g(t)$ is irreducible in $K[t]$ and not all the coefficients a_i are p -th powers in K .