Separable Extensions and Primitive Element Theorem

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

In this file:

1. §3.2.7: Separable polynomials and perfect fields;
2. §3.2.8: Separable extensions and the Primitive Element Theorem.

Definition. For a field K, a polynomial $f(x) \in K[x]$ is said to be separable over K if it has no repeated roots in its splitting field over K.

Example. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$, but not when regarded as a polynomial over $\mathbb{F}_3$:

$$f(x) = (x - 2)^3 \in \mathbb{F}_3[x].$$

Example. $K = \mathbb{F}_2(t)$ and $f(x) = x^2 - t \in K[x]$. The splitting field $L = K(\sqrt{t})$ of f over K has degree 2 over K, but

$$f(x) = x^2 - t = (x - \sqrt{t})^2 \in L[x],$$

so f is not separable.

Lemma. Let K be any field and let $f \in K[x]$ with positive degree. Then the following are equivalent:

1. f is separable over K;
2. f and f' are relatively prime as elements in $K[x]$;
3. f has no repeated roots in ~~any~~ every field extension L of K.

Proof. Let $f = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, $p_i \in K[x]$ irreducible, pairwise non-associates. Let L_f be the splitting field of f over K.

1. 1) $\Rightarrow$ 2): For each j, f and p_j share at least one root $a_j \in L_f$. Then $f'(a_j) \neq 0$ implies that $p_j \nmid f'$. Thus f and f' have no common irreducible factors in $K[x]$, i.e., they are relatively prime in $K[x]$.
2. 2) $\Rightarrow$ 3): f and f' are relatively prime in $K[x]$. Thus there exist $a(x), b(x) \in K[x]$ such that
$$a(x)f(x) + b(x)f'(x) = 1 \in K[x]$$
It follows that f has no repeated root in any extension L of K.
3. 3) $\Rightarrow$ 1): trivial.

§3.2.8: Separable extensions and the Primitive Element Theorem

Definition. An algebraic extension $K \subset L$ is said to be separable if the minimal polynomial of every $a \in L$ over K is separable over K.

The Primitive Element Theorem. A finite separable extension is simple.

Proof: See Lecture Notes.

Corollary. If K has characteristic 0 or is a finite field, then very finite extension of K is simple.

Remark: A field K is said to be Perfect if either $\mathrm{Char}(K) = 0$, or $\mathrm{char}(K) = p$ and Frobenius morphism $\sigma : K \to K$ is surjective. A finite extension of perfect field is separable. See lecture notes for the proof.