Lecture 10 : Separable Extensions II

Objectives

(1) Roots of an irreducible polynomial have equal multiplicity.
(2) Separable finite algebraic extensions and separable degree.
(3) Transitivity of separable extensions

Key words and phrases: Separable degree, extensions of embeddings.

Proposition 10.1. *Let F be a field and $f(x) \in F[x]$ be a monic irreducible polynomial. Then all roots of $f(x)$ have equal multiplicity. If char $F = 0$ then all roots of $f(x)$ are simple and if char $F = p > 0$ then all roots of $f(x)$ have multiplicity p^n for some n.*

Proof. Let α, β be roots of $f(x)$ in $\overline{F}$. Consider the F-isomorphism $\sigma : F(\alpha) \to F(\beta)$ given by $\sigma(\alpha) = \beta$. Then σ can be extended to an automorphism of $\overline{F}$. Let $f(x) = (x-\alpha)^m h(x)$ where $h(x) \in \overline{F}[x]$ and α is not a root of $h(x)$. Then $f(x) = \tau(f(x)) = (x-\beta)^m \tau(h(x))$. Hence the multiplicity of β is at least m. By symmetry we conclude that both roots have the same multiplicity.

We know that irreducible polynomials are separable if char $F = 0$. Let char $F = p > 0$. Suppose $f(x)$ has roots of positive multiplicity. Then there exists a separable polynomial $g(x)$ so that $f(x) = g(x^{p^n})$. Let $r_1, r_2, \ldots, r_g$ be distinct roots of $f(x)$ in $\overline{F}$. Then

$$f(x) \quad = \quad (x-r_1)^{p^n}(x-r_2)^{p^n} \ldots (x-r_g)^{p^n}$$

□

Separability and extensions of embeddings

Let $E = k(a)$ be an algebraic extension of a field k. Let $p(x) = \text{irr}(a, k)$. We have seen that if $\sigma : k \to L$ is an embedding of fields where L is algebraically closed then the number of embeddings $\tau : E \to L$ extending σ is equal to the number of distinct roots of $p^\sigma(x)$ in L. Hence if $p(x)$ is separable, then the number of extensions of σ to embeddings of E into L is $[E : k]$.

Conversely, if σ has $[E:k]$ extensions, then for any such extension τ, $\tau(\alpha)$ is a root of $p^{\sigma}(x)$. Hence $p(x)$ is separable. We now discuss this phenomenon for finite algebraic extensions.

Let $\sigma : F \to L$ be an embedding of fields where L is an algebraic closure of $\sigma(F)$. Let $\tau : F \to L'$ be an embedding of fields where L' is an algebraic closure of $\tau(F)$. Let E be an algebraic extension of F. Let S_σ (resp. S_τ) denote the set of extensions of σ (resp. τ) to embeddings of E into L (resp. L'). Consider the following diagram of fields and embeddings:

$$\begin{array}{ccccc}
L' & & \xleftarrow{\quad\lambda\quad} & & L \\
| & & & & | \\
\tau^*(E) & \xleftarrow{\tau^*} & E & \xrightarrow{\sigma^*} & \sigma^*(E) \\
| & & | & & | \\
\tau(F) & \xleftarrow{\tau} & F & \xrightarrow{\sigma} & \sigma(F)
\end{array}$$

Let λ be an extension of the embedding $\tau \circ \sigma^{-1} : \sigma(F) \to \tau(F)$ to an isomorphism $\lambda : L \to L'$.

Theorem 10.2. *The map*

$$\psi : S_\sigma \to S_\tau, \;\; \psi(\sigma^*) = \lambda \circ \sigma^*$$

is a bijection.

Proof. If $\sigma^* \in S_\sigma$ then for any $x \in F$ we have

$$\lambda \circ \sigma^*(x) = \lambda \circ \sigma(x) = \tau \circ \sigma^{-1}(\sigma(x)) = \tau(x).$$

Hence $\lambda \circ \sigma^*$ is an extension of τ to an embedding of E into L'. Hence λ induces a mapping $\psi : S_\sigma \to S_\tau$ defined by $\psi(\sigma^*) = \lambda \circ \sigma^*$. Since λ is an isomorphism, ψ is a bijection.

□

Definition 10.3. *If E/F is an algebraic extension then the cardinality of S_σ is called the separable degree of E/F and it is denoted by $[E:F]_s$.*

Proposition 10.4. *Let $k \subseteq F \subseteq E$ be a tower of finite algebraic extensions. Then $[E : k]_s \leq [E : k]$ and*

$$[E : k]_s = [E : F]_s[F : k]_s.$$

Proof. First we show that the separable degree is multiplicative in a tower of field extensions. Let $\sigma : k \to L$ be an embedding into an algebraically closed field L. Let $(\sigma_i)_{i\in I}$ be distinct extensions of σ to embeddings of F into L. Each σ_i has $[E : F]_s$ extensions to embeddings of E into L. Let these be (τ_{ij}). Hence (τ_{ij}) has cardinality $[F : k]_s[E : k]_s$. If $\gamma : E \to L$ is an embedding extending σ, then $\gamma|_F$ is an extension of σ to an embedding of F into L. Hence $\gamma|_F = \tau_{ij}$. This proves the multiplicativity of separable degree in a tower of field extensions.

Since E/k is finite, there exist elements $a_1, a_2, \ldots, a_n$ such that

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, a_2, \ldots, a_n).$$

Each step in the above tower is a simple algebraic extension. Hence the separable degree of each step is atmost its degree. Since the separable degree and degree of a field extension are multiplicative, we have $[E : k]_s \leq [E : k]$. □

Corollary 10.5. *Let $k \subset F \subset K$ be a tower of finite extensions. Then $[E : k]_s = [E : k]$ if and only if the corresponding equality holds in each step of the tower.*

Theorem 10.6. *Let E/k be a finite extension. Then E/k is separable if and only if $[E : k]_s = [E : k]$.*

Proof. Let E/k be finite separable extension. Then $E = k(a_1, a_2, \ldots, a_n)$ for some $a_1, a_2, \ldots, a_n \in E$. Then each a_i is separable over k. Hence a_i is separable over $k(a_1, a_2, \ldots, a_{i-1})$ for $i = 1, 2, \ldots, n$.

$$[k(a_1, a_2, \ldots, a_i) : k(a_1, a_2, \ldots, a_{i-1})]_s = k(a_1, a_2, \ldots, a_i) : k(a_1, a_2, \ldots, a_{i-1})].$$

for $i = 1, 2, \ldots, n$, whence $[E : k]_s = [E : k]$.

Conversely let $[E : k]_s = [E : k]$. Then using the fact that the separable degree and degree are multiplicative and the separable degree is atmost the degree, we conclude that for any $a \in E$, $[E : k(a)]_s[k(a) : k]_s = [E : k]_s =$

$[E : k]$. Hence $[k(a) : k]_s = [k(a) : k]$. Hence $\mathrm{irr}(a, k)$ is separable. Thus E/k is a separable extension.

□