Lecture 9 : Separable Extensions I

Objectives

(1) Criterion for multiple roots in terms of derivatives
(2) Irreducible polynomials are separable over fields of characteristic zero.
(3) Characterization of perfect fields of positive characteristic,

Key words and phrases: Separable polynomial, separable element, separable extensions, derivative of a polynomial, perfect fields.

Let F be a field. We have seen that the discriminant of a polynomial $f(x) \in F[x]$ vanishes if and only if $f(x)$ has a repeated root. Calculation of discriminant can be difficult. In this section we discuss an effective criterion in terms of derivatives of polynomials whether certain root of $f(x)$ is repeated. We will also study fields F so that no irreducible polynomial in $F[x]$ has repeated roots.

Let E be a splitting field of a monic polynomial $f(x) \in F[x]$ of degree n. Write in $E[x]$ the unique factorization of $f(x)$.

$$f(x) = (x - r_1)^{e_1}(x - r_2)^{e_2} \cdots (x - r_g)^{e_n}.$$

where $r_1, \ldots, r_g \in E$ and $e_1, e_2, \ldots, e_g$ are positive integers.

Definition 9.1. *The numbers $e_1, e_2, \ldots, e_n$ are called the multiplicities of $r_1, r_2, \ldots, r_n$ respectively. If $e_i = 1$ for some i, then r_i is called a simple root. If $e_i > 1$ then r_i is called a multiple root. A polynomial $f(x)$ with no multiple roots is called a* **separable polynomial.**

Proposition 9.2. *The numbers of roots and their multiplicities are independent of a splitting field chosen for $f(x)$ over F.*

Proof. Let E and K be splitting fields of $f(x)$ over F. Then there is an $F-$isomorphism $\sigma : E \to K$. This isomorphism gives rise to an isomorphism

$$\phi_\sigma : E[x] \to K[x], \quad \varphi_\sigma \left(\sum_i a_i x^i \right) = \sum_i \sigma(a_i) x^i.$$

Let $f(x) = \prod_{i=1}^{g}(x - r_i)^{e_i}$ be the unique factorization of $f(x) \in E[x]$. Then $\phi_\sigma(f(x)) = \prod_{i=1}^{g}(x - \sigma(r_i))^{e_i}$. Since $K[x]$ is UFD, $\sigma(r_1), \ldots, \sigma(r_g)$ are the roots of $\phi_\sigma(f(x)) = f(x)$ with multiplicities $e_1, \ldots, e_g$ in K respectively. $\square$

The derivative criterion for multiple roots

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. We can define derivative of $f(x)$ without appealing to limits. This is preferable since F may not be equipped with a distance function.

The derivative of $f(x)$, is defined by $f'(x) := \sum_{i=0}^{m} ia_ix^{i-1}$. It is easy to check that the usual formulas for $(f(x) \pm g(x))', (f(x)g(x))'$ and $(f(x)/g(x))'$ where $g(x) \neq 0$ hold for derivatives of polynomials.

Theorem 9.3. *Let $f(x) \in F[x]$ be a monic polynomial.*
(1) *If $f'(x) = 0$ then every root of $f(x)$ is a multiple root.*
(2) *If $f'(x) \neq 0$ then $f(x)$ has simple roots if and only if* $\gcd(f, f') = 1$.

Proof. (1) Let $f(x) = (x - r)g(x)$. Then

$$0 = f'(x) = g(x) + (x - r)g'(x).$$

Thus $g(x) = -(x-r)g'(x)$, so r is a root of $g(x)$. Hence r is a multiple root.

(2) ($\Leftarrow$) Let $\gcd(f, f') = 1$ and let r be a multiple root of $f(x)$. Then $f(x) = (x - r)^2g(x)$ in some splitting field E of $f(x)$ over F. Thus

$$f'(x) = (x - r)^2g'(x) + 2(x - r)g(x).$$

Hence $f'(r) = 0$. If $d(x) = \gcd(f(x), f'(x)) \in F[x]$ then

$$d(x) = p(x)f(x) + q(x)f'(x)$$

for some $p(x), q(x) \in F[x]$. Hence $d(r) = 0$. Therefore, deg $d(x) \geq 1$, so $\gcd(f, f') \neq 1$, which is a contradiction. Therefore $f(x)$ has only simple roots.

($\Rightarrow$). Let $r_1, r_2, \ldots, r_n$ be the roots of $f(x)$ and assume that they are simple. Then

$$f(x) = (x - r_1)(x - r_2)\cdots(x - r_n) \text{ and } f'(x) = \sum_{i=1}^{n} \frac{f(x)}{(x-r_i)}.$$

Therefore $(x - r_i)$ does not divide $f'(x)$ any i. Hence f and f' have no common root. Therefore $\gcd(f, f') = 1$.

□

Proposition 9.4. (1) *Let $f(x) \in F[x]$ be an irreducible polynomial. Then $f(x)$ is separable if and only if $f' \neq 0$.*
(2) *Irreducible monic polynomials over a field of characteristic zero are separable.*

Proof. (1) ($\Rightarrow$) If $f' = 0$, then every root of $f(x)$ is a multiple root.

($\Leftarrow$) Suppose r is a multiple root of $f(x)$. Then $f'(r) = 0$. Since $f(x)$ is irreducible, $f(x) \mid f'(x)$. But this is a contradiction since $\deg f'(x) < \deg f(x)$. Therefore $f(x)$ is separable.

(2) If char $F = 0$, and $f(x)$ is of positive degree, then $f'(x) \neq 0$. □

Proposition 9.5. *Let F be a field of positive characteristic p. Then $x^p - a \in F[x]$ is either irreducible in $F[x]$ or $a \in F^p$.*

Proof. Suppose $f(x) = x^p - a = g(x)h(x)$ where $1 \leq \deg g = m < p$ Let b be a root of $f(x)$ in a splitting field E of $f(x)$. Then $a = b^p$, so $f(x) = (x - b)^p$. Hence b is also a root of $g(x)$. Thus $g(x) = (x - b)^m$ Then $b^m \in F$. Since $(p, m) = 1$, there exists $x, y \in \mathbb{Z}$ such that $px + my = 1$. Hence $b = b^{px+my} = a^x(b^m)^y \in F$. Thus $b^p = a \in F^p$. □

Example 9.6. We construct an irreducible polynomial with a multiple root. Let $F = \mathbb{F}_p(t)$ be the quotient field of the polynomial ring $\mathbb{F}_p[t]$. Let $f(x) = x^p - t \in F[x]$. Then $t \notin F^p$. Suppose t is a p^{th} power and

$$t = \frac{g(t)^p}{h(t)^p} = \frac{\left(\sum_i a_i t^i\right)^p}{\left(\sum_i b_i t^i\right)^p}.$$

Then $t(\sum b_i^p t^{ip}) = \sum_i a_i^p t^{ip}$. Hence $a_i = b_i = 0$ for all i. Thus $x^p - t$ is irreducible. Another way to see that $x^p - t$ is irreducible is to apply Eisenstein's Criterion with t as a prime element. Let E be a splitting field of $f(x)$ over F and u be a root of $f(x)$. Then $u^p = t$ so $x^p - t = (x - u)^p$, Hence $f(x)$ has only one root in E.

Proposition 9.7. *Let $f(x) \in F[x]$ where char $F = p$, be an irreducible polynomial. If $f(x)$ is not separable then there exists $g(x) \in F[x]$ such that $f(x) = g(x^p)$.*

Proof. Since $f(x) = \sum_i a_i x^i$ is irreducible and inseparable, we have $f'(x) = \sum(ia_i)x^{i-1} = 0$. Therefore $i = pt_i$ for some $t_i \in \mathbb{N}$. Hence

$$f(x) = \sum a_{pt_i} x^{pt_i} = \sum a_{pi}(x^p)^{t_i}.$$

□

Perfect Fields

We have seen that irreducible polynomial over fields of characteristic 0 are separable. But over a field of positive characteristic, irreducible polynomial may not be separable. We now discuss a condition on a field F of positive characteristic which will ensure that irreducible polynomials in $F[x]$ are separable.

Definition 9.8. *Let $F \subseteq K$ be a field extension. An algebraic element $\alpha \in K$ is a called* **separable element** *over F if $irr(\alpha, F)$ is separable. We say K/F is a* **separable algebraic extension** *if each element of K is separable. We say F is a* **perfect field** *if each algebraic extension is separable.*

Any field of characteristic zero is perfect. By the previous example $\mathbb{F}_p(t)$ is not perfect. This is basically due to t not being a p^{th} power in $\mathbb{F}_p(t)$.

Theorem 9.9. *Let F be a field of positive characteristic p. Then F is perfect if and only if*

$$F = F^p = \{a^p \mid a \in F\}.$$

Proof. Suppose $a \in F \backslash F^p$. Then $x^p - a \in F[x]$ is irreducible and inseparable. Hence F is not perfect.

($\Leftarrow$) Let $F = F^p$ and $f(x) \in F[x]$ be an irreducible polynomial. If $f(x)$ is inseparable, then $f(x) = g(x^p) = \sum a_i(x^p)^i = \sum(b_i)^p(x^p)^i = (\sum b_i x^i)^p$ for some $b_i \in F$. This contradicts irreducibility of $f(x)$. Hence $f(x)$ is separable.

□

Corollary 9.10. *Every finite field is perfect.*

Proof. Let $|F| = p^n$. By Lagrange theorem applied to the multiplicative group $F^\times$ we get $\alpha^{p^n-1} = 1$ for all $\alpha \in F^\times$. Hence $\alpha^{p^n} = \alpha$ for all $\alpha \in F$. Therefore $\alpha = (\alpha^{p^{n-1}})^p$. □