Separable and Inseparable Extensions

Kevin James

Definition

A polynomial $p(x) \in F[x]$ is called <u>separable</u> if it has no multiple roots. A polynomial which is not separable is called <u>inseparable</u>.

Definition

A polynomial $p(x) \in F[x]$ is called separable if it has no multiple roots. A polynomial which is not separable is called inseparable.

Example

1. The polynomial $x^2 - 2$ is separable over $\mathbb{Q}$. The polynomial $(x^2 - 2)^2$ is inseparable over $\mathbb{Q}$.
2. The polynomial $x^2 - t$ is inseparable over the field $\mathbb{F}_2(t)$ (the rational functions of t over $\mathbb{F}_2$).

Definition

A polynomial $p(x) \in F[x]$ is called separable if it has no multiple roots. A polynomial which is not separable is called inseparable.

Example

1. The polynomial $x^2 - 2$ is separable over $\mathbb{Q}$. The polynomial $(x^2 - 2)^2$ is inseparable over $\mathbb{Q}$.
2. The polynomial $x^2 - t$ is inseparable over the field $\mathbb{F}_2(t)$ (the rational functions of t over $\mathbb{F}_2$).

Definition

The derivative of the polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$ is defined to be

$$D_x f(x) = \sum_{k=1}^{n} k a_k x^{k-1}.$$

Proposition

The polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative.

Proposition

The polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative.

Example

1. $\left(x^{p^n} - x\right)$ over $\mathbb{F}_p$ has derivative -1. Thus it is separable.
2. If $p|n$ then over $\mathbb{F}_p$, the polynomial $x^n - 1$ has multiple roots.

Proposition

The polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative.

Example

1. $(x^{p^n} - x)$ over $\mathbb{F}_p$ has derivative -1. Thus it is separable.
2. If $p|n$ then over $\mathbb{F}_p$, the polynomial $x^n - 1$ has multiple roots.

Corollary

Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proposition

Let F be a field of characteristic p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \qquad (ab)^p = a^p b^p,$$

that is the map $\phi(a) = a^p$ is an injective field homomorphism $F \to F$.

Proposition

Let F be a field of characteristic p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \qquad (ab)^p = a^p b^p,$$

that is the map $\phi(a) = a^p$ is an injective field homomorphism $F \to F$.

Definition

The map in the previous proposition is called the Frobenius endomorphism of F.

Proposition

Let F be a field of characteristic p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \qquad (ab)^p = a^p b^p,$$

that is the map $\phi(a) = a^p$ is an injective field homomorphism $F \to F$.

Definition

The map in the previous proposition is called the Frobenius endomorphism of F.

Corollary

Suppose that F is a finite field of characteristic p. Then every element of F is a p^{th} power in F.

Proposition

Every irreducible polynomial over a finite field F is separable. A polynomial in $F[x]$ is separable if and only if it is the product of irreducible polynomials in $F[x]$.

Definition

A field K of characteristic p is called <u>perfect</u> if every element of K is a p^{th} power in K.

Example

There is (up to ismomophism one) field of size p^n for any prime p and $n \in \mathbb{N}$.

Proposition

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ such that

$$p(x) = p_{sep}(x^{p^k}).$$

Proposition

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ such that

$$p(x) = p_{sep}(x^{p^k}).$$

Definition

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. The degree of $p_{\text{sep}}(x)$ is called the separable degree of $p(x)$, denoted $\deg_s p(x)$. The integer p^k is called the inseparable degree of $p(x)$, denoted $\deg_i p(x)$.

Proposition

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ such that

$$p(x) = p_{sep}(x^{p^k}).$$

Definition

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. The degree of $p_{\text{sep}}(x)$ is called the separable degree of $p(x)$, denoted $\deg_s p(x)$. The integer p^k is called the inseparable degree of $p(x)$, denoted $\deg_i p(x)$.

Definition

K/F is separable if every $\alpha \in K$ is the root of a separable polynomial in $F[x]$ (or equivalently, $\forall \alpha \in K$, $m_{F,\alpha}(x)$ is separable. Any field which is not separable is said to be inseparable.

Corollary

Every finite extension of a perfect field is separable. In particular, every extension of $\mathbb{Q}$ *or any finite field is separable.*