Algebraic Geometric Codes

Recitation 07

Shir Peleg

Tel Aviv University

April 5, 2022

Separable extensions

Definition 1

An irreducible polynomial f in $F[x]$ is separable if and only if it has distinct roots in any extension of F (that is if it may be factored in distinct linear factors over an algebraic closure of F).
Let E/F be a field extension. An element $\alpha \in E$ is separable over F if it is algebraic over F, and its minimal polynomial is separable. The extension E/F is separable if it contains only separable elements.

Separable extensions

Definition 1

An irreducible polynomial f in $F[x]$ is separable if and only if it has distinct roots in any extension of F (that is if it may be factored in distinct linear factors over an algebraic closure of F).
Let E/F be a field extension. An element $\alpha \in E$ is separable over F if it is algebraic over F, and its minimal polynomial is separable. The extension E/F is separable if it contains only separable elements.

- We only have inseparable extensions for fields with positive characteristics. So from now we assume $char(K) = p > 0$.

Separable extensions

Definition 1

An irreducible polynomial f in $F[x]$ is separable if and only if it has distinct roots in any extension of F (that is if it may be factored in distinct linear factors over an algebraic closure of F).
Let E/F be a field extension. An element $\alpha \in E$ is separable over F if it is algebraic over F, and its minimal polynomial is separable. The extension E/F is separable if it contains only separable elements.

- We only have inseparable extensions for fields with positive characteristics. So from now we assume $char(K) = p > 0$.
- If an irreducible $g \in F[x]$ is not separable then $g = h(x^{p^n})$, for an irreducible $h \in F[x]$.

Separable extensions

Claim 1.1

1. *If* α, β *are separable then* $K(\alpha, \beta)$ *is a separable extension.*
2. *If* $L = K(\alpha_1, \ldots, \alpha_n)$ *all separable then there is* $\alpha \in L$ *s.t.* $L = K(\alpha)$.

Separable extensions

Claim 1.1

1. *If* α, β *are separable then* $K(\alpha, \beta)$ *is a separable extension.*
2. *If* $L = K(\alpha_1, \ldots, \alpha_n)$ *all separable then there is* $\alpha \in L$ *s.t.* $L = K(\alpha)$.

Definition 2

Let L/K be a field extension. Define $L_{sep} = \{\alpha \in L \mid \alpha \text{ is separable over} K\}$. It holds that L_{sep}/K is a field extension. If L/K is normal then L_{sep}/K is normal.

Separable extensions

Claim 1.1

1. *If α, β are separable then $K(\alpha, \beta)$ is a separable extension.*
2. *If $L = K(\alpha_1, \dots, \alpha_n)$ all separable then there is $\alpha \in L$ s.t. $L = K(\alpha)$.*

Definition 2

Let L/K be a field extension. Define $L_{sep} = \{\alpha \in L \mid \alpha \text{ is separable over} K\}$. It holds that L_{sep}/K is a field extension. If L/K is normal then L_{sep}/K is normal.

Proof.

Let $\alpha, \beta \in L_{sep}$ from item 1 in the claim, it follows that $\alpha + \beta, \alpha \cdot \beta, \alpha - \beta, \alpha/\beta$ are separable $\in L_{sep}$.

Separable extensions

Claim 1.1

1. *If α, β are separable then $K(\alpha, \beta)$ is a separable extension.*
2. *If $L = K(\alpha_1, \ldots, \alpha_n)$ all separable then there is $\alpha \in L$ s.t. $L = K(\alpha)$.*

Definition 2

Let L/K be a field extension. Define $L_{sep} = \{\alpha \in L \mid \alpha \text{ is separable over} K\}$. It holds that L_{sep}/K is a field extension. If L/K is normal then L_{sep}/K is normal.

Proof.

Let $\alpha, \beta \in L_{sep}$ from item 1 in the claim, it follows that $\alpha + \beta, \alpha \cdot \beta, \alpha - \beta, \alpha/\beta$ are separable $\in L_{sep}$. The second fact follows from the fact that if α is separable so does all its conjugates. □

Purely Inseparable extensions

Claim 2.1

It holds that $L_{sep} = K \iff \forall\alpha \in L,\ p_\alpha = x - a$ *for some* $n \in \mathbb{N}$, $a \in K$.

Proof.

$\Rightarrow$ Let $\alpha \in L$. If $\alpha \in K$ then the claim holds for $n = 0$. If $\alpha \notin K$, then α is not separable over K. This implies that we can write $p_\alpha(x) = g(x^{p^n})$ (for maximal n). g is an irreducible separable polynomial, and one of its roots is $\alpha^{p^n} \in L$, and thus $\alpha^{p^n} \in K$. This implies that $p_\alpha | x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$. One can show that this implies that $p_\alpha = x^{p^k} - \alpha^{p^k}$. Thus $n = k$.

Purely Inseparable extensions

Claim 2.1

It holds that $L_{sep} = K \iff \forall \alpha \in L,\ p_\alpha = x - a$ *for some* $n \in \mathbb{N},\ a \in K$.

Proof.

$\Rightarrow$ Let $\alpha \in L$. If $\alpha \in K$ then the claim holds for $n = 0$. If $\alpha \notin K$, then α is not separable over K. This implies that we can write $p_\alpha(x) = g(x^{p^n})$ (for maximal n). g is an irreducible separable polynomial, and one of its roots is $\alpha^{p^n} \in L$, and thus $\alpha^{p^n} \in K$. This implies that $p_\alpha | x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$. One can show that this implies that $p_\alpha = x^{p^k} - \alpha^{p^k}$. Thus $n = k$.
$\Leftarrow$ Let $\alpha \in L$, $p_\alpha = x^{p^n} - a$, which is separable *iffn* $= 0$ and $\alpha = a \in K$. □

Purely Inseparable extensions

Claim 2.1

It holds that $L_{sep} = K \iff \forall \alpha \in L,\ p_\alpha = x - a$ *for some* $n \in \mathbb{N},\ a \in K$.

Proof.

$\Rightarrow$ Let $\alpha \in L$. If $\alpha \in K$ then the claim holds for $n = 0$. If $\alpha \notin K$, then α is not separable over K. This implies that we can write $p_\alpha(x) = g(x^{p^n})$ (for maximal n). g is an irreducible separable polynomial, and one of its roots is $\alpha^{p^n} \in L$, and thus $\alpha^{p^n} \in K$. This implies that $p_\alpha | x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$. One can show that this implies that $p_\alpha = x^{p^k} - \alpha^{p^k}$. Thus $n = k$.
$\Leftarrow$ Let $\alpha \in L$, $p_\alpha = x^{p^n} - a$, which is separable *iffn* $= 0$ and $\alpha = a \in K$. □

If L/K satisfies the previous items it is called purely inseparable.

Purely Inseparable extensions

Claim 2.2

L/L_{sep} is purely inseparable.

Purely Inseparable extensions

Claim 2.2

L/L_{sep} is purely inseparable.

Proof.

Let $\alpha \in L$. If α is separable over L_{sep} then it is separable over K and thus is in L_{sep}. □

Purely Inseparable extensions

Claim 2.2

L/L_{sep} is purely inseparable.

Proof.

Let $\alpha \in L$. If α is separable over L_{sep} then it is separable over K and thus is in L_{sep}. □

Claim 2.3

1. *L/K is purely inseparable implies that $[L : K]$ is a power of p.*
2. *$[L : K]/[L_{sep} : K]$ is a power of p.*

We denote $[L : K]_i = [L : K]/[L_{sep} : K]$, the inseparable degree of the extension.