Algebraic Geometric Codes

Recitation 02

Shir Peleg

Tel Aviv University

March 1, 2022

Filed Extensions

Definition

When we have a field that contains another field $F \subseteq E$, we say that E is a filed extension of F, and denote it by E/F.

For example $\mathbb{C}/\mathbb{R}, \mathbb{R}/\mathbb{Q}$.

Filed Extensions

Definition

When we have a field that contains another field $F \subseteq E$, we say that E is a filed extension of F, and denote it by E/F.

For example $\mathbb{C}/\mathbb{R}, \mathbb{R}/\mathbb{Q}$.

There are two ways to define such extensions: either we have the larger field E, and we find a subfield of it, or we add new elements to a given field F.
For example $F(x)$ the field of rational functions in the variable x over F.

Filed Extensions – degree

Let E/F, be a filed extension. It holds that E is a vector space over F. The dimension of E as a vector space over F is called the degree of the extension. It can be infinite.

Examples:

Filed Extensions – degree

Let E/F, be a filed extension. It holds that E is a vector space over F. The dimension of E as a vector space over F is called the degree of the extension. It can be infinite.

Examples:

- $\mathbb{C}/\mathbb{R}$ has degree 2, as we have the basis $\{1, i\}$.

Filed Extensions – degree

Let E/F, be a filed extension. It holds that E is a vector space over F. The dimension of E as a vector space over F is called the degree of the extension. It can be infinite.

Examples:

- $\mathbb{C}/\mathbb{R}$ has degree 2, as we have the basis $\{1, i\}$.
- $F(x)/F$ has infinite degree because the set $1, x, x^2, \ldots$ is linearly independent by definition.

Filed Extensions – degree

Let E/F, be a filed extension. It holds that E is a vector space over F. The dimension of E as a vector space over F is called the degree of the extension. It can be infinite.

Examples:

- $\mathbb{C}/\mathbb{R}$ has degree 2, as we have the basis $\{1, i\}$.
- $F(x)/F$ has infinite degree because the set $1, x, x^2, \ldots$ is linearly independent by definition.
- What is the degree of $\mathbb{R}/\mathbb{Q}$?

Filed Extensions – algebraic elements

Definition

Let E/F, b a filed extension. Let $\alpha \in E$, we say that α is algebraic over F if there is a polynomial $p_\alpha \in F[x]$ such that $p_\alpha(\alpha) = 0$.
We say that the extension E/F, is an algebraic extension if all the elements in E are algebraic over F.

Examples:

Filed Extensions – algebraic elements

Definition

Let E/F, b a filed extension. Let $\alpha \in E$, we say that α is algebraic over F if there is a polynomial $p_\alpha \in F[x]$ such that $p_\alpha(\alpha) = 0$.
We say that the extension E/F, is an algebraic extension if all the elements in E are algebraic over F.

Examples:

- $\mathbb{C}/\mathbb{R}$ is an algebraic extension, as for every element $\alpha = ai + b$ we have $p_\alpha = x^2 - 2bx - (b^2 + a^2)$.

Filed Extensions – algebraic elements

Definition

Let E/F, b a filed extension. Let $\alpha \in E$, we say that α is algebraic over F if there is a polynomial $p_\alpha \in F[x]$ such that $p_\alpha(\alpha) = 0$.
We say that the extension E/F, is an algebraic extension if all the elements in E are algebraic over F.

Examples:

- $\mathbb{C}/\mathbb{R}$ is an algebraic extension, as for every element $\alpha = ai + b$ we have $p_\alpha = x^2 - 2bx - (b^2 + a^2)$.
- $F(y)/F$ is not an algebraic extension as y is not algebraic over F.

Filed Extensions – algebraic elements

Definition

Let E/F, b a filed extension. Let $\alpha \in E$, we say that α is algebraic over F if there is a polynomial $p_\alpha \in F[x]$ such that $p_\alpha(\alpha) = 0$.
We say that the extension E/F, is an algebraic extension if all the elements in E are algebraic over F.

Examples:

- $\mathbb{C}/\mathbb{R}$ is an algebraic extension, as for every element $\alpha = ai + b$ we have $p_\alpha = x^2 - 2bx - (b^2 + a^2)$.
- $F(y)/F$ is not an algebraic extension as y is not algebraic over F.
- Fact: Let E/F, K/E be algebraic extensions then K/F is algebraic.

Algebraic (in)dependence

Definition

Let E/F be a field extension. A subset $S \subseteq E$ is called *algebraically dependent* over F if there is a subset $s_1, \ldots, s_n \subseteq S$ and a non zero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.

Algebraic (in)dependence

Definition

Let E/F be a field extension. A subset $S \subseteq E$ is called *algebraically dependent* over F if there is a subset $s_1, \ldots, s_n \subseteq S$ and a non zero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.

Example: $E = F[x, y]/(y - x^2 - 1)$, the set $\{x, y\}$ is algebraically dependent.

Algebraic (in)dependence

Definition

Let E/F be a field extension. A subset $S \subseteq E$ is called *algebraically dependent* over F if there is a subset $s_1, \ldots, s_n \subseteq S$ and a non zero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.

Example: $E = F[x, y]/(y - x^2 - 1)$, the set $\{x, y\}$ is algebraically dependent.
Note that is $s_1, \ldots, s_n$ are algebraically independent then $F(s_1, \ldots, s_n) \cong F(x_1, \ldots, x_n)$.

Algebraic (in)dependence

Definition

Let E/F be a field extension. A subset $S \subseteq E$ is called *algebraically dependent* over F if there is a subset $s_1, \ldots, s_n \subseteq S$ and a non zero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.

Example: $E = F[x, y]/(y - x^2 - 1)$, the set $\{x, y\}$ is algebraically dependent.
Note that is $s_1, \ldots, s_n$ are algebraically independent then $F(s_1, \ldots, s_n) \cong F(x_1, \ldots, x_n)$.

Definition

Let E/F be a field extension. A transcendental basis of E over F is a maximal subset if E that is algebraically independent over F.

Transcendental Extensions

Claim

Let E/F be a field extension, and S be an algebraically independent set, and let $a \in E$. Then $S \cup \{a\}$ is algebraically dependent $\iff$ a is algebraic over $F(S)$.

Proof.

Transcendental Extensions

Claim

Let E/F be a field extension, and S be an algebraically independent set, and let $a \in E$. Then $S \cup \{a\}$ is algebraically dependent $\iff$ a is algebraic over $F(S)$.

Proof.

$\Rightarrow$ As S is algebraically independent and $S \cup \{a\}$ is algebraically dependent there are $s_1, \ldots, s_n \in S$, and $f \in F[x_1, \ldots, x_n, x_{n+1}]$ s.t. $f(s_1, \ldots, s_n, a) = 0$. We can define $f_a = f(s_1, \ldots, s_n, x)$. Note that f_a is note identically zero, thus $f_a \in F(S)[x]$, and $f_a(a) = 0$. The other direction is similar. □

Transcendental Extensions

Corollary

Let E/F be a field extension, and S be an algebraically independent set. Then S is a transcendental basis of E/F iff $E/F(S)$ is algebraic.

Theorem

Let E/F be a field extension. Assume E has a finite transcendental basis, then any transcendental bases have the same size.

Proof

Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be two transcendental bases, we will show that $m \leq n$, which, after changing the order, will result in $m = n$.

Transcendental Extensions

Corollary

Let E/F be a field extension, and S be an algebraically independent set. Then S is a transcendental basis of E/F iff $E/F(S)$ is algebraic.

Theorem

Let E/F be a field extension. Assume E has a finite transcendental basis, then any transcendental bases have the same size.

Proof

Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be two transcendental bases, we will show that $m \leq n$, which, after changing the order, will result in $m = n$.
b_1 is algebraic over $F(a_1, \ldots, a_n)$. So there is a non-zero polynomial p such that $p(b_1, a_1, \ldots, a_n) = 0$.

Transcendental Extensions

Proof Cont.

b_1 is algebraic over $F(a_1, \ldots, a_n)$. So there is a non-zero polynomial p such that $p(b_1, a_1, \ldots, a_n) = 0$. b_1 must appear somewhere in the polynomial, so must some a_i. Without loss of generality, we can assume a_1 appears in $p(b_1, a_1, \ldots, a_n)$. So a_1 is algebraic over $F(b_1, a_2, \ldots, a_n)$. Thus so does E.

Transcendental Extensions

Proof Cont.

b_1 is algebraic over $F(a_1, \ldots, a_n)$. So there is a non-zero polynomial p such that $p(b_1, a_1, \ldots, a_n) = 0$. b_1 must appear somewhere in the polynomial, so must some a_i. Without loss of generality, we can assume a_1 appears in $p(b_1, a_1, \ldots, a_n)$. So a_1 is algebraic over $F(b_1, a_2, \ldots, a_n)$. Thus so does E.
Once we have that E is algebraic over $F(b_1, \ldots, b_r, a_{r+1}, \ldots, a_n)$, we again "exchange" an a_i for a b_j. b_{r+1} is algebraic over the field $F(b_1, \ldots, b_r, a_{r+1}, \ldots, a_n)$. So there is a non-zero polynomial p s.t. $p(b_1, \ldots, b_{r+1}, a_{r+1}, \ldots, a_n) = 0$. Since the b_i's are algebraically independent, one of the a_i's, WLOG a_{r+1}, appears in this expression.

Transcendental Extensions

Proof Cont.

b_1 is algebraic over $F(a_1, \ldots, a_n)$. So there is a non-zero polynomial p such that $p(b_1, a_1, \ldots, a_n) = 0$. b_1 must appear somewhere in the polynomial, so must some a_i. Without loss of generality, we can assume a_1 appears in $p(b_1, a_1, \ldots, a_n)$. So a_1 is algebraic over $F(b_1, a_2, \ldots, a_n)$. Thus so does E.
Once we have that E is algebraic over $F(b_1, \ldots, b_r, a_{r+1}, \ldots, a_n)$, we again "exchange" an a_i for a b_j. b_{r+1} is algebraic over the field $F(b_1, \ldots, b_r, a_{r+1}, \ldots, a_n)$. So there is a non-zero polynomial p s.t. $p(b_1, \ldots, b_{r+1}, a_{r+1}, \ldots, a_n) = 0$. Since the b_i's are algebraically independent, one of the a_i's, WLOG a_{r+1}, appears in this expression.
We get that E is algebraic over $F(b_1, \ldots, b_{r+1}, a_{r+2}, \ldots, a_n)$. When this process terminates we see that E is algebraic over $F(b_1, \ldots, b_m, a_{m+1}, \ldots, a_n)$. Hence $m \leq n$.

Transcendental Extensions

Definition

The *transcendence degree* of E/F is the size of its transcendental bases. It is denoted by $tr(E/F)$ or $t.deg(E/F)$.

Definition

E/F is called *purely transcendental* if $E = F(S)$ where S is a transcendental basis of E/F.

Claim

Let E/F, K/E be field extensions, then
$t.deg(K/F) = t.deg(E/F) + t.deg(K/E)$.

What is the *t.deg* of the following fields?

What is the *t.deg* of the following fields?

- $F(x)/F$?

What is the *t.deg* of the following fields?

- $F(x)/F$? $F(x_1, \ldots, x_n)/F$?

What is the *t.deg* of the following fields?

- $F(x)/F$? $F(x_1, \ldots, x_n)/F$?
- $\mathbb{C}/\mathbb{R}$?

What is the *t.deg* of the following fields?

- $F(x)/F$? $F(x_1, \ldots, x_n)/F$?
- $\mathbb{C}/\mathbb{R}$?
- $\mathbb{R}/\mathbb{Q}$?

What is the $t.deg$ of the following fields?

- $F(x)/F$? $F(x_1, \dots, x_n)/F$?
- $\mathbb{C}/\mathbb{R}$?
- $\mathbb{R}/\mathbb{Q}$?
- $Frac(F(x,y)/P(x,y))/F$ where P is irreducible?

Reminders - Galois theory

Definition

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.

Reminders - Galois theory

Definition

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.

- $x^2 + 1$ is a separable polynomial over $\mathbb{R}$. $\mathbb{C}/\mathbb{R}$ is a separable extension.

Reminders - Galois theory

Definition

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.

- $x^2 + 1$ is a separable polynomial over $\mathbb{R}$. $\mathbb{C}/\mathbb{R}$ is a separable extension.
- $x^p - t^p$ is not a separable polynomial over $\mathbb{F}_p(t^p)$. As, $x^p - t^p = (x - t)^p$. Thus the extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is not separable.

Reminders - Galois theory

Definition

The algebraic field extension E/F is normal (we also say that E is normal over F) if every irreducible polynomial over F that has at least one root in E splits over E. In other words, if $\alpha \in L$, then all conjugates of α over F (that is, all roots of the minimal polynomial of α over F) belong to E.

Definition

E/K is called a *Galois extension* if E/K is normal and separable.