Algebraic Geometric Codes

Recitation 06

Shir Peleg

Tel Aviv University

March 29, 2022

Remainders: Galois Definitions

Definition 1

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 2

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

Definition 3

Let $f \in K[x]$ and let $\alpha, \beta \in \overline{K}$ s.t. $f(\alpha) = f(\beta) = 0$ then α, β are called conjugates.

Algebraic Closure

In this course, we always think of algebraic extensions as fields inclusion. We extend this assumption in the following way: For a field K, we assume there is a unique field $\overline{K}$ which is **the** algebraic closure of K (i.e, a field that is an algebraic extension of K and is algebraically closed).

Algebraic Closure

In this course, we always think of algebraic extensions as fields inclusion. We extend this assumption in the following way: For a field K, we assume there is a unique field $\overline{K}$ which is **the** algebraic closure of K (i.e, a field that is an algebraic extension of K and is algebraically closed).
Remark: The algebraic closure is unique up to Isomorphism.

Algebraic Closure

In this course, we always think of algebraic extensions as fields inclusion. We extend this assumption in the following way: For a field K, we assume there is a unique field $\overline{K}$ which is **the** algebraic closure of K (i.e, a field that is an algebraic extension of K and is algebraically closed).
Remark: The algebraic closure is unique up to Isomorphism.
Thus for every algebraic extension L/K, we can have that $K \subseteq L \subseteq \overline{K}$.

Algebraic Closure

In this course, we always think of algebraic extensions as fields inclusion. We extend this assumption in the following way: For a field K, we assume there is a unique field $\overline{K}$ which is **the** algebraic closure of K (i.e, a field that is an algebraic extension of K and is algebraically closed).
Remark: The algebraic closure is unique up to Isomorphism.
Thus for every algebraic extension L/K, we can have that $K \subseteq L \subseteq \overline{K}$.
We can consider the following set:

$$Ism_K(L) = \{\sigma|_L \mid \sigma : \overline{K} \to \overline{K}, \text{ s.t. } \forall x \in K, \sigma(x) = x\}.$$

This set is also a group.

Automorphisms

Let L/K be an algebriac extension. We denote by $Aut(L/K)$ the group of all automorphisms of L/K, that are: $\sigma : L \to L$ field isomorphism with $\forall x \in K, \sigma(x) = x$.

Automorphisms

Let L/K be an algebriac extension. We denote by $Aut(L/K)$ the group of all automorphisms of L/K, that are: $\sigma : L \to L$ field isomorphism with $\forall x \in K, \sigma(x) = x$.

Example 4

$L = \mathbb{Q}(\sqrt{2})$, define $\sigma(\sqrt{2}) = -\sqrt{2}$. Then $\sigma \in Aut(L/\mathbb{Q})$.

Automorphisms

Let L/K be an algebriac extension. We denote by $Aut(L/K)$ the group of all automorphisms of L/K, that are: $\sigma : L \to L$ field isomorphism with $\forall x \in K, \sigma(x) = x$.

Example 4

$L = \mathbb{Q}(\sqrt{2})$, define $\sigma(\sqrt{2}) = -\sqrt{2}$. Then $\sigma \in Aut(L/\mathbb{Q})$.

Theorem 5

Let $L_1, L_2/K$ and let $\varphi : L_1 \to L_2$ be a isomorphism over K, then there is $\sigma \in Aut(\overline{K}/K)$ with $\sigma|_{L_1} = \varphi$.

Automorphisms

Let L/K be an algebriac extension. We denote by $Aut(L/K)$ the group of all automorphisms of L/K, that are: $\sigma : L \to L$ field isomorphism with $\forall x \in K, \sigma(x) = x$.

Example 4

$L = \mathbb{Q}(\sqrt{2})$, define $\sigma(\sqrt{2}) = -\sqrt{2}$. Then $\sigma \in Aut(L/\mathbb{Q})$.

Theorem 5

Let $L_1, L_2/K$ and let $\varphi : L_1 \to L_2$ be a isomorphism over K, then there is $\sigma \in Aut(\overline{K}/K)$ with $\sigma|_{L_1} = \varphi$.

Corollary 6

$Aut(L/K) \subseteq Ism_K(L)$.

Normal extensions and embeddings

Claim 6.1

Let $\alpha \in L/K$, and let $\sigma \in Ism_K(L)$. It holds that $\alpha, \sigma(\alpha)$ are conjugates.

Normal extensions and embeddings

Claim 6.1

Let $\alpha \in L/K$, and let $\sigma \in Ism_K(L)$. It holds that $\alpha, \sigma(\alpha)$ are conjugates.

Proof.

Let $f = f_\alpha$, its minimal polynomial. It holds that $\sigma(0) = 0$ and thus $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, and therefore $\alpha, \sigma(\alpha)$ are conjugates. □

Normal extensions and embeddings

Claim 6.1

Let $\alpha \in L/K$, and let $\sigma \in Ism_K(L)$. It holds that $\alpha, \sigma(\alpha)$ are conjugates.

Proof.

Let $f = f_\alpha$, its minimal polynomial. It holds that $\sigma(0) = 0$ and thus $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, and therefore $\alpha, \sigma(\alpha)$ are conjugates. □

Theorem 7

Let L/K be an algebraic extension and assume $L \subseteq \overline{K}$. TFAE

1. *L/K is normal.*
2. *L is the splitting field of some $\{f_\alpha(x) \in \mathbb{K}[x]\}_\alpha$.*
3. *Every $\sigma \in Ism_K(L)$ satisfies $\sigma(L) = L$.*

Normal Extensions

Proof.

We will only show 1 $\iff$ 3.

Normal Extensions

Proof.

We will only show $1 \iff 3$.

$1 \to 3$: Let $\sigma \in Ism_K(L)$, let $\alpha \in L$. we want to show that $\sigma(\alpha) \in L$. From the previous claim it follows that $\sigma(\alpha), \alpha$ are conjugates, and as $\alpha \in L$ and L is normal, $\sigma(\alpha) \in L$. The other inclusion follows from a stronger property (uniqueness of splitting fields).

Normal Extensions

Proof.

We will only show $1 \iff 3$.

$1 \to 3$: Let $\sigma \in Ism_K(L)$, let $\alpha \in L$. we want to show that $\sigma(\alpha) \in L$. From the previous claim it follows that $\sigma(\alpha), \alpha$ are conjugates, and as $\alpha \in L$ and L is normal, $\sigma(\alpha) \in L$. The other inclusion follows from a stronger property (uniqueness of splitting fields).

$3 \Rightarrow 1$, we want to show that if $p \in K[x]$ is irreducible and has a root $\alpha \in L$, then all the roots of p are in L. Let $\beta \in \overline{K}$ be another root of p.

Normal Extensions

Proof.

We will only show $1 \iff 3$.

$1 \to 3$: Let $\sigma \in Ism_K(L)$, let $\alpha \in L$. we want to show that $\sigma(\alpha) \in L$. From the previous claim it follows that $\sigma(\alpha), \alpha$ are conjugates, and as $\alpha \in L$ and L is normal, $\sigma(\alpha) \in L$. The other inclusion follows from a stronger property (uniqueness of splitting fields).

$3 \Rightarrow 1$, we want to show that if $p \in K[x]$ is irreducible and has a root $\alpha \in L$, then all the roots of p are in L. Let $\beta \in \overline{K}$ be another root of p. It holds that

$$K(\alpha) \cong K[x]/(p) \cong K(\beta).$$

Note that this is an iso over K, from the claim, there is $\sigma \in Ism_K(L)$ with $\sigma|_{K(\alpha)}(K(\alpha)) = K(\beta)$, and as $\sigma(L) = L$ it follows that $\beta \in K(\beta) \subseteq L$. □

Ism = Aut

Corollary 8

If L is normal then $Ism_K(L) = Aut(L/K)$.

Definition 9

Let $H \subseteq Aut(L/K)$ be a subgroup of automorhisms. We denote

$$L^H = \{\alpha \in L \mid \forall \sigma \in H, \sigma(\alpha) = \alpha.\}$$

Finite fields

Theorem 10

1. *Consider* $\overline{\mathbb{F}}_q$. *Let* $\varphi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$, *with* $\varphi_q(x) = x^q$. *Then* $\varphi_q \in Aut(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.
2. *It holds that* $Aut(\mathbb{F}_{q^n}/\mathbb{F}_q) = (\varphi_q^i \mid i \in [n])$.

Finite fields

Theorem 10

1. *Consider* $\overline{\mathbb{F}}_q$. *Let* $\varphi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$, *with* $\varphi_q(x) = x^q$. *Then* $\varphi_q \in Aut(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.
2. *It holds that* $Aut(\mathbb{F}_{q^n}/\mathbb{F}_q) = (\varphi_q^i \mid i \in [n])$.

Proof.

1. Follows from the fact that $char(\mathbb{F}_q) \mid q$, and that $\forall x \in \mathbb{F}_q, x^q = x$.
2. It holds that $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, and thus it can not be that $\varphi_q^i = id$ for $i \leq n$.

□

Separable extensions

Definition 11

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 11

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.

Separable extensions

Definition 11

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.

Separable extensions

Claim 11.1

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. $L = K(\alpha)$.*

Trace and Norm

Let $\alpha \in \overline{K}$. We define the following linear map $\alpha : K(\alpha) \to K(\alpha)$, $\alpha(x) = \alpha \cdot x$. We define $Tr(\alpha) = Tr(M_\alpha), Norm(\alpha) = det(M_\alpha)$.

Claim 11.2

Denote the minimal polynomail of α, $p_\alpha = \sum_{i=1}^{n} a_i x^i$.

$$Tr(\alpha) = -a_{n-1} = \sum_{\sigma \in Ism_K(L)} \sigma(\alpha),$$

$$Norm(\alpha) = (-1)^n a_0 = \prod_{\sigma \in Ism_K(L)} \sigma(\alpha).$$

Trace and Norm

Proof.

Consider the basis $1, \alpha, \ldots, \alpha^{n-1}$ of $K(\alpha)/K$.

$$M_\alpha = \begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & -a_{n-1} \end{bmatrix}$$

Trace and Norm

Proof.

Consider the basis $1, \alpha, \ldots, \alpha^{n-1}$ of $K(\alpha)/K$.

$$M_\alpha = \begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & -a_{n-1} \end{bmatrix}$$

The First equalities follows from this representation.

Trace and Norm

Proof.

Consider the basis $1, \alpha, \ldots, \alpha^{n-1}$ of $K(\alpha)/K$.

$$M_\alpha = \begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & -a_{n-1} \end{bmatrix}$$

The First equalities follows from this representation. The second equalities follows from the fact that

$$p_\alpha(x) = \prod_{\sigma \in Ism_K(L)} (x - \sigma(\alpha)).$$