Algebraic Geometric Codes

Recitation 11

Shir Peleg

Tel Aviv University

May 17, 2022

Cyclic extensions

Recall that a Galois extension F/K is called *cyclic* if $\mathrm{Gal}(F/K)$ is a cyclic group.

Cyclic extensions

Recall that a Galois extension F/K is called *cyclic* if $\mathrm{Gal}(F/K)$ is a cyclic group.

Lemma 1

Let F be a field of characteristic p. Let n coprime to p. Let $\zeta \in \bar{F}$ be an n-th primitive root of unity. Then, $F(\zeta)/F$ is a cyclic extension.

Cyclic extensions

Recall that a Galois extension F/K is called *cyclic* if $\mathrm{Gal}(F/K)$ is a cyclic group.

Lemma 1

Let F be a field of characteristic p. Let n coprime to p. Let $\zeta \in \bar{F}$ be an n-th primitive root of unity. Then, $F(\zeta)/F$ is a cyclic extension.

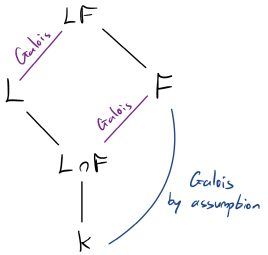
For the proof of Lemma 1 we recall the following lemma from Galois Theory.

Cyclic extensions

Lemma 2

Let $K \subseteq L, F$ be fields s.t. F/K is a finite Galois extension. Then LF/L is Galois and

$$\mathrm{Gal}(LF/L) \cong \mathrm{Gal}(F/(L \cap F)).$$ *In particular,* $[LF : L] = [F : L \cap F]$.



Cyclic extensions

Proof of Lemma 2

We first show that LF/L is Galois.

Cyclic extensions

Proof of Lemma 2

We first show that LF/L is Galois.
The separability of LF/L is clear. Indeed, every element of F is separable over K, let alone over L. Thus, every element of LF is separable over L.

Proof of Lemma 2

We first show that LF/L is Galois.
The separability of LF/L is clear. Indeed, every element of F is separable over K, let alone over L. Thus, every element of LF is separable over L.
As for normality, recall the characterization of normal extensions as splitting fields. Now, as F/K is normal, F is the splitting field of

$$\{f_j(x) \in K[x]\}_{j\in J}.$$

Let $S_j \subseteq K$ be the roots of $f_j(x)$, and $S = \cup_j S_j$. Then, $F = K(S)$. But then,

$$LF = L(S)$$

is the splitting field of $\{f_j(x)\}_{j\in J}$ where $f_j(x) \in L[x]$. Hence, LF/L is normal.

Cyclic extensions

Proof of Lemma 2

As F/K is finite and separable, $F = K(a)$ for some $a \in F$.

Cyclic extensions

Proof of Lemma 2

As F/K is finite and separable, $F = K(a)$ for some $a \in F$.
Let $f(x) \in K[x]$ be the minimal polynomial of a over K. Since F/K is Galois, $f(x)$ splits completely in F and all its roots are simple.

Proof of Lemma 2

As F/K is finite and separable, $F = K(a)$ for some $a \in F$.
Let $f(x) \in K[x]$ be the minimal polynomial of a over K. Since F/K is Galois, $f(x)$ splits completely in F and all its roots are simple.
Let $g(x) \in L[x]$ be the minimal polynomial of a over L. Since $K \subseteq L$ we have that $g(x) \mid f(x)$.

Proof of Lemma 2

As F/K is finite and separable, $F = K(a)$ for some $a \in F$.
Let $f(x) \in K[x]$ be the minimal polynomial of a over K. Since F/K is Galois, $f(x)$ splits completely in F and all its roots are simple.
Let $g(x) \in L[x]$ be the minimal polynomial of a over L. Since $K \subseteq L$ we have that $g(x) \mid f(x)$.
Thus the roots of $g(x)$ is a subset of the roots of $f(x)$ and so they are in F.
This implies that $g(x) \in F[x]$, and so $g(x) \in (L \cap F)[x]$. Now,

$$LF = LK(a) = L(a),$$

and so

$$[LF : L] = [L(a) : L] = \deg g(x). \tag{1}$$

Cyclic extensions

Proof of Lemma 2

$g(x)$ is irreducible over L and so certainly over $L \cap F$. Thus,

$$\deg g(x) = [(L \cap F)(a) : L \cap F].$$

Proof of Lemma 2

$g(x)$ is irreducible over L and so certainly over $L \cap F$. Thus,

$$\deg g(x) = [(L \cap F)(a) : L \cap F].$$

As $a \in F$, $(L \cap F)(a) \subseteq F$.

Proof of Lemma 2

$g(x)$ is irreducible over L and so certainly over $L \cap F$. Thus,

$$\deg g(x) = [(L \cap F)(a) : L \cap F].$$

As $a \in F$, $(L \cap F)(a) \subseteq F$. On the other hand,

$$F = K(a) \subseteq (L \cap F)(a),$$

and so $(L \cap F)(a) = F$.

Proof of Lemma 2

$g(x)$ is irreducible over L and so certainly over $L \cap F$. Thus,

$$\deg g(x) = [(L \cap F)(a) : L \cap F].$$

As $a \in F$, $(L \cap F)(a) \subseteq F$. On the other hand,

$$F = K(a) \subseteq (L \cap F)(a),$$

and so $(L \cap F)(a) = F$. Hence, $\deg g(x) = [F : L \cap F]$. With Equation (1), we get

$$[LF : L] = [F : L \cap F].$$

Proof of Lemma 2.

Note that $F/(L \cap F)$ is Galois as F/K is Galois and $K \subseteq L \cap F$.

Proof of Lemma 2.

Note that $F/(L \cap F)$ is Galois as F/K is Galois and $K \subseteq L \cap F$.
Consider the restriction homomorphism

$$\varphi : \mathrm{Gal}(LF/L) \to \mathrm{Gal}(F/(L \cap F))$$
$$\sigma \mapsto \sigma|_F$$

φ is a monomorphism. Indeed, assume that $\varphi(\sigma) = \sigma|_F = \mathrm{id}|_F$. As $\sigma|_L = \mathrm{id}|_L$ we have that $\sigma = \mathrm{id}_{LF}$.

Proof of Lemma 2.

Note that $F/(L \cap F)$ is Galois as F/K is Galois and $K \subseteq L \cap F$.
Consider the restriction homomorphism

$$\varphi : \mathrm{Gal}(LF/L) \to \mathrm{Gal}(F/(L \cap F))$$
$$\sigma \mapsto \sigma|_F$$

φ is a monomorphism. Indeed, assume that $\varphi(\sigma) = \sigma|_F = \mathrm{id}|_F$. As $\sigma|_L = \mathrm{id}|_L$ we have that $\sigma = \mathrm{id}_{LF}$.
As

$$|\mathrm{Gal}(LF/L)| = [LF : L] = [F : L \cap F] = |\mathrm{Gal}(F/(L \cap F))|$$

we have that φ is also onto. Thus, $\mathrm{Gal}(LF/L) \cong \mathrm{Gal}(F/(L \cap F))$. □

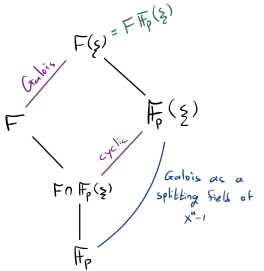
Cyclic extensions

Proof of Lemma 1

We have that

$$F(\zeta) = F\mathbb{F}_p(\zeta).$$

Now $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ is Galois as it is the splitting field of the separable polynomial $x^n - 1$ over $\mathbb{F}_p$.



Proof of Lemma 1

By Lemma 2, $F(\zeta)/F$ is Galois.

Proof of Lemma 1

By Lemma 2, $F(\zeta)/F$ is Galois. Moreover,

$$\mathrm{Gal}(F(\zeta)/F) \cong \mathrm{Gal}(\mathbb{F}_p(\zeta)/(F \cap \mathbb{F}_p(\zeta))).$$

Cyclic extensions

Proof of Lemma 1

By Lemma 2, $F(\zeta)/F$ is Galois. Moreover,

$$\mathrm{Gal}(F(\zeta)/F) \cong \mathrm{Gal}(\mathbb{F}_p(\zeta)/(F \cap \mathbb{F}_p(\zeta))).$$

The RHS is a Galois extension of finite fields and as such it is cyclic (generated by the Frobenoius automorphism). Thus, $F(\zeta)/F$ is cyclic.

Cyclic extensions

Theorem 3

Let E be a field of characteristic p. Let F/E be a field extension of degree n which is coprime to p. Assume that E contains an n-th primitive root of unity. Then,

$$\begin{aligned} F/E \text{ is cyclic} &\iff F = E(a) \text{ for some } a \in F \text{ s.t. } b := a^n \in E \\ &\iff F \text{ is the splitting field of } x^n - b \in E[x]. \end{aligned}$$

Proof

Assume that $F = E(a)$ for $b = a^n \in E$. Then,

$$x^n - b = x^n - a^n = \prod_{\zeta \in \mu_n} (x - \zeta a),$$

where $\mu_n \subseteq E$ is the set of n-th roots of unity.

Cyclic extensions

Proof

Hence, F is the splitting field over E of the separable polynomial $x^n - b$. The separability follows as p and n are coprime, and F/E is Galois.

Proof

Hence, F is the splitting field over E of the separable polynomial $x^n - b$. The separability follows as p and n are coprime, and F/E is Galois.
As we assume that $[F : E] = [E(a) : E] = n$, $x^n - b$ is the minimal polynomial of a over E. Thus, $\{\zeta a \mid \zeta \in \mu_n\}$ are the E-conjugates of a.

Proof

Hence, F is the splitting field over E of the separable polynomial $x^n - b$. The separability follows as p and n are coprime, and F/E is Galois.
As we assume that $[F : E] = [E(a) : E] = n$, $x^n - b$ is the minimal polynomial of a over E. Thus, $\{\zeta a \mid \zeta \in \mu_n\}$ are the E-conjugates of a.
An element $\sigma \in \mathrm{Gal}(F/E)$ is determined by its action on a. Note that $\sigma(a)$ is also a root of $x^n - b$. Thus, $\sigma(a) := \sigma_\zeta(a) = \zeta a$ for some $\zeta \in \mu_n$

Proof

Hence, F is the splitting field over E of the separable polynomial $x^n - b$. The separability follows as p and n are coprime, and F/E is Galois.
As we assume that $[F : E] = [E(a) : E] = n$, $x^n - b$ is the minimal polynomial of a over E. Thus, $\{\zeta a \mid \zeta \in \mu_n\}$ are the E-conjugates of a.
An element $\sigma \in \mathrm{Gal}(F/E)$ is determined by its action on a. Note that $\sigma(a)$ is also a root of $x^n - b$. Thus, $\sigma(a) := \sigma_\zeta(a) = \zeta a$ for some $\zeta \in \mu_n$
For every conjugate ζa there is $\sigma_\zeta \in \mathrm{Gal}(F/E)$ s.t. $\sigma_\zeta(a) = \zeta a$. Thus,

$$\mathrm{Gal}(F/E) = \{\sigma_\zeta \mid \zeta \in \mu_n\}.$$

Cyclic extensions

Proof

Moreover, the map

$$\mu_n \to \mathrm{Gal}(F/E) = \{\sigma_\zeta \mid \zeta \in \mu_n\}$$
$$\zeta \mapsto \sigma_\zeta$$

is a group isomorphism as can be easily verified. Thus, F/E is cyclic.
In the other direction, assume F/E is cyclic and we ought to find $a \in F$ s.t. $a^n \in E$ and $F = E(a)$.

Proof

Moreover, the map

$$\begin{aligned} \mu_n &\to \mathrm{Gal}(F/E) = \{\sigma_\zeta \mid \zeta \in \mu_n\} \\ \zeta &\mapsto \sigma_\zeta \end{aligned}$$

is a group isomorphism as can be easily verified. Thus, F/E is cyclic.
In the other direction, assume F/E is cyclic and we ought to find $a \in F$ s.t. $a^n \in E$ and $F = E(a)$.
Let σ be a generator of the cyclic group $\mathrm{Gal}(F/E)$. It can be shown that the elements of $\mathrm{Gal}(F/E)$ are linearly independent over E (even over $\bar{E}$). thus,

$$\psi = \sum_{j=0}^{n-1} \zeta^j \sigma^j \neq 0,$$

Cyclic extensions

Proof

Let t be s.t. $\psi(t) \neq 0$, and let

$$a := \psi(t) = \sum_{j=0}^{n-1} \zeta^j \sigma^j(t).$$

We will show that $F = E(a)$ and that $a^n \in E$.

Cyclic extensions

Proof

Let t be s.t. $\psi(t) \neq 0$, and let

$$a := \psi(t) = \sum_{j=0}^{n-1} \zeta^j \sigma^j(t).$$

We will show that $F = E(a)$ and that $a^n \in E$.
As $\zeta \in E$ we have that

$$\begin{aligned}\sigma(a) &= \sum_{j=0}^{n-1} \zeta^j \sigma^{j+1}(t) = \zeta^{-1} \sum_{j=0}^{n-1} \zeta^{j+1} \sigma^{j+1}(t) = \zeta^{-1} \sum_{j=0}^{n-1} \zeta^j \sigma^j(t) \\ &= \zeta^{-1} a.\end{aligned}$$

Proof.

So $\sigma(a) = \zeta^{-1}a$ and so the E-Galois conjugates of a are

$$\left\{a, \zeta^{-1}a, \ldots, (\zeta^{-1})^{n-1}a\right\} = \left\{a, \zeta a, \ldots, \zeta^{n-1}a\right\}.$$

Thus, the minimal polynomial of a over E is

$$f(x) = \prod_{j=0}^{n-1}(x - \zeta^j a) = x^n - a^n \in E[x].$$

Thus, $F = E(a)$ and $a^n \in E$. □

Technical lemma

Lemma 4

Assume F/E is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.

Technical lemma

Lemma 4

Assume F/E is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.
Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.

Technical lemma

Lemma 4

Assume F/E is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.
Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.
Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*
2. $\pi(y) \in F_{\mathfrak{P},s}$.

Technical lemma

Lemma 4

Assume F/E is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.
Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.
Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*
2. $\pi(y) \in F_{\mathfrak{P},s}$.

Then,

$$\pi\left(Tr_{F/E}(y)\right) = e(\mathfrak{P}/\mathfrak{p}) \cdot Tr_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}(\pi(y)).$$

Technical lemma

Lemma 5

Assume F/E is Galois. Function field over a perfect field.

Technical lemma

Lemma 5

Assume F/E is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.

Technical lemma

Lemma 5

Assume F/E is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$. Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*

Technical lemma

Lemma 5

Assume F/E is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of F lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$. Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*

Then,

$$\pi\left(Tr_{F/E}(y)\right) = e(\mathfrak{P}/\mathfrak{p}) \cdot Tr_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(\pi(y)).$$

Proof of 5

Proof

Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.

Proof of 5

Proof

Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.

Proof of 5

Proof

Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that

Proof of 5

Proof

Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that
$v_{\mathfrak{P}'}(y) > 0$ and so $v_{\sigma_i^{-1}\mathfrak{P}}(y) > 0$, and so

$$v_{\mathfrak{P}}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) > 0 \quad \Longrightarrow \quad \sigma y \in \mathcal{O}_{\mathfrak{P}} \text{ and } \pi(\sigma y) = 0.$$

Proof of 5

Proof

Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that
$v_{\mathfrak{P}'}(y) > 0$ and so $v_{\sigma_i^{-1}\mathfrak{P}}(y) > 0$, and so

$$v_{\mathfrak{P}}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) > 0 \quad \Longrightarrow \quad \sigma y \in \mathcal{O}_{\mathfrak{P}} \text{ and } \pi(\sigma y) = 0.$$

$$\begin{aligned} \pi(Tr_{F/E}(y)) &= \sum_{i=1}^{n} \pi(\sigma_i(y)) = \sum_{\sigma_i \in \mathcal{D}} \pi(\sigma_i(y)) \\ &= \sum_{\alpha \in Aut(F_{\mathfrak{P}}/E_p)} |\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| \cdot \alpha(\pi(y)). \end{aligned}$$

Proof of 5

Proof

Recall

$$|\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| = I(\mathfrak{P}/\mathfrak{p}).$$

And

$$e(\mathfrak{P}/p) = \frac{[F : E]_i}{[F_{\mathfrak{P}} : E_{\mathfrak{p}}]_i} I(\mathfrak{P}/\mathfrak{p}).$$

Proof of 5

Proof

Recall

$$|\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| = I(\mathfrak{P}/\mathfrak{p}).$$

And

$$e(\mathfrak{P}/p) = \frac{[F : E]_i}{[F_{\mathfrak{P}} : E_{\mathfrak{p}}]_i} I(\mathfrak{P}/\mathfrak{p}).$$

which implies

$$\pi(Tr_{F/E}(y)) = e(\mathfrak{P}/\mathfrak{p}) \sum_{\alpha \in Aut(F_{\mathfrak{P}}/E_p)} \alpha(\pi(y)) = e(\mathfrak{P}/\mathfrak{p})\, Tr_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(\pi(y))$$