Algebraic Geometric Codes

Recitation 09

Shir Peleg

Tel Aviv University

May 8, 2022

Fields with genus 0.

Theorem 1

Let F/K be a function field with genus 0. Then F is either a rational function field (i.e. $F = K(u)$ for some $u \in F \setminus K$) or there are $t, u \in F \setminus K$ s.t $F = K(t, u)$, and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Fields with genus 0.

Theorem 1

Let F/K be a function field with genus 0. Then F is either a rational function field (i.e. $F = K(u)$ for some $u \in F \setminus K$) or there are $t, u \in F \setminus K$ s.t $F = K(t, u)$, and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Proof.

let m be a canonical divisor of F/K. Then $\deg(m) = 2g - 2 = -2$.

Fields with genus 0.

Theorem 1

Let F/K be a function field with genus 0. Then F is either a rational function field (i.e. $F = K(u)$ for some $u \in F \setminus K$) or there are $t, u \in F \setminus K$ s.t $F = K(t, u)$, and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Proof.

let m be a canonical divisor of F/K. Then $\deg(m) = 2g - 2 = -2$. By applying the Riemann Roch theorem on $-m$, we get that

$$\dim \mathcal{L}(-m) - \dim \mathcal{L}(m - (-m)) = \deg(-m) + 1 - g.$$

Fields with genus 0.

Theorem 1

Let F/K be a function field with genus 0. Then F is either a rational function field (i.e. $F = K(u)$ for some $u \in F \setminus K$) or there are $t, u \in F \setminus K$ s.t $F = K(t, u)$, and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Proof.

let m be a canonical divisor of F/K. Then $\deg(m) = 2g - 2 = -2$. By applying the Riemann Roch theorem on $-m$, we get that

$$\dim \mathcal{L}(-m) - \dim \mathcal{L}(m - (-m)) = \deg(-m) + 1 - g.$$

As $\deg(m + m) = -4$, we have $\dim \mathcal{L}(2m) = 0$.

Fields with genus 0.

Theorem 1

Let F/K be a function field with genus 0. Then F is either a rational function field (i.e. $F = K(u)$ for some $u \in F \setminus K$) or there are $t, u \in F \setminus K$ s.t $F = K(t, u)$, and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Proof.

let m be a canonical divisor of F/K. Then $\deg(m) = 2g - 2 = -2$. By applying the Riemann Roch theorem on $-m$, we get that

$$\dim \mathcal{L}(-m) - \dim \mathcal{L}(m - (-m)) = \deg(-m) + 1 - g.$$

As $\deg(m + m) = -4$, we have $\dim \mathcal{L}(2m) = 0$. Therefore

$$\dim \mathcal{L}(-m) = \deg(-m) + 1 - g = 3.$$

Proof

Proof cont.

Let $x, y \in \mathcal{L}(-m)$, be linearly independent over K (there are such as the dimension is 3). Consider $t = \frac{x}{y}$. We will show that $\deg(t)_\infty \leq 2$. From a theorem in class it follows that $[F : K(t)] \leq 2$.

Proof

Proof cont.

Let $x, y \in \mathcal{L}(-m)$, be linearly independent over K (there are such as the dimension is 3). Consider $t = \frac{x}{y}$. We will show that $\deg(t)_\infty \leq 2$. From a theorem in class it follows that $[F : K(t)] \leq 2$.

Indeed, $(t) = (x) - (y) = ((x) - m) - ((y) - m)$. As $(y), (x) \in \mathcal{L}(-m)$, it holds that $(x) + -m, (y) + -m \geq 0$. Thus $0 \leq (t)_\infty \leq (y) - m$ (there can be some cancellations with $(x) - m$).

Proof

Proof cont.

Let $x, y \in \mathcal{L}(-m)$, be linearly independent over K (there are such as the dimension is 3). Consider $t = \frac{x}{y}$. We will show that $\deg(t)_\infty \leq 2$. From a theorem in class it follows that $[F : K(t)] \leq 2$.

Indeed, $(t) = (x) - (y) = ((x) - m) - ((y) - m)$. As $(y), (x) \in \mathcal{L}(-m)$, it holds that $(x) + -m, (y) + -m \geq 0$. Thus $0 \leq (t)_\infty \leq (y) - m$ (there can be some cancellations with $(x) - m$).
We conclude that

$$\deg((t)_\infty) \leq \deg((y) - m) = \deg((y)) + \deg(-m) = 2.$$

Proof

Proof cont.

Now consider both possible options:

- $[F : K(t)] = 1$ we are done as the theorem holds for $u = t$.

Proof

Proof cont.

Now consider both possible options:

- $[F : K(t)] = 1$ we are done as the theorem holds for $u = t$.
- $[F : K(t)] = 2$. Last time we saw that in this case $F = K(u, t)$ where $u^2 = d(x)$, and $g = \lfloor \frac{\deg(d)-1}{2} \rfloor$ as $g = 0$ it follows that $\deg(d) = 1$ or $\deg(d) = 2$.

Proof

Proof cont.

Now consider both possible options:

- $[F : K(t)] = 1$ we are done as the theorem holds for $u = t$.
- $[F : K(t)] = 2$. Last time we saw that in this case $F = K(u, t)$ where $u^2 = d(x)$, and $g = \lfloor \frac{\deg(d)-1}{2} \rfloor$ as $g = 0$ it follows that $\deg(d) = 1$ or $\deg(d) = 2$.
  If $\deg(d) = 1$ then $t \in K(u)$, and the theorem holds (F is a rational function filed).

Proof

Proof cont.

Now consider both possible options:

- $[F : K(t)] = 1$ we are done as the theorem holds for $u = t$.
- $[F : K(t)] = 2$. Last time we saw that in this case $F = K(u, t)$ where $u^2 = d(x)$, and $g = \lfloor \frac{\deg(d)-1}{2} \rfloor$ as $g = 0$ it follows that $\deg(d) = 1$ or $\deg(d) = 2$.
  If $\deg(d) = 1$ then $t \in K(u)$, and the theorem holds (F is a rational function filed).
  If $\deg(d) = 2$ then we can write $d = at^2+bt+c$, when replacing $t' = t+\frac{-b}{2a}$, we get that $at^2 + bt + c = a(t'^2) + (c + \frac{b^2a+b^2}{4a}) = at'^2 + c'$. Note that both $a, c' \in K^\times$ (or F is a rational function field.)

How do we know which of the previous cases hold?

Theorem 2

Let F/K be a function field with genus 0, then F is a rational function field $\iff$ there is a divisor of degree 1.

How do we know which of the previous cases hold?

Theorem 2

Let F/K be a function field with genus 0, then F is a rational function field $\iff$ there is a divisor of degree 1.

Proof.

$\Rightarrow$ we proved in a previous recitation that the valuation v_∞ has degree 1.

How do we know which of the previous cases hold?

Theorem 2

Let F/K be a function field with genus 0, then F is a rational function field $\iff$ there is a divisor of degree 1.

Proof.

$\Rightarrow$ we proved in a previous recitation that the valuation v_∞ has degree 1.
Let a be a divisor with $\deg(a) = 1$. Similarly to before, using R.R theorem and the fact that $\deg(m - a) < 0$ we have

$$\dim \mathcal{L}(a) = \deg(a) + 1 - g = 2.$$

How do we know which of the previous cases hold?

Proof.

Thus, there is $x \in F \setminus K$ such that $x \in \mathcal{L}(a)$.

How do we know which of the previous cases hold?

Proof.

Thus, there is $x \in F \setminus K$ such that $x \in \mathcal{L}(a)$. We want $a \geq 0$ (we will see why soon), so, as $(x) + a \geq 0$, and $\deg((x) + a) = 1$, we can replace $a = (x) + a$ if needed.

How do we know which of the previous cases hold?

Proof.

Thus, there is $x \in F \setminus K$ such that $x \in \mathcal{L}(a)$. We want $a \geq 0$ (we will see why soon), so, as $(x) + a \geq 0$, and $\deg((x) + a) = 1$, we can replace $a = (x) + a$ if needed.

We will show that $\deg((x)_\infty) \leq 1$, and so $[F : K(x)] = \deg((x)_\infty) = 1$, and $F = K(x)$ is a rational function field.

How do we know which of the previous cases hold?

Proof.

Thus, there is $x \in F \setminus K$ such that $x \in \mathcal{L}(a)$. We want $a \geq 0$ (we will see why soon), so, as $(x) + a \geq 0$, and $\deg((x) + a) = 1$, we can replace $a = (x) + a$ if needed.

We will show that $\deg((x)_\infty) \leq 1$, and so $[F : K(x)] = \deg((x)_\infty) = 1$, and $F = K(x)$ is a rational function field.

Indeed $(x) + a \geq 0$, and $a \geq 0$ it implies, as $(x)_0, (x)_\infty$ are co prime that $(x)_\infty + a \geq 0$ and thus $\deg((x)_\infty) \leq 1$ as we wanted.

Fields with genus 1

Claim 2.1

Let $F = K(x, y)$ where $y^2 = d(x), \deg(d) = 3$, and genus 1. Then there is a place p of F/K with $(x)_\infty = 2p$.

Fields with genus 1

Claim 2.1

Let $F = K(x, y)$ where $y^2 = d(x), \deg(d) = 3$, and genus 1. Then there is a place p of F/K with $(x)_\infty = 2p$.

Proof.

We know that $[F : K(x)] = \deg((x)_\infty) \leq 2$. If $F = K(x)$ then the genus is 0, which is not the case. Thus $\deg((x)_\infty) = 2$.

Fields with genus 1

Claim 2.1

Let $F = K(x, y)$ where $y^2 = d(x), \deg(d) = 3$, and genus 1. Then there is a place p of F/K with $(x)_\infty = 2p$.

Proof.

We know that $[F : K(x)] = \deg((x)_\infty) \leq 2$. If $F = K(x)$ then the genus is 0, which is not the case. Thus $\deg((x)_\infty) = 2$.
As $0 \leq (x)_\infty$ we have either:

- $(x)_\infty = p$ for some prime divisor p of $\deg(p) = 2$.

Fields with genus 1

Claim 2.1

Let $F = K(x, y)$ where $y^2 = d(x), \deg(d) = 3$, and genus 1. Then there is a place p of F/K with $(x)_\infty = 2p$.

Proof.

We know that $[F : K(x)] = \deg((x)_\infty) \leq 2$. If $F = K(x)$ then the genus is 0, which is not the case. Thus $\deg((x)_\infty) = 2$.
As $0 \leq (x)_\infty$ we have either:

- $(x)_\infty = p$ for some prime divisor p of $\deg(p) = 2$.
- $(x)_\infty = 2p$ for some prime divisor p of $\deg(p) = 1$.

Fields with genus 1

Claim 2.1

Let $F = K(x, y)$ where $y^2 = d(x), \deg(d) = 3$, and genus 1. Then there is a place p of F/K with $(x)_\infty = 2p$.

Proof.

We know that $[F : K(x)] = \deg((x)_\infty) \leq 2$. If $F = K(x)$ then the genus is 0, which is not the case. Thus $\deg((x)_\infty) = 2$.
As $0 \leq (x)_\infty$ we have either:

- $(x)_\infty = p$ for some prime divisor p of $\deg(p) = 2$.
- $(x)_\infty = 2p$ for some prime divisor p of $\deg(p) = 1$.
- $(x)_\infty = q + p$ for some prime divisors p, q of $\deg(q) = \deg(p) = 1$.

Fields with genus 1

Proof.

Recall

- $(x)_\infty = p$ for some prime place p of $\deg(p) = 2$.
- $(x)_\infty = 2p$ for some prime divisor p of $\deg(p) = 1$.
- $(x)_\infty = q + p$ for some prime divisors p, q of $\deg(q) = \deg(p) = 1$.

We also have that

$$2(y)_\infty = (y^2)_\infty = (d(x))_\infty = \deg(d)(x)_\infty = 3(x)_\infty.$$

Fields with genus 1

Proof.

Recall

- $(x)_\infty = p$ for some prime place p of $\deg(p) = 2$.
- $(x)_\infty = 2p$ for some prime divisor p of $\deg(p) = 1$.
- $(x)_\infty = q + p$ for some prime divisors p, q of $\deg(q) = \deg(p) = 1$.

We also have that

$$2(y)_\infty = (y^2)_\infty = (d(x))_\infty = \deg(d)(x)_\infty = 3(x)_\infty.$$

That means that every entry in $(x)_\infty$ is even, i.e. only item 2 is possible. As we wanted.

General fields of genus 1.

Theorem 3

The other direction also holds. I.e. if F/K withe genus 1, and there is a place p of F/K with $\deg(p) = 1$, then $F = K(x, y)$ with $y^2 = d(x)$ and $\deg(d) = 3$ without multiple factors and $(x)_\infty = 2p$.

General fields of genus 1.

Theorem 3

The other direction also holds. I.e. if F/K withe genus 1, and there is a place p of F/K with $\deg(p) = 1$, then $F = K(x, y)$ with $y^2 = d(x)$ and $\deg(d) = 3$ without multiple factors and $(x)_\infty = 2p$.

Proof.

Consider $n \in \mathbb{N}^+$, $\deg(n \cdot p) = n$, and similarly to before, for $n > 2g - 2 = 0$,

$$\dim \mathcal{L}(n \cdot p) = n + 1 - g = n.$$

General fields of genus 1.

Theorem 3

The other direction also holds. I.e. if F/K withe genus 1, and there is a place p of F/K with $\deg(p) = 1$, then $F = K(x, y)$ with $y^2 = d(x)$ and $\deg(d) = 3$ without multiple factors and $(x)_\infty = 2p$.

Proof.

Consider $n \in \mathbb{N}^+$, $\deg(n \cdot p) = n$, and similarly to before, for $n > 2g - 2 = 0$,

$$\dim \mathcal{L}(n \cdot p) = n + 1 - g = n.$$

Furthermore

$$K = \mathcal{L}(p) \subset \mathcal{L}(2p) \subset \cdots \subset \mathcal{L}(n \cdot p).$$

General fields of genus 1.

Proof.

$$\mathcal{L}(p) = Span_K(1) \quad \mathcal{L}(2p) = Span_K(1, x)$$
$$\mathcal{L}(3p) = Span_K(1, x, y) \quad \mathcal{L}(4p) = Span_K(1, x, y, x^2)$$
$$\mathcal{L}(5p) = Span_K(1, x, y, x^2, xy) \quad \mathcal{L}(6p) = Span_K(1, x, y, x^2, xy, x^3, y^2)$$

General fields of genus 1.

Proof.

$$\mathcal{L}(p) = Span_K(1) \quad \mathcal{L}(2p) = Span_K(1, x)$$
$$\mathcal{L}(3p) = Span_K(1, x, y) \quad \mathcal{L}(4p) = Span_K(1, x, y, x^2)$$
$$\mathcal{L}(5p) = Span_K(1, x, y, x^2, xy) \quad \mathcal{L}(6p) = Span_K(1, x, y, x^2, xy, x^3, y^2)$$

Thus there is a linear combination

$$y^2 = a + bx + cy + dx^2 + exy + fx^3,$$

with $f \neq 0$. If we define $y' = y - \frac{1}{2}(ex + c)$ we get that $y'^2 = d(x)$.