Function Fields of Genus 0 or 1

Recitation 11

Tomer Manket

Tel Aviv University

Previously: Degree 2 Extensions of $K(x)$

Theorem 1

Let K be a field with $\mathrm{char}(K) \neq 2$. Assume $F = K(x, y)$ where x is transcendental over K and $y^2 = d(x)$ for some square-free polynomial $d \in K[X]$ of degree $m \geq 1$. Then

- *F/K is a function field.*
- *$[F : K(x)] = 2$.*
- *The genus of F/K is given by $g = \left\lceil \frac{m}{2} \right\rceil - 1$.*

Example 2

Let $F = \mathbb{F}_5(x, y)$ where

$$y^2 = x^2 + 3$$

Then $F/\mathbb{F}_5$ is a function field with genus $g = \left\lceil \frac{2}{2} \right\rceil - 1 = 0$.

Example 3

Let $F = \mathbb{F}_3(x, y)$ where

$$y^2 = x^3 - x = x(x + 1)(x - 1)$$

Then $F/\mathbb{F}_3$ is a function field with genus $g = \left\lceil \frac{3}{2} \right\rceil - 1 = 2 - 1 = 1$.

Theorem 4

Let F/K be a function field. Assume that there exists $x \in F \setminus K$ such that $[F : K(x)] = 2$ and that $\operatorname{char}(K) \neq 2$. Then there exists $y \in F$ such that $F = K(x, y)$ and $y^2 = d(x)$ for some square-free $d \in K[X]$ of degree at least 1.

Function fields of genus 0

Theorem 5

Let F/K be a function field of genus 0. Then F/K is either a rational function field (i.e. $F = K(t)$ for some $t \in F \setminus K$), or a a quadratic extension of such a field. In the second case, if $\mathrm{char}(K) \neq 2$ then there exist $t, u \in F \setminus K$ such that $F = K(t, u)$ and $u^2 = at^2 + c$ for some $a, c \in K^\times$.

Proof.

Let $\mathfrak{w}$ be a canonical divisor of F/K. We know that $\deg(\mathfrak{w}) = 2g - 2 = -2$. Then $\deg(-\mathfrak{w}) = 2 > -2 = 2g - 2$, so by Riemann-Roch Theorem,

$$\dim(-\mathfrak{w}) = \deg(-\mathfrak{w}) + 1 - g = 2 + 1 - 0 = 3.$$

Hence there exist $x, y \in \mathcal{L}(-\mathfrak{w})$ which are linearly independent over K.

Proof cont.

Consider $t = \frac{x}{y} \in F \setminus K$. Since $x, y \in \mathcal{L}(-\mathfrak{w})$ we have that

$$(x) - \mathfrak{w} \geq 0 \;\text{ and }\; (y) - \mathfrak{w} \geq 0,$$

and so

$$(t) = (x) - (y) = \underbrace{[(x) - \mathfrak{w}]}_{\geq 0} - \underbrace{[(y) - \mathfrak{w}]}_{\geq 0}.$$

It follows that $0 \leq (t)_\infty \leq (y) - \mathfrak{w}$. Thus,

$$\deg(t)_\infty \leq \deg((y) - \mathfrak{w}) = \deg(y) - \deg \mathfrak{w} = 0 - (-2) = 2.$$

Now by a theorem you proved in class,

$$[F : K(t)] = \deg(t)_\infty \leq 2.$$

Proof cont.

Hence F is either $K(t)$ or a quadratic extension of $K(t)$.

Now, assume $[F : K(t)] = 2$ and $\mathrm{char}(K) \neq 2$. By Theorem 4, there exists $u \in F$ such that $F = K(t, u)$ and $u^2 = d(t)$ for some square-free $d \in K[X]$ of degree $m \geq 1$. Since F/K has genus $g = 0$, we get that $\left\lceil \frac{m}{2} \right\rceil - 1 = 0$, i.e. $m = 1$ or $m = 2$. Hence $d(X) = aX^2 + bX + c$ where $a, b, c \in K$ and $a \neq 0$ or $b \neq 0$.

- If $a = 0$: Then $u^2 = bt + c$ (and $b \neq 0$), so

$$t = \frac{u^2 - c}{b} \in K(u) \implies F = K(t, u) = K(u)$$

  and F is a rational function field.

Proof cont.

- If $a \neq 0$: Then $u^2 = at^2 + bt + c$, so by completing the square we get

$$u^2 = a\left(t^2 + \frac{b}{a}t\right) + c = a\left(t + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}\,.$$

Letting $t' := t + \frac{b}{2a}$ and $c' = c - \frac{b^2}{4a} \in K$, we get that

$$F = K(t,u) = K(t',u) \;\text{ and }\; u^2 = at'^2 + c'.$$

Finally, if $c' = 0$ then $u^2 = at'^2$, i.e. $\left(\frac{u}{t'}\right)^2 = a \in K$. But then $\frac{u}{t'} \in F$ is algebraic over K, and so $\frac{u}{t'} \in K$ and $u \in K(t')$. Hence in this case, $F = K(t',u) = K(t')$ is a rational function field.

$\square$

How can we distinguish the two possibilities?

Theorem 6

Let F/K be a function field with genus 0. Then F is a rational function field over K iff it has a divisor of degree one.

Proof.

$(\Rightarrow)$: If $F = K(x)$ then $\mathfrak{p}_\infty$ is a (prime) divisor of degree one.

$(\Leftarrow)$: Let $\mathfrak{a}$ be a divisor with $\deg \mathfrak{a} = 1$. Since $\deg \mathfrak{a} = 1 > -2 = 2g - 2$, we get by Riemann-Roch that

$$\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g = 1 + 1 - 0 = 2.$$

Thus, there exists $z \in \mathcal{L}(\mathfrak{a}) \setminus K$. Then $\mathfrak{a}' := (z) + \mathfrak{a} \geq 0$. Note that $\mathfrak{a}'$ also has degree 1 and dimension 2 (same as $\mathfrak{a}$).

Proof cont.

In particular, there exists $x \in \mathcal{L}(\mathfrak{a}') \setminus K$. Hence $(x) + \mathfrak{a}' \geq 0$, i.e. $(x)_0 - (x)_\infty + \mathfrak{a}' \geq 0$ and so $(x)_\infty \leq (x)_0 + \mathfrak{a}'$.

As $(x)_0$ and $(x)_\infty$ have disjoint supports and $\mathfrak{a}' \geq 0$, this implies that $(x)_\infty \leq \mathfrak{a}'$. In particular, $\deg(x)_\infty \leq \deg \mathfrak{a}' = 1$.

Finally, since $x \in F \setminus K$ we obtain

$$1 \leq [F : K(x)] = \deg(x)_\infty \leq 1$$

so $[F : K(x)] = 1$, i.e. $F = K(x)$ is a rational function field. □

Remark 1

Note that we can replace "divisor" by "prime divisor" in the theorem statement.

Example 7 (A non-rational function field of genus 0)

Let $F = \mathbb{R}(x, y)$ where x is transcendental over $\mathbb{R}$ and

$$y^2 = -x^2 - 1.$$

Then $F/\mathbb{R}$ is a function field with $[F : \mathbb{R}(x)] = 2$ and genus $g = 0$. In addition, each prime divisor of $F/\mathbb{R}$ has degree 2. By the previous theorem, F is not a rational function field.

Remark 2

If F/K is a function field with K algebraically closed or K a finite field, then there always exists a divisor of degree 1. So in these cases, F is rational iff $g = 0$.

Function fields of genus 1

Lemma 8

Let F/K be a function field of genus $g = 1$. Suppose $F = K(x, y)$ where $y^2 = d(x)$ for $d \in K[X]$ of degree 3. Then there exists a prime divisor $\mathfrak{p}$ of degree 1 such that $(x)_\infty = 2\mathfrak{p}$.

Proof.

First,

$$\deg(x)_\infty = [F : K(x)] = [K(x)(y) : K(x)] \leq 2.$$

If $[F : K(x)] = 1$ then $F = K(x)$ is a rational function field and so $g = 0$, a contradiction. Hence $\deg(x)_\infty = 2$.

Proof cont.

As $\deg(x)_\infty = 2$ and $(x)_\infty \geq 0$, there are 3 possibilities:

- $(x)_\infty = \mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of $\deg \mathfrak{p} = 2$.
- $(x)_\infty = 2\mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of $\deg \mathfrak{p} = 1$.
- $(x)_\infty = \mathfrak{p} + \mathfrak{q}$ for some $\mathfrak{p}, \mathfrak{q} \in \mathbb{P}$ with $\deg \mathfrak{p} = \deg \mathfrak{q} = 1$.

However, note that

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

That implies that all the coefficients in $(x)_\infty$ are even. Thus, it must be that $(x)_\infty = 2\mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}$ of degree 1. □

Conversely, we have

Theorem 9

Let K be a field with $\mathrm{char}(K) \neq 2$, and let F/K be a function field of genus $g = 1$ that has a prime divisor $\mathfrak{p}$ of degree 1. Then $F = K(x, y)$ where $y^2 = d(x)$ for a square-free $d \in K[X]$ of degree 3, and $(x)_\infty = 2\mathfrak{p}$.

Proof.

For each $n \in \mathbb{N}$, $\deg(n\mathfrak{p}) = n \deg \mathfrak{p} = n$. Therefore, if $n > 2g - 2 = 0$ then by Riemann-Roch,

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

Furthermore,

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

Proof cont.

In particular, there exist $x, y \in F$ such that

$$\mathcal{L}(2\mathfrak{p}) = \text{Span}_K\{1, x\} \quad \text{and} \quad \mathcal{L}(3\mathfrak{p}) = \text{Span}_K\{1, x, y\}.$$

Since $x \in \mathcal{L}(2\mathfrak{p}) \setminus \mathcal{L}(\mathfrak{p})$ we must have $(x)_\infty = 2\mathfrak{p}$. Similarly, $y \in \mathcal{L}(3\mathfrak{p}) \setminus \mathcal{L}(2\mathfrak{p})$ implies that $(y)_\infty = 3\mathfrak{p}$. Then for $i, j \in \mathbb{N}$ we have

$$(x^i y^j)_\infty = i(x)_\infty + j(y)_\infty = (2i + 3j)\mathfrak{p}.$$

It is easy to verify that

$$\begin{aligned} \mathcal{L}(\mathfrak{p}) &= \text{Span}_K\{1\} & \mathcal{L}(2\mathfrak{p}) &= \text{Span}_K\{1, x\} \\ \mathcal{L}(3\mathfrak{p}) &= \text{Span}_K\{1, x, y\} & \mathcal{L}(4\mathfrak{p}) &= \text{Span}_K\{1, x, y, x^2\} \\ \mathcal{L}(5\mathfrak{p}) &= \text{Span}_K\{1, x, y, x^2, xy\} & \mathcal{L}(6\mathfrak{p}) &= \text{Span}_K\{1, x, y, x^2, xy, x^3, y^2\} \end{aligned}$$

Proof cont.

Thus, there is a linear combination (with $f \neq 0$)

$$y^2 = a + bx + cy + dx^2 + exy + fx^3, \tag{1}$$

i.e.

$$y^2 - (ex + c)y = a + bx + dx^2 + fx^3. \tag{2}$$

Now, as $\mathrm{char}(K) \neq 2$ we can complete the square to get

$$\left(y - \frac{1}{2}(ex + c)\right)^2 = a + bx + dx^2 + fx^3 + \frac{1}{4}(ex + c)^2. \tag{3}$$

Now letting $y' = y - \frac{1}{2}(ex + c)$ gives $y'^2 = d(x)$ for $d \in K[X]$ of degree 3.

Clearly, $K(x, y) = K(x, y')$. Thus it remains to show that $F = K(x, y)$ and that d is square-free.

Proof cont.

Indeed, we saw that $\deg(x)_\infty = 2$ and $\deg(y)_\infty = 3$ are coprime, so by Question 2 in PS 3 we obtain $F = K(x, y)$.

Finally, assume to the contrary that d is not square-free. By (3), it has degree 3 and leading coefficient f, so it must be of the form

$$d(X) = f \cdot (X - \alpha)^2 (X - \beta).$$

But then for $y'' := \frac{y'}{x-\alpha} \in F$ we get $y''^2 = \frac{y'^2}{(x-\alpha)^2} = f \cdot (x - \beta)$. But then

$$F = K(x, y') = K(x, y'') = K(y'')$$

so F is a rational function field, contradicting $g = 1$.

∎