Degree 2 Extensions of $K(x)$

Recitation 10

Tomer Manket

Tel Aviv University

Let F/K be a function field such that

1. $[F : K(x)] = 2$ for some $x \in F \setminus K$
2. $\mathrm{char}(K) \neq 2$

We'll be interested in the following questions:

- Can we characterize these function fields?
- What is the Riemann-Roch space $\mathcal{L}(n(x)_\infty)$, for $n \in \mathbb{N}$?
- What is its dimension $\dim n(x)_\infty$?
- What is the genus g?

Degree 2 Extensions

Definition 1

Let K be a field. A polynomial $g \in K[X]$ is *square-free* if $p^2 \nmid g$ in $K[X]$, for every $p \in K[X]$ with $\deg p \geq 1$.

Lemma 2

Let F/K be a function field. Assume that there exists $x \in F \setminus K$ such that $[F : K(x)] = 2$ and that $\mathrm{char}(K) \neq 2$. 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.

Proof.

Let $y_1 \in F \setminus K(x)$. Then $1 < [K(x)(y_1) : K(x)] \leq [F : K(x)] = 2$ so $F = K(x, y_1)$ and $y_1^2 + by_1 + c = 0$ for some $b, c \in K(x)$.

Degree 2 Extension

Proof.

As char$(K) \neq 2$, *completing the square gives*

$$\left(y_1 + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c.$$

Let $y_2 := y_1 + \frac{b}{2}$. *Then* $K(x, y_2) = K(x, y_1) = F$ *and* $y_2^2 = \frac{f}{g}$ *for* $f, g \in K[x]$. *Then* $y_3 := gy_2$ *satisfies* $K(x, y_3) = K(x, y_2) = F$ *and*

$$y_3^2 = (gy_2)^2 = g^2 y_2^2 = gf =: h \in K[x].$$

Note that h *is neither in* K *nor a square in* $K[x]$ *(otherwise* $y_3 \in K[x]$ *and* $K(x, y_3) = K(x) \neq F$*). To conclude, let* $h = p_1^{m_1} \cdots p_r^{m_r}$ *be a decomposition of* h *to irreducible factors in* $K[x]$ *(so at least one* m_i *is odd). Let* $p := p_1^{\lfloor m_1/2 \rfloor} \cdots p_r^{\lfloor m_r/2 \rfloor}$. *Then* $y := \frac{y_3}{p} \in F$ *satisfies the assertions.* □

For example, if $y_3^2 = x^3(x+1)(2x+1)^4$ we take

$$y := \frac{y_3}{x(2x+1)^2} \implies y^2 = x(x+1)$$

(clearly $K(x, y_3) = K(x, y)$).

Conversely, we have

Claim 3

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 $d \in K[x]$ of degree at least 1. Then F/K is a function field with $[F : K(x)] = 2$.

Proof.

Left as an exercise. □

Remark 4

In the above claim, it is necessary that $d(x)$ be square-free. Indeed, consider $K = \mathbb{F}_3$ and $F = K(x, y)$ where $y^2 = -(x^4 - x^2 + 1)$. In PS 1 you showed that K is not algebraically closed in F, so F/K is not a function field. Note that in this case,

$$d(x) = -(x^4 + 2x^2 + 1) = -(x^2 + 1)^2.$$

Some preparations

Claim 5

Let F/K be a function field, $x \in F \setminus K$ and $0 \neq f(X) \in K[X]$. Then

1. *$(x)_\infty$ and $(f(x))_0$ have disjoint supports.*
2. $(f(x))_\infty = \deg(f) \cdot (x)_\infty$.

Proof.

If $f \in K^\times$ this is trivial. Otherwise, $f = \sum_{i=0}^n c_i x^i$ where $n = \deg(f) \geq 1$. Let $\emptyset \neq J = \{i : c_i \neq 0\}$ and $\mathfrak{p} \in \mathbb{P}$. Then

$$\nu_\mathfrak{p}(x) \geq 0 \implies \nu_\mathfrak{p}(f(x)) \geq \min_{i \in J}\{\nu_\mathfrak{p}(c_i x^i)\} = \min_{i \in J}\{i\nu_\mathfrak{p}(x)\} \geq 0,$$

$$\nu_\mathfrak{p}(x) < 0 \implies \nu_\mathfrak{p}(f(x)) = \min_{i \in J}\{i\nu_\mathfrak{p}(x)\} = n\nu_\mathfrak{p}(x) < 0$$

and both parts easily follow.

Some preparations

Lemma 6

Let F/K be a function field. Let $x \in F \setminus K$ and $0 \neq r = \frac{f_1(x)}{f_2(x)} \in K(x)$ such that $f_1, f_2 \in \mathrm{K}[X]$ are coprime. Then,

1. $(r) = (f_1(x))_0 - (f_2(x))_0 + (\deg f_2 - \deg f_1) \cdot (x)_\infty$.
2. $(x)_\infty$, $(f_1(x))_0$, $(f_2(x))_0$ *are pairwise disjoint.*
3. *For all $n \in \mathbb{Z}$,*

$$r \in \mathcal{L}(n(x)_\infty) \iff \deg f_1 \leq n \text{ and } f_2 \in K^\times.$$

Proof of (1).

By Claim 5, for $i = 1, 2$ we have

$$(f_i(x)) = (f_i(x))_0 - (f_i(x))_\infty = (f_i(x))_0 - \deg(f_i) \cdot (x)_\infty.$$

Substitution in $(r) = (f_1(x)) - (f_2(x))$ gives the desired result. □

Some preparations

Proof of (2).

By Claim 5, $(x)_\infty$ and $(f_i(x))_0$ are disjoint for $i = 1, 2$. It remains to show that $(f_1(x))_0$ and $(f_2(x))_0$ are disjoint.

Suppose $\mathfrak{p} \in \mathbb{P}$ is such that $\nu_\mathfrak{p}(f_1(x)), \nu_\mathfrak{p}(f_2(x)) > 0$. Then $\nu_\mathfrak{p}(x) \geq 0$, and so for every $g(X) \in K[X]$ we have $\nu_\mathfrak{p}(g(x)) \geq 0$.

As f_1 and f_2 are coprime, there exist $g_1, g_2 \in K[X]$ such that $f_1 g_1 + f_2 g_2 = 1$. Thus,

$$0 = \nu_\mathfrak{p}(1) = \nu_\mathfrak{p}(f_1 g_1 + f_2 g_2) \geq \min(\nu_\mathfrak{p}(f_1 g_1), \nu_\mathfrak{p}(f_2 g_2)).$$

However, $\nu_\mathfrak{p}(f_i g_i) = \nu_\mathfrak{p}(f_i) + \nu_\mathfrak{p}(g_i) > 0$, a contradiction. □

Some preparations

Proof of (3).

Let $n \in \mathbb{Z}$. Then $r \in \mathcal{L}(n(x)_\infty) \iff (r) + n(x)_\infty \geq 0$, i.e. iff

$$(f_1(x))_0 - (f_2(x))_0 + (n + \deg f_2 - \deg f_1) \cdot (x)_\infty \geq 0. \qquad (1)$$

Now, $(f_1(x))_0$, $(f_2(x))_0$ and $(x)_\infty$ are pairwise disjoint, so (1) holds iff

$$(f_2(x))_0 = 0 \quad \text{and} \quad n + \deg f_2 - \deg f_1 \geq 0.$$

This holds iff $f_2(x) \in K^\times$ (so $\deg f_2 = 0$) and $n - \deg f_1 \geq 0$, i.e.

$$\deg f_1 \leq n \quad \text{and} \quad f_2 \in K^\times.$$

$\square$

Some preparations

Let $\sigma \in \text{Aut}(F/K)$. Then σ induces a bijection $\sigma\colon \mathbb{P} \to \mathbb{P}$

$$\mathfrak{p} \mapsto \sigma\mathfrak{p}$$

where $\sigma\mathfrak{p} \in \mathbb{P}$ is the prime divisor with $\mathcal{O}_{\sigma\mathfrak{p}} = \sigma(\mathcal{O}_{\mathfrak{p}})$.

Proposition 7

Let $\sigma \in \text{Aut}(F/K)$ and let $\mathcal{D}$ be the divisors group of F/K.

1. *The induced bijection $\sigma\colon \mathbb{P} \to \mathbb{P}$ can be extended to a group isomorphism $\sigma\colon \mathcal{D} \to \mathcal{D}$.*
2. *For every $x \in F$, $\sigma((x)) = (\sigma(x))$ and $\sigma((x)_\infty) = (\sigma(x))_\infty$.*
3. *For every $\mathfrak{a} \in \mathcal{D}$, $\mathcal{L}(\sigma\mathfrak{a}) = \sigma(\mathcal{L}(\mathfrak{a}))$.*

Proof.

Left as an exercise.

The space $\mathcal{L}(n(x)_\infty)$

Lemma 8

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

$$\dim n(x)_\infty = 2n + 2 - \left\lceil \frac{m}{2} \right\rceil.$$

Note that the existence of such y is guaranteed by Lemma 2.

Proof.

First, $2(y) = (y^2) = (d(x))$*, so by Claim 5,*

$$(y)_\infty = \frac{1}{2}(d(x))_\infty = \frac{1}{2} \cdot \deg d \cdot (x)_\infty = \frac{m}{2}(x)_\infty.$$

Hence for $i \in \mathbb{N}$*,*

$$\begin{aligned}(x^i y) &= i(x) + (y) = i(x)_0 - i(x)_\infty + (y)_0 - (y)_\infty \\ &= i(x)_0 - \left(i + \frac{m}{2}\right)(x)_\infty + (y)_0.\end{aligned}$$

Thus, an element $x^i y$ *is in* $\mathcal{L}(n(x)_\infty)$ *iff*

$$0 \le (x^i y) + n(x)_\infty = i(x)_0 + \left(n - i - \frac{m}{2}\right)(x)_\infty + (y)_0. \qquad (2)$$

By claim 5, the supports of $(x)_\infty$ *and* $(y)_0 = \frac{1}{2}(d(x))_0$ *are disjoint (and so are those of* $(x)_\infty$ *and* $(x)_0$*), so (2) holds iff* $i \le n - \frac{m}{2}$*.*

Proof.

Now, by Lemma 6 we also have $x^i \in \mathcal{L}(n(x)_\infty)$ *for* $i = 0, 1, \ldots, n$.

Thus,

$$B := \{x^i \mid 0 \leq i \leq n\} \cup \left\{x^i y \mid 0 \leq i \leq n - \frac{m}{2}\right\} \subseteq \mathcal{L}(n(x)_\infty).$$

As $\{1, y\}$ *is linearly independent over* $K(x)$ *and* x *is transcendental over* K*, the set* B *is linearly independent over* K*. Therefore,*

$$\dim n(x)_\infty \geq |B| = (n+1) + \left(n - \left\lceil \frac{m}{2} \right\rceil + 1\right) = 2n + 2 - \left\lceil \frac{m}{2} \right\rceil.$$

To show the opposite inequality, first note that the extension $F/K(x)$ *is Galois (normal as* $[F : K(x)] = 2$*, separable as* $\mathrm{char}(K) \neq 2$*). Then* $\mathrm{Gal}(F/K(x)) = \{id, \sigma\}$.

Proof.

Clearly, $\sigma(x) = x$ (as σ fixes $\mathrm{K}(x)$). Furthermore, the minimal polynomial of y over $K(x)$ is $X^2 - d$ and its roots are $\pm y$, so $\sigma(y) = -y$. In particular, by Proposition 7,

$$\sigma(\mathcal{L}(n(x)_\infty)) = \mathcal{L}(n(\sigma(x))_\infty) = \mathcal{L}(n(x)_\infty). \tag{3}$$

Now, suppose $z \in F$ is in $\mathcal{L}(n(x)_\infty)$. We can write $z = f + gy$ for $f, g \in K(x)$, so that $\sigma(z) = f - gy$. By (3) we also have $\sigma(z) \in \mathcal{L}(n(x)_\infty)$. Thus,

$$f = \frac{1}{2}(z + \sigma(z)) \in \mathcal{L}(n(x)_\infty)$$

and

$$f^2 - dg^2 = z\sigma(z) \in \mathcal{L}(2n(x)_\infty).$$

Proof.

By Lemma 6, we get that $f \in \mathrm{K}[x]$ and $\deg f \leq n$, and similarly $f^2 - dg^2 \in \mathrm{K}[x]$ has degree at most $2n$.

In particular, $dg^2 \in K[x]$ and $\deg(dg^2) \leq 2n$. Since d is square-free it must be that $g \in \mathrm{K}[x]$. Hence

$$\deg(dg^2) \leq 2n \implies m + 2\deg g \leq 2n \implies \deg g \leq n - \frac{m}{2}.$$

Thus, $z = f + gy = \sum_{j=0}^{n} \alpha_j x^j + \sum_{i=0}^{n-\lceil \frac{m}{2} \rceil} \beta_i x^i y$. Therefore

$$\mathcal{L}(n(x)_\infty) \subseteq \mathrm{Span}_K(B) \implies \dim n(x)_\infty \leq |B| = 2n + 2 - \left\lceil \frac{m}{2} \right\rceil.$$

All together, we get that $\dim n(x)_\infty = 2n + 2 - \left\lceil \frac{m}{2} \right\rceil$, and so B is a K-basis of $\mathcal{L}(n(x)_\infty)$. □

The genus

Theorem 9

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

$$g = \left\lceil \frac{m}{2} \right\rceil - 1 = \begin{cases} \frac{m-2}{2} & m \text{ even} \\ \frac{m-1}{2} & m \text{ odd.} \end{cases}$$

Proof.

Recall $\deg(x)_\infty = [F : K(x)] = 2$. Thus, by Riemann-Roch, for a large enough n,

$$2n + 2 - \left\lceil \frac{m}{2} \right\rceil = \dim n(x)_\infty = \deg n(x)_\infty - g + 1 = 2n - g + 1.$$

□