$y^2 = x^3 - x$ over $\mathbb{F}_5$

Unit 17

Gil Cohen

December 30, 2024

Overview

Tame cyclic extensions of K(x)

We now consider a function field F $=$ K(x, y) s.t.

$$y^n = a \cdot \prod_{i=1}^{s} p_i(x)^{n_i}$$

where

1. $a \neq 0$;
2. The $p_1(x), \ldots, p_s(x) \in \mathrm{K}[x]$ are distinct, irreducible and monic;
3. $n_1, \ldots, n_s \in \mathbb{Z} \setminus \{0\}$;
4. char(K) $\nmid n$; and
5. $\forall i \in [s] \;\; \gcd(n, n_i) = 1$.

E.g.,

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

$$y^9 = x + \frac{1}{x} = \frac{x^2+1}{x} \quad \text{(note that field arithmetics matters here.)}$$

Tame cyclic extensions of $\mathsf{K}(x)$

Theorem 1

1. K *is the full constant field of* F *and* $[F : \mathsf{K}(x)] = n$*;*
2. *The prime divisors that correspond to* $p_1(x), \ldots, p_s(x)$ *in* $\mathbb{P}(\mathsf{K}(x))$ *are totally ramified in* $\mathsf{F}/\mathsf{K}(x)$*.*
3. *All prime divisors* $\mathfrak{q}$ *lying over* $\mathfrak{p}_\infty \in \mathbb{P}(\mathsf{K}(x))$ *have ramification index* $e(\mathfrak{q}/\mathfrak{p}_\infty) = \frac{n}{d}$ *where*
$$d = \gcd\left(n, \sum_{i=1}^{s} n_i \deg p_i(x)\right).$$
4. *No prime divisor other than those listed above ramify in* $\mathsf{F}/\mathsf{K}(x)$*.*
5. *Finally, the genus* g *of* $\mathsf{F}/\mathsf{K}(x)$ *is*
$$g = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{s} \deg p_i(x)\right) - \frac{d-1}{2}.$$

Overview

1. Tame cyclic extensions of $K(x)$
2. Our running example
3. Rational places and the genus
4. Kummer's Theorem
5. Riemann-Roch spaces and a little code
6. The canonical divisor

Our example

Consider our running example, the function field $\mathrm{F} = \mathbb{F}_q(x, y)$ s.t.

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

For concreteness, we take $q = 5$ and note that Theorem 1 applies as

- $x, x-1, x+1$ are distinct and irreducible in $\mathbb{F}_5[x]$.
- $\operatorname{char} \mathbb{F}_5$ does not divide $n = 2$
- Each of $x, x-1, x+1$ appears with multiplicity $n_i = 1$ on the RHS, which is coprime to $n = 2$.

Overview

1. Tame cyclic extensions of $K(x)$
2. Our running example
3. Rational places and the genus
4. Kummer's Theorem
5. Riemann-Roch spaces and a little code
6. The canonical divisor

Our example

By Theorem 1, the prime divisors $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_{-1} \in \mathbb{P}(\mathbb{F}_5(x))$ are totally ramified.

Every prime divisor $\mathfrak{P} \in \mathbb{P}(\mathrm{F})$ over $\mathfrak{p}_\infty \in \mathbb{P}(\mathbb{F}_5(x))$ has ramification index $\frac{n}{d} = \frac{2}{d}$ where

$$d = \gcd\left(n, \sum_{i=1}^{s} n_i \deg p_i(x)\right) = \gcd(2,3) = 1.$$

Here

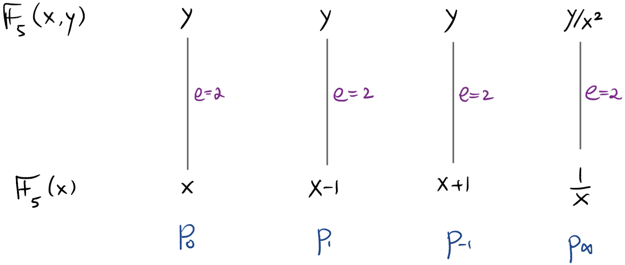
$$p_1(x) = x,\;\; p_2(x) = x+1,\;\; p_3(x) = x-1 \;\text{ and }\; n_1 = n_2 = n_3 = 1.$$

Thus, the ramification index is 2 and so there is a unique prime divisor lying over $\mathfrak{p}_\infty$.

By Theorem 1, no other prime divisor ramifies in $\mathrm{F}/\mathbb{F}_5(x)$.

Our example

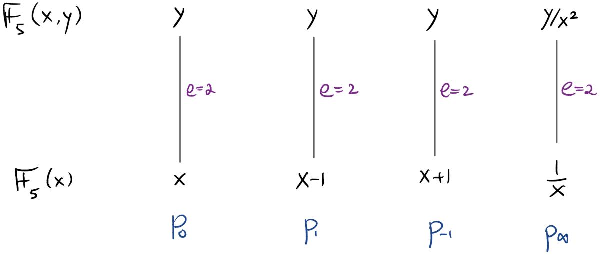
Below is a diagram summarizing the above. We label a prime divisor $\mathfrak{p}$ by a local parameter (or uniformizer) of $\mathfrak{p}$, namely, an element $t \in \mathrm{F}$ with $v_{\mathfrak{p}}(t) = 1$. Equivalently, $\mathfrak{m}_{\mathfrak{p}} = t\mathcal{O}_{\mathfrak{p}}$.



As for the genus, since $d = 1$ and $n = 2$, Theorem 1 yields

$$g(\mathrm{F}) = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{s} \deg p_i(x)\right) - \frac{d-1}{2} = \frac{1}{2}(-1+3) = 1.$$

Our example



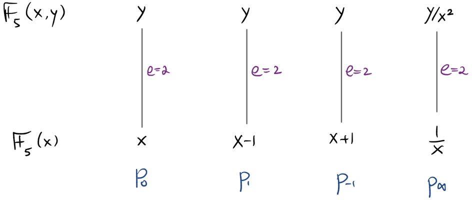
To see that y is a local parameter for $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_{-1}$ note that for each $\alpha \in \{0, \pm 1\}$, if we denote by $\mathfrak{P}_\alpha \in \mathbb{P}(\mathsf{F})$ the prime divisor lying over $\mathfrak{p}_\alpha$ then

$$2 \cdot \upsilon_{\mathfrak{P}_\alpha}(y) = \upsilon_{\mathfrak{P}_\alpha}(y^2) = e(\mathfrak{P}_\alpha/\mathfrak{p}_\alpha) \cdot \upsilon_{\mathfrak{p}_\alpha}(x^3 - x) = e(\mathfrak{P}_\alpha/\mathfrak{p}_\alpha),$$

and so we confirm that $e(\mathfrak{P}_\alpha/\mathfrak{p}_\alpha) = 2$ and that

$$\upsilon_{\mathfrak{P}_\alpha}(y) = 1.$$

Our example



As for the prime divisor $\mathfrak{P}_\infty/\mathfrak{p}_\infty$,

$$2 \cdot \upsilon_{\mathfrak{P}_\infty}(y) = \upsilon_{\mathfrak{P}_\infty}(y^2) = e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) \cdot \upsilon_{\mathfrak{p}_\infty}(x^3 - x) = -3 \cdot e(\mathfrak{P}_\infty/\mathfrak{p}_\infty),$$

and so $\upsilon_{\mathfrak{P}_\infty}(y) = -3$. As

$$\upsilon_{\mathfrak{P}_\infty}(x) = e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) \cdot \upsilon_{\mathfrak{p}_\infty}(x) = 2 \cdot (-1) = -2,$$

we get that

$$\upsilon_{\mathfrak{P}_\infty}(y/x^2) = \upsilon_{\mathfrak{P}_\infty}(y) - 2 \cdot \upsilon_{\mathfrak{P}_\infty}(x) = -3 - 2 \cdot (-2) = 1.$$

We could have also taken $\frac{x}{y}$.

Overview

1. Tame cyclic extensions of $K(x)$
2. Our running example
3. Rational places and the genus
4. Kummer's Theorem
5. Riemann-Roch spaces and a little code
6. The canonical divisor

Kummer's Theorem

Throughout this section we consider finite separable extensions F/L of E/K such that $\mathsf{F} = \mathsf{E}(y)$.

Consider $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ such that

$$y \in \mathcal{O}'_{\mathfrak{p}} \triangleq \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}} = \{z \in \mathsf{F} \mid z \text{ is integral over } \mathcal{O}_{\mathfrak{p}}\},$$

where the last equality is a theorem we will prove. Another result states that the minimal polynomial

$$\varphi(T) = \sum c_i T^i \in \mathsf{E}[T]$$

of such y over E is in fact in $\mathcal{O}_{\mathfrak{p}}[T]$.

In what follows, we denote by $\bar{\varphi}(T) \in \mathsf{E}_{\mathfrak{p}}[T]$ the projection of $\varphi(T)$ to $\mathsf{E}_{\mathfrak{p}}[T]$ (where, recall, $\mathsf{E}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$), namely,

$$\bar{\varphi}(T) = \sum (c_i + \mathfrak{m}_{\mathfrak{p}}) T^i = \sum c_i(\mathfrak{p}) T^i = \sum \bar{c}_i T^i.$$

Kummer's Theorem

Theorem 2 (Kummer's Theorem)

Let F/L *be a finite separable extension of* E/K*, and let* $y \in \mathsf{F}$ *be s.t.* $\mathsf{F} = \mathsf{E}(y)$*. Let* $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *be s.t.* $y \in \mathcal{O}'_{\mathfrak{p}}$*.*

Let $\varphi(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ *be the minimal polynomial of* y *over* E*. Factor*

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i} \in \mathsf{E}_{\mathfrak{p}}[T]$$

where $\gamma_i(T) \in \mathsf{E}_{\mathfrak{p}}[T]$ *are irreducible and distinct (and* $\varepsilon_i \geq 1$*).*

If $\varepsilon_1 = \cdots = \varepsilon_r = 1$ *then there are exactly* r *prime divisors* $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(\mathsf{F})$ *lying over* $\mathfrak{p}$*. Moreover, for every* $i \in [r]$

1. $e(\mathfrak{P}_i/\mathfrak{p}) = 1$
2. $f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T)$
3. $\gamma_i(y) \in \mathfrak{m}_{\mathfrak{P}_i}$

$\mathfrak{p}_2$ and $\mathfrak{p}_{-2}$

Since $y^2 = x^3 - x$ and $x^3 - x \in \mathcal{O}_{\mathfrak{p}_2}$ we have that $y \in \mathcal{O}'_{\mathfrak{p}_2}$. Indeed,

$$\varphi(T) = T^2 - (x^3 - x) \in \mathcal{O}_{\mathfrak{p}_2}[T]$$

is a monic polynomial that vanishes at y.

Since $\mathrm{F}/\mathbb{F}_5(x)$ is finite and separable, we can apply Kummer's Theorem (Theorem 2). We have that the projection of $\varphi(T)$ modulo $\mathfrak{m}_{\mathfrak{p}_2}$,

$$\varphi_2(T) = T^2 - (2^3 - 2) = T^2 - 1 = (T+1)(T-1).$$

Hence, by Kummer's Theorem, there are two prime divisors lying over $\mathfrak{p}_2$. One denoted as $\mathfrak{P}_{2,-1}$ for which $y + 1 \in \mathfrak{m}_{\mathfrak{P}_{2,-1}}$, and the other, $\mathfrak{P}_{2,1}$, satisfies $y - 1 \in \mathfrak{m}_{\mathfrak{P}_{2,1}}$.

$\mathfrak{p}_2$ and $\mathfrak{p}_{-2}$

Is $y+1$ local parameter for $\mathfrak{P}_{2,-1}$?

Denote for the moment $\mathfrak{P} = \mathfrak{P}_{2,-1}$. We have that

$$\upsilon_{\mathfrak{P}}(y^2-1) = \upsilon_{\mathfrak{P}}((y+1)(y-1)) = \upsilon_{\mathfrak{P}}(y+1) + \upsilon_{\mathfrak{P}}(y-1).$$

Now,

$$y+1 \in \mathfrak{m}_{\mathfrak{P}} \quad \Longrightarrow \quad y-1 \notin \mathfrak{m}_{\mathfrak{P}}$$

as otherwise $(y+1)-(y-1) = 2 \in \mathfrak{m}_{\mathfrak{P}}$.

Thus, $\upsilon_{\mathfrak{P}}(y-1) = 0$ (note $\upsilon_{\mathfrak{P}}(y-1) \geq 0$ as $y \in \mathcal{O}'_{\mathfrak{p}}$) and so

$$\upsilon_{\mathfrak{P}}(y^2-1) = \upsilon_{\mathfrak{P}}(y+1).$$

Now,

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

where $x^2+2x+3 \in \mathbb{F}_5[x]$ is irreducible.

$\mathfrak{p}_2$ and $\mathfrak{p}_{-2}$

To recap,

$$v_{\mathfrak{P}}(y^2-1) = v_{\mathfrak{P}}(y+1)$$

and

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

where $x^2+2x+3 \in \mathbb{F}_5[x]$ is irreducible.

Therefore,

$$v_{\mathfrak{P}}(y^2-1) = e(\mathfrak{P}/\mathfrak{p}_2) \cdot v_{\mathfrak{p}_2}((x-2)(x^2+2x+3)) = 1.$$

Thus, $v_{\mathfrak{P}}(y+1) = 1$ and so $y+1$ is a local parameter for $\mathfrak{P} = \mathfrak{P}_{2,-1}$.

A similar calculation shows that $y-1$ is a local parameter for $\mathfrak{P}_{2,1}$.

$\mathfrak{p}_2$ and $\mathfrak{p}_{-2}$

As for $\mathfrak{p}_{-2}$, since $y^2 = x^3 - x$ and $x^3 - x \in \mathcal{O}_{\mathfrak{p}_{-2}}$ we have that $y \in \mathcal{O}'_{\mathfrak{p}_{-2}}$. Indeed,

$$\varphi(T) = T^2 - (x^3 - x) \in \mathcal{O}_{\mathfrak{p}_{-2}}[T]$$

is a monic polynomial that vanishes at y.

We have that the projection

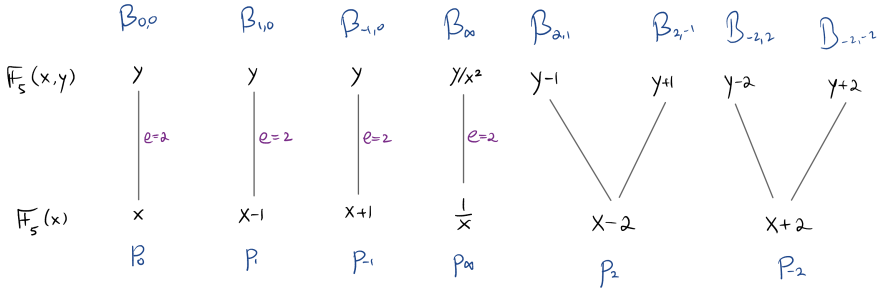
$$\varphi_{-2}(T) = T^2 - ((-2)^3 - (-2)) = T^2 + 1 = (T+2)(T-2).$$

Hence, by Kummer's Theorem, there are two prime divisors lying over $\mathfrak{p}_{-2}$. One $\mathfrak{P}_{-2,-2}$ for which $y + 2 \in \mathfrak{m}_{\mathfrak{P}_{-2,-2}}$, and the other, $\mathfrak{P}_{-2,2}$, satisfies $y - 2 \in \mathfrak{m}_{\mathfrak{P}_{-2,2}}$.

As before, one can show that these are local parameters.

All rational prime divisors so far

We have $\mathrm{N(F)} = 8$ rational prime divisors and recall $g(\mathrm{F}) = 1$.



Overview

Riemann-Roch spaces

We have that

$$(x)_{\mathbb{F}_5(x)} = \mathfrak{p}_0 - \mathfrak{p}_\infty,$$

and so

$$(x)_{\mathsf{F}} = 2\mathfrak{P}_{0,0} - 2\mathfrak{P}_\infty.$$

Now, for $\mathfrak{P} \in \mathbb{P}(\mathsf{F})$,

$$\begin{aligned} \upsilon_{\mathfrak{P}}(y) \neq 0 \quad &\Longleftrightarrow \quad \upsilon_{\mathfrak{P}}(y^2) \neq 0 \quad \Longleftrightarrow \quad \upsilon_{\mathfrak{P}}(x^3 - x) \neq 0 \\ &\Longleftrightarrow \quad \upsilon_{\mathfrak{p}}(x^3 - x) \neq 0, \end{aligned}$$

where $\mathfrak{p} \in \mathbb{P}(\mathbb{F}_5(x))$ is the prime divisor lying under $\mathfrak{P}$.

Thus, the poles and zeros of y are

$$\mathfrak{P}_{0,0}, \mathfrak{P}_{1,0}, \mathfrak{P}_{-1,0}, \mathfrak{P}_\infty.$$

In fact, our previous calculations show that

$$(y)_{\mathsf{F}} = \mathfrak{P}_{0,0} + \mathfrak{P}_{1,0} + \mathfrak{P}_{-1,0} - 3\mathfrak{P}_\infty.$$

Riemann-Roch spaces

In particular,

$$\begin{aligned}(x)_{\mathsf{F},\infty} &= 2\mathfrak{P}_\infty,\\ (y)_{\mathsf{F},\infty} &= 3\mathfrak{P}_\infty.\end{aligned}$$

Thus,

$$\begin{aligned}\mathcal{L}(0\cdot\mathfrak{P}_\infty) &= \mathsf{Span}_{\mathbb{F}_5}\left\{1\right\}\\ \mathcal{L}(1\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1\right\}\\ \mathcal{L}(2\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1,x\right\}\\ \mathcal{L}(3\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1,x,y\right\}\\ \mathcal{L}(4\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1,x,y,x^2\right\}\\ \mathcal{L}(5\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1,x,y,x^2,xy\right\}\\ \mathcal{L}(6\cdot\mathfrak{P}_\infty) &\supseteq \mathsf{Span}_{\mathbb{F}_5}\left\{1,x,y,x^2,xy,x^3\right\}.\end{aligned}$$

But in fact, all are equalities as we now show.

Riemann-Roch spaces

deg-dim = g-1

deg	0	1	2	2g-2	2g-1	2g	...
dim	1			g/g-1	g	g+1	...

canonical ↗

↑ otherwise

Note that $\dim \mathcal{L}(1 \cdot \mathfrak{P}_\infty) = 1$ by Riemann-Roch and since $g(\mathrm{F}) = 1$.

deg-dim = 0

deg	0	1	2	3
dim	1	1	2	3

A little Goppa code

We can take the length $n = 7$ Goppa code over $\mathbb{F}_5$,

$$C = \{\, (z(\mathfrak{P}_{0,0}), z(\mathfrak{P}_{1,0}), z(\mathfrak{P}_{-1,0}), z(\mathfrak{P}_{2,1}), z(\mathfrak{P}_{2,-1}), z(\mathfrak{P}_{-2,2}), z(\mathfrak{P}_{-2,-2})) \\ \mid z \in \mathcal{L}(r \cdot \mathfrak{P}_\infty)\}.$$

E.g., for $r = 3$, as $\mathcal{L}(3 \cdot \mathfrak{P}_\infty) = \mathrm{Span}\,\{1, x, y\}$, the code is generated by

$$(x(\mathfrak{P}_{0,0}), x(\mathfrak{P}_{1,0}), x(\mathfrak{P}_{-1,0}), x(\mathfrak{P}_{2,1}), x(\mathfrak{P}_{2,-1}), x(\mathfrak{P}_{-2,2}), x(\mathfrak{P}_{-2,-2}))\,,$$
$$(y(\mathfrak{P}_{0,0}), y(\mathfrak{P}_{1,0}), y(\mathfrak{P}_{-1,0}), y(\mathfrak{P}_{2,1}), y(\mathfrak{P}_{2,-1}), y(\mathfrak{P}_{-2,2}), y(\mathfrak{P}_{-2,-2}))\,,$$

and the all ones vector, namely, by

$$(0, 1, 4, 2, 2, 3, 3)\,,$$
$$(0, 0, 0, 1, 4, 2, 3)\,,$$
$$(1, 1, 1, 1, 1, 1, 1)\,.$$

It has dimension $k = 3$ and, recall, distance

$$d \geq n - k - g + 1 = 7 - 3 - 1 + 1 = 4.$$

Note MDS codes give for $k = 3$ on block-length $n = 7$ distance $7 - 3 + 1 = 5$. But I think (internet search...) that the above code over $\mathbb{F}_5$ is optimal.

Overview

1. Tame cyclic extensions of $K(x)$
2. Our running example
3. Rational places and the genus
4. Kummer's Theorem
5. Riemann-Roch spaces and a little code
6. The canonical divisor

The canonical divisor

Recall that a divisor $\mathfrak{a}$ is canonical iff $\dim \mathfrak{a} = g$ and $\deg g = 2g - 2$. In our case we are looking for dimension 1, degree 0 divisor.

Thus, the zero divisor is a canonical divisor of a genus 1 function field. Thus, the class of canonical divisors coincides with the class a principal divisors in such function fields.

The duality between functions and differentials on genus 1 function fields (aka elliptic curves) reflects deeper symmetries in the curve's geometry and arithmetic.