Wild towers

Unit 28

Gil Cohen

June 6, 2022

Overview

1. Artin-Schreier extensions
2. Elementary abelian extensions
3. Elementary abelian $\mathfrak{p}$-extensions of $K(x)$
4. The Hermitian tower
5. The Garcia-Stichtenoth tower

Artin-Schreier extensions

Throughout this unit (and as is now typically assumed), K is a perfect field.

Definition 1

Let E/K be a function field of characteristic $p > 0$. Suppose that $u \in \mathrm{E}$ is s.t.

$$\forall v \in \mathrm{E} \qquad u \neq v^p - v.$$

Let

$$\mathrm{F} = \mathrm{E}(y) \quad \text{where} \quad y^p - y = u.$$

The extension F/E is called an Artin-Schreier extension.

Artin-Schreier extensions

$$\mathsf{F} = \mathsf{E}(y) \quad \text{where} \quad y^p - y = u \qquad (\forall v \in \mathsf{E} \quad u \neq v^p - v).$$

For $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ define the integer $m_{\mathfrak{p}}$ as follows: If

$$\exists z \in \mathsf{E} \qquad \upsilon_{\mathfrak{p}}(u - (z^p - z)) \geq 0$$

define $m_{\mathfrak{p}} = -1$. Otherwise, set

$$m_{\mathfrak{p}} = -\max_{z \in \mathsf{E}} \upsilon_{\mathfrak{p}}(u - (z^p - z)).$$

Claim 2

$$\forall \mathfrak{p} \in \mathbb{P}(\mathsf{E}) \qquad \gcd(p, m_{\mathfrak{p}}) = 1.$$

Artin-Schreier extensions

To prove Claim 2 we need two claims.

Claim 3

Let K be a perfect field and M a finite extension of K. Then,

$$\forall z \in \mathrm{M} \quad \exists y \in \mathrm{M} \ \text{ s.t } \ z = y^p.$$

Proof.

Denote

$$f(T) = T^p - z \in \mathrm{M}[T].$$

Let $\alpha \in \bar{\mathrm{M}}$ be a root of $f(T)$. Then,

$$z = \alpha^p \quad \Longrightarrow \quad f(T) = T^p - \alpha^p = (T - \alpha)^p.$$

Thus, the minimal polynomial $f(T)$ of α over M is of the form

$$f(T) = (T - \alpha)^m \in \mathrm{M}[T]$$

for some $1 \leq m \leq p$.

Artin-Schreier extensions

Proof.

The minimal polynomial $f(T)$ of α over M is of the form

$$f(T) = (T - \alpha)^m \qquad 1 \leq m \leq p.$$

Unless $m = 1$, the extension $\mathrm{M}(\alpha)/\mathrm{M}$ is inseparable, and then so is $\mathrm{M}(\alpha)/\mathrm{K}$.

But $\mathrm{M}(\alpha)/\mathrm{K}$ is finite, which contradicts K being perfect.

Artin-Schreier extensions

Claim 4

For every $x_1, x_2 \in \mathsf{E}^\times$ with $\upsilon_\mathfrak{p}(x_1) = \upsilon_\mathfrak{p}(x_2)$ there exists $y \in \mathsf{E}$ s.t.

1. $\upsilon_\mathfrak{p}(y) = 0$; and
2. $\upsilon_\mathfrak{p}(x_1 - y^p x_2) > \upsilon_\mathfrak{p}(x_1)$.

Proof.

As $\upsilon_\mathfrak{p}(\frac{x_1}{x_2}) = 0$ we have $\bar{z} \triangleq (\frac{x_1}{x_2})(\mathfrak{p}) \neq 0$ and so by Claim 3,

$$\exists \bar{y} \in \mathsf{E}_\mathfrak{p} \quad \bar{y}^p = \bar{z}.$$

Let $y \in \mathcal{O}_\mathfrak{p}$ be s.t. $y(\mathfrak{p}) = \bar{y}$. Then, $\upsilon_\mathfrak{p}(y) = 0$, and

$$\upsilon_\mathfrak{p}\left(y^p - \frac{x_1}{x_2}\right) > 0 \quad \Longrightarrow \quad \upsilon_\mathfrak{p}(x_1 - y^p x_2) > \upsilon_\mathfrak{p}(x_1).$$

Proof. (Proof of Claim 2)

To prove the claim we show that if there is $z_1 \in \mathsf{E}$ s.t.

$$\upsilon_{\mathfrak{p}}(u - (z_1^p - z_1)) = -\ell p < 0$$

then there is $z_2 \in \mathsf{E}$ s.t.

$$\upsilon_{\mathfrak{p}}(u - (z_2^p - z_2)) > -\ell p.$$

Indeed, take $t \in \mathsf{E}$ with $\upsilon_{\mathfrak{p}}(t) = -\ell$ and note that

$$\upsilon_{\mathfrak{p}}(u - (z_1^p - z_1)) = \upsilon_{\mathfrak{p}}(t^p).$$

By Claim 4, invoked with

$$x_1 = u - (z_1^p - z_1) \qquad x_2 = t^p$$

we can find $y \in \mathsf{E}$ with $\upsilon_{\mathfrak{p}}(y) = 0$ and

$$\upsilon_{\mathfrak{p}}(u - (z_1^p - z_1) - (yt)^p) > -\ell p.$$

Artin-Schreier extensions

Proof.

$$v_{\mathfrak{p}}(u - (z_1^p - z_1) - (yt)^p) > -\ell p.$$

As

$$v_{\mathfrak{p}}(yt) = v_{\mathfrak{p}}(t) = -\ell > -\ell p,$$

we get

$$v_{\mathfrak{p}}(u - (z_1^p - z_1) - ((yt)^p - yt)) > -\ell p.$$

The proof then follows by setting $z_2 = z_1 + yt$. □

Artin-Schreier extensions

Recall the notation of Definition 1,

$$\mathsf{F} = \mathsf{E}(y) \quad \text{where} \quad y^p - y = u \quad \text{with} \quad u \in \mathsf{E}.$$

Theorem 5

F/E *is a cyclic Galois extension of degree* p*. Moreover,*

$$\mathrm{Gal}(\mathsf{F}/\mathsf{E}) = \{\sigma_\nu \mid \nu = 0, 1, \ldots, p-1\}$$

with

$$\sigma_\nu(y) = y + \nu \quad \text{for} \quad \nu = 0, 1, \ldots, p-1.$$

I will leave it to you to prove this theorem though note that for every ν as above

$$y^p - y = u \quad \Longrightarrow \quad (y+\nu)^p - (y+\nu) = u$$

and so the E-conjugates of y are $y + \nu$ for $\nu = 0, 1, \ldots, p-1$.

Artin-Schreier extensions

Theorem 6

With the notation of Definition 1,

1. $e(\mathfrak{p}) = 1 \iff m_{\mathfrak{p}} = -1.$
2. $e(\mathfrak{p}) = p \iff m_{\mathfrak{p}} > 0.$

Moreover,

$$\forall \mathfrak{P}/\mathfrak{p} \qquad d(\mathfrak{P}/\mathfrak{p}) = (m_{\mathfrak{p}} + 1)(p-1).$$

Artin-Schreier extensions

Proof.

Assume $m_{\mathfrak{p}} = -1$, namely,

$$\exists z \in \mathsf{E} \qquad \upsilon_{\mathfrak{p}}(u - (z^p - z)) \geq 0.$$

Denote

$$y_1 = y - z \qquad u_1 = u - (z^p - z),$$

and note that $\mathsf{F} = \mathsf{E}(y) = \mathsf{E}(y_1)$ and that

$$\varphi(T) = T^p - T - u_1$$

is the minimal polynomial of y_1 over E. Indeed,

$$\begin{aligned} \varphi(y_1) &= (y - z)^p - (y - z) - u_1 \\ &= y^p - y - (z^p - z) - u_1 \\ &= y^p - y - u = 0, \end{aligned}$$

and since the degree of y_1-s minimal polynomial is p.

Artin-Schreier extensions

Proof.

$$\exists z \in \mathrm{E} \qquad \upsilon_{\mathfrak{p}}(u-(z^p-z)) \geq 0.$$

Denote

$$y_1 = y - z \qquad\qquad u_1 = u - (z^p - z),$$

and let

$$\varphi(T) = T^p - T - u_1$$

be the minimal polynomial of y_1 over E.

As $\upsilon_{\mathfrak{p}}(u_1) \geq 0$ we have that $y_1 \in \mathcal{O}'_{\mathfrak{p}}$. Thus, by a theorem we proved (F/E is finite and separable),

$$\forall \mathfrak{P}/\mathfrak{p} \qquad 0 \leq d(\mathfrak{P}/\mathfrak{p}) \leq \upsilon_{\mathfrak{P}}(\varphi'(y_1)) = \upsilon_{\mathfrak{P}}(-1) = 0.$$

Dedekind Different Theorem then implies $e(\mathfrak{P}/\mathfrak{p}) = 1$.

Proof.

We turn to prove that

$$m_{\mathfrak{p}} > 0 \quad \Longrightarrow \quad e(\mathfrak{p}) = p.$$

Note that this will complete the proof, but for the computation of the different exponent, as $e(\mathfrak{p}) \in \{1, p\}$.

Let $z \in \mathrm{E}$ be s.t.

$$\upsilon_{\mathfrak{p}}(u - (z^p - z)) = -m_{\mathfrak{p}}.$$

Set

$$y_1 = y - z \qquad u_1 = u - (z^p - z).$$

Again we have that $\varphi(T) = T^p - T - u_1$ is the minimal polynomial of y_1 over E. For every $\mathfrak{P}/\mathfrak{p}$,

$$e(\mathfrak{P}/\mathfrak{p}) \cdot (-m_{\mathfrak{p}}) = e(\mathfrak{P}/\mathfrak{p}) \cdot \upsilon_{\mathfrak{p}}(u_1) = \upsilon_{\mathfrak{P}}(u_1) = \upsilon_{\mathfrak{P}}(y_1^p - y_1) = p \cdot \upsilon_{\mathfrak{P}}(y_1).$$

Artin-Schreier extensions

Proof.

$$-m_{\mathfrak{p}} \cdot e(\mathfrak{P}/\mathfrak{p}) = p \cdot \upsilon_{\mathfrak{P}}(y_1). \tag{1}$$

By Claim 2, $\gcd(p, m_{\mathfrak{p}}) = 1$ and so, using also the fundamental equality,

$$e(\mathfrak{P}/\mathfrak{p}) = p.$$

We turn to prove that

$$\forall \mathfrak{P}/\mathfrak{p} \qquad d(\mathfrak{P}/\mathfrak{p}) = (m_{\mathfrak{p}} + 1)(p-1).$$

Note that this follows by Dedekind's Different Theorem when $m_{\mathfrak{p}} = -1$, and so we assume $m_{\mathfrak{p}} > 0$.

By Equation (1),

$$\upsilon_{\mathfrak{P}}(y_1) = -m_{\mathfrak{p}}.$$

Artin-Schreier extensions

Proof.

Let x be a local parameter for $\mathfrak{p}$. By Claim 2, we can find $i, j \geq 0$ s.t.

$$1 = ip - jm_{\mathfrak{p}}.$$

Therefore

$$t \triangleq x^i y_1^j$$

is a local parameter for $\mathfrak{P}$. Indeed,

$$\upsilon_{\mathfrak{P}}(x^i y_1^j) = i \cdot e(\mathfrak{P}/\mathfrak{p}) + j \cdot \upsilon_{\mathfrak{P}}(y_1) = ip - jm_{\mathfrak{p}} = 1.$$

By a result we proved, in such case of total ramification,

$$d(\mathfrak{P}/\mathfrak{p}) = \upsilon_{\mathfrak{P}}(\psi'(t)),$$

where $\psi(T) \in \mathrm{E}[T]$ is the minimal polynomial of t over E.

We turn to investigate $\psi(T)$.

Artin-Schreier extensions

Proof.

Let $G = \mathrm{Gal}(F/E)$. Recall that by Theorem 5,

$$\mathrm{Gal}(F/E) = \{\sigma_\nu \mid \nu = 0, 1, \ldots, p-1\}$$

with $\sigma(y_1) = y_1 + \nu$ for $\nu = 0, 1, \ldots, p-1$. Then,

$$\psi(T) = \prod_{\nu \in G} (T - \sigma(t)) = (T - t) \cdot \varphi(T),$$

and so

$$\psi'(T) = \varphi(T) + (T - t)\varphi'(T) \quad \Longrightarrow \quad \psi'(t) = \varphi(t).$$

Thus,

$$d(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\psi'(t)) = v_{\mathfrak{P}}(\varphi(t)) = v_{\mathfrak{P}}\Big(\prod_{\sigma \neq \mathrm{id}} (t - \sigma(t))\Big)$$

$$= \sum_{\sigma \neq \mathrm{id}} v_{\mathfrak{P}}(t - \sigma(t)).$$

Artin-Schreier extensions

Proof.

Fix $\sigma \neq \mathrm{id}$, namely, $\sigma(y_1) = y_1 + \nu$ for some $\nu \in \{1, 2, \ldots, p-1\}$. Then,

$$t - \sigma(t) = x^i y_1^j - x^i (y_1 + \nu)^j = -x^i \cdot \sum_{\ell=1}^{j} \binom{j}{\ell} y_1^{j-\ell} \nu^\ell.$$

As $\upsilon_{\mathfrak{p}}(y_1) = -m_{\mathfrak{p}} < 0$, by the strict triangle inequality,

$$\begin{aligned} \upsilon_{\mathfrak{P}}(t - \sigma(t)) &= \upsilon_{\mathfrak{P}}(x^i) + \upsilon_{\mathfrak{P}}(j\nu y_1^{j-1}) \\ &= i \cdot \upsilon_{\mathfrak{P}}(x) + (j-1)\upsilon_{\mathfrak{P}}(y_1) \\ &= ip + (j-1)(-m_{\mathfrak{p}}) \\ &= (ip - jm_{\mathfrak{p}}) + m_{\mathfrak{p}} \\ &= m_{\mathfrak{p}} + 1. \end{aligned}$$

Note that we used that $j \neq 0$ which follows from $ip - jm_{\mathfrak{p}} = 1$.

Artin-Schreier extensions

Proof.

To summarize,

$$d(\mathfrak{P}/\mathfrak{p}) = \sum_{\sigma \neq \mathrm{id}} \upsilon_{\mathfrak{P}}(t - \sigma(t)),$$

$$\upsilon_{\mathfrak{P}}(t - \sigma(t)) = m_{\mathfrak{p}} + 1 \qquad \forall \sigma \neq \mathrm{id}.$$

Thus,

$$d(\mathfrak{P}/\mathfrak{p}) = (m_{\mathfrak{p}} + 1)(|G| - 1) = (m_{\mathfrak{p}} + 1)(p - 1),$$

which concludes the proof.

□

Artin-Schreier extensions

Claim 7

With the notation of Definition 1, if there is $\mathfrak{p} \in \mathbb{P}(E)$ with $m_{\mathfrak{p}} > 0$ then K is the full constant field of F and

$$g_F = g_E \cdot p + \frac{p-1}{2}\left(-2 + \sum_{\mathfrak{p} \in \mathbb{P}(E)} (m_{\mathfrak{p}} + 1) \cdot \deg \mathfrak{p}\right).$$

That K is the full constant field is proven similarly to the Kummer case.

The genus computation is immediate given Theorem 6 using Hurwitz Genus Formula, so we omit the proofs.

Artin-Schreier extensions

We remark that the condition

$$\forall v \in \mathsf{E} \qquad u \neq v^p - v.$$

follows if there is $\mathfrak{P} \in \mathbb{P}(\mathsf{F})$ for which

$$\upsilon_{\mathfrak{P}}(u) < 0 \quad \& \quad (p, v_{\mathfrak{P}}(u)) = 1.$$

Indeed, if $u = v^p - v$ then $\upsilon_{\mathfrak{P}}(v) < 0$ (otherwise $\upsilon_{\mathfrak{p}}(v^p - v) \geq 0$) and so

$$\upsilon_{\mathfrak{P}}(u) = \upsilon_{\mathfrak{P}}(v^p - v) = p \cdot \upsilon_{\mathfrak{P}}(v),$$

which contradicts $(p, v_{\mathfrak{P}}(u)) = 1$.

It can be shown that every cyclic extension of degree that is equal to the characteristic is Artin-Schreier. We proceed to consider a generalization.

Overview

1. Artin-Schreier extensions
2. Elementary abelian extensions
3. Elementary abelian $\mathfrak{p}$-extensions of $K(x)$
4. The Hermitian tower
5. The Garcia-Stichtenoth tower

Elementary abelian extensions

The above can be generalized to the so-called elementary abelian extension or in their other name Artin-Schreier type extensions.

A polynomial of the form

$$h(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 \in \mathrm{K}[T],$$

where $\operatorname{char} \mathrm{K} = p$, is called an additive (linearized) polynomial. Indeed,

$$\forall u, v \in \bar{\mathrm{K}} \qquad h(u+v) = h(u) + h(v).$$

Note that $h(T)$ is separable over K iff $a_0 \neq 0$. Indeed, separability holds iff $h(T)$ and $h'(T)$ have no common factor of degree > 0, but $h'(T) = a_0$.

Hence, if $h(T)$ is a separable polynomial having its roots in K then the roots form a subgroup of the additive group $(\mathrm{K}, +)$ of order p^n.

Elementary abelian extensions

Let E/K be a function field, $\operatorname{char} \mathsf{K} = p > 0$. Let $h(T)$ be a degree p^n additive separable polynomial whose roots are in K.

Let $u \in \mathsf{E}$ and suppose that for each $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ either

$$\exists z = z(\mathfrak{p}) \in \mathsf{E} \qquad \upsilon_{\mathfrak{p}}(u - h(z)) \geq 0,$$

or

$$(p, \max_{z \in \mathsf{E}}(\upsilon_{\mathfrak{p}}(u - h(z)))) = 1.$$

Define $m_{\mathfrak{p}} \triangleq -1$ in the first case, and otherwise

$$m_{\mathfrak{p}} \triangleq -\max_{z \in \mathsf{E}} \upsilon_{\mathfrak{p}}(u - h(z)).$$

For example, when $h(z) = z^p - z$ we proved this is the case in Claim 2.

Let

$$\mathsf{F} = \mathsf{E}(y) \qquad h(y) = u.$$

Elementary abelian extensions

Theorem 8

With the above notation, if there is $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *with* $m_{\mathfrak{p}} > 0$ *the following holds:*

1. F/E *is Galois with Galois group isomorphic to* $(\mathbb{Z}/p\mathbb{Z})^n$.
2. K *is the full constant field of* F.
3. *Each* $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *with* $m_{\mathfrak{p}} = -1$ *is unramified in* F/E.
4. *Each* $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *with* $m_{\mathfrak{p}} > 0$ *is totally ramified in* F/E.
5. $d(\mathfrak{P}/\mathfrak{p}) = (p^n - 1)(m_{\mathfrak{p}} + 1)$.
6. *Lastly,*

$$g_{\mathsf{F}} = p^n \cdot g_{\mathsf{E}} + \frac{p^n - 1}{2}\left(-2 + \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} (m_{\mathfrak{p}} + 1) \cdot \deg \mathfrak{p}\right).$$

Overview

1. Artin-Schreier extensions
2. Elementary abelian extensions
3. Elementary abelian $\mathfrak{p}$-extensions of $K(x)$
4. The Hermitian tower
5. The Garcia-Stichtenoth tower

Elementary abelian $\mathfrak{p}$-extensions of $\mathsf{K}(x)$

Consider the function field $\mathsf{F} = \mathsf{K}(x, y)$ with

$$y^q + \mu y = f(x) \in \mathsf{K}[x],$$

where $q = p^s > 1$ ($p = \operatorname{char} \mathsf{K}$) and $\mu \in \mathsf{K}^\times$.

Assume $m \triangleq \deg f > 0$ is prime to p, and that all roots $T^q + \mu T$ are in K.

Elementary abelian $\mathfrak{p}$-extensions of $\mathsf{K}(x)$

Theorem 9

1. $[\mathsf{F} : \mathsf{K}(x)] = q$, *and* K *is the full constant field of* F.
2. $\mathsf{F}/\mathsf{K}(x)$ *is Galois. Moreover, the set*

$$\Gamma = \{\gamma \in \mathsf{K} \mid \gamma^q + \mu\gamma = 0\}$$

is a subgroup of order q *of* $(\mathsf{K}, +)$. *Moreover,*

$$\begin{aligned} \Gamma &\to \mathsf{Gal}(\mathsf{F}/\mathsf{K}(x)) \\ \gamma &\mapsto \sigma_\gamma, \end{aligned}$$

where $\sigma_\gamma(y) = y + \gamma$ *is a group isomorphism.*

3. $\mathfrak{p}_\infty \in \mathbb{P}(\mathsf{K}(x))$ *is totally ramified. It is the only prime divisor of* $\mathsf{K}(x)$ *that ramifies.*
4. *The genus of* F *is*

$$g_{\mathsf{F}} = \frac{(q-1)(m-1)}{2}.$$

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

First one needs to prove an analog to Claim 2 but we omit the proof.

We turn to show that $m_{\mathfrak{p}_\infty} = m$. Indeed, taking $z = 0$,

$$v_{\mathfrak{p}_\infty}(f(x) - (z^q + \mu z)) = v_{\mathfrak{p}_\infty}(f(x)) = -m.$$

Now, recall that

$$m_{\mathfrak{p}_\infty} = -\max_{z \in K(x)} v_{\mathfrak{p}_\infty}(f(x) - (z^q + \mu z)),$$

and so if $m_{\mathfrak{p}_\infty} \neq m$ then $m_{\mathfrak{p}_\infty} < m$, and so

$$\exists z \in K(x) \qquad v_{\mathfrak{p}_\infty}(f(x) - (z^q + \mu z)) > -m = v_{\mathfrak{p}_\infty}(f(x)).$$

This is only possible if

$$-m = v_{\mathfrak{p}_\infty}(f(x)) = v_{\mathfrak{p}_\infty}(z^q + \mu z) = q \cdot v_{\mathfrak{p}_\infty}(z),$$

which contradicts $(m, q) = 1$.

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

Thus, Items 1,2 follows by Theorem 8.

As $f(x) \in K[x]$ for every $\mathfrak{p} \in \mathbb{P}(K(x)) \setminus \{\mathfrak{p}_\infty\}$,

$$v_{\mathfrak{p}}(f(x) - (z^q + \mu z)) \geq v_{\mathfrak{p}}(f(x)) \geq 0,$$

and so, by Theorem 8, $\mathfrak{p}_\infty$ is the only prime divisor that ramifies, and it totally ramifies. By Theorem 8,

$$\begin{aligned} g_F &= q \cdot g_{K(x)} + \frac{q-1}{2}\left(-2 + \sum_{\mathfrak{p} \in \mathbb{P}(K(x))} (m_{\mathfrak{p}} + 1) \cdot \deg \mathfrak{p}\right) \\ &= \frac{q-1}{2}(-2 + (m+1) \cdot 1) \\ &= \frac{(q-1)(m-1)}{2}. \end{aligned}$$

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Theorem (Theorem 9 continued)

Still with the notation above, let $\mathfrak{P}_\infty \in \mathbb{P}(F)$ be the unique prime divisor lying over $\mathfrak{p}_\infty$. Then,

$$(x)_{\mathfrak{P}_\infty} = q \cdot \mathfrak{P}_\infty,$$
$$(y)_{\mathfrak{P}_\infty} = m \cdot \mathfrak{P}_\infty.$$

Moreover, for every $r \geq 0$,

$$\mathcal{L}(r \cdot \mathfrak{P}_\infty) = \mathrm{Span}\left\{x^i y^j \;\middle|\; 0 \leq i,\ 0 \leq j \leq q-1,\ qi + mj \leq r\right\}.$$

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

That

$$(x)_{\mathfrak{P}_\infty} = q \cdot \mathfrak{P}_\infty$$

follows as $e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) = q$.

Now, if $\mathfrak{P} \in \mathbb{P}(F)$ is a pole of y then

$$v_{\mathfrak{P}}(y^q + \mu y) < 0 \quad \Longrightarrow \quad v_{\mathfrak{P}}(f(x)) < 0 \quad \Longrightarrow \quad v_{\mathfrak{P}}(x) < 0,$$

and so the only pole of y is $\mathfrak{P}_\infty$. Now,

$$v_{\mathfrak{P}_\infty}(y^q + \mu y) = v_{\mathfrak{P}_\infty}(f(x)) = e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) \cdot v_{\mathfrak{p}_\infty}(f(x)) = q \cdot (-m).$$

Thus,

$$v_{\mathfrak{P}_\infty}(y^q + \mu y) = v_{\mathfrak{P}_\infty}(y^q) = q \cdot v_{\mathfrak{P}_\infty}(y),$$

and so

$$v_{\mathfrak{P}_\infty}(y) = -m.$$

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

We move on to prove that

$$\mathcal{L}(r \cdot \mathfrak{P}_\infty) = \text{Span}\left\{x^i y^j \;\middle|\; 0 \le i,\ 0 \le j \le q-1,\ qi + mj \le r\right\}.$$

The $\supseteq$ inclusion is trivial.

For the $\subseteq$ direction, recall that $1, y, \ldots, y^{q-1}$ is a local integral basis of $F/K(x)$ at $\mathfrak{p}$ iff

$$\forall \mathfrak{P}/\mathfrak{p} \qquad d(\mathfrak{P}/\mathfrak{p}) = \upsilon_{\mathfrak{P}}(\varphi'(y)),$$

where $\varphi(T) \in K(x)[T]$ is the minimal polynomial of y over $K(x)$.

In our case, the minimal polynomial of y over $K(x)$ is

$$\varphi(T) = T^q + \mu T - f(x) \in K(x)[T],$$

which is contained in $\mathcal{O}_{\mathfrak{p}}[T]$ for every $\mathfrak{p} \neq \mathfrak{p}_\infty$.

Elementary abelian $\mathfrak{p}$-extensions of $\mathrm{K}(x)$

Proof.

Fix $\mathfrak{p} \neq \mathfrak{p}_\infty$. As $\varphi'(T) = \mu$

$$\forall \mathfrak{P}/\mathfrak{p} \qquad \upsilon_{\mathfrak{P}}(\varphi'(y)) = \upsilon_{\mathfrak{P}}(\mu) = 0 = d(\mathfrak{P}/\mathfrak{p}),$$

where the last equality follows by Dedekind Different Theorem and since $\mathfrak{p}_\infty$ is the only prime divisor that ramifies.

Thus, $1, y, \ldots, y^{q-1}$ is a local integral basis at $\mathfrak{p}$.

Take $z \in \mathcal{L}(r \cdot \mathfrak{P}_\infty)$ and write

$$z = \sum_{j=0}^{q-1} z_j y^j \qquad z_j \in \mathrm{K}(x).$$

As $\mathfrak{P}_\infty$ is the only pole of z, we have that

$$\forall \mathfrak{p} \neq \mathfrak{p}_\infty \qquad z \in \mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y].$$

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

$$z = \sum_{j=0}^{q-1} z_j y^j \qquad z_j \in K(x),$$

$$\forall \mathfrak{p} \neq \mathfrak{p}_\infty \qquad z \in \mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y].$$

Thus,

$$\forall j \quad z_j \in K[x],$$

and so we can write

$$z = \sum_{j=0}^{q-1} \sum_{i \geq 0} a_{ij} x^i y^j$$

The different summands have distinct pole orders as $(q, m) = 1$ and

$$\upsilon_{\mathfrak{P}_\infty}(x^i y^j) = iq + jm.$$

The proof follows by the strict triangle inequality.

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Theorem (Theorem 9 continued)

Still with the notation above, for every $\alpha \in K$ the equation

$$T^q + \mu T = f(\alpha)$$

either has q distinct roots in K or no roots in K.

In the first case, if

$$\beta^q + \mu\beta = f(\alpha)$$

then there is a unique prime divisor $\mathfrak{P}_{\alpha,\beta}/\mathfrak{p}_\alpha$ s.t. $y(\mathfrak{P}_{\alpha,\beta}) = \beta$. In particular, $\mathfrak{p}_\alpha$ splits completely.

In the second case, all extensions of $\mathfrak{p}_\infty$ have degree > 1.

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

If there is $\beta \in K$ s.t.

$$\beta^q + \mu\beta = f(\alpha)$$

then for every γ s.t.

$$\gamma^q + \mu\gamma = 0$$

(and we assume there are q such γ-s in K),

$$(\beta + \gamma)^q + \mu(\beta + \gamma) = f(\alpha).$$

Hence,

$$T^q + \mu T - f(\alpha) = \prod_{j=1}^{q}(T - \beta_j),$$

for distinct $\beta_1, \ldots, \beta_q \in K$.

The proof for this case follows by Kummer's Theorem.

Elementary abelian $\mathfrak{p}$-extensions of $K(x)$

Proof.

In the second case,

$$T^q + \mu T - f(\alpha)$$

has no irreducible factor of degree 1 and so, by Kummer's Theorem,

$$\forall \mathfrak{P}/\mathfrak{p} \quad f(\mathfrak{P}/\mathfrak{p}) > 1,$$

as required. □

Overview

1. Artin-Schreier extensions
2. Elementary abelian extensions
3. Elementary abelian $\mathfrak{p}$-extensions of $K(x)$
4. The Hermitian tower
5. The Garcia-Stichtenoth tower

The Hermitian tower

Definition 10

Let p be a prime and $q = p^m$. The Hermitian function field over $\mathbb{F}_{q^2}$ is defined by

$$\mathbb{F}_{q^2}(x, y) \quad \text{where} \quad y^q + y = x^{q+1}.$$

Note that the LHS and RHS are the trace and norm functions, respectively, from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$. That is,

$$\mathrm{Tr}(y) = \mathrm{N}(x).$$

The Hermitian tower

Theorem 11

The Hermitian function field $\mathsf{H}/\mathbb{F}_{q^2}$ has the following properties:

1. *It has*
$$\mathsf{N}(\mathsf{H}) = q^3 + 1$$
rational prime divisors: the unique prime divisor lying over $\mathfrak{p}_\infty \in \mathbb{P}(\mathbb{F}_{q^2}(x))$, and for each $\alpha \in \mathbb{F}_{q^2}$ and each of the q elements $\beta \in \mathbb{F}_{q^2}$ satisfying $\beta^q + \beta = \alpha^{q+1}$, there is a unique rational prime divisor $\mathfrak{P}_{\alpha,\beta}$ that lies over $\mathfrak{p}_\alpha$. Moreover,
$$x(\mathfrak{P}_{\alpha,\beta}) = \alpha \qquad y(\mathfrak{P}_{\alpha,\beta}) = \beta.$$
2. *Its genus*
$$g_{\mathsf{H}} = \frac{q(q-1)}{2}.$$
3. *For every $r \geq 0$,*
$$\mathcal{L}(r \cdot \mathfrak{P}_\infty) = \left\{ x^i y^j \;\middle|\; 0 \leq i,\ 0 \leq j \leq q-1,\ iq + j(q+1) \leq r \right\}$$

The Hermitian tower

Proof.

We wish to apply Theorem 9. First note that indeed $(q+1, p) = 1$.

Second, we need to verify that all roots of $T^q + T$ are in $\mathbb{F}_{q^2}$.

Indeed, $T^q + T$ is an $\mathbb{F}_q$-linear map from $\mathbb{F}_q^2$ (here we ignore the multiplicative structure of $\mathbb{F}_{q^2}$) to $\mathbb{F}_q$ that is onto. Thus, its kernel is a one dimensional subspace of $\mathbb{F}_q^2$. In particular, there are q solutions in $\mathbb{F}_{q^2}$ to $T^q + T = 0$.

Considering the cosets of the kernel, for every $\alpha \in \mathbb{F}_{q^2}$, $\alpha^{q+1} \in \mathbb{F}_q$, and so there are q solutions in $\mathbb{F}_{q^2}$ to

$$T^q + T = \alpha^{q+1}.$$

The proof readily follows from Theorem 9 and by Kummer's Theorem.

The Hermitian tower

Let p be a prime and $q = p^m$. Consider now the recursive tower $\mathcal{H} = (\mathrm{H}_0, \mathrm{H}_1, \ldots)$ over $\mathbb{F}_{q^2}$ with the defining equation

$$Y^q + Y = X^{q+1}.$$

Namely, $\mathrm{H}_0 = \mathbb{F}_{q^2}(x_0)$ and

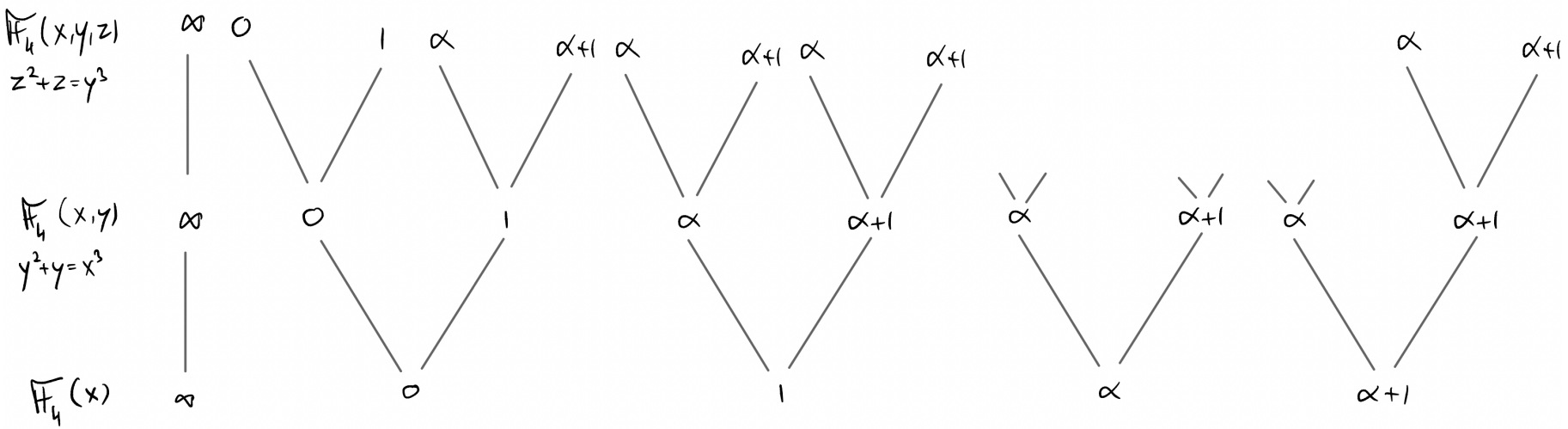
$$\mathrm{H}_i = \mathbb{F}_q(x_0, \ldots, x_i) \qquad x_i^q + x_i = x_{i-1}^{q+1}.$$

It is easy to see that Theorem 11 implies that

$$\mathrm{N}(\mathrm{H}_i) = q^{i+2} + 1$$

We turn to analyze the genus $g_i = g(\mathrm{H}_i)$ but before doing so, a picture.

The Hermitian tower



Here

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) \qquad \alpha^2 + \alpha + 1 = 0.$$

The Hermitian tower

We know that

$$g_0 = 0 \qquad g_1 = \frac{q(q-1)}{2}.$$

We turn to compute g_2, the genus of $\mathsf{H}_2/\mathbb{F}_{q^2}$, namely,

$$\mathbb{F}_{q^2}(x,y,z) \qquad y^q + y = x^{q+1}, \quad z^q + z = y^{q+1}.$$

To this end we invoke Theorem 8 which states that

$$g_2 = q \cdot g_1 + \frac{q-1}{2}\left(-2 + \sum_{\mathfrak{P} \in \mathbb{P}(\mathsf{H}_1)} (m_{\mathfrak{P}} + 1) \cdot \deg \mathfrak{P}\right).$$

By Theorem 8 and since the only prime divisor of H_1 with $m_{\mathfrak{P}} > 0$ is the prime divisor $\mathfrak{P}_\infty$, the unique prime divisor lying over $\mathfrak{p}_\infty \in \mathbb{P}(\mathbb{F}_{q^2}(x))$, we have

$$\begin{aligned} g_2 &= q \cdot g_1 + \frac{q-1}{2}\left(m_{\mathfrak{P}_\infty} - 1\right) \\ &= \frac{q-1}{2}\left(q^2 + m_{\mathfrak{P}_\infty} - 1\right). \end{aligned}$$

The Hermitian tower

Now,

$$-m_{\mathfrak{P}_\infty} = \max_{w \in \mathsf{H}_1} v_{\mathfrak{P}_\infty}\left(y^{q+1} - (w^q + w)\right).$$

First, a standard calculation shows that

$$v_{\mathfrak{P}_\infty}(y) = -(q+1).$$

Thus,

$$v_{\mathfrak{P}_\infty}\left(y^{q+1} - (w^q + w)\right) \geq -(q+1)^2.$$

Equality can be shown using that $(q, q+1) = 1$. Thus,

$$m_{\mathfrak{P}_\infty} = (q+1)^2$$

and so

$$g_2 = \frac{q-1}{2}\left(q^2 + m_{\mathfrak{P}_\infty} - 1\right) = q(q^2-1).$$

The Hermitian tower

$$g_0 = 0 \qquad g_1 = \frac{q(q-1)}{2} \qquad g_2 = q(q^2-1).$$

Using this argument throughout the tower, we get that

$$\begin{aligned} g_i &= q \cdot g_{i-1} + \frac{q-1}{2}\left(-2 + \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{H}_{i-1})} (m_{\mathfrak{p}} + 1) \cdot \deg \mathfrak{p}\right) \\ &= q \cdot g_{i-1} + \frac{q-1}{2}\left(m_{\infty}^{(i-1)} - 1\right) \\ &= q \cdot g_{i-1} + \frac{q-1}{2}\left((q+1)^i - 1\right) \\ &\approx q \cdot g_{i-1} + \frac{q^{i+1}}{2}. \end{aligned}$$

Thus,

$$g_i \approx \frac{i}{2} \cdot q^{i+1}.$$

The Hermitian tower

$$n_i = q^{i+2} + 1 \qquad g_i \approx \frac{i}{2} \cdot q^{i+1}.$$

Thus,

$$\frac{g_i}{n_i} \approx \frac{i}{2q}.$$

So, if we wish to obtain a Goppa code over $\mathbb{F}_{q^2}$ based on the Hermitian tower, having block length (around) n, then we need to pick i s.t.

$$n = n_i = q^{i+2}$$

but then we get

$$\rho + \delta \geq 1 - \frac{g_i}{n_i} = 1 - \Theta\left(\frac{i}{q}\right),$$

and so if we wish to minimize the alphabet size, we are still forced to take $q = \Omega(i)$, and so the best choice is

$$i, q = \Theta\left(\frac{\log n}{\log \log n}\right).$$

Overview

1. Artin-Schreier extensions
2. Elementary abelian extensions
3. Elementary abelian $\mathfrak{p}$-extensions of $K(x)$
4. The Hermitian tower
5. The Garcia-Stichtenoth tower

The Garcia-Stichtenoth Tower

Definition 12

Let p be a prime and $q = p^m$. The Garcia-Stichtenoth function field over $\mathbb{F}_{q^2}$ is defined by

$$\mathbb{F}_{q^2}(x, y) \quad \text{where} \quad y^q + y = \frac{x^q}{x^{q-1} + 1}. \tag{2}$$

The respective recursive tower is denoted by $\mathcal{GS} = (\mathrm{GS}_0, \mathrm{GS}_1, \ldots)$.

The difference between the defining equation of the Hermitian function field and the latter is that the RHS is divided by the trace of x. That is,

$$\mathrm{Tr}(y) = \frac{\mathrm{N}(x)}{\mathrm{Tr}(x)}.$$

The Garcia-Stichtenoth Tower

The $\mathcal{GS}$ tower, was introduced by Garcia and Stichtenoth in their seminal paper "On the asymptotic behavior of some towers of function fields over finite fields" in 1996.

In fact, they used the defining equation

$$y^q - y = \frac{x^q}{1 - x^{q-1}} \tag{3}$$

which defines the same function field - a fact that I leave for you to verify. Hint: use $\alpha \in \mathbb{F}_{q^2}$ with $\alpha^{q-1} = -1$ to change variables (why such α exists?).

We will work with the defining equation given by (3).

The Garcia-Stichtenoth Tower

Lemma 13

Equation (3) does indeed define a recursive tower over $\mathbb{F}_{q^2}$. Moreover, all extensions $\mathrm{GS}_i/\mathrm{GS}_{i-1}$ are Galois of degree q, and $\mathfrak{p}_\infty \in \mathrm{GS}_0$ is totally ramified in all extensions.

Proof.

Separability of $\mathrm{GS}_i/\mathrm{GS}_{i-1}$ is clear, and that this extension is Galois follows as it is an Artin-Schreier type extension.

Let $\mathfrak{P} \in \mathbb{P}(\mathrm{GS}_1)$ be a prime divisor over $\mathfrak{p}_\infty \in \mathbb{P}(\mathrm{GS}_0)$. Then,

$$\begin{aligned} v_{\mathfrak{P}}(y^q - y) &= e(\mathfrak{P}/\mathfrak{p}_\infty) \cdot v_{\mathfrak{p}_\infty}\left(\frac{x^q}{1 - x^{q-1}}\right) \\ &= e(\mathfrak{P}/\mathfrak{p}_\infty) \cdot (-1). \end{aligned}$$

Thus, $v_{\mathfrak{P}}(y^q - y) < 0$ and so

$$-e(\mathfrak{P}/\mathfrak{p}_\infty) = q \cdot v_{\mathfrak{P}}(y) \quad \Longrightarrow \quad e(\mathfrak{P}/\mathfrak{p}_\infty) = q \ \ \& \ \ v_{\mathfrak{P}}(y) = -1.$$

The Garcia-Stichtenoth Tower

Proof.

By the fundamental equality there is a unique prime divisor $\mathfrak{P}_\infty \in \mathbb{P}(\mathrm{GS}_1)$ lying over $\mathfrak{p}_\infty$, and it is rational.

We can iterate this argument and by that show that $\mathfrak{p}_\infty$ totally ramifies in all extensions.

By a result we proved, $\mathbb{F}_{q^2}$ is indeed the constant field of the tower. □

The Garcia-Stichtenoth Tower

Lemma 14

Let $\Sigma \triangleq \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. *Then,*

$$\{\mathfrak{p}_{x_0-\alpha} \mid \alpha \in \Sigma\} \subseteq \mathsf{Split}(\mathcal{GS}).$$

Proof.

By a result we proved, it suffices to show that for every $\alpha \in \Sigma$,

$$h(\alpha) = \frac{\alpha^q}{1-\alpha^{q-1}} \neq \infty \tag{4}$$

and that there are

$$q = \deg f(Y) = \deg(Y^q - Y)$$

solutions $\beta \in \Sigma$ to the equation

$$\beta^q - \beta = \frac{\alpha^q}{1-\alpha^{q-1}}.$$

Proof.

We wish to show that there are q solutions $\beta \in \Sigma$ to the equation

$$\beta^q - \beta = \frac{\alpha^q}{1-\alpha^{q-1}}. \tag{5}$$

To this end, take $\beta \in \overline{\mathbb{F}_q}$ and note that

$$\beta^{q^2} - \beta^q = \frac{\alpha^{q^2}}{(1-\alpha^{q-1})^q} = \frac{\alpha}{(1-\alpha^{q-1})^q},$$

and so

$$\begin{aligned}\beta^{q^2} - \beta &= \frac{\alpha}{(1-\alpha^{q-1})^q} + \frac{\alpha^q}{1-\alpha^{q-1}} \\ &= \frac{(\alpha-\alpha^q)+(\alpha^q-\alpha^{q^2})}{(1-\alpha^{q-1})^{q+1}} = 0.\end{aligned}$$

The Garcia-Stichtenoth Tower

Proof.

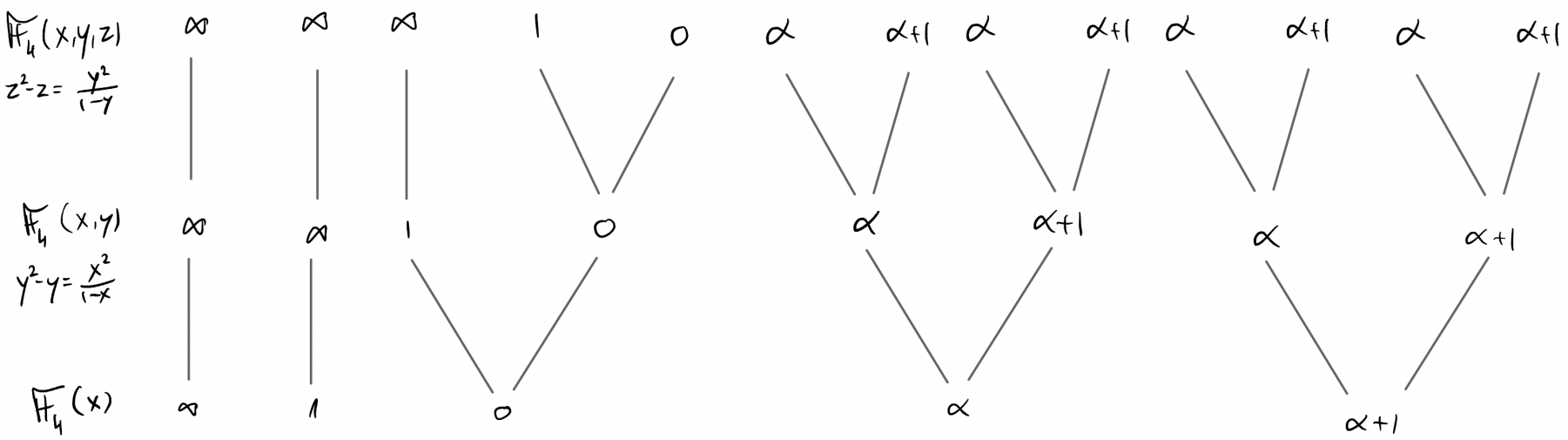
Thus, $\beta \in \mathbb{F}_{q^2}$. To see that $\beta \notin \mathbb{F}_q$ recall that

$$\beta^q - \beta = \frac{\alpha^q}{1 - \alpha^{q-1}} \neq 0.$$

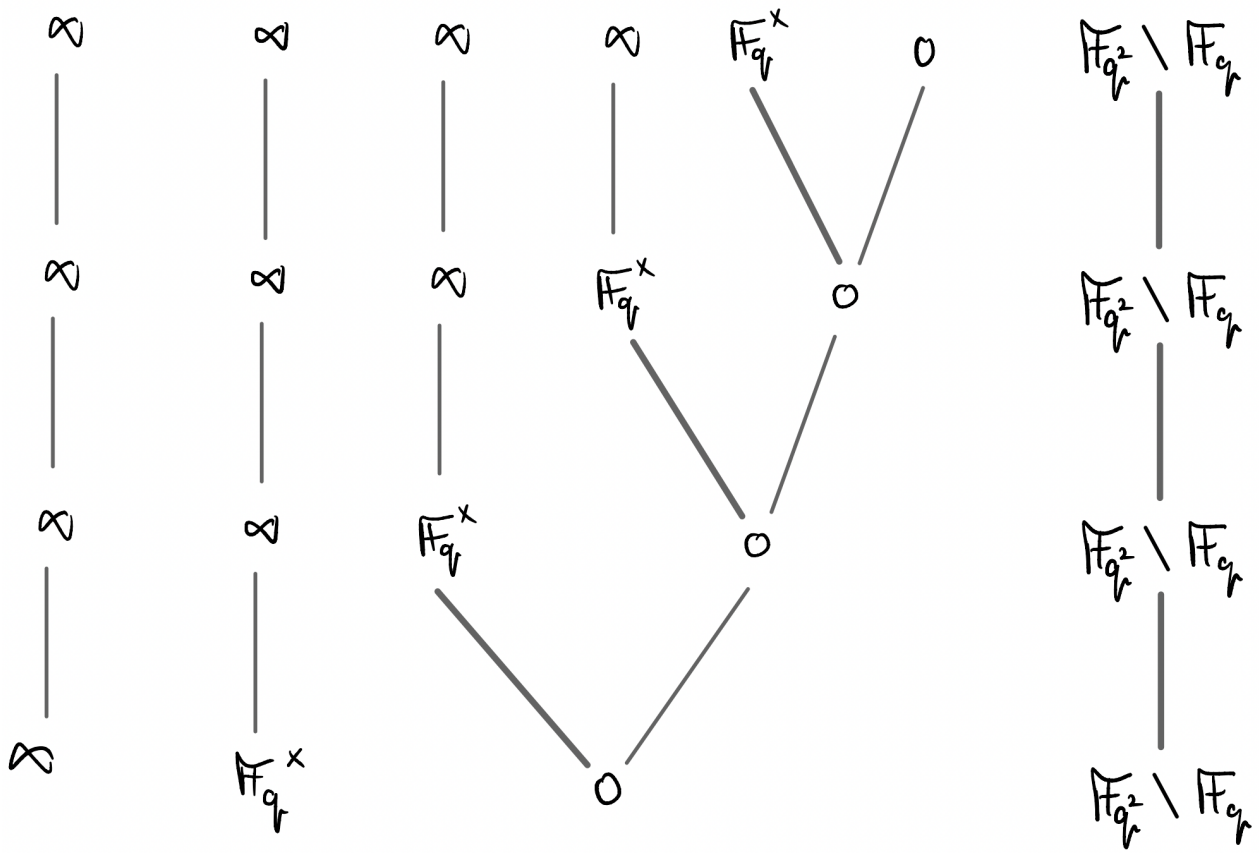
Hence, $\beta \in \Sigma$.

Clearly, Equation (5) has q distinct solutions. The proof then follows by a result we proved.

The Garcia-Stichtenoth Tower



The Garcia-Stichtenoth Tower



Lemma 15

$$\mathrm{Ram}(\mathcal{GS}) \subseteq \{\mathfrak{p}_\alpha \mid \alpha \in \mathbb{F}_q \cup \{\infty\}\}.$$

The Garcia-Stichtenoth Tower

To summarize, by Lemma 14 and Lemma 15

$$s \triangleq |\mathrm{Split}(\mathcal{GS})| \geq |\mathbb{F}_{q^2} \setminus \mathbb{F}_q| = q^2 - q,$$
$$r \triangleq |\mathrm{Ram}(\mathcal{GS})| \leq |\mathbb{F}_q \cup \{\infty\}| = q + 1.$$

Had $\mathcal{GS}$ been a tame tower, a result we proved would have implied that

$$\lambda(\mathcal{GS}) \geq \frac{2s}{r-2} \geq \frac{2q(q-1)}{q-1} = 2q,$$

which would contradict the Drinfeld-Vladut bound $\lambda \leq q - 1$.

However, recall our general bound

$$\lambda(\mathcal{F}) \geq \frac{2s}{2g_0 - 2 + \sum_{\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})} a_{\mathfrak{p}} \deg \mathfrak{p}}$$

where $d(\mathfrak{P}/\mathfrak{p}) \leq a_{\mathfrak{p}} \cdot e(\mathfrak{P}/\mathfrak{p})$.

The Garcia-Stichtenoth Tower

As we will see in the seminar part of the course, for $\mathcal{GS}$

$$d(\mathfrak{P}/\mathfrak{p}) = 2 \cdot (e(\mathfrak{P}/\mathfrak{p}) - 1),$$

and so $a_{\mathfrak{p}} = 2$. We thus have that

$$\begin{aligned}
\lambda(\mathcal{F}) &\geq \frac{2s}{2g_0 - 2 + \sum_{\mathfrak{p} \in \mathsf{Ram}(\mathcal{F})} a_{\mathfrak{p}} \deg \mathfrak{p}} \\
&\geq \frac{2q(q-1)}{-2 + 2(q+1)} \\
&= q - 1,
\end{aligned}$$

and so $\mathcal{GS}$ is optimal.