

Artin-Schreier extensions of minimal genus

Herivelto Borges
(joint with N. Arakelian and M. Coutinho)

ICMC - Universidade de São Paulo

COGNAC CONFERENCE 2023 - CIRM

The problem

- $\mathcal{X} :=$ (projective, non-singular, geometrically irreducible) algebraic curve of genus $g(\mathcal{X}) \geq 2$, defined over an algebraically closed field \mathbb{K} of characteristic $p > 0$, with function field $\mathbb{K}(\mathcal{X})$.

The problem

- $\mathcal{X} :=$ (projective, non-singular, geometrically irreducible) algebraic curve of genus $g(\mathcal{X}) \geq 2$, defined over an algebraically closed field \mathbb{K} of characteristic $p > 0$, with function field $\mathbb{K}(\mathcal{X})$.
- GOAL: To construct curves with many automorphisms.

A strategy

We consider the following general problem:

Let $\mathcal{Y} : f(x, y) = 0$ be a curve of genus $g(\mathcal{Y}) \geq 2$ and p -rank $\gamma(\mathcal{Y}) = 0$. Characterize functions $u \in \mathbb{K}(\mathcal{Y})$ for which the ramified Artin-Schreier cover

$$\mathcal{X} : \begin{cases} z^p - z = u \\ f(x, y) = 0 \end{cases}$$

has the smallest possible genus, that is, $g(\mathcal{X}) = p \cdot g(\mathcal{Y})$.

The minimal genus

Let $g(\mathcal{Y})$ be the genus of the quotient curve $\mathcal{Y} = \mathcal{X}/G$. The Hurwitz genus formula the following equation gives

$$2g(\mathcal{X}) - 2 = |G|(2g(\mathcal{Y}) - 2) + \sum_{P \in \mathcal{X}} d_P, \quad (1)$$

where

$$d_P = \sum_{i \geq 0} \left(|G_P^{(i)}| - 1 \right).$$

In particular, if G is a p -group, then $G_P^{(0)} = G_P^{(1)}$, and then

$$d_P \geq 2(|G_P^{(1)}| - 1).$$

The minimal genus

Let $g(\mathcal{Y})$ be the genus of the quotient curve $\mathcal{Y} = \mathcal{X}/G$. The Hurwitz genus formula the following equation gives

$$2g(\mathcal{X}) - 2 = |G|(2g(\mathcal{Y}) - 2) + \sum_{P \in \mathcal{X}} d_P, \quad (1)$$

where

$$d_P = \sum_{i \geq 0} \left(|G_P^{(i)}| - 1 \right).$$

In particular, if G is a p -group, then $G_P^{(0)} = G_P^{(1)}$, and then

$$d_P \geq 2(|G_P^{(1)}| - 1).$$

-
- if $|G| = p$, then $|G_P^{(0)}| = |G_P^{(1)}| = p$ gives $d_P \geq 2(p - 1)$, and then (1) gives

$$g(\mathcal{X}) \geq p \cdot g(\mathcal{Y}).$$

Back to $\text{Aut}(\mathcal{X})$: a few facts

Let \mathcal{X} be a curve of genus $g(\mathcal{X}) \geq 2$ over an algebraically closed field \mathbb{K} of characteristic $p \geq 0$, with function field $\mathbb{K}(\mathcal{X})$. By definition,

$$\text{Aut}(\mathcal{X}) = \text{Aut}_{\mathbb{K}}(\mathbb{K}(\mathcal{X})).$$

Back to $\text{Aut}(\mathcal{X})$: a few facts

Let \mathcal{X} be a curve of genus $g(\mathcal{X}) \geq 2$ over an algebraically closed field \mathbb{K} of characteristic $p \geq 0$, with function field $\mathbb{K}(\mathcal{X})$. By definition,

$$\text{Aut}(\mathcal{X}) = \text{Aut}_{\mathbb{K}}(\mathbb{K}(\mathcal{X})).$$

- Hurwitz (1893): $p = 0 \implies |\text{Aut}(\mathcal{X})| \leq 84(g - 1)$

Back to $\text{Aut}(\mathcal{X})$: a few facts

Let \mathcal{X} be a curve of genus $g(\mathcal{X}) \geq 2$ over an algebraically closed field \mathbb{K} of characteristic $p \geq 0$, with function field $\mathbb{K}(\mathcal{X})$. By definition,

$$\text{Aut}(\mathcal{X}) = \text{Aut}_{\mathbb{K}}(\mathbb{K}(\mathcal{X})).$$

- Hurwitz (1893): $p = 0 \implies |\text{Aut}(\mathcal{X})| \leq 84(g - 1)$
- Stichtenoth (1973): $|\text{Aut}(\mathcal{X})| < 16g^4$, unless \mathcal{X} is the Hermitian curve.

Back to $\text{Aut}(\mathcal{X})$: a few facts

Let \mathcal{X} be a curve of genus $g(\mathcal{X}) \geq 2$ over an algebraically closed field \mathbb{K} of characteristic $p \geq 0$, with function field $\mathbb{K}(\mathcal{X})$. By definition,

$$\text{Aut}(\mathcal{X}) = \text{Aut}_{\mathbb{K}}(\mathbb{K}(\mathcal{X})).$$

- Hurwitz (1893): $p = 0 \implies |\text{Aut}(\mathcal{X})| \leq 84(g - 1)$
- Stichtenoth (1973): $|\text{Aut}(\mathcal{X})| < 16g^4$, unless \mathcal{X} is the Hermitian curve.
- Henn (1976): $|\text{Aut}(\mathcal{X})| < 8g^3$, up to four exceptions: A certain hyperelliptic curve over $\overline{\mathbb{F}}_2$, the Roquette curve, the Hermitian curve, and the Suzuki curve.

Two more families of curves \mathcal{X} with large $\text{Aut}(\mathcal{X})$

Other examples of curves with large automorphism groups are the **Ree**, and the **GK** curves.

Two more families of curves \mathcal{X} with large $\text{Aut}(\mathcal{X})$

Other examples of curves with large automorphism groups are the **Ree**, and the **GK** curves. All such curves have the following:

Two more families of curves \mathcal{X} with large $\text{Aut}(\mathcal{X})$

Other examples of curves with large automorphism groups are the **R**ee, and the **GK** curves. All such curves have the following:

- **common property:** They all have ZERO p -rank.

Two more families of curves \mathcal{X} with large $\text{Aut}(\mathcal{X})$

Other examples of curves with large automorphism groups are the **Ree**, and the **GK** curves. All such curves have the following:

- **common property:** They all have ZERO p -rank.
- That is, they are curves with no unramified p -cyclic covers.

Zero p-rank vs. Large automorphism groups

- (Nakajima (1987)) Let \mathcal{X} be a curve with $g := g(\mathcal{X}) \geq 2$ and S a Sylow p -subgroup of $\text{Aut}(\mathcal{X})$. If $\gamma = \gamma(\mathcal{X})$ is the p -rank of \mathcal{X} , then

$$|S| \leq \begin{cases} 4(g-1) & \text{if } \gamma > 0 \\ \max \{g, 4pg^2/(p-1)^2\} & \text{if } \gamma = 0 \end{cases}$$

Zero p -rank vs. Large automorphism groups

- (Nakajima (1987)) Let \mathcal{X} be a curve with $g := g(\mathcal{X}) \geq 2$ and S a Sylow p -subgroup of $\text{Aut}(\mathcal{X})$. If $\gamma = \gamma(\mathcal{X})$ is the p -rank of \mathcal{X} , then

$$|S| \leq \begin{cases} 4(g-1) & \text{if } \gamma > 0 \\ \max\{g, 4pg^2/(p-1)^2\} & \text{if } \gamma = 0 \end{cases}$$

- (Giulietti -Korchmáros (2019)) For $p > 2$ and $G \leq \text{Aut}(\mathcal{X})$, there exists a constant $c_p > 0$ such that if $|G| > c_p g^2$, then the p -rank of \mathcal{X} is zero.

p -ranks in p -power Galois covers

Theorem (Deuring-Shafarevich)

Let $G \leq \text{Aut}(\mathcal{X})$ be such that $|G| = p^r$. Then

$$\gamma - 1 = p^r (\gamma' - 1) + \sum_{i=1}^s (p^r - \ell_i),$$

where γ and γ' are the p -ranks of \mathcal{X} and its quotient curve \mathcal{X}/G , while ℓ_1, \dots, ℓ_s are the sizes of the short orbits of G on the points of \mathcal{X} .

p -ranks in p -power Galois covers

Theorem (Deuring-Shafarevich)

Let $G \leq \text{Aut}(\mathcal{X})$ be such that $|G| = p^r$. Then

$$\gamma - 1 = p^r (\gamma' - 1) + \sum_{i=1}^s (p^r - \ell_i),$$

where γ and γ' are the p -ranks of \mathcal{X} and its quotient curve \mathcal{X}/G , while ℓ_1, \dots, ℓ_s are the sizes of the short orbits of G on the points of \mathcal{X} .

Corollary

Let $\mathcal{Y} : f(x, y) = 0$ be a curve with $\gamma(\mathcal{Y}) = 0$. If $\pi : \mathcal{X} \rightarrow \mathcal{Y}$ is an Artin-Schreier extension of minimal genus, then $\gamma(\mathcal{X}) = 0$.

Back to our problem:

Construct curves \mathcal{X} with many automorphisms arising from:

Let $\mathcal{Y} : f(x, y) = 0$ be a curve with many automorphisms (and zero p -rank), and let $u \in \mathbb{K}(\mathcal{Y})$ be a function for which the ramified Artin-Schreier cover

$$\mathcal{X} : \begin{cases} z^p - z = u \\ f(x, y) = 0 \end{cases}$$

has the smallest possible genus, namely $g(\mathcal{X}) = p \cdot g(\mathcal{Y})$.

A prototype

Theorem

Up to isomorphism,

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

is the only Artin-Schreier cover of minimal genus of the Hermitian curve $\mathcal{H} : y^q + y = x^{q+1}$, ramified over $Q_\infty \in \mathcal{H}$.

A prototype

Theorem

Up to isomorphism,

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

is the only Artin-Schreier cover of minimal genus of the Hermitian curve $\mathcal{H} : y^q + y = x^{q+1}$, ramified over $Q_\infty \in \mathcal{H}$.

Proof.

Artin-Schreier theory. □

A curve with many automorphisms

The curve

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

has the following basic properties: It has

- LOW genus $g(\mathcal{X}) = pq(q - 1)/2$.

A curve with many automorphisms

The curve

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

has the following basic properties: It has

- LOW genus $g(\mathcal{X}) = pq(q - 1)/2$.
- MANY rational points

A curve with many automorphisms

The curve

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

has the following basic properties: It has

- LOW genus $g(\mathcal{X}) = pq(q - 1)/2$.
- MANY rational points
- ZERO p-rank

A curve with many automorphisms

The curve

$$\mathcal{X} : y^q + y = (x^p - x)^{q+1}$$

has the following basic properties: It has

- LOW genus $g(\mathcal{X}) = pq(q - 1)/2$.
- MANY rational points
- ZERO p-rank
- A **LARGE** automorphism group.

The automorphism group of \mathcal{X}

Theorem

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then $\text{Aut}(\mathcal{X})$ is given by the set of maps

$$\varphi_{a,b,c} : (x, y) \mapsto (ax + b, a^{q+1}y + a(b^p - b)^q(x^p - x) + c),$$

where $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_{q^2}$, and $b \in \mathbb{K}$ such that $c^q + c = (b^p - b)^{q+1}$.

In particular, $|\text{Aut}(\mathcal{X})| = pq^3(p-1) > 4g(\mathcal{X})^{3/2}$.

The automorphism group of \mathcal{X}

Theorem

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then $\text{Aut}(\mathcal{X})$ is given by the set of maps

$$\varphi_{a,b,c} : (x, y) \mapsto (ax + b, a^{q+1}y + a(b^p - b)^q(x^p - x) + c),$$

where $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_{q^2}$, and $b \in \mathbb{K}$ such that $c^q + c = (b^p - b)^{q+1}$. In particular, $|\text{Aut}(\mathcal{X})| = pq^3(p-1) > 4g(\mathcal{X})^{3/2}$.

- Checking that $\varphi_{a,b,c} \in \text{Aut}(\mathcal{X})$ is straightforward. Since all such maps fix the point $P_\infty \in \mathcal{X}$, we have $pq^3(p-1) \mid \#\text{Aut}(\mathcal{X})_{P_\infty}$, and then the unique Sylow p -subgroup of $\text{Aut}(\mathcal{X})_{P_\infty}$ satisfies

$$\text{Aut}(\mathcal{X})_{P_\infty}^{(1)} \geq pq^3 > pq(q-1) + 1 = 2g(\mathcal{X}) + 1.$$

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

- 1 $\mathbb{G} = \mathbb{G}_P$.

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

- 1 $\mathbb{G} = \mathbb{G}_P$.
- 2 \mathcal{X} is birationally equivalent to one of the following curves:

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

- 1 $\mathbb{G} = \mathbb{G}_P$.
- 2 \mathcal{X} is birationally equivalent to one of the following curves:
 - the Hermitian curve.

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

- 1 $\mathbb{G} = \mathbb{G}_P$.
- 2 \mathcal{X} is birationally equivalent to one of the following curves:
 - the Hermitian curve.
 - the Suzuki curve $\mathbf{v}(X^{n_0}(X^n + X) - (Y^n + Y))$ with $p = 2$, $q = n$, $n_0 = 2^r$, $r \geq 1$, $n = 2n_0^2$ and $g = n_0(n - 1)$.

A special ingredient for the proof

Theorem (Giulletti-Korchmáros (2007))

Let \mathcal{X} be a curve of genus $g \geq 2$ over \mathbb{F}_q , and let $\mathbb{G} \leq \text{Aut}(\mathcal{X})$ be such that $|\mathbb{G}_P^{(1)}| > 2g + 1$ for some point $P \in \mathcal{X}$. Then one of the following cases occurs:

- ① $\mathbb{G} = \mathbb{G}_P$.
- ② \mathcal{X} is birationally equivalent to one of the following curves:
 - the Hermitian curve.
 - the Suzuki curve $\mathbf{v}(X^{n_0}(X^n + X) - (Y^n + Y))$ with $p = 2$, $q = n$, $n_0 = 2^r$, $r \geq 1$, $n = 2n_0^2$ and $g = n_0(n - 1)$.
 - the Ree curve $\mathbf{v}(Y^{n^2} - (1 + (X^n - X)^{n-1})Y^n + (X^n - X)^{n-1}Y - X^n(X^n - X)^{n+3n_0})$ with $p = 3$, $q = n$, $n_0 = 3^r$, $n = 3n_0^2$ and $g = \frac{3}{2}n_0(n - 1)(n + n_0 + 1)$.

The Weierstrass semigroup at P_∞

Lemma

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then

The Weierstrass semigroup at P_∞

Lemma

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then

- ① $H(P_\infty) = \langle q, p(q+1), q^2+1 \rangle$, and

The Weierstrass semigroup at P_∞

Lemma

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then

- 1 $H(P_\infty) = \langle q, p(q+1), q^2+1 \rangle$, and
- 2 $\mathcal{L}(qP_\infty) = \langle 1, x \rangle$ and $\mathcal{L}(p(q+1)P_\infty) = \langle 1, x, \dots, x^p, y \rangle$.

The Weierstrass semigroup at P_∞

Lemma

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then

- 1 $H(P_\infty) = \langle q, p(q+1), q^2+1 \rangle$, and
- 2 $\mathcal{L}(q\mathcal{P}_\infty) = \langle 1, x \rangle$ and $\mathcal{L}(p(q+1)\mathcal{P}_\infty) = \langle 1, x, \dots, x^p, y \rangle$.

- Note that $\text{Aut}(\mathcal{X}) = \text{Aut}(\mathcal{X})_{P_\infty}$ implies that the Riemann-Roch spaces $\mathcal{L}(q\mathcal{P}_\infty)$ and $\mathcal{L}(p(q+1)\mathcal{P}_\infty)$ are invariant by $\text{Aut}(\mathcal{X})$. Thus any $\sigma \in \text{Aut}(\mathcal{X})$ is such that

$$\sigma(x) = ax + b \quad \text{and} \quad \sigma(y) = cy + f(x),$$

where $\deg f(x) \leq p$.

The Weierstrass semigroup at P_∞

Lemma

Let $\mathcal{X} : y^q + y = (x^p - x)^{q+1}$, with $p < q$. Then

- 1 $H(P_\infty) = \langle q, p(q+1), q^2+1 \rangle$, and
- 2 $\mathcal{L}(qP_\infty) = \langle 1, x \rangle$ and $\mathcal{L}(p(q+1)P_\infty) = \langle 1, x, \dots, x^p, y \rangle$.

- Note that $\text{Aut}(\mathcal{X}) = \text{Aut}(\mathcal{X})_{P_\infty}$ implies that the Riemann-Roch spaces $\mathcal{L}(qP_\infty)$ and $\mathcal{L}(p(q+1)P_\infty)$ are invariant by $\text{Aut}(\mathcal{X})$. Thus any $\sigma \in \text{Aut}(\mathcal{X})$ is such that

$$\sigma(x) = ax + b \quad \text{and} \quad \sigma(y) = cy + f(x),$$

where $\deg f(x) \leq p$.

- Taking the equation of \mathcal{X} into account, the result follows.

Elementary abelian p -extensions

- Via iteration, one can easily check that the “minimal genus condition” arising from the inequality $g(\mathcal{X}) \geq p \cdot g(\mathcal{Y})$, in the Artin-Schreier setting, can be extended to the case of elementary abelian p -extensions of degree p^r , where we have

$$g(\mathcal{X}) \geq p^r \cdot g(\mathcal{Y}).$$

Elementary abelian p -extensions

- Via iteration, one can easily check that the “minimal genus condition” arising from the inequality $g(\mathcal{X}) \geq p \cdot g(\mathcal{Y})$, in the Artin-Schreier setting, can be extended to the case of elementary abelian p -extensions of degree p^r , where we have

$$g(\mathcal{X}) \geq p^r \cdot g(\mathcal{Y}).$$

- In particular, we may consider curves of type

$$\mathcal{X} : y^q + y = L(x)^{q+1},$$

where $L(x)$ is an additive separable polynomial.

For example: $y^q + y = (x^{p^r} - x)^{q+1}$

Using the same method, one can study the automorphism group of $\mathcal{X}_r : y^q + y = (x^{p^r} - x)^{q+1}$ and prove that if $p^r \geq q$, then

$$|\text{Aut } \mathcal{X}_r| = p^{2r} (p^r - 1) q^3.$$

For example: $y^q + y = (x^{p^r} - x)^{q+1}$

Using the same method, one can study the automorphism group of $\mathcal{X}_r : y^q + y = (x^{p^r} - x)^{q+1}$ and prove that if $p^r \geq q$, then

$$|\text{Aut } \mathcal{X}_r| = p^{2r} (p^r - 1) q^3.$$

In particular, since $g(\mathcal{X}_r) = p^r q(q - 1)/2$, we have

- $|\text{Aut } \mathcal{X}_r| > 4g(\mathcal{X}_r)^2$ (a very large automorphism group)

For example: $y^q + y = (x^{p^r} - x)^{q+1}$

Using the same method, one can study the automorphism group of $\mathcal{X}_r : y^q + y = (x^{p^r} - x)^{q+1}$ and prove that if $p^r \geq q$, then

$$|\text{Aut } \mathcal{X}_r| = p^{2r} (p^r - 1) q^3.$$

In particular, since $g(\mathcal{X}_r) = p^r q(q - 1)/2$, we have

- $|\text{Aut } \mathcal{X}_r| > 4g(\mathcal{X}_r)^2$ (a very large automorphism group)
- Furthermore, note that the case $q = p$ gives

$$|\text{Aut } \mathcal{X}_r| = p^{2r+3} (p^r - 1),$$

For example: $y^q + y = (x^{p^r} - x)^{q+1}$

Using the same method, one can study the automorphism group of $\mathcal{X}_r : y^q + y = (x^{p^r} - x)^{q+1}$ and prove that if $p^r \geq q$, then

$$|\text{Aut } \mathcal{X}_r| = p^{2r} (p^r - 1) q^3.$$

In particular, since $g(\mathcal{X}_r) = p^r q(q - 1)/2$, we have

- $|\text{Aut } \mathcal{X}_r| > 4g(\mathcal{X}_r)^2$ (a very large automorphism group)
- Furthermore, note that the case $q = p$ gives

$$|\text{Aut } \mathcal{X}_r| = p^{2r+3} (p^r - 1),$$

For example: $y^q + y = (x^{p^r} - x)^{q+1}$

Using the same method, one can study the automorphism group of $\mathcal{X}_r : y^q + y = (x^{p^r} - x)^{q+1}$ and prove that if $p^r \geq q$, then

$$|\text{Aut } \mathcal{X}_r| = p^{2r} (p^r - 1) q^3.$$

In particular, since $g(\mathcal{X}_r) = p^r q(q - 1)/2$, we have

- $|\text{Aut } \mathcal{X}_r| > 4g(\mathcal{X}_r)^2$ (a very large automorphism group)
- Furthermore, note that the case $q = p$ gives

$$|\text{Aut } \mathcal{X}_r| = p^{2r+3} (p^r - 1),$$

and this provides a family of curves \mathcal{X}_r for which the p -Sylow subgroups $S \leq \text{Aut}(\mathcal{X}_r)$ attain Nakajima's bound

$$|S| \leq \max \{g, 4pg^2/(p - 1)^2\} = p^{2r+3}.$$

A remark

- Note that there is already an extensive study on the automorphism groups of curves of type

$$\mathcal{C} = \mathbf{v}(A(Y) - B(X))$$

where $A(Y)$ is linearized polynomial, and $p \nmid \deg B$.

A remark

- Note that there is already an extensive study on the automorphism groups of curves of type

$$\mathcal{C} = \mathbf{v}(A(Y) - B(X))$$

where $A(Y)$ is linearized polynomial, and $p \nmid \deg B$.

- In general, for the cases considered here, we have $p \mid \deg B$.
For example, $y^q + y = (x^p - x)^{q+1}$.

The End

THANK YOU!