

# Smooth curves having a large automorphism $p$ -group in characteristic $p > 0$ .

Magali Rocher

Institut de Mathématiques de Bordeaux- FRANCE.

AGCT 12- CIRM- March 30 th, 2009.

# Notation.

- $k$  is an algebraically closed field of characteristic  $p \geq 0$ .
- $C/k$  is a connected nonsingular projective curve with genus  $g \geq 2$ .
- $\text{Aut}_k(C)$  is the full  $k$ -automorphism group of  $C$ .

# The case of characteristic 0.

- In characteristic 0:

$$\boxed{|\mathrm{Aut}_k(C)| \leq 84(g-1)} \quad (\text{Hurwitz bound-1892})$$

- Problem: classification of automorphism groups for a given genus.
- Partial answers:
  - for *Hurwitz groups*, i.e.  $|\mathrm{Aut}_k(C)| = 84(g-1)$ .
  - more generally, for *large groups*  $G \subset \mathrm{Aut}_k(C)$ , i.e.

$$|G| \geq 4(g-1) \quad [\text{Kulkarni 1997}] [\text{Breuer 2000}]$$

By the Hurwitz formula,  $g_{C/G} = 0$  and  $C \rightarrow C/G$  ramified in 3 or 4 points.

## The case of characteristic $p > 0$ .

In characteristic  $p > 0$ :

- $\text{Aut}_k(C)$  is still finite [Schmid 1938].
- But the bound is **biquadratic**:

$$|\text{Aut}_k(C)| \leq 16g^4 \quad [\text{Stichtenoth-1973}]$$

except for  $C : W^q + W = X^{1+q}$ ,  $q = p^n \geq 3$ .

This is due to **wild ramification**.

## Definition of a big action.

From now on,  $\text{char}(k) = p > 0$ .

### Definition

Let  $C/k$  be a connected nonsingular projective curve with genus  $g \geq 2$ .

Let  $G$  be a subgroup of  $\text{Aut}_k(C)$ .

A pair  $(C, G)$  is called a **big action** if:

- $G$  is a  $p$ -group.
- 

$$|G| > \frac{2p}{p-1} g.$$

## Ramification conditions.

Let  $(C, G)$  be a big action.

Apply the Hurwitz and Deuring-Shafarevitch formulas to  $C \rightarrow C/G$ .

- Then, only one point  $\infty \in C$  is ramified and even totally ramified.
- Let  $G_i$  be the  $i$ -th lower ramification group of  $G$  at  $\infty$ .  
Then  $\boxed{G = G_{-1} = G_0 = G_1}$ .
- $\boxed{C/G \simeq \mathbb{P}_k^1}$  and  $\boxed{C/G_2 \simeq \mathbb{P}_k^1}$ . In particular,  $G_2 \neq \{e\}$ .

# Choice of the bound: the "embedding problem".

Why  $\boxed{\frac{2p}{p-1}}$  instead of  $\boxed{\frac{p}{p-1}}$  as in [Giulletti-Korchmaros, 2007])?

- $|G| > \boxed{2}^p g$  is necessary for  $G_2 \boxed{\subsetneq} G_1 = G$ .  
*(see  $W^p - W = X^2$ ,  $p > 2$ , with  $G = \langle \sigma \rangle$ ,  $\sigma(X) = X$  and  $\sigma(W) = W + 1$ ).*
- So  $G/G_2 \simeq \{X \rightarrow X + y, y \in V\}$   
 with  $C/G_2 - \{\infty\} = \text{Spec} k[X]$  and  $V \subset k$  an  $\mathbb{F}_p$ -vector space with:

$$\boxed{0 \longrightarrow G_2 \longrightarrow G \xrightarrow{\pi} V \simeq (\mathbb{Z}/p\mathbb{Z})^v \longrightarrow 0,}$$

where

$$\pi : \begin{cases} G \rightarrow V \\ g \rightarrow g(X) - X. \end{cases}$$

## Examples related to curves with many rational points.

Notation:  $q := p^e$ ,  $e \in \mathbb{N}^*$ ,  $K := \mathbb{F}_q(X)$ ,  $K^{alg}$  fixed,  $m \in \mathbb{N}$ .

Definition (Perret 1991, Lauter 1999, Auer 2000)

We define  $K^m \subset K^{alg}$  as the largest abelian extension  $L$  of  $K$

- with conductor  $\leq m^\infty$
- such that every place in  $S := \{(X - y), y \in \mathbb{F}_q\}$  splits completely in  $L$ .

Let  $C_m/\mathbb{F}_q$  be the nonsingular projective curve with function field  $K^m$ .

Remark

$$\text{Gal}(K^m/K) \simeq \frac{1 + Z\mathbb{F}_q[[Z]]}{\langle 1 + Z^m\mathbb{F}_q[[Z]], 1 - yZ, y \in \mathbb{F}_q \rangle}, \quad \text{with } Z = X^{-1}.$$

$\text{Gal}(K^m/K)$  has exponent 1 or  $p \Leftrightarrow m < m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ . (Lauter)

# Big actions with $G_2$ abelian of arbitrary large exponent.

## Proposition (Matignon-Rocher 2008)

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$  extends to a  $p$ -group  $G_m \subset \text{Aut}_{\mathbb{F}_q}(C_m)$  with

$$0 \longrightarrow \text{Gal}(K^m/K) \longrightarrow G_m \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

For  $e$  and  $m$  large enough,  $(C_m, G_m)$  is a big action.

- If  $e \geq 6$ ,  $(C_{m^2}, G_{m^2})$  is a big action with  $G_2 = \text{Gal}(K^{m^2}/K)$  abelian of exponent  $p^2$ .

## Remark

Same method to construct  $G_2$  abelian of arbitrary large exponent.

# Link with algebraic curves with many rational points.

## Remark

Let  $N_m$  be the number of  $\mathbb{F}_q$ -rational points on  $C_m$ . Then

$$N_m := |C_m(\mathbb{F}_q)| = 1 + q |\mathrm{Gal}(K^m/K)| = 1 + |G_m|.$$

Hence,

$$\frac{|G_m|}{g_{C_m}} \sim \frac{N_m}{g_{C_m}}.$$

## Construction of a "minimal subextension".

### Problem:

- Construct a subextension of  $K^{m_2}$  such that  $G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$  with  $t \geq 0$  minimal.

### Difficulty: The "embedding problem".

- In the previous case, the stability under translation is due to uniqueness.
- How to reduce to a system of equations that remains globally stable?
- $t = 0$  is excluded. (cocycle in the addition of Witt vectors.)  
More generally, there is no big action with  $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$  except for  $n = 1$ .

### Answer:

- In [M-R], construction of a "minimal subextension" with  $t = O(\log_p(g))$ .

Big actions with  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$  [Rocher 2009].

Notation. Let  $(C, G)$  be a big action with  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $n \geq 1$ .  
Let  $L := k(C)$  and  $k(X) := L^{G_2}$ . Then

$$L/k(X) : \quad W_i^p - W_i = g_i(X) \in k[X], \quad 1 \leq i \leq n.$$

## Definition

Let

$$A := \frac{\wp(L) \cap k[X]}{\wp(k[X])} := \langle \overline{g_1(X)}, \dots, \overline{g_n(X)} \rangle \quad \text{with} \quad \wp := F - \text{id}.$$

$A$  is the  $\mathbb{F}_p$ -vector subspace of  $k[X]$  dual to  $G_2$  with respect to the Artin-Schreier pairing:

$$\begin{cases} G_2 \times A \rightarrow \mathbb{Z}/p\mathbb{Z} \\ (g, \overline{\wp w}) \rightarrow g(w) - w \end{cases}$$

## Action of $V$ on $A$ .

### Recall

$$0 \longrightarrow G_2 \longrightarrow G \longrightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^v \longrightarrow 0$$

Then,  $V$  acts on  $A$  by translation:

$$\phi : \begin{cases} V \rightarrow \text{Aut}(A) \simeq \text{GL}_n(\mathbb{F}_p) \\ y \rightarrow \phi(y) \end{cases}$$

with

$$\phi(y) : \begin{cases} A \rightarrow A \\ \overline{f(X)} \rightarrow \overline{f(X+y)} \end{cases}$$

### Remark

$\text{Im } \phi$  is a unipotent subgroup of  $\text{GL}_n(\mathbb{F}_p)$ .

## An adapted basis for $A$ .

We construct a basis  $\{\overline{f_1(X)}, \dots, \overline{f_n(X)}\}$  in which the matrix of  $\phi(y)$  reads:

$$\Phi(y) := \begin{pmatrix} 1 & \ell_{1,2}(y) & \ell_{1,3}(y) & \dots & \ell_{1,n}(y) \\ 0 & 1 & \ell_{2,3}(y) & \dots & \ell_{2,n}(y) \\ 0 & 0 & \dots & \dots & \ell_{i,n}(y) \\ 0 & 0 & 0 & 1 & \ell_{n-1,n}(y) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_p) \quad \forall y \in V$$

In other words,

$$\forall i \in \{1, \dots, n\}, \forall y \in V, f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \quad \text{mod } \mathfrak{p}(k[X]).$$

i.e. stability of the system of equations under translation by  $V$ .

Case  $n = 1$ , i.e.  $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ .

## Theorem (Lehr-Matignon 2005)

Let  $(C, G)$  be a big action such that  $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ .

- Then

$$C \sim C_S : W^p - W = X S(X) \in k[X]$$

with  $S(X) = (a_0 \text{id} + a_1 F + \dots + F^s)(X)$  **additive** of degree  $p^s$ ,  $s \geq 1$ .

- Consider the **palindromic polynomial** of  $S$  [Elkies]:

$$\text{Ad}_S := F^s \sum_{j=0}^s (a_j F^j + F^{-j} a_j) \quad \text{and} \quad Z(\text{Ad}_S) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}.$$

Case  $n = 1$ , i.e.  $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ .

## Theorem

- Let  $A_{\infty,1}$  be the wild inertia subgroup of  $\text{Aut}_k(C)$  at  $\infty$ . Then

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & A_{\infty,1} & \xrightarrow{\pi} & Z(\text{Ad}_S) \longrightarrow 0 \\
 & & \parallel & & \cup & & \cup \\
 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G & \xrightarrow{\pi} & V \longrightarrow 0
 \end{array}$$

For  $p \geq 3$ , unique **extraspecial group** of exponent  $p$  and order  $p^{2s+1}$ .

- Conversely, if

$$C_S : W^p - W = XS(X) \in k[X]$$

with  $S(X)$  additive of degree  $p^s$ ,  $s \geq 1$ ,  $(C_S, A_{\infty,1})$  is a big action with  $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ .

# A ring filtration of $k[X]$ related to the additive polynomials.

Problem: Generalize the case  $n = 1$ .

## Definition

Let  $t \geq 1$ . We define  $\Sigma_t$  as the  $k$ -vector subspace of  $k[X]$  generated by 1 and the products of at most  $t$  additive polynomials.

## Lemma

- Let  $a \in \mathbb{N}$  with  $p$ -adic expansion:  $a = a_0 + a_1 p + \dots + a_\ell p^\ell$ ,  $0 \leq a_i \leq p - 1$ .

Then

$$X^a \in \Sigma_t \iff S_p(a) := a_0 + a_1 + \dots + a_\ell \leq t.$$

- Let  $f(X) \in k[X] - \{0\}$  such that  $f(X) = \sum_{a \in \mathbb{N}} c_a(f) X^a$ .

Then

$$f \in \Sigma_t \iff \forall a \in \mathbb{N} \text{ with } c_a(f) \neq 0, S_p(a) \leq t.$$

# Parametrization of the big actions with $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ .

Theorem (Rocher 2009)

Let  $(C, G)$  be a big action such that  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $n \geq 1$ . Then,

$$\forall i \in \{1, \dots, n\}, \quad f_i \in \Sigma_{i+1}.$$

Remark

- This generalizes the case  $n = 1$  where  $f(X) = XS(X) \in \Sigma_2$ .
- For  $n \geq 2$ , the converse is no longer true.  
Obstruction related to the **embedding problem**.

## The special case: each $f_i \in \Sigma_{i+1} - \Sigma_i$ .

### Theorem (Rocher 2009)

Let  $(C, G)$  be a big action with  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $n \geq 2$ , such that

$$\forall i \in \{1, \dots, n\}, \quad f_i \in \Sigma_{i+1} - \Sigma_i.$$

Then,

- $n \leq p - 1$ .
- $\forall i \in \{1, \dots, n\}, \deg(f_i) = 1 + ip^s$ .
- $\dim_{\mathbb{F}_p} V = s + 1$ .
- The upper ramification filtration of  $G_2$  satisfies:

$$\forall i \in \{1, \dots, n\}, \quad \frac{(G_2)^{v_i}}{(G_2)^{v_{i+1}}} \simeq \mathbb{Z}/p\mathbb{Z} \quad \text{with} \quad v_i = 1 + ip^s.$$

# Parametrization of the family for $p = 5$ and $\dim_{\mathbb{F}_p} V = 2$ .

- One deduces an algorithmic method to parametrize the functions  $f_i$ 's.
- We illustrate this method for  $p = 5$  and  $\dim_{\mathbb{F}_p} V = 2$ .

# Parametrization of the family for $p = 5$ and $\dim_{\mathbb{F}_p} V = 2$ .

- $n = 2$  [Rocher 2009]

$$f_1(X) = X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2$$

$$f_2(X) = b_{11}^5X^{11} + 4b_{11}^{25}X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5}X^3 + b_1X$$

where  $b_{11} \in k^\times$  and  $b_1 \in k$  are algebraically independent parameters.

## Remark

- The space of parameters is a Zariski open of the affine space  $\mathbb{A}_k^2$ : it is irreducible, hence only one possibility for  $G$  (up to isomorphism).*
- Two curves  $C(b_{11}, b_1)$  and  $C(b'_{11}, b'_1)$  are isomorphic if and only if*

$$\left(\frac{b'_{11}}{b_{11}}\right)^{24} = 1 \quad \text{and} \quad b'_1 = c \frac{b'_{11}}{b_{11}} b_1 \quad \text{with} \quad c \in \mathbb{F}_5^\times.$$

- $n = 3$  [Rocher 2009]

$$f_1(X) = X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2$$

$$f_2(X) = b_{11}^5 X^{11} + 4b_{11}^{25} X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5} X^3 + 2(c_6 - c_6^5)b_{11}^{-5} X$$

$$\begin{aligned} f_3(X) = & 4b_{11}^{10} X^{16} + 4b_{11}^{30} X^{12} + c_{11}^5 X^{11} + 4b_{11}^{50} X^8 + 4c_{11}^{25} X^7 \\ & + c_6^5 X^6 + 4(b_{11}^{75} + b_{11}^3)b_{11}^{-5} X^4 \\ & + \{(b_{11}^{25} + b_{11})c_{11}b_{11}^{-5} + 2(b_{11}^{25} + b_{11})^2 c_{11}^5 b_{11}^{-10}\} X^3 \\ & + 2(c_6^5 b_{11}^{25} + c_6 b_{11})b_{11}^{-5} X^2 + c_1 X \end{aligned}$$

where  $b_{11} \in k^\times$ ,  $c_6 \in k$  and  $c_1 \in k$  are algebraically independent parameters and  $c_{11} \in k$  satisfies

$$c_{11}^{25} + 4(b_{11}^{25} + b_{11})b_{11}^{-5}c_{11}^5 + c_{11} = 0.$$

### Remark

*The space of parameters is no more connected.*

*One finds two non-isomorphic models for the group  $G$  (MAGMA).*

## Application: towards a classification of big actions.

The criterion to classify big actions is  $\frac{|G|}{g^2}$ .

Let  $(C, G)$  be a big action.

- By [Stichtenoth, 1973],  $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$ .
- If  $\frac{|G|}{g^2} \geq \frac{4}{(p-1)^2}$ , then  $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ . Description in [L-M].
- If  $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$ , then  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $1 \leq n \leq 3$ . Proof in [M-R].  
Classification and parametrization given in [Rocher 2].