On smooth curves endowed with a large automorphism $p$-group in characteristic $p > 0$.

Michel Matignon and Magali Rocher.

Abstract

Let $k$ be an algebraically closed field of characteristic $p > 0$ and $C$ a connected nonsingular projective curve over $k$, with genus $g \geq 2$. This paper continues the work begun in [LM05], namely the study of "big actions", i.e. the pairs $(C,G)$ where $G$ is a $p$-subgroup of the $k$-automorphism group of $C$ such that $|G| > \frac{2p}{g}$. If $G_2$ denotes the second ramification group of $G$ at the unique ramification point of the cover $C \rightarrow C/G$, we display necessary conditions on $G_2$ for $(C,G)$ to be a big action, which allows us to pursue the classification of big actions. Our main source of examples comes from the construction of curves with many rational points using ray class field theory for global function fields, as initiated by J-P. Serre and followed by [La99] and [Au99]. In particular, we obtain explicit examples of big actions with $G_2$ abelian of large exponent.

1 Introduction.

Setting. Let $k$ be an algebraically closed field and $C$ a connected nonsingular projective curve over $k$, with genus $g \geq 2$. If $\text{char}(k) = 0$, Hurwitz exhibits a linear bound for the $k$-automorphism group of the curve $C$, namely: $|\text{Aut}_k(C)| \leq 84(g - 1)$. If $\text{char}(k) = p > 0$, the Hurwitz bound is no longer true when $g$ grows large, but the finiteness result still holds (cf. [Sch38]) and one gets polynomial bounds on $|\text{Aut}_k(C)|$ (cf. [St73] and [Sin74]). In this situation, the full automorphism group may be very large as compared with the case $\text{char}(k) = 0$. This is due to the appearance of wild ramification, which leads us to concentrate on large automorphism $p$-groups in $\text{char}(k) = p > 0$. In this spirit, Nakajima (cf. [Na87]) studies the size of Sylow $p$-subgroups of $\text{Aut}_k(C)$ and emphasizes the influence of another important invariant of the curve: the $p$-rank, denoted by $\gamma$. Indeed, if $G$ is a Sylow $p$-subgroup of $\text{Aut}_k(C)$, we deduce from [Na87] that $|G| \leq \frac{2p}{p-1}g$, except for $\gamma = 0$. On the contrary, when $\gamma = 0$, the upper bound on $|G|$ is no more linear in $g$, namely $|G| \leq \max\{g, \frac{4p}{(p-1)^2}g^2\}$. As shown in [St73], the quadratic upper bound $\frac{4p}{(p-1)^2}g^2$ can really be attained, which demonstrates that, in this case, $\text{Aut}_k(C)$ may be especially large. Following Nakajima’s work, Lehr and Matignon explore the "big actions", that is to say the pairs $(C,G)$ where $G$ is a $p$-subgroup of $\text{Aut}_k(C)$ such that $\frac{|G|}{g} > \frac{2p}{g}$ (see [LM05]). In particular, they exhibit a classification of the big actions that satisfy

$$
\frac{4}{(p-1)^2} \leq \frac{|G|}{g^2}.
$$

Motivation and outline of the paper. Let $(C,G)$ be a big action. As shown in [LM05], there is a point of $C$, say $\infty$, such that $G$ is equal to the wild inertia subgroup $G_1$ of $G$ at $\infty$. Let $G_2$ be the second ramification group of $G$ at $\infty$ in lower notation. Then, the quotient curve $C/G_2$ is isomorphic to the projective line $\mathbb{P}^1_k$ and the quotient group $G/G_2$ acts as a group of translations of $\mathbb{P}^1_k$ fixing $\infty$, through $X \rightarrow X + y$, where $y$ runs over a subgroup $V$ of $k$. In this way, the group $G$ appears as an extension of $G_2$ by the $p$-elementary abelian group $V$ via the exact sequence:

$$
0 \rightarrow G_2 \rightarrow G = G_1 \rightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^v \rightarrow 0
$$

The aim of this paper is, on the one hand, to give necessary conditions on $G_2$ for $(C,G)$ to be a big action and, on the other hand, to display realizations of big actions with $G_2$ abelian of large exponent. In section 2, we first prove that $G_2$ must be equal to $D(G)$, the commutator subgroup of $G$. In section 3, given a big action $(C,G)$ and an additive polynomial map: $\mathbb{P}^1_k \rightarrow C/G_2 \simeq \mathbb{P}^1_k$, we display a new big action $(\tilde{C},\tilde{G})$ such that $\tilde{G}_2 \simeq G_2$. In section 4, we demonstrate that $G_2$ cannot be cyclic except when $G_2$ has order $p$. Some of these results on $G_2$ are necessary to pursue the classification of big actions initiated by Lehr and Matignon, more precisely to explore the case: $\frac{2}{(p-1)^2} \leq \frac{|G|}{g}$. Indeed, we prove in section 5 that such an inequality requires $G_2$ to be an elementary abelian $p$-group whose order divides $p^3$. In sequel papers, M. Rocher goes further: she studies big
actions with a $p$-elementary abelian $G_2$ (see [Ro2]), which enables her to display the classification of big actions satisfying $\frac{4}{(p^r-1)} \leq \frac{|G|}{q}$ (see [Ro3]). In section 6, following [Lan99] and [An99], we consider the maximal abelian extension of $K := \mathbb{F}_q(X)$ ($q = p^r$) denoted by $K^m_2$, which is unramified outside $X = \infty$, completely split over the set $S$ of the finite rational places and whose conductor is smaller than $m \infty$, with $m \in \mathbb{N}$. Class field theory gives a description of the Galois group $G_2(m)$ of this extension, but also precisies its upper ramification groups, which allows us to compute the genus of the extension. Moreover, it follows from the unicity and the maximality of $K^m_2$ that the group of big actions on curves and an analogous ramification condition for finite $p$-groups acting on $k((z))$.

Notation and preliminary remarks. Let $k$ be an algebraically closed field of characteristic $p > 0$. We denote by $F$ the Frobenius endomorphism for a $k$-algebra. Then, $\varphi$ means the Frobenius operator minus identity. We denote by $k\{F\}$ the $k$-subspace of $k[X]$ generated by the polynomials $F^i(X)$, with $i \in \mathbb{N}$. It is a ring under the composition. Furthermore, for all $\alpha$ in $k$, $F\alpha = \alpha^p F$. The elements of $k\{F\}$ are the additive polynomials, i.e. the polynomials $P(X)$ of $k[X]$ such that for all $\alpha$ and $\beta$ in $k$, $P(\alpha + \beta) = P(\alpha) + P(\beta)$. Moreover, a separable polynomial is additive if and only if the set of its roots is a subgroup of $k$ (see [Go96] chap. 1).

Let $f(X)$ be a polynomial of $k[X]$. Then, there is a unique polynomial $\text{red}(f)(X)$ in $k[X]$, called the reduced representative of $f$, which is $p$-power free, i.e. $\text{red}(f)(X) \in \bigoplus_{(i,p) = 1} k X^i$, and such that $\text{red}(f)(X) = f(X) \mod \varphi(k[X])$. We say that the polynomial $f$ is reduced mod $\varphi(k[X])$ if and only if it coincides with its reduced representative $\text{red}(f)$. The equation $W^p - W = f(X)$ defines a $p$-cyclic étale cover of the affine line that we denote by $C_f$. Conversely, any $p$-cyclic étale cover of the affine line $Spec k[X]$ corresponds to a curve $C_f$ where $f$ is a polynomial of $k[X]$ (see [Mi80] III.4.12, p. 127). By Artin-Schreier theory, the covers $C_f$ and $C_{\text{red}(f)}$ define the same $p$-cyclic covers of the affine line. The curve $C_f$ is irreducible if and only if $\text{red}(f) \neq 0$.

Throughout the text, $C$ always denotes a nonsingular smooth projective curve with genus $g$ and $Aut_k(C)$ means its $k$-automorphism group. Our main references for ramification theory are [Se68] and [An99].

**2 First results on ”big actions”**.

To precise the background of our work, we begin by collecting and completing the first results on big actions already obtained in [LM05]. The expression ”big actions” stands for curves endowed with a big automorphism $p$-group. The first task is to recall what we mean by ”big”.

**Definition 2.1.** Let $G$ be a subgroup of $Aut_k(C)$. We say that the pair $(C, G)$ is a big action if $G$ is a finite $p$-group, if $g \neq 0$ and if

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

(1)

**Proposition 2.2.** [LM05] Assume that $(C, G)$ is a big action with $g \geq 2$. Then, there is a point of $C$ (say $\infty$) such that $G$ is the wild inertia subgroup of $G$ at $\infty$: $G_1$. Moreover, the quotient $C/G$ is isomorphic to the projective line $\mathbb{P}^1_k$ and the ramification locus (respectively branch locus) of the cover $\pi : C \to C/G$ is the point $\infty$ (respectively $\pi(\infty)$). For all $i \geq 0$, we denote by $G_i$ the $i$-th lower ramification group of $G$ at $\infty$. Then,

1. $G_2$ is non trivial and it is strictly included in $G_1$.

2. The Hurwitz genus formula applied to $C \to C/G$ reads:

$$2g = \sum_{i \geq 2} (|G_i| - 1)$$

(2)
3. The quotient curve $C/G_2$ is isomorphic to the projective line $\mathbb{P}^1_k$. Moreover, the quotient group $G/G_2$ acts as a group of translations of the affine line $C/G_2 \setminus \{\infty\} = \text{Spec}k[X]$, through $X \rightarrow X + y$, where $y$ runs over a subgroup $V$ of $k$. Then, $V$ is an $\mathbb{F}_p$-subvector space of $k$. We denote by $v$ its dimension. Thus, we obtain the exact sequence:

$$0 \rightarrow G_2 \rightarrow G = G_1 \rightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^v \rightarrow 0$$

where

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

4. Let $H$ be a normal subgroup of $G$ such that $g_{C/H} > 0$. Then, $(C/H, G/H)$ is also a big action. Moreover, the group $G/H$ fixes the image of $\infty$ in the cover $C \rightarrow C/H$. In particular, if $g_{C/H} = 1$, then $p = 2$, $C/H$ is birational to the curve $W^2 + W = X^3$ and $G/H$ is isomorphic to $G_8$, the quaternion group of order 8 (see [Si86], Appendix A, Prop. 1.2).

**Remark 2.3.** Note that, for $g = 1$, one can find big actions $(C, G)$ such that $G$ is not included in a decomposition group of $\text{Aut}_k(C)$ as in Proposition 2.2.

The following lemma generalizes and completes the last point of Proposition 2.2.

**Lemma 2.4.** Let $G$ a finite $p$-subgroup of $\text{Aut}_k(C)$. We assume that the quotient curve $C/G$ is isomorphic to $\mathbb{P}^1_k$ and that there is a point of $C$ (say $\infty$) such that $G$ is the wild inertia subgroup of $G$ at $\infty$: $G_1$. We also assume that the ramification locus (respectively branch locus) of the cover $\pi : C \rightarrow C/G$ is the point $\infty$ (respectively $\pi(\infty)$). Let $G_2$ be the second ramification group of $G$ at $\infty$ and $H$ a subgroup of $G$.

1. Then, $C/H$ is isomorphic to $\mathbb{P}^1_k$ if and only if $H \supseteq G_2$.

2. In particular, if $(C, G)$ is a big action with $g \geq 2$ and if $H$ is a normal subgroup of $G$ such that $H \subsetneq G_2$, then $g_{C/H} > 0$ and $(C/H, G/H)$ is also a big action.

**Proof:** When applied to the cover $C \rightarrow C/G \simeq \mathbb{P}^1_k$, the Hurwitz genus formula (see e.g. [Si93]) reads: $2(g - 1) = 2|G| (g_{C/G} - 1) + \sum_{i \geq 0} (|G_i| - 1)$. When applied to the cover $C \rightarrow C/H$, it yields: $2(g - 1) = 2|H| (g_{C/H} - 1) + \sum_{i \geq 0} (|H \cap G_i| - 1)$. Since $H \subset G = G_0 = G_1$, it follows that:

$$2|H|g_{C/H} = 2(|G| - |H|) + \sum_{i \geq 0} (|G_i| - |H \cap G_i|) = \sum_{i \geq 2} (|G_i| - |H \cap G_i|)$$

Therefore, $g_{C/H} = 0$ if and only if for all $i \geq 2$, $G_i = H \cap G_i$, i.e. $G_i \subset H$, which is equivalent to $G_2 \subset H$. The second point then derives from Proposition 2.2.4. $\square$

The very first step to study big actions is to precise their description when $g = 1$. Write $C = X^2 - W = f(X) = X S(X) + c X \in k[X]$, where $S$ in $k\{F\}$ is an additive polynomial with degree $s \geq 1$ in $F$. If we denote by $m$ the degree of $f$, then $m = 1 + p^s = i_0$, where $i_0 \geq 2$ is the integer such that:

$$G = G_0 \supseteq G_2 = G_3 = \cdots = G_{i_0} \supseteq G_{i_0 + 1} = \cdots$$

2. Write $S(F) = \sum_{j=0}^{s} a_j F^j$, with $a_s \neq 0$. Then, following [El97] (section 4), we can define an additive polynomial related to $f$, called the "palindromic polynomial" of $f$:

$$Ad_f := \frac{1}{a_s} F^s (\sum_{j=0}^{s} a_j F^j + F^{-j} a_j)$$

The set of roots of $Ad_f$, denoted by $Z(Ad_f)$, is an $\mathbb{F}_p$-subvector space of $k$, isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{2s}$. Besides, $Z(Ad_f) = \{ y \in k, f(X + y) - f(X) = 0 \mod p[k[X]] \}$. 

3
3. Let $G_{\infty,1}$ be the wild inertia subgroup of $\text{Aut}_E(C)$ at $\infty$. Then, $G_{\infty,1}$ is a central extension of $\mathbb{Z}/p\mathbb{Z}$ by the elementary abelian $p$-group $Z(\text{Ad} f)$ which can be identified with a subgroup of translations \{ $X \to X + y$, $y \in k$ \} of the affine line. Furthermore, if we denote by $Z(G_{\infty,1})$ the center of $G_{\infty,1}$ and by $D(G_{\infty,1})$ its commutator subgroup, $Z(G_{\infty,1}) = D(G_{\infty,1}) = \langle \sigma \rangle$, where $\sigma(X) = X$ and $\sigma(W) = W + 1$. Thus, we get the following exact sequence:

$$0 \to Z(G_{\infty,1}) = D(G_{\infty,1}) \simeq \mathbb{Z}/p\mathbb{Z} \to G_{\infty,1} \overset{\pi}{\to} Z(\text{Ad} f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$$

where 

$$\pi : \begin{cases} G_{\infty,1} \to Z(\text{Ad} f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \\ g \to g(X) - X \end{cases}$$

For $p > 2$, $G_{\infty,1}$ is the unique extraspecial group with exponent $p$ and order $p^{2s+1}$. The case $p = 2$ is more complicated (see [LM05] 4.1).

4. There exists an $\mathbb{F}_p$-vector space $V \subset Z(\text{Ad} f)$ $\simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$ such that $G = \pi^{-1}(V) \subset G_{\infty,1}$ and such that we get the exact sequence:

$$0 \to G_2 \simeq \mathbb{Z}/p\mathbb{Z} \to G \overset{\pi}{\to} V \to 0.$$

Therefore, the key idea to study big actions is to use Proposition 2.2.4 and Lemma 2.4.2 to go back to the well-known situation described above. This motivates the following

**Theorem 2.6.** Let $(C,G)$ be a big action with $g \geq 2$. Let $G$ be a normal subgroup in $G$ such that $G$ is strictly included in $G_2$. Then, there exists a group $H$, normal in $G$, such that $G \subset H \subset G_2$ and $[G_2 : H] = p$. In this case, $(C/H,G/H)$ enjoys the following properties.

1. The pair $(C/H,G/H)$ is a big action and the exact sequence of Proposition 2.2:

$$0 \to G_2 \to G \overset{\pi}{\to} V \to 0$$

induces the following one:

$$0 \to G_2/H = (G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z} \to G/H \overset{\pi}{\to} V \to 0$$

2. The curve $C/H$ is birational to $C_f$: $W^p - W = f(X) = X S(X) + c X \in k[X]$, where $S$ is an additive polynomial of degree $s \geq 1$ in $F$. Let $\text{Ad} f$ be the palindromic polynomial related to $f$ as defined in Proposition 2.5. Then, $V \subset Z(\text{Ad} f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$.

3. Let $E$ be the wild inertia subgroup of $\text{Aut}_E(C/H)$ at $\infty$. We denote by $D(E)$ its commutator subgroup of $E$ and by $Z(E)$ its center. Then, $E$ is an extraspecial group of order $p^{2s+1}$ and

$$0 \to D(E) = Z(E) \simeq \mathbb{Z}/p\mathbb{Z} \to E \overset{\pi}{\to} Z(\text{Ad} f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$$

4. Moreover, $G/H$ is a normal subgroup in $E$. It follows that $G_2$ is equal to $D(G)$, the commutator subgroup of $G$, which is also equal to $D(G) G^p$, the Frattini subgroup of $G$.

**Proof:** First of all, the existence of the group $H$ comes from [Sun82] (Chap. 2, Thm. 1.12). We deduce from Lemma 2.4.2 that $(C/H,G/H)$ is still a big action. Then, $G = G_1 \supset G_2$ (resp. $G/H = (G/H)_1 \supset (G/H)_2$). As the first jump always coincides in lower and upper ramification, it follows that $G_2 = G^2$ (resp.$(G/H)_2 = (G/H)^2$). By [Se68] (Second Part, Chap. IV, Prop. 14), $(G/H)_2 = (G/H)^2 = G^2 H/H = G_2 H/H = G_2/H$. The first assertion follows. The second and the third point directly derive from Proposition 2.5.

We now prove the last statement. By Proposition 2.5, $Z(E) = (G/H)_2 = G_2/H \subset G/H$. So, $G/H$ is a subgroup of $E$ containing $Z(E)$. Moreover, since $(\mathbb{Z}/p\mathbb{Z})^{2s}$ is abelian, $\pi(G/H)$ is normal in $E/Z(E)$. It follows that $G/H$ is normal in $E$. We eventually show that $G_2 = D(G)$. On the one hand, since $G/G_2$ is abelian, $D(G)$ is included in $G_2$. On the other hand, assume that $D(G)$ is strictly included in $G_2$. Then, the first point applied to $G = D(G)$ ensures the existence of a group $H$, normal in $G$, with $D(G) \subset H \subset G_2$. Let $[G_2 : H] = p$ such that $(C/H,G/H)$ is a big action. Since $D(G) \subset H$, $G/H$ is an abelian subgroup of $E$. As $G/H$ is also a normal group in $E$, [Hu67] (Satz 13.7) implies $[G/H] \leq p^{s+1}$. Hence $[G/H] \leq \frac{2p}{\sigma + 1}$, which contradicts condition (1) for the big action $(C/H,G/H)$. It follows that $D(G) = G_2$. In addition, as $G_2$ is an elementary abelian $p$-group, then $G^p = G^p_1 \subset G_2 = D(G)$. As a consequence, $G_2 = D(G) G^p$ which is equal to the Frattini subgroup of $G$, since $G$ is a $p$-group. □
Remark 2.7. When applying Theorem 2.6 to \( G = G_{i_0+1} \), where \( i_0 \) is defined as in Proposition 2.5, one obtains Theorem 8.6(i) of [LM05]. In particular, for all big actions \((C, G)\) with \( q \geq 2\), there exists an index \( p \)-subgroup \( H \) of \( G_2 \), normal in \( G \), such that \((C/H, G/H)\) is a big action with \( C/H \) birational to \( W^p - W = f(X) = X S(X) + c X \in k[X] \), where \( S \) is an additive polynomial of degree \( s \geq 1 \) in \( F \). Note that, in this case, \( i_0 = 1 + p^s \).

As \( G_2 \) cannot be trivial for a big action, we gather from the last point of Theorem 2.6 the following result.

**Corollary 2.8.** Let \((C, G)\) be a big action with \( q \geq 2\). Then \( G \) cannot be abelian.

It is natural to wonder whether \( G_2 \) can be non abelian. Although we do not know yet the answer to this question, we can mention a special case in which \( G_2 \) is always abelian, namely:

**Corollary 2.9.** Let \((C, G)\) be a big action with \( q \geq 2\). If the order of \( G_2 \) divides \( p^3 \), then \( G_2 \) is abelian.

**Proof:** There is actually only one case to study, namely: \( |G_2| = p^3 \). We denote by \( Z(G_2) \) the center of \( G_2 \). The case \( |Z(G_2)| = 1 \) is impossible since \( G_2 \) is a \( p \)-group. If \( |Z(G_2)| = p \), then \( Z(G_2) \) is cyclic. But, as \( G_2 \) is a \( p \)-group, normal in \( G \) and included in \( D(G) \) (see Theorem 2.6), \( G_2 \) is cyclic, which contradicts the strict inclusion of \( Z(G_2) \) in \( G_2 \). If \( |Z(G_2)| = p^2 \), then \( G_2/Z(G_2) \) is cyclic and \( G_2 \) is abelian, which leads to the same contradiction as above. This leaves only one possibility: \( |Z(G_2)| = p^3 \), which means that \( G_2 = Z(G_2) \). \( \square \)

**Corollary 2.10.** Let \((C, G)\) be a big action with \( q \geq 2\). We keep the notation of Proposition 2.2. Let \( G_{\infty, 1} \) be the wild inertia subgroup of \( \text{Aut}_k(C) \) at \( \infty \). Then, \((C, G_{\infty, 1})\) is a big action whose second lower ramification group is equal to \( D(G_{\infty, 1}) = D(G) \). In particular, \( G \) is equal to \( G_{\infty, 1} \) if and only if \(|G/D(G)| = |G_{\infty, 1}/D(G_{\infty, 1})| \).

**Proof:** As \( G \) is included in \( G_{\infty, 1} \), then \( D(G) \subset D(G_{\infty, 1}) \). If the inclusion is strict, one can find a subgroup \( \mathcal{G} \) such that \( G \subseteq \mathcal{G} \subset G_{\infty, 1} \) with \( |\mathcal{G} : G| = p \) (see [Su82], Chap. 2, Thm. 19). Then, \( G \) is a normal subgroup of \( \mathcal{G} \). It follows that \( D(G) \) is also a normal subgroup of \( \mathcal{G} \). As \( |\mathcal{G}| \leq |G| \), the pair \((C, \mathcal{G})\) is a big action. So, by Theorem 2.6, \( G_2 = D(G) \). Since \( D(G) \) is normal in \( \mathcal{G} \) and \( g(C/D(G)) = 0 \), we gather from Lemma 2.4.1 that \( D(G) = G_2 = D(G) \). The claim follows by reiterating the process. \( \square \)

**Remark 2.11.** Let \((C, G_{\infty, 1})\) be a big action as in Corollary 2.10. Then, \( G_{\infty, 1} \) is a \( p \)-Sylow subgroup of \( \text{Aut}_k(C) \). Moreover, we deduce from [GK07] (Thm. 1.3) that \( G_{\infty, 1} \) is the unique \( p \)-Sylow subgroup of \( \text{Aut}_k(C) \) except in four special cases: the hyperelliptic curves: \( W^p - W = X^2 \) with \( p > 2 \), the Hermitian curves and the Deligne-Lusztig curves arising from the Suzuki groups and the Ree groups (see equations in [GK07], Thm. 1.1).

### 3 Base change and big actions.

Starting from a given big action \((C, G)\), we now display a way to produce a new one: \((\tilde{C}, \tilde{G})\), with \( \tilde{G}_2 \cong G_2 \) and \( g_{\tilde{C}} = p^s g_C \). The main tool is a base change associated with an additive polynomial map: \( \mathbb{P}^1_k \stackrel{S}{\rightarrow} C/G_2 \cong \mathbb{P}^1_k \).

**Proposition 3.1.** Let \((C, G)\) be a big action with \( q \geq 2\). We denote by \( L := k(C) \) the function field of the curve \( C \), by \( k(X) := L^{G_2} \) the subfield of \( L \) fixed by \( G_2 \) and by \( k(T) := L^{G_1} \), with \( T = \prod_{v \in V} (X - v) \). Write \( X = S(Z) \), where \( S(Z) \) is a separable additive polynomial of \( k[Z] \) with degree \( p^s \), \( s \in \mathbb{N} \).

1. Then, \( L \) and \( k(Z) \) are linearly disjoined over \( k(X) \).

2. Let \( \tilde{C} \) be the smooth projective curve over \( k \) with function field \( k(\tilde{C}) := L[Z] \). Then, \( k(\tilde{C})/k(T) \) is a Galois extension with group \( \tilde{G} \cong G \times (\mathbb{Z}/p\mathbb{Z})^s \). Furthermore, \( g_{\tilde{C}} = p^s g_C \). It follows that \( |\tilde{G}| = |G| = |G_{\infty, 1}| \). So, \((\tilde{C}, \tilde{G})\) is still a big action with second ramification group \( \tilde{G}_2 \cong G_2 \times \{0\} \subset \tilde{G} \times (\mathbb{Z}/p\mathbb{Z})^s \). This can be illustrated by the following diagram:

\[
\begin{array}{c}
C \\
\downarrow \\
C/G_2 \cong \mathbb{P}^1_k \\
\downarrow \\
\mathbb{P}^1_k \end{array} \quad \text{←} \quad \begin{array}{c}
\tilde{C} \\
\downarrow \\
\tilde{G}_2 \cong \mathbb{P}^1_k \\
\downarrow \\
\mathbb{P}^1_k \end{array}
\]
Proof of Proposition 3.1: The proof of this proposition requires two preliminary lemmata.

**Lemma 3.2.** Let $K := k((z))$ be a formal power series field over $k$. Let $K_1/K$ be a Galois extension whose group $G$ is a $p$-group. Let $K_0/K$ be a $p$-cyclic extension. Assume that $K_0$ and $K_1$ are linearly disjoined over $K$. Put $L := K_0K_1$.

\[
\begin{align*}
K_1 & \rightarrow L = K_0K_1 \\
G & \mid \mid \\
K & \rightarrow K_0 
\end{align*}
\]

We suppose that the conductor of $K_0/K$ (see e.g. [Se68] Chap. 15, Cor. 2) is 2. Then, $L/K_1$ also has conductor 2.

**Proof:** Consider a chief series of $G$ (cf. [Su82], Chap. 2, Thm. 1.12), i.e. a series such that:

\[
G = G_0 \supseteq G_1 \cdots \supseteq G_n = \{0\}
\]

with $G_i$ normal in $G$ and $[G_{i-1} : G_i] = p$. One shows, by induction on $i$, that the conductor of the extension $K_0K_i^{G_i} / K_i^{G_i}$ is 2. Therefore, one can assume $G \simeq \mathbb{Z}/p\mathbb{Z}$. In this case, $L/k((z))$ is a Galois extension with group $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Write the ramification filtration of $G$ in lower notation:

\[
G = G_0 = \cdots = G_{i_0} \supseteq G_{i_0+1} = \cdots
\]

1. First, assume that $G_{i_0+1} = \{0\}$. Then, an exercise shows that, for any index $p$-subgroup $H$ of $G$, the extensions $L/L^H$ (case $\alpha$) and $L^H/K$ (case $\beta$) are $p$-cyclic with conductor $i_0 + 1$. When applied to $H = Gal(L/K_0)$, case $\beta$ gives $i_0 = 1$. Therefore, one concludes by applying case $\alpha$ to $H = Gal(L/K_1)$.

2. Now, assume that $G_{i_0+1} \neq \{0\}$. As above, let $H$ be an index $p$-subgroup of $G$. An exercise using the classical properties of ramification theory shows that:

(a) If $H = G_{i_0+1}$, then $L/L^H$ (resp. $L^H/K$) is a $p$-cyclic extension with conductor $i_0 + i_1 + 1$ (resp. $i_0 + 1$).

(b) If $H \neq G_{i_0+1}$, then $L/L^H$ (resp. $L^H/K$) is a $p$-cyclic extension with conductor $i_0 + 1$ (resp. $i_0 + \frac{i_0}{p} + 1$).

Apply this result to $H := Gal(L/K_0)$. Since $K_0/K$ has conductor 2, it follows that $i_0 + 1 = 2$, so $i_0 = 1$ and $Gal(L/K_0) = G_{i_0+1}$. Therefore, $Gal(L/K_1) \neq G_{i_0+1}$ and we infer from case $\beta$ that $L/K_1$ has conductor $i_0 + 1 = 2$. □

**Lemma 3.3.** Let $W$ be a finite $\mathbb{F}_p$-subvector space of $k$. Let $W_1$ and $W_2$ be two $\mathbb{F}_p$-subvector spaces of $W$ such that $W = W_1 \bigoplus W_2$. Define $T := \prod_{w \in W} (Z - w) - \prod_{w \in W} (Z - w)$, for $i$ in $\{1, 2\}$. Then, $k(T) \subset k(T_i) \subset k(Z)$. Moreover,

1. The extensions $k(T_1)/k(T)$ and $k(T_2)/k(T)$ are linearly disjoined over $k(T)$.

2. For all $i$ in $\{1, 2\}$, $k(Z)/k(T)$ (resp. $k(Z)/k(T_i)$) is a Galois extension with group isomorphic to $W$ (resp. $W_i$).

3. For all $i$ in $\{1, 2\}$, $k(T_1)/k(T)$ is a Galois extension with group isomorphic to $\frac{W}{W_i}$.

This induces the following diagram:

\[
\begin{array}{ccc}
k(T_1) & \xrightarrow{W_1} & k(Z) \\
| & \bigg| & | \\
\frac{W}{W_1} & \xrightarrow{W} & \frac{W}{W_2} \\
| & \bigg| & | \\
k(T) & \xrightarrow{W} & k(T_2)
\end{array}
\]

**Proof:** Use for example [Go96] (1.8). □

**Proof of Proposition 3.1:**
1. The first point derives from Lemma 2.4.1.

2. Put \( W := S^{-1}(V) \), with \( V \) defined as in Proposition 2.2.3, \( W_1 := S^{-1}((0)) \simeq (\mathbb{Z}/p\mathbb{Z})^s \), since \( S \) is an additive separable polynomial of \( k[Z] \) with degree \( p^s \) (see e.g. [Go96] chap. 1). Call \( W_2 \) any \( \mathbb{F}_p \)-subvector space of \( W \) such that \( W = W_1 \bigoplus W_2 \). Then, Lemma 3.3 applied to the extension \( k(Z)/k(T) \) induces the following diagram:

\[
L = k(C) \quad \quad \quad k(\tilde{C})
\]

\[
G_2 \quad | \quad \quad \quad |
\]

\[
L^{G_2} = k(X) = k(Z)^W_1 \quad \quad \quad k(Z)
\]

\[
W_1 \bigoplus W_2 \quad | \quad \quad \quad W_2
\]

\[
L^{G_1} = k(T) = k(Z)^W \quad \quad \quad k(Z)^W_2
\]

In particular, Lemma 3.3 implies that \( k(Z)^W_1 \cap k(Z)^W_2 = k(T) \). Since \( k(C) \cap k(Z) = k(X) \) (cf. first point of the proposition), we deduce that \( k(C) \) and \( k(Z)^W_2 \) are linearly disjoint over \( k(T) \). As \( k(Z)^W_2/k(T) \) is a Galois extension with group \( \frac{W}{W_2} \simeq W_1 \simeq (\mathbb{Z}/p\mathbb{Z})^s \), it follows that \( k(\tilde{C})/k(T) \) is a Galois extension with group \( \tilde{G} \simeq Gal(k(C)/k(T)) \times Gal(k(Z)^W_2/k(T)) \simeq G \times (\mathbb{Z}/p\mathbb{Z})^s \).

Now, consider a flag of \( \mathbb{F}_p \)-subvector spaces of \( W_1 \):

\[ W_1 = W_1^{(1)} \supseteq W_1^{(2)} \supseteq \cdots \supseteq W_1^{(s+1)} = \{0\} \]

such that \( [W_1^{(i-1)} : W_1^{(i)}] = p \). It induces the following inclusions:

\[ k(Z) = k(Z)^{W_1^{(i+1)}} \supseteq k(Z)^{W_1^{(i)}} \supseteq \cdots \supseteq k(Z)^{W_1^{(1)}} = k(X) \]

Then, apply Lemma 3.2 to \( K_1/K \): the completion at \( \infty \) of the extension \( k(C)/k(X) \), whose group \( G_2 \) is a \( p \)-group, and to \( K_0/K \): the completion at \( \infty \) of the \( p \)-cyclic extension \( k(Z)^{W_1^{(i)}}/k(Z)^{W_1^{(i-1)}} \) whose conductor is \( 2 \). By induction, we thus prove that the extension \( k(\tilde{C})/k(T) \) also has conductor \( 2 \). It follows from the Hurwitz genus formula that \( g_{\tilde{C}} = p^s g_C \). Finally, the last statement on \( \tilde{G}_2 \) is a consequence of Lemma 2.4.1. □

**Remark 3.4.** Under the conditions of Proposition 3.1, it can happen that \( G \) is a \( p \)-Sylow subgroup of \( Aut_k(C) \) without \( \tilde{G} \) being a \( p \)-Sylow subgroup of \( Aut_k(\tilde{C}) \).

Indeed, take \( C : W^p - W = X^{1+p} \) and \( S(Z) = Z^p - Z \). Then, \( \tilde{C} \) is parametrized by \( \tilde{W}^p - \tilde{W} = (Z^p - Z) (Z^{p^2} - Z^p) = -Z^2 + 2 Z^{1+p} - Z^{1+p^2} \) mod \( \varphi(k[Z]) \). We denote by \( G_{\infty,1}(C) \) (resp. \( G_{\infty,1}(\tilde{C}) \)) the wild inertia subgroup of \( Aut_k(C) \) (resp. \( Aut_k(\tilde{C}) \)) at \( X = \infty \) (resp. \( Z = \infty \)). Note that \( G_{\infty,1}(C) \) (resp. \( G_{\infty,1}(\tilde{C}) \)) is a \( p \)-Sylow subgroup of \( Aut_k(C) \) (resp. \( Aut_k(\tilde{C}) \)). Take \( G := G_{\infty,1}(C) \). From Proposition 2.5, we deduce that \( |\tilde{G}| = p |G| = p |G_{\infty,1}(C)| = p^4 \), whereas \( |G_{\infty,1}(\tilde{C})| = p^5 \).

## 4 A new step towards a classification of big actions.

If big actions are defined through the value taken by the quotient \( \frac{|G|}{g} \), it occurs that the key criterion to classify them is the value of another quotient: \( \frac{|G|}{g} \). Indeed, the quotient \( \frac{|G|}{g} \) has, to some extent, a "sieve" effect among big actions. In what follows, we pursue the work of Lehr and Matignon who describe big actions for the two highest possible values of this quotient, namely \( \frac{|G|}{g} = \frac{4}{(p^2-1)^2} \) and \( \frac{|G|}{g} = \frac{4}{(p-1)^2} \) (cf. [LM05] Thm. 8.6). More precisely, we investigate the big actions \( (C,G) \) that satisfy:

\[
M := \frac{4}{(p^2-1)^2} \leq \frac{|G|}{g^2}
\]

The choice of the lower bound \( M \) can be explained as follows: as shown in the proof of ([LM05], Thm. 8.6), a lower bound \( M \) on the quotient \( \frac{|G|}{g^2} \) involves an upper bound on the order of the second
where $i_0$ is defined as in Proposition 2.5. Therefore, we have to choose $M$ small enough to obtain a wide range of possibilities for the quotient, but meanwhile large enough to get serious restrictions on the order of $G_2$. The optimal bound seems to be $M := \frac{p^4 - 1}{p^2 - 1}$, insofar as, for such a choice of $M$, the upper bound on $G_2$ implies that its order divides $p^3$, and then that $G_2$ is abelian (cf. Corollary 2.9).

Proposition 4.1. Let $(C, G)$ be a big action with $g \geq 2$ satisfying condition 3. Then, the order of $G_2$ divides $p^3$. It follows that $G_2$ is abelian.

Proof: Put $p^m := \frac{G_2}{G_2 \cdot i_{o+1}}$, with $m \geq 1$, and $A_m := \frac{G_2}{G_2 \cdot i_{o+1}} - 1 = \frac{p^m}{M \cdot (p^m - 1)^2}$. Then, inequality (4) reads: $1 \leq \frac{G_2}{G_2 \cdot i_{o+1}} \leq p^m A_m$, which gives: $1 \leq \frac{G_2 \cdot i_{o+1}}{G_2} \leq A_m$. Since $(A_m)_{m \geq 1}$ is a decreasing sequence with $A_4 < 1$, we conclude that $m \in \{1, 2, 3\}$.

If $m = 3$, then $1 \leq \frac{G_2 \cdot i_{o+1}}{G_2} < 1$. So $|G_2| = 1$ and $|G_2| = p^3$. If $m = 2$, then $1 \leq \frac{G_2 \cdot i_{o+1}}{G_2} \leq 2 = p^2$. So $|G_2| = p^2 |G_2 \cdot i_{o+1}|$, with $|G_2 \cdot i_{o+1}| \in \{1, p, p^2\}$. This leaves only one case to exclude, namely $|G_2 \cdot i_{o+1}| = p^2$. In this case, $|G_2| = p^4$ and formula (2) yields a lower bound on the genus, namely: $2 g \geq (i_0 - 1)(p^4 - 1)$. Let $s$ be the integer defined in Remark 2.7. Then, $i_0 = 1 + p^s$.

Besides, by Theorem 2.6, $V \subset (\mathbb{Z}/p\mathbb{Z})^{2s}$. Consequently, $|G| = |G_2||V| \leq p^{t + 2s}$ and

$$\frac{|G|}{g^2} \leq \frac{p^{t + 2s}}{p^{t + 2s} - 1} = \frac{4}{p^{t + 2s} - 1} < \frac{4}{p^{t + 2s} - 1}$$

which contradicts equality (3). If $m = 1$, then $1 \leq \frac{G_2 \cdot i_{o+1}}{G_2} < 1$ with $A_1 := p (p + 1)^2 = \left\{ \begin{array}{ll} p^4, & \text{if } p \geq 3, \\
 p^5, & \text{if } p = 2. \end{array} \right.$

Since $G_2$ is a $p$-group, we get: $\left\{ \begin{array}{ll} 1 \leq |G_2| \leq p^3, & \text{if } p \geq 3, \\
 1 \leq |G_2| \leq p^4, & \text{if } p = 2. \end{array} \right.$ As $|G_2| = p |G_2 \cdot i_{o+1}|$, there are two cases to exclude: $|G_2 \cdot i_{o+1}| = p^{t + \epsilon}$, with $\epsilon = 0$ if $p \geq 3$ and $\epsilon \in \{0, 1\}$ if $p = 2$. Then $|G_2| = p^{t + \epsilon}$. If $\epsilon = 0$, we are in the same situation as in the previous case. If $\epsilon = 1$, (2) yields $2 g \geq (i_0 - 1)(p^5 - 1)$.

Since this case only occurs for $p = 2$, we eventually get an inequality:

$$\frac{|G|}{g^2} \leq \frac{p^{t + 2s}}{p^{t + 2s} - 1} = \frac{128}{961} \leq \frac{4}{g^2} \leq \frac{4}{p^2 - 1}$$

which contradicts condition (3). Therefore, the order of $G_2$ divides $p^3$. Then, we gather from Corollary 2.9 that $G_2$ is abelian.

But we can even prove better: under these conditions, $G_2$ has exponent $p$.

Proposition 4.2. Let $(C, G)$ be a big action with $g \geq 2$ satisfying condition 3. Then $G_2$ is abelian with exponent $p$.

Proof: By Proposition 4.1, $G_2$ is abelian, with order dividing $p^3$. As a consequence, if $G_2$ has exponent strictly greater than $p$, either $G_2$ is cyclic with order $p^2$ or $p^3$, or $G_2$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We begin with a lemma excluding the second case. Note that one can find big actions $(C, G)$ with $G_2$ abelian of exponent $p^2$. Nevertheless, it requires the $p$-rank of $G_2$ to be large enough (see section 6).

Lemma 4.3. Let $(C, G)$ be a big action with $g \geq 2$ satisfying condition 3. Then $G_2$ cannot be isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof: Assume $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then, the lower ramification filtration of $G$ reads as in one of the four following cases:

i) $G = G_1 \supset G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_1 \ast \mathbb{Z}/p\mathbb{Z} \supset G_{i_0 + i_1} = \{0\}$.

ii) $G = G_1 \supset G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_1 \ast \mathbb{Z}/p\mathbb{Z} \supset G_{i_0 + i_1} = \{0\}$.

iii) $G = G_1 \supset G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_1 \ast \mathbb{Z}/p\mathbb{Z} \supset G_{i_0 + i_1 + i_2} = \{0\}$.

iv) $G = G_1 \supset G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_1 \ast \mathbb{Z}/p^2\mathbb{Z} \supset G_{i_0 + i_1 + i_2} = \{0\}$.
We now focus on the ramification filtration of $G_2$, temporary denoted by $H$ for convenience. Then, for all $i \geq 0$, the lower ramification groups of $H$ are: $H_i = H \cap G_i$.

In case i), the lower ramification of $H$ reads:

$$H = H_0 = \cdots = H_{i_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+1} = \cdots = H_{i_0+i_1} \simeq \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+i_1+1} = \{0\}.$$  

Consider the upper ramification groups: $H^{p_0} = H^{\varphi(i_0)} = H_{i_0}$ and $H^{p_1} = H^{\varphi(i_0+i_1)} = H_{i_0+i_1}$, where $\varphi$ denotes the Herbrand function. Then, the ramification filtration in upper notation reads:

$$H^0 = \cdots = H^{p_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{p_0+1} = \cdots = H^{p_1} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{p_1+1} = \{0\}.$$  

Since $H$ is abelian, it follows from Hasse-Arf theorem that $\nu_0$ and $\nu_1$ are integers. Consequently, the formula:

$$\forall m \in \mathbb{N}, \quad \varphi(m) + 1 = \frac{1}{|H_0|} \sum_{i=0}^{m} |H_i|$$  

gives $\nu_0 = i_0$ and $\nu_1 = i_0 + \frac{i_1}{p}$. Besides, $\textbf{[Ma71]}$ (Thm. 6) implies $H^{p_0} \supset H^{p_0} \supset (H^{p_0})^p$ with $(H^{p_0})^p = H^p = G_2^p \simeq \mathbb{Z}/p\mathbb{Z}$. Thus, $H^{p_0} \supset H^{p_1}$, which involves: $p\nu_0 \leq \nu_1$ and $i_1 \geq p^2(p-1)i_0$.

Then, the Hurwitz genus formula applied to $C \rightarrow C/H \simeq \mathbb{P}^1_k$ yields a lower bound for the genus:

$$2g = (i_0 - 1)(|H| - 1) + i_1(|H_{i_0+1}| - 1) \geq (p-1)(i_0 + 1)(p^3 + p + 1).$$

Let $s$ be the integer defined in Remark 2.7. Then, $i_0 = 1 + p^s$. Moreover, by Theorem 2.6, $|G| = |G_2||V| \leq p^{i_0+2}$. It follows that $\frac{|G|}{p} \leq \frac{p^3(p^2+1)^2}{(p^3+2(p^2+1)^2)$. Since $\frac{p^3(p^2+1)^2}{(p^3+2(p^2+1)^2} < 1$ for $p \geq 2$, this contradicts condition (3).

In case ii), the lower ramification filtration of $H$ reads:

$$H = H_0 = \cdots = H_{i_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+1} = \cdots = H_{i_0+i_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H_{i_0+i_1+1} = \{0\}.$$  

Keeping the same notation as in case i), the upper ramification filtration reads:

$$H = H^0 = \cdots = H^{\nu_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_0+1} = \cdots = H^{\nu_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H^{\nu_1+1} = \{0\},$$  

with $\nu_0 = \varphi(i_0) = i_0$ and $\nu_1 = \varphi(i_0 + i_1) = i_0 + \frac{i_1}{p}$. Once again, $H^{p_0} \supset (H^{p_0})^p \simeq \mathbb{Z}/p\mathbb{Z}$ implies $H^{p_0} \supset H^{p_1}$, which involves $p\nu_0 \leq \nu_1$ and $i_1 \geq i_0(p-1)$. Then, the Hurwitz genus formula yields:

$$2g = (i_0 - 1)(|H| - 1) + i_1(|H_{i_0+1}| - 1) \geq (p-1)p^s(p^3 + p^2 + 1) \geq (p-1)p^s(p^3 + p + 1).$$

Thus, we get the same lower bound on the genus as in the preceding case, hence the same contradiction.

In case iii), the lower ramification filtration of $H$ reads:

$$H_{i_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+1} = \cdots = H_{i_0+i_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H_{i_0+i_1+1} = \cdots = H_{i_0+i_1+i_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset \{0\}.$$  

Keeping the same notation as above and introducing $H^{p_2} = H^{\varphi(i_0+i_1+i_2)} = H_{i_0+i_1+i_2}$, the upper ramification filtration reads:

$$H^{p_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{p_0+1} = \cdots = H^{\nu_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H^{\nu_1+1} = \cdots = H^{p_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{p_2+1} = \{0\}$$  

with $\nu_0 = \varphi(i_0) = i_0$, $\nu_1 = \varphi(i_0 + i_1) = i_0 + \frac{i_1}{p}$ and $\nu_2 = \varphi(i_0 + i_1 + i_2) = i_0 + \frac{i_1}{p} + \frac{i_2}{p}$. Since $H^{p_0} \supset (H^{p_0})^p \simeq \mathbb{Z}/p\mathbb{Z}$, we obtain: $H^{p_0} \supset H^{p_2}$. Then, $p\nu_0 \leq \nu_2$, which involves $p^2(p-1)i_0 \leq i_1p + i_2$. With such inequalities, the Hurwitz genus formula gives a new lower bound for the genus, namely:

$$2g = (i_0 - 1)(|H| - 1) + i_1(|H_{i_0+1}| - 1) + i_2(|H_{i_0+i_1+1}| - 1) \geq (p-1)(p^s(p^2 + p + 1) + (p^s+1)(p-1)p^2)$$

From $2g \geq (p-1)(p^{s+1} + p^{s+1} + p^s + p^s - p^2) \geq (p-1)p^s(p^3 + p)$, we infer the inequality:

$$\frac{|G|}{g^2} \leq \frac{4}{p^2 - 1} \frac{p^2s+5(p+1)^2}{p^2s(p^3 + p)^2} = \frac{4}{p(p+1)^2} \frac{p^2s(p^3 + p)^2}{(p^2 - 1)^2}$$

Since $\frac{p(p+1)^2}{(p^2 - 1)^2} < 1$ for $p \geq 2$, this contradicts condition (3).
H_{i_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+1} = \cdots = H_{i_0+i_1} \simeq (\mathbb{Z}/p^2\mathbb{Z}) \supset H_{i_0+i_1+1} = \cdots = H_{i_0+i_1+i_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset \{0\}.

induces the following upper ramification filtration:

H^{v_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{v_0+1} = \cdots = H^{v_1} \simeq (\mathbb{Z}/p^2\mathbb{Z}) \supset H^{v_1+1} = \cdots = H^{v_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{v_2+1} = \{0\}.

This is almost the same situation as in case iii), except that $H_{i_0+1}$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ instead of $(\mathbb{Z}/p\mathbb{Z})^2$. But, since the only thing that plays a part in the proof is the order of $H_{i_0+1}$, which is the same in both cases, namely $p^2$, we conclude with the same arguments as in case iii). □

**Remark 4.4.** The previous method based on the analysis of the ramification filtration of $G_2$ fails to exclude the case $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$ for a big action satisfying (3). Indeed, if $H := G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$, the lower ramification filtration of $H$:

$H_0 = \cdots = H_{i_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \supset H_{i_0+1} = \cdots \supset H_{i_0+i_1} \simeq \mathbb{Z}/p\mathbb{Z} \supset H_{i_0+i_1+1} = \{0\}.$

induces the upper ramification filtration:

$H^0 = \cdots = H^{v_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \supset H^{v_0+1} = \cdots = H^{v_1} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{v_1+1} = \{0\}.

with $v_0 = \varphi(i_0) = i_0$ and $v_1 = \varphi(i_0 + i_1) = i_0 + \frac{i_1}{p}$. Since $H^{v_0+i} \supset (H^{v_0})^p \simeq \mathbb{Z}/p\mathbb{Z}$, we obtain:

$p^2 v_0 \leq v_1$, hence $i_1 \geq (p - 1)p i_0$. Let $s$ be the integer defined in Remark 2.7. Then, the Hurwitz genus formula yields:

$$2g = (i_0 - 1)(|H| - 1) + i_1(|H_{i_0+1} - 1| \geq (p - 1)(p^s(p^2 + 1) + p^2 - p) \geq (p - 1)p^s(p^2 + 1).$$

If we denote by $v$ the dimension of the $\mathbb{F}_p$-vector space $V$, we eventually get:

$$\frac{|G|}{g^2} \leq \frac{4}{(p^2 - 1)^2} p^{2 + v}\frac{p^2 + 1}{p^{2s}(p^2 + 1)^2}.$$.

In this case, condition (3) requires $p^{1 + \frac{n}{2} - s} > p^2$. Since $\frac{n}{2} \leq s$, this implies $p + 1 > p^{1 + \frac{n}{2} - s} \geq p^2$, hence $\frac{n}{2} = s$. This means that $V = \mathbb{Z}(\text{Ad}_f)$, where $f$ is the function defined in Remark 2.7 and $\text{Ad}_f$ its palindromic polynomial as defined in Proposition 2.5. Therefore, one does not obtain yet any contradiction.

Accordingly, to exclude the cyclic cases $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$ and $G_2 \simeq \mathbb{Z}/p^3\mathbb{Z}$ and thus complete the proof of Proposition 4.2, we need to shift from a ramification point of view on $G_2$ to the embedding problem: $G_2 \subseteq G_1$. This enables us to prove the more general result on big actions formulated in the next part.

### 5 Big actions with a cyclic second ramification group $G_2$.

The aim of this section is to prove that there does not exist any big action whose second ramification group $G_2$ is cyclic, except for the trivial case $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

**Theorem 5.1.** Let $(C, G)$ be a big action. If $G_2 \simeq (\mathbb{Z}/p^n\mathbb{Z})$, then $n = 1$.

**Proof:**

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

1. **First of all**, we prove that we can assume $n = 2$.

   Indeed, for $n > 2$, $\mathcal{H} := G_2^{n-2}$ is a normal subgroup in $G$, strictly included in $G_2$. So Lemma 2.4.2 asserts that the pair $(C/\mathcal{H}, G/\mathcal{H})$ is a big action. Besides, the second lower ramification group of $G/\mathcal{H}$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

2. **Notation and preliminary remarks.**

   We denote by $L := k(C)$ the function field of $C$ and by $k(X) := L^{G_2}$ the subfield of $L$ fixed by $G_2$. Following Artin-Schreier-Witt theory (see [Bo83] Chap. IX, ex. 19), we define the $W_2(\mathbb{F}_p)$-module

$$\hat{A} := \frac{\varphi(W_2(L)) \cap W_2(k(X))}{\varphi(W_2(k(X)))}.$$
where $W_2(L)$ denotes the ring of Witt vectors of length 2 with coordinates in $L$. The inclusion $k[X] \subset k(X)$ induces an injection

$$A := \frac{\wp(W_2(L)) \cap W_2(k[X])}{\wp(W_2(k[X]))} \hookrightarrow \hat{A}$$

Since $L/L^{G_2}$ is étale outside $X = \infty$, it follows from [Mi80] (III, 4.12) that we can identify $A$ with $\hat{A}$. Consider the Artin-Schreier-Witt pairing:

$$\begin{cases} G_2 \times A \to W_2(\mathbb{F}_p) \\ (g, x) \mapsto [g, x] := gx - x \end{cases}$$

where $g \in G_2 \subset \text{Aut}_k(L)$, $x \in L$ such that $\wp x \in k[X]$ and $[g, x]$ denotes the class of $gx \mod \wp(k[X])$. This pairing is non degenerate, which proves that, as a group, $A$ is dual to $G_2$.

As a $\mathbb{Z}$-module, $A$ is generated by $(f_0(X), g_0(X))$ in $W_2(k[X])$ and then, $L = k(X, W_0, V_0)$ with $\wp(W_0, V_0) = (f_0(X), g_0(X))$. An exercise left to the reader shows that one can choose $f_0(X)$ and $g_0(X)$ reduced mod $\wp(k[X])$ (see definition of a reduced polynomial in section 1). We denote by $m_0$ (resp. $n_0$) the degree of $f_0$ (resp. $g_0$). Note that they are prime to $p$. The $p$-cyclic cover $L^{G_2}/L^{G_2}$ is parametrized by: $W_0^p - W_0 = f_0(X)$. We deduce from Proposition 2.5 that $f_0(X) = XS(X) + cX$, where $S$ is an additive polynomial with degree $s \geq 1$ in $F$. After an homothety on $X$, we can assume $S$ to be monic. Furthermore, note that $s \geq 2$. Indeed, if $s = 1$, the two inequalities established in Remark 4.4: $|G| \leq p^{2+2s} \leq p^4$ and $2g \geq (p - 1)(p^2 + 1 + p^2 - p) = (p - 1)(p^2 + p^2) \equiv \frac{p^3}{2} \leq \frac{p^3}{p-1} < \frac{p^3}{p-3}$, which contradicts (1).

3. **The embedding problem.**

For any $y \in V$, the class of $(f_0(X + y), g_0(X + y))$ in $A$ induces a new generating system of $A$, which means that:

$$\mathbb{Z} (f_0(X), g_0(X)) = \mathbb{Z} (f_0(X + y), g_0(X + y)) \mod \wp(W_2(k[X]))). \quad (5)$$

As $A$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, (5) ensures the existence of an integer $n(y)$ such that

$$(f_0(X + y), g_0(X + y)) = n(y) (f_0(X), g_0(X)) \mod \wp(W_2(k[X])) ) \quad (6)$$

where $n(y) := a_0(y) + b_0(y)p$, with $a_0(y) \in \mathbb{N}$, $0 < a_0(y) < p$, and $b_0(y) \in \mathbb{N}$, $0 \leq b_0(y) < p$. We calculate $n(y) (f_0(X), g_0(X)) = a_0(y) (f_0(X), g_0(X)) + b_0(y)p (f_0(X), g_0(X))$. On the one hand, $a_0(y) (f_0(X), g_0(X)) = (a_0(y) f_0(X), a_0(y) g_0(X) + c(a_0(y)) f_0(X))$, where $c(a_0(y))$ is given by the recursive formula:

$$\forall i \in \mathbb{N}, \quad c(i + 1) = c(i) + \frac{1}{p} (1 + i^p - (1 + i)^p) \mod p$$

On the other hand,

$$b_0(y)p (f_0(X), g_0(X)) = b_0(y) (0, f_0(X)^p) = (0, b_0(y) f_0(X)) \mod \wp(W_2(k[X]))$$

As a conclusion, (6) reads:

$$(f_0(X + y), g_0(X + y)) = (a_0(y) f_0(X), a_0(y) g_0(X) + \ell_0(y) f_0(X)) \mod \wp(W_2(k[X])) \quad (7)$$

where $\ell_0(y) := c(a_0(y)) + b_0(y)$. We notice that, for all $y \in V$, $a_0(y) = 1 \mod p$. Indeed, the equality of the first coordinate of Witt vectors in (6) implies $f_0(X + y) = a_0(y) f_0(X) \mod \wp(k[X])$. Thus, by induction, $f_0(X + py) = a_0(y)^p f_0(X) \mod \wp(k[X])$. Since $V$ is an elementary abelian $p$-group, $f_0(X + py) = f_0(X)$, which involves: $a_0(y)^p = 1 \mod p$ and $a_0(y) = 1 \mod p$. So, (7) becomes:

$$(f_0(X + y), g_0(X + y)) = (f_0(X), g_0(X) + \ell_0(y) f_0(X)) + (P^p(X), Q^p(X)) - (P(X), Q(X)) \quad (8)$$

with $P(X)$ and $Q(X)$ polynomials of $k[X]$. In order to circumvent the problem related to the special formula giving the opposite of Witt vectors for $p = 2$, we would rather write (8) as follows:

$$(f_0(X + y), g_0(X + y)) + (P(X), Q(X)) = (f_0(X), g_0(X) + \ell_0(y) f_0(X)) + (P^p(X), Q^p(X)) \quad (9)$$
The first coordinate of (9) reads:

\[ f_0(X + y) + P(X) = f_0(X) + P(X)^p \]  (10)

On the second coordinate of (9), the addition law in the ring of Witt vectors gives the following equality in \( k[X] \):

\[
go_0(X + y) + Q(X) + \psi(f_0(X + y), P(X)) = go_0(X) + \ell_0(y) f_0(X) + Q(X)^p + \psi(f_0(X), P(X)^p) \]  (11)

where \( \psi \) is defined as follows:

\[
\psi(a, b) := \frac{1}{p} (a^p + b^p - (a + b)^p) = -\frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = \sum_{i=1}^{p-1} \frac{(-1)^i}{i} a^i b^{p-i} \mod p
\]

As a consequence, (11) gives:

\[
\Delta_y(g_0) := go_0(X + y) - go_0(X) = \ell_0(y) f_0(X) + \delta \mod \varphi(k[X])
\]  (12)

with

\[
\delta := \psi(f_0(X), P(X)^p) - \psi(f_0(X + y), P(X)) = \sum_{i=1}^{p-1} \frac{(-1)^i}{i} \{ f_0(X)^i P(X)^{p(p-i)} - f_0(X + y)^i P(X)^{p(p-i)} \}
\]

**Lemma 5.2.** With the notation defined above, \( \delta \) is equal to:

\[
\delta = \sum_{i=1}^{p-1} \frac{(-1)^i}{i} y^{p-i} X^{i+p^{s+1}} + \text{lower degree terms in } X
\]  (13)

**Proof:** We search for the monomials in \( \delta \) that have degree in \( X \) greater or equal to \( p^{s+1} + 1 \). We first focus on \( f_0(X)^i P(X)^{p(p-i)} \). We can infer from equality (11) that \( P(X) \) has degree \( p^{s-1} \) and that its leading coefficient is \( y^{1/p} \). Furthermore, [LM05] (proof of Prop. 8-1) shows that \( P(X) - P(0) \) is an additive polynomial. So, we can write: \( P(X) = y^{1/p} X^{p^{s-1}} + P_1(X) \), where \( P_1(X) \) is a polynomial of \( k[X] \) with degree at most \( p^{s-2} \). Then, for all \( i \in \{1, \ldots, p-1\} \),

\[
f_0(X)^i P(X)^{p(p-i)} = f_0(X)^i (y X^{p-i} P_1(X)^p)^{p-i} = f_0(X)^i \left( \sum_{j=0}^{p-i} \binom{p-i}{j} y^j X^{p-i} P_1(X)^p \right)^{p(p-i)}.
\]

Since \( f_0(X) \) has degree: \( 1 + p^s \), this gives in \( \delta \) a monomial of degree at most: \( i (1 + p^s) + j p^s + p (p - i - j) p^{s-2} = p^s + (i + j) (p - 1) p^{s-1} + i \). If \( j \leq p - i - 1 \), this degree is at most: \( p^s + (p-1)^2 p^{s-1} + i = (p-1) p^{s} + p^{s-1} + i \), which is strictly lower than \( p^{s+1} + 1 \), for \( s \geq 2 \) and \( 1 \leq i \leq p - 1 \). As a consequence, the monomials of degree greater or equal to \( p^{s+1} + 1 \) can only occur when the index \( j \) is equal to \( p - i \), namely in \( f_0(X)^i y^{p-i} X^{p(p-i)} \). As \( f_0(X) = X S(X) + c X \), where \( S \) is a monic additive polynomial of degree \( s \) in \( F \), \( f_0 \) reads:

\[
f_0(X) = X^{1+p^s} + P_2(X)
\]

where \( P_2(X) \) is a polynomial in \( k[X] \) with degree at most \( 1 + p^{s-1} \). Then, for all \( i \) in \( \{1, \ldots, p-1\} \),

\[
f_0(X)^i y^{p-i} X^{p(p-i)} = y^{p-i} X^{p(p-i)} \left( \sum_{k=0}^{i} \binom{i}{k} X^{i+p^{s-1}} \right)^{i+p^{s-1}}.
\]

Accordingly, we get a monomial of degree at most: \( p^s (p - i) + k (1 + p^s) + (i - k) (1 + p^{s-1}) = p^s (p - i) + i (1 + p^{s-1}) + k (p^s - p^{s-1}) \). When \( 0 \leq k \leq i - 1 \), the maximal degree obtained in this way is \( i + p^{s-1} - p^s + p^{s+1} \), which is strictly lower than \( p^{s+1} + 1 \). Therefore, for all \( i \) in \( \{1, \ldots, p-1\} \), the only contribution to take into account is \( k = i \), which produces in \( \delta \) the sum:

\[
\sum_{i=1}^{p-1} \frac{(-1)^i}{i} y^{p-i} X^{i+p^{s+1}}.
\]

We now search for monomials with degree greater or equal to \( p^{s+1} + 1 \) in the second part of \( \delta \), namely:

\[
f_0(X + y)^i P(X)^{p^{-i}}
\]

This has degree at most:

\[
i (1 + p^s) + (p - i) p^{s-1} = i p^s + (p - i) p^{s-1} + i,
\]

which is strictly lower than \( p^{s+1} + 1 \), for \( s \geq 2 \) and \( 1 \leq i \leq p - 1 \). Therefore, \( f_0(X + y)^i P(X)^{p^{-i}} \) does not give any monomial in \( \delta \) with degree greater or equal to \( p^{s+1} + 1 \). Thus, we get the expected formula. \( \Box \)

4. We notice that \( g_0(X) \) cannot be of the form \( X \Sigma(X) + \gamma X \), with \( \Sigma \in k[F] \) and \( \gamma \in k \).

Otherwise, the left-hand side of (12) reads:

\[
\Delta_y(g_0) := go_0(X + y) - go_0(X) = X \Sigma(Y) + y \Sigma(X) + y (\Sigma(y) + \gamma y),
\]

which only gives a linear contribution in \( X \) after reduction mod \( \varphi(k[X]) \). By Lemma 5.2, \( \deg f_0 = 1 + p^s < \deg \delta = p^{s+1} + p - 1 \), which involves that the degree of the right-hand side of (12) is \( p - 1 + p^{s+1} > 1 \), hence a contradiction.

Therefore, we can define an integer \( a \leq n_0 = \deg g_0 \) such that \( X^a \) is the monomial of \( g_0(X) \) with highest degree which is not of the form \( 1 + p^n \), with \( n \in \mathbb{N} \). Note that since \( g_0 \) is reduced mod \( \varphi(k[X]) \), \( a \neq 0 \mod p \). We also notice that the monomials in \( g_0(X) \) with degree
5. We show that $p$ divides $a - 1$.

Assume that $p$ does not divide $a - 1$. In this case, the monomial $X^{a-1}$ is reduced mod $\varphi(k[X])$. Since the monomials of $g_0(X)$ with degree strictly greater than $a$ only give a linear contribution in $\Delta_y(g_0) \mod \varphi(k[X])$, (12) reads as follows, for all $y$ in $V$:

$$c_a(g_0) a y X^{a-1} + \text{lower degree terms} = -y X^{p+1} + p - 1 + \text{lower degree terms \ mod \ \varphi(k[X])}$$

where $c_a(g_0) \neq 0$ denotes the coefficient of $X^a$ in $g_0$. If $a - 1 > p^{t+1} + p - 1$, the coefficient $c_a(g_0) a y = 0$, for all $y$ in $V$. Since $a \neq 0 \mod p$, it leads to $V = \{0\}$, so $G_1 = G_2$, which is impossible for a big action (see Proposition 2.2.1). We gather from (14) that $a - 1 = p^{t+1} + p - 1$, which contradicts: $a \neq 0 \mod p$.

Thus, $p$ divides $a - 1$. So, we can write $a = 1 + \lambda p^t$, with $t > 0$, $\lambda$ prime to $p$ and $\lambda \geq 2$ because of the definition of $a$. We also define $j_0 := a - p^t = 1 + (\lambda - 1) p^t$. Note that $p j_0 > a$.

Indeed,

$$p j_0 \leq a \iff p(1 + (\lambda - 1) p^t) \leq 1 + \lambda p^t \iff \lambda \leq \frac{1 - p + p^{t+1}}{p^t (p - 1)} = \frac{-1}{p^t} + \frac{p}{p - 1} - \frac{1}{2} \leq 2$$

which is impossible since $\lambda \geq 2$.

6. We determine the coefficient of $X^{j_0}$ in the left hand-side of (12).

Since $p$ does not divide $j_0$, the monomial $X^{j_0}$ is reduced mod $\varphi(k[X])$. In the left-hand side of (12), namely $\Delta_y(g_0) \mod \varphi(k[X])$, the monomial $X^{j_0}$ comes from monomials of $g_0(X)$ of the form: $X^b$, with $b \in \{j_0 + 1, \ldots, a\}$. As a matter of fact, the monomials of $g_0(X)$ with degree strictly greater than $a$ only give a linear contribution mod $\varphi(k[X])$, whereas $j_0 = 1 + (\lambda - 1) p^t > 1$. For all $b \in \{j_0 + 1, \ldots, a\}$, the monomial $X^b$ of $g_0(X)$ generates $(b) y^{b-j_0} X^{j_0}$ in $\Delta_y(g_0)$. Since $p j_0 > a \geq b$ (see above), these monomials $X^b$ do not produce any $X^{j_0} p^n$, with $n \geq 1$, which would also give $X^{j_0}$ after reduction mod $\varphi(k[X])$. It follows that the coefficient of $X^{j_0}$ in the left-hand side of (12) is $T(Y) := \sum_{b=j_0+1}^a c_b(g_0) (b_{j_0}) Y^{b-j_0}$, where $c_b(g_0)$ denotes the coefficient of $X^b$ in $g_0(X)$. As the coefficient of $Y^{-j_0}$ in $T(Y)$ is $c_a(g_0) (a_{j_0}) = c_a(g_0) (1 + \lambda p^t) \equiv c_a(g_0) \lambda \not\equiv 0 \mod p$, the polynomial $T(Y)$ has degree $a - j_0 = p^t$.

7. We identify with the coefficient of $X^{j_0}$ in the right-hand side of (12) and gather a contradiction.

We first assume that the monomial $X^{j_0}$ does not occur in the right-hand side of (12). Then, $T(y) = 0$ for all $y$ in $V$, which means that $V$ is included in the set of roots of $T$. Thus, $|V| \leq p^t$.

To compute the genus $g$, put $M_0 := n_0$ and $M_1 := \max\{p m_0, n_0\}$. Then, by [Ga99], the Hurwitz genus formula applied to $C \to C/G \simeq \mathbb{P}^1_k$ yields: $2(g - 1) = 2|G|/|G_2| \geq p_1^t \geq p^{t+1} + p$ and $p^{t+1} + p - 1 < n_0$, we infer $M_1 = n_0$. Moreover, since $n_0 \geq a = 1 + \lambda p^t \geq 1 + 2 p^t > 2 p^t$, we obtain a lower bound for the genus: $2 g = (p - 1) p (n_0 - 1 + p^{s+1}) \geq 2 p^{t+1} (p - 1)$. As $|G| = |G_2||V| \leq p^{2t}$, it entails an inequality $\frac{|G_2|}{g} \leq \frac{2 p^{t+1}}{p - 1} \leq \frac{2}{p - 1} \geq \frac{2}{p^t}$, which contradicts (11).

As a consequence, the monomial $X^{j_0}$ appears in the right-hand side of (12), which implies that $j_0 \leq p^{s+1} + p - 1$. Using (14), we get: $j_0 = 1 + (\lambda - 1) p^t \leq p^{s+1} + p - 1 < a = 1 + \lambda p^t$.

This yields:

$$\lambda - 1 \leq p^{s+1} - t + \frac{2 - p}{p^t} < \lambda$$

If $s + 1 - t \leq -1$, since $t \geq 1$, (15) gives: $\lambda - 1 \leq \frac{t}{p} + \frac{2 - p}{p^t} < 1$, which contradicts $\lambda \geq 2$. It follows that $s + 1 - t \geq 0$. Then, (15) combined with: $0 \leq \frac{p - 2}{p^t} < 1$ leads to $\lambda - 1 = p^{s+1} - t$.

We gather that $j_0 = 1 + (\lambda - 1) p^t = p^{s+1} + p - 1 < a = 1 + \lambda p^t$. Therefore, in the right-hand side of (12), the monomial $X^{j_0} = X^{1 + p^t}$ only occurs in $\delta$. By Lemma 5.2, the coefficient of $X^{j_0} = X^{1 + p^t}$ in $\delta$ is $-y^{p-1}$. By equating the coefficient of $X^{j_0}$ in each side of (12), we get $T(y) = -y^{p-1}$, for all $y$ in $V$. Put $T(Y) := T(Y) + y^{p-1}$. Since $deg T = p^t > p - 1$, the
Therefore, when \((C, G)\) is a big action, \(G_2 \simeq (\mathbb{Z}/p^n\mathbb{Z})\) implies \(n = 1\). More generally, if \(G_2\) is abelian of exponent \(p^n\), with \(n \geq 2\), there exists an index \(p\)-subgroup of \(G_2^n\), say \(H\), normal in \(G\) such that the pair \((C/H, G/H)\) is a big action with \((G/H)_2 = G_2/H \simeq \mathbb{Z}/p^n \mathbb{Z} \times (\mathbb{Z}/p^n\mathbb{Z})^t\), with \(t \in \mathbb{N}^*\). A natural question is to search for a lower bound on the \(p\)-rank: \(t\) depending on the genus \(g\) of the curve. As seen in the proof of Theorem 5.1, the difficulty lies in the embedding problem, i.e. in finding an extension which is stable under the translations by \(V\). In the next section, we exhibit big actions with \(G_2\) abelian of exponent at least \(p^n\). In particular, we construct big actions \((C, G)\) with \(G \simeq \mathbb{Z}/p^n \mathbb{Z} \times (\mathbb{Z}/p^n\mathbb{Z})^t\) where \(t = O(\log p)\).

6 Examples of big actions with \(G_2\) abelian of exponent strictly greater than \(p\).

In characteristic 0, an analogue of big actions is given by the actions of a finite group \(G\) on a compact Riemann surface \(C\) with genus \(g_C \geq 2\) such that \(|G| = 84(g_C - 1)\). Such a curve \(C\) is called a Hurwitz curve and such a group \(G\) a Hurwitz group (cf. \cite{Co90}). In particular, the lowest genus Hurwitz curves are the Klein’s quartic with \(G \simeq \text{PSL}_2(\mathbb{F}_7)\) (cf. \cite{El99}) and the Fricke-Macbeath curve with genus 7 and \(G \simeq \text{PSL}_2(\mathbb{F}_8)\) (cf. \cite{Mc65}).

Let \(C\) be a Hurwitz curve with genus \(g_c\). Let \(n \geq 2\) be an integer and let \(C_n\) be the maximal unramified Galois cover whose group is abelian, with exponent \(n\). The Galois group of the cover \(C_n/C\) is isomorphic to \((\mathbb{Z}/n\mathbb{Z})^{2g_c}\). We infer from the unicity of \(C_n\) that the \(\mathbb{C}\)-automorphisms of \(C\) have \(n^{2g_c}\) prolongations to \(C_n\). Therefore, \(g_{C_n} - 1 = n^{2g_c}(g_C - 1)\). Consequently, \(C_n\) is still a Hurwitz curve (see \cite{Mc61}).

Now, let \((C, G)\) be a big action. Then \(C \to C/G\) is an étale cover of the affine line whose group is a \(p\)-group. From the Deuring-Shafarevich formula (see e.g. \cite{Bo00}), it follows that the Hasse-Witt invariant of \(C\) is zero. This means that there are no nontrivial connected étale Galois covers of \(C\) with group a \(p\)-group. Therefore, if we want to generalize the method mentioned above to produce Galois covers of \(C\) corresponding to big actions, it is necessary to introduce ramification. A means to do so is to consider ray class fields of function fields, as studied by K. Lauter \cite{Lau99} and R. Auer \cite{Au99}. Since the cover \(C \to C/G_2\) is an étale cover of the affine line \(\text{Spec} k[X]\) totally ramified at \(\infty\), we focus on the special case of ray class fields of the rational function field \(\mathbb{F}_q(X)\), where \(q = p^e\) (see \cite{Au99}, III.8). Such ray class fields allows us to produce families of big actions \((C, G)\) (where \(C\) is defined over \(k = \mathbb{F}_p^{(g)}\) with specific conditions imposed on ramification and endowed with an abelian \(G_2\) of exponent as large as we want.

Definition 6.1. \((\text{Au}99, \text{Part II})\) Let \(K\) be the rational function field: \(\mathbb{F}_q(X)\), with \(q = p^e\) and \(e \in \mathbb{N}^*\). Let \(S\) be the set of all finite rational places, namely \(\{(X - y), y \in \mathbb{F}_q\}\). Let \(m \geq 0\) be an integer. Fix \(K^{al}\) an algebraic closure of \(K\) in which all extensions of \(K\) are assumed to lie. We define \(K^{m}_S \subset K^{al}\) as the largest abelian extension \(L/K\) with conductor \(m\), such that every place in \(S\) splits completely in \(L\).

Remark 6.2. 1. We define the splitting set of any finite Galois extension \(L/K\), denoted by \(S(L)\), as the set consisting of the places of \(K\) that split completely in \(L\). If \(K^{m}_S/K\) is the extension defined in Definition 6.1, then \(S \subset S(K^{m}_S)\).

2. In what follows, we only consider finite Galois extensions \(L/K\) that are unramified outside \(X = \infty\) and (totally) ramified at \(X = \infty\). Therefore, the support of the conductor of \(L/K\) is reduced to the place \(\infty\). So, we systematically confuse the conductor \(m\) with its degree \(m\).

3. We could more generally define \(K^{m}_S\) for \(S\) a non-empty subset of the finite rational places, i.e. \(S := \{(X - y), y \in V \subset \mathbb{F}_q\}\). However, to get big actions, it is necessary to consider the case where \(V\) is a subgroup of \(\mathbb{F}_q\). In what follows, we focus on the case \(V = \mathbb{F}_q\), as announced in Definition 6.1.

Remark 6.3. We keep the notation of Definition 6.1.

1. The existence of the extension \(K^{m}_S/K\) is based on global class field theory (see \cite{Au99}, Part II).

2. \(K^{m}_S/K\) is a finite abelian extension whose constant field is \(\mathbb{F}_q\).
3. The reason for Lauter and Auer’s interest in such ray class fields is that they provide for examples of global function fields with many rational places, or what amounts to the same, of algebraic curves with many rational points. Indeed, let $C(m)/\mathbb{F}_q$ be the nonsingular projective curve with function field $K^m_S$. If we denote by $N_m := |C(m)(\mathbb{F}_q)|$ the number of $\mathbb{F}_q$-rational points on the curve $C(m)$, then: $N_m = 1 + q[K^m_S : K]$. The main difficulty lies in computing $[K^m_S : K]$. We first wonder when $K^m_S$ coincide with $K$. Here are partial answers.

4. Let $q = p^e$, with $e \in \mathbb{N}$. If $e$ is even, put $r := \sqrt{e}$ and if $e$ is odd, put $r := \sqrt[3]{e}$. Then, for all $i$ in $\{0, \cdots, r + 1\}$, $K^i_S = K = \mathbb{F}_q(X)$. (see [Au92], III, Lemma 8.7 and formula (13)). Note that the previous estimate $N_m = 1 + q[K^m_S : K]$, combined with the Hasse-Weil bound (see e.g. [St93] V.2.3), furnishes another proof of $K^m_S = K$ when $i < 1 + r$.

5. More generally, Lauter displays a method to compute the degree of the extension $K^m_S/K$ via a formula giving the order of its Galois group: $G_S(m)$ (see [Lau94], Thm. 1). Her proof consists in starting from the following presentation of $G_S(m)$:

$$G_S(m) \simeq \frac{1 + Z \mathbb{F}_q[[Z]]}{< 1 + Z^m \mathbb{F}_q[[Z]], 1 - yZ, y \in \mathbb{F}_q>}$$

where $Z = X^{-1}$, which indicates that $G_S(m)$ is an abelian finite $p$-group. Then, she transforms the multiplicative structure of the group into an additive group of generalized Witt vectors.

In particular, she deduces from this theorem the smallest conductor $m$ such that $G_S(m)$ has exponent strictly greater than $p$ (see next proposition).

**Proposition 6.4.** ([Lau94], Prop. 4) We keep the notation defined above. If $q = p^e$, the smallest conductor $m$ for which the group $G_S(m)$ is not of exponent $p$ is $m_2 := p^{\lceil e/2 \rceil} + 1 + p + 1$, where $\lceil e/2 \rceil$ denotes the upper integer part of $e/2$.

We now emphasize the link with big actions. Let $F$ be a function field with full constant field $\mathbb{F}_q$. Let $C/\mathbb{F}_q$ be the smooth projective curve whose function field is $F$ and $C^{alg} := C \times_{\mathbb{F}_q} k$ with $k = \mathbb{F}_p^{alg}$. If $G$ is a finite $p$-subgroup of $Aut_{\mathbb{F}_q} C$, then $G$ can be identified with a subgroup of $Aut_k C^{alg}$. In this case, $(C^{alg}, G)$ is a big action if and only if $g_{C^{alg}} = g_G > 0$ and $\frac{|C|}{g_G} > \frac{2p}{p+1}$. For convenience, in the sequel, we shall say that $(C, G)$ is a big action if $(C^{alg}, G)$ is a big action.

In what follows, we consider the curve $C(m)/\mathbb{F}_q$ whose function field is $K^m_S$ and, starting from this, we construct a $p$-group $G(m)$ acting on $C(m)$ by extending the translations $X \rightarrow X + y$, with $y \in \mathbb{F}_q$. In particular, we obtain an upper bound for the genus of $C(m)$, which allows us to circumvent the problem related to the computation of the degree $[K^m_S : K]$ when checking whether $(C(m), G(m))$ is a big action.

**Proposition 6.5.** We keep the notation defined above.

1. Let $C(m)/\mathbb{F}_q$ be the nonsingular projective curve with function field $K^m_S$. Then, the group of translations: $X \rightarrow X + y$, $y \in \mathbb{F}_q$, extends to a $p$-group of $\mathbb{F}_q$-automorphisms of $C(m)$, say $G(m)$, with the following exact sequence:

$$0 \rightarrow G_S(m) \rightarrow G(m) \rightarrow \mathbb{F}_q \rightarrow 0$$

2. Let $L$ be an intermediate field of $K^m_S/K$. Assume $L = (K^m_S)^H$, i.e. the extension $L/K$ is Galois with group: $G_S(m)/H$. For all $i \geq 0$, we define $L^i$ as the $i$-th upper ramification field of $L$, i.e. the subfield of $L$ fixed by the $i$-th upper ramification group of $G_S(m)/H$ at at $\infty$: $G_S^i(m)/H$, where $G_S^i(m)$ denotes the $i$-th upper ramification group of $G_S(m)$ at at $\infty$. Then,

$$\forall i \geq 0, \quad L^i = L \cap K_S^i$$

In particular, when $L = K^m_S$ and $i \leq m$, $L^i = K_S^i$, i.e. $G_S^i(m) = \text{Gal}(K^m_S/K_S^i)$.

3. Let $L$ be an intermediate field of $K^m_S/K$. Define $n := \min\{i \in \mathbb{N}, L \subset K^i_S\}$. Then, the genus of the extension $L/K$ is given by the formula:

$$g_L = 1 + [L : K] \left(-1 + \frac{n}{2}\right) - \frac{1}{2} \sum_{j=0}^{n-1} [L \cap K_S^j : K]$$

where the sum is empty for $n = 0$.

Note that if $n > 0$, then $g_L < [L : K] \left(-1 + \frac{n}{2}\right)$.  

15
Proof:

1. The set \( S \) is globally invariant under the translations: \( X \rightarrow X + y, \ y \in \mathbb{F}_q \). That is the same for \( \infty \), so the translations by \( \mathbb{F}_q \) do not change the conditions imposed on ramification. As a consequence, owing to the maximality and the unicity of \( K_S^\ast \), they can be extended to \( \mathbb{F}_q \)-automorphisms of \( K_S^\ast \). This proves the first assertion.

2. The second point directly derives from [Au99] (II, Thm. 5.8).

3. The genus formula is obtained by combining the preceding results, the Hurwitz genus formula and the Discriminant formula (see [Au99], I, 3.7). Now assume that \( n = 0 \). Then, \( L \subset K_S^0 = \mathbb{F}_q(X) \) and \( g_L = 0 \). Conversely, assume \( g_L = 0 \). If \( n \neq 0 \), Remark 6.3.4 implies that \( n \geq 2 \geq 3 \). Using the preceding formula and Remark 6.3.4, \( g_L = 0 \) reads:

\[
2 + (n - 2) |L : K| = \sum_{j=0}^{n-1} [K_j \cap L : K] = 2 + \sum_{j=2}^{n-1} [K_j \cap L : K] \leq 2 + (n - 2) |L : K|
\]

It follows that, for all \( j \) in \( \{2, \ldots, n-1\} \), \( K_j \cap L = L \). In particular, \( L \subset K_S^2 = K_S^0 \), hence a contradiction. Finally, since \( n > 0 \) implies \( n \geq 3 \) and since \( K = K_S^0 = K_S^1 \), one notices that

\[
g_L = [L : K] \left(-1 + \frac{n}{2}\right) - \frac{1}{2} \sum_{j=2}^{n-1} |L \cap K_j^2 : K| < [L : K] \left(-1 + \frac{n}{2}\right)
\]

4. Assume that \( m \geq r + 2 \). We gather from Remark 6.3.4 that \( n := \min\{i \in \mathbb{N}, K_S^m \subset K_S^i\} \geq r + 2 \geq 3 \). Then, it follows from the previous point that

\[
g_K^m < [K_S^m : K] \left(-1 + \frac{n}{2}\right) \leq [K_S^m : K] \left(-1 + \frac{m}{2}\right)
\]

As \( |G(m)| = q[K_S^m : K] \), we deduce the expected inequality. In particular, when \( \frac{q}{1 + \sqrt{q}} > \frac{2p}{p-1} \), the pair \((C(m), G(m))\) is a big action. It remains to show that, in this case, \( G_2(m) \) is equal to \( G_S(m) \). Lemma 2.4.2 first proves that \( G_2(m) \supset G_S(m) \). Let \( L := (K_S^m)^{G_2(m)} \) be the subfield of \( L \) fixed by \( G_2(m) \) and define \( n := \min\{i \in \mathbb{N}, L \subset K_S^i\} \). Assume \( G_S(m) \supset G_2(m) \). Then \( L \supset (K_S^m)^{G_S(m)} = K \). We infer from Remark 6.3.4 that \( n \geq r + 2 \), which proves, using the previous point, that \( g_L > 0 \). But, since \((C(m), G(m))\) is a big action, \( C/G_2(m) \simeq \mathbb{P}_1 \), so \( g_L = 0 \), hence a contradiction. We eventually explain the last statement. By Proposition 6.5.2, \( G_S^{m_2 - 1}(m_2) = \text{Gal}(K_S^{m_2}/K_S^{m_2 - 1}) \), which induces the following exact sequence:

\[
0 \rightarrow G_S^{m_2 - 1}(m_2) \rightarrow G_S(m_2) \rightarrow G_S(m_2 - 1) \rightarrow 0
\]

We infer from Proposition 6.4 that \( G_S(m_2 - 1) \) has exponent \( p \) whereas the exponent of \( G_S(m_2) \) is at least \( p^2 \). It follows that \( G_S^{m_2 - 1}(m_2) \) cannot be trivial. Since \( G_S^{m_2 - 1}(m_2) = \{0\} \) (use Proposition 6.5.2), we deduce from the elementary properties of the ramification groups that \( G_S^{m_2 - 1}(m_2) \) is \( p \)-elementary abelian. Therefore, \( G_S(m_2) \) has exponent smaller than \( p^2 \) and the claim follows. □

Remark 6.6. Let \( N_m \) be the number of \( \mathbb{F}_q \)-rational points on the curve \( C(m) \) as defined in Remark 6.3.3. Then, \( N_m = 1 + q |G_S(m)| = 1 + |G(m)| \). This highlights the equivalence of the two ratios: \( \frac{|G(m)|}{g_C(m)} \) and \( \frac{N_m}{g_C(m)} \). In particular, this equivalence emphasizes the link between the problem of big actions and the search of algebraic curves with many rational points.

As seen in Remark 6.3.4, \( K_i = K \) for all \( i \) in \( \{0, \ldots, r+1\} \), where \( r = \sqrt{q} \) or \( \sqrt{q^p} \) according to whether \( q \) is a square or not. The following extensions \( K_S^m \), for \( m \geq r + 2 \), are partially parametrized, at least for the first ones, in [Au99] (Prop. 8.9). In the table below, we exhibit a complete description of the extensions \( K_S^m \) for \( m \) varying from 0 to \( m_2 = p^r/p + 1 \), in the special case \( p = 5 \) and...
In this case,
\[
\frac{|G(m_2)|}{g_{K_{m_2}^S}} \approx 9,6929 \cdots \tag{16}
\]

**Comments on the construction of the table:** For all \( i \in \{0, \cdots, 14\} \), put \( L_i := K(W_0, \cdots, W_i) \).

1. We first prove that the splitting set of each extension \( K(W_i)/K \) (see Remark 6.2.1) contains \( S \). Indeed, fix \( y \in \mathbb{F}_q \) and call \( P_y \) the corresponding place in \( S : (X - y) \). We have to distinguish three cases. By [Sil93] (Prop. VI. 4.1), \( P_y \) completely splits in the extension \( K(W)/K \), where \( W' + W = X^{u(1+r)} \), with \( 1 \leq u \leq 4 \), if the polynomial \( T' + T - y^{u(1+r)} \) has a root in \( K \), which is true since \( y^{u(1+r)} = (F^a + I)(\frac{1}{2} y^{u(1+r)}) \). Likewise, \( P_y \) completely splits in the extension \( K(W)/K \), where \( W' - W = X^{v} (X^{v_q} - X^r) \), with \( 1 \leq v < u \leq 5 \), since \( y^{v_q} - y^v = 0 \). Finally, \( P_y \) completely splits in the extension \( K(W)/K \), where \( [W, W'] + [W, W] = [X^{1+r}, 0] \), since \( [y^{1+r}, 0] = (F^a + I)\left[\frac{1}{2} y^{1+r}, -\frac{2^{r-2} q^{2/(1+r)}}{2^{1/(1+r)}} p\right] \). To conclude, we remark that \( L_i = L_{i-1} K(W_i) \) for all \( i \in \{1, \cdots, 14\} \). Then, \( S(L_i) = S(L_{i-1}) \cap S(K(W_i)) \) (cf. [Au99], Cor. 3.2.b), which allows us to gather, by induction on \( i \), that the splitting set of each \( L_i \) contains \( S \).

2. We now compute the conductor \( m(K(W_i)) \) of each extension \( K(W_i)/K \). As above, we have to distinguish three kinds of extensions. First, the extension \( K(W)/K \), where \( W' + W = X^{u(1+r)} \), with \( 1 \leq u \leq 4 \), has conductor \( u' + u + 1 \) (see [Au99], Prop. 8.9.a). Besides, the extension \( K(W)/K \), where \( W' - W = X^{v} (X^{v_q} - X^r) \), with \( 1 \leq v < u \leq 5 \), has conductor \( u' + v + 1 \) (see [Au99], Prop. 8.9.b). Finally, the conductor of the extension \( K(W)/K \), where \( [W, W'] + [W, W] = [X^{1+r}, 0] \) is given by the formula: \( 1 + \max\{p(1+r), 0\} + 1 + p + p^{r+1} = m_2 \) (see [Ca99], Thm. 1.1). As a conclusion, since \( m(L_i) = \max\{m(L_{i-1}), m(K(W_i))\} \) (cf. [Au99], Cor. 3.2.b), an induction on \( i \) allows us to obtain the expected conductor for \( L_i \).

3. We gather from the two first points the inclusions: \( K(W_0) \subset K_{m_2}^S \), \( K(W_0, W_1) \subset K_{m_2}^S \), \( K(W_0, \cdots, W_4) \subset K_{m_2}^S \). Equally is eventually obtained by calculating the degree of each extension \( K_{m_2}^S/K \) via [Lau99] (Thm. 1) or [Au99] (p. 54-55, formula (13)).

We deduce from what precedes an example of big actions with \( G_2 \) abelian of exponent \( p^2 \), with a small \( p \)-rank. More precisely, we construct a subextension of \( K_{m_2}^S/K \) with the commutative diagram:

\[
\begin{array}{cccccc}
0 & \longrightarrow & G_S(m_2) & \longrightarrow & G(m_2) & \longrightarrow & \mathbb{F}_q & \longrightarrow & 0 \\
\phi & \downarrow & \downarrow & & \downarrow & & \downarrow & & 0 \\
0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & \mathbb{F}_q & \longrightarrow & 0
\end{array}
\]

such that the pair \((C(m_2)/\ker(\phi), G)\) is a big action where \( G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \) with \( t = O(\log_p g) \), \( g \) being the genus of the curve \( C(m_2)/\ker(\phi) \). Contrary to the previous case where the
Proposition 6.7. We keep the notation defined above. In particular, \( K = \mathbb{F}_q(X) \) with \( q = p^e \).
Assume \( e = 2s \), with \( s \geq 1 \), and put \( r := p^s \). We define
\[
\phi_0(X) := X^{1+r} \quad \text{with} \quad a \neq 0, \quad a \in \Gamma := \{ \gamma \in \mathbb{F}_q, \gamma^r + \gamma = 0 \}
\]
and
\[
\forall i \in \{1, \ldots, p-1\}, \quad f_i(X) = X^{i+r} (X^q - X) = X^{ip^{s-1}} (X^q - X)
\]
Let \( L := K(W_i) \) be the extension of \( K \) parametrized by the Artin-Schreier-(Witt) equations:
\[
W_0^p - W_0 = f_0(X) \quad \forall i \in \{1, \ldots, p-1\}, \quad W_i^q - W_i = f_i(X) \quad \text{and} \quad [W_0, W_p]^p - [W_0, W_p] = [f_0(X), 0]
\]
For all \( i \) in \( \{0, 1, \ldots, p-1\} \), put \( L_i := K(W_0, \ldots, W_i) \).

1. \( L \) is an abelian extension of \( K \) such that every place in \( S \) completely splits in \( L \). Moreover,
\[
L_0 \subset K^{r+2}_S, \quad \forall i \in \{1, \ldots, p-1\}, \quad L_i \subset K^{r+i+1}_S + L \subset K^{m_2}_S
\]
where \( m_2 = p^{s+1} + p + 1 \) is the integer defined in Proposition 6.4. (see table below).

2. The extension \( L/K \) has degree \([L : K] = p^{2+(p-1)e} \). Let \( G_L \) be its Galois group. Then
\[
G_L \simeq \mathbb{Z}/p^2 \mathbb{Z} \times (\mathbb{Z}/p \mathbb{Z})^t \quad \text{with} \quad t = (p-1)e
\]

3. The extension \( L/K \) is stable under the translations: \( X \mapsto X + y \), with \( y \in \mathbb{F}_q \). Therefore, the translations by \( \mathbb{F}_q \) extend to form a \( p \)-group of \( \mathbb{F}_q \)-automorphisms of \( L \), say \( G \), with the following exact sequence:
\[
0 \longrightarrow G_L \longrightarrow G \longrightarrow \mathbb{F}_q \longrightarrow 0
\]

4. Let \( g_L \) be the genus of the extension \( L/K \). Then,
\[
g_L = \frac{1}{2} \left( p^{2+2s(p-1)} (p^{s+1} + p - 1) - p^s (p^2 - p + 1) - p^{2+s+1} \left( \sum_{i=0}^{p-2} q^i \right) \right)
\]
In particular, when \( e \) grows large, \( g_L \sim \frac{1}{2} p^{2(p-1) \frac{e}{2} + 3} \) and \( t = O(\log_p g_L) \).

Note that, for \( p = 5 \) and \( e = 4 \), one gets \( g_L \approx 9.7049 \cdots \), which is slightly bigger than the quotient obtained for the whole extension \( K^{m_2}_S \) (see (16)).

Proof:

1. Fix \( y \) in \( \mathbb{F}_q \) and call \( P_y := (X - y) \), the corresponding place in \( S \). As \( f_i(y) = 0 \) for all \( i \) in \( \{1, \ldots, p-1\} \), the place \( P_y \) completely splits in each extension \( K(W_i) \) with \( W^q_i - W_i = f_i(X) \). Therefore, to prove that \( P_y \) completely splits in \( L \), it is sufficient to show that \( [f_0(y), 0] \) is in \( \mathfrak{o}(W_2(\mathbb{F}_q)) \). By [Bo83] (Chap. IX, ex. 18), this is equivalent to show that \( Tr([f_0(y), 0]) = 0 \), where \( Tr \) means the trace map from \( W_2(\mathbb{F}_q) \) to \( W_2(\mathbb{F}_p) \). We first notice that, when \( y \) is in \( \mathbb{F}_q \), \( \gamma := f_0(y) = a y^{1+r} \) lies in \( \Gamma \). It follows that:
\[
Tr([\gamma, 0]) = \sum_{i=0}^{2s-1} F^i [\gamma, 0] = \sum_{i=0}^{s-1} [\gamma p^i, 0] + \sum_{i=0}^{s-1} [\gamma^r p^i, 0] = \sum_{i=0}^{s-1} [\gamma p^i, 0] + \sum_{i=0}^{s-1} [-\gamma^r p^i, 0]
\]
For \( p > 2 \), \( -\gamma^r p^i, 0 \) and \( Tr([\gamma, 0]) = 0 \). For \( p = 2 \), since \( p[\gamma, 0] = [0, \gamma^p] \), one gets:
\[
Tr([\gamma, 0]) = [0, \gamma^p + \gamma p^2 + \cdots + \gamma^{p-1}] = [0, (\gamma + \gamma p + \cdots + \gamma^{p-1})p] = [0, Tr_{\mathbb{F}_p}(\gamma)^p]
\]
As \( \Gamma \) coincides with \( \{\beta^p - \beta, \beta \in \mathbb{F}_q\} \) (see e.g. [Au99] p. 58), \( Tr_{\mathbb{F}_p}(\gamma) = 0 \) and \( Tr([\gamma, 0]) = 0 \).
To establish the expected inclusions, it remains to compute the conductor of each extension \( L_i \).
First of all, [Au99] (I, ex. 3.3) together with [So83] (Prop III.7.10) shows that the conductor of \( L_0 \) is \( r + 2 \). Thus, \( L_0 \subset K^{r+2}_S \). Moreover, as \( f_i(X) = X^{i+p^{s+1}} - X^{1+ip^{s-1}} \mod \mathfrak{o}(\mathbb{F}_q[X]) \), we
The equations, conductor and degree of each extension $L_i$ are finally gathered in the table below.

| $L_i$ | conductor $m$ | $[L_i : K]$ | New equations |
|-------|--------------|--------------|---------------|
| $K$   | $0 \leq m \leq r + 1 = p^s + 1$ | $1$          |               |
| $L_0$ | $r + 2 \leq m \leq p^{s+1} + 1 = m_2 - p$ | $p$          | $W_0' - W_0 = f_0(X)$ |
| $L_1$ | $m = p^{s+1} + 2 = m_2 - (p - 1)$ | $p^{s+e}$    | $W_1' - W_1 = f_1(X)$ |
| $L_2$ | $m = p^{s+1} + 3 = m_2 - (p - 2)$ | $p^{s+e}$    | $W_2' - W_2 = f_2(X)$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $L_i$ | $m = p^{s+1} + i + 1 = m_2 - (p - i)$ | $p^{s+e}$    | $W_i' - W_i = f_i(X)$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $L_{p-1}$ | $m = p^{s+1} + p = m_2 - 1$ | $p^{s+1}(p-1)e$ | $W_{p-1}' - W_{p-1} = f_{p-1}(X)$ |
| $L$   | $m = p^{s+1} + p + 1 = m_2$ | $p^{2s+2(p-1)e}$ | $[W_0, W_p]^p - [W_0, W_p] = [f_0(X), 0]$ |

2. See table above.

3. Fix $y \in \mathbb{F}_q$. Consider $\sigma$ in $G(m_2)$ (defined as in Proposition 6.5) such that $\sigma(X) = X + y$.

(a) We first prove that $\sigma(W_0) \in L_0$. Indeed, as $y \in \mathbb{F}_q$ and $a \in \Gamma = \{ \gamma \in \mathbb{F}_q, \gamma^r + \gamma = 0 \}$,

$$
\psi(\sigma(W_0) - W_0) = \sigma(\psi(W_0)) - \psi(W_0) = f_0(X + y) - f_0(X) = a y X^r + a y^r X + f_0(y) = -a y^r X^r + a y^r X + f_0(y) = \psi(P_y(X)) + f_0(y)
$$

where $P_y(X) := (I + F + F^2 + \cdots + F^{r-1})(-a y^r X)$. Since $f_0(y) \in \psi(\mathbb{F}_q)$ (see proof of the first point), it follows that $\psi(P_y(X)) + f_0(y)$ belongs to $\psi(\mathbb{F}_q[X])$. Therefore, $\sigma(W_0) \in L_0 = \mathbb{F}_q(X, W_0)$.

(b) We now prove that, for all $i \in \{1, \cdots, p - 1\}$, $\sigma(W_i) \in L_i$. Indeed,

$$
(F^e - id) (\sigma(W_i) - W_i) = \sigma(W_i^q - W_i) - (W_i^q - W_i) = f_i(X + y) - f_i(X) = (X + y)^i X^{s-i} - X^{s-i} X^r
$$

$$
= (X^r + y^r X^r) \cdot (X - X^r) = (X^r + y^r X^r - X^r) = \sum_{j=1}^{s-i} (\frac{j}{i}) y^{-j} X^{s-i} \cdot f_j(X) \mod (F^e - id)(\mathbb{F}_q[X]) = (F^e - id)(\sum_{j=1}^{s-i} (\frac{j}{i}) y^{-j} X^{s-i} W_j) \mod (F^e - id)(\mathbb{F}_q[X])
$$

where the sum is empty for $i = 1$. It follows that $\sigma(W_i) \in L_i = \mathbb{F}_q(X, W_0, W_1, \cdots, W_i)$.

(c) To conclude, we show that $\sigma(W_p) \in L$, which requires the use of Remark 6.3.4. Indeed, compute:

$$
\Delta := \psi(\sigma([W_0, W_p] - [W_0, W_p])) = \psi([[W_0, W_p]] - \psi([W_0, W_p])) = [f_0(X + y), 0] - [f_0(X), 0]
$$

As shown in the proof of the first point, $[f_0(y), 0]$ lies in $\psi(\mathbb{F}_q)$. Then,

$$
\Delta = [f_0(X + y), 0] - [f_0(X), 0] - [f_0(y), 0] - [P_y(X), 0] + [P_y(X), 0]^p \mod \psi(\mathbb{F}_q[X])
$$

with $y$ in $\mathbb{F}_q$ and $P_y$ defined as above. Let $W(\mathbb{F}_q)$ be the ring of Witt vectors with coefficients in $\mathbb{F}_q$. Then, for any $y \in \mathbb{F}_q$, we denote by $\hat{y}$ the Witt vector $\hat{y} := (y, 0, 0, \cdots) \in \mathbb{F}_q$. Therefore,

$$
\Delta = \psi([f_0(X + y), 0] - [f_0(X), 0] - [f_0(y), 0] - [P_y(X), 0] + [P_y(X), 0]^p \mod \psi(\mathbb{F}_q[X]))
$$

for $y$ in $\mathbb{F}_q$.
\( W(k) \). For any \( P(X) := \sum_{i=0}^s a_i X^i \in \mathbb{F}_q[X] \), we denote by \( P(X) := \sum_{i=0}^s a_i X^i \in W(\mathbb{F}_q)[X] \). The addition in the ring of Witt vectors yields:
\[
\Delta = [0, A] \mod \varphi(W_2(\mathbb{F}_q)[X])
\]
where \( A \) is the reduction modulo \( p W_2(\mathbb{F}_q)[X] \) of:
\[
\frac{1}{p} \left( \tilde{\delta}_0(X+y)^p - \tilde{\delta}_0(X)^p - \tilde{\delta}_0(y)^p + \tilde{\delta}_y(X)^p - \tilde{\delta}_y(X)^p \right) - \left( \tilde{\delta}_0(X+y)^p - \tilde{\delta}_0(X)^p - \tilde{\delta}_0(y)^p + \tilde{\delta}_y(X)^p - \tilde{\delta}_y(X)^p \right)
\]
Since \( \tilde{\delta}_0(X+y) - \tilde{\delta}_0(X) - \tilde{\delta}_0(y) + \tilde{\delta}_y(X) - \tilde{\delta}_y(X) = 0 \mod p W(\mathbb{F}_q)[X] \), \( A \) becomes:
\[
A = \frac{1}{p} \left( \tilde{\delta}_0(X+y)^p - \tilde{\delta}_0(X)^p - \tilde{\delta}_0(y)^p + \tilde{\delta}_y(X)^p - \tilde{\delta}_y(X)^p \right) \mod p W(\mathbb{F}_q)[X]
\]
We observe that:
\[
\tilde{\delta}_0(X+y)^p = \tilde{\alpha}^p (X+y)^p (X+y)^{p-1} \mod p^2 W(\mathbb{F}_q)[X]
\]
\[
= \tilde{\alpha}^p (X+y)^p (X+p^p) \mod p^2 W(\mathbb{F}_q)[X]
\]
\[
= \tilde{\alpha}^p \sum_{i=0}^{p} \sum_{j=0}^{p} \left( \begin{array}{c} p \\ i \end{array} \right) \left( \begin{array}{c} p \\ j \end{array} \right) X^{j+ip^p} y^{p-j+p^p (p-i)} \mod p^2 W(\mathbb{F}_q)[X]
\]
As \( \left( \begin{array}{c} p \\ i \end{array} \right) \left( \begin{array}{c} p \\ j \end{array} \right) = 0 \mod p^2 \) when \( 0 < i < p \) and \( 0 < j < p \), one obtains:
\[
\tilde{\delta}_0(X+y)^p - \tilde{\delta}_0(X)^p - \tilde{\delta}_0(y)^p = \tilde{\alpha}^p \sum_{(i,j) \in I} \left( \begin{array}{c} p \\ i \end{array} \right) \left( \begin{array}{c} p \\ j \end{array} \right) X^{j+ip^p} y^{p-j+p^p (p-i)} \mod p^2 W(\mathbb{F}_q)[X]
\]
with
\[
I := \{(i,j) \in \mathbb{N}^2, 0 \leq i \leq p, 0 \leq j \leq p, ij = 0 \mod p, (i,j) \neq (0,0), (i,j) \neq (p,p)\}
\]
Besides,
\[
\tilde{\delta}_y(X)^p - \tilde{\delta}_y(X)^p = \left( \sum_{i=0}^{p-1} (\tilde{\alpha} \tilde{y}^r X)^p \right) - \left( \sum_{i=0}^{p-1} (\tilde{\alpha} \tilde{y}^r X)^p \right) \mod p^2 W(\mathbb{F}_q)[X]
\]
\[
= \left( \sum_{i=0}^{p-1} (\tilde{\alpha} \tilde{y}^r X)^p \right) - \left( \sum_{i=0}^{p-1} (\tilde{\alpha} \tilde{y}^r X)^p \right) \mod p^2 W(\mathbb{F}_q)[X]
\]
\[
= -\tilde{\alpha}^p \tilde{y}^r X^p + \tilde{\alpha}^p \tilde{y}^r X^{p+p} + p \tilde{T}_y(X) \mod p^2 W(\mathbb{F}_q)[X]
\]
with \( \tilde{T}_y(X) \in W(\mathbb{F}_q)[X] \). As \( y \in \mathbb{F}_q \) and \( a \in \Gamma \), we get:
\[
\tilde{T}_y(X)^p - \tilde{T}_y(X)^p = -\tilde{\alpha}^p \tilde{y}^r X^p - \tilde{\alpha}^p \tilde{y}^r X^{p+p} + p \tilde{T}_y(X) \mod p^2 W(\mathbb{F}_q)[X]
\]
As a consequence,
\[
A = \tilde{\alpha}^p \sum_{(i,j) \in I_1} \frac{1}{p} \left( \begin{array}{c} p \\ i \end{array} \right) \left( \begin{array}{c} p \\ j \end{array} \right) X^{j+ip^p} y^{p-j+p^p (p-i)} + \tilde{T}_y(X) \mod p \varphi(\mathbb{F}_q[X])
\]
with
\[
I_1 := \{(i,j) \in I, (i,j) \neq (0,0), (i,j) \neq (0,p)\}
\]
So, \( A \) reads:
\[
A = \tilde{\alpha}^p \sum_{(i,j) \in I_1} \frac{1}{p} \left( \begin{array}{c} p \\ i \end{array} \right) \left( \begin{array}{c} p \\ j \end{array} \right) X^{j+ip^p} y^{p-j+p^p (p-i)} + \tilde{T}_y(X) \mod \varphi(\mathbb{F}_q[X])
\]
with \( \tilde{T}_y \in \mathbb{F}_q[X] \). We first consider the sum. Since, for \( i = 0, i = p \) and \( j = p \), one gets monomials whose degree (after eventual reduction mod \( \varphi(\mathbb{F}_q[X]) \)) is strictly lower than \( 1 + p^s \), one can write:
\[
A = \tilde{\alpha}^p \sum_{j=1}^{p-1} \frac{1}{p} \left( \begin{array}{c} p \\ j \end{array} \right) X^{j+ip^p} y^{p-j} + \tilde{R}_y(X) + \tilde{T}_y(X) \mod \varphi(\mathbb{F}_q[X])
\]
Let $n$ be a positive integer. We keep the notation defined above. In particular, Proposition 6.8. If $G$ is a finite group, the ramification group $G_{n}$ is defined as the least subgroup of $G$ with\property{p}$ and $G_{n+1}$ is defined as the least subgroup of $G_{n}$ with\property{p}$.

The preceding proposition can be generalized to construct a big action endowed with a second ramification group $G_{n}$ of exponent at least $p$. If $G$ is a finite group, the ramification group $G_{n}$ is defined as the least subgroup of $G$ with\property{p}$.

The preceding proposition can be generalized to construct a big action endowed with a second ramification group $G_{n}$ of exponent at least $p$. If $G$ is a finite group, the ramification group $G_{n}$ is defined as the least subgroup of $G$ with\property{p}$.

**Proposition 6.8.** We keep the notation defined above. In particular, $G = \mathbb{Z}/p\mathbb{Z}$, with $e = 2s$ and $s \geq 1$. Let $n \geq 2$. Put $m_{n} := 1 + p^{n-1}(1 + p)$. If $m_{n} > \frac{2n}{p-1}$, the pair $(G(m_{n}), G(m_{n}))$, as defined in Proposition 6.5, is a big action with a second ramification group $G_{n}(m_{n})$ of exponent at least $p^{n}$. This completes the proof of Proposition 6.8.
Proof: Proposition 6.5.4 first ensures that $\langle C(m_n), G(m_n) \rangle$ is a big action. Consider the $p^n$-cyclic extension $K(W_1, \ldots, W_n) / K$ parametrized as follows, with Witt vectors of length $n$:

$$[W_1,\ldots,W_n]^p - [W_1,\ldots,W_n] = [f_0(X),0,\ldots,0]$$

where $f_0(X) = a X^{1+r}$ is defined as in Proposition 6.7, i.e. $r = p^a$, $a^r + a = 0$, $a \neq 0$. The same proof as in Proposition 6.7.1 shows that all places of $S$ completely split in $K(W_1,\ldots,W_n)$. Moreover, by [Ga99] (Thm. 1.1) the conductor of the extension $K(W_1,\ldots,W_n)$ is $1 + \max\{p^{n-1}(1+p^a),0\} = m_n$. It follows that $K(W_1,\ldots,W_n)$ is included in $K_S^{m_n}$. Therefore, $G_S(m_n)$ has a quotient of exponent $p^n$ and the claim follows. \(\square\)

The next proposition is an analogue of Proposition 6.7 in the case where $e$ is odd. We do not mention the proof which is mainly similar to the proof of Proposition 6.7.

Proposition 6.9. We keep the notation defined above. In particular, $K = \mathbb{F}_q(X)$ with $q = p^e$. Assume $e = 2s - 1$, with $s \geq 2$, and put $r := \sqrt[2s]{p} \equiv p$. We define

$$\forall i \in \{1,\ldots,p-1\}, f_i(X) = X^{ip^s/p} (X^q - X) = X^{ip^{s+1}} (X^q - X)$$

$$\forall i \in \{1,\ldots,p-1\}, g_i(X) = X^{ip^s/p^2} (X^q - X) = X^{ip^{s+1}} (X^q - X)$$

Let $L := K(W_i, V_j)_{1 \leq i \leq p, 1 \leq j \leq p-1}$ be the extension of $K$ parametrized by the Artin-Schreier-(Witt) equations:

$$\forall i \in \{1,\ldots,p-1\}, W^q_i - W_i = f_i(X) \quad \text{and} \quad \forall j \in \{1,\ldots,p-1\}, V^q_j - V_j = g_j(X)$$

$$[W_1, W_p]^p - [W_1, W_p] = [X^{1+p^s}, 0] - [X^{1+p^{s-1}}, 0]$$

For all $i$ and $j$ in $\{1,\ldots,p-1\}$, put $L_{i,0} := K(W_k)_{1 \leq k \leq i}$ and $L_{p-1,j} := K(W_i, V_k)_{1 \leq p-1,1 \leq k \leq j}$.  

1. $L$ is an abelian extension of $K$ such that every place in $S$ completely splits in $L$. Then,

$$\forall i, j \in \{1,\ldots,p-1\}, L_{i,0} \subset K_S^{p^s+j+1} \quad L_{p-1,j} \subset K_S^{p^{s+1}+j+1} \quad \text{and} \quad L \subset K_S^{m_2}$$

where $m_2 = p^{s+1} + p + 1$ is the integer defined in Proposition 6.4. (see table below.)

2. The extension $L/K$ has degree $[L : K] = p^{2(p-1)e+1}$. Let $G_L$ be its Galois group. Then

$$G_L \simeq \mathbb{Z}/p^2 \mathbb{Z} \times (\mathbb{Z}/p^2 \mathbb{Z})^t$$

with $t = 2(p-1)e - 1$

3. The extension $L/K$ is stable under the translations: $X \rightarrow X + y$, with $y \in \mathbb{F}_q$. Therefore, the translations by $\mathbb{F}_q$ extend to form a $p$-group of $\mathbb{F}_q$-automorphisms of $L$, say $G$, with the following exact sequence:

$$0 \rightarrow G_L \rightarrow G \rightarrow \mathbb{F}_q \rightarrow 0$$

4. Let $g_L$ be the genus of the extension $L/K$. Then,

$$g_L = \frac{1}{2} \left( p^{1+2(p-1)e} (p^{s+1} + p - 1) - p^{(p-1)e} (p^{s+1} - p^s - p + 1) - p^s + p^e \left( \sum_{i=0}^{2p-3} q^i \right) \right)$$

In particular, when $e$ grows large, $g_L \sim \frac{1}{2} p^{2+4s(p-1)+s}$ and $t = O(\log p \cdot g_L)$.

We gather in the table below the conductors, degrees and equations of each extension.

| $L_{i,j}$ | conductor $m$ | $[L_{i,j} : K]$ | New equations |
|----------|----------------|-----------------|---------------|
| $K$      | $0 \leq m \leq r + 1 = p^s + 1$ | 1               |               |
| $L_{1,0}$| $m = r + 2 = p^s + 2$ | $p^e$           | $W^q_i - W_i = f_i(X)$ |
|         | $\ldots$       | $\ldots$       | $\ldots$      |
| $L_{i,0}$| $m = p^s + i + 1$ | $p^{e_i}$       | $W^q_i - W_i = f_i(X)$ |
| $\ldots$| $\ldots$       | $\ldots$       | $\ldots$      |
| $L_{p-1,0}$| $p^s + p \leq m \leq p^{s+1} + 1$ | $p^{(p-1)e}$ | $W^q_{p-1} - W_{p-1} = f_{p-1}(X)$ |
| $L_{p-1,1}$| $m = p^{s+1} + 2 = m_2 - (p-1)$ | $p^{e_{p-1}}$ | $V^q_i - V_i = g_i(X)$ |
| $\ldots$| $\ldots$       | $\ldots$       | $\ldots$      |
| $L_{p-1,j}$| $m = p^{s+1} + j + 1 = m_2 - (p - j)$ | $p^{(p+j-1)e}$ | $V^q_i - V_i = g_i(X)$ |
| $\ldots$| $\ldots$       | $\ldots$       | $\ldots$      |
| $L_{p-1,p-1}$| $m = p^{s+1} + p = m_2 - 1$ | $p^{2(p-1)e}$ | $V^q_{p-1} - V_{p-1} = g_{p-1}(X)$ |
| $L$      | $m = p^{s+1} + p + 1 = m_2$ | $p^{1+2(p-1)e}$ | $[W_1, W_p]^p - [W_1, W_p] =$ |

$[X^{1+p^s}, 0] - [X^{1+p^{s-1}}, 0]$ |
Let \((C, G)\) be a big action. We recall that there exists a point \(\infty \in C\) such that \(G\) is equal to \(G_1(\infty)\) the wild inertia subgroup of \(G\) at \(\infty\), which means that the cover \(\pi : C \to C/G\) is totally ramified at \(\infty\). Moreover, the quotient curve \(C/G\) is isomorphic to the projective line: \(\mathbb{P}^1_k\) and \(\pi\) is étale above the affine line: \(\mathbb{A}^1_k = \mathbb{P}^1_k - \{\infty\} = \text{Spec } k[T]\). The inclusion \(k[T] \subset k((T^{-1}))\) induces a Galois extension \(k(C) \otimes_{k(T)} k((T^{-1})) = k((Z))\) over \(k(T^{-1})\) with group equal to \(G\) and ramification groups in lower notation equal to \(G_i := G_i(\infty)\). Then, the genus of \(C\) is given by the formula:

\[
g = \frac{1}{2} \left( \sum_{i \geq 2} (|G_i| - 1) \right) > 0\text{ (see (2)). It follows that:}
\]

\[
\frac{|G|}{\sum_{i \geq 2} (|G_i| - 1)} = \frac{|G|}{2g} > \frac{p}{p-1}.
\]

This leads to the definition below.

**Definition 7.1.** We call "local big action" any pair \((k([Z]), G)\) where \(G\) is a finite \(p\)-subgroup of \(\text{Aut}_k(k([Z]))\) whose ramification groups in lower notation at \(\infty\) satisfy the two inequalities:

\[
g(G) := \frac{1}{2} \left( \sum_{i \geq 2} (|G_i| - 1) \right) > 0 \quad \text{and} \quad \frac{|G|}{g(G)} > \frac{2p}{p-1}.
\]

It follows from the Katz-Gabber Theorem (see [Ka86] Thm. 1.4.1 or [G100] cor. 1.9) that big actions \((C, G)\) and local big actions \((k([Z]), G)\) are in 1-to-1 correspondence via the following functor induced by the inclusion \(k[T] \subset k((T^{-1}))\):

\[
\left\{ \begin{array}{c}
\text{finite étale Galois covers of } \text{Spec } k[T]
\text{with Galois group a p-group}
\end{array} \right\} \longrightarrow \left\{ \begin{array}{c}
\text{finite étale Galois covers of } \text{Spec } k((T^{-1}))
\text{with Galois group a p-group}
\end{array} \right\}
\]

Therefore, we can infer from the global point of view properties related to local extensions that would be difficult to prove directly. For instance, if \((k([Z]), G)\) is a local big action, we can deduce that \(G_2\) is strictly included in \(G_1\). Furthermore, we obtain:

\[
\frac{|G|}{g(G)^2} \leq \frac{4p}{(p-1)^2}.
\]

**References**

[Au99] R. Auer, *Ray Class Fields of Global Function Fields with Many Rational Places*. Dissertation at the University of Oldenburg, www.bis.uni-oldenburg.de/dissertation/ediss.html, (1999).

[Au00] R. Auer, *Ray class fields of global function fields with many rational places*. Acta Arith. 95 (2000), no. 2, 97-122.

[Bo83] N. Bourbaki, *Algèbre commutative*. Élémens de Mathématiques, Masson, Paris, (1983)

[Bou00] I. Bouw, *The p-rank of curves and covers of curves*. Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), 267–277, Progr. Math., 187, Birkhäuser, Basel, (2000).

[Co90] M. Conder, *Hurwitz groups: a brief survey*. Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 359-370.

[El97] N. Elkies *Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups* in Applications of curves over finite fields, (Seattle, WA, 1997), Contemporary Mathematics, vol 245, American Mathematical Society, (Providence, RI, 1999)

[El99] N. Elkies, *The Klein quartic in number theory. The eightfold way*, 51-101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, (1999).

[Ga99] M. Garuti, *Linear systems attached to cyclic inertia*. Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 377-386, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.
P. Gille, Le groupe fondamental sauvage d’une courbe affine en caractéristique $p > 0$. Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), 217–231, Progr. Math., 187, Birkhäuser, Basel, 2000.

M. Giulietti, G. Korchmáros, On large automorphism groups of algebraic curves in positive characteristic arXiv:0706.2320, 15 Jun 2007

D. Goss, Basic structures of function field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol.35, (Springer, Berlin, 1996)

B. Huppert, Endliche Gruppen. I., Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York (1967)

N. Katz, Local-to-global extensions of representations of fundamental groups. Ann. Inst. Fourier (Grenoble) 36 (1986), no. 4, 69-106.

K. Lauter, A Formula for Constructing Curves over Finite Fields with Many Rational Points. Journal of Number Theory 74 (1999), no. 1, 56-72.

C. Lehr, M. Matignon, Automorphism groups for $p$-cyclic covers of the affine line. Compositio Math. 141 (2005).

M. Marshall, Ramification groups of abelian local field extensions. Canad. J. Math. 23 (1971) 271–281

A.M. Macbeath, On a theorem of Hurwitz. Proc. Glasgow Math. Assoc. 5 90-96 (1961).

A.M. Macbeath, On a curve of genus 7. Proc. London Math. Soc. (3) 15 527-542 (1965).

J. S. Milne, Étale cohomology, Princeton Mathematical Series, 33, Princeton University Press, (Princeton, N.J., 1980)

S. Nakajima, $p$-ranks and automorphism groups of algebraic curves. Trans. Amer. Math. Soc. 303 (1987).

M. Rocher, Large $p$-groups actions with a $p$-elementary abelian second ramification group. (2008), available on arXiv.

M. Rocher, Large $p$-groups actions with $\frac{|G|}{g} \geq \frac{1}{p^2-1}p$ (2008). In preparation.

H. L. Schmid, Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik, J.Reine Angew. Math. 179, p5-15 (1938)

J-P. Serre, Corps locaux. Deuxième édition. Hermann, Paris, (1968).

J. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

B. Singh, On the group of automorphisms of function field of genus at least two J. Pure Appl. Algebra 4 (1974), 205-229.

H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II, Arch. Math. (Basel) 24 (1973).

H. Stichtenoth, Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin, (1993).

M. Suzuki, Group Theory I. Grundlehren der Mathematischen Wissenschaften, 247. (Springer-Verlag, Berlin-New York, 1982.)

M. Suzuki, Group theory. II. Grundlehren der Mathematischen Wissenschaften, 248. Springer-Verlag, New York, (1986)
Michel MATIGNON
Institut de Mathématiques de Bordeaux, Université de Bordeaux I, 351 cours de la Libération,
33405 Talence Cedex, France
e-mail : Michel.Matignon@math.u-bordeaux1.fr

Magali ROCHER
Institut de Mathématiques de Bordeaux, Université de Bordeaux I, 351 cours de la Libération,
33405 Talence Cedex, France
e-mail : Magali.Rocher@math.u-bordeaux1.fr