Algebra & Number Theory

Volume 2

2008

No. 8

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

Michel Matignon and Magali Rocher

mathematical sciences publishers

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

Michel Matignon and Magali Rocher

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 our study of *big actions*, that is, pairs (C, G) where G is a p-subgroup of the k-automorphism group of C such that $|G|/g > 2\,p/(p-1)$. If G_2 denotes the second ramification group of G at the unique ramification point of the cover $C \to C/G$, 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 continued by Lauter and by Auer. In particular, we obtain explicit examples of big actions with G_2 abelian of large exponent.

1. Introduction

This is the first of a set of three papers (together with [Rocher 2008a; 2008b]) whose main object is to study G-actions on connected nonsingular projective curves of genus $g \geq 2$ defined over an algebraically closed field of characteristic $p > 0$, when G is a p-group such that $|G| > 2\,g\,p/(p-1)$. One of our aims is to display some universal families and discuss the corresponding deformation space.

For more than a century, the study of finite groups G acting faithfully on smooth complete curves defined over an algebraically closed field k of characteristic $p \geq 0$ has produced a vast literature. Already back in the nineteenth century progress was made in the case of characteristic zero, with the works of Schwartz, Klein, Hurwitz, Wiman and others. The full automorphism group of a compact Riemann surface of genus $g \geq 2$ was proved by Hurwitz [1892] to be finite and of order at most $84\,(g-1)$.

MSC2000: primary 14H37; secondary 11R37, 11G20, 14H10.

Keywords: automorphisms, curves, p-groups, ray class fields, Artin–Schreier–Witt theory.

Work supported in part by the European Community's Sixth Framework Programme under Contract MRTN-CT-2006-035495.

An open question concerns the classification of full automorphism groups of compact Riemann surfaces C of fixed genus $g \geq 2$. This classification has been partially achieved for large automorphism groups G, "large" meaning that the order of G is greater than $4\,(g-1)$ [Kulkarni 1997]. This lower bound imposes strict restrictions on the genus g_0 of the quotient curve C/G, namely $g_0 = 0$, on the number r of points of C/G ramified in C, namely $r \in \{3, 4\}$, and on the corresponding ramification indices; see [Kulkarni 1997; Breuer 2000, Lemma 3.18]. Following this work, Magaard et al. [2002] exhibited the list of large groups $\operatorname{Aut}(C)$ of compact Riemann surfaces of genus g up to $g = 10$, determining in each case the dimension and number of components of the corresponding loci in the moduli space of genus g curves.

General results on Hurwitz spaces and other moduli spaces parametrizing deformations have been obtained in the case of characteristic zero and extended to positive characteristic $p > 0$ when p does not divide the order of the automorphism group; see [Bertin and Romagny 2008], for instance. For instance, if C is a compact Riemann surface with genus $g \geq 2$ and G an automorphism group of C, the deformations of the cover $\varphi : C \to C/G$ are parametrized by a moduli space of dimension $3g_0 - 3 + |\mathcal{B}| + \dim \operatorname{Aut}(C/G - \mathcal{B})$, where g_0 is the genus of C/G and $\mathcal{B}$ the branch locus of φ. By the Hurwitz genus formula, g_0 only depends on $|G|$, g, $|\mathcal{B}|$ and the orders of the inertia groups. All these results are no longer true in positive characteristic $p > 0$ when φ is wildly ramified. Likewise, in positive characteristic $p > 0$, the Hurwitz bound is no longer true for automorphism groups G whose order is not prime to p. The finiteness result still holds [Schmid 1938] but the Hurwitz linear bound is replaced with biquadratic bounds [Stichtenoth 1973a; 1973b]. These biquadratic bounds are optimal: so, in positive characteristic, the automorphism groups may be very large compared with the case of characteristic zero, as a result of wild ramification.

Wild ramification points also contribute to the dimension of the tangent space to the global infinitesimal deformation functor of a curve C together with an automorphism group G, and it is precisely this that makes computations difficult. Following [Bertin and Mézard 2000], in the case where G is cyclic of order p, Pries [2005] and Kontogeorgis [2007] have obtained lower and upper bounds for the dimension of the tangent space, with explicit computations in some special cases, in particular when G is an abelian p-group. (See also [Cornelissen and Kato 2003]).

To rigidify the situation in characteristic $p > 0$ as has been done in characteristic zero, one idea is to consider large automorphism p-groups. From [Nakajima 1987] we deduce that if G is a p-subgroup of $\operatorname{Aut}_k(C)$ such that $|G| > 2\,p\,g/(p-1)$, the Hasse–Witt invariant of C is zero. The Deuring–Shafarevich formula (see [Bouw 2000], for instance) then implies that the genus of the quotient curve C/G is zero and that the branch locus of the cover $C \to C/G$ is reduced to one point. From now on, we define a *big action* as a pair (C, G) where G is a p-subgroup of $\mathrm{Aut}_k(C)$ such that $|G|/g > 2\,p/(p-1)$.

Outline of the paper. Let (C, G) be a big action with $g \geq 2$. As shown in [Lehr and Matignon 2005], there is a point of C, say ∞, such that G is equal to the wild inertia subgroup G_1 of G at ∞. Let G_2 be the second ramification group of G at ∞ in lower notation. 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 ∞, through $X \to X + y$, 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

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

The purpose of this paper is twofold: to give necessary conditions on G_2 for (C, G) to be a big action, and to display realizations of big actions with G_2 abelian of large exponent. We gather here the main results of the first part (Sections 2–5):

Theorem. *Let (C, G) be a big action with $g \geq 2$.*

1. *Let H be a subgroup of G. Then C/H has genus* 0 *if and only if $H \supset G_2$* (Lemma 2.4.1).
2. *Let H be a normal subgroup of G such that $H \subsetneq G_2$. Then $(C/H, G/H)$ is a big action with second ramification group $(G/H)_2 = G_2/H$* (Lemma 2.4.2).
3. *The group G_2 is equal to $D(G)$, the commutator subgroup of G* (Theorem 2.7). *In particular, G cannot be abelian.*
4. *The group G_2 cannot be cyclic unless G_2 has order p* (Theorem 5.1).
5. *If $|G|/g^2 \geq 4/(p^2-1)^2$, then G_2 is an elementary abelian p-group with order dividing p^3* (Proposition 4.1).

These results highlight the major role played by G_2 in the study of big actions. They are also crucial in pursuing the classification of big actions initiated in [Lehr and Matignon 2005]. The companion paper [Rocher 2008a] is devoted to big actions with a p-elementary abelian G_2, and its results led to the classification of the big actions satisfying $|G|/g^2 \geq 4/(p^2-1)^2$, in [Rocher 2008b].

After exploring restrictions on G_2, the second part of the paper is devoted to examples of big actions with G_2 abelian, knowing that we do not know yet examples of big actions with a nonabelian G_2.

In Section 6, following [Lauter 1999] and [Auer 1999], we consider the maximal abelian extension K_S^m of $K := \mathbb{F}_q(X)$ (where $q = p^e$) that 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 precise description of the Galois group $G_S(m)$ of this extension. Moreover, it follows from the uniqueness and the maximality of K_S^m that the group of translations $X \mapsto X+y$ ($y \in \mathbb{F}_q$) extends to a p-group of $\mathbb{F}_q$-automorphisms of K_S^m, say $G(m)$, with the exact sequence

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

This provides examples of big actions whose $G_2 = G_S(m)$ is abelian of exponent as large as we want, but it also relates the problem of big actions to the search of algebraic curves with many rational points compared with their genera.

In Section 7 we use the Katz–Gabber theorem to highlight the link between 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 $\wp$ 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 α 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 α and β in k, $P(\alpha+\beta) = P(\alpha)+P(\beta)$. A separable polynomial is additive if and only if the set of its roots is a subgroup of k [Goss 1996, Chapter 1].

Let $f(X)$ be a polynomial of $k[X]$. There is a unique polynomial $\mathrm{red}(f)(X)$ in $k[X]$, called the reduced representative of f, which is p-power free, (meaning that $\mathrm{red}(f)(X) \in \bigoplus_{(i,p)=1} k\,X^i$) and such that $\mathrm{red}(f)(X) = f(X) \bmod \wp(k[X])$. We say that the polynomial f is reduced mod $\wp(k[X])$ if and only if it coincides with its reduced representative $\mathrm{red}(f)$. 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 $\operatorname{Spec} k[X]$ corresponds to a curve C_f where f is a polynomial of $k[X]$; see [Milne 1980, III.4.12, p. 127]. By Artin–Schreier theory, the covers C_f and $C_{\mathrm{red}(f)}$ define the same p-cyclic covers of the affine line. The curve C_f is irreducible if and only if $\mathrm{red}(f) \neq 0$.

Throughout the text, C always denotes a nonsingular smooth projective curve with genus g and $\mathrm{Aut}_k(C)$ means its k-automorphism group. Our main references for ramification theory are [Serre 1968] and [Auer 1999].

2. First results on big actions

To pinpoint the background of our work, we begin by collecting and completing the first results on big actions already obtained in [Lehr and Matignon 2005]. A *big action* is a curve 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 $\mathrm{Aut}_k(C)$. We say that the pair (C, G) is a big action if G is a finite p-group, if $g \neq 0$ and if

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

Proposition 2.2 [Lehr and Matignon 2005]. *Assume that (C, G) is a big action with $g \geq 2$. Then there is a point of C (say ∞) such that G is the wild inertia subgroup G_1 of G at ∞. 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 ∞ (respectively $\pi(\infty)$). For all $i \geq 0$, we denote by G_i the i-th lower ramification group of G at ∞.*

1. *G_2 is nontrivial and it is strictly included in G_1.*
2. *The Hurwitz genus formula applied to $C \to C/G$ reads*

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

Thus, (2–1) can be written as $|G| > 2\,g/(p-1)\,p$, with $2\,g/(p-1) \in \mathbb{N}^*$.

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 $C/G_2 - \{\infty\} = \mathrm{Spec}\, k[X]$, through $X \mapsto X + y$, where y runs over a subgroup V of k. Then V is an $\mathbb{F}_p$-vector subspace of k. We denote by v its dimension. Thus, we obtain the exact sequence*

$$0 \longrightarrow G_2 \longrightarrow G = G_1 \xrightarrow{\pi} V \simeq (\mathbb{Z}/\,p\,\mathbb{Z})^v \longrightarrow 0,$$

where $\pi : G \to V$ is defined by $g \mapsto g(X) - X$.

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 ∞ in the cover $C \to C/H$. 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 Q_8, the quaternion group of order* 8 (see [Silverman 1986, Appendix A, Proposition 1.2]).

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

2. Let (C, G) be a big action. Call L the function field of C and $k(X) = L^{G_2}$. As seen above, the Galois extension $L/k(X)$ is only ramified at $X = \infty$. Therefore, the support of the conductor of $L/k(X)$, as defined in [Serre 1968, chapitre 15, corollaire 2] reduces to the place ∞. So, in what follows, we systematically confuse the conductor $m\,\infty$ with its degree m. In this case, one can also see m as the smallest integer $n > 0$ such that the n-th upper ramification group G^n of G at ∞ is trivial; see [Auer 2000, I.3].

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

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

1. *C/H is isomorphic to $\mathbb{P}^1_k$ if and only if $H \supset G_2$.*
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. Moreover, its second ramification group is $(G/H)_2 = G_2/H$.*

Proof. Applied to the cover $C \to C/G \simeq \mathbb{P}^1_k$, the Hurwitz genus formula (see for instance [Stichtenoth 1993]) yields $2(g-1) = 2|G|\,(g_{C/G} - 1) + \sum_{i\geq 0}(|G_i| - 1)$. When applied to the cover $C \to C/H$, 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 $G_2 \subset H$, proving 1.

Together with part 1, Proposition 2.2.4 shows that $(C/H, G/H)$ is a big action. Then $G = G_1 \supsetneq G_2$ and $G/H = (G/H)_1 \supsetneq (G/H)_2$. Since the first jump always coincides in lower and upper ramification, it follows that $G_2 = G^2$ and $(G/H)_2 = (G/H)^2$. By [Serre 1968, chapitre IV, proposition 14], we obtain $(G/H)_2 = (G/H)^2 = G^2H/H = G_2H/H = G_2/H$. □

The very first step in studying big actions is to give a precise description of them when $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$. The following proposition collects and reformulates the results already obtained for this case.

Proposition 2.5 [Lehr and Matignon 2005, Propositions 5.5, 8.1, 8.3]. *Let (C, G) be a big action, with $g \geq 2$, such that $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.*

1. *Then C is birational to the curve $C_f : W^p - W = f(X) = X\,S(X) + c\,X \in k[X]$, 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*

$$G = G_0 = G_1 \supsetneq G_2 = G_3 = \cdots = G_{i_0} \supsetneq G_{i_0+1} = \cdots$$

2. *Write* $S(F)=\sum_{j=0}^{s} a_j F^j$, *with* $a_s \neq 0$. *Define* (following [Elkies 1999b, Section 4]) *the palindromic polynomial of* f *as the additive polynomial*

$$\mathrm{Ad}_f := a_s^{-p^s} F^s \left(\sum_{j=0}^{s} a_j\, F^j + F^{-j}\, a_j \right).$$

The set of roots of Ad_f, *denoted by* $Z(\mathrm{Ad}_f)$, *is an* $\mathbb{F}_p$*-vector subspace of* k, *isomorphic to* $(\mathbb{Z}/p\mathbb{Z})^{2s}$. *Moreover,*

$$Z(\mathrm{Ad}_f)=\{y \in k,\ f(X+y)-f(X)=0 \mod \wp(k[X])\}.$$

3. *Let* $A_{\infty,1}$ *be the wild inertia subgroup of* $\mathrm{Aut}_k(C)$ *at* ∞. *Then* $A_{\infty,1}$ *is a central extension of* $\mathbb{Z}/p\mathbb{Z}$ *by the elementary abelian* p*-group* $Z(\mathrm{Ad}_f)$ *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* $Z(A_{\infty,1})$ *the center of* $A_{\infty,1}$ *and by* $D(A_{\infty,1})$ *its commutator subgroup,* $Z(A_{\infty,1}) = D(A_{\infty,1}) = \langle\sigma\rangle$, *where* $\sigma(X) = X$ *and* $\sigma(W) = W+1$. *Thus, we get the exact sequence*

$$0 \longrightarrow Z(A_{\infty,1}) = D(A_{\infty,1}) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow A_{\infty,1} \xrightarrow{\pi} Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \longrightarrow 0,$$

where $\pi : A_{\infty,1} \to Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$ *is defined by* $g \mapsto g(X)-X$. *For* $p>2$, $A_{\infty,1}$ *is the unique extraspecial group with exponent* p *and order* p^{2s+1}. (The case $p=2$ is more complicated; see [Lehr and Matignon 2005, 4.1]).

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

$$0 \longrightarrow G_2 \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G \xrightarrow{\pi} V \longrightarrow 0.$$

Remark 2.6. Proposition 2.5 still holds for big actions (C, G) with $g=1$ when G is included in a decomposition group of $\mathrm{Aut}_k(C)$; see [Lehr and Matignon 2005, Proposition 8.3]. In particular, this is true for the pair $(C/H, G/H)$ when (C, G) is a big action with $g \geq 2$ and H a normal subgroup of G such that $g_{C/H}=1$ (see Proposition 2.2.4).

Therefore, the key idea in studying 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 result:

Theorem 2.7. *Let* (C, G) *be a big action with* $g \geq 2$. *Let* $\mathcal{G}$ *be a normal subgroup in* G *such that* $\mathcal{G}$ *is strictly included in* G_2. *There exists a group* H, *normal in* G, *such that* $\mathcal{G} \subset H \subsetneq G_2$ *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*

$$0 \longrightarrow G_2 \longrightarrow G \xrightarrow{\pi} V \longrightarrow 0$$

of Proposition 2.2 induces the following one:

$$0 \longrightarrow G_2/H = (G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G/H \xrightarrow{\pi} V \longrightarrow 0.$$

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 Ad_f be the palindromic polynomial related to f* (Proposition 2.5). *Then $V \subset Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$.*
3. *Let E be the wild inertia subgroup of* $\mathrm{Aut}_k(C/H)$ *at ∞. 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*

$$0 \longrightarrow D(E) = Z(E) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow E \xrightarrow{\pi} Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \longrightarrow 0.$$

4. *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 the Frattini subgroup of G.*

Proof. The existence of the group H comes from [Suzuki 1982, Chapter 2, Theorem 1.12]. The first assertion now follows from Lemma 2.4.2. The second and third derive directly from Proposition 2.5.

We now prove part 4. 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 $G_2 = D(G)$. Since G/G_2 is abelian, $D(G)$ is included in G_2. Now assume that $D(G)$ is strictly included in G_2. Then the first point applied to $\mathcal{G} = D(G)$ ensures the existence of a group H, normal in G, with $D(G) \subset H \subset G_2$, $[G_2 : H] = p$ and 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, [Huppert 1967, Satz 13.7] implies $|G/H| \leq p^{s+1}$. Furthermore, by Proposition 2.5.1 (and Remark 2.6), C/H is birational to a curve $W^p - W = X\,S(X) + c\,X \in k[X]$, where S is an additive polynomial of $k[X]$ with degree p^s. It follows that $g_{C/H} = \frac{1}{2}(p-1)\,p^s$. Combined with the bound on $|G/H|$, this gives $|G/H|/g_{C/H} \leq 2\,p/(p-1)$, which contradicts condition (2–1) for the big action $(C/H, G/H)$. Hence $D(G) = G_2$.

It remains to prove the statement about the Frattini subgroup of G. As G is a p-group, its Frattini subgroup, Fratt(G), is equal to $D(G)G^p$, where G^p means the subgroup generated by the p powers of elements of G [Leedham-Green and McKay 2002, Proposition 1.2.4]. As G/G_2 is an elementary abelian p-group, then $G^p = G_1^p \subset G_2 = D(G)$. As a consequence, $G_2 = D(G)G^p = \mathrm{Fratt}(G)$. □

Remark 2.8. When applying Theorem 2.7 to $\mathcal{G} = G_{i_0+1}$, where i_0 is defined as in Proposition 2.5, one obtains [Lehr and Matignon 2005, Theorem 8.6(i)]. In particular, for all big actions (C, G) with $g \geq 2$, there exists a subgroup H of index p in G_2, with H 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, $i_0 = 1 + p^s$.

Since G_2 cannot be trivial for a big action, we gather from the last part of Theorem 2.7 the following result.

Corollary 2.9. *Let (C, G) be a big action with $g \geq 2$. Then G cannot be abelian.*

It is natural to wonder whether G_2 can be nonabelian. 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 2.10. *Let (C, G) be a big action with $g \geq 2$. 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. G_2 is a p-group, normal in G and included in $D(G)$ (see Theorem 2.7); hence, by [Suzuki 1986, Proposition 4.21, p. 75], G_2 is also 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 $G_2 = Z(G_2)$. □

Corollary 2.11. *Let (C, G) be a big action with $g \geq 2$. Let $A_{\infty,1}$ be the wild inertia subgroup of* $\mathrm{Aut}_k(C)$ *at ∞. Then $(C, A_{\infty,1})$ is a big action whose second lower ramification group is equal to $D(A_{\infty,1}) = D(G)$. In particular, G is equal to $A_{\infty,1}$ if and only if $|G/D(G)| = |A_{\infty,1}/D(A_{\infty,1})|$.*

Proof: As G is included in $A_{\infty,1}$, then $D(G) \subset D(A_{\infty,1})$. If the inclusion is strict, one can find a subgroup $\mathcal{G}$ such that $G \subsetneq \mathcal{G} \subset A_{\infty,1}$, with $[\mathcal{G} : G] = p$; see [Suzuki 1982, Chapter 2, Theorem 19]. Note that $D(G) \subset D(\mathcal{G})$. We now prove that $D(G) \supset D(\mathcal{G})$. As $|G| \leq |\mathcal{G}|$, the pair $(C, \mathcal{G})$ is also a big action. So, by Theorem 2.7.4, $\mathcal{G}_2 = D(\mathcal{G})$. Since (C, G) is a big action, $g(C/D(G))$ vanishes by Proposition 2.2.3. It follows from Lemma 2.4.1 that $D(G) \supset \mathcal{G}_2 = D(\mathcal{G})$, hence $D(G) = D(\mathcal{G})$. The claim follows by reiterating the process. □

Remark 2.12. Let $(C, A_{\infty,1})$ be a big action as in Corollary 2.11. Then $A_{\infty,1}$ is a p-Sylow subgroup of $\mathrm{Aut}_k(C)$. Moreover, we deduce from [Giulietti and Korchmáros 2007, Theorem 1.3] that $A_{\infty,1}$ is the unique p-Sylow subgroup of $\mathrm{Aut}_k(C)$ except in four special cases: the hyperelliptic curves $W^{p^n} - W = X^2$ with $p > 2$, the Hermitian curves and the Deligne–Lusztig curves arising from the Suzuki groups and the Ree groups; see the equations in [Giulietti and Korchmáros 2007, Theorem 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 $\tilde{G}_2 \simeq G_2$ and $g_{\tilde{C}} = p^s g_C$. The chief tool is a base change associated with an additive polynomial map $\mathbb{P}^1_k \xrightarrow{S} C/G_2 \simeq \mathbb{P}^1_k$.

Proposition 3.1. *Let (C, G) be a big action with $g \geq 2$. 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, $s \in \mathbb{N}$. Then*:

1. *L and $k(Z)$ are linearly disjoint 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 $\tilde{G} \simeq G \times (\mathbb{Z}/p\mathbb{Z})^s$. Furthermore, $g_{\tilde{C}} = p^s\, g_C$. It follows that $|\tilde{G}|/g_{\tilde{C}} = |G|/g$. So, $(\tilde{C}, \tilde{G})$ is still a big action with second ramification group $\tilde{G}_2 \simeq G_2 \times \{0\} \subset G \times (\mathbb{Z}/p\mathbb{Z})^s$. This can be illustrated by the diagram*

$$\begin{tikzcd}
C \arrow[d] & \tilde{C} \arrow[l] \arrow[d] \\
C/G_2 \simeq \mathbb{P}^1_k & \mathbb{P}^1_k \arrow[l, "S"']
\end{tikzcd}$$

The proof requires two preliminary lemmas.

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 $\mathcal{G}$ is a p-group. Let K_0/K be a cyclic extension of degree p. Assume that K_0 and K_1 are linearly disjoint over K. Put $L := K_0K_1$*:

$$\begin{tikzcd}
K_1 \arrow[r, dash] & L = K_0K_1 \\
K \arrow[u, dash, "\mathcal{G}"] \arrow[r, dash] & K_0 \arrow[u, dash]
\end{tikzcd}$$

Suppose that the conductor of K_0/K (see Remark 2.3.2) *is* 2. *Then L/K_1 also has conductor* 2.

Proof. Consider a principal series of $\mathcal{G}$, that is, a sequence

$$\mathcal{G} = \mathcal{G}_0 \supsetneq \mathcal{G}_1 \ldots \supsetneq \mathcal{G}_n = \{0\},$$

with $\mathcal{G}_i$ normal in $\mathcal{G}$ and $[\mathcal{G}_{i-1} : \mathcal{G}_i] = p$. One shows, by induction on i, that the conductor of each extension $K_0K_1^{\mathcal{G}_i}/K_1^{\mathcal{G}_i}$ is 2. Therefore, it is sufficient to prove the result for $\mathcal{G} \simeq \mathbb{Z}/p\mathbb{Z}$. By induction on i, it can be extended to the general case.

So, assume $\mathcal{G} \simeq \mathbb{Z}/p\mathbb{Z}$. Then $L/k((z))$ is a Galois extension with group $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Write the ramification filtration of G in lower notation:

$$G = G_0 = \cdots = G_{i_0} \supsetneq G_{i_0+1} = \cdots = G_{i_1} \supsetneq G_{i_1+1} = \cdots$$

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

Now assume instead that $G_{i_0+1} \neq \{0\}$. As above, let H be a subgroup of index p in G. An exercise using the classical properties of ramification theory (see [Serre 1968, chapitre IV], for instance) shows that

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

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

Lemma 3.3. *Let W be a finite $\mathbb{F}_p$-vector subspace of k. Let W_1 and W_2 be two $\mathbb{F}_p$-subvectors spaces of W such that $W = W_1 \bigoplus W_2$. Define $T := \prod_{w \in W}(Z - w)$ and $T_i := \prod_{w \in W_i}(Z - w)$, 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 disjoint 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 $\{1, 2\}$, $k(T_i)/k(T)$ is a Galois extension with group isomorphic to W/W_i.*

This induces the diagram

$$\begin{tikzcd}
k(T_1) \arrow[r, dash, "W_1"] \arrow[d, dash, "W/W_1"'] & k(Z) \arrow[d, dash, "W_2"] \\
k(T) \arrow[r, dash, "W/W_2"] & k(T_2)
\end{tikzcd}$$

Proof. Use for example [Goss 1996, (1.8)]. □

Proof of Proposition 3.1. Statement 1 derives from Lemma 2.4.1. For 2, we put $W := S^{-1}(V)$, with V defined as in Proposition 2.2.3, and $W_1 := S^{-1}(\{0\})$; then $W_1 \simeq (\mathbb{Z}/p\mathbb{Z})^s$, since S is an additive separable polynomial of $k[Z]$ with degree p^s (see [Goss 1996, Chapter 1], for instance). Let W_2 be any $\mathbb{F}_p$-vector subspace of W such that $W = W_1 \bigoplus W_2$. Then Lemma 3.3 applied to the extension $k(Z)/k(T)$

induces the diagram

$$\begin{tikzcd}
L = k(C) \arrow[r, dash] \arrow[d, dash, "G_2"'] & k(\tilde{C}) \arrow[d, dash] \\
L^{G_2} = k(X) = k(Z)^{W_1} \arrow[r, dash, "W_1"] \arrow[d, dash, "W/W_1"'] & k(Z) \arrow[d, dash, "W_2"] \\
L^{G_1} = k(T) = k(Z)^{W} \arrow[r, dash, "W/W_2"] & k(Z)^{W_2}
\end{tikzcd}$$

In particular, Lemma 3.3 implies that $k(Z)^{W_1} \cap k(Z)^{W_2} = k(T)$. Since $k(C) \cap k(Z) = k(X)$ (see statement 1 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 $W/W_2 \simeq W_1 \simeq (\mathbb{Z}/p\mathbb{Z})^s$, it follows that $k(\tilde{C})/k(T)$ is a Galois extension with group $\tilde{G} \simeq \mathrm{Gal}(k(C)/k(T)) \times \mathrm{Gal}(k(Z)^{W_2}/k(T)) \simeq G \times (\mathbb{Z}/p\mathbb{Z})^s$.

Now, consider a flag of $\mathbb{F}_p$-vector subspaces of W_1:

$$W_1 = W_1^{(1)} \supsetneq W_1^{(2)} \supsetneq \ldots \supsetneq W_1^{(s+1)} = \{0\}$$

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

$$k(Z) = k(Z)^{W_1^{(s+1)}} \supsetneq k(Z)^{W_1^{(s)}} \supsetneq \ldots \supsetneq k(Z)^{W_1^{(1)}} = k(X).$$

We now prove the claim by induction on the integer $s \geq 1$, p^s being the degree of the additive polynomial S. Considering the flag above, it is sufficient to solve the case $s = 1$. Let K_1/K be the completion at ∞ of the extension $k(C)/k(X)$, whose group G_2 is a p-group and let K_0/K be the completion at ∞ of the cyclic extension of degree p and conductor 2: $k(Z)/k(X)$. To apply Lemma 3.2, we need to show that the two completions are linearly disjoint. Otherwise, $K_1 \cap K_0 = K_0$, which gives the inclusion $K \subset K_0 \subset K_1$. Consider a subgroup H of index p in G_2 such that $K_0 = K_1^H$. Let $k(X) \subset k(C)^H \subset k(C)$ be the corresponding extension of $k(X)$. Then $k(C)^H/k(X)$ is an étale p-cyclic cover of the affine line with conductor 2. It follows from the Hurwitz genus formula that the genus $g_{C/H}$ of the quotient curve C/H is 0, which contradicts Lemma 2.4.1. As a consequence, K_0 and K_1 are linearly disjoint over K and, by Lemma 3.2, the extension $k(\tilde{C})/k(C)$ has conductor 2. We deduce from the Hurwitz genus formula that $g_{\tilde{C}} = p\, g_C$. Finally, the last statement on $\tilde{G}_2$ is a consequence of Theorem 2.7.4. □

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

Indeed, take $C : W^p - W = X^{1+p}$ and $S(Z) = Z^p - Z$. Then $\tilde{C}$ is parametrized by $\tilde{W}^p - \tilde{W} = (Z^p - Z)\,(Z^{p^2} - Z^p) = -Z^2 + 2\,Z^{1+p} - Z^{1+p^2} \bmod \wp(k[Z])$. We denote by $A_{\infty,1}(C)$ (resp. $A_{\infty,1}(\tilde{C})$) the wild inertia subgroup of $\mathrm{Aut}_k(C)$ (resp. $\mathrm{Aut}_k(\tilde{C})$)

at $X = \infty$ (resp. $Z = \infty$). Note that $A_{\infty,1}(C)$ (resp. $A_{\infty,1}(\tilde{C})$) is a p-Sylow subgroup of $\mathrm{Aut}_k(C)$ (resp. $\mathrm{Aut}_k(\tilde{C})$). Take $G := A_{\infty,1}(C)$. From Proposition 2.5, we deduce that $|\tilde{G}| = p\,|G| = p\,|A_{\infty,1}(C)| = p^4$, whereas $|A_{\infty,1}(\tilde{C})| = p^5$.

4. A new step towards a classification of big actions

If big actions are defined through the value taken by the quotient $|G|/g$, it turns out that the key criterion to classify them is the value of another quotient, $|G|/g^2$. Indeed, the quotient $|G|/g^2$ has, to some extent, a sieve effect among big actions. If (C, G) is a big action, we first deduce from [Nakajima 1987, Theorem 1] that $|G|/g^2 \le 4\,p/(p-1)^2$. 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 $|G|/g^2 = 4\,p/(p-1)^2$ and $|G|/g^2 = 4/(p-1)^2$; see [Lehr and Matignon 2005, Theorem 8.6]. More precisely, we investigate the big actions (C, G) that satisfy

$$M := \frac{4}{(p^2-1)^2} \le \frac{|G|}{g^2}. \qquad (4\text{–}1)$$

The choice of the lower bound M can be explained as follows: as shown in the proof of [Lehr and Matignon 2005, Theorem 8.6], a lower bound M on the quotient $|G|/g^2$ produces an upper bound on the order of the second ramification group, namely

$$|G_2| \le \frac{4}{M}\frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}|-1)^2}, \qquad (4\text{–}2)$$

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 $M := 4/(p^2-1)^2$, 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 (Corollary 2.10).

Proposition 4.1. *Let (C, G) be a big action with $g \ge 2$ satisfying condition* (4–1). *Then the order of G_2 divides p^3. It follows that G_2 is abelian.*

Proof. Put $p^m := |G_2/G_{i_0+1}|$, with $m \ge 1$, and

$$Q_m := \frac{4}{M}\frac{|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2} = \frac{4}{M}\frac{p^m}{(p^m-1)^2}.$$

Then inequality (4–2) becomes $1 < |G_2| = p^m|G_{i_0+1}| \le p^m Q_m$, which gives $1 \le |G_{i_0+1}| \le Q_m$. Since $(Q_m)_{m\ge1}$ is a decreasing sequence with $Q_4 < 1$, we conclude that $m \in \{1, 2, 3\}$.

If $m = 3$, then $1 \le |G_{i_0+1}| \le Q_3 < p$. So $|G_{i_0+1}| = 1$ and $|G_2| = p^3$. If $m = 2$, then $1 \le |G_{i_0+1}| \le Q_2 = p^2$. So $|G_2| = p^2\,|G_{i_0+1}|$, with $|G_{i_0+1}| \in \{1, p, p^2\}$. This leaves only one case to exclude, namely $|G_{i_0+1}| = p^2$. In this case, $|G_2| = p^4$ and formula (2–2) 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 2.8. Then $i_0 = 1 + p^s$. Besides, by Theorem 2.7, $V \subset (\mathbb{Z}/p\mathbb{Z})^{2s}$. Consequently, $|G| = |G_2|\,|V| \leq p^{4+2s}$ and

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

which contradicts inequality (4–1).

If $m = 1$, then $1 \leq |G_{i_0+1}| \leq Q_1$, with

$$Q_1 := p\,(p+1)^2 < \begin{cases} p^4 & \text{if } p \geq 3, \\ p^5 & \text{if } p = 2. \end{cases}$$

Because G_{i_0+1} is a p-group, we get $1 \leq |G_{i_0+1}| \leq p^3$ if $p \geq 3$, or $1 \leq |G_{i_0+1}| \leq p^4$ if $p = 2$. Since $|G_2| = p\,|G_{i_0+1}|$, there are two cases to exclude: $|G_{i_0+1}| = p^{3+\epsilon}$, with $\epsilon = 0$ if $p \geq 3$ and $\epsilon \in \{0, 1\}$ if $p = 2$. Then $|G_2| = p^{4+\epsilon}$. If $\epsilon = 0$, we are in the same situation as in the previous case. If $\epsilon = 1$, (2–2) yields $2\,g \geq (i_0 - 1)(p^5 - 1)$. Since this case only occurs for $p = 2$, we eventually get the inequality

$$\frac{|G|}{g^2} \leq \frac{4\,p^{5+2s}}{p^{2s}\,(p^5-1)^2} = \frac{128}{961} < \frac{4}{9} = \frac{4}{(p^2-1)^2},$$

which contradicts condition (4–1). Therefore, the order of G_2 divides p^3. Then we conclude from Corollary 2.10 that G_2 is abelian. □

But we can even prove better:

Proposition 4.2. *Let (C, G) be a big action with $g \geq 2$ satisfying condition* (4–1). *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 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* (4–1). *Then G_2 cannot be isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. Assume $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. The lower ramification filtration of G has one of the following forms:

1. $G = G_1 \supsetneq G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+1} \simeq \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+i_1+1} = \{0\}$.
2. $G = G_1 \supsetneq G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset G_{i_0+i_1+1} = \{0\}$.
3. $G = G_1 \supsetneq G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset G_{i_0+i_1+1} \simeq \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+i_1+i_2+1} = \{0\}$.

4. $G = G_1 \supsetneq G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+1} \simeq \mathbb{Z}/p^2\mathbb{Z} \supset G_{i_0+i_1+1} \simeq \mathbb{Z}/p\mathbb{Z} \supset G_{i_0+i_1+i_2+1} = \{0\}$.

We now focus on the ramification filtration of G_2, temporary denoted by H for convenience. 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 $H =: H_0$ reads

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

Consider the upper ramification groups $H^{v_0} = H^{\varphi(i_0)} = H_{i_0}$ and $H^{v_1} = H^{\varphi(i_0+i_1)} = H_{i_0+i_1}$, where φ denotes the Herbrand function [Serre 1968, IV.3]. Then the ramification filtration in upper notation reads

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

Since H is abelian, it follows from the Hasse–Arf theorem (loc. cit.) that v_0 and v_1 are integers. Consequently, the equality

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

gives $v_0 = i_0$ and $v_1 = i_0 + i_1/p^2$. By [Marshall 1971, Theorem 6] we have $H^{v_0} \supsetneq H^{p\,v_0} \supset (H^{v_0})^p$ with $(H^{v_0})^p = H^p = G_2^p \simeq \mathbb{Z}/p\mathbb{Z}$. Thus, $H^{pv_0} \supset H^{v_1}$, which implies $pv_0 \leq v_1$ and $i_1 \geq p^2(p-1)i_0$. Then the Hurwitz genus formula applied to $C \to C/H \simeq \mathbb{P}^1_k$ yields a lower bound for the genus:

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

Let s be the integer defined in Remark 2.8. Then $i_0 = 1 + p^s$. Moreover, by Theorem 2.7, $|G| = |G_2|\,|V| \leq p^{3+2s}$. It follows that

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

Since $p^3(p+1)^2/(p^3+p+1)^2 < 1$ for $p \geq 2$, this contradicts condition (4–1).

In case (ii), the lower ramification filtration of $H = H_0$ reads

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

Keeping the notation of case (i), the upper ramification filtration is

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

with $v_0 = \varphi(i_0) = i_0$ and $v_1 = \varphi(i_0 + i_1) = i_0 + i_1/p$. Once again, $H^{pv_0} \supset (H^{v_0})^p \simeq \mathbb{Z}/p\mathbb{Z}$ implies $H^{p\,v_0} \supset H^{v_1}$, which involves $p\,v_0 \leq v_1$ and $i_1 \geq i_0\,p\,(p-1)$. Then the Hurwitz genus formula yields

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

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 becomes

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

Keeping the same notation as above and introducing $H^{\nu_2} = H^{\varphi(i_0+i_1+i_2)} = H_{i_0+i_1+i_2}$, the upper ramification filtration is

$$\begin{aligned}&H^{\nu_0} \simeq \mathbb{Z}/p^2\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z} \supset H^{\nu_0+1} = \cdots\\ &\qquad = H^{\nu_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H^{\nu_1+1} = \cdots = H^{\nu_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_2+1} = \{0\},\end{aligned}$$

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

$$\begin{aligned}2\,g &= (i_0-1)(|H|-1)+i_1(|H_{i_0+1}|-1)+i_2(|H_{i_0+i_1+1}|-1)\\ &\geq (p-1)\,(p^s\,(p^2+p+1)+(p^s+1)\,(p-1)\,p^2).\end{aligned}$$

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

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

Since $p\,(p+1)^2/(p^2+1)^2 < 1$ for $p \geq 2$, this contradicts condition (4–1).

In case (iv), the lower ramification filtration of H, namely

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

induces the upper ramification filtration

$$\begin{aligned}&H^{\nu_0} \simeq \mathbb{Z}/p^2\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z} \supset H^{\nu_0+1} = \cdots\\ &\qquad = H^{\nu_1} \simeq (\mathbb{Z}/p^2\mathbb{Z}) \supset H^{\nu_1+1} = \cdots = H^{\nu_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_2+1} = \{0\}.\end{aligned}$$

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 preceding 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 (4–1). Indeed, if $H := G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$, the lower ramification filtration of H,

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

induces the upper ramification filtration

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

with $\nu_0 = \varphi(i_0) = i_0$ and $\nu_1 = \varphi(i_0+i_1) = i_0+i_1/p$. Since $H^{p\nu_0} \supset (H^{\nu_0})^p \simeq \mathbb{Z}/p\mathbb{Z}$, we obtain $p\,\nu_0 \le \nu_1$, hence $i_1 \ge (p-1)\,p\,i_0$. Let s be the integer defined in Remark 2.8. The Hurwitz genus formula yields

$$\begin{aligned} 2\,g &= (i_0-1)(|H|-1) + i_1(|H_{i_0+1}|-1) \\ &\ge (p-1)\,(p^s\,(p^2+1) + p^2 - p) \ge (p-1)\,p^s\,(p^2+1). \end{aligned}$$

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

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

In this case, condition (4–1) requires $p^{1+(v/2)-s}(p+1) > p^2$. Since $v/2 \le s$, this implies $p+1 > p^{1+s-v/2} \ge p$, hence $v/2 = s$. This means that $V = Z(\mathrm{Ad}_f)$, where f is the function defined in Remark 2.8 and 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 $G_2 \subsetneq G_1$. This enables us to prove the more general result on big actions formulated later.

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 $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$. For Witt vectors and Artin–Schreier–Witt theory, our main reference is [Bourbaki 1983, chapitre IX].

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 $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$. We proceed in steps.

1. *We first prove that we can assume $n = 2$.* Indeed, for $n > 2$, $\mathcal{H} := G_2^{p^{n-2}}$ 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 $\mathbb{Z}/p^2\mathbb{Z}$.

Notation and preparatory 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 [Bourbaki 1983, chapitre IX, exercice 19], we define the $W_2(\mathbb{F}_p)$-module

$$\tilde{A} := \frac{\wp(W_2(L)) \cap W_2(k(X))}{\wp(W_2(k(X)))},$$

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

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

Since L/L^{G_2} is étale outside $X = \infty$, it follows from [Milne 1980, III, 4.12] that we can identify A with $\tilde{A}$. Consider the Artin–Schreier–Witt pairing

$$\begin{aligned} G_2 \times A &\longrightarrow W_2(\mathbb{F}_p), \\ (g, \overline{\wp x}) &\longmapsto [g, \overline{\wp x}\rangle := gx - x, \end{aligned}$$

where $g \in G_2 \subset \mathrm{Aut}_k(L)$, $x \in L$ such that $\wp x \in k[X]$ and $\overline{\wp x}$ denotes the class of $\wp x$ mod $\wp(k[X])$. This pairing is nondegenerate, 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 the definition of a reduced polynomial on page 890). We denote by m_0 the degree of f_0 and by n_0 that of g_0. Note that they are prime to p. The p-cyclic cover $L^{G_2^p}/L^{G_2}$ is parametrized by $W_0^p - W_0 = f_0(X)$. We deduce from Proposition 2.5 that $f_0(X) = XS(X) + c\,X$, 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 inequalities $|G| \leq p^{2+2s} \leq p^4$ and $2\,g \geq (p-1)\,(p^s\,(p^2+1) + p^2 - p) = (p-1)\,(p^3 + p^2)$ of Remark 4.4 imply

$$\frac{|G|}{g} \leq \frac{2\,p}{p-1}\,\frac{p^3}{p^3+p^2} < \frac{2\,p}{p-1},$$

which contradicts (2–1).

2. *The embedding problem.* Let V be the $\mathbb{F}_p$-vector space defined in Proposition 2.2.3. 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

$$\mathbb{Z}(f_0(X), g_0(X)) = \mathbb{Z}(f_0(X+y), g_0(X+y)) \mod \wp(W_2(k[X])). \tag{5–1}$$

Since A is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, (5–1) ensures the existence of an integer $n(y)$ such that

$$(f_0(X+y), g_0(X+y)) = n(y)\,(f_0(X), g_0(X)) \mod \wp(W_2(k[X])), \tag{5–2}$$

where $n(y) := a_0(y) + b_0(y)\,p$ for integers $a_0(y)$ and $b_0(y)$ such that $0 < a_0(y) < p$ and $0 \leq b_0(y) < p$. 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, we have

$$a_0(y)\,(f_0(X), g_0(X)) = \big(a_0(y)f_0(X), a_0(y)g_0(X) + c(a_0(y))f_0(X)\big),$$

where $c(a_0(y))$ is given by the recursion

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

On the other hand,

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

Consequently, (5–2) becomes

$$(f_0(X+y), g_0(X+y)) = (a_0(y)f_0(X), a_0(y)g_0(X) + \ell_0(y)f_0(X)) \mod \wp(W_2(k[X])), \tag{5–3}$$

where $\ell_0(y) := c(a_0(y)) + b_0(y)$. We notice that $a_0(y) = 1 \mod p$ for all y in V. Indeed, the equality of the first coordinate of Witt vectors in (5–3) implies that $f_0(X+y) = a_0(y)\,f_0(X) \mod \wp(k[X])$. 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 we get $f_0(X+py) = f_0(X)$, which entails $a_0(y)^p = 1 \mod p$ and $a_0(y) = 1 \mod p$. So (5–3) becomes

$$\begin{aligned}(f_0(X+y), g_0(X+y)) \\ = (f_0(X), g_0(X) + \ell_0(y)f_0(X)) + (P^p(X), Q^p(X)) - (P(X), Q(X)),\end{aligned} \tag{5–4}$$

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 (5–4) as

$$\begin{aligned}(f_0(X+y), g_0(X+y)) + (P(X), Q(X)) \\ = (f_0(X), g_0(X) + \ell_0(y)\,f_0(X)) + (P(X)^p, Q(X)^p).\end{aligned} \tag{5–5}$$

The first coordinate of (5–5) reads

$$f_0(X+y) + P(X) = f_0(X) + P(X)^p. \tag{5–6}$$

On the second coordinate of (5–5), the addition law in the ring of Witt vectors gives in $k[X]$ the equality

$$\begin{aligned} &g_0(X+y)+Q(X)+\psi(f_0(X+y),\,P(X)) \\ &\qquad\qquad = g_0(X)+\ell_0(y)\,f_0(X)+Q(X)^p+\psi(f_0(X),\,P(X)^p), \end{aligned} \tag{5–7}$$

where ψ is defined by

$$\begin{aligned} \psi(a,b) &:= \frac{1}{p}\,(a^p+b^p-(a+b)^p) = -\frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}a^i\,b^{p-i} \\ &= \sum_{i=1}^{p-1}\frac{(-1)^i}{i}\,a^i\,b^{p-i} \mod p. \end{aligned}$$

As a consequence, (5–7) gives

$$\Delta_y(g_0) := g_0(X+y)-g_0(X) = \ell_0(y)\,f_0(X)+\delta \mod \wp(k[X]), \tag{5–8}$$

with

$$\begin{aligned} \delta &:= \psi(f_0(X),\,P(X)^p)-\psi(f_0(X+y),\,P(X)) \\ &= \sum_{i=1}^{p-1}\frac{(-1)^i}{i}\,\{f_0(X)^i\,P(X)^{p(p-i)}-f_0(X+y)^i\,P(X)^{p-i}\}. \end{aligned}$$

Lemma 5.2. *With the notation defined above, δ is equal to*

$$\delta=\sum_{i=1}^{p-1}\frac{(-1)^i}{i}\,y^{p-i}X^{i+p^{s+1}} + \textit{lower-degree terms in } X. \tag{5–9}$$

Proof. We search for the monomials in δ that have degree at least $p^{s+1}+1$ in X. We first focus on $f_0(X)^i\,P(X)^{p(p-i)}$. We can infer from equality (5–6) that $P(X)$ has degree p^{s-1} and that its leading coefficient is $y^{1/p}$. By [Lehr and Matignon 2005, proof of Proposition 8-1], $P(X)-P(0)$ 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 $k[X]$ of degree at most p^{s-2}. Then, for all i in $\{1,\dots,p-1\}$, $f_0(X)^i\,P(X)^{p\,(p-i)} = f_0(X)^i\,(y\,X^{p^s}+P_1(X)^p)^{p-i} = f_0(X)^i\,(\sum_{j=0}^{p-i}\binom{p-i}{j}\,y^j\,X^{jp^s}\,P_1(X)^{p(p-i-j)})$. Since $f_0(X)$ has degree $1+p^s$, this gives in δ 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 $j\le p-i-1$, 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 less than $p^{s+1}+1$, for $s\ge 2$ and $1\le i\le p-1$. As a consequence, monomials of degree at least $p^{s+1}+1$ can only occur when the index j is equal to $p-i$, namely in $f_0(X)^i\,y^{p-i}\,X^{p^s(p-i)}$. 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 $\{1,\dots,p-1\}$, we have $f_0(X)^i\,y^{p-i}\,X^{p^s(p-i)} = y^{p-i}\,X^{p^s(p-i)}\big(\sum_{k=0}^{i}\binom{i}{k}X^{(1+p^s)j}\,P_2(X)^{i-k}\big)$. Accordingly, we get a monomial of degree at most to $p^s\,(p-i)+k\,(1+p^s)+(i-k)\,(1+p^{s-1})$, a number we can rewrite as $p^s\,(p-i)+i\,(1+p^{s-1})+k\,(p^s-p^{s-1})$. 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 δ 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 δ, 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 less 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 δ with degree greater or equal to $p^{s+1}+1$. Thus, we get the expected formula. □

3. *We next show 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 (5–8) reads $\Delta_y(g_0):=g_0(X+y)-g_0(X)=X\;\Sigma(y)+y\;\Sigma(X)+y\;\Sigma(y)+\gamma\,y$, which only gives a linear contribution in X after reduction mod $\wp(k[X])$. 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 (5–8) 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 $\wp(k[X])$, $a\not\equiv 0$ mod p. We also notice that the monomials in $g_0(X)$ with degree greater than a are of the form X^{1+p^n}; hence, as explained above, they only give linear monomials in $\Delta_y(g_0)$ mod $\wp(k[X])$. Therefore, after reduction mod $\wp(k[X])$, the degree of the left-hand side of (5–8) is at most $a-1$. Since the degree of the right-hand side is $p^{s+1}+p-1$, it follows that

$$a-1\geq p^{s+1}+p-1. \tag{5–10}$$

4. *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 $\wp(k[X])$. Since the monomials of $g_0(X)$ with degree greater than a only give a linear contribution in $\Delta_y(g_0)$ mod $\wp\,(k[X])$, (5–8) reads as follows, for all y in V:

$$\begin{aligned}c_a(g_0)\,a\;yX^{a-1}&+\text{lower-degree terms}\\ &=-y\;X^{p^{s+1}+p-1}+\text{lower-degree terms}\quad\text{mod }\wp\,(k[X]),\end{aligned}$$

where $c_a(g_0)\neq 0$ denotes the coefficient of X^a in g_0. If $a-1>p^{s+1}+p-1$, 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 (5–10) that $a-1=p^{s+1}+p-1$, which contradicts $a\neq 0$ mod p.

Thus p divides $a-1$. So, we can write $a=1+\lambda\, p^t$, with $t>0$, λ 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 $pj_0 > a$. Indeed,

$$pj_0 \leq a \Leftrightarrow p(1+(\lambda-1)p^t) \leq 1+\lambda\, p^t \Leftrightarrow \lambda \leq \frac{1-p+p^{t+1}}{p^t(p-1)} = \frac{-1}{p^t} + \frac{p}{p-1} < \frac{p}{p-1} \leq 2,$$

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

5. *We determine the coefficient of* X^{j_0} *in the left hand-side of* (5–8). Since p does not divide j_0, the monomial X^{j_0} is reduced mod $\wp(k[X])$. On the left-hand side of (5–8), namely $\Delta_y(g_0)$ mod $\wp(k[X])$, the monomial X^{j_0} comes from monomials of $g_0(X)$ of the form X^b, with b in $\{j_0+1,\dots,a\}$. As a matter of fact, the monomials of $g_0(X)$ with degree greater than a only give a linear contribution mod $\wp(k[X])$, whereas $j_0 = 1+(\lambda-1)\,p^t > 1$. For all $b \in \{j_0+1,\dots,a\}$, the monomial X^b of $g_0(X)$ generates $\binom{b}{j_0}\, y^{b-j_0}\, X^{j_0}$ 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 $\wp(k[X])$. It follows that the coefficient of X^{j_0} in the left-hand side of (5–8) is $T(y)$ with $T(Y) := \sum_{b=j_0+1}^{a} c_b(g_0)\binom{b}{j_0}\, Y^{b-j_0}$, where $c_b(g_0)$ denotes the coefficient of X^b in $g_0(X)$. As the coefficient of Y^{a-j_0} in $T(Y)$ is $c_a(g_0)\binom{a}{j_0} = c_a(g_0)\binom{1+\lambda p^t}{1+(\lambda-1)p^t} \equiv c_a(g_0)\,\lambda \not\equiv 0 \mod p$, the polynomial $T(Y)$ has degree $a-j_0 = p^t$.

6. *We identify with the coefficient of* X^{j_0} *in the right-hand side of* (5–8) *and obtain a contradiction.* We first assume that the monomial X^{j_0} does not occur in the right-hand side of (5–8). 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 $M_0 := m_0$ and $M_1 := \max\{p\, m_0,\ n_0\}$. Then, by [Garuti 2002], the Hurwitz genus formula applied to $C \to C/G_2 \simeq \mathbb{P}^1_k$ yields

$$2\,(g-1) = 2\,|G_2|\,(g_{C/G_2}-1)+d = -2\,p^2+d,$$

with $d := (p-1)\,(M_0+1)+p\,(p-1)\,(M_1+1)$. From $p\, m_0 = p\,(p^s+1) = p^{s+1}+p$ and $p^{s+1}+p-1 < n_0$, 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 the lower bound $2\,g = (p-1)\,p\,(n_0-1+p^{s-1}) \geq 2\,p^{t+1}\,(p-1)$ for the genus. Since $|G| = |G_2|\,|V| \leq p^{2+t}$, this entails

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

which contradicts (2–1).

As a consequence, the monomial X^{j_0} appears in the right-hand side of (5–8), which implies that $j_0 \leq p^{s+1}+p-1$. Using (5–10), we get $j_0 = 1+(\lambda-1)\,p^t \leq$

$p^{s+1}+p-1<a=1+\lambda\, p^t$. This yields

$$\lambda-1\le p^{s+1-t}+\frac{p-2}{p^t}<\lambda. \tag{5–11}$$

If $s+1-t\le -1$, since $t\ge 1$, (5–11) gives $\lambda-1\le 1/p+(p-2)/p<1$, which contradicts $\lambda\ge 2$. It follows that $s+1-t\ge 0$. Then (5–11), combined with the inequalities $0\le (p-2)/p^t<1$, leads to $\lambda-1=p^{s+1-t}$. We gather that $j_0=1+(\lambda-1)\,p^t=1+p^{s+1}>\deg f_0=1+p^s$. Therefore, in the right-hand side of (5–8), the monomial $X^{j_0}=X^{1+p^{s+1}}$ only occurs in δ. By Lemma 5.2, the coefficient of $X^{j_0}=X^{1+p^{s+1}}$ in δ is $-y^{p-1}$. By equating the coefficient of X^{j_0} in each side of (5–8), we get $T(y)=-y^{p-1}$, for all y in V. Put $\tilde{T}(Y):=T(Y)+Y^{p-1}$. Since $\deg T=p^t>p-1$, the polynomial $\tilde{T}$ has still degree p^t and satisfies $\tilde{T}(y)=0$ for all y in V. Once again, it leads to $|V|\le p^t$, which contradicts (2–1) as above. □

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 $n\ge 2$, there exists a subgroup H of index p in G_2^p, with H normal in G, such that the pair $(C/H, G/H)$ is a big action with $(G/H)_2=G_2/H\simeq\mathbb{Z}/p^2\mathbb{Z}\times(\mathbb{Z}/p\mathbb{Z})^t$, 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^2. In particular, we construct big actions (C,G) with $G_2\simeq\mathbb{Z}/p^2\mathbb{Z}\times(\mathbb{Z}/p\mathbb{Z})^t$ where $t=O(\log_p g)$.

6. Examples of big actions with G_2 abelian of exponent 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 $g_C\ge 2$ such that $|G|=84(g_C-1)$. Such a curve C is called a *Hurwitz curve* and such a group G a *Hurwitz group* [Conder 1990]. In particular, the lowest genus Hurwitz curves are the Klein's quartic with $G\simeq\mathrm{PSL}_2(\mathbb{F}_7)$ (cf. [Elkies 1999a]) and the Fricke–Macbeath curve with genus 7 and $G\simeq\mathrm{PSL}_2(\mathbb{F}_8)$ [Macbeath 1965].

Let C be a Hurwitz curve with genus g_c. Let $n\ge 2$ 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 uniqueness of C_n that the $\mathbb{C}$-automorphisms of C have n^{2g_c} prolongations to C_n. Therefore, $g_{C_n}-1=n^{2g}(g_C-1)$. Consequently, C_n is still a Hurwitz curve; see [Macbeath 1961].

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 [Bouw

2000], for example), 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 [1999] and R. Auer [1999]. Since the cover $C \to C/G_2$ is an étale cover of the affine line $\operatorname{Spec} k[X]$ totally ramified at ∞, we focus on the special case of ray class fields of the rational function field $\mathbb{F}_q(X)$, where $q = p^e$ [Auer 1999, III.8]. Such ray class fields allow us to produce families of big actions (C, G) (where C is defined over $k = \mathbb{F}_p^{\mathrm{alg}}$) with specific conditions imposed on ramification and endowed with an abelian G_2 of exponent as large as we want.

Definition 6.1 [Auer 1999, Part II]. Let $K := \mathbb{F}_q(X)$ be the rational function field, 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^{alg} an algebraic closure of K in which all extensions of K are assumed to lie. We define $K_S^m \subset K^{\mathrm{alg}}$ as the largest abelian extension L/K with conductor $\leq m\,\infty$, such that every place in S splits completely in L.

Remarks 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_S^m/K is the extension defined in Definition 6.1, then $S \subset S(K_S^m)$.

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 ∞. So, we systematically confuse the conductor $m\,\infty$ with its degree m.

3. We could more generally define K_S^m for S a nonempty 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.

Remarks 6.3. We keep the notation of Definition 6.1.

1. The existence of the extension K_S^m/K is based on global class field theory; see [Auer 1999, Part II].
2. K_S^m/K is a finite abelian extension whose full constant field is $\mathbb{F}_q$.
3. The reason why Lauter and Auer are interested 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_S^m. 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 $N_m = 1 + q\,[K_S^m : K]$. The main difficulty lies in computing $[K_S^m : K]$. We first wonder when K_S^m coincide with K. Here are partial answers.

4. Let $q = p^e$, with $e \in \mathbb{N}$. If e is even, put $r := \sqrt{q}$ and if e is odd, put $r := \sqrt{qp}$. Then, for all i in $\{0, \dots, r+1\}$, $K_S^i = K = \mathbb{F}_q(X)$; see [Auer 1999, III, Lemma 8.7 and formula (13)]. Note that the previous estimate $N_m = 1+q\,[K_S^m : K]$, combined with the Hasse–Weil bound (see [Stichtenoth 1993, V.2.3], for instance), furnishes another proof of $K_S^i = K$ when $i < 1+r$.
5. More generally, Lauter displays a method to compute the degree of the extension K_S^m/K via a formula giving the order of its Galois group $G_S(m)$ [Lauter 1999, Theorem 1]. Lauter's proof starts from the following presentation of $G_S(m)$:
$$G_S(m) \simeq \frac{1 + Z\,\mathbb{F}_q[\![Z]\!]}{\langle 1 + Z^m\,\mathbb{F}_q[\![Z]\!],\, 1 - yZ,\ y \in \mathbb{F}_q\rangle},$$
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 stricly greater than p (see next proposition).

Proposition 6.4 [Lauter 1999, Proposition 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 $\lceil\cdot\rceil$ is the ceiling function.*

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 $C^{\mathrm{alg}} := C \times_{\mathbb{F}_q} k$ with $k = \mathbb{F}_p^{\mathrm{alg}}$. If G is a finite p-subgroup of $\mathrm{Aut}_{\mathbb{F}_q} C$, then G can be identified with a subgroup of $\mathrm{Aut}_k C^{\mathrm{alg}}$. In this case, (C^{alg}, G) is a big action if and only if $g_{C^{\mathrm{alg}}} = g_C > 0$ and $|G|/g_C > 2\,p/(p-1)$. 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_S^m and, starting from this, we construct a p-group $G(m)$ acting on $C(m)$ by extending the translations $X \to X + y$, 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 $[K_S^m : K]$ 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_S^m. Then the group of translations $X \to X + y$, $y \in \mathbb{F}_q$, extends to a p-group of $\mathbb{F}_q$-automorphisms of $C(m)$, say $G(m)$, with the exact sequence*
$$0 \longrightarrow G_S(m) \longrightarrow G(m) \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

2. *Let L be an intermediate field of K_S^m/K. Assume $L = (K_S^m)^H$, 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 ∞: $G_S^i(m)H/H$, where $G_S^i(m)$ denotes the i-th upper ramification group of $G_S(m)$ at ∞. Then, for all $i \geq 0$,*

$$L^i = L \cap K_S^i.$$

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

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

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

where the sum is empty for $n = 0$. In particular, g_L vanishes if and only if $L \subset K_S^0$; in all other cases, $g_L < [L:K]\,(-1+n/2)$.

4. *If $m \geq r+2$, then $|G(m)|/g_{K_S^m} > q/(-1+\frac{1}{2}m)$. It follows that if $q/(-1+\frac{1}{2}m) \geq 2\,p/(p-1)$, the pair $(C(m), G(m))$ is a big action. In this case, the second lower ramification group $G_2(m)$ of $G(m)$ is equal to $G_S(m)$. In particular, with m_2 as in Proposition 6.4, if $p > 2$ and $e \geq 4$ or $p = 2$ and $e \geq 6$, the pair $(C(m_2), G(m_2))$ is a big action whose second ramification group $G_S(m_2)$ is abelian of exponent p^2.*

Proof. 1. The set S is globally invariant under the translations $X \mapsto X + y$, $y \in \mathbb{F}_q$. That is the same for ∞, 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^m, they can be extended to $\mathbb{F}_q$-automorphisms of K_S^m. This proves the first assertion.

2. This follows directly from [Auer 1999, II, Theorem 5.8].

3. The genus formula is obtained by combining the preceding results, the Hurwitz genus formula and the discriminant formula [Auer 1999, 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 $n \geq r+2 \geq 3$. Using the preceding formula and Remark 6.3.4, $g_L = 0$ reads

$$2+(n-2)\,[L:K] = \sum_{j=0}^{n-1} [K_S^j \cap L : K] = 2 + \sum_{j=2}^{n-1} [K_S^j \cap L : K] \leq 2 + (n-2)\,[L:K].$$

It follows that, for all j in $\{2, \dots, n-1\}$, $K_S^j \cap L = L$. 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

$$g_L = [L:K]\,(-1+n/(2)) - \frac{1}{2}\sum_{j=2}^{n-1}[L\cap K_S^j : K] < [L:K]\,(-1+n/(2)).$$

Assume that $m \geq r+2$. We gather from Remark 6.3.4 that $n := \min\{i \in \mathbb{N},\, K_S^m \subset K_S^i\} \geq r+2 \geq 3$. It follows from the third point that

$$g_{K_S^m} < [K_S^m : K]\,(-1+n/(2)) \leq [K_S^m : K]\,(-1+m/(2)).$$

As $|G(m)| = q[K_S^m : K]$, we deduce the expected inequality. In particular, when $q/(-1+\frac{1}{2}m) > 2\,p/(p-1)$, 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 $G_S(m) \supset G_2(m)$. 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 $G_S(m) \supsetneq G_2(m)$. Then $L \supsetneq (K_S^m)^{G_S(m)} = K$. 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, $C/G_2(m) \simeq \mathbb{P}_k^1$, so $g_L = 0$, hence a contradiction. We eventually explain the last statement. By Proposition 6.5.2, $G_S^{m_2-1}(m_2) = \mathrm{Gal}(K_S^{m_2}/K_S^{m_2-1})$, which induces the exact sequence

$$0 \longrightarrow G_S^{m_2-1}(m_2) \longrightarrow G_S(m_2) \longrightarrow G_S(m_2-1) \longrightarrow 0.$$

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 $G_S^{m_2}(m_2) = \{0\}$ (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: $|G(m)|/g_{C(m)}$ and $N_m/g_{C(m)}$. 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, $K_S^i = K$ for all i in $\{0,\ldots,r+1\}$, where $r = \sqrt{q}$ or $\sqrt{qp}$ 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 [Auer 1999, Proposition 8.9]. The table on the next page gives a complete description of the extensions K_S^m for m varying from 0 to $m_2 = p^{\lceil e/2\rceil+1} + p + 1$, in the special case $p = 5$ and $e = 4$. This involves $q = p^e = 625$, $s = e/2 = 2$, $r = p^s = 25$ and $m_2 = 131$. The table below should suggest the general method to parametrize such extensions.

conductor m	$[K_S^m{:}K]$	new equations
$0 \le m \le \ r+1=26$	1	
$27 \le m \le 2r+1=51$	5^2	$W_0^r + W_0 = X^{1+r}$
$m = 2r+2 = 52$	5^6	$W_1^q - W_1 = X^{2r}\,(X^q - X)$
$53 \le m \le 3r+1=76$	5^8	$W_2^r + W_2 = X^{2(1+r)}$
$m = 3r+2 = 77$	5^{12}	$W_3^q - W_3 = X^{3r}\,(X^q - X)$
$m = 3r+3 = 78$	5^{16}	$W_4^q - W_4 = X^{3r}\,(X^{2q} - X^2)$
$79 \le m \le 4r+1=101$	5^{18}	$W_5^r + W_5 = X^{3(1+r)}$
$m = 4r+2 = 102$	5^{22}	$W_6^q - W_6 = X^{4r}\,(X^q - X)$
$m = 4r+3 = 103$	5^{26}	$W_7^q - W_7 = X^{4r}\,(X^{2q} - X^2)$
$m = 4r+4 = 104$	5^{30}	$W_8^q - W_8 = X^{4r}\,(X^{3q} - X^3)$
$105 \le m \le 5r+1=126$	5^{32}	$W_9^r + W_9 = X^{4(1+r)}$
$m = 5r+2 = 127$	5^{36}	$W_{10}^q - W_{10} = X^{5r}\,(X^q - X)$
$m = 5r+3 = 128$	5^{40}	$W_{11}^q - W_{11} = X^{5r}\,(X^{2q} - X^2)$
$m = 5r+4 = 129$	5^{44}	$W_{12}^q - W_{12} = X^{5r}\,(X^{3q} - X^3)$
$m = 5r+5 = 130$	5^{48}	$W_{13}^q - W_{13} = X^{5r}\,(X^{4q} - X^4)$
$m = m_2 = 131$	5^{50}	$[W_0, W_{14}]^r + [W_0, W_{14}] = [X^{1+r}, 0]$

In this case,

$$\frac{|G(m_2)|}{g_{K_S^{m_2}}} \simeq 9,6929\ldots \tag{6–1}$$

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

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 [Stichtenoth 1993, Proposition VI. 4.1], P_y completely splits in the extension $K(W)/K$, where $W^r + W = X^{u\,(1+r)}$, with $1 \le u \le 4$, if the polynomial $T^r + T - y^{u\,(1+r)}$ has a root in K, which is true since $y^{u(1+r)} = (F^s + I)\,(\frac{1}{2}\,y^{u(1+r)})$. Likewise, P_y completely splits in the extension $K(W)/K$, where $W^q - W = X^{u\,r}\,(X^{v\,q} - X^v)$, with $1 \le v < u \le 5$, since $y^{vq} - y^v = 0$. Finally, P_y completely splits in the extension $K(W, \tilde{W})/K$, where $[W, \tilde{W}]^r + [W, \tilde{W}] = [X^{1+r}, 0]$, since
$$[y^{1+r}, 0] = (F^s + I)\Big[\frac{1}{2}\,y^{1+r}, -\frac{2^p - 2}{4p}\,y^{(1+r)p}\Big].$$
To conclude, we remark that $L_i = L_{i-1}\,K(W_i)$ for all i in $\{1, \ldots, 14\}$. Then $S(L_i) = S(L_{i-1}) \cap S(K(W_i))$, by [Auer 1999, Corollary 3.2.b], which allows us to conclude, 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 must distinguish three kinds of extensions. The extension $K(W)/K$, where $W^r + W = X^{u\,(1+r)}$, with $1 \le u \le 4$, has conductor $ur + u + 1$ [Auer 1999, Proposition 8.9a]. The extension $K(W)/K$, where now $W^q - W = X^{u\,r}\,(X^{v\,q} - X^v)$, with $1 \le v < u \le 5$, has conductor $ur + v + 1$ [Auer 1999, Proposition 8.9b]. Finally, the conductor of the extension $K(W, \tilde{W})/K$, where $[W, \tilde{W}]^r + [W, \tilde{W}] = [X^{1+r}, 0]$ is given by the formula $1 + \max\{p(1+r), -\infty\} = 1 + p + p^{s+1} = m_2$ [Garuti 2002, Theorem 1.1]. As a conclusion, since $m(L_i) = \max\{m(L_{i-1}), m(K(W_i))\}$ [Auer 1999, Corollary 3.2b], an induction on i allows us to obtain the expected conductor for L_i.
3. We obtain from 1 and 2 the inclusions $K(W_0) \subset K_S^{27}$, $K(W_0, W_1) \subset K_S^{52}, \ldots$ $K(W_0, \ldots, W_{14}) \subset K_S^{m_2}$. Equality is finally obtained by calculating the degree of each extension K_S^m/K via [Lauter 1999, Theorem 1] or [Auer 1999, (13), pp. 54–55]. □

We deduce from the foregoing 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 $K_S^{m_2}$ with the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & G_S(m_2) \arrow[r] \arrow[d, "\varphi"'] & G(m_2) \arrow[r] \arrow[d] & \mathbb{F}_q \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & H \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & \mathbb{F}_q \arrow[r] & 0 \\
& 0 & 0 & &
\end{tikzcd}$$

such that the pair $(C(m_2)/\mathrm{Ker}(\varphi), G)$ 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 $C(m_2)/\mathrm{Ker}(\varphi)$. Contrary to the previous case where the stability under the translations by $\mathbb{F}_q$ was ensured by the maximality of $K_S^{m_2}$, the difficulty now lies in producing a system of equations defining a subextension of $K_S^{m_2}$ which remains globally invariant through the action of the group of translations $X \to X + y$, $y \in \mathbb{F}_q$. Write $q = p^e$. We have to distinguish the case e even and e odd.

Proposition 6.7. *Assume that $p > 2$. We keep the notation defined above. In particular, $K = \mathbb{F}_q(X)$ with $q = p^e$. Assume that $e = 2s$, with $s \ge 1$, and put $r := p^s$. Define*

$$f_0(X) := a\,X^{1+r} \quad \textit{with } a \neq 0,\ a \in \Gamma := \{\gamma \in \mathbb{F}_q, \gamma^r + \gamma = 0\},$$

$$f_i(X) := X^{ir/p}\,(X^q - X) = X^{ip^{s-1}}\,(X^q - X) \quad \textit{for all } i \in \{1, \ldots, p-1\}.$$

Let $L := K(W_i)_{0 \le i \le p}$ be the extension of K parametrized by the Artin–Schreier–Witt equations $W_0^p - W_0 = f_0(X)$, $W_i^q - W_i = f_i(X)$ for all $i \in \{1, \ldots, p-1\}$, and $[W_0, W_p]^p - [W_0, W_p] = [f_0(X), 0]$.

For all i in $\{0, 1, \dots, p-1\}$, put $L_i := K(W_0, \dots, W_i)$. Let $C_L/\mathbb{F}_q$ be the nonsingular projective curve with function field L.

1. *L is an abelian extension of K and every place in S completely splits in L. Moreover, $L_0 \subset K_S^{r+2}$, $L_i \subset K_S^{p^{s+1}+i+1}$ for all $i \in \{1, \dots, p-1\}$, and $L \subset K_S^{m_2}$, where $m_2 = p^{s+1} + p + 1$ is the integer defined in Proposition 6.4.* (See table on the next page.)
2. *L/K has degree $[L : K] = p^{2+(p-1)e}$, and its Galois group G_L satisfies*
$$G_L \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \quad \text{with } t = (p-1)\,e.$$
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 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*
$$g_L = \frac{1}{2}\Big(p^{2+2s(p-1)}\,(p^{s+1} + p - 1) - p^s\,(p^2 - p + 1) - p^{2s+1}\sum_{i=0}^{p-2} q^i\Big).$$
In particular, when e grows large, $g_L \sim \frac{1}{2}p^{(2p-1)e/2+3}$ and $t = O(\log_p g_L)$.
5. *For $s \geq 2$, (C_L, G) is a big action with $G_2 = G_L$.* (Note that, for $p = 5$ and $e = 4$, one gets $|G|/g_L \simeq 9,7049\dots$, which is slightly bigger than the quotient obtained for the whole extension $K_S^{m_2}$ in (6–1).)

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 $\{1, \dots, p-1\}$, the place P_y completely splits in each extension $K(W_i)$ with $W_i^q - W_i = f_i(X)$. Therefore, to prove that P_y completely splits in L, it is sufficient to show that $[f_0(y), 0] \in \wp(W_2(\mathbb{F}_q))$. By [Bourbaki 1983, chapitre IX, exercice 18], this is equivalent to show that $\mathrm{Tr}([f_0(y), 0]) = 0$, 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 Γ. It follows that
$$\begin{aligned}\mathrm{Tr}([\gamma, 0]) &= \sum_{i=0}^{2s-1} F^i\,[\gamma, 0] = \sum_{i=0}^{s-1} [\gamma^{p^i}, 0] + \sum_{i=0}^{s-1} [\gamma^{rp^i}, 0] \\ &= \sum_{i=0}^{s-1} [\gamma^{p^i}, 0] + \sum_{i=0}^{s-1} [-\gamma^{p^i}, 0].\end{aligned}$$

As $p > 2$, $[-\gamma^{p^i}, 0] = -[\gamma^{p^i}, 0]$ and $\mathrm{Tr}([\gamma, 0]) = 0$. To establish the expected inclusions, it remains to compute the conductor of each extension L_i. First of all, [Auer 1999, I, exercise 3.3] together with [Stichtenoth 1993, Proposition III.7.10] shows that the conductor of L_0 is $r+2$. Thus, $L_0 \subset K_S^{r+2}$. Moreover, since $f_i(X) =$

$X^{i+p^{s+1}}-X^{1+ip^{s-1}} \bmod \wp(\mathbb{F}_q[X])$, we infer from [Auer 1999, I, Exercise 3.3 and Corollary 3.2] that the conductor of L_i is $1+i+p^{s+1}$. So, $L_i \subset K_S^{1+i+p^{s+1}}$. To complete the proof, it remains to show that L has conductor m_2, which follows from [Garuti 2002] (see comments above).

The equations, conductor and degree of each extension L_i are as follows:

ext’n	conductor m	$[L_i{:}K]$	new equations
K	$0\le m\le r+1=p^s+1$	1	
L_0	$r+2\le m\le p^{s+1}+1=m_2-p$	p	$W_0^p-W_0=f_0(X)$
L_1	$m=p^{s+1}+2=m_2-(p-1)$	p^{1+e}	$W_1^q-W_1=f_1(X)$
L_2	$m=p^{s+1}+3=m_2-(p-2)$	p^{1+2e}	$W_2^q-W_2=f_2(X)$
. . .	. . . .	. . . .	. . . .
L_i	$m=p^{s+1}+i+1=m_2-(p-i)$	p^{1+ie}	$W_i^q-W_i=f_i(X)$
. . .	. . . .	. . . .	. . . .
L_{p-1}	$m=p^{s+1}+p=m_2-1$	$p^{1+(p-1)e}$	$W_{p-1}^q-W_{p-1}=f_{p-1}(X)$
L	$m=p^{s+1}+p+1=m_2$	$p^{2+(p-1)e}$	$[W_0,\, W_p]^p-[W_0,\, W_p]$ $=[f_0(X),0]$

2. See preceding table.

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

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

$$\begin{aligned}\wp(\sigma(W_0)-W_0)&=\sigma(\wp(W_0))-\wp(W_0)=f_0(X+y)-f_0(X)\\&=a\,y\,X^r+a\,y^r\,X+f_0(y)=-a^r\,y^{r^2}\,X^r+a\,y^r\,X+f_0(y)\\&=\wp(P_y(X))+f_0(y),\end{aligned}$$

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

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

$$\begin{aligned}(F^e-\mathrm{id})\,(\sigma(W_i)-W_i)&=\sigma(W_i^q-W_i)-(W_i^q-W_i)=f_i(X+y)-f_i(X)\\&=(X+y)^{ip^{s-1}}\,(X^q-X)-X^{ip^{s-1}}\,(X^q-X)\\&=(X^{p^{s-1}}+y^{p^{s-1}})^i\,(X^q-X)-X^{ip^{s-1}}\,(X^q-X)\\&=\sum_{j=1}^{i-1}\binom{i}{j}\,y^{(i-j)p^{s-i}}\,f_j(X)\quad\bmod\ (F^e-\mathrm{id})\,(\mathbb{F}_q[X]),\end{aligned}$$

where the sum is empty for $i = 1$. It turn, the right-hand side equals

$$(F^e - \mathrm{id})\Big(\sum_{j=1}^{i-1} \binom{i}{j}\, y^{(i-j)p^{s-i}}\, W_j\Big) \quad \mathrm{mod}\ (F^e - \mathrm{id})\,(\mathbb{F}_q[X]).$$

It follows that $\sigma(W_i) \in L_i = \mathbb{F}_q(X, W_0, W_1, \dots, W_i)$.

(c) We next show, using Remark 6.3.4, that $\sigma(W_p) \in L$. To this end, set

$$\Delta := \wp(\sigma\,[W_0, W_p] - [W_0, W_p]),$$

so

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

We know from the proof of part 1 that $[f_0(y), 0]$ lies in $\wp(W_2(\mathbb{F}_q))$. Then

$$\Delta = [f_0(X+y), 0] - [f_0(X), 0] - [f_0(y), 0] - [P_y(X), 0] + [P_y(X), 0]^p \qquad \mathrm{mod}\ \wp(W_2(\mathbb{F}_q[X])),$$

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 $\tilde{y}$ the Witt vector $\tilde{y} := (y, 0, 0, \dots) \in W(k)$. For any $P(X) := \sum_{i=0}^{s} a_i\, X^i \in \mathbb{F}_q[X]$, set $\tilde{P}(X) := \sum_{i=0}^{s} \tilde{a}_i\, X^i \in W(\mathbb{F}_q)[X]$. Addition in the ring of Witt vectors yields

$$\Delta = [0, A] \quad \mathrm{mod}\ \wp(W_2(\mathbb{F}_q[X])),$$

where A is the reduction modulo $p\,W_2(\mathbb{F}_q)[X]$ of

$$\frac{1}{p}\{\tilde{f}_0(X+\tilde{y})^p - \tilde{f}_0(X)^p - \tilde{f}_0(\tilde{y})^p + \tilde{P}_y(X)^p - \tilde{P}_y(X)^{p^2} \\ - (\tilde{f}_0(X+\tilde{y}) - \tilde{f}_0(X) - \tilde{f}_0(\tilde{y}) - \tilde{P}_y(X) + \tilde{P}_y(X)^p)^p\}.$$

Since $\tilde{f}_0(X+\tilde{y}) - \tilde{f}_0(X) - \tilde{f}_0(\tilde{y}) + \tilde{P}_y(X) - \tilde{P}_y(X)^p = 0 \bmod p\,W(\mathbb{F}_q)[X]$, we get

$$A = \frac{1}{p}\,\{\tilde{f}_0(X+\tilde{y})^p - \tilde{f}_0(X)^p - \tilde{f}_0(\tilde{y})^p + \tilde{P}_y(X)^p - \tilde{P}_y(X)^{p^2}\} \quad \mathrm{mod}\ p\,W(\mathbb{F}_q)[X].$$

We observe that, modulo $\mathrm{mod}\ p^2\,W(\mathbb{F}_q)[X]$,

$$\begin{aligned}\tilde{f}_0(X+\tilde{y})^p &= \tilde{a}^p\,(X+\tilde{y})^p\,(X+\tilde{y})^{p^{s+1}} = \tilde{a}^p\,(X+\tilde{y})^p\,(X^{p^s} + \tilde{y}^{p^s})^p \\ &= \tilde{a}^p \sum_{i=0}^{p}\sum_{j=0}^{p} \binom{p}{i}\binom{p}{j}\, X^{j+ip^s}\, \tilde{y}^{p-j+p^s\,(p-i)}\end{aligned}$$

Since $\binom{p}{i}\binom{p}{j} = 0 \bmod p^2$ when $0 < i < p$ and $0 < j < p$, one obtains

$$\tilde{f}_0(X+\tilde{y})^p - \tilde{f}_0(X)^p - \tilde{f}_0(\tilde{y})^p = \tilde{a}^p \sum_{(i,j)\in I} \binom{p}{i}\binom{p}{j} X^{j+ip^s}\, \tilde{y}^{p-j+p^s\,(p-i)} \qquad \bmod p^2\, W(\mathbb{F}_q)[X],$$

where I is the set of $(i, j) \in \{0, 1, \dots, p\}^2 \setminus \{(0,0)\,, (p, p)\}$ such that

$$ij = 0 \mod p,\ (i, j).$$

Again modulo $\bmod p^2\, W(\mathbb{F}_q)[X]$, we have

$$\begin{aligned}\tilde{P}_y(X)^p - \tilde{P}_y(X)^{p^2} &= \Big(\sum_{i=0}^{s-1} (-\tilde{a}\,\tilde{y}^r\, X)^{p^i}\Big)^p - \Big(\sum_{i=0}^{s-1} (-\tilde{a}\,\tilde{y}^r\, X)^{p^i}\Big)^{p^2}\\ &= \Big(\sum_{i=0}^{s-1} (-\tilde{a}\,\tilde{y}^r\, X)^{p^i}\Big)^p - \Big(\sum_{i=0}^{s-1} (-\tilde{a}\,\tilde{y}^r\, X)^{p^{i+1}}\Big)^p\\ &= -\tilde{a}^p\,\tilde{y}^{rp}\,X^p + \tilde{a}^{rp}\,\tilde{y}^{r^2p}\,X^{pr} + p\,\tilde{T}_y(X),\end{aligned}$$

with $\tilde{T}_y(X) \in W(\mathbb{F}_q)[X]$. Since $y \in \mathbb{F}_q$ and $a \in \Gamma$, we get

$$\tilde{P}_y(X)^p - \tilde{P}_y(X)^{p^2} = -\tilde{a}^p\,\tilde{y}^{rp}\,X^p - \tilde{a}^p\,\tilde{y}^p\,X^{pr} + p\,\tilde{T}_y(X) \bmod p^2\, W(\mathbb{F}_q)[X].$$

As a consequence,

$$A = \tilde{a}^p \sum_{(i,j)\in I_1} \frac{1}{p}\binom{p}{i}\binom{p}{j} X^{j+ip^s}\,\tilde{y}^{p-j+p^s\,(p-i)} + \tilde{T}_y(X) \quad \bmod p\,\wp(\mathbb{F}_q[X]),$$

where $I_1 = I \setminus \{(0, p),\ (p, 0)\}$. Thus

$$A = a^p \sum_{(i,j)\in I_1} \frac{1}{p}\binom{p}{i}\binom{p}{j} X^{j+ip^s}\, y^{p-j+p^s\,(p-i)} + T_y(X),$$

with $T_y \in \mathbb{F}_q[X]$. We first consider the sum. Since, for $j = 0$, $j = p$ and $i = 0$, one gets monomials whose degree (possibly after reduction mod $\wp(\mathbb{F}_q[X])$) is lower than $1 + p^s$, one can write

$$A = a^p \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} X^{j+p^{s+1}}\, y^{p-j} + R_y(X) + T_y(X) \quad \bmod \wp(\mathbb{F}_q[X]),$$

where $R_y(X)$ is a polynomial of $\mathbb{F}_q[X]$ of degree lower than $1 + p^s = 1 + r$. We now focus on the polynomial $T_y(X) \in \mathbb{F}_q[X]$. It is made of monomials of the forms $X^{i_0+i_1p+\cdots+i_{s-1}p^{s-1}}$, with $i_0 + i_1 + \cdots + i_{s-1} = p$, and $X^{i_1p+\cdots+i_sp^s}$, with $i_1+i_2+\cdots+i_s = p$. Since $X^{i_1p+\cdots+i_s\,p^s} = X^{i_1+\cdots+i_sp^{s-1}} \bmod \wp(\mathbb{F}_q[X])$, it follows that T_y does not have any monomial with degree higher than $1 + p^s$ after reduction mod $\wp(\mathbb{F}_q[X])$. Hence

$$A = a^p \sum_{j=1}^{p-1} \frac{1}{p} \binom{p}{j} X^{j+p^{s+1}} y^{p-j} + R_y^{[1]}(X) \mod \wp(\mathbb{F}_q[X]),$$

where $R_y^{[1]}(X)$ is a polynomial of $\mathbb{F}_q[X]$ with degree strictly lower than $1+r$. Since $f_j(X) = X^{j+p^{s+1}} - X^{1+jp^{s-1}} \mod \wp(\mathbb{F}_q[X])$ for all j in $\{1, \dots, p-1\}$, we conclude that

$$A = a^p \sum_{j=1}^{p-1} \frac{1}{p} \binom{p}{j} y^{p-j} f_j(X) + R_y^{[2]}(X) \mod \wp(\mathbb{F}_q[X]),$$

where $R_y^{[2]}(X)$ is a polynomial of $\mathbb{F}_q[X]$ of degree lower than $1+r$. Then

$$A = \sum_{j=1}^{p-1} c_j(y) f_j(X) + R_y^{[2]}(X) \mod \wp(\mathbb{F}_q[X]),$$

with $c_j(y) := a^p \frac{1}{p} \binom{p}{j} y^{p-j} \in \mathbb{F}_q$. It follows that, modulo $\wp(\mathbb{F}_q[X])$,

$$A = \sum_{j=1}^{p-1} (F^e - \mathrm{id})(c_j(y) W_j) + R_y^{[2]}(X) = (F - \mathrm{id}) \sum_{j=1}^{p-1} P_j(W_j) + R_y^{[2]}(X),$$

where $P_j(W_j) = (\mathrm{id} + F + \cdots + F^{e-1})(c_j(y) W_j) \in \mathbb{F}_q[W_j]$. We gather that

$$\wp(\sigma [W_0, W_p] - [W_0, W_p]) \\ = \wp\Big(\Big[0, \sum_{j=1}^{p-1} P_j(W_j)\Big]\Big) + [0, R_y^{[2]}(X)] \mod \wp(W_2(\mathbb{F}_q[X])).$$

As a consequence, $[0, R_y^{[2]}(X)]$ lies in $\wp(W_2(K_S^{m_2}))$, so there exists $V \in K_S^{m_2}$ such that $V^p - V = R_y^{[2]}(X)$ Accordingly, $K(V)$ is a K-subextension of $K_S^{m_2}$ with conductor $1 + \deg(R_y^{[2]}(X)) \leq 1 + r$. In particular, $K(V) \subset K_S^{r+1} = K = \mathbb{F}_q(X)$, which implies that $R_y^{[2]}(X) \in \wp(K)$. Therefore,

$$\wp(\sigma [W_0, W_p] - [W_0, W_p]) = \wp\Big(\Big[0, \sum_{j=1}^{p-1} P_j(W_j)\Big]\Big) \mod \wp(W_2(K)),$$

which allows us to conclude that $\sigma(W_p)$ is in $L = K(W_0, W_1, \dots, W_p)$. This finishes the proof of Proposition 6.7.3.

4. Since $L \subset K_S^{m_2}$ and $L \not\subset K_S^{m_2-1}$, the formula in Proposition 6.5.3 yields

$$\begin{aligned}
g_L &= 1 + [L:K]\Big(-1 + \frac{m_2}{2}\Big) - \frac{1}{2}\sum_{j=0}^{m_2-1}[L \cap K_S^j : K] \\
&= 1 + p^{2+(p-1)e}\Big(-1 + \frac{p^{s+1}+p+1}{2}\Big) \\
&\qquad\qquad\qquad - \frac{1}{2}\Big(r+2+(m_2-p-(r+2)+1)p + \sum_{i=1}^{p-1} p^{1+ie}\Big) \\
&= \tfrac{1}{2}p^{2+(p-1)e}(p^{s+1}+p-1) - \frac{1}{2}\Big(p^s + p^{s+2} - p^{s+1} + \sum_{i=1}^{p-1} p^{1+i2s}\Big) \\
&= \tfrac{1}{2}p^{2+(p-1)e}(p^{s+1}+p-1) - \tfrac{1}{2}p^s(p^2-p+1) - \tfrac{1}{2}p^{2s+1}(1+q+q^2+\cdots+q^{p-2}).
\end{aligned}$$

5. See Proposition 6.5.4. □

Remark 6.8. For $p = 2$, the equations given in Proposition 6.7 become

$$\begin{aligned}
W_0^p - W_0 &= f_0(X) := X^{1+r}, \\
W_1^q - W_1 &= f_1(X) := X^{p^{s-1}}(X^q - X), \\
[W_0, W_2]^p - [W_0, W_2] &= [f_0(X), 0].
\end{aligned}$$

This last equation is no longer totally split over $\mathbb{F}_q$. One can circumvent this by replacing it with

$$[W_0, W_2]^p - [W_0, W_2] = [c^r X^{1+r}, 0] - [c\, X^{1+r}, 0] \quad \text{with} \quad c^r + c = 1.$$

In this case, we obtain the same results as in Proposition 6.7. The proof is left to the reader.

Proposition 6.7 can be generalized to construct a big action whose second ramification group G_2 is abelian of exponent as large as we want.

Proposition 6.9. *We keep the notation of Proposition 6.7. In particular, $q = p^e$, with $p > 2$, $e = 2s$ and $s \geq 1$. Let $n \geq 2$. Put $m_n := 1 + p^{n-1}(1 + p^s)$. If $q/(-1+m_n/2) > 2\,p/(p-1)$, the pair $(C(m_n), G(m_n))$, as defined in Proposition 6.5, is a big action with a second ramification group $G_S(m_n)$ abelian of exponent at least p^n.*

Proof. Proposition 6.5.4 first ensures that $(C(m_n), G(m_n)$ is a big action. Consider the p^n-cyclic extension $K(W_1, \ldots, W_n)/K$ parametrized with Witt vectors of length n as

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

where $f_0(X) = a\,X^{1+r}$ is defined as in Proposition 6.7, i.e., $r = p^s$, $a^r + a = 0$, $a \neq 0$. The same proof as in Proposition 6.7.1 shows that all places of S completely split in $K(W_1, \dots, W_n)$. Moreover, by [Garuti 2002] (Theorem 1.1) the conductor of the extension $K(W_1, \dots, W_n)$ is $1 + max\{p^{n-1}\,(1+p^s), 0\} = m_n$. It follows that $K(W_1, \dots, W_n)$ is included in $K_S^{m_n}$. Therefore, $G_S(m_n)$ has a quotient of exponent p^n and the claim follows. □

The next proposition is an analogue of Proposition 6.7 in the case where e is odd. We do not spell out the proof, which is in the main similar to the proof of Proposition 6.7. Note that, contrary to the case where e is even, the equations still work for $p = 2$.

Proposition 6.10. *We keep the notation defined above. In particular,* $K = \mathbb{F}_q(X)$ *with* $q = p^e$. *Assume that* $e = 2s - 1$, *with* $s \geq 2$, *and put* $r := \sqrt{qp} = p^s$. *We define*

$$f_i(X) = X^{ir/p}\,(X^q - X) = X^{ip^{s-1}}\,(X^q - X) \quad \textit{for all } i \in \{1, \dots, p-1\},$$
$$g_i(X) = X^{ir/p^2}\,(X^q - X) = X^{ip^{s-2}}\,(X^q - X) \quad \textit{for all } i \in \{1, \dots, p-1\}.$$

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*

$$W_i^q - W_i = f_i(X) \textit{for all } i \in \{1, \dots, p-1\},$$
$$V_j^q - V_j = g_j(X) \textit{for all } j \in \{1, \dots, p-1\},$$
$$[W_1, W_p]^p - [W_1, W_p] = [X^{1+p^s}, 0] - [X^{1+p^{s-1}}, 0].$$

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

1. *L is an abelian extension of K such that every place in S completely splits in L, satisfying* $L_{i,0} \subset K_S^{p^s+i+1}$ *for all* i, $j \in \{1, \dots, p-1\}$, $L_{p-1,j} \subset K_S^{p^{s+1}+j+1}$, *and* $L \subset K_S^{m_2}$, *where* $m_2 = p^{s+1} + p + 1$ *is the integer defined in Proposition 6.4.* (See table below on the next page.)
2. *The extension* L/K *has degree* $[L : K] = p^{2(p-1)e+1}$. *Let* G_L *be its Galois group. Then*

$$G_L \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \quad \textit{with } t = 2\,(p-1)\,e - 1.$$

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 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*

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

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

We gather here the conductors, degrees and equations of each extension:

ext'n	conductor m	$[L_{i,j}{:}K]$	new equations
K	$0\le m\le r+1=p^s+1$	1	
$L_{1,0}$	$m=r+2=p^s+2$	p^e	$W_1^q-W_1=f_1(X)$
. . . . . .	. . . . . .	. . . . . .	. . . . . .
$L_{i,0}$	$m=p^s+i+1$	p^{ie}	$W_i^q-W_i=f_i(X)$
. . . . . .	. . . . . .	. . . . . .	. . . . . .
$L_{p-1,0}$	$p^s+p\le m\le p^{s+1}+1$	$p^{(p-1)e}$	$W_{p-1}^q-W_{p-1}=f_{p-1}(X)$
$L_{p-1,1}$	$m=p^{s+1}+2=m_2-(p-1)$	p^{pe}	$V_1^q-V_1=g_1(X)$
. . . . . .	. . . . . .	. . . . . .	. . . . . .
$L_{p-1,j}$	$m=p^{s+1}+j+1=m_2-(p-j)$	$p^{(p+j-1)e}$	$V_j^q-V_j=g_j(X)$
. . . . . .	. . . . . .	. . . . . .	. . . . . .
$L_{p-1,p-1}$	$m=p^{s+1}+p=m_2-1$	$p^{2(p-1)e}$	$V_{p-1}^q-V_{p-1}=g_{p-1}(X)$
L	$m=p^{s+1}+p+1=m_2$	$p^{1+2\,(p-1)e}$	$[W_1,\,W_p]^p-[W_1,\,W_p]=$ $[X^{1+p^s},0]-[X^{1+p^{s-1}},0]$

7. A local approach to big actions

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 ∞, which means that the cover $\pi:C\to C/G$ is totally ramified at ∞. Moreover, the quotient curve C/G is isomorphic to the projective line $\mathbb{P}_k^1$ and π is étale above the affine line $\mathbb{A}_k^1=\mathbb{P}_k^1-\pi(\infty)=\operatorname{Spec}k[T]$. 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 (2–2) as $g=\frac{1}{2}\sum_{i\ge 2}(|G_i|-1)>0$. It follows that

$$\frac{|G|}{\sum_{i\ge 2}(|G_i|-1)}=\frac{|G|}{2g}>\frac{p}{p-1}.$$

This leads to:

Definition 7.1. A *local big action* is any pair $(k((Z)),G)$ where G is a finite p-subgroup of $\operatorname{Aut}_k(k((Z)))$ whose ramification groups in lower notation at ∞ satisfy the inequalities

$$g(G) := \frac{1}{2}\sum_{i\geq 2}(|G_i|-1) > 0 \qquad \text{and} \qquad \frac{|G|}{g(G)} > \frac{2p}{p-1}.$$

It follows from the Katz–Gabber Theorem (see [Katz 1986, Theorem 1.4.1] or [Gille 2000, corollaire 1.9]) that big actions (C, G) and local big actions $(k((Z)), G)$ are in one-to-one correspondence via the following functor induced by the inclusion $k[T] \subset k((T^{-1}))$:

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

Thus 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 deduce that G_2 is stricly included in G_1. Moreover, we obtain

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

References

[Auer 1999] R. Auer, *Ray class fields of global function fields with many rational places*, Ph.D. thesis, University of Oldenburg, 1999, Available at http://www.bis.uni-oldenburg.de/dissertation/fb06.html.

[Auer 2000] R. Auer, "Ray class fields of global function fields with many rational places", *Acta Arith.* **95**:2 (2000), 97–122. MR 2002e:11162 Zbl 0963.11067

[Bertin and Mézard 2000] J. Bertin and A. Mézard, "Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques", *Invent. Math.* **141**:1 (2000), 195–238. MR 2001f:14023 Zbl 0993.14014

[Bertin and Romagny 2008] J. Bertin and M. Romagny, "Champs d'Hurwitz", preprint, 2008, Available at http://people.math.jussieu.fr/~romagny/champs_de_hurwitz.pdf.

[Bourbaki 1983] N. Bourbaki, *Algèbre commutative, Chapitres 8 et 9*, Masson, Paris, 1983.

[Bouw 2000] I. I. Bouw, "The p-rank of curves and covers of curves", pp. 267–277 in *Courbes semi-stables et groupe fondamental en géométrie algébrique* (Luminy, 1998), edited by J.-B. Bost et al., Progr. Math. **187**, Birkhäuser, Basel, 2000. MR 2001j:14042 Zbl 0979.14015

[Breuer 2000] T. Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Mathematical Society Lecture Note Series **280**, Cambridge University Press, Cambridge, 2000. MR 2002i:14034 Zbl 0952.30001

[Conder 1990] M. Conder, "Hurwitz groups: a brief survey", *Bull. Amer. Math. Soc.* (*N.S.*) **23**:2 (1990), 359–370. MR 91d:20032 Zbl 0716.20015

[Cornelissen and Kato 2003] G. Cornelissen and F. Kato, "Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic", *Duke Math. J.* **116**:3 (2003), 431–470. MR 2004c:14044 Zbl 1092.14032

[Elkies 1999a] N. D. Elkies, "The Klein quartic in number theory", pp. 51–101 in *The eightfold way*, edited by S. Levy, Math. Sci. Res. Inst. Publ. **35**, Cambridge Univ. Press, Cambridge, 1999. MR 2001a:11103 Zbl 0991.11032

[Elkies 1999b] N. D. Elkies, "Linearized algebra and finite groups of Lie type, I: Linear and symplectic groups", pp. 77–107 in *Applications of curves over finite fields* (Seattle, 1997), edited by M. D. Fried, Contemp. Math. **245**, Amer. Math. Soc., Providence, RI, 1999. MR 2001a:20082 Zbl 0976.20032

[Garuti 2002] M. A. Garuti, "Linear systems attached to cyclic inertia", pp. 377–386 in *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, 1999), edited by M. D. Fried and Y. Ihara, Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, RI, 2002. MR 2003i:14014 Zbl 1072.14017

[Gille 2000] P. Gille, "Le groupe fondamental sauvage d'une courbe affine en caractéristique $p > 0$", pp. 217–231 in *Courbes semi-stables et groupe fondamental en géométrie algébrique* (Luminy, 1998), edited by J.-B. Bost et al., Progr. Math. **187**, Birkhäuser, Basel, 2000. MR 2002a:14027 Zbl 0978.14034

[Giulietti and Korchmáros 2007] M. Giulietti and G. Korchmáros, "On large automorphism groups of algebraic curves in positive characteristic", preprint, 2007. arXiv 0706.2320

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Math. (3) **35**, Springer, Berlin, 1996. MR 97i:11062 Zbl 0874.11004

[Huppert 1967] B. Huppert, *Endliche Gruppen, I*, Grundlehren der Math. Wiss. **134**, Springer, Berlin, 1967. MR 37 #302 Zbl 0217.07201

[Hurwitz 1892] A. Hurwitz, "Ueber algebraische Gebilde mit eindeutigen Transformationen in sich", *Math. Ann.* **41**:3 (1892), 403–442. MR 1510753

[Katz 1986] N. M. Katz, "Local-to-global extensions of representations of fundamental groups", *Ann. Inst. Fourier* (*Grenoble*) **36**:4 (1986), 69–106. MR 88a:14032 Zbl 0564.14013

[Kontogeorgis 2007] A. Kontogeorgis, "On the tangent space of the deformation functor of curves with automorphisms", *Algebra Number Theory* **1**:2 (2007), 119–161. MR 2008j:14056

[Kulkarni 1997] R. S. Kulkarni, "Riemann surfaces admitting large automorphism groups", pp. 63–79 in *Extremal Riemann surfaces* (San Francisco, 1995), edited by J. R. Quine and P. Sarnak, Contemp. Math. **201**, Amer. Math. Soc., Providence, RI, 1997. MR 98g:30070 Zbl 0863.30050

[Lauter 1999] K. Lauter, "A formula for constructing curves over finite fields with many rational points", *J. Number Theory* **74**:1 (1999), 56–72. MR 99k:11088 Zbl 1044.11054

[Leedham-Green and McKay 2002] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series **27**, Oxford University Press, Oxford, 2002. Oxford Science Publications. MR 2003f:20028 Zbl 1008.20001

[Lehr and Matignon 2005] C. Lehr and M. Matignon, "Automorphism groups for p-cyclic covers of the affine line", *Compos. Math.* **141**:5 (2005), 1213–1237. MR 2006f:14029 Zbl 1083.14028

[Macbeath 1961] A. M. Macbeath, "On a theorem of Hurwitz", *Proc. Glasgow Math. Assoc.* **5** (1961), 90–96. MR 26 #4244 Zbl 0134.16603

[Macbeath 1965] A. M. Macbeath, "On a curve of genus 7", *Proc. London Math. Soc.* (3) **15** (1965), 527–542. MR 31 #1605 Zbl 0146.42705

[Magaard et al. 2002] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, "The locus of curves with prescribed automorphism group", pp. 112–141 in *Communications in arithmetic fundamental groups* (Kyoto, 1999/2001), Sūrikaisekikenkyūsho Kōkyūroku **1267**, 2002. MR 1954371 arXiv math.0205314

[Marshall 1971] M. A. Marshall, "Ramification groups of abelian local field extensions", *Canad. J. Math.* **23** (1971), 271–281. MR 43 #189 Zbl 0211.06704

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, Princeton, 1980. MR 81j:14002 Zbl 0433.14012

[Nakajima 1987] S. Nakajima, "p-ranks and automorphism groups of algebraic curves", *Trans. Amer. Math. Soc.* **303**:2 (1987), 595–607. MR 88h:14037 Zbl 0644.14010

[Pries 2005] R. Pries, "Equiramified deformations of covers in positive characteristic", preprint, 2005. arXiv math.AG/0403056

[Rocher 2008a] M. Rocher, "Large p-group actions with a p-elementary abelian derived group", preprint, 2008. To appear in *J. Algebra*. arXiv 0801.3834

[Rocher 2008b] M. Rocher, "Large p-group actions with $|G|/g^2 \geq 4/(p^2-1)^2$", preprint, 2008. arXiv 0804.3494

[Schmid 1938] H. L. Schmid, "Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik.", *J. Reine Angew. Math.* **179** (1938), 5–15. Zbl 0019.00301

[Serre 1968] J.-P. Serre, *Corps locaux*, 2nd ed., Hermann, Paris, 1968. Translated as *Local fields*, Springer, New York, 1979. MR 50 #7096 Zbl 0174.24301

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Stichtenoth 1973a] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, I: Eine Abschätzung der Ordnung der Automorphismengruppe", *Arch. Math.* (*Basel*) **24** (1973), 527–544. MR 49 #2749 Zbl 0282.14006

[Stichtenoth 1973b] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, II: Ein spezieller Typ von Funktionenkörpern", *Arch. Math.* (*Basel*) **24** (1973), 615–631. MR 53 #8068 Zbl 0282.14007

[Stichtenoth 1993] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993. MR 94k:14016 Zbl 0816.14011

[Suzuki 1982] M. Suzuki, *Group theory, I*, Grundlehren der Math. Wiss. **247**, Springer, Berlin, 1982. MR 82k:20001c Zbl 0472.20001

[Suzuki 1986] M. Suzuki, *Group theory, II*, Grundlehren der Math. Wiss. **248**, Springer, New York, 1986. MR 87e:20001 Zbl 0586.20001

Communicated by Bjorn Poonen
Received 2008-02-01 Revised 2008-08-14 Accepted 2008-09-17

Michel.Matignon@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux,
Université de Bordeaux 1, 351 cours de la Libération,
33405 Talence Cedex, France
http://www.math.u-bordeaux1.fr/~matignon/

Magali.Rocher@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux,
Université de Bordeaux 1, 351 cours de la Libération,
33405 Talence Cedex, France
http://www.math.u-bordeaux.fr/~mrocher/