N° d'ordre : 3656

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX 1

Ecole doctorale de mathématiques et d'informatique

par Melle Magali Rocher

pour obtenir le grade de

DOCTEUR

Spécialité : Mathématiques pures

Courbes algébriques en caractéristique $p > 0$ munies d'un gros p-groupe d'automorphismes.

Soutenue publiquement le 14 novembre 2008,

Après avis de

M	Chinburg Ted, professeur, Université de Pennsylvanie	Rapporteur
M	Kontogeorgis Aristides, professeur, Université d'Athènes.	Rapporteur

Devant la commission d'examen formée de

M	Debes Pierre, professeur, Université de Lille 1	Président
M	Kontogeorgis Aristides, professeur, Université d'Athènes	Rapporteur
M	Liu Qing, professeur Université de Bordeaux 1	Examinateur
M	Matignon Michel, professeur, Université de Bordeaux 1	Directeur
Mme.	Mezard Ariane, professeur, Université de Versailles-Saint-Quentin	Examinatrice
M	Ritzenthaler Christophe, maître de conférences , Université de Marseille 2	Examinateur.

Table des matières

Remerciements.

L'aventure (mathématique, mais aussi humaine) de ces trois années de thèse n'aurait pu débuter sans la confiance qu'a su placer en moi celui qui, après avoir été mon enseignant durant mon année de préparation à l'agrégation, a accepté de devenir mon directeur de thèse. Je remercie Michel Matignon pour la confiance qu'il m'a accordée, mais aussi pour sa disponibilité sans faille, sa patience rare, son immense générosité et sa bonne humeur inconditionnelle qui ont su rendre moins fastidieux de longues journées et de longs week-end de travail. Sur une route jallonnée de moments de doute et de découragement, son dynamisme et son entrain si communicatifs ont toujours su remotiver mon ardeur au travail. Je dois enfin confesser mon admiration et mon respect pour son inépuisable culture mathématique nourrie d'une profonde passion de la recherche et d'une insatiable curiosité intellectuelle.

Mes remerciements vont ensuite à Ted Chinburg et Aristides Kontogeorgis qui, malgré leur charge de travail et leurs obligations respectives, ont bien voulu être les rapporteurs de cette thèse. Je remercie également Pierre Debes, Qing Liu, Ariane Mézard et Christophe Ritzenthaler qui m'ont fait l'honneur d'accepter d'être membre de mon jury.

Je voudrais exprimer ma reconnaissance à Sylvain Maugeais et Matthieu Romagny pour leur relecture attentive de mon manuscrit et les précieux conseils qu'ils m'ont prodigués durant la rédaction du chapitre introductif, chapitre qui a fait prendre conscience à la novice que je suis l'étendue des connaissances et des techniques qu'il me reste encore à découvrir. Néanmoins, face au sphinx mathématique, je sais que je pourrais trouver parmi les personnes citées plus haut, des alliés précieux toujours prêts à nouer le dialogue et à m'offrir leurs lumières. A tous ces interlocuteurs, auxquels je me dois de rajouter Irene Bouw et Stefan Wewers, je voudrais exprimer ma gratitude pour leur patience et leur attention.

Sur la route qui m'a conduite à cette thèse, il faudrait sans doute chercher en amont tous les professeurs de sciences, de lettres ou autres, qui, du plus loin qu'il m'en souvienne, ont su cultiver en moi le goût -presque esthétique, presque mystique- de la connaissance et de la réflexion, la curiosité du savoir et des choses de l'esprit, tout cela conjugué avec un plaisir du travail, ce travail qui, loin de l'instrument de torture caché derrière son étymologie, m'est apparu comme l'une des clefs de la satisfaction personnelle et de l'épanouissement de l'esprit. Pour citer Mazarine Pingeot, "étais-je vraiment en train de passer à côté de ma vie, ou de forer d'autres profondeurs, d'explorer d'autres mondes qui n'étaient qu'un détour pour mieux y revenir, à cette vie ?"

Si la genèse de cette thèse tient à des rencontres mathématiques et intellectuelles, elle trouve aussi son origine en un lieu, le laboratoire de l'I.M.B., qui pendant quatre années, m'a offert des conditions de travail particulièrement agréables et propices, depuis un bureau confortable, douillet, lumineux, jusqu'à un parc, paisible "trou de verdure" silencieux au sein duquel je prenais plaisir à laisser vagabonder mes pensées.
Mon séjour au sein du laboratoire me laissera ainsi le souvenir d'une aventure forte et enrichissante dans bien des domaines de l'esprit. Ces murs auront été pour moi le théâtre de rencontres singulières, lesquelles auront incontestablement transformé ma manière d'envisager l'enseignement, la recherche, mais aussi bien d'autres champs de la pensée. Je remercie ainsi tous les membres du laboratoire, professeurs et doctorants, avec lesquels j'ai pu partager des discussions cocasses, lorsque, après des heures de dur labeur, devenait pressant le besoin de se détendre, mais aussi à l'occasion des discussions plus profondes sur des sujets mathématiques, littéraires, sociaux ou psychologiques.

Parmi tous mes anciens professeurs, je tiens à rendre un hommage appuyé et chaleureux à Jean Fresnel dont il convient de saluer la remarquable générosité à l'égard des étudiants et des collègues, chacun pouvant venir à toute heure le consulter sans jamais craindre de le lasser ni de le trouver à court d'idées. Sa culture mais aussi sa bonne humeur et son humour en font un interlocuteur aussi précieux qu'agréable.

Un grand merci à l'équipe des ingénieurs informatiques qui m'a toujours accueillie avec le sourire et dont l'aide fut précieuse face aux imprévisbles facéties des outils modernes. Une pensée également pour un service de secrétariat affable et efficace, en particulier pour Madame Bergerot dont la gentillesse ne s'est jamais démentie depuis le temps où je l'ai connue étudiante.

Merci enfin à mes étudiants qui ont entretenu mon goût pour l'enseignement. S'ils auront, je l'espère, un peu appris tandis que je m'évertuais craie en main, pour moi tout du moins ce contact n'aura pas été vain, puisqu'il m'a donné l'occasion de réfléchir sur ma discipline, ma manière de l'appréhender et ma capacité à la restituer. Que vaudrait un savoir que l'on ne pourrait pas transmettre, quel prix aurait une connaissance que l'on n'aurait nul plaisir à partager ?

Mes pensées vont enfin à ma famille : mes parents, mon frère, ma grand-mère, à tous mes amis, sans oublier ceux qui ne sont plus parmi nous mais dont le souvenir demeure toujours aussi vivace dans mon coeur. Merci à chacun d'eux pour m'avoir permis de grandir dans un foyer heureux, insouciant et paisible, pour avoir facilité mes conditions de vie et de travail, pour m'avoir entouré de leur amour et de leur attention, comme un abri contre les orages et les tourments. Rien de tout cela n'aurait été possible sans leur confiance, leur dévotion et leur soutien. Même si ma prose barbare ne leur parle guère, je leur dédie chacune de ces lignes.

Chapitre 1

Chapitre introductif.

Soient k un corps algébriquement clos de caractéristique $p \geq 0$ et C une courbe algébrique projective lisse connexe définie sur k et de genre $g \geq 2$. Soit G un groupe (nécessairement fini) de k-automorphismes de C. L'objet de cette thèse est d'étudier l'action de G sur C en caractéristique positive $p > 0$ lorsque G est un p-groupe tel que $|G| > \frac{2p}{p-1}\, g$. Ce chapitre introductif vise principalement à replacer notre travail dans un contexte plus général et à justifier notre problématique : nous rappelons ainsi un certain nombre de résultats déjà connus mais aussi de questions ouvertes, et actuellement en discussion, autour des G-actions de courbes, en caractéristique nulle et en caractéristique positive $p > 0$ dans le cas d'une action modérée (paragraphe 1.1), puis en caractéristique positive $p > 0$ lorsque p divise l'ordre de G et qu'apparaît de la ramification sauvage (paragraphe 1.2). Dans le paragraphe suivant, nous expliquons les motivations initiales et les applications possibles, en particulier la recherche de groupes de monodromie maximaux (paragraphe 1.3). Nous terminons ce chapitre préliminaire par une présentation des résultats obtenus dans les trois chapitres suivants de la thèse (paragraphe 1.4).

1.1 La caractéristique nulle et le cas modéré.

1.1.1 Définitions et notations préliminaires.

On commence ici par donner quelques définitions et notations qui, sauf mention explicite du contraire, seront conservées tout au long de ce chapitre introductif. On note k un corps algébriquement clos de caractéristique $p \geq 0$, C une courbe algébrique projective lisse, connexe, définie sur k, de genre $g \geq 2$ et $\mathrm{Aut}_k(C)$ le groupe des k-automorphismes de C. Fixons G un groupe fini. L'action (supposée fidèle) du groupe G sur la courbe C est la donnée d'un morphisme injectif : $\phi : G \to \mathrm{Aut}_k(C)$. On peut donc toujours identifier G à un sous-groupe de $\mathrm{Aut}_k(C)$. Le couple (C, ϕ) est appelé une G-courbe. Deux G-courbes (C, ϕ) et (C', ϕ') sont équivalentes s'il existe un G-isomorphisme $f : C \to C'$, i.e. un isomorphisme tel que, pour tout $s \in G$ et tout $x \in C$, $f(\phi(s)x) = \phi'(s)f(x)$. Dans la suite, on omettra de mentionner le morphisme ϕ. Ainsi, pour alléger les notations, l'action sera notée de manière abrégée : $(s, x) \to sx$ et on parlera de la G-courbe C au lieu de la G-courbe (C, ϕ).

Soit $\pi : C \to C/G$ le revêtement galoisien de groupe G associé à la G-courbe C. Si $p > 0$, on suppose, dans cette première partie uniquement, que p ne divise pas l'ordre de G. Ceci implique en particulier que l'action est modérée, i.e. que p ne divise pas l'ordre des groupes d'inertie, le groupe d'inertie au point $x \in C$ étant le sous-groupe stabilisateur $G_x := \{s \in G, sx = x\}$. Un point $x \in C$ est appelé point de ramification si son groupe d'inertie G_x est non trivial. L'orbite d'un tel point est appelé orbite singulière. A tous les points de ramification d'une même orbite singulière, correspond exactement un point de branchement $y \in C/G$. Le nombre de points de branchement coïncide donc avec le nombre d'orbites singulières. Soit $x \in C$ un point de ramification. Le groupe d'inertie G_x est un groupe cyclique dont l'ordre est l'indice de ramification de x, lequel est premier à p. On note désormais $\{x_1, \ldots, x_r\}$ un système de représentants des orbites singulières de la G-courbe C, $\{y_1, \ldots, y_r\}$ les points de branchement correspondants et $\{n_1, \ldots, n_r\}$ les indices de ramification, i.e. les ordres des groupes d'inertie. On suppose les n_i rangés par ordre croissant. Le r-uplet $(n_1, \ldots, n_r)$ est alors appelé signature de la G-courbe C.

1.1.2 Introduction à l'étude des groupes d'automorphismes des surfaces de Riemann compactes.

Avec Schwarz, Klein, Hurwitz, Wiman et d'autres, le XIX ième siècle a vu émerger bon nombre de travaux consacrés à l'étude des groupes d'automorphismes des surfaces de Riemann compactes. Sans être exhaustif, nous rappelons ici quelques-uns des jalons qui ont marqué cette histoire.

Dans ce paragraphe, k est le corps des nombres complexes $\mathbb{C}$. Pour tout $g_0 \geq 0$, il existe, à homéomorphisme près, une unique surface réelle X_{g_0} compacte, connexe et orientée de genre g_0 (cf. [Se92] § 6.2). Cette surface X_{g_0} admet une présentation standard comme polygone à $2g_0$ arêtes notées $a_1, b_1, a_1^{-1}, b_1^{-1}, \dots, a_{g_0}, b_{g_0}, a_{g_0}^{-1}, b_{g_0}^{-1}$ identifiées de manière adéquate. De cette description, on déduit une présentation du groupe fondamental $\pi_1(X_{g_0})$ donnée par $2\,g_0$ générateurs $a_1, b_1, \dots, a_{g_0}, b_{g_0}$ liés par la relation :

$$\prod_{i=1}^{g_0} [a_i, b_i] = 1,$$

où $[a_i, b_i]$ désigne le commutateur de a_i et de b_i, i.e. $[a_i, b_i] = a_i\, b_i\, a_i^{-1}\, b_i^{-1}$ ([Se92] 6.2). Soit $\{y_1, \dots, y_r\}$ un ensemble de $r \geq 0$ points de X_{g_0}. Soit $\pi_1(g_0, r)$ le groupe fondamental de la courbe $X_{g_0} - \{y_1, \dots, y_r\}$. Chaque point y_i définit dans $\pi_1(g_0, r)$ une classe de conjugaison C_i correspondant au lacet entourant le point y_i dans une direction fixée. On montre que le groupe fondamental $\pi_1(g_0, r)$ admet une présentation donnée par $2g_0 + r$ générateurs $a_1, b_1, \dots, a_{g_0}, b_{g_0}, c_1, \dots, c_r$ liés par la relation :

$$\prod_{j=1}^{g_0} [a_j, b_j] \prod_{i=1}^{r} c_i = 1, \tag{1.1}$$

où chaque c_i appartient à C_i ([Se92], § 6.2).

1.1.3 Finitude du groupe des automorphismes et borne d'Hurwitz.

Désormais, C est une surface de Riemann compacte de genre $g \geq 2$, $\mathrm{Aut}(C)$ le groupe des automorphismes (analytiques, ou, de manière équivalente, algébriques) de C et G un sous-groupe de $\mathrm{Aut}(C)$. Les courbes C (resp. C/G) sont homéomorphes à X_g (resp. X_{g_0}) comme définis ci-dessus. En reliant les caractéristiques d'Euler des surfaces X_g et X_{g_0} (cf. [FaKa92] p.21), on obtient la formule dite de Riemann-Hurwitz reliant le genre g de C, le genre g_0 de la courbe quotient C/G et la signature $(n_1, \dots, n_r)$:

$$2\,(g-1) = 2\,|G|\,(g_0 - 1) + |G| \sum_{i=1}^{r} (1 - \frac{1}{n_i}). \tag{1.2}$$

Un groupe fini G est alors groupe d'automorphismes d'une surface de Riemann compacte de genre $g \geq 2$ si et seulement si G est image d'un groupe $\pi_1(g_0, r)$ admettant une présentation comme celle donnée par la formule (1.1). Dans ce cas, g_0 est le genre de la courbe quotient C/G, $y_1, \dots, y_r$ correspondent aux points de branchement du revêtement : $C \to C/G$ et les images des éléments c_i sont les générateurs des groupes d'inertie G_{x_i} ([Se92] Thm. 6.3.2).

Un autre résultat capital est la finitude du groupe des automorphismes d'une surface de Riemann compacte de genre $g \geq 2$. En effet, le groupe $\mathrm{Aut}(C)$ agit sur l'ensemble fini des points de Weierstrass de C. Cette action est fidèle, sauf lorsque C est hyperelliptique, auquel cas le noyau de l'action est d'ordre 2, engendré par l'involution hyperelliptique de C. Schwarz démontre ainsi que le groupe $\mathrm{Aut}(C)$ est fini. De la formule de Riemann-Hurwitz, Hurwitz ([Hur92]) déduit ensuite une borne linéaire pour l'ordre de ce groupe :

$$|\mathrm{Aut}(C)| \leq 84\,(g-1). \tag{1.3}$$

Cette borne est optimale et les courbes atteignant la borne d'Hurwitz sont appelées courbes d'Hurwitz et leur groupe d'automorphismes des groupes d'Hurwitz. Un groupe fini est groupe d'Hurwitz si et seulement s'il admet un système de générateurs : a, b, c, d'ordre respectif 2, 3 et 7 avec $abc = 1$. Les groupes d'Hurwitz ont encore fait l'objet de nombreux travaux dont un aperçu est donné dans [Con90].

On ne sait classifier les courbes d'Hurwitz que pour de petits genres. Ainsi, la seule courbe d'Hurwitz de genre $g \leq 3$ est la quartique de Klein (cf. [Kl79] et [El99]). Son groupe d'automorphismes est isomorphe à $\mathrm{PSL}_3(\mathbb{F}_2)$. Fricke a montré que la courbe d'Hurwitz suivante apparaissait pour $g = 7$ et que son groupe d'automorphismes était isomorphe à $\mathrm{SL}_2(\mathbb{F}_8)$. En 1965, Macbeath ([Mc65]) a donné des équations du plongement canonique de la courbe correspondante. La quartique de Klein et la courbe de Fricke-Macbeath sont les deux seules courbes d'Hurwitz dont les équations sont connues. Les courbes d'Hurwitz suivantes apparaissent pour $g = 13$ et $g = 17$. En 2001, Larsen ([Lar01]) a démontré que la suite des genres g des courbes d'Hurwitz se comportait asymptotiquement comme le cube des entiers.

1.1.4 Groupes d'automorphismes dits "larges" et "super-larges".

Soit C une surface de Riemann compacte de genre $g \geq 2$. Si l'on cherche à réaliser une classification des groupes G d'automorphismes de C, une idée, déjà suggérée par l'étude des courbes d'Hurwitz, est de considérer des groupes G suffisamment larges : grâce à la formule de Riemann-Hurwitz, ceci permet en effet de rigidifier la situation de ramification. Ainsi, si G est un groupe "large", i.e. d'ordre strictement supérieur à $4(g-1)$, la courbe quotient C/G est de genre $g_0 = 0$ et le nombre de points de branchements r du revêtement $C \to C/G$ est 3 ou 4 (cf. [Ku91]). Kulkarni dresse alors la liste des signatures $(n_1, n_2, \dots, n_r)$ possibles ([Ku91], Prop. 4.2). Si l'on considère à présent un groupe "super-large", c'est-à-dire d'ordre strictement supérieur à $12(g-1)$, Kulkarni montre que $g_0 = 0$, $r = 3$ et donne les signatures possibles ([Ku91], Prop. 4.6). Breuer fait de même lorsque G vérifie $|G| \geq 24\,(g-1)$ (cf. [Br00] Lemme 3.18).

1.1.5 Action de $\mathrm{Aut}(C)$ sur le module des différentielles.

Le choix de groupes d'automorphismes suffisamment larges permet ainsi de rigidifier la situation de ramification en imposant de fortes restrictions sur le genre g_0 de la courbe quotient et les données de ramification du revêtement $C \to C/G$. Grâce aux résultats rappelés dans le paragraphe 1.2, on sait de plus que ces groupes sont quotients des groupes fondamentaux $\pi_1(g_0, r)$ dont une présentation est donnée par (1.1). Pour dresser une classification de ces groupes d'automorphismes, on considère les représentations associées à l'action fidèle de ces groupes sur $H^0(C, \Omega_C)$, l'espace vectoriel, de dimension g sur $\mathbb{C}$, des formes différentielles holomorphes de C (cf. [FaKa92] p. 270 ou [Br00] p. 41). En effet, les sous-groupes finis de $\mathrm{GL}_g(\mathbb{C})$ résultant de cette action satisfont un certain nombre de conditions étudiées par I. Kuribayashi, A. Kuribayashi, Kimura, Ohmori, Kobayashi... A. Kuribayashi et Kimura ([KuKi90]) ont ainsi dressé une liste complète de ces groupes linéaires finis jusqu'au genre $g \leq 5$. A l'aide du logiciel de calcul GAP, Breuer ([Br00]) a étendu cette classification jusqu'au genre 48, listant tous les caractères des représentations induites par l'action des groupes, et par suite les groupes correspondants.

Dans la liste de Breuer, on trouve des groupes d'automorphismes $\mathrm{Aut}(C)$ mais aussi tous leurs sous-groupes. Magaard et alii ([MSSV02]) ont identifié dans la liste les groupes qui sont exactement des groupes d'automorphismes d'une surface de Riemann de genre g. Ils obtiennent ainsi la liste des groupes d'automorphismes $\mathrm{Aut}(C)$ en genre 3 et donnent les équations des courbes correspondantes. Ils poursuivent la liste des groupes d'automorphismes jusqu'au genre 10 sous l'hypothèse supplémentaire que le groupe est large, i.e. $|\mathrm{Aut}(C)| > 4(g-1)$. Ils précisent de plus la dimension et le nombre des composantes connexes du lieu correspondant dans l'espace de modules des courbes de genre g.

Le fait que le groupe des automorphismes opère de manière fidèle sur l'espace vectoriel des formes différentielles holomorphes, reste vrai en caractéristique $p > 0$ (cf. [HKT08] Lemme 11.12 et Théorème 11.23). D'autre part, un résultat dû à Chevalley-Weil, généralisé par Nakajima (1984) et Kani (1986) dans le cas modéré puis par Kock (2004) dans le cas de la ramification faible, i.e. dans le cas où le deuxième groupe de ramification en tout point est trivial, permet de décrire la structure du G-module $H^0(C, \Omega_C)$ (cf. [Bor01]). Borne ([Bor06]) et Kontogeorgis ([Kon06]) ont tenté de généraliser cela au cas de caractéristique $p > 0$.

1.1.6 Action de $\mathrm{Aut}(C)$ sur le premier groupe d'homologie.

Soit C une surface de Riemann compacte, connexe, de genre $g \geq 1$. On étudie ici l'action fidèle de $\mathrm{Aut}(C)$ sur $H_1(C)$ le premier groupe d'homologie (cf. [FaKa92] § V.3), afin d'identifier $\mathrm{Aut}(C)$ à un sous-groupe fini du groupe symplectique $\mathrm{Sp}_{2g}(\mathbb{Z})$. En effet, le groupe $H_1(C)$ est muni d'une forme bilinéaire alternée non dégénérée, à valeurs dans $\mathbb{Z}$, liée à l'intersection des cycles. Cette forme bilinéaire est conservée par les éléments de $\mathrm{Aut}(C)$. On en déduit un homomorphisme $h : \mathrm{Aut}(C) \to \mathrm{Sp}_{2g}(\mathbb{Z})$ (cf. [FaKa92] p. 287), où $\mathrm{Sp}_{2g}(\mathbb{Z})$ désigne le groupe des matrices symplectiques de $\mathrm{GL}_{2g}(\mathbb{Z})$, i.e. les matrices $S \in \mathrm{GL}_{2g}(\mathbb{Z})$ vérifiant : $S\,J_0\,{}^tS = J_0$ avec

$$J_0 := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Cet homomorphisme est injectif pour $g \geq 2$. Ceci nous permet en particulier d'identifier les groupes $\mathrm{Aut}(C)$ avec des sous-groupes finis de $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Si $g \geq 2$ et $n \geq 3$, l'homomorphisme $h_n : \mathrm{Aut}(C) \to \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$, déduit de h par réduction modulo n, est encore injectif ([FaKa92] p. 293). Nous verrons au paragraphe 1.2.2 que ces résultats se généralisent au cas de la caractéristique $p > 0$, en considérant cette fois l'action du groupe des automorphismes d'une courbe lisse (ou simplement stable, sans partie torique) C de genre g sur les points de ℓ-torsion du schéma de Picard : $\mathrm{Pic}^0(C)$, pour ℓ un nombre premier distinct de 2 et de p.

1.1.7 Les données d'Hurwitz.

Revenons à présent au cas général d'une courbe algébrique C projective lisse, connexe, définie sur un corps k algébriquement clos de caractéristique $p \geq 0$, et de genre $g \geq 2$. Soit G un groupe d'automorphismes de C. Si $p > 0$, on suppose comme précédemment que p ne divise pas l'ordre de G. Pour mener l'étude des déformations de la G-courbe C, il est utile d'introduire les données d'Hurwitz (cf. [BeRo08]). Soit x un point de ramification de C. Le groupe d'inertie G_x, comme défini dans les préliminaires, est muni d'une représentation fidèle de degré 1 :

$$\chi_x : G_x \to \mathrm{GL}(M_x/M_x^2) \simeq k^*$$

du groupe cyclique G_x dans l'espace cotangent de C au point x, M_x désignant l'idéal maximal de l'anneau local $O_{C,x}$. Le caractère de la représentation, lui aussi noté χ_x, est primitif, i.e. d'ordre $|G_x|$. Ceci nous amène à considérer l'ensemble des couples (H, χ), où H est un sous-groupe cyclique de G et χ un caractère primitif de H. Deux couples (H, χ) et (H', χ') sont dits conjugués s'il existe $s \in G$ tel que :

$$H' = sHs^{-1} \quad \text{et} \quad \chi'(sts^{-1}) = \chi(t) \quad \forall\, t \in H.$$

Ainsi, si $y = sx$, avec $s \in G$, alors (G_y, χ_y) et (G_x, χ_x) sont conjugués. Ceci permet de définir le G-type d'une orbite singulière, disons l'orbite de x, comme étant la classe de conjugaison de (G_x, χ_x), désormais notée $[G_x, \chi_x]$. Décomposons à présent l'ensemble des points de ramification F en une réunion d'orbites (les orbites singulières correspondant chacune à un point de branchement) : $F = F_1 \cup F_2 \cup \ldots \cup F_r$, et notons $[H_i, \chi_i]$ le type de F_i. On appelle donnée d'Hurwitz de l'action de G sur C la collection des classes de conjugaison $\{[H_i, \chi_i], 1 \leq i \leq r\}$, de type distincts ou non, des r orbites singulières. Lorsque $r = 0$, c'est à dire lorsque le revêtement $C \to C/G$ est étale, la donnée d'Hurwitz correspondante est dite vide. On dit qu'une G-courbe C est de type (g, G, ξ) si C est de genre g et a pour donnée d'Hurwitz ξ. Autrement dit, si l'on note $\{x_1, \ldots, x_r\}$ un système de représentants des orbites singulières de la G-courbe C et si ξ s'écrit $\xi = \{[H_i, \chi_i], 1 \leq i \leq r\}$, alors $[G_{x_i}, \chi_{x_i}] = [H_i, \chi_i]$.

Fixons $g \geq 2$ et ξ une donnée d'Hurwitz. D'après Bertin [Be96], il existe un schéma quasi projectif des modules $H_{g,G,\xi}$ sur k pour les G-courbes lisses de type (g, G, ξ). Les composantes connexes sont précisément les composantes irréductibles de $H_{g,G,\xi}$. Leur nombre, appelé nombre de Nielsen, ne dépend pas du corps de base k algébriquement clos. Soit $H_{g,G,r}$ le module des G-courbes C de genre g et de signature $(n_1, n_2, \ldots, n_r)$: celui-ci est réunion disjointe des espaces d'Hurwitz $H_{g,G,\xi}$, où ξ parcourt les données d'Hurwitz de cardinal r ([BeRo08], § 6.2). Si C est une G-courbe de type (g, G, ξ), la formule (1.2) nous assure que le genre g_0 de C/G ne dépend que de g, de l'ordre de G et de la signature : $(n_1, \ldots, n_r)$. En particulier, g_0 ne dépend pas de la composante connexe.

Nous avons vu également dans la partie 1.1.2 que $H_{g,G,\xi}$ est non vide si et seulement si G est engendré par des éléments $a_1, b_1, \ldots, a_{g_0}, b_{g_0}, c_1 \ldots, c_r$ tels que :

$$\forall\, i \in \{1, \ldots, r\},\ H_i = \langle c_i \rangle \quad \text{et} \quad \prod_{j=1}^{g_0} [a_j, b_j] \prod_{i=1}^{r} c_i = 1.$$

On remarque en particulier que lorsque $g_0 = 0$, la condition se limite au fait que chaque H_i soit engendré par c_i et que $\prod_{i=1}^{r} c_i = 1$.

On considère à présent deux morphismes : le morphisme d'oubli de l'action de G :

$$\Phi :\ H_{g,G,\xi} \to M_g,$$

où M_g désigne l'espace des modules des courbes de genre g et le morphisme discriminant :

$$\Psi :\ H_{g,G,\xi} \to M_{g_0,r},$$

où $M_{g_0,r}$ désigne l'espace des modules des courbes de genre g_0 avec r points distincts marqués. Le morphisme Ψ envoie ainsi une G-courbe C sur la classe de la courbe quotient C/G marquée par les r points de branchement du revêtement $C \to C/G$. Ces deux morphismes sont finis. De plus, si $H_{g,G,\xi}$ est non vide, le morphisme discriminant envoie chaque composante connexe de $H_{g,G,\xi}$ sur $M_{g_0,r}$. Ainsi, chacune de ces composantes connexes a la même dimension

$$\delta_{g,G,\xi} :=\ \dim M_{g_0,r} = 3\,g_0 - 3 + r. \tag{1.4}$$

L'image de Φ, notée $M_{g,G,\xi}$, coïncide avec le lieu dans M_g des courbes de genre g admettant une G-action de type (g, G, ξ). Comme Φ est fini, si $M_{g,G,\xi}$ est non-vide, alors chacune de ses composantes a aussi pour dimension $\delta_{g,G,\xi}$, nombre qui ne dépend finalement que de g, de l'ordre de G et de la signature $(n_1, \ldots, n_r)$.

1.2 La caractéristique $p > 0$ et le cas de ramification sauvage.

1.2.1 La finitude du groupe des automorphismes.

Dans toute cette seconde partie, sauf mention explicite du contraire, k est un corps algébriquement clos de caractéristique $p > 0$ et C une courbe algébrique projective lisse, connexe, définie sur k, de genre $g \geq 2$. On note $\mathrm{Aut}_k(C)$ le groupe des k-automorphismes de C et G un sous-groupe de $\mathrm{Aut}_k(C)$. Si p est premier avec l'ordre de G, celui-ci est encore majoré par la borne d'Hurwitz ([Gro63]). Par contre, si p divise l'ordre de G, la borne d'Hurwitz n'est plus valable. Cependant, le groupe des automorphismes est encore un groupe fini ([Sch38]), dont l'ordre est borné par un polynôme en g (cf. [St73], [Sin74]).

1.2.2 Action de $\mathrm{Aut}_k(C)$ sur le groupe $\mathrm{Pic}^0(C)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$.

Dans ce paragraphe, on montre que l'on peut identifier le groupe des automorphismes $\mathrm{Aut}_k(C)$ à un sous-groupe fini de $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$. En effet, $\mathrm{Aut}_k(C)$ s'injecte dans le groupe des k-automorphismes du schéma de Picard : $\mathrm{Aut}_k(\mathrm{Pic}^0(C))$ (cf. [DeMu69]). Pour décrire $\mathrm{Aut}_k(C)$, on peut donc considérer son action sur les points de $\mathrm{Pic}^0(C)$. Ainsi, soit ℓ un nombre premier distinct de p et de 2 et soit $[\ell]$ la multiplication par ℓ dans $\mathrm{Pic}^0(C)$. Le noyau de $[\ell]$ est traditionnellement noté $\mathrm{Ker}\,[\ell] = \mathrm{Pic}^0(C)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$. On obtient ainsi un homomorphisme injectif (cf. [Se60]) :

$$h_\ell \ : \ \mathrm{Aut}_k(C) \hookrightarrow \mathrm{Aut}_k(\mathrm{Pic}^0[\ell]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_\ell).$$

On peut donc identifier $\mathrm{Aut}_k(C)$ à un sous-groupe fini de $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$. L'homomorphisme h_ℓ est aussi utilisé par Bertin et Mézard ([BeMe00], § 5) pour construire un espace de modules fin $\mathcal{M}_{g,\ell}[G]$ avec structure de niveau $G \hookrightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ pour les revêtements galoisiens de groupe G. Si l'on introduit le pairing de Weil (cf. [Mi80], § 16), on généralise ainsi au cas de la caractéristique $p > 0$ l'injection de $\mathrm{Aut}(C)$ dans le groupe symplectique $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ obtenue en caractéristique nulle (voir § 1.1.6).

Cette action est susceptible de nous fournir une nouvelle borne sur l'ordre de $\mathrm{Aut}_k(C)$. Ainsi, en faisant varier ℓ, on obtient une borne sur la valuation p-adique v_p de $|\mathrm{Aut}_k(C)|$, et par suite sur l'ordre des p-sous-groupes de Sylow de $\mathrm{Aut}_k(C)$. Plus précisément, pour $p > 2$, Lehr et Matignon ([LM06b], § 3.3) montrent que :

$$v_p(|\mathrm{Aut}_k(C)|) \leq a + [\frac{a}{p}] + [\frac{a}{p^2}] + \dots \quad \text{avec} \quad a := [\frac{2g}{p-1}].$$

La notation $[x]$ désigne ici la partie entière du réel x. On renvoie à [LM06b] pour une formule analogue lorsque $p = 2$. La borne obtenue sur l'ordre des p-sous-groupes de Sylow de $\mathrm{Aut}_k(C)$ est ainsi exponentielle en g. Cette borne est très mauvaise pour les courbes lisses, si on la compare par exemple avec les bornes polynomiales de Stichtenoth (cf. [St73]). La raison en est que les énoncés précédents, en particulier l'injection, restent valables pour les courbes stables sans partie torique, i.e. les arbres de courbes lisses (cf. [DeMu69]). Lehr et Matignon ([LM06b], § 3.3) montrent d'ailleurs que cette borne exponentielle est optimale puisqu'elle est atteinte pour certaines courbes stables ayant beaucoup de composantes irréductibles.

1.2.3 La conjecture d'Abhyankar : l'existence de revêtements galoisiens de groupe G.

On se demande à présent quels groupes G peuvent apparaître comme groupe d'automorphismes. Dans ce paragraphe, k est un corps algébriquement clos de caractéristique $p > 0$ et X une courbe algébrique projective lisse, connexe, définie sur k et de genre g quelconque. On fixe $\{x_1, \dots, x_r\}$ un ensemble de r points de X. Soit Y une courbe projective lisse et connexe et $\phi : Y \to X$ un revêtement galoisien de groupe G, dont les points de branchement sont les x_i. Un problème important est de déterminer les groupes G pour lesquels un tel revêtement ϕ existe et, dans ce cas, de préciser la filtration de ramification associée à chaque point x_i. L'existence d'un tel revêtement dans le cas $r > 0$ fait l'objet de la conjecture d'Abhyankar ([Ab57]) formulée comme suit. Soit G un groupe fini et soit $p(G)$ le sous-groupe de G engendré par les p-sous-groupes de Sylow de G. Soit X une courbe projective lisse et connexe de genre g définie sur un corps algébriquement clos de caractéristique $p > 0$. Soit $\{x_1, \dots, x_r\}$ un ensemble fini de $r \geq 1$ points de X. Alors, il existe un revêtement $\phi : Y \to X$ galoisien de groupe G de courbes projectives lisses, étale sur $X - \{x_1, \dots, x_r\}$ si et seulement si le groupe quotient $G/p(G)$ peut être engendré par au plus $2g + r - 1$ générateurs.

Raynaud ([Ray94]) a démontré la conjecture pour la droite affine, i.e. pour $X = \mathbb{P}^1_k$ et $r = 1$. Harbater ([Har94]) en a déduit la preuve dans le cas général. Un problème non résolu demeure cependant celui de la détermination de la filtration de ramification correspondante. Ce problème a fait l'objet de travaux récents, notamment ceux de R. Pries ([Pr06]).

Examinons à présent le cas $r = 0$. Un p-groupe G est groupe de Galois d'un revêtement étale connexe de

X si et seulement si G est engendré par h éléments, où h est le p-rang de la jacobienne de X, autrement dit l'invariant de Hasse-Witt de X. Dans le cas plus général d'un groupe G dont l'ordre est divisible par p, on ne dispose pour l'heure que de résultats partiels (cf. [PaSt00]).

1.2.4 Classification des courbes avec de gros groupes d'automorphismes.

On reprend désormais les notations du paragraphe 1.2.1. La borne linéaire d'Hurwitz n'étant plus valable en caractéristique $p > 0$, on voit apparaître des courbes qui, à genre donné, ont de plus gros groupes d'automorphismes qu'en caractéristique nulle, phénomène qui s'explique par l'apparition de ramification sauvage. De nombreux travaux ont pour objet de classifier de telles courbes et de préciser leur groupe d'automorphismes. Sans être exhaustif, on peut citer [Roq70], [St73], [Hen78], [HaPe93], [HKT08] (Chap. 11.12)...

Lorsque $2 \leq g < p-1$, Roquette ([Roq70]) montre que la borne d'Hurwitz connaît une seule exception : la courbe d'équation $W^p - W = X^2$ avec $p \geq 5$. Dans cette situation, $g = \frac{1}{2}(p-1)$ et le groupe des automorphismes est extension centrale du groupe cyclique d'ordre 2 par $\mathrm{PGL}_2(\mathbb{F}_p)$. Ainsi, $|\mathrm{Aut}_k(C)| = 2\,p\,(p^2-1)$. Stichtenoth ([St73]) établit ensuite qu'en caractéristique $p > 0$, les seules courbes C pour lesquelles

$$|\mathrm{Aut}_k(C)| \geq 16\,g^4$$

sont les courbes hermitiennes :

$$X^{1+q} + Y^{1+q} + Z^{1+q} = 0 \quad \text{avec} \quad q = p^n,\ n \in \mathbb{N}^*,\ p^n \geq 3.$$

Dans ce cas, $g = \frac{1}{2}\,q\,(q-1)$ et $\mathrm{Aut}_k(C) \simeq \mathrm{PGU}_3(\mathbb{F}_{q^2}) \subset \mathrm{PGL}_3(\mathbb{F}_{q^2})$, i.e. le groupe unitaire lié à la forme hermitienne $(x,y,z) \to x\,x^F + y\,y^F + z\,z^F$, le Frobenius

$$F : \begin{cases} \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} \\ x \to x^q \end{cases}$$

étant une involution sur $\mathbb{F}_{q^2}$ (cf. [Leo96]). Ainsi, $|\mathrm{Aut}_k(C)| = q^3\,(q^3+1)\,(q^2-1)$. Enfin, Henn ([Hen78]) [1] donne une classification des courbes C telles que $|\mathrm{Aut}_k(C)| \geq 8\,g^3$. Celles-ci sont isomorphes soit à des courbes hyperelliptiques, soit à des courbes hermitiennes, soit à des courbes de Deligne-Lusztig (on renvoie à [Hen78] ou à [GK07] pour les équations de ces courbes et la description des groupes d'automorphismes correspondants).

1.2.5 La filtration de ramification.

La possibilité d'obtenir de plus gros groupes d'automorphismes en caractéristique positive s'explique par l'apparition de ramification sauvage. Mais l'apparition de ramification sauvage a aussi d'autres incidences. Ainsi, nous avons vu dans la première partie (§ 1.1.3) qu'en caractéristique nulle comme dans le cas d'une action modérée, le genre g_0 de la courbe quotient C/G ne dépend que de g, de l'ordre du groupe G et de la signature : $(n_1, \ldots, n_r)$, i.e. des ordres des groupes d'inertie (cf. formule (1.2)). En particulier, g_0 ne dépend pas de la composante connexe de $H_{g,G,r}$. Ce résultat n'est plus vrai en caractéristique $p > 0$, lorsque p divise l'ordre de G et plus précisément l'ordre des groupes d'inertie. Pour obtenir une formule analogue, il faut introduire la filtration de ramification inférieure du groupe G. Ainsi, si $x \in C$ est un point de ramification, on définit une suite décroissante de sous-groupes de G, appelés groupes de ramification inférieure de G en x ([St93] Def. III.8.5) :

$$\forall\, i \geq -1, \quad G_i(x) := \{\sigma \in G, v_x(\sigma(t_x) - t_x) \geq i+1\},$$

où t_x est un paramètre uniformisant au point x et v_x est la valuation en x. On appelle $G_{-1}(x)$ le groupe de décomposition de G en x, $G_0(x)$ le groupe d'inertie et $G_1(x)$ le groupe d'inertie sauvage. Ce dernier est l'unique p-sous-groupe de Sylow du groupe d'inertie. Comme k est algébriquement clos, le groupe de décomposition et le groupe d'inertie coïncident avec le stabilisateur G_x. En caractéristique nulle, comme en caractéristique positive $p > 0$ lorsque p ne divise pas l'ordre de G, les groupes de ramification $G_i(x)$ sont triviaux dès que $i \geq 1$. Mais lorsque $p > 0$ divise l'ordre de G, ces groupes interviennent dans la formule donnant le genre g_0 de la courbe quotient C/G. Si l'on note $x_1, \ldots, x_r$ les points de ramification de C, avec $r \geq 0$, la formule d'Hurwitz devient ([St93] Thm. III.4.12 et Thm. III.8.8) :

$$2\,(g-1) = 2\,|G|\,(g_0 - 1) + \sum_{j=1}^{r} \sum_{i=0}^{\infty} (|G_i(x_j)| - 1). \tag{1.5}$$

[1] Nakajima ([Na87a]) avait constaté un oubli dans la preuve de Henn : "Stichtenoth's result was improved by Henn. But his proof contains a gap (last paragraph of p. 104). I do not know if the gap can be covered." Ce manquement est comblé dans [GK08]- (voir aussi [HKT08], Chapitre 11.12).

1.2.6 Préliminaires à l'étude des déformations.

Au paragraphe 1.1.7, nous avons défini des espaces de modules $H_{g,G,\xi}$ permettant de décrire les déformations d'une G-courbe C de genre g et de donnée d'Hurwitz ξ, en caractéristique nulle et en caractéristique positive lorsque l'action est modérée. En particulier, nous avons vu (cf. formule (1.4)) que chacune des composantes connexes de $H_{g,G,\xi}$ avait la même dimension $\delta_{g,G,\xi}$ ne dépendant que du genre g_0 de la courbe quotient C/G et du nombre r de points de branchement de $C \to C/G$.

Lorsque k est de caractéristique positive $p > 0$ et que G est un groupe d'ordre divisible par p, les résultats précédents ne sont plus valables à cause de l'apparition de ramification sauvage. Pour pouvoir décrire les déformations d'une G-courbe en toute généralité, il est donc nécessaire d'introduire de nouveaux espaces de modules. Suivant les travaux de Tufféry ([Tu93]), Maugeais [Mau08] et autres, étant donnés un groupe fini G et un entier g, on appelle $\mathcal{M}_g[G]$ l'espace de modules des courbes propres et lisses de genre g : $C \to S$, S étant un schéma quelconque, munies d'une action de G fidèle dans chaque fibre.

Si C est une G-courbe de genre g définie sur un corps k algébriquement clos de caractéristique $p > 0$, le revêtement $\pi : C \to C/G$ induit un point x de $\mathcal{M}_g[G]$ qui appartient à la fibre spéciale $\mathcal{M}_g[G] \times \mathbb{F}_p$. Etudier les déformations de π revient donc à étudier l'anneau local complété de $\mathcal{M}_g[G]$ en x, voire l'anneau local complété de $\mathcal{M}_g[G] \times \mathbb{F}_p$ en x si l'on se restreint aux déformations en égale caractéristique $p > 0$ (cf. [BeMe00] § 5). Dans cette déformation, n'intervient que la composante connexe de $\mathcal{M}_g[G]$ contenant x le long de laquelle le genre des courbes quotients par G est constant, égal à $g_0 = g(C/G)$. En effet, le genre des courbes quotients est déterminé, via la formule d'Hurwitz (1.5), par le degré δ du diviseur de ramification : $\delta = 2\,(g-1) - 2\,|G|\,(g_0 - 1)$, degré qui reste constant au cours de la déformation. Par contre, les autres données de ramification du revêtement π comme le nombre de points de ramification et la filtration en chacun de ces points, peuvent varier au cours de la déformation.

Les $\mathcal{M}_g[G]$ sont des espaces de modules fins, même si ce ne sont pas des schémas mais des champs algébriques. Si l'on veut travailler avec des espaces de modules fins représentables par des schémas, on peut introduire les espaces de modules $\mathcal{M}_{g,\ell}[G]$ faisant intervenir la structure de niveau ℓ (cf. § 2.2).

1.2.7 Bornes sur les p-sous-groupes de Sylow de $\mathrm{Aut}_k(C)$.

L'importance de la ramification sauvage incite à s'intéresser plus particulièrement aux p-sous-groupes de $\mathrm{Aut}_k(C)$. Stichtenoth ([St73]) donne une borne quadratique sur l'ordre du p-sous-groupe de Sylow $G_1(x)$ du groupe d'inertie G_x en tout point x de C :

$$|G_1(x)| \leq \frac{4\,p}{p-1}\, g^2.$$

Il démontre de plus que seules trois situations sont possibles, situations qui s'excluent l'une l'autre :

1. La courbe quotient $C/G_1(x)$ n'est pas rationnelle et $|G_1(x)| \leq g$.
2. La courbe quotient $C/G_1(x)$ est rationnelle, le revêtement $C \to C/G_1(x)$ se ramifie ailleurs qu'au point x et
$$|G_1(x)| \leq \frac{p}{p-1}\, g.$$
3. Les courbes quotients $C/G_1(x)$ et $C/G_2(x)$ sont rationnelles, le revêtement $C \to C/G_1(x)$ se ramifie seulement au point x et
$$|G_1(x)| \leq \frac{4\,|G_2(x)|}{(|G_2(x)|-1)^2}\, g^2 \leq \frac{4\,p}{(p-1)^2}\, g^2.$$

Les résultats de Stichtenoth soulèvent tout naturellement la question de la classification des groupes d'automorphismes $G \subset \mathrm{Aut}_k(C)$ satisfaisant la condition suivante :

$$\text{Il existe un point}\, x \,\text{de}\, C \,\text{tel que} \qquad |G_1(x)| > \frac{p}{p-1}\, g. \tag{1.6}$$

Une réponse à ce problème est apportée par Giuletti et Korchmáros ([GK07].) Lorsque la condition (1.6) est vérifiée, ceux-ci montrent que le groupe G fixe le point x, i.e. $G = G_x$ ou bien que la courbe C est isomorphe soit à une courbe hyperelliptique, soit à une courbe hermitienne, soit à une courbe de Deligne-Lusztig (on renvoie à [GK07] pour les équations des courbes et la description des groupes correspondants).

1.2.8 Sous-groupes de Sylow de $\mathrm{Aut}_k(C)$ dans le cas d'un revêtement p-cyclique de la droite projective, ramifié en un seul point.

Lehr et Matignon [LM05] caractérisent les p-sous-groupes de Sylow du groupe des automorphismes $\mathrm{Aut}_k(C)$ dans le cas où $C \to \mathbb{P}^1_k$ est un revêtement p-cyclique de la droite projective, ramifié en exactement un point.

Supposons ainsi que C soit définie par l'équation : $W^p - W = f(X)$, où $f(X)$ un polynôme de $k[X]$ de degré m premier à p, $m \geq 2$ et $\{m, p\} \neq \{2, 3\}$. Notons $A_{\infty,1}$ le groupe d'inertie sauvage du groupe des automorphismes $\mathrm{Aut}_k(C)$ au point $X = \infty$. Alors, $A_{\infty,1}$ est un p-sous groupe de Sylow de $\mathrm{Aut}_k(C)$ et il est normal sauf lorsque $f(X) = X^m$ avec $m < p$ et m divisant $1 + p$. De plus, $A_{\infty,1}$ est extension centrale d'un groupe cyclique d'ordre p par un p-groupe abélien élémentaire $V \simeq (\mathbb{Z}/p\mathbb{Z})^t$, $t \geq 0$, lequel correspond à un sous-groupe de translations de la droite affine : $X \to X + y$, $y \in V$.

Réciproquement, tout extension de $\mathbb{Z}/p\mathbb{Z}$ par un p-groupe abélien élémentaire $V \simeq (\mathbb{Z}/p\mathbb{Z})^t$, $t \geq 0$, peut être réalisé de cette façon ([LM05] Thm. 1.1). Par [St73], on obtient également des bornes sur l'ordre du p-Sylow $|A_{\infty,1}|$ puis sur le quotient $\frac{|A_{\infty,1}|}{g^2}$:

$$|A_{\infty,1}| \leq p\,(m-1)^2 \quad \text{et} \quad \frac{|A_{\infty,1}|}{g^2} \leq \frac{4\,p}{(p-1)^2}.$$

Dans la seconde borne, le cas d'égalité se produit lorsque $f(X)$ admet une écriture particulière en terme de polynômes additifs, i.e. de polynômes de $k\{F\}$, le k-sous-espace vectoriel de $k[X]$ engendré par les puissances positives du Frobenius F (cf. [Go96] chap. 1). Ainsi, si l'on suppose $f(X)$ réduit modulo $(F - id)(k[X])$, i.e. si les exposants des monômes de $f(X)$ sont tous premiers à p et si

$$\frac{|A_{\infty,1}|}{g} > \frac{p}{p-1} \quad (\frac{2}{3} \text{ pour } p = 2),$$

alors $f(X) = c\,X + X\,S(X) \in k[X]$, où $S(X)$ est un polynôme additif de $k[X]$ de degré p^s ([LM05] Prop. 8.3). Dans ce cas,

$$\frac{|A_{\infty,1}|}{g} = \frac{2\,p^{s+1}}{(p-1)} \quad \text{et} \quad \frac{|A_{\infty,1}|}{g^2} = \frac{4\,p}{(p-1)^2}.$$

1.2.9 Les grosses actions.

Soient k un corps algébriquement clos de caractéristique $p > 0$ et C une courbe algébrique projective lisse, connexe, définie sur k, de genre $g \geq 1$. Pour poursuivre cette étude, nous allons remplacer la condition (1.6) par deux hypothèses plus contraignantes :

1. $G \subset \mathrm{Aut}_k(C)$ est lui-même un p-groupe.
2. L'inégalité $|G_1(x)| > \frac{p}{p-1}\,g$ devient :

$$|G| > \frac{2\,p}{p-1}\,g. \tag{1.7}$$

Sous ces deux hypothèses, nous dirons que le couple (C, G) constitue une *grosse action.*

Notre première tache va être de justifier la pertinence de ces nouvelles hypothèses. Pour donner une première idée, on peut dire que l'intérêt de la borne (1.7) est de rigidifier la situation de ramification du revêtement : $C \to C/G$, comme il a été fait en caractéristique nulle avec les groupes d'automorphismes dits "larges" et "super-larges". Plus précisément, en comparant nos hypothèses aux résultats de Nakajima ([Na87a], Thm. 1), on démontre que la borne (1.7) impose la nullité de l'invariant de Hasse-Witt de la courbe C. Dans cette situation, la formule de Deuring-Shafarevitch (cf. [Bou00]) implique qu'il existe un seul point x de C qui soit ramifié. Il suit qu'en ce point, la ramification est totale. Dès lors, puisque G est un p-groupe :

$$G = G_x = G_0(x) = G_1(x).$$

Le point de ramification x étant unique, on note désormais les groupes de ramification G_i à la place de $G_i(x)$. On se trouve donc dans le dernier des trois cas de figure décrit par Stichtenoth (voir § 2.7) si bien que les courbes quotient C/G et C/G_2 sont rationnelles. Par conséquent, G_2 ne peut pas être trivial. La formule du genre d'Hurwitz (cf. (1.5)) appliquée au revêtement $C \to C/G$ donne à présent :

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

En particulier, la condition (1.7) se réécrit :

$$|G| > \frac{2\,g}{p-1}\,p \quad \text{avec} \quad \frac{2\,g}{p-1} \in \mathbb{N}^*.$$

L'apparition du 2 au numérateur de la borne (1.7) présente un autre avantage majeur par rapport à la borne (1.6) : dans le cas d'une grosse action, G_2 est strictement inclus dans G_1 ([LM05]). Ceci n'est plus vrai si l'on prend un p-groupe $G \subset \mathrm{Aut}_k(C)$ vérifiant seulement l'inégalité large $|G| \geq \frac{2\,p}{p-1}\,g$, comme en témoigne le contre-exemple lié à la courbe $W^p - W = X^2$, avec $p > 2$. Dès lors, le groupe quotient G/G_2 agit comme un p-groupe d'automorphismes de la courbe rationnelle C/G_2, si bien que ce groupe quotient s'identifie à un groupe de translations de la droite affine : $X \to X + y$, où y décrit un $\mathbb{F}_p$-sous espace vectoriel V de k de dimension finie $v > 0$. Ceci relie l'étude des grosses actions au problème de plongement lié à la suite exacte :

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

avec

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

1.2.10 Grosses actions (C, G) avec un G_2 cyclique d'ordre p.

Dans l'étude des grosses actions, un premier cas crucial est celui des grosses actions dont le G_2 est cyclique d'ordre p. On peut en effet se ramener à ce cas par quotient en utilisant la proposition suivante.

Proposition 1.2.1. *Soit (C, G) une grosse action de genre $g \geq 2$. Soit H un sous-groupe normal de G tel que $g_{C/H} > 0$ (ce qui est vrai en particulier lorsque H est strictement inclus dans G_2 comme nous l'établirons plus loin). Alors, le couple $(C/H, G/H)$ est encore une grosse action (cf. [LM05] Prop. 8.5) et son deuxième groupe de ramification est G_2/H (voir § 1.4.1).*

Les résultats décrivant une grosse action dont le G_2 est cyclique d'ordre p sont regroupés dans le théorème ci-dessous. Ils sont issus en droite ligne des travaux de Lehr et Matignon [LM05] évoqués au paragraphe 2.8. Précisons que, dans toute la suite de ce paragraphe, si $f \in k[X] - (F - id)(k[X])$, on notera C_f la courbe projective lisse définie par l'équation affine : $W^p - W = f(X)$.

Theorem 1.2.2. *Soit (C, G) une grosse action de genre $g \geq 2$ telle que G_2 est cyclique d'ordre p.*

1. *La courbe C est isomorphe à une courbe C_f d'équation affine :*

$$W^p - W = f(X) = c\,X + X\,S(X) \in k[X],$$

où $S(X) = a_0\,X + a_1\,X^p + \ldots + a_{s-1}\,X^{p^{s-1}} + a_s\,X^{p^s}$ est un polynôme additif de $k[X]$ de degré p^s, avec $s \geq 1$. De plus, après une translation et une homothétie sur X, on peut supposer $c = 0$ et $a_s = 1$.

2. *Suivant Elkies ([El97], section 4), on définit un polynôme additif lié à f, appelé le polynôme palindromique de f :*

$$\mathrm{Ad}_f := \frac{1}{a_s^{p^s}}\,F^s\,(\sum_{j=0}^{s} a_j\,F^j + F^{-j}\,a_j),$$

où F désigne l'opérateur Frobenius. L'ensemble de ses racines $Z(\mathrm{Ad}_f)$ est un $\mathbb{F}_p$-espace vectoriel isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{2s}$.

3. *Le sous-groupe d'inertie sauvage $A_{\infty,1}$ de $\mathrm{Aut}_k(C)$ au point $X = \infty$ est extension de son centre $Z(A_{\infty,1})$, groupe cyclique d'ordre p égal à son groupe dérivé $D(A_{\infty,1})$, par le p-groupe abélien élémentaire $Z(\mathrm{Ad}_f)$, i.e.*

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

où

$$\pi : \begin{cases} A_{\infty,1} \to Z(\mathrm{Ad}_f) \\ g \to g(X) - X. \end{cases}$$

Pour $p > 2$, $A_{\infty,1}$ est l'unique groupe extraspécial d'exposant p et d'ordre p^{2s+1}.

4. *Il existe un sous $\mathbb{F}_p$-espace vectoriel V de $Z(\mathrm{Ad}_f)$ tel que $G = \pi^{-1}(V)$.*

5. *La filtration de ramification inférieure de G au point ∞ s'écrit :*

$$G = G_0 = G_1 \supsetneq G_2 = \ldots = G_{i_0} \simeq \mathbb{Z}/p\mathbb{Z} \supsetneq \{0\}, \tag{1.8}$$

avec $i_0 = 1 + p^s$.

6. La filtration de ramification supérieure de G s'écrit :

$$G = G^0 = G^1 \supsetneq G^2 = \ldots = G^{\phi(i_0)} \simeq \mathbb{Z}/p\,\mathbb{Z} \supsetneq \{0\}, \tag{1.9}$$

où ϕ désigne la fonction de Herbrand (cf. [Se68] § IV,3). Ici, $\phi(i_0) = 1 + \frac{1}{p^s}$.

Lehr et Matignon [LM05] établissent également la réciproque :

Proposition 1.2.3. *Soit C_f la courbe projective lisse définie sur k par l'équation affine :*

$$W^p - W = f(X) := c\,X + X\,S(X) \in k[X],$$

où S est un polynôme additif de degré p^s, avec $s \geq 1$. Soit $A_{\infty,1}$ le sous-groupe d'inertie sauvage de $\mathrm{Aut}_k(C_f)$ au point ∞. Alors $(C_f, A_{\infty,1})$ est une grosse action dont le deuxième groupe de ramification est cyclique d'ordre p.

On s'intéresse à présent aux déformations d'une telle action. Pour cela, on introduit $\mathcal{A} := k[c, a_0, \cdots, a_s][\frac{1}{a_s}]$ le localisé de l'anneau des polynômes à $s+2$ indéterminées. La famille

$$\mathrm{Spec}\,(\frac{\mathcal{A}[X,W]}{W^p - W - f(X)}) \longrightarrow \mathrm{Spec}\,\mathcal{A}$$

où $f(X) := c\,X + X\,(a_0\,X + a_1\,X^p + \ldots + a_s\,X^{p^s}) \in \mathcal{A}[X]$, est une famille affine lisse. Elle peut être compactifiée par :

$$\mathrm{Proj}\,(\frac{\mathcal{A}[X,W,Z]}{W^p\,Z^{p^s-p+1} - W\,Z^{p^s} - Z^{1+p^s}\,f(\frac{X}{Z})}) \longrightarrow \mathrm{Spec}\,\mathcal{A},$$

laquelle est une famille projective avec une forte singularité en $Z = 0$. On peut montrer (communication de Sylvain Maugeais) que la normalisation induit une famille lisse projective :

$$\mathcal{C} \longrightarrow \mathrm{Spec}\,\mathcal{A} \simeq \mathbb{A}^{s+1} \times \mathbb{G}_m.$$

La fibre au point $(c, a_0, a_1, \ldots, a_s \neq 0) \in \mathrm{Spec}\,\mathcal{A}$ est isomorphe à la courbe C_f, avec $f(X) := c\,X + X\,(a_0\,X + a_1\,X^p + \ldots + a_s\,X^{p^s})$. On suppose désormais que $p > 2$ et on note G le groupe extraspécial d'ordre p^{2s+1} et d'exposant p. La famille $\mathcal{C}$ est munie d'une G-action qui induit, en chaque fibre, l'action $(C_f, A_{\infty,1}(C_f))$, où $A_{\infty,1}(C_f) \simeq G$ désigne le sous-groupe d'inertie sauvage de $\mathrm{Aut}_k(C_f)$ au point ∞. On en déduit le morphisme :

$$\left\{ \begin{array}{lcc} \mathbb{A}^{s+1} \times \mathbb{G}_m \subset \mathbb{A}^{s+2} & \longrightarrow & \mathcal{M}_g[G] \times \mathbb{F}_p \\ (c, a_0, a_1, \ldots, a_s \neq 0) & \longmapsto & \text{classe d'équivalence de} \quad (C_f, G) \\ & & \text{avec} \quad f(X) := c\,X + X\,(a_0\,X + a_1\,X^p + \ldots + a_s\,X^{p^s}). \end{array} \right.$$

Le corps k étant algébriquement clos, on montre que deux G-courbes C_{f_1} et C_{f_2} sont équivalentes si et seulement s'il existe (λ, μ) dans $k^\times \times k$ tels que $f_2(X) = f_1(\lambda\,X + \mu)$ (cf. [LM05] § 8.2). Il suit que l'espace des modules grossier associé à $\mathcal{M}_g[G] \times \mathbb{F}_p$ est quotient de l'ouvert $\mathbb{A}^{s-1} \times \mathbb{G}_m$ par un groupe cyclique. Ainsi, $\mathcal{M}_g[G] \times \mathbb{F}_p$ est irréductible de dimension s. La dimension obtenue sera comparée plus loin aux bornes données par Pries pour l'espace des déformations (cf. § 2.12).

Remarquons tout d'abord que, dans notre situation, les déformations sont équiramifiées, puisque la filtration de ramification inférieure (resp. supérieure) du groupe est fixée par (1.8) (resp. (1.9)).

On constate également que dans notre exemple, $(\mathcal{M}_g[G])_{\mathrm{red}} = (\mathcal{M}_g[G] \times \mathbb{F}_p)_{\mathrm{red}}$. En effet, supposons que (C_η, G) soit une déformation de (C_f, G) en caractéristique nulle. Alors, la courbe quotient C_η/G_2 s'identifierait à la droite projective et $G_1/G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$ s'identifierait à un sous-groupe de $\mathrm{PGL}_2(K)$, avec K corps de caractéristique nulle. Il suit de [Su82] (Thm. 6.17) que $p = 2$, $s = 2$, d'où $g = \frac{p-1}{2}\,p^s = 1$, ce qui est une contradiction.

On généralise ce résultat en montrant que pour toute grosse action (C, G) de genre $g \geq 2$, l'anneau de déformations est de caractéristique $p > 0$ lorsque $p \geq 2$. En effet, le couple $(C/G_2, G/G_2)$ est une action faiblement ramifiée, i.e. de second groupe de ramification trivial. Il suit de plus de la Proposition 2.1 et du Théorème 2.2 que p^2 divise l'ordre du p-groupe abélien élémentaire G/G_2. La théorie des déformations de telles actions faiblement ramifiées est connue d'après les travaux de [CoKa03], [CoMe06] et [ByCo08]. On en déduit le résultat annoncé.

1.2.11 Début de classification pour les grosses actions.

Si les grosses actions sont définies via la valeur du quotient $\frac{|G|}{g}$, on s'aperçoit que c'est un autre quotient, en l'occurence $\frac{|G|}{g^2}$, qui joue un rôle de crible pour leur classification, l'idée étant qu'une borne inférieure sur $\frac{|G|}{g^2}$ induit une borne supérieure sur l'ordre de G_2 ([LM05] section 8.4). Par [Na87a] (Thm. 1), on sait déjà que

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

Lehr et Matignon ([LM05] Thm. 8.6) obtiennent une caractérisation des grosses actions (C, G) vérifiant :

$$\frac{|G|}{g^2} \geq \frac{4}{(p-1)^2}. \tag{1.10}$$

Theorem 1.2.4. *Soit (C, G) une grosse action de genre $g \geq 2$. La condition (1.10) est vérifiée si et seulement si G_2 est cyclique d'ordre p, i.e. si et seulement si C est birationnelle à une courbe d'équation $W^p - W = c\,X + X\,S(X) \in k[X]$, où S est un polynôme additif de $k[X]$ de degré p^s, avec $s \geq 1$.*
Deux cas sont alors possibles :

1. *Soit $G = A_{\infty,1}$ et $V = Z(\mathrm{Ad}_f)$, auquel cas, $\frac{|G|}{g^2} = \frac{4\,p}{(p-1)^2}$.*
2. *Soit G est un sous-groupe d'indice p de $A_{\infty,1}$ et V un hyperplan de $Z(\mathrm{Ad}_f)$, auquel cas $\frac{|G|}{g^2} = \frac{4}{(p-1)^2}$.*

1.2.12 Etude des déformations via le formal patching.

R. Pries consacre une série de travaux ([Pr05], [Pr06], [PrOb08]) aux déformations équiramifiées de courbes en caractéristique positive.

Soient k un corps algébriquement clos de caractéristique $p > 0$ et $\mathcal{X}$ une courbe algébrique, projective, lisse, connexe définie sur k. Soit $\varphi : \mathcal{Y} \to \mathcal{X}$ un revêtement galoisien de groupe G fini, ramifié en un ensemble fini B de points de $\mathcal{X}$. Par des méthodes de patching formel (cf. [Har03]), l'étude des déformations de φ se ramène à celle du I-revêtement de germes de courbes $\phi : Y \to X$, où X est le germe de $\mathcal{X}$ en b, i.e. $X = \mathrm{Spec}\,\widehat{\mathcal{O}}_{\mathcal{X},b}$, Y le germe de $\mathcal{Y}$ en $\eta := \varphi^{-1}(b)$ et I le groupe d'inertie de φ en η (cf. [Pr05] § 4.4). Dans ce cas, I est isomorphe au produit semi-direct : $P \rtimes \mathbb{Z}/m\mathbb{Z}$, où P est un p-groupe d'ordre p^e et m un entier non divisible par p. Nous verrons également au paragraphe suivant que Bertin et Mézard ([BeMe00]) ramènent, par des méthodes cohomologiques, l'étude des déformations globales à celles des déformations locales, ce qui peut aussi se montrer par des méthodes de recollement analytique (cf. [HarSt99].)

Pries traite le cas des déformations en égale caractéristique d'un I-revêtement ϕ de germes de courbes. Pour cela, elle introduit un foncteur F_ϕ paramétrisant les déformations non obstruées de ϕ, ce qui signifie que le lieu de branchement et la filtration de ramification ne changent pas ([Pr05] § 3.1). Elle établit en particulier l'existence d'un espace de module M_ϕ représentant le foncteur F_ϕ dans une certaine catégorie. De plus, par passage à un quotient, M_ϕ est un sous-schéma d'un produit de schémas, chacun d'eux étant un espace de modules pouvant être explicitement décrit en fonction de la ramification de filtration de ϕ. Elle en déduit des bornes inférieures et supérieures pour la dimension de Krull d_ϕ de M_ϕ, bornes qui ne dépendent que de la filtration de ramification de ϕ en numérotation supérieure.

Par la théorie du corps de classes, Pries étudie plus particulièrement le cas où I est un p-groupe abélien ([Pr05] § 4.3). Dans ce cas, M_ϕ est produit direct de copies de $\mathbb{G}_a$ modulo l'action de $\mathbb{F}_p^\times$: elle en déduit une formule exacte pour d_ϕ en terme des sauts dans la filtration de ramification supérieure de ϕ. De plus, dans cette situation, la borne supérieure sur d_ϕ est atteinte.

La borne supérieure sur d_ϕ est encore atteinte lorsque I est produit semi-direct d'un p-groupe abélien élémentaire $P := (\mathbb{Z}/p\mathbb{Z})^e$ par $\mathbb{Z}/m\mathbb{Z}$ ([Pr05] § 3.5). On retrouve ainsi le résultat de Cornelissen-Kato dans le cas où $\mathcal{Y}$ est ordinaire, i.e. d'invariant de Hasse-Witt égal à son genre (cf. [CoKa03]). Dans [PrOb08], Pries et Obus calculent la valeur de d_ϕ lorsque I est produit semi-direct de $P := (\mathbb{Z}/p^e\mathbb{Z})$ par $\mathbb{Z}/m\mathbb{Z}$.

La borne supérieure sur d_ϕ trouvée par Pries n'est cependant pas toujours atteinte. Considérons par exemple le cas où I est un p-groupe d'ordre p^e, i.e. $m = 1$. Notons $(\sigma_i)_{1 \leq i \leq e}$ les sauts en ramification supérieure de ϕ comptés avec leur multiplicité ℓ_i, i.e. :

$$\sigma_1 = \ldots = \sigma_{\ell_1} < \sigma_{\ell_1+1} = \ldots = \sigma_{\ell_1+\ell_2} < \ldots < \sigma_{\ell_{r-1}+1} = \ldots = \sigma_{\ell_1+\ell_2+\ldots+\ell_r},$$

où

$$\frac{G^j}{G^{j+1}} \simeq (\mathbb{Z}/p\,\mathbb{Z})^{\ell_j}.$$

Alors, d'après les bornes trouvées dans [Pr05], la dimension de Krull d_ϕ est encadrée comme suit :

$$n_1 \leq d_\phi \leq \sum_{i=1}^{e} n_i \quad \text{avec} \quad n_i = \lfloor \sigma_i \rfloor - \lfloor \frac{\sigma_i}{p} \rfloor,$$

où $\lfloor x \rfloor$ désigne la partie entière inférieure du réel x.

En reprenant les notations du paragraphe 2.10, on considère la courbe projective lisse C_{f_0} d'équation affine :

$$W^p - W = f_0(X) := X^{1+p^s}$$

avec $s \geq 1$ et $p \geq 3$. On prend alors pour G le sous-groupe d'inertie sauvage $A_{\infty,1}$ de $\mathrm{Aut}_k(C)$ au point $X = \infty$. On déduit du paragraphe 2.10 que (C, G) est une grosse action dont le deuxième groupe de ramification est cyclique d'ordre p, que G est le groupe extraspécial d'exposant p et d'ordre p^{2s+1} et que les σ_i définis ci-dessus prennent les valeurs suivantes : $\sigma_1 = \ldots = \sigma_{2s} = 1$ et $\sigma_{2s+1} = 1 + \frac{1}{p^s}$. D'où :

$$1 \leq d_\phi \leq 2s + 1.$$

Comme $\dim(\mathrm{Aut}(\mathbb{P}^1 - \{\infty\})) = 2$ et que les déformations sont non obstruées, il suit des travaux de Pries ([Pr05] § 4.4) que :

$$d_\phi = \dim(\mathcal{M}_g[G] \times \mathbb{F}_p) + 2.$$

Or, les résultats du paragraphe 2.10 indiquent que $\dim(\mathcal{M}_g[G] \times \mathbb{F}_p) = s$, d'où $d_\phi = s+2$. La borne maximale donnée par Pries n'est donc pas atteinte dans ce cas, lorsque $s \geq 2$.

1.2.13 Etude des déformations via les méthodes cohomologiques.

Utilisation des déformations dans les problèmes de relèvement en inégale caractéristique.

Les méthodes de déformations interviennent également pour étudier les problèmes de relèvement en inégale caractéristique. Bertin et Mézard ([BeMe00]) utilisent ainsi les méthodes cohomologiques des déformations pour traiter du problème de relèvement en caractéristique nulle des revêtements galoisiens de courbes lisses sur un corps k algébriquement clos de caractéristique $p > 0$.

Soit C une courbe complète, lisse et connexe définie sur k et $\pi : C \to C/G$ un revêtement galoisien de groupe G. Un problème difficile est celui du relèvement de π en caractéristique zéro, i.e. le relèvement galoisien à un anneau de valuation discrète R dominant l'anneau des vecteurs de Witt $W(k)$. On sait déjà que, dans certains cas, les bornes d'Hurwitz ou de Stichtenoth sur l'ordre du groupe des automorphismes rendent ce relèvement impossible. Bertin et Mézard abordent ce problème de relèvement des revêtements galoisiens en utilisant les déformations, le caractère galoisien étant conservé au cours de la déformation. Lorsque la ramification est modérée, il n'y a pas d'obstruction au relèvement infinitésimal des déformations (cf. [Gro63]). L'anneau versel de déformation est alors une algèbre de séries formelles sur $W(k)$. Mais, dans le cas général, il existe des obstructions qui sont localisées aux points de ramification sauvage.

Bertin et Mézard définissent tout d'abord les foncteurs des déformations globales D_{gl} et des déformations locales D_G d'un revêtement galoisien ([BeMe00], § 2). Ces foncteurs admettent des anneaux de déformations versels R_{gl} et R_G et leurs espaces tangents peuvent être identifiés à certains premiers groupes de cohomologie équivariants.

Plus précisément, soit Λ un anneau de valuation discrète complet de caractéristique nulle et soit k son corps résiduel de caractéristique p. On peut par exemple choisir $\Lambda = W(k)$, l'anneau des vecteurs de Witt à coefficients dans k. Soit $C \to C/G$ un revêtement galoisien, où C est une courbe algébrique projective lisse définie sur k et G un sous-groupe fini de $\mathrm{Aut}_k(C)$. Bertin et Mézard montrent que le foncteur des déformations infinitésimales D_{gl} de (C, G) admet une déformation verselle et que son espace tangent $D_{gl}(k[\epsilon])$ s'identifie à $H^1(G, \mathcal{T}_C)$, où $\mathcal{T}_C$ est le faisceau tangent à la courbe C.

On considère à présent $x \in C$ un point de ramification sauvage de C, i.e. un point tel que son groupe d'inertie G_x est d'ordre divisible par p. On note $\widehat{\mathcal{O}}_{C,x} \simeq k[[T]]$ l'anneau local complété de la courbe C au point x et $\widehat{\mathcal{T}}_{C,x}$ la fibre complétée du faisceau tangent au point x. Bertin et Mézard prouvent que le foncteur D_G des déformations infinitésimales d'une représentation $\rho : G \hookrightarrow \mathrm{Aut}\, k[[T]]$ admet une déformation verselle et que l'espace tangent $D_G(k[\epsilon])$ s'identifie à $H^1(G, \Theta)$, où $\Theta = k[[T]]\frac{d}{dT}$ est le $k[[T]]$-module des champs de vecteurs formels.

Bertin et Mézard démontrent ensuite un principe local-global qui relie les déformations globales aux déformations locales et qui établit que les obstructions sont de nature locale ([BeMe00], §3). Pour préciser les énoncés, il est tout d'abord nécessaire de rappeler certaines définitions de cohomologie équivariante (cf. [Gro57]). Soient C et G définis comme ci-avant. Soit F un $(G, \mathcal{O}_C)$-module. Si π est le revêtement $C \to \Sigma : C/G$, on peut alors considérer le faisceau $\pi_*^G(F)$ sur Σ défini par :

$$V \to \Gamma(V, \pi_*(F))^G = \Gamma(\pi^{-1}(V), F)^G,$$

où V est un ouvert de Σ. On définit alors deux foncteurs covariants sur la catégorie des $(G, \mathcal{O}_C)$-modules : π_*^G et $\Gamma^G(C, .)$, avec $\Gamma^G(C, F) = \Gamma(C, F)^G$. Les foncteurs dérivés sont respectivement un faisceau de modules sur Σ noté $R^q\,\pi_*^G(C, F)$ et un groupe noté $H^q(G, F) = R^q\Gamma^G(C, F)$. Le k-espace vectoriel $H^q(G, F)$ est le groupe de cohomologie équivariante de G à coefficients dans le G-faisceau F.

Soient $y_1, y_2, \ldots, y_r \in C/G$ les images des points de ramification sauvage de $C \to C/G$. Pour $1 \leq i \leq r$, on note x_i un point au-dessus de y_i. Soit le foncteur des déformations locales $D_{loc} = \prod_i D_{G_{x_i}}$, où $D_{G_{x_i}}$ est le foncteur des déformations infinitésimales de l'action induite par G_{x_i} sur $\widehat{\mathcal{O}}_{C,x_i} \simeq k[[T]]$. Le choix du point x_i est sans importance, car si on prend un autre point x'_i dans l'orbite de x_i sous G, on obtient un foncteur $D_{G_{x'_i}}$ isomorphe à $D_{G_{x_i}}$. Par localisation en ces points, on définit un morphisme :

$$\varphi : D_{gl} \to D_{loc}.$$

Comme l'espace tangent au foncteur $D_{G_{x_i}}$ vérifie :

$$D_{G_{x_i}}(k[\epsilon]) \simeq H^1(G_{x_i}, \mathcal{T}_{C,x_i}),$$

l'espace tangent au foncteur D_{loc} satisfait :

$$D_{loc}(k[\epsilon]) \simeq \bigoplus_{i=1}^{r} H^1(G_{x_i}, \widehat{\mathcal{T}}_{C,x_i}).$$

On a de plus la suite exacte :

$$0 \longrightarrow H^1(C/G, \pi_*^G(\mathcal{T}_C)) \longrightarrow H^1(G, \mathcal{T}_C) \longrightarrow H^0(C/G, R^1\pi_*^G(\mathcal{T}_C)) \longrightarrow 0,$$

avec

$$H^0(C/G, R^1\pi_*^G(\mathcal{T}_C)) \simeq \bigoplus_{i=1}^{r} H^1(G_{x_i}, \widehat{\mathcal{T}}_{C,x_i}).$$

L'application de localisation $H^1(G, \mathcal{T}_C) \to \bigoplus H^1(G_{x_i}, \widehat{\mathcal{T}}_{C,x_i})$ est donc surjective. Le noyau $H^1(C/G, \pi_*^G(\mathcal{T}_C))$ est l'espace tangent au foncteur $\operatorname{Ker}\varphi$. Ce foncteur peut être interprété comme le foncteur des déformations équivariantes localement triviales, c'est-à dire celles qui induisent une déformation triviale sur un voisinage formel de chaque x_i. On montre alors que le morphisme $\varphi : D_{gl} \to D_{loc}$ est lisse. De plus, si on note R_i l'anneau de déformations versel de $D_{G_{x_i}}$ et R_{gl} celui de D_{gl}, alors $R_1 \widehat{\otimes} \ldots \widehat{\otimes} R_r$ est l'anneau de déformations versel de D_{loc} et

$$R_{gl} = (R_1 \widehat{\otimes} \ldots \widehat{\otimes} R_r)[[U_1, \ldots, U_N]],$$

avec $N = \dim_k H^1(C/G, \pi_*^G(\mathcal{T}_C))$. Ainsi, l'anneau local complet qui supporte une déformation formelle verselle globale est formellement lisse sur le produit tensoriel des anneaux locaux complets R_i qui supportent les déformations verselles localisées aux points de ramification sauvage x_i.

Bertin et Mézard se concentrent donc sur les déformations locales au voisinage formel d'un point x de ramification sauvage ([BeMe00], §4). Ils étudient plus particulièrement le cas où le groupe d'inertie $G_x = \langle\sigma\rangle$ est cyclique d'ordre p, première étape d'une étude par dévissage d'un groupe d'inertie plus compliqué. Dans ce cas, où l'existence d'un relèvement en caractéristique nulle est établie ([OSS89], [GrMa98]), ils donnent une description de l'anneau versel R_{G_x} et calculent sa dimension de Krull, comme expliqué ci-dessous.

Soit R_σ l'anneau de déformation versel local associé à l'automorphisme σ de $k[[T]]$, d'ordre p et de conducteur m, ave $p > 2$ et $m > 1$, $(p, m) \neq (3, 2)$. Le groupe cyclique d'ordre p, $G := \langle\sigma\rangle$, s'identifie au groupe d'inertie à l'infini d'un G-revêtement $\pi : C \to \mathbb{P}^1$, défini sur k et étale sur $\mathbb{A}^1$. Les conditions sur p et m assurent de plus que le genre du revêtement π est supérieur ou égal à 2. On fixe une structure de niveau ℓ sur la courbe C, où $\ell \geq 3$ est un premier distinct de p (cf. § 2.2 et § 2.6). Le revêtement π s'identifie alors à un point x d'un espace modulaire $\mathcal{M}_{g,\ell}[G]$. Le point x appartient alors à la fibre spéciale de $\mathcal{M}_{g,\ell}[G]$ et l'anneau R_{gl} de déformations versel de (C,G) est relié à $\mathcal{M} := \mathcal{M}_{g,\ell}[G]$ par la relation :

$$R_{gl} \simeq \widehat{\mathcal{O}}_{\mathcal{M},x}.$$

Bertin et Mézard calculent la dimension de Krull de $\widehat{\mathcal{O}}_{\mathcal{M},x}$, c'est-à-dire la dimension de $\mathcal{M}$:

$$\dim_{\mathrm{Krull}} \widehat{\mathcal{O}}_{\mathcal{M},x} = m-1.$$

Ils en déduisent la dimension de l'anneau de déformation versel local R_σ associé à l'automorphisme σ défini précédemment. Par le principe local-global, l'anneau de déformations universel global vérifie en effet :

$$\dim_{\mathrm{Krull}} R_{gl} = m-1 = \dim_{\mathrm{Krull}} R_\sigma + \dim_k H^1(\Sigma, \pi_*^G(\mathcal{T}_C)),$$

avec

$$\dim_k H^1(\Sigma, \pi_*^G(\mathcal{T}_C)) = -3 + \lfloor \frac{(m+1)(p-1)}{p} \rfloor.$$

En écrivant $m = pq - l$, avec $q \geq 1$ et $1 \leq l \leq p-1$, ils concluent que :

$$\dim_{\mathrm{Krull}} R_\sigma = \begin{cases} q & \text{si } l \neq 1 \\ q+1 & \text{si } l = 1. \end{cases}$$

Le cas d'égale caractéristique.

En étudiant le relèvement à la caractéristique nulle des revêtements galoisiens, Bertin et Mézard ont établi des résultats sur les déformations infinitésimales d'une G-courbe C dans le cas où le groupe G est cyclique d'ordre p. Kontogeorgis ([Kon07]) étend le travail de Bertin et Mézard dans le cadre de l'égale caractéristique $p > 0$. Puisque les quotients des groupes de ramification successifs : G_i/G_{i+1} sont, pour $i \geq 1$, des p-groupes abéliens élémentaires, Kontogeorgis va se concentrer sur les déformations infinitésimales équivariantes d'une G-courbe C de genre g lorsque G est un p-groupe abélien élémentaire.

Soit k un corps algébriquement clos de caractéristique $p \geq 0$. Soit C une courbe algébrique projective lisse, définie sur k. Le foncteur des déformations de C indépendamment de toute action de groupe, est déjà connu et largement étudié : on sait, par exemple, que son espace tangent est $H^1(\mathcal{T}_C)$, où $\mathcal{T}_C$ est le faisceau tangent à la courbe C. Fixons à présent un sous-groupe G du groupe des automorphismes de C. Comme nous l'avons vu au paragraphe précédent avec Bertin et Mézard, on peut alors définir un nouveau foncteur des déformations et l'espace tangent de ce foncteur est donné par le groupe de cohomologie équivariante de Grothendieck $H^1(G, \mathcal{T}_C)$. De plus, sa dimension sur k mesure les directions pour déformer la G-courbe C. Dans ce cas, les points x_i de ramification sauvage contribuent, via les groupes $H^1(G_{x_i}, \widehat{\mathcal{T}}_{C,x_i})$, au calcul de la dimension de l'espace tangent du foncteur des déformations.

En appliquant la théorie des groupes de Galois des corps locaux, l'idée est de casser le groupe de ramification à chaque point de ramification sauvage en une suite d'extensions de p-groupes abéliens élémentaires. Cette décomposition est utilisée pour réduire le calcul de l'espace tangent au cas d'un p-groupe abélien élémentaire. Kontogeorgis donne alors des bornes supérieures et inférieures à la dimension de l'espace tangent du foncteur des déformations. En particulier, si le groupe d'inertie G_x du point de ramification sauvage x est produit semi-direct d'un p-groupe abélien élémentaire par un groupe cyclique tel qu'il y ait seulement un saut en $i$ème position dans la suite de ramification inférieure, Kontogeorgis donne la valeur exacte de la dimension de la contribution locale $H^1(G_x, \mathcal{T}_{C,x})$. Dans le cas $i = 1$, il retrouve ainsi les résultats de [CoKa03] sur les déformations de courbes ordinaires. Il compare aussi ses résultats aux bornes de Pries (cf. § 2.12).

En guise d'application, revenons au cas des déformations de la courbe :

$$C_{f_0} : \quad W^p - W = f_0(X) := X^{1+p^s} \quad \text{avec} \quad p \geq 3, \qquad s \geq 1$$

munie de l'action du groupe d'inertie sauvage $G := A_{\infty,1}$ (voir § 2.10 et § 2.12). Les formules de Kontogeorgis donnent les bornes suivantes :

$$s+1 \leq \dim H^1(G, \widehat{\mathcal{T}}_{C,\infty}) = \dim H^1(G, \mathcal{T}_C) \leq s+2+p^{s-1}.$$

1.3 Motivation et application : la monodromie arithmétique.

L'étude des grosses actions trouve également son origine dans des problèmes de monodromie, en particulier la recherche des groupes de monodromie (sauvage) maximaux. Nos références sont ici [Liu02] et [Ma06].

Soient (K, v) un corps complet (ou hensélien) muni d'une valuation discrète, O_K son anneau de valuation, M_K l'idéal maximal de O_K et π une uniformisante. On suppose que le corps résiduel $k := O_K/M_K$ est algébriquement clos de caractéristique $p > 0$. On commence par rappeler un résultat de Grothendieck prouvant l'existence d'une réduction semi-stable pour les variétés abéliennes. Soit A une variété abélienne sur K. Grothendieck prouve l'existence d'une extension K'/K finie et séparable telle que la composante neutre de la fibre spéciale du modèle de Néron $\mathcal{A}'^0$ de $A' = A \times K'$ sur $O_{K'}$ soit semi-abélienne, i.e.

$$0 \longrightarrow T \longrightarrow \mathcal{A}'^0 \times k \longrightarrow B \longrightarrow 0,$$

où T est un tore et B une variété abélienne sur k. On dit alors que A admet une réduction semi-stable sur K'.

On introduit à présent la notion de réduction semi-stable (resp. stable) pour une courbe C définie sur K. On considère tout d'abord une courbe X connexe projective définie sur k. On dit que X est semi-stable si elle est réduite et si ses singularités sont des points doubles ordinaires. On dit que X est stable si elle est semi-stable, connexe, projective, si $p_a(X) \geq 2$ et si ses composantes irréductibles isomorphes à $\mathbb{P}^1$ intersectent les autres composantes irréductibles en au moins trois points. Considérons à présent une courbe C définie sur K. On dit que C admet une réduction semi-stable (resp. stable) s'il existe un modèle $\mathcal{C}$ sur $\operatorname{Spec} O_K$ avec une fibre spéciale $\mathcal{C}_s$ semi-stable (resp. stable) sur k.

Le résultat suivant, dû à Deligne et Mumford ([DeMu69]), établit l'existence d'une telle réduction. Ainsi, si C est une courbe projective lisse, géométriquement connexe, de genre $g \geq 2$, définie sur K, il existe une extension K'/K finie et séparable telle que $C \times K'$ admette un unique modèle stable $\mathcal{C}$ sur $O_{K'}$. La fibre spéciale $\mathcal{C} \times k$ ne dépend pas de l'extension K'/K : on l'appelle la réduction potentiellement stable de C. On peut alors faire le lien avec la réduction semi-stable pour les variétés abéliennes : la courbe C admet une réduction stable sur K si et seulement si sa jacobienne admet une réduction semi-stable sur K.

On cherche à présent l'extension minimale K'/K permettant d'obtenir cette réduction stable. Soit C une courbe définie sur K (voire une variété abélienne). Il existe une unique extension minimale K'/K telle que $C \times K'$ admette une réduction stable. On appelle cette extension l'extension de monodromie finie, son groupe de Galois $\mathrm{Gal}(K'/K)$ le groupe de monodromie et son p-sous-groupe de Sylow $\mathrm{Gal}(K'/K)_p$ le groupe de monodromie sauvage. Si l'extension K'/K est de degré $p^n\, e$, avec e premier à p, le groupe quotient $\mathrm{Gal}(K'/K)/\mathrm{Gal}(K'/K)_p$ est cyclique d'ordre e. Il correspond à l'extension cyclique modérée $K'^t := K(\pi^{1/e})$, appelée extension de monodromie modérée. Le groupe de monodromie $\mathrm{Gal}(K'/K)$ est ainsi produit semi-direct d'un groupe cyclique d'ordre e premier à p et du p-groupe de monodromie sauvage. On se pose alors les problèmes suivants :

1. Identifier les groupes (resp. les p-groupes) qui peuvent apparaître comme groupe de monodromie (resp. groupes de monodromie sauvage).
2. Dans le cas des courbes, trouver les groupes de monodromie sauvage qui, à genre donné, sont de taille maximale.

De l'unicité du modèle stable $\mathcal{C}$, on déduit une action fidèle du groupe de monodromie sur la réduction potentiellement stable de C :

$$\mathrm{Gal}(K'/K) \hookrightarrow \mathrm{Aut}_k(\mathcal{C} \times k).$$

Si l'on suppose à présent que $\mathcal{C} \times k$ est lisse de genre $g \geq 2$, on peut appliquer les bornes connues pour les groupes d'automorphismes des courbes lisses de genre $g \geq 2$. En particulier, le groupe de monodromie modérée étant cyclique d'ordre e, on déduit de [Na87b] que $e \leq 4g + 2$. Par Stichtenoth [St73] et Nakajima [Na87a], on sait aussi que $|\mathrm{Gal}(K'/K)_p| \leq \max\{4g, \frac{4p}{(p-1)^2}\, g^2\}$. Mais ces problèmes ont également des liens avec nos "grosses actions", comme le montre l'exemple qui suit.

Lehr et Matignon [LM06a] ont déterminé l'extension de monodromie de certains revêtements p-cycliques de la droite projective sur une extension de $\mathbb{Q}_p$ pour lesquels le groupe de monodromie sauvage est de taille maximale à genre donné. Ainsi, soit $p \geq 2$, $s \geq 1$, $K = \mathbb{Q}_p^{nr}(p^{1/(p^s+1)}, \zeta)$, où ζ est une racine primitive p-ième de l'unité. Considérons le revêtement $C \to \mathbb{P}^1_K$ défini par l'équation :

$$Z^p = f(X) = 1 + p^{1/(p^s+1)}\, X^{p^s} + X^{p^s+1}.$$

Alors, C a potentiellement bonne réduction et sa fibre spéciale est birationelle à la courbe C_{f_0} d'équation :

$$w^p - w = t^{1+p^s}.$$

L'extension de monodromie K'/K est l'extension obtenue en adjoignant au corps de décomposition d'un certain polynôme $\mathcal{L}(Y)$, appelé polynôme de monodromie, les racines p-ièmes $f(y)^{1/p}$, lorsque y parcourt les zéros de $\mathcal{L}(Y)$. De plus, le groupe de monodromie est le sous-groupe d'inertie $A_{\infty,1}$ de $\mathrm{Aut}_k(C_{f_0})$ au point $t=\infty$. D'après ce qui précède (cf. § 2.10), lorsque $p>2$, $A_{\infty,1}$ est le groupe extraspécial d'exposant p et d'ordre p^{2s+1}. Ce groupe de monodromie, qui coïncide avec le groupe de monodromie sauvage, est maximal pour le genre $g=\frac{(p-1)}{2}\,p^s$.

Dans le cas $p=2$ et $g=2$, Lehr et Matignon ([LM06a]) complètent dans le cas d'inégale caractéristique les travaux de Silverberg et Zarhin ([SiZa05]) concernant la monodromie des surfaces abéliennes sur un corps local.

1.4 Présentation des principaux résultats de la thèse.

Cette thèse est composée de trois chapitres dont le but est d'étudier les grosses actions, i.e. les couples (C,G) où C est une courbe projective lisse connexe définie sur un corps k algébriquement clos de caractéristique positive $p>0$, de genre $g\geq 1$ et G un p-groupe de k-automorphismes de C vérifiant $\frac{|G|}{g}>\frac{2p}{p-1}$.

Pour fixer les notations, nous rappelons quelques-uns des résultats exposés au paragraphe 2.9. Si (C,G) est une grosse action, il existe un point ∞ de C tel que G coïncide avec le groupe d'inertie sauvage G_1 de G au point ∞. De plus, la courbe quotient C/G est isomorphe à la droite projective $\mathbb{P}^1_k$. Le deuxième groupe G_2 de ramification de G au point ∞ est non trivial, strictement inclus dans $G_1=G$. La courbe quotient C/G_2 est isomorphe à la droite projective et le groupe quotient G/G_2 agit comme un groupe de translations de la droite affine $C/G_2-\{\infty\}$. De cette manière, G apparaît comme une extension de G_2 par un p-groupe abélien élémentaire V, selon la suite exacte suivante :

$$0\longrightarrow G_2\longrightarrow G=G_1\xrightarrow{\pi} V\simeq(\mathbb{Z}/p\,\mathbb{Z})^v\longrightarrow 0, \tag{1.11}$$

avec

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

1.4.1 Chapitre 2 : étude du deuxième groupe de ramification d'une grosse action.

Le deuxième chapitre de la thèse (cf. [MR08]) est plus particulièrement consacré à l'étude du deuxième groupe de ramification G_2. Il vise d'une part à donner des conditions nécessaires sur G_2 afin que (C,G) soit une grosse action et, d'autre part, à exhiber des exemples de grosses actions avec un G_2 abélien d'exposant quelconque.

Les principaux résultats obtenus sur G_2 dans la première partie du chapitre 2 sont regroupés dans le théorème suivant :

Théorème : Soit (C,G) une grosse action de genre $g\geq 2$.

1. Soit H un sous-groupe de G. Alors, C/H est de genre 0 si et seulement si $H\supset G_2$ (Lemme 2.2.4).
2. Soit H un sous-groupe strict de G_2, normal dans G. Alors, $(C/H,G/H)$ est une grosse action de deuxième groupe de ramification $(G/H)_2=G_2/H$ (Lemme 2.2.4).
3. Le groupe G_2 coïncide avec $D(G)$, le groupe dérivé G (Théorème 2.2.7).
4. Le groupe G_2 n'est cyclique que s'il est d'ordre p (Théorème 2.5.1).
5. Si $\frac{|G|}{g^2}\geq\frac{4}{(p^2-1)^2}$, alors G_2 est un p-groupe abélien élémentaire d'ordre divisant p^3 (Proposition 2.4.1).

Ces résultats mettent en lumière le rôle déterminant joué par G_2 dans l'étude des grosses actions. On voit en particulier que G_2 se définit de manière purement algébrique en tant que groupe dérivé de G. On remarque aussi qu'il n'existe pas de sous-groupe strict H de G_2 tels que C/H soit de genre nul. Le deuxième point, appelé "théorème de transfert", permet de se ramener au cas d'une grosse action avec un G_2 d'ordre inférieur, en particulier au cas connu (cf. § 2.10) d'une grosse action dont le G_2 est cyclique d'ordre p. Enfin, si l'on déduit du deuxième point que pour une grosse action, G ne peut être abélien, on ignore pour l'heure s'il existe des grosses actions avec un G_2 non abélien.

La seconde partie de ce chapitre donne justement des exemples de grosses actions avec des G_2 abéliens, d'exposant quelconque. Pour produire une telle grosse action, l'idée est de considérer une courbe projective lisse connexe C et un revêtement galoisien $\pi : C \to \mathbb{P}^1_k$ de groupe H abélien, lequel jouera le rôle du G_2 de la grosse action. Il s'agit dès lors de construire un gros p-groupe de k-automorphismes de C en relevant un groupe suffisamment large de translations, lesquelles doivent laisser invariantes les équations de l'extension L/L^H, où L est le corps de fonctions de C. On retrouve ainsi la suite exacte (1.11).

Dans le sixième paragraphe de ce premier chapitre, on considère ainsi l'extension abélienne maximale K_S^m de $K = \mathbb{F}_q(X)$ ($q = p^e$) qui est non ramifiée en dehors de $X = \infty$, totalement décomposée au dessus de l'ensemble des places rationnelles de K à distance finie et de conducteur inférieur à $m\infty$, avec $m \in \mathbb{N}$. Ces extensions ont été étudiées par Auer ([Au99], [Au00]) et Lauter ([Lau99]) dans leur recherche de courbes algébriques avec beaucoup de points rationnels. La théorie du corps de classe nous donne une description précise du groupe de Galois $G_S(m)$ de l'extension K_S^m/K. De l'unicité et la maximalité de K_S^m, on déduit que le groupes des translations par $\mathbb{F}_q$ se prolongent en un p-groupe de $\mathbb{F}_q$-automorphismes de K_S^m : $G(m)$, ce qui donne une suite exacte semblable à (1.11) :

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

Ceci fournit des exemples de grosses actions avec un $G_2 = G_S(m)$ abélien d'exposant aussi grand que l'on veut. Ces exemples permettent aussi de relier le problème des grosses actions à celui des courbes algébriques avec beaucoup de points rationnels. Dans une dernière partie, on utilise enfin le théorème de Katz-Gabber pour mettre en lumière le lien entre les grosses actions sur les courbes et une condition analogue de ramification pour les p-groupes finis agissant sur $k((z))$.

1.4.2 Chapitre 3 : grosses actions dont le G_2 est p-abélien élémentaire.

Le troisième chapitre de cette thèse (cf. [Ro09]) est consacré à l'étude des grosses actions (C, G) dont le deuxième groupe de ramification G_2 est p-abélien élémentaire. Rappelons que G_2 est défini de manière purement algébrique puisqu'il coïncide avec le groupe dérivé de G.

Le cas d'une grosse action dont le G_2 est p-abélien élémentaire s'avère crucial dans l'étude et la classification des grosses actions. Ainsi, si (C, G) est une grosse action et si H est un sous-groupe de G strictement inclus dans G_2, nous avons vu dans le premier chapitre que $(C/H, G/H)$ est encore une grosse action dont le deuxième groupe de ramification est G_2/H. Si l'on applique ce résultat à $H = \mathrm{Fratt}(G_2)$ le sous-groupe de Frattini de G_2, on se ramène ainsi au cas d'une grosse action dont le deuxième groupe de ramification est p-abélien élémentaire. Une seconde motivation concerne la poursuite de la classification des grosses actions initiée par Lehr et Matignon [LM05]. En effet, nous avons vu au paragraphe 2.11 que les grosses actions vérifiant que $\frac{|G|}{g^2} \geq \frac{4}{(p-1)^2}$ corrrespondent aux revêtements p-cycliques étales de la droite affine paramétrés par une équation d'Artin-Schreier : $W^p - W = X\,S(X) + c\,X \in k[X]$ où S parcourt l'ensemble des polynômes additifs de $k[X]$(cf. § 2.11, Théorème 1.2.4) On désire à présent poursuivre cette classification des grosses actions sous la condition $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$. Or, nous avons vu dans le premier chapitre que cette condition impose que le G_2 soit un p-groupe abélien élémentaire d'ordre divisant p^3, d'où la nécessité de se pencher sur ce cas.

Le principal résultat de ce chapitre est le suivant :
Théorème : (Théorème 3.3.14) Soit (C, G) une grosse action telle que $G_2 (= D(G))$ soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$. Pour tout $t \geq 1$, on note Σ_t le sous-k-espace vectoriel de $k[X]$ engendré par 1 et le produit d'au plus t polynômes additifs. Alors, le corps de fonctions de C peut être paramétré par n équations d'Artin-Schreier de la forme :

$$\forall\, i \in \{1, \ldots, n\}, \quad W_i^p - W_i = f_i(X) \in \Sigma_{i+1}.$$

En d'autres termes, chaque f_i peut s'écrire comme combinaison linéaire sur k de produits d'au plus $i+1$ polynômes additifs de $k[X]$.

Ce résultat généralise le cas, étudié au paragraphe 1.2.10, d'une grosse action dont le G_2 est cyclique d'ordre p (cf. § 2.10, Thm. 1.2.2 et Prop. 1.2.3) Mais contrairement au cas $n = 1$, ce critère n'est pas une caractérisation et la réciproque n'est plus vraie dès que $n \geq 2$. Ainsi, une famille de fonctions (f_i) vérifiant ces conditions ne donnent pas nécessairement naissance à une grosse action. Les obtructions sont liées au problème de plongement évoqué dans le premier chapitre et lié à la suite exacte (voir (1.11)) :

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

Pour résoudre ce problème, on étudie la représentation induite

$$\phi : G/G_2 \to \mathrm{Aut}(G_2) \simeq \mathrm{GL}_n(\mathbb{F}_p),$$

via la représentation duale pour le pairing d'Artin-Schreier. Cette dernière exprime l'action de V par translation sur les équations paramétrant la courbe, équations qui sont définies modulo $(F - id)(k[X])$.

On se concentre ensuite sur deux cas particuliers. Au paragraphe 4, on étudie d'abord le cas où il n'y a qu'un seul saut dans la filtration de ramification de G_2. Dans ce cas, les représentations mentionnées ci-dessus sont triviales et chacune des fonctions f_i est dans Σ_2. Dans le paragraphe 5, on étudie la situation que l'on pourrait qualifier d'opposée : celle où chaque f_i est dans $\Sigma_{i+1} - \Sigma_i$. On donne tout d'abord une caractérisation de ce cas au moyen d'arguments issus de la théorie des groupes. On montre alors que, sous cette condition, le nombre de sauts dans la filtration de ramification de G_2 est maximale. On calcule ensuite le degré des fonctions f_i et la dimension v du k-espace vectoriel V. Le dernier paragraphe est consacré à des exemples de familles illustrant les résultats du paragraphe 5. Pour $p = 5$, $n \leq p-1$ et $\dim_k V = 2$, on exhibe des familles universelles, ce qui permet de discuter de l'espace des déformations. On peut en particulier comparer la dimension obtenue avec les bornes données par Pries (voir § 2.11).

1.4.3 Chapitre 4 : classification des grosses actions vérifiant $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Le but de ce dernier chapitre (cf. [Ro08]) est de poursuivre la classification des grosses actions amorcée au paragraphe 1.2.11. Nous poursuivons ici cette classification sous la condition $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$, sachant que nous avons montré dans le premier chapitre que cette borne impose que le deuxième groupe de ramification G_2 soit p-abélien élémentaire d'ordre divisant p^3. Grâce aux résultats du deuxième chapitre, on connaît par ailleurs la forme des équations de la courbe dans un tel cas.

Ce dernier chapitre se divise en deux parties. Dans la première, on s'intéresse à la finitude du nombre de valeurs prises par les quotients $\frac{|G|}{g}$ et $\frac{|G|}{g^2}$ pour les grosses actions (C, G) satisfaisant la condition $\mathcal{G}_M$, i.e. les grosses actions telles que $\frac{|G|}{g^2} \geq M$, pour $M > 0$ un entier fixé. Dans la seconde partie, on réalise la classification de ces grosses actions lorsque $M = \frac{4}{(p^2-1)^2}$.

Résumons ici les principaux résultats de la première partie, qui seront autant d'outils pour la classification de la seconde partie.

Proposition : Soit $M > 0$ un entier fixé et soit (C, G) une grosse action satisfaisant $\mathcal{G}_M$. Alors, l'ordre de G_2 ne prend qu'un nombre fini de valeurs. (Lemme 4.4.1).

En s'interrogeant de même sur la finitude des valeurs prises par g, $|G|$ et donc par le quotient $\frac{|G|}{g}$ lorsque (C, G) satisfait $\mathcal{G}_M$, nous sommes amenés à discuter de l'inclusion $\mathrm{Fratt}(G_2) \subset [G_2, G]$, où $\mathrm{Fratt}(G_2)$ est le sous-groupe de Frattini de G_2 et $[G_2, G]$ le commutateur de G_2 et de G. Ces deux groupes revêtent en effet une importance particulière pour notre problème. La trivialité de $\mathrm{Fratt}(G_2)$ caractérise le fait que G_2 soit p-abélien élémentaire. La trivialité de $[G_2, G]$ équivaut quant à elle au fait que G_2 est inclus dans le centre de G, i.e. que le représentation $\phi : G/G_2 \to \mathrm{Aut}(G_2)$ évoquée au chapitre 2 est triviale.

Proposition : Soit $M > 0$ un entier fixé et soit (C, G) une grosse action satisfaisant $\mathcal{G}_M$.

1. Si $\mathrm{Fratt}(G_2) \subsetneq [G_2, G]$, le quotient $\frac{|G|}{g}$ ne peut prendre qu'un nombre fini de valeurs (Proposition 4.4.6 et Corollaire 4.4.7).
2. Si $\mathrm{Fratt}(G_2) = [G_2, G]$, le résultat précédent n'est plus vrai ; c'est seulement le quotient $\frac{|G|}{g^2}$ qui prend un nombre fini de valeurs, lorsque G_2 est abélien et lorsque $p > 2$ (Proposition 4.4.9 et Corollaire 4.4.11).

On montre en réalité un résultat plus fort que ce second point :
Théorème : Supposons que $p > 2$. Soit (C, G) une grosse action telle que $\mathrm{Fratt}(G_2) = [G_2, G] \neq \{e\}$. Alors, G_2 est non abélien (Théorème 4.4.10).

Rappelons que l'on ignore encore s'il existe des grosses actions dont les G_2 soient non abéliens.

Dans la première partie de ce chapitre, on cherche d'autre part à faire le lien entre les sous-groupes G de $\mathrm{Aut}_k(C)$ tels que (C, G) soit une grosse action et le p-sous-groupe de Sylow S_p de $\mathrm{Aut}_k(C)$ contenant G (voir § 3). Le résultat principal est que G et S_p possèdent le même groupe dérivé, c'est-à-dire, pour une grosse action, le même deuxième groupe de ramification. Dans notre classification, on pourra donc se restreindre au cas des seuls p-Sylow de $\mathrm{Aut}_k(C)$.

Dans la seconde partie de ce chapitre, on donne enfin la classification et la paramétrisation des grosses actions (C, G) vérifiant $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$. Selon l'ordre de G_2 et selon si l'inclusion $\{e\} = \mathrm{Fratt}(G_2) \subset [G_2, G]$ est stricte ou non, on précise les équations des fonctions f_i, de l'espace V des translations et on décrit le groupe G. Ceci est l'occasion d'une discussion autour des espaces de déformation de telles actions. On peut à nouveau comparer la dimension obtenue avec les bornes données par Pries (voir § 1.2.11).

Chapitre 2

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

2.1 Introduction.

Setting and motivation. This chapter is the first of a set of three papers (together with [Ro09] and [Ro08]), 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 $|G| > \frac{2\,p}{p-1}\,g$. One of our aims is to display some universal families and to 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 C of genus $g \geq 2$ was proved by Hurwitz to be finite and of order at most $84\,(g-1)$ (cf. [Hur92]). An open question concerns the classification of full automorphism groups of compact Riemann surfaces 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 $4\,(g-1)$ (cf. [Ku91]). 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 (cf. [Ku91] and [Br00] Lemma 3.18). Following the works of Kulkarni, Kuribayashi and Breuer, Magaard et alii ([MSSV02]) exhibited the list of large groups $\mathrm{Aut}(C)$ 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 e.g.[BeRo08]). 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 $3g_0 - 3 + |\mathcal{B}| + \dim \mathrm{Aut}\,(C/G - \mathcal{B})$, 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 widly 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 (cf. [Sch38]) but the Hurwitz linear bound is replaced with biquadratic bounds (cf. [St73]). 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 (cf. [BeMe00], [CoKa03], [Pr05] and [Kon07]). Following Bertin and Mézard's work in the case where G is cyclic of order p (cf. [BeMe00]), Pries ([Pr05]) and Kontogeorgis ([Kon07]) 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.

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's work (cf. [Na87a]), we deduce that if G is a p-subgroup of $\mathrm{Aut}_k(C)$ such that $|G| > \frac{2\,p}{p-1}\,g$, the Hasse-Witt invariant of C is zero. The Deuring-Shafarevich formula (see e.g. [Bou00]) 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 $|G| > \frac{2\,p}{p-1}\,g$.

Outline of the chapter. Let (C, G) be a big action with $g \geq 2$. As shown in [LM05], 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 chapter 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 2.2 to 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 2.2.4.1).
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 2.2.4.2).
3. The group G_2 is equal to $D(G)$, the commutator subgroup of G (Thm. 2.2.7).
   In particular, G cannot be abelian.
4. The group G_2 cannot be cyclic unless G_2 has order p (Thm. 2.5.1).
5. If $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$, then G_2 is an elementary abelian p-group with order dividing p^3 (Prop. 2.4.1).

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 by Lehr and Matignon (cf. [LM05]). Chapter 3 is devoted to big actions with a p-elementary abelian G_2, and its results led to the classification of the big actions satisfying $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$ (cf. [Ro08] or Chapter 4).

After exploring restrictions on G_2, the second part of this chapter 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 2.6, following [Lau99] and [Au99], 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 $\{X \to X + y,\, y \in \mathbb{F}_q\}$ 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 also relates the problem of big actions to the search of algebraic curves with many rational points compared with their genera.

In Section 2.7, 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 (see [Go96] chap. 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 $\mathrm{red}(f)(X) = f(X) \mod \wp(k[X])$. 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 $\mathrm{Spec}\,k[X]$

corresponds to a curve C_f where f is a polynomial of $k[X]$ (see [Mi80] III.4.12, p. 127). By Artin-Schreier theory, the covers C_f and $C_{\mathrm{red}(f)}$ 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 [Se68] and [Au99].

2.2 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 [LM05]. 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 2.2.1. *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 2.2.2. *[LM05] 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 ∞ : G_1. Moreover, the quotient C/G is isomorphic to the projective line $\mathbb{P}^1_k$ and the ramification locus (respectively branch locus) of the cover $\pi : C \to C/G$ is the point ∞ (respectively $\pi(\infty)$). For all $i \geq 0$, we denote by G_i the i-th lower ramification group of G at ∞. Then*

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 :*

$$2\,g = \sum_{i \geq 2} (|G_i| - 1). \tag{2.2}$$

In particular, (2.1) can be written as $|G| > \frac{2\,g}{p-1}\,p$, with $\frac{2\,g}{p-1} \in \mathbb{N}^*$.

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 $X \to X + y$, 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

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

4. *Let H be a normal subgroup of G such that $g_{C/H} > 0$. Then $(C/H, G/H)$ is also a big action. Moreover, the group G/H fixes the image of ∞ 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 quarternion group of order 8 (see [Si86], Appendix A, Prop. 1.2).*

Remark 2.2.3. 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.*

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 [Se68] Chap.15 Cor.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 [Au00] I.3).*

The following lemma generalizes and completes the last part of Proposition 2.2.2.

Lemma 2.2.4. *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 :

1. Applied to the cover $C \to C/G \simeq \mathbb{P}^1_k$, the Hurwitz genus formula (see e.g. [St93]) 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 $2(g-1) = 2|H|\,(g_{C/H}-1)+\sum_{i\geq 0}(|H\cap G_i\rceil -1)$. 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.
2. Together with part 1, Proposition 2.2.2.4 shows that $(C/H, G/H)$ is a big action. Then $G = G_1 \supsetneq G_2$ (resp. $G/H = (G/H)_1 \supsetneq (G/H)_2$). 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 [Se68] (Second Part, Chap. IV, Prop. 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 in [LM05] (cf. Prop. 5.5, 8.1 and 8.3).

Proposition 2.2.5. *[LM05]. 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*
$$G = G_0 = G_1 \supsetneq G_2 = G_3 = \ldots = G_{i_0} \supsetneq G_{i_0+1} = \ldots =$$
2. *Write $S(F) = \sum_{j=0}^{s} a_j F^j$, with $a_s \neq 0$. Following [El97] (Section 4), define the palindromic polynomial of f as the additive polynomial*
$$\mathrm{Ad}_f := \frac{1}{a_s^{p^s}}\,F^s\,(\sum_{j=0}^{s} a_j\,F^j + F^{-j}\,a_j).$$
The set of roots of Ad_f, denoted by $Z(\mathrm{Ad}_f)$, 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 following 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
$$\pi : \begin{cases} A_{\infty,1} \to Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \\ g \to g(X) - X. \end{cases}$$
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 [LM05] 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 2.2.6. *Proposition 2.2.5 still holds for big actions (C, G) with $g = 1$ when G is included in a decomposition group of $\mathrm{Aut}_k(C)$ ([LM05] Prop. 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 Prop. 2.2.2.4).*

Therefore, the key idea in studying big actions is to use Proposition 2.2.2.4 and Lemma 2.2.4.2 to go back to the well-known situation described above. This motivates the following result :

Theorem 2.2.7. *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. Then 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 2.2.2 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 of f (Proposition 2.2.5). 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 [Su82] (Chap. 2, Thm. 1.12). The first assertion now follows from Lemma 2.2.4.2. The second and third derive directly from Proposition 2.2.5.

We now prove part 4. By Proposition 2.2.5, $Z(E) = (G/H)_2 = G_2/H \subset G/H$. 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, [Hu67] (Satz 13.7) implies $|G/H| \leq p^{s+1}$. Furthermore, by Theorem 2.2.5.1 (and Remark 2.2.6), 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 $g_{C/H} = \frac{p-1}{2}\,p^s$. Combined with the bound on $|G/H|$, this gives $\frac{|G/H|}{g_{C/H}} \leq \frac{2\,p}{p-1}$, 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, $\mathrm{Fratt}(G)$, is equal to $D(G)G^p$, where G^p means the subgroup generated by the p powers of elements of G (cf. [LGM02] Prop. 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 2.2.8. *When applying Theorem 2.2.7 to $\mathcal{G} = G_{i_0+1}$, where i_0 is defined as in Proposition 2.2.5, one obtains Theorem 8.6(i) of [LM05]. 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 2.2.7 the following result.

Corollary 2.2.9. *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 2.2.10. *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. But G_2 is a p-group, normal in G and included in $D(G)$ (see Theorem 2.2.7). Hence, by [Su86] (Prop. 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 2.2.11. *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 [Su82], Chap. 2, Thm. 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 2.2.7.4, $\mathcal{G}_2 = D(\mathcal{G})$. Since (C, G) is a big action, $g(C/D(G))$ vanishes by Proposition 2.2.2.3. It follows from Lemma 2.2.4.1 that $D(G) \supset \mathcal{G}_2 = D(\mathcal{G})$, hence $D(G) = D(\mathcal{G})$. The claim follows by reiterating the process. □

Remark 2.2.12. *Let $(C, A_{\infty,1})$ be a big action as in Corollary 2.2.11. Then $A_{\infty,1}$ is a p-Sylow subgroup of $\mathrm{Aut}_k(C)$. Moreover, we deduce from [GK07] (Thm. 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 [GK07], Thm. 1.1).*

2.3 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 2.3.1. *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 $\frac{|\tilde{G}|}{g_{\tilde{C}}} = \frac{|G|}{g}$. 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 following 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 2.3.2. *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 $L := K_0 K_1$.*

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

Suppose that the conductor of K_0/K (see Rem. 2.2.3.2) is 2. *Then L/K_1 also has conductor* 2.

Proof : Consider a chief series of $\mathcal{G}$ (cf. [Su82], Chap. 2, Thm. 1.12), 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 $K_0 K_1^{\mathcal{G}_i}/K_1^{\mathcal{G}_i}$ 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 :

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

1. 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 $H = Gal(L/K_0)$, case (β) gives $i_0 = 1$. Therefore, one concludes by applying case (α) to $H = Gal(L/K_1)$.
2. 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 e.g. [Se68] Chap. IV) 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. $i_0 + \frac{i_1}{p} + 1$).

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

Lemma 2.3.3. *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 $\frac{W}{W_i}$.*

This induces the diagram :

$$\begin{tikzcd}
k(T_1) \arrow[r, dash, "W_1"] \arrow[d, dash, "\frac{W}{W_1}"] & k(Z) \arrow[d, dash, "W_2"] \\
k(T) \arrow[r, dash, "\frac{W}{W_2}"] & k(T_2)
\end{tikzcd}$$

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

Proof of Proposition 2.3.1 :

1. Statement 1 derives from Lemma 2.2.4.1.
2. Put $W := S^{-1}(V)$, with V defined as in Proposition 2.2.2.3, 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 e.g. [Go96] chap. 1). Let W_2 be any $\mathbb{F}_p$-vector subspace of W such that $W = W_1 \bigoplus W_2$. Then Lemma 2.3.3 applied to the extension $k(Z)/k(T)$ induces the diagram :

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

In particular, Lemma 2.3.3 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 $\frac{W}{W_2} \simeq W_1 \simeq (\mathbb{Z}/p\mathbb{Z})^s$, it follows that $k(\tilde{C})/k(T)$ is a Galois extension with group $\tilde{G} \simeq Gal(k(C)/k(T)) \times Gal(k(Z)^{W_2}/k(T)) \simeq G \times (\mathbb{Z}/p\mathbb{Z})^s$.
Now, consider a flag of $\mathbb{F}_p$-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 2.3.2, 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 2.2.4.1. As a consequence, K_0 and K_1 are linearly disjoint over K and, by Lemma 2.3.2, 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 2.2.7.4. □

Remark 2.3.4. *Under the conditions of Proposition 2.3.1, 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 $\tilde{W}^p - \tilde{W} = (Z^p - Z)\,(Z^{p^2} - Z^p) = -Z^2 + 2\,Z^{1+p} - Z^{1+p^2}$ mod $\wp(k[Z])$. 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 2.2.5, we deduce that* $|\tilde{G}| = p\,|G| = p\,|A_{\infty,1}(C)| = p^4$, *whereas* $|A_{\infty,1}(\tilde{C})| = p^5$.

2.4 A new step towards a classification of big actions.

If big actions are defined through the value taken by the quotient $\frac{|G|}{g}$, it turns out that the key criterion to classify them is the value of another quotient, $\frac{|G|}{g^2}$. Indeed, the quotient $\frac{|G|}{g^2}$ has, to some extent, a sieve effect among big actions. If (C, G) is a big action, we first deduce from [Na87a] (Thm.1) that $\frac{|G|}{g^2} \leq \frac{4\,p}{(p-1)^2}$. 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 $\frac{|G|}{g^2} = \frac{4\,p}{(p-1)^2}$ and $\frac{|G|}{g^2} = \frac{4}{(p-1)^2}$ (cf. [LM05] Thm. 8.6). More precisely, we investigate the big actions (C, G) that satisfy

$$M := \frac{4}{(p^2-1)^2} \leq \frac{|G|}{g^2}. \tag{2.3}$$

The choice of the lower bound M can be explained as follows : as shown in the proof of ([LM05], Thm. 8.6), a lower bound M on the quotient $\frac{|G|}{g^2}$ produces an upper bound on the order of the second ramification group, namely

$$|G_2| \leq \frac{4}{M} \frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}|-1)^2}, \tag{2.4}$$

where i_0 is defined as in Proposition 2.2.5. Therefore, we have to choose M small enough to obtain a wide range of possibilities for the quotient, but meanwhile large enough to get serious restrictions on the order of G_2. The optimal bound seems to be $M := \frac{4}{(p^2-1)^2}$, 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 2.2.10).

Proposition 2.4.1. *Let (C, G) be a big action with $g \geq 2$ satisfying condition* (2.3)*. 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 $m \geq 1$, 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 (2.4) becomes : $1 < |G_2| = p^m |G_{i_0+1}| \leq p^m Q_m$, which gives : $1 \leq |G_{i_0+1}| \leq Q_m$. Since $(Q_m)_{m \geq 1}$ is a decreasing sequence with $Q_4 < 1$, we conclude that $m \in \{1, 2, 3\}$.

If $m = 3$, then $1 \leq |G_{i_0+1}| \leq Q_3 < p$. So $|G_{i_0+1}| = 1$ and $|G_2| = p^3$. If $m = 2$, then $1 \leq |G_{i_0+1}| \leq Q_2 = p^2$. 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 (4.1) 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 2.2.8. Then $i_0 = 1 + p^s$. Besides, by Theorem 2.2.7, $V \subset (\mathbb{Z}/p\mathbb{Z})^{2s}$. 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 (2.3).

If $m = 1$, then $1 \leq |G_{i_0+1}| \leq Q_1$ with $Q_1 := p\,(p+1)^2 < \left\{ \begin{array}{ll} p^4\,, & if\, p \geq 3 \\ p^5\,, & if\, p = 2 \end{array} \right.$.

Because G_{i_0+1} is a p-group, we get : $\begin{cases} 1 \leq |G_{i_0+1}| \leq p^3\,, & if\, p \geq 3 \\ 1 \leq |G_{i_0+1}| \leq p^4\,, & if\, p = 2 \end{cases}$. 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 $\epsilon = 1$, (4.1) yields $2\,g \geq (i_0 - 1)(p^5 - 1)$. Since this case only occurs for $p = 2$, we eventually get an inequality :

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

which contradicts condition (2.3). Therefore, the order of G_2 divides p^3. Then we conclude from Corollary 2.2.10 that G_2 is abelian. □

But we can even prove better :

Proposition 2.4.2. *Let (C, G) be a big action with $g \geq 2$ satisfying condition (2.3).Then G_2 is abelian with exponent p.*

Proof : By Proposition 2.4.1, 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 2.6).

Lemma 2.4.3. *Let (C, G) be a big action with $g \geq 2$ satisfying condition (2.3). Then G_2 cannot be isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

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

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

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

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

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

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 reads

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

Consider the upper ramification groups : $H^{\nu_0} = H^{\varphi(i_0)} = H_{i_0}$ and $H^{\nu_1} = H^{\varphi(i_0+i_1)} = H_{i_0+i_1}$, where φ denotes the Herbrand function (cf. [Se68] IV.3). Then the ramification filtration in upper notation reads

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

Since H is abelian, it follows from Hasse-Arf theorem (loc. cit.) that ν_0 and ν_1 are integers. Consequently, the equality

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

gives $\nu_0 = i_0$ and $\nu_1 = i_0 + \frac{i_1}{p^2}$. By [Mar71] (Thm. 6), we have $H^{\nu_0} \supsetneq H^{p\,\nu_0} \supset (H^{\nu_0})^p$ with $(H^{\nu_0})^p = H^p = G_2^p \simeq \mathbb{Z}/p\mathbb{Z}$. Thus, $H^{p\nu_0} \supset H^{\nu_1}$, which implies $p\nu_0 \leq \nu_1$ 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 2.2.8. Then $i_0 = 1 + p^s$. Moreover, by Theorem 2.2.7, $|G| = |G_2||V| \leq p^{3+2s}$. 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 $\frac{p^3(p+1)^2}{(p^3+p+1)^2} < 1$ for $p \geq 2$, this contradicts condition (2.3).

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

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

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

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

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

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

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

In case iii), the lower ramification filtration of H becomes

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

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

$$H^{\nu_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_0+1} = \ldots = H^{\nu_1} \simeq (\mathbb{Z}/p\mathbb{Z})^2 \supset H^{\nu_1+1} = \ldots = H^{\nu_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_2+1} = \{0\},$$

with $\nu_0 = \varphi(i_0) = i_0$, $\nu_1 = \varphi(i_0+i_1) = i_0 + \frac{i_1}{p}$ and $\nu_2 = \varphi(i_0+i_1+i_2) = i_0 + \frac{i_1}{p} + \frac{i_2}{p^2}$. 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 $p\,\nu_0 \le \nu_2$, which involves $p^2\,(p-1)\,i_0 \le i_1\,p + i_2$. With such inequalities, the Hurwitz genus formula gives a new lower bound for the genus, namely

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

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

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

Since $\frac{p\,(p+1)^2}{(p^2+1)^2} < 1$ for $p \ge 2$, this contradicts condition (2.3).

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

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

induces the upper ramification filtration

$$H^{\nu_0} \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_0+1} = \ldots = H^{\nu_1} \simeq (\mathbb{Z}/p^2\mathbb{Z}) \supset H^{\nu_1+1} = \ldots = H^{\nu_2} \simeq \mathbb{Z}/p\mathbb{Z} \supset H^{\nu_2+1} = \{0\}.$$

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

Remark 2.4.4. *The previous method, based on the analysis of the ramification filtration of G_2, fails to exclude the case $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$ for a big action satisfying* (2.3)*. Indeed, if $H := G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$, the lower ramification filtration of H*

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

induces the upper ramification filtration

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

with $\nu_0 = \varphi(i_0) = i_0$ and $\nu_1 = \varphi(i_0+i_1) = i_0 + \frac{i_1}{p}$. 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 2.2.8. Then the Hurwitz genus formula yields :

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

If we denote by v the dimension of the $\mathbb{F}_p$-vector space V, we eventually 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 (2.3) *requires $p^{1+\frac{v}{2}-s}(p+1) > p^2$. Since $\frac{v}{2} \le s$, this implies $p+1 > p^{1+s-\frac{v}{2}} \ge p$, hence $\frac{v}{2} = s$. This means that $V = Z(\mathrm{Ad}_f)$, where f is the function defined in Remark 2.2.8 and Ad_f its palindromic polynomial as defined in Proposition 2.2.5. 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 2.4.2, 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.

2.5 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 [Bour83] (Chap. IX).

Theorem 2.5.1. *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 2.2.4.2 asserts that the pair $(C/\mathcal{H}, G/\mathcal{H})$ is a big action. Besides, the second lower ramification group of $G/\mathcal{H}$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

2. *Notation and 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 (see [Bour83] Chap. IX, ex. 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 [Mi80] (III, 4.12) that we can identify A with $\tilde{A}$. Consider the Artin-Schreier-Witt pairing

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

   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 in Section 2.1). 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 2.2.5 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 2.4.4 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).

3. *The embedding problem.*
   Let V be the $\mathbb{F}_p$-vector space defined in Proposition 2.2.2.3. 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

$$\mathbb{Z}(f_0(X), g_0(X)) \;=\; \mathbb{Z}(f_0(X+y), g_0(X+y)) \quad \bmod \wp(W_2(k[X])). \tag{2.5}$$

   Since A is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, (2.5) ensures the existence of an integer $n(y)$ such that

$$(f_0(X+y), g_0(X+y)) = n(y)\,(f_0(X), g_0(X)) \qquad \bmod \wp(W_2(k[X])), \tag{2.6}$$

   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

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

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

$$c(1) = 1 \qquad \text{and} \qquad \forall\, i \in \mathbb{N}, \quad c(i+1) = c(i) + \frac{1}{p}\,(1 + i^p - (1+i)^p) \qquad \bmod\ p.$$

On the other hand,

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

Consequently, (2.6) becomes

$$(f_0(X+y), g_0(X+y)) = (a_0(y) f_0(X), a_0(y) g_0(X) + \ell_0(y) f_0(X)) \quad \bmod\ \wp(W_2(k[X])), \tag{2.7}$$

where $\ell_0(y) := c(a_0(y)) + b_0(y)$. We notice that $a_0(y) = 1 \bmod p$, for all y in V. Indeed, the equality of the first coordinate of Witt vectors in (4.6) implies that $f_0(X+y) = a_0(y)\, f_0(X) \ \bmod\ \wp(k[X])$. Thus, by induction, $f_0(X+py) = a_0(y)^p\, f_0(X) \ \bmod\ \wp(k[X])$. Since V is an elementary abelian p-group, $f_0(X+py) = f_0(X)$, which entails $a_0(y)^p = 1 \bmod p$ and $a_0(y) = 1 \bmod p$. So (4.6) becomes

$$(f_0(X+y), g_0(X+y)) = (f_0(X), g_0(X) + \ell_0(y) f_0(X)) + (P^p(X), Q^p(X)) - (P(X), Q(X)), \tag{2.8}$$

with $P(X)$ and $Q(X)$ polynomials of $k[X]$. In order to circumvent the problem related to the special formula giving the opposite of Witt vectors for $p = 2$, we would rather write (2.8) as follows

$$(f_0(X+y), g_0(X+y)) + (P(X), Q(X)) = (f_0(X), g_0(X) + \ell_0(y)\, f_0(X)) + (P(X)^p, Q(X)^p). \tag{2.9}$$

The first coordinate of (2.9) reads

$$f_0(X+y) + P(X) = f_0(X) + P(X)^p. \tag{2.10}$$

On the second coordinate of (2.9), the addition law in the ring of Witt vectors gives in $k[X]$ the equality

$$g_0(X+y) + Q(X) + \psi(f_0(X+y), P(X)) = g_0(X) + \ell_0(y)\, f_0(X) + Q(X)^p + \psi(f_0(X), P(X)^p), \tag{2.11}$$

where ψ is defined by

$$\psi(a,b) := \frac{1}{p}\,(a^p + b^p - (a+b)^p) = \frac{-1}{p} \sum_{i=1}^{p-1} \binom{p}{i} a^i\, b^{p-i} = \sum_{i=1}^{p-1} \frac{(-1)^i}{i}\, a^i\, b^{p-i} \qquad \bmod\ p.$$

As a consequence, (2.11) gives

$$\Delta_y(g_0) := g_0(X+y) - g_0(X) = \ell_0(y)\, f_0(X) + \delta \qquad \bmod\ \wp(k[X]), \tag{2.12}$$

with

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

Lemma 2.5.2. *With the notation defined above, δ is equal to*

$$\delta = \sum_{i=1}^{p-1} \frac{(-1)^i}{i}\, y^{p-i} X^{i+p^{s+1}} + \textit{lower-degree terms in } X\ . \tag{2.13}$$

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 (2.10) that $P(X)$ has degree p^{s-1} and that its leading coefficient is $y^{1/p}$. By [LM05] (see proof of Prop. 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 $\{1, \ldots, p-1\}$, $f_0(X)^i\, P(X)^{p\,(p-i)} = f_0(X)^i\,(y\, X^{p^s} + P_1(X)^p)^{p-i} = f_0(X)^i\, (\sum_{j=0}^{p-i} \binom{p-i}{j}\, y^j\, X^{jp^s}\, P_1(X)^{p(p-i-j)})$. 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 $j \leq p-i-1$, this degree is at most $p^s + (p-1)^2\, p^{s-1} + i = (p-1)\,p^s + p^{s-1} + i$, which is strictly less than $p^{s+1}+1$, for $s \geq 2$ and $1 \leq i \leq p-1$. 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 $\{1, \ldots, p-1\}$, we have $f_0(X)^i\, y^{p-i}\, X^{p^s(p-i)} = y^{p-i}\, X^{p^s(p-i)}\, (\sum_{k=0}^{i} \binom{i}{k} X^{(1+p^s)j}\, P_2(X)^{i-k})$. Accordingly, we get a monomial of degree at most $p^s\,(p-i) + k\,(1+p^s) + (i-k)\,(1+p^{s-1})$, 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 stricly lower than $p^{s+1}+1$. Therefore, for all i in $\{1, \dots, p-1\}$, the only contibution 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. □

4. *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 (2.12) 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 2.5.2, $\deg f_0 = 1 + p^s < \deg \delta = p^{s+1} + p - 1$, which involves that the degree of the right-hand side of (2.12) is $p - 1 + p^{s+1} > 1$, hence a contradiction.
Therefore, we can define an integer $a \leq n_0 = \deg g_0$ such that X^a is the monomial of $g_0(X)$ with highest degree which is not of the form $1 + p^n$, with $n \in \mathbb{N}$. Note that since g_0 is reduced mod $\wp(k[X])$, $a \not\equiv 0 \mod p$. We also notice that the monomials in $g_0(X)$ with degree strictly 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 (2.12) is at most $a-1$. Since the degree of the right-hand side is $p^{s+1} + p - 1$, it follows that
$$a - 1 \geq p^{s+1} + p - 1. \tag{2.14}$$

5. *We show that p divides $a-1$.*
Assume that p does not divide $a-1$. In this case, the monomial X^{a-1} is reduced mod $\wp(k[X])$. Since the monomials of $g_0(X)$ with degree greater than a only give a linear contribution in $\Delta_y(g_0)$ mod $\wp\,(k[X])$, (2.12) reads as follows, for all y in V :
$$c_a(g_0)\, a\, yX^{a-1} + \text{lower-degree terms } = -y\, X^{p^{s+1}+p-1} + \text{ lower degree terms } \mod \wp\,(k[X]),$$
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 2.2.2.1). We gather from (2.14) 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 $\lambda \geq 2$.

6. *We determine the coefficient of X^{j_0} in the left hand-side of* (2.12).
Since p does not divide j_0, the monomial X^{j_0} is reduced mod $\wp(k[X])$. On the left-hand side of (2.12), 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 (2.12) 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 $a - j_0 = p^t$.

7. *We identify with the coefficient of X^{j_0} in the right-hand side of* (2.12) *and obtain a contradiction.*
We first assume that the monomial X^{j_0} does not occur in the right-hand side of (2.12). Then $T(y) = 0$

for all y in V, which means that V is included in the set of roots of T. Thus, $|V| \leq p^t$. To compute the genus g, put $M_0 := m_0$ and $M_1 := \max\{p\, m_0,\, n_0\}$. Then, by [Ga99], 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 a lower bound for the genus $2\,g = (p-1)\,p\,(n_0 - 1 + p^{s-1}) \geq 2\,p^{t+1}\,(p-1)$. 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 (2.12), which implies that $j_0 \leq p^{s+1} + p - 1$. Using (2.14), we get $j_0 = 1 + (\lambda - 1)\,p^t \leq p^{s+1} + p - 1 < a = 1 + \lambda\, p^t$. This yields

$$\lambda - 1 \leq p^{s+1-t} + \frac{p-2}{p^t} < \lambda. \tag{2.15}$$

If $s + 1 - t \leq -1$, since $t \geq 1$, (2.15) gives : $\lambda - 1 \leq \frac{1}{p} + \frac{p-2}{p} < 1$, which contradicts $\lambda \geq 2$. It follows that $s+1-t \geq 0$. Then (2.15) combined with the inequalities $0 \leq \frac{p-2}{p^t} < 1$ leads to $\lambda - 1 = p^{s+1-t}$. We gather that $j_0 = 1 + (\lambda-1)\,p^t = 1 + p^{s+1} > \deg f_0 = 1 + p^s$. Therefore, in the right-hand side of (2.12), the monomial $X^{j_0} = X^{1+p^{s+1}}$ only occurs in δ. By Lemma 2.5.2, 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 (2.12), 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 $|V| \leq p^t$, 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 $n \geq 2$, 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 2.5.1, 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 $t = O(\log_p g)$.

2.6 Examples of big actions with G_2 abelian of exponent strictly greater than p.

In characteristic 0, an anologue of big actions is given by the actions of a finite group G on a compact Riemann surface C with genus $g_C \geq 2$ such that $|G| = 84(g_C - 1)$. Such a curve C is called a *Hurwitz curve* and such a group G a *Hurwitz group* (cf. [Con90]). In particular, the lowest genus Hurwitz curves are the Klein's quartic with $G \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ (cf. [El99]) and the Fricke-Macbeath curve with genus 7 and $G \simeq \mathrm{PSL}_2(\mathbb{F}_8)$ (cf. [Mc65]).

Let C be a Hurwitz curve with genus g_c. Let $n \geq 2$ be an integer and let C_n be the maximal unramified Galois cover whose group is abelian, with exponent n. The Galois group of the cover C_n/C is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. We infer from the uniqueness of C_n that the $\mathbb{C}$-automorphims 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 [Mc61]).

Now let (C, G) be a big action. Then $C \to C/G$ is an étale cover of the affine line whose group is a p-group. From the Deuring-Shafarevich formula (see e.g. [Bou00]), 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 mentionned 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 [Lau99] and R. Auer [Au99]. Since the cover $C \to C/G_2$ is an étale cover of the affine line $\mathrm{Spec}\, k[X]$ totally ramified at ∞, we focus on the special case of ray class fields of the rational function field $\mathbb{F}_q(X)$, where $q = p^e$ (see [Au99], III.8). Such ray class fields allow us to produce families of big actions (C, G) (where C is defined over $k = \mathbb{F}_p^{alg}$) with specific conditions imposed on ramification and endowed with an abelian G_2 of exponent as large as we want.

Definition 2.6.1. *([Au99], 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 $K_S^m \subset K^{alg}$ as the largest abelian extension L/K with conductor $\leq m\,\infty$, such that every place in S splits completely in L.*

Remark 2.6.2. 1. *We define the splitting set $S(L)$ of any finite Galois extension L/K 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 2.6.1, 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 reduces 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 2.6.1.*

Remark 2.6.3. *We keep the notation of Definition 2.6.1.*

1. *The existence of the extension K_S^m/K is based on global class field theory (see [Au99], 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 $\{0, \ldots, r+1\}$, $K_S^i = K = \mathbb{F}_q(X)$. (see [Au99], 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 e.g. [St93] V.2.3), 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 $G_S(m)$ (see [Lau99], Thm. 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 2.6.4. *([Lau99], Prop. 4) We keep the notation defined above. If $q = p^e$, the smallest conductor m for which the group $G_S(m)$ is not of exponent p is $m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$, where $\lceil . \rceil$ 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 $C^{alg} := C \times_{\mathbb{F}_q} k$ with $k = \mathbb{F}_p^{alg}$. If G is a finite p-subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(C)$, then G can be identified with a subgroup of $\mathrm{Aut}_k(C^{alg})$. In this case, (C^{alg}, G) is a big action if and only if $g_{C^{alg}} = g_C > 0$ and $\frac{|G|}{g_C} > \frac{2\,p}{p-1}$. 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 2.6.5. *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*

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

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

3. *Let L be an intermediate field of K_S^m/K. Define $n := \min\{i \in \mathbb{N}, L \subset K_S^i\}$. Then the genus of the extension L/K is given by the formula :*
$$g_L = 1 + [L:K]\,(-1+\frac{n}{2}) - \frac{1}{2}\sum_{j=0}^{n-1}[L \cap K_S^j : K],$$
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, $g_L < [L:K]\,(-1+\frac{n}{2})$.

4. *If $m \geq r+2$, $\frac{|G(m)|}{g_{K_S^m}} > \frac{q}{-1+\frac{m}{2}}$. It follows that if $\frac{q}{-1+\frac{m}{2}} \geq \frac{2\,p}{p-1}$, 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 2.6.4, 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 $X \to X + y$, $y \in \mathbb{F}_q$. 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 uniqueness 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 [Au99] (II, Thm. 5.8).
3. The genus formula is obtained by combining the preceding results, the Hurwitz genus formula and the discriminant formula (see [Au99], I, 3.7). Now assume that $n = 0$. Then $L \subset K_S^0 = \mathbb{F}_q(X)$ and $g_L = 0$. Conversely, assume $g_L = 0$. If $n \neq 0$, Remark 2.6.3.4 implies that $n \geq r + 2 \geq 3$. Using the preceding formula and Remark 2.6.3.4, $g_L = 0$ 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
$$g_L = [L:K]\,(-1+\frac{n}{2}) - \frac{1}{2}\sum_{j=2}^{n-1}[L \cap K_S^j : K] < [L:K]\,(-1+\frac{n}{2}).$$
4. Assume that $m \geq r+2$. We gather from Remark 2.6.3.4 that $n := \min\{i \in \mathbb{N}, K_S^m \subset K_S^i\} \geq r+2 \geq 3$. It follows from part 3 that
$$g_{K_S^m} < [K_S^m : K]\,(-1+\frac{n}{2}) \leq [K_S^m : K]\,(-1+\frac{m}{2}).$$
As $|G(m)| = q[K_S^m : K]$, we deduce the expected inequality. In particular, when $\frac{q}{-1+\frac{m}{2}} > \frac{2\,p}{p-1}$, 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 2.2.4.2 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 $G_2(m)$. 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 2.6.3.4 that $n \geq r+2$, which proves, using the previous point, that $g_L > 0$. But, since $(C(m), G(m))$ is a big action, $C/G_2(m) \simeq \mathbb{P}^1_k$, so $g_L = 0$, hence a contradiction. We eventually explain the last statement. By Proposition 2.6.5.2, $G_S^{m_2-1}(m_2) = Gal(K_S^{m_2}/K_S^{m_2-1})$, 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 2.6.4 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 2.6.5.2), 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 2.6.6. *Let N_m be the number of $\mathbb{F}_q$-rational points on the curve $C(m)$ as defined in Remark 2.6.3.3. Then $N_m = 1 + q\,|G_S(m)| = 1 + |G(m)|$. This highlights the equivalence of the two ratios $\frac{|G(m)|}{g_{C(m)}}$ and $\frac{N_m}{g_{C(m)}}$. In particular, this equivalence emphasizes the link between the problem of big actions and the search for algebraic curves with many rational points.*

As seen in Remark 2.6.3.4, $K_S^i = K$ 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 [Au99] (Prop. 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 $m_2 = 131$. This table should suggest the general method to parametrize such extensions.

conductor m	$[K_S^m : K]$	New equations
$0 \leq m \leq r+1 = 26$	1	
$r+2 = 27 \leq m \leq 2r+1 = 51$	5^2	$W_0^r + W_0 = X^{1+r}$
$m = 2r+2 = 52$	5^6	$W_1^q - W_1 = X^{2r}\,(X^q - X)$
$2r+3 = 53 \leq m \leq 3r+1 = 76$	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}	$W_4^q - W_4 = X^{3r}\,(X^{2q} - X^2)$
$3r+4 = 79 \leq m \leq 4r+1 = 101$	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}	$W_8^q - W_8 = X^{4r}\,(X^{3q} - X^3)$
$4r+5 = 105 \leq m \leq 5r+1 = 126$	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,

$$\frac{|G(m_2)|}{g_{K_S^{m_2}}} \simeq 9,6929\ldots \tag{2.16}$$

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 2.6.2.1) contains S. Indeed, fix y in $\mathbb{F}_q$ and call $P_y := (X - y)$ the corresponding place in S. We have to distinguish three cases. By [St93] (Prop. VI. 4.1), P_y completely splits in the extension $K(W)/K$, where $W^r + W = X^{u\,(1+r)}$, with $1 \leq u \leq 4$, 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 $1 \leq v < u \leq 5$, 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 $[y^{1+r}, 0] = (F^s + I)\,[\frac{1}{2}\,y^{1+r}, -\frac{2^p - 2}{4p}\,y^{(1+r)\,p}]$. Finally, we remark that $L_i = L_{i-1}\,K(W_i)$ for all i in $\{1, \ldots, 14\}$. Then $S(L_i) = S(L_{i-1}) \cap S(K(W_i))$ (cf. [Au99], Cor. 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 $1 \leq u \leq 4$, has conductor $ur + u + 1$ (see [Au99], Prop. 8.9.a). The extension $K(W)/K$, where $W^q - W = X^{u\,r}\,(X^{v\,q} - X^v)$, with $1 \leq v < u \leq 5$, has conductor $ur + v + 1$ (see [Au99], Prop. 8.9.b). 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 $1 + \max\{p(1+r), -\infty\} = 1 + p + p^{s+1} = m_2$ (see [Ga99], Thm. 1.1). As a conclusion, since $m(L_i) = \max\{m(L_{i-1}), m(K(W_i))\}$ (cf. [Au99], Cor. 3.2.b), an induction on i allows us to obtain the expected conductor for L_i.
3. We 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 [Lau99] (Thm. 1) or [Au99] (p. 54-55, formula (13)). □

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

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

and

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

Let $L := K(W_i)_{0 \leq i \leq p}$ be the extension of K parametrized by the Artin-Schreier-(Witt) equations

$$W_0^p - W_0 = f_0(X) \quad \forall\, i \in \{1, \ldots, p-1\}, \; W_i^q - W_i = f_i(X) \quad \textit{and} \quad [W_0, W_p]^p - [W_0, W_p] = [f_0(X), 0].$$

For all i in $\{0, 1, \ldots, p-1\}$, put $L_i := K(W_0, \ldots, W_i)$. 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,*

$$L_0 \subset K_S^{r+2} \quad ,\forall\, i \in \{1, \ldots, p-1\}, \;\; L_i \subset K_S^{p^{s+1}+i+1} \;\; \textit{with}\, L \subset K_S^{m_2},$$

where $m_2 = p^{s+1} + p + 1$ is the integer defined in Proposition 2.6.4. (see table on next page).

2. *L/K has degree $[L : K] = p^{2+(p-1)e}$, and its Galois group G_L satisfies*

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

3. *The extension L/K is stable under the translations $X \to X + y$, 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*

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

In particular, when e grows large, $g_L \sim \frac{1}{2}\, p^{(2p-1)\,\frac{e}{2}+3}$ 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 $\frac{|G|}{g_L} \simeq 9,7049\ldots$, which is slightly bigger than the quotient obtained for the whole extension $K_S^{m_2}$ (see (2.16)).

Proof :

1. Fix y in $\mathbb{F}_q$ and call $P_y := (X - y)$, the corresponding place in S. As $f_i(y) = 0$ for all i in $\{1, \ldots, p-1\}$, the place P_y completely splits in each extension $K(W_i)$ with $W_i^q - W_i = f_i(X)$. 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 [Bour83] (Chap. IX, ex. 18), this is equivalent to show that $Tr([f_0(y), 0]) = 0$, where Tr means the trace map from $W_2(\mathbb{F}_q)$ to $W_2(\mathbb{F}_p)$. We first notice that, when y is in $\mathbb{F}_q$, $\gamma := f_0(y) = a\,y^{1+r}$ lies in Γ. It follows that

$$Tr([\gamma, 0]) = \sum_{i=0}^{2s-1} F^i\,[\gamma, 0] = \sum_{i=0}^{s-1} [\gamma^{p^i}, 0] + \sum_{i=0}^{s-1} [\gamma^{r\,p^i}, 0] = \sum_{i=0}^{s-1} [\gamma^{p^i}, 0] + \sum_{i=0}^{s-1} [-\gamma^{p^i}, 0].$$

As $p > 2$, $[-\gamma^{p^i}, 0] = -[\gamma^{p^i}, 0]$ and $Tr([\gamma, 0]) = 0$. To establish the expected inclusions, it remains to compute the conductor of each extension L_i. First of all, [Au99] (I, ex. 3.3) together with [St93] (Prop III,7.10) shows that the conductor of L_0 is $r + 2$. Thus, $L_0 \subset K_S^{r+2}$. Moreover, as $f_i(X) = X^{i+p^{s+1}} - X^{1+ip^{s-1}} \bmod \wp(\mathbb{F}_q[X])$, we infer from [Au99] (I, ex. 3.3) and [Au99] (I, Cor. 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 [Ga99] (see comments above).

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

L_i	conductor m	$[L_i : K]$	New equations
K	$0 \leq m \leq r+1 = p^s+1$	1	
L_0	$r+2 \leq m \leq p^{s+1}+1 = m_2 - p$	p	$W_0^p - W_0 = f_0(X)$
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}	$W_2^q - W_2 = f_2(X)$
$\ldots\ldots$	$\ldots\ldots$	$\ldots\ldots$	$\ldots\ldots$
L_i	$m = p^{s+1}+i+1 = m_2 - (p-i)$	p^{1+ie}	$W_i^q - W_i = f_i(X)$
$\ldots\ldots$	$\ldots\ldots$	$\ldots\ldots$	$\ldots\ldots$
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 2.6.5) such that $\sigma(X) = X + y$.
   (a) We prove that $\sigma(W_0) \in L_0$. Indeed, as $y \in \mathbb{F}_q$ and $a \in \Gamma = \{\gamma \in \mathbb{F}_q, \gamma^r + \gamma = 0\}$,

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

where $P_y(X) := (I + F + F^2 + \ldots + F^{s-1})\,(-a\,y^r\,X)$. 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, for all i in $\{1, \ldots, p-1\}$, $\sigma(W_i) \in L_i$. Indeed,

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

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

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

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

   (c) We next show, using Remark 2.6.3.4, that $\sigma(W_p) \in L$. To this end, set

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

So

$$\begin{aligned}\Delta \quad &= \sigma(\wp([W_0, W_p])) - \wp([W_0, W_p])\\ &= [f_0(X+y), 0] - [f_0(X), 0].\end{aligned}$$

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

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

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 $\tilde{y} := (y, 0, 0, \ldots) \in W(k)$. 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

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

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

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

We observe that

$$\begin{aligned}\tilde{f}_0(X+\tilde{y})^p &= \tilde{a}^p\,(X+\tilde{y})^p\,(X+\tilde{y})^{p^{s+1}} && \bmod\ p^2\,W(\mathbb{F}_q)[X]\\ &= \tilde{a}^p\,(X+\tilde{y})^p\,(X^{p^s}+\tilde{y}^{p^s})^p && \bmod\ p^2\,W(\mathbb{F}_q)[X]\\ &= \tilde{a}^p\,\textstyle\sum_{i=0}^{p}\sum_{j=0}^{p}\binom{p}{i}\binom{p}{j}\,X^{j+ip^s}\,\tilde{y}^{p-j+p^s\,(p-i)} && \bmod\ p^2\,W(\mathbb{F}_q)[X].\end{aligned}$$

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

$$I:=\{(i,j)\in\mathbb{N}^2,\,0\le i\le p, 0\le j\le p,\,ij=0 \mod p, (i,j)\ne(0,0)\,,(i,j)\ne(p,p)\}.$$

We obtain

$$\begin{aligned}\tilde{P}_y(X)^p-\tilde{P}_y(X)^{p^2} &= (\textstyle\sum_{i=0}^{s-1}(-\tilde{a}\,\tilde{y}^r\,X)^{p^i})^p-(\sum_{i=0}^{s-1}(-\tilde{a}\,\tilde{y}^r\,X)^{p^i})^{p^2} && \bmod\ p^2\,W(\mathbb{F}_q)[X]\\ &= (\textstyle\sum_{i=0}^{s-1}(-\tilde{a}\,\tilde{y}^r\,X)^{p^i})^p-(\sum_{i=0}^{s-1}(-\tilde{a}\,\tilde{y}^r\,X)^{p^{i+1}})^p && \bmod\ p^2\,W(\mathbb{F}_q)[X]\\ &= -\tilde{a}^p\,\tilde{y}^{rp}\,X^p+\tilde{a}^{rp}\,\tilde{y}^{r^2p}\,X^{pr}+p\,\tilde{T}_y(X) && \bmod\ p^2\,W(\mathbb{F}_q)[X],\end{aligned}$$

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

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

As a consequence,

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

where

$$I_1:=I-\{(0,p),(p,0)\}$$

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 (after eventual reduction mod $\wp(\mathbb{F}_q[X])$) is less than $1+p^s$, one can write

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

where $R_y(X)$ is a polynomial of $\mathbb{F}_q[X]$ with degree less 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 $X^{i_0+i_1\,p+\ldots+i_{s-1}\,p^{s-1}}$ with $i_0+i_1+\ldots+i_{s-1}=p$, and $X^{i_1\,p+\ldots+i_s\,p^s}$, with $i_1+i_2+\ldots+i_s=p$. Since $X^{i_1\,p+\ldots+i_s\,p^s}=X^{i_1+\ldots+i_s\,p^{s-1}} \bmod \wp(\mathbb{F}_q[X])$, 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,

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

where $R_y^{[1]}(X)$ is a polynomial of $\mathbb{F}_q[X]$ with degree less 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 $\{1,\ldots,p-1\}$, we conclude that

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

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

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

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

$$\begin{aligned} A \;\; &= \textstyle\sum_{j=1}^{p-1} (F^e - id)\,(c_j(y)\, W_j) + R_y^{[2]}(X) && \mod \wp(\mathbb{F}_q[X]) \\ &= (F - id)\, \textstyle\sum_{j=1}^{p-1}\; P_j(W_j) + R_y^{[2]}(X) && \mod \wp(\mathbb{F}_q[X]) \end{aligned}$$

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

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

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,

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

which allows to conclude that $\sigma\,(W_p)$ is in $L = K(W_0, W_1, \ldots, W_p)$. This finishes the proof of Proposition 2.6.7.3.

4. Since $L \subset K_S^{m_2}$ and $L \not\subset K_S^{m_2-1}$, the formula in Proposition 2.6.5.3. yields

$$\begin{aligned} g_L \;\; &= 1 + [L:K]\,(-1 + \tfrac{m_2}{2}) - \tfrac{1}{2} \textstyle\sum_{j=0}^{m_2-1} [L \cap K_S^j : K] \\ &= 1 + p^{2+(p-1)e}\,(-1 + \tfrac{p^{s+1}+p+1}{2}) - \tfrac{1}{2}(r + 2 + (m_2 - p - (r+2) + 1)\, p + \textstyle\sum_{i=1}^{p-1}\; p^{1+i\,e}) \\ &= \tfrac{1}{2}\, p^{2+(p-1)e}\,(p^{s+1} + p - 1) - \tfrac{1}{2}\,(p^s + p^{s+2} - p^{s+1} + \textstyle\sum_{i=1}^{p-1}\; p^{1+i\,2\,s}) \\ &= \tfrac{1}{2}\, p^{2+(p-1)e}\,(p^{s+1} + p - 1) - \tfrac{1}{2}\, p^s (p^2 - p + 1) - \tfrac{1}{2}\, p^{2s+1} (1 + q + q^2 + \ldots + q^{p-2}) \end{aligned}$$

5. See Proposition 2.6.5.4. □

Remark 2.6.8. *For $p = 2$, the equations given in Proposition 2.6.7 become*

$$W_0^p - W_0 = f_0(X) := X^{1+r}$$

$$W_1^q - W_1 = f_1(X) := X^{p^{s-1}}\,(X^q - X)$$

$$[W_0, W_2]^p - [W_0, W_2] = [f_0(X), 0].$$

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

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

In this case, we obtain the same results as in Proposition 2.6.7. The proof is left to the reader.

Proposition 2.6.7 can be generalized to construct a big action whose second ramification group G_2 is abelian of exponent as large as we want.

Proposition 2.6.9. *We keep the notation of Proposition 2.6.7. In particular, $q = p^e$, with $p > 2$, $e = 2\,s$ and $s \geq 1$. Let $n \geq 2$. Put $m_n := 1 + p^{n-1}\,(1 + p^s)$. If*

$$\frac{q}{-1 + m_n/2} > \frac{2\,p}{p-1},$$

the pair $(C(m_n), G(m_n))$, as defined in Proposition 2.6.5, is a big action with a second ramification group $G_S(m_n)$ abelian of exponent at least p^n.

Proof : Proposition 2.6.5.4 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 2.6.7, i.e. $r = p^s$, $a^r + a = 0$, $a \neq 0$. The same proof as in Proposition 2.6.7.1 shows that all places of S completely split in $K(W_1, \ldots, W_n)$. Moreover, by [Ga99] (Thm. 1.1) the conductor of the extension $K(W_1, \ldots, W_n)$ is $1 + max\{p^{n-1}\,(1 + p^s), 0\} = m_n$. It follows that $K(W_1, \ldots, W_n)$ is included in $K_S^{m_n}$. Therefore, $G_S(m_n)$ has a quotient of exponent p^n and the claim follows. □

Tne next proposition is an analogue of Proposition 2.6.7 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 2.6.7. Note that, contrary to the case where e is even, the equations still work for $p = 2$.

Proposition 2.6.10. *We keep the notation defined above. In particular, $K = \mathbb{F}_q(X)$ with $q = p^e$. Assume that $e = 2\,s - 1$, with $s \geq 2$, and put $r := \sqrt{qp} = p^s$. We define*

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

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

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

$$\forall\, i \in \{1, \ldots, p-1\},\ W_i^q - W_i = f_i(X) \quad \textit{and} \quad \forall\, j \in \{1, \ldots, p-1\},\ V_j^q - V_j = g_j(X)$$

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

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

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

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

   where $m_2 = p^{s+1} + p + 1$ is the integer defined in Proposition 2.6.4. (see table on next page.)
2. *The extension L/K has degree $[L : K] = p^{2(p-1)e+1}$, and its Galois group G_L satisfies*

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

3. *The extension L/K is stable under the translations $X \to X + y$, 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*

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

   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 :

$L_{i,j}$	conductor m	$[L_{i,j}:K]$	New equations
K	$0 \leq m \leq r+1 = p^s+1$	1	
$L_{1,0}$	$m = r+2 = p^s+2$	p^e	$W_1^q - W_1 = f_1(X)$
......	......	......	......
$L_{i,0}$	$m = p^s+i+1$	p^{ie}	$W_i^q - W_i = f_i(X)$
......	......	......	......
$L_{p-1,0}$	$p^s+p \leq m \leq p^{s+1}+1$	$p^{(p-1)e}$	$W_{p-1}^q - W_{p-1} = f_{p-1}(X)$
$L_{p-1,1}$	$m = p^{s+1}+2 = m_2-(p-1)$	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	$m = p^{s+1}+p+1 = m_2$	$p^{1+2\,(p-1)e}$	$[W_1,W_p]^p - [W_1,W_p] =$ $[X^{1+p^s},0] - [X^{1+p^{s-1}},0]$

2.7 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 $\mathbb{P}^1_k$ and π is étale above the affine line $\mathbb{A}^1_k = \mathbb{P}^1_k - \pi(\infty) = Spec\,k[T]$. 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 (4.1) as $g = \frac{1}{2}\left(\sum_{i\geq 2}(|G_i|-1)\right) > 0$. It follows that

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

This leads to :

Definition 2.7.1. *A local big action is any pair $(k((Z)),G)$ where G is a finite p-subgroup of $\mathrm{Aut}_k(k((Z))$ whose ramification groups in lower notation at ∞ satisfy the inequalities*

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

It follows from the Katz-Gabber Theorem (see [Ka86] Thm. 1.4.1 or [Gi00] Cor. 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 $k[T] \subset k((T^{-1}))$:

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

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

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

Chapitre 3

Large p-group actions with a p-elementary abelian derived group.

3.1 Introduction.

General background. This chapter is the second one in a series of three papers (together with [MR08] and [Ro08]) dedicated to the 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 $|G| > \frac{2\,p}{p-1}\, g$. Here, we more specifically study such actions in the case where the derived group G' of G is p-elementary abelian.

Let k be an algebraically closed field of characteristic $p > 0$ and C a connected nonsingular projective curve over k, with genus $g \geq 2$. As in characteristic zero, the k-automorphism group of the curve C, $\mathrm{Aut}_k(C)$, is a finite group whose order is bounded from above by a polynomial in g (cf. [Sin74]). But, contrary to the case of characteristic zero, the bound is no longer linear but biquadratic, namely : $|\mathrm{Aut}_k(C)| \leq 16\, g^4$, except for the Hermitian curves : $W^q + W = X^{1+q}$, with $q = p^n$ (cf. [St73]). The difference is due to the appearance of wild ramification, which leads us to focus on the size of the p-subgroups of $\mathrm{Aut}_k(C)$. In his study of the Sylow p-subgroups of $\mathrm{Aut}_k(C)$, Nakajima emphasizes the influence of the p-rank γ of the curve (cf. [Na87a]). Indeed, if G is a Sylow p-subgroup of $\mathrm{Aut}_k(C)$, then $|G| \leq \frac{2\,p}{p-1}\, g$, except for $\gamma = 0$. When $\gamma = 0$, $|G| \leq \max\{g, \frac{4\,p}{(p-1)^2}\, g^2\}$ and the quadratic upper bound $\frac{4\,p}{(p-1)^2}\, g^2$ can really be attained. Following Nakajima's work, Lehr and Matignon explore the *big actions*, that is to say the pairs (C, G) where G is a p-subgroup of $\mathrm{Aut}_k(C)$ such that $|G| > \frac{2\,p}{p-1}\, g$ (see [LM05]).

Setting. Let (C, G) be a big action as defined above. Then there is a point of C (say ∞) such that G is equal to the wild inertia subgroup G_1 of G at ∞. The quotient curve 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 $\pi(\infty)$). Let G_2 be the second ramification group of G at ∞ in lower notation. Then G_2 is strictly included in G and the quotient curve C/G_2 is isomorphic to $\mathbb{P}^1_k$. Furthermore, 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. This induces the exact sequence

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

where, for all g in G, $\pi(g) := g(X) - X$. In Chapter 2, we more specifically concentrated on the properties of G_2. In particular, we proved that G_2 coincides with the derived group (or commutator subgroup) of G. This group is denoted by G' or $D(G)$.

Motivations. If (C, G) is a big action and H a normal subgroup of G such that $H \subsetneq G'$, then $(C/H, G/H)$ is still a big action whose derived group is G'/H (cf. Chapter 2 § 2.2). In particular, when applying this result to $H = \mathrm{Fratt}(G')$ the Frattini subgroup of G', one obtains a big action whose derived group is p-elementary abelian. Lehr and Matignon first characterize the big actions such that $G' \simeq \mathbb{Z}/p\mathbb{Z}$. Indeed they prove that they correspond to the p-cyclic étale covers of the affine line given by an Artin-Schreier equation : $W^p - W = X\, S(X) + c\, X \in k[X]$, where $S(X)$ runs over the additive polynomials of $k[X]$. In this case, they also determine the wild inertia subgroup of $\mathrm{Aut}_k(C)$ at ∞. In particular, for $p > 2$, it is the extraspecial group of exponent p and order p^{2s+1}, where p^s denotes the degree of the polynomial $S(X)$ (see [LM05] or Chapter 1 § 1.2.10).

We now intend to generalize the parametrization obtained in the p-cyclic case for $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$ with $n \geq 2$. As an application, we shall pursue in a Chapter 4 the classification of big actions. More precisely, we shall parametrize those satisfying $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$, knowing that, under this condition, we previously showed that G' is a p-elementary abelian group of order dividing p^3 (cf. Chapter 2 § 2.4).

Outline of the chapter. The main result of this chapter is the following (cf. Theorem 3.3.14) :

Theorem : *Let (C, G) be a big action such that the derived group G' of G is isomorphic to $(\mathbb{Z}/p\,\mathbb{Z})^n$, $n \geq 1$. For all $t \geq 1$, let Σ_t be the k-vector subspace of $k[X]$ generated by 1 and the products of at most t additive polynomials.*
Then the function field of the curve can be parametrized by n Artin-Schreier equations :

$$\forall\, i \in \{1, \ldots, n\}, \quad W_i^p - W_i = f_i(X) \in \Sigma_{i+1}.$$

In other words, each f_i can be written as a linear combination over k of products of at most $i+1$ additive polynomials of $k[X]$.

This result generalizes the p-cyclic case mentioned above, i.e. $n = 1$, but, contrary to this case, the converse is no longer true for $n \geq 2$, which means that such a family $(f_i)_{1 \leq i \leq n}$ does not necessary give birth to a big action, except under specific conditions that are studied in what follows. The obstruction essentially lies in the embedding problem associated with the exact sequence mentioned in the setting :

$$0 \longrightarrow G_2 = G' \simeq (\mathbb{Z}/p\,\mathbb{Z})^n \longrightarrow G \longrightarrow V \longrightarrow 0.$$

More precisely, we study the induced representation $\phi : G/G' \to \mathrm{Aut}(G') \simeq \mathrm{GL}_n(\mathbb{F}_p)$ via the representation dual with respect to the Artin-Schreier pairing (see Section 3.2).

Sections 3.4 and 3.5 are devoted to two special cases of main interest. In Section 3.4, we investigate the case where there is only one jump in the upper ramification filtration of G'. Then the representation mentioned above is trivial or, equivalently, each function f_i belongs to Σ_2. In Section 3.5, we give a group-theoretic characterization of what can be regarded as the opposite case, namely : each $f_i \in \Sigma_{i+1} - \Sigma_i$. Then there is a maximal number of jumps in the upper ramification filtration of G'. This case is relevant insofar as the representation ϕ is nontrivial and provides much information. To conclude, Section 3.6 is devoted to examples illustrating Section 3.5. In particular, we display a universal family parametrizing the big actions (C, G) such that each $f_i \in \Sigma_{i+1} - \Sigma_i$, for $p = 5$, a given $n \leq p-1$ and $\dim_{\mathbb{F}_p} V = 2$. This allows us to discuss the deformation space of such a big action.

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, $P(\alpha + \beta) = P(\alpha) + P(\beta)$. Moreover, a separable polynomial is additive if and only if the set of its roots is a subgroup of k (see [Go96] chap. 1).

Let $f(X)$ be a polynomial of $k[X]$. Then there is a unique polynomial $\mathrm{red}(f)(X)$ in $k[X]$, called the reduced representative of f, which is p-power free, i.e. $\mathrm{red}(f)(X) \in \bigoplus_{(i,p)=1} k\, X^i$, 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 $\mathrm{Spec}\, k[X]$ corresponds to a curve C_f where f is a polynomial of $k[X]$ (see [Mi80] III.4.12, p. 127). By Artin-Schreier theory, the covers C_f and $C_{\mathrm{red}(f)}$ define the same p-cyclic covers of the affine line. The curve C_f is irreducible if and only if $\mathrm{red}(f) \neq 0$.

3.2 An embedding problem.

3.2.1 Notations.

Notation 3.2.1. *Throughout this section, the pair (C, G) is a big action and G' denotes the derived group (i.e. the commutator subgroup) of G.*

1. *Assume that G' is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$. We denote by $L := k(C)$ the function field of C and by $k(X) := L^{G'}$ the subfield of L fixed by G'. Then the extension $L/L^{G'}$ is an étale cover of the affine line* $\operatorname{Spec} k[X]$ *whose Galois group is $G' \simeq (\mathbb{Z}/p\,\mathbb{Z})^n$. Therefore, it can be parametrized by n Artin-Schreier equations : $W^p - W = g_i(X)$, with $1 \leq i \leq n$.*
2. *As recalled in the setting (Section 3.1), the quotient group G/G' acts as a group of translations of* $\operatorname{Spec}k[X]$*, through $X \to X + y$, where y runs over a subgroup V of k. We remark that V is an $\mathbb{F}_p$-subvector space of k. We denote by v its dimension and thus obtain the exact sequence :*

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

where, for all g in G, $\pi(g) := g(X) - X$. We also fix a set theoretical section, i.e. a map $s : V \to G$, such that $\pi \circ s = id_V$.

3.2.2 An $\mathbb{F}_p$-vector space dual of G'.

Definition 3.2.2. *Following Artin-Schreier theory (see [Bour83], chap. IX, ex. 19), we define the $\mathbb{F}_p$-vector space :*

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

generated by the classes of the functions $g_i(X)$ modulo $\wp(k(X))$. The inclusion $k[X] \subset k(X)$ induces an injection :

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

Since the extension $L/k(X)$ is étale outside ∞, the functions $g_i(X)$ can be chosen in $k[X]$ (cf. [Mi80] III, 4.12) . It follows that we can identify A with $\tilde{A}$.

Remark 3.2.3. *Consider the Artin-Schreier pairing :*

$$\begin{cases} G' \times A \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \\ (g, \overline{\wp w}) \longrightarrow [g, \overline{\wp w}\rangle := g(w) - w. \end{cases}$$

where g belongs to $G' \subset \operatorname{Aut}_k(L)$, w is an element of L such that $\wp\, w \in k[X]$ and $\overline{\wp w}$ denotes the class of $\wp\, w$ mod $\wp(k[X])$. This pairing is non degenerate, which implies that, as an $\mathbb{F}_p$-vector space, A is dual to G'.

3.2.3 Two dual representations.

We now introduce two representations dual with respect to the Artin-Schreier pairing. The first representation, say ϕ, expresses the action of G on G' via conjugation. The second one, say ρ, expresses the action of V on A by translation.

Definition 3.2.4. 1. *For all y in V, we consider the automorphism $\phi(y)$ of G' defined as follows :*

$$\phi(y) : \begin{cases} G' \to G' \\ g \to s(y)^{-1}\, g\, s(y). \end{cases}$$

Since G' is abelian, $\phi(y)$ does not depend on the lifting $s(y)$ in G chosen for y. This induces a representation $\phi : V \to \operatorname{Aut}(G')$.

2. *For all y in V, we consider the automorphism $\rho(y)$ of A defined as follows :*

$$\rho(y) : \begin{cases} A \to A \\ \overline{\wp w} \to \overline{\wp(s(y)(w))}, \end{cases}$$

where w is an element of L such that $\wp\, w \in k[X]$. As G' acts trivially on $\wp(L) \cap k(X)$, then $\rho(y)$ is independent of the lifting $s(y)$ in G chosen for y. This induces a representation $\rho : V \to \operatorname{Aut}(A)$.

Remark 3.2.5. *Note that for all $\overline{f(X)}$ in A and for all y in V, $\rho(y)\overline{f(X)} = \overline{f(X + y)}$.*

Proposition 3.2.6. *The two representations ρ and ϕ are dual with respect to the Artin-Schreier pairing.*

Proof : For all y in V, for all g in G' and for all w in L such that $\wp\, w$ is in $k[X]$,

$$\begin{aligned}[\phi(y)(g)\,,\,\overline{\wp w}\rangle &= [s(y)^{-1}\, g\, s(y), \overline{\wp w}\rangle \\ &= s(y)^{-1}\, g\, s(y)(w) - w = s(y)^{-1}\, g\, s(y)(w) - s(y)^{-1}\, s(y)(w) \\ &= s(y)^{-1}\, (g\, s(y)(w) - s(y)(w)) = g\, s(y)(w) - s(y)(w),\end{aligned}$$

since $g\ s(y)(w) - s(y)(w) = [g, \overline{\wp(s(y)(w))}\rangle \in \mathbb{F}_p$.
As a conclusion, $[\phi(y)(g)\,,\,\overline{\wp w}\rangle = [g\,,\,\overline{\wp(s(y)(w))}\rangle = [g\,,\,\rho(y)(\overline{\wp w})\rangle$. $\square$

Since the image of ρ is a unipotent subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, one can find a basis for the $\mathbb{F}_p$-vector space A in which the image of the representation ρ can be identified with a subgroup of the upper triangular matrices in $\mathrm{GL}_n(\mathbb{F}_p)$. A means to do so is to endow A with a filtration which proves to be dual of the upper ramification filtration of G'.

3.2.4 Dual filtrations on A and G'.

The following three subsections are classical. Nevertheless, it is more convenient to recall both the proofs and the construction so as to fix the notation.

A filtration and an adapted basis for A.

Definition 3.2.7. *1. We first gather from the canonical map "degree" a map defined on A in the following way :*

$$\deg : \left\{ \begin{array}{l} A \to \mathbb{N} \cup \{-\infty\} \\ \overline{f(X)} \to \inf\{\,\deg\,(f + \wp(P)),\ P \in k[X]\,\}. \end{array} \right.$$

2. For all i in $\mathbb{N}$, we define a sequence of $\mathbb{F}_p$-vector subspaces of A as follows :

$$A^i := \{\overline{f(X)} \in A,\ \deg(\overline{f(X)}) < i\}.$$

3. From the increasing sequence : $\{0\} = A^0 \subset A^1 \subset A^2 \subset \dots A^r \subset A^{r+1} = A$, we extract a strictly increasing sequence $(A^{\mu_i})_{0 \leq i \leq s}$ such that :

$$\{0\} = A^0 = \ldots = A^{\mu_0} \subsetneq A^{\mu_0+1} = \ldots = A^{\mu_1} \subsetneq A^{\mu_1+1} = \ldots \subsetneq \ldots A^{\mu_s} \subsetneq A^{\mu_s+1} = A,$$

where the jumps μ_i are uniquely determined by the condition : $A^{\mu_i} \subsetneq A^{\mu_i+1}$. By definition of the function "degree" on A, each integer μ_i is prime to p. By convenience of notation, put $\mu_{s+1} := \mu_s + 1$ so that $A = A^{\mu_{s+1}}$.

4. Starting from a basis of A^{μ_1}, we complete it in a basis of A^{μ_2}, and so on until A^{μ_s+1}. In this way, we construct a basis of A, say : $\{\overline{f_1(X)}, \ldots, \overline{f_n(X)}\}$, which is said to be "adapted" to the filtration defined above. Moreover, we impose specific conditions on the degree m_i of each $\overline{f_i(X)}$:

(a) $\forall\, i \in \{1, \ldots, n\}$, m_i is prime to p.

(b) $\forall\, i \in \{1, \ldots, n-1\}$, $m_i \leq m_{i+1}$.

(c) $\forall\, (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_p^n$ not all zeros,

$$\deg\,(\sum_{i=1}^{n} \lambda_i\, \overline{f_i(X)}) = \max_{i=1,\ldots,n} \{\deg \lambda_i\, \overline{f_i(X)}\}.$$

Remark 3.2.8. *For all i in $\{0, \ldots, s+1\}$, we denote by n_i the dimension of A^{μ_i} over $\mathbb{F}_p$. Note that $n_0 = 0$ and $n_{s+1} = n$. Moreover, for all $i \in \{0, \ldots, s\}$, $m_{n_i+1} = m_{n_i+2} = \ldots = m_{n_{i+1}} = \mu_i$.*

The adapted basis defined above provides a new parametrization of the function field L. Indeed, for all i in $\{1, \ldots, n\}$, we fix a representative mod $\wp(k[X])$ of $\overline{f_i(X)}$: $f_i(X)$ and assume it to be reduced mod $\wp(k[X])$. As m_i is prime to p, $f_i(X)$ still has degree m_i. We also suppose that for all i in $\{1, \ldots, n\}$, $f_i(0) = 0$. From now on, the extension $L/k(X)$ is parametrized by the n Artin-Schreier equations : $W_i^p - W_i = f_i(X)$ with $1 \leq i \leq n$.

The link with the upper ramification filtration of G'.

In what follows, we highlight the correspondence between the jumps $(\mu_i)_{0\leq i\leq s}$ in the filtration of A and the jumps $(\nu_i)_{0\leq i\leq r}$ in the upper ramification filtration of G'. Since G' is abelian, the Hasse-Arf Theorem (see e.g. [Se68], Chap. IV) asserts that the jumps in the upper ramification filtration are integers. So the ramification filtration reads as follows :

$$G' = (G')^0 = \ldots = (G')^{\nu_0} \supsetneq (G')^{\nu_0+1} = \ldots = (G')^{\nu_1} \supsetneq \ldots = (G')^{\nu_r} \supsetneq (G')^{\nu_r+1} = \{0\}.$$

By convenience, put $\nu_{r+1} := \nu_r + 1$.

Proposition 3.2.9. *Keeping the notation above, $r = s$ and for all i in $\{0,\ldots,s+1\}$, $\mu_i = \nu_i$.*
It follows that the filtration of A and G' are dual with respect to the Artin-Schreier pairing, that is to say $(G')^{\nu_i}$ is the orthogonal of A^{μ_i}, for all i in $\{0,\ldots,s+1\}$.

Proof : Let ν_i be a jump in the upper ramification filtration of G', with $0 \leq i \leq r$. Since the $(G')^{\nu_i}$ are $\mathbb{F}_p$-subvectors spaces of G', one can find an index p-subgroup of G', say H, such that $(G')^{\nu_i+1} \subset H$ and $(G')^{\nu_i} \not\subset H$. As $L^H/L^{G'}$ is a p-cyclic cover of the affine line inside L, with Galois group equal to G'/H, it is parametrized by an Artin-Schreier equation : $W^p - W = f(X) = \sum_{i=1}^n \lambda_i\, f_i(X)$ with $(\lambda_i)_{1\leq i\leq n} \in (\mathbb{F}_p)^n - \{(0,0,\ldots,0)\}$. Condition (c) in Definition 3.2.7.4 requires : $\deg(f) = \max_{1\leq i\leq n}\{\deg\,\lambda_i\, f_i(X)\} \in \{m_i,\, 1\leq i\leq n\} = \{\mu_i,\, 0\leq i\leq s\}$. Besides, the group G' induces an upper ramification filtration on G'/H, namely $(\frac{G'}{H})^\nu = \frac{(G')^\nu H}{H}$ (see [Se68], Chap. IV, Prop. 14). Therefore, the ramification filtration of G'/H reads :

$$\mathbb{Z}/p\,\mathbb{Z} \simeq \frac{G'}{H} = (\frac{G'}{H})^0 = \ldots = (\frac{G'}{H})^{\nu_i} \supsetneq (\frac{G'}{H})^{\nu_i+1} = \{0\}.$$

This is precisely the p-cyclic case for which it is well-known that the only jump of ramification : ν_i is equal to $\deg(f)$ (see [Se68], Chap. IV, ex. 4, p. 80). Therefore, $\nu_i \in \{\mu_j,\, 0\leq j\leq s\}$.

Conversely, consider μ_i, for $0\leq i\leq s$. Then by Remark 3.2.8, $\mu_i = m_{n_{i+1}}$, i.e. the degree of the function $f_{n_{i+1}}$. There exists an index p-subgroup H of G' such that $L^H/L^{G'}$ is the p-cyclic cover of the affine line inside L parametrized by the equation : $W^p - W = f_{n_{i+1}}(X)$. We define the integer $\nu(G') \in \{\nu_i,\, 0\leq i\leq r+1\}$ such that $(G')^{\nu(G')+1} \subset H$ and $(G')^{\nu(G')} \not\subset H$. As seen above, $m_{n_{i+1}} = \nu(G')$. Therefore, $\mu_i \in \{\nu_j,\, 0\leq j\leq r\}$. Accordingly, $\{\nu_i,\, 0\leq i\leq r\} = \{\mu_i,\, 0\leq i\leq s\}$. They are both strictly increasing sequence, so $r = s$ and for all i in $\{0,\ldots,s\}$, $\mu_i = \nu_i$. In addition, $\mu_{s+1} = \mu_s + 1 = \nu_r + 1 = \nu_{r+1}$, which completes the proof of the proposition. □

The different exponent and the genus of the extension.

In this section, we establish a formula to calculate the different exponent and the genus of the extension $L/L^{G'}$. We keep the notations defined in Sections 3.2.4.1 and 3.2.4.2.

Proposition 3.2.10. *Let (C,G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$.*
The different exponent of the extension $L/L^{G'}$ is given by the formula :

$$d = (p-1)\sum_{i=1}^{n} p^{i-1}\,(m_i + 1).$$

Proof : Since G' is abelian, one can apply to $L/L^{G'}$ the upper index version of the Hilbert's different formula as given in [Au99] (p. 120) : $d = \sum_{i=0}^{\infty}(|G'| - [G' : (G')^i])$. In our case, this formula reads :

$$d = (\nu_0 + 1)\,(|G'| - [G' : (G')^{\nu_0}]) + \sum_{j=1}^{r}(\nu_j - \nu_{j-1})\,(|G'| - [G' : (G')^{\nu_j}]).$$

Using Proposition 3.2.9, we obtain :

$$\begin{aligned} d &= (\nu_0+1)\,(|G'|-|A^{\mu_0}|)+\textstyle\sum_{j=1}^{r}(\nu_j-\nu_{j-1})\,(|G'|-|A^{\mu_j}|)\\ &= (\mu_0+1)\,(p^n-p^{n_0})+\textstyle\sum_{j=1}^{s}(\mu_j-\mu_{j-1})\,(p^n-p^{n_j})\\ &= \textstyle\sum_{j=0}^{s}(p^n-p^{n_j})\,(\mu_j+1)+\sum_{j=1}^{s+1}(p^{n_j}-p^n)\,(\mu_{j-1}+1)\\ &= \textstyle\sum_{j=1}^{s+1}(p^n-p^{n_{j-1}})\,(\mu_{j-1}+1)+\sum_{j=1}^{s+1}(p^{n_j}-p^n)\,(\mu_{j-1}+1)\\ &= \textstyle\sum_{j=1}^{s+1}(p^{n_j}-p^{n_{j-1}})\,(\mu_{j-1}+1)\\ &= \textstyle\sum_{i=1}^{s+1}\sum_{j=n_{i-1}+1}^{n_i}p^{j-1}\,(p-1)\,(\mu_{i-1}+1)\\ &= (p-1)\textstyle\sum_{i=1}^{s+1}\sum_{j=n_{i-1}+1}^{n_i}p^{j-1}\,(m_j+1)\\ &= (p-1)\textstyle\sum_{i=1}^{n}p^{i-1}\,(m_i+1). \qquad \square \end{aligned}$$

Note that another proof of this formula can be obtained by applying the formula given by Garcia and Stichtenoth in [GS91].

Corollary 3.2.11. *Let (C,G) be a big action such that $G'\simeq(\mathbb{Z}/p\mathbb{Z})^n$, with $n\geq 1$. The genus of the extension $L/L^{G'}$ is given by the formula :*

$$g=\frac{1}{2}\,(p-1)\sum_{i=1}^{n}p^{i-1}\,(m_i-1).$$

Proof : This result directly derives from the Hurwitz genus formula (see e.g. [St93]) combined with the formula given in Proposition 3.2.10.□

3.2.5 Matricial representations of ρ and ϕ.

From now on, we work in the adapted basis constructed for A in Section 3.2.4.1 : $\{\overline{f_1(X)},\dots,\overline{f_n(X)}\}$. For any y in V, we denote by $L(y)$ the matrix of the automorphism $\rho(y)$ in this basis. As indicated in Remark 3.2.5, we recall that for all y in V and for all i in $\{1,\dots,n\}$, $\rho(y)\,\overline{f_i(X)}=\overline{f_i(X+y)}$. Moreover, the conditions imposed on the degree of the functions $\overline{f_i(X)}$ imply that the matrix $L(y)$ belongs to $T^u_{1,n}(\mathbb{F}_p)$, the subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ made of the upper triangular matrices with identity on the diagonal. Thus, $L(y)$ reads as follows :

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

In other words,

$$\forall\, y\in V,\ ,f_1(X+y)-f_1(X)=0 \qquad \mathrm{mod}\ \ \wp(k[X]).$$

$$\forall\, i\in\{2,\dots,n\},\ \forall\, y\in V,\ ,f_i(X+y)-f_i(X)=\sum_{j=1}^{i-1}\ell_{j,i}(y)\,f_j(X) \qquad \mathrm{mod}\ \ \wp(k[X]). \tag{3.1}$$

Proposition 3.2.12. *Let (C,G) be a big action such that $G'\simeq(\mathbb{Z}/p\mathbb{Z})^n$, with $n\geq 2$.*

1. *For all i in $\{1,\dots,n-1\}$, $\ell_{i,i+1}$ is a linear form from V to $\mathbb{F}_p$.*
2. *For all i in $\{1,\dots,n-1\}$, put $\mathcal{L}_{i,i+1}(X):=\prod_{y\in\mathrm{Ker}\ell_{i,i+1}}(X-y)$. Then whenever $\ell_{i,i+1}$ is non identically zero, there exists λ_i in $k-\{0\}$ such that, for all y in V, $\ell_{i,i+1}(y)=\lambda_i\,\mathcal{L}_{i,i+1}(y)$. In this case, $V=Z(\lambda_i^p\,\mathcal{L}_{i,i+1}^p-\lambda_i\,\mathcal{L}_{i,i+1})$.*

Proof : The matricial multiplication first ensures that for all i in $\{1,\dots,n-1\}$, $\ell_{i,i+1}$ is a linear form from V to $\mathbb{F}_p$. Besides, from the preliminary remarks of Section 3.1, we infer that $P_V(X):=\prod_{y\in V}(X-y)$ is a separable additive polynomial of degree p^v, where v denotes the dimension of the $\mathbb{F}_p$-vector space V. Then for all i in $\{1,\dots,n-1\}$, $\mathcal{L}_{i,i+1}(X):=\prod_{y\in\mathrm{Ker}\ell_{i,i+1}}(X-y)$ is an additive polynomial which divides $P_V(X)$. We now assume that $\ell_{i,i+1}$ is a nonzero linear form. In this case, $\mathcal{L}_{i,i+1}(X)$ has degree p^{v-1} and there exists λ_i in $k-\{0\}$ such that for all y in V, $\ell_{i,i+1}(y)=\lambda_i\,\mathcal{L}_{i,i+1}(y)$. Since for all y in V, $\ell_{i,i+1}(y)$ lies in $\mathbb{F}_p$, then $\lambda_i^p\,\mathcal{L}_{i,i+1}^p-\lambda_i\,\mathcal{L}_{i,i+1}=\lambda_i^p\,P_V$. The claim follows. □

Remark 3.2.13. *By duality with respect to the Artin-Schreier pairing, the adapted basis of A fixed in Definition 3.2.7.4 gives a basis of G', say $\{g_1, \ldots, g_n\}$, in which, the matrix of the automorphism $\phi(y)$ is the transpose matrix of $L(y)$ for all y in V, namely a lower triangular matrix of $\mathrm{GL}_n(\mathbb{F}_p)$ with identity on the diagonal.*

Proposition 3.2.14. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$.*
For all integer d such that $1 \leq d \leq n$, we denote by A_d the $\mathbb{F}_p$-vector subspace of A generated by $\{\overline{f_i(X)}, 1 \leq i \leq d\}$ (cf. Definition 3.2.7.4). Let H_d be the orthogonal of A_d with respect to the Artin-Schreier pairing, namely the $\mathbb{F}_p$-vector subspace of G' spanned by $\{g_i, d+1 \leq i \leq n\}$ if $d < n$ and $H_n = \{0\}$ (cf. Remark 3.2.13). Then the pair $(C/H_d, G/H_d)$ is a big action with $(\frac{G}{H_d})' = \frac{G'}{H_d}$. It follows that $|\frac{G}{G'}| = |\frac{G/H_d}{(G/H_d)'}|$ and that the exact sequence

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

induces the following one :

$$0 \longrightarrow (G/H_d)' \simeq (\mathbb{Z}/p\,\mathbb{Z})^d \longrightarrow G/H_d \xrightarrow{\pi} V \longrightarrow 0.$$

Proof : Since $\rho(V) \subset T^u_{1,n}(\mathbb{F}_p)$, A_d is stable under the action of ρ, that is to say under the translations : $X \to X + y$, with $y \in V$. By duality, H_d is stable under the action of ϕ, i.e. by conjugation by the elements of G. It follows that H_d is a subgroup of G', normal in G. In this case, Chapter 2 (see Lemma 2.2.4 and Theorem 2.2.6) implies that the pair $(C/H_d, G/H_d)$ is a big action with $(\frac{G}{H_d})' = \frac{G'}{H_d} \subset \frac{G}{H_d}$. The claim follows. □

Corollary 3.2.15. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$. Consider the functions $f_i(X) \in k[X]$ defined as in Section 3.2.4.1. Then $f_1(X) = X\,S_1(X) + c_1\,X$, where $S_1 \in k\{F\}$ is an additive polynomial. Furthermore, after an homothety and a translation on X, one can assume that S_1 is monic and $c_1 = 0$.*

Proof : The function field of the curve C/H_d, as defined in Proposition 3.2.14, is parametrized by the d Artin- Schreier equations : $W_i^p - W_i = f_i(X)$, with $1 \leq i \leq d$. In particular, for $d = 1$ $(C/H_1, G/H_1)$ is a big action whose second lower ramification group has order p. Then [LM05] asserts that $f_1(X) = X\,S_1(X) + c_1\,X$ in $k[X]$, where $S_1 \in k\{F\}$ is an additive polynomial. □

3.2.6 Characterization of the trivial representation.

To conclude this section, we give a characterization of the case where the representation ρ or ϕ is trivial.

Proposition 3.2.16. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\,\mathbb{Z})^n$, with $n \geq 1$.*
Then the following assertions are equivalent.

1. *The representation ϕ is trivial, namely $\phi(V) = \{id\}$.*
2. *The derived group G' is included in the center $Z(G)$ of G.*
3. *The representation ρ is trivial, i.e.*

$$\forall\, i \in \{1, \ldots, n\}, \quad \forall\, y \in V, \quad f_i(X + y) - f_i(X) = 0 \mod \wp(k[X]).$$

4. *For all i in $\{1, \ldots, n\}$, the function f_i reads : $f_i(X) = X\,S_i(X) + c_i\,X \mod \wp(k[X])$, where S_i is an additive polynomial of degree $s_i \geq 1$ in F. Write $S_i(F) = \sum_{j=0}^{s_i} a_{i,j}\,F^j$ with $a_{i,s_i} \neq 0$. Then following [El97] (Section 3.4), we can define an additive polynomial related to f_i, called the "palindromic polynomial" of f_i :*

$$\mathrm{Ad}_{f_i} := \frac{1}{a_{i,s_i}^{p^{s_i}}}\, F^{s_i} (\sum_{j=0}^{s_i} a_{i,j}\,F^j + F^{-j}\,a_{i,j}).$$

In this case,

$$V \subset \bigcap_{i=1}^{n} Z(\mathrm{Ad}_{f_i}).$$

The proof of this proposition requires a preliminary lemma.

Lemma 3.2.17. *When keeping the notation defined above, $\cap_{y \in V} \mathrm{Ker}\,(\phi(y) - id) = Z(G) \cap G'$.*

Proof of Lemma 3.2.17 : Consider g in G'. Then g lies in $\cap_{y \in V} \operatorname{Ker}(\phi(y) - id)$ if and only if $\phi(y)(g) = g$ for all y in V. For all g_1 in G, put $y_1 := \pi(g_1)$. By definition, the equality $\phi(y_1)(g) = g$ means that $g_1^{-1}\, g\, g_1 = g$. This proves the expected formula. □.

Proof of Proposition 3.2.16 : The equivalence between the first and the second assertion derives from Lemma 3.2.17. As the equivalence between the first and the third point comes from the duality of ϕ and ρ (cf. Proposition 3.2.6), the only point that has to be explained is the equivalence between the last assertion and the three preceding ones.

So, assume that the second point is satisfied. For all i in $\{1, \dots, n\}$, there exists an index p-subgroup H_i of G' such that the function field of the curve $C/H_i :\ W_i^p - W_i = f_i(X)$ is a p-cyclic étale cover of the affine line with Galois group equal to G/H_i. By the second point, G' is included in $Z(G)$, which implies that H_i is normal in G. From Chapter 2 (see Lemma 2.2.4 and Theorem 2.2.6), we infer that $(C/H_i, G/H_i)$ is a big action whose derived group $(G/H_i)' = G'/H_i$ is p-cyclic. By [LM05] (Prop. 8.3), $f_i(X) = c_i\, X + X\, S_i(X) \mod \wp(k[X])$, with $S_i \in k\{F\}$. In addition, V is included in $Z(\mathrm{Ad}_{f_i})$. Conversely, if $f_i(X) = X\ S_i(X) + c_i X$, then it follows from Proposition 5.5 in [LM05] that $Z(\mathrm{Ad}_{f_i}) = \{y \in k,\ f_i(X+y) - f_i(X) = 0 \mod \wp(k[X])\,\}$. Thus, the third point is verified. □

3.3 The link with the additive polynomials.

The aim of this section is to highlight the role played by the additive polynomials of $k[X]$ in the parametrization of big actions with a p-elementary abelian derived group.

3.3.1 A ring filtration of $k[X]$ induced by the additive polynomials.

Definition 3.3.1. *We define Σ_1 as the k-vector subspace of $k[X]$ generated by 1 and by the additive polynomials of $k[X]$. More generally, for any $n \geq 1$, we define Σ_n as the k-vector subspace of $k[X]$ generated by 1 and the products of at most n additive polynomials of $k[X]$. For $n = 0$, we put $\Sigma_0 = k$ and for $n < 0$, we put $\Sigma_n = \{0\}$.*

Remark 3.3.2.

1. *For $n \geq 1$, this definition means that f is a polynomial of Σ_n if and only if there is a way to write f as a linear combination over k of products of at most n additive polynomials.*
2. *The sequence $(\Sigma_n)_{n \in \mathbb{Z}}$ enjoys the following properties :*
   - *(a)* $1 \in \Sigma_0$
   - *(b) For all integer n in $\mathbb{Z}$, $\Sigma_n \subset \Sigma_{n+1}$*
   - *(c) For all integer m and n in $\mathbb{Z}$, $\Sigma_m\, \Sigma_n \subset \Sigma_{m+n}$.*
   - *(d)* $\bigcup_{n \in \mathbb{Z}} \Sigma_i = k[X]$

   In particular, the sequence $(\Sigma_n)_{n \in \mathbb{Z}}$ is an increasing ring filtration of $k[X]$.

For a given f in $k[X]$, we search for the minimal integer n such that f belongs to Σ_n. It requires the introduction of the order function related to the ring filtration.

Definition 3.3.3. *Let a be an integer whose p-adic expansion reads : $a = a_0 + a_1\, p + a_2\, p + \ldots + a_t\, p^t$, with $t \in \mathbb{N}$ and $0 \leq a_i \leq p-1$, for all $i \in \{0, 1, 2, \ldots, t\}$. We define the integer $\mathrm{S_p}(a) \in \mathbb{N}$ as the sum of the digits of a, namely :*

$$\mathrm{S_p}(a) := a_0 + a_1 + a_2 + \ldots + a_t.$$

Remark 3.3.4. *For all integer m in $\mathbb{N}$, $\mathrm{S_p}(m) = (p-1)\, v_p(m!)$, where v_p denotes the p-adic valuation. We gather that, if m_1 and m_2 are two non-negative integers , $\mathrm{S_p}(m_1 + m_2) \leq \mathrm{S_p}(m_1) + \mathrm{S_p}(m_2)$.*

Lemma 3.3.5. *Let $a \in \mathbb{N}$ and $n \in \mathbb{N}$. Then the monomial X^a lies in Σ_n if and only if $\mathrm{S_p}(a) \leq n$. It follows that $\inf\{n \in \mathbb{N},\ X^a \in \Sigma_n\} = \mathrm{S_p}(a)$.*

Proof : Assume that $X^a \in \Sigma_n$. It means that X^a is a linear combination over k of monomials of the form $X^{p^{\gamma_1} + p^{\gamma_2} + \ldots + p^{\gamma_t}}$, with $t \leq n$ and $\gamma_1 \leq \gamma_2 \leq \ldots \leq \gamma_t$. It follows that a also reads $a = p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_t}$ with $t \leq n$ and $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_t$. Therefore, Remark 3.3.4 implies $\mathrm{S_p}(a) = \mathrm{S_p}(p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_t}) \leq \mathrm{S_p}(p^{\alpha_1}) + \mathrm{S_p}(p^{\alpha_2}) + \ldots + \mathrm{S_p}(p^{\alpha_t}) = t \leq n$.

Conversely, we suppose that $\mathrm{S_p}(a) \leq n$ and prove the result by induction on n. If $n = 0$, then $\mathrm{S_p}(a) = 0$ and $X^a = X^0 = 1 \in \Sigma_0$. We now assume that the property is true for n and suppose that $\mathrm{S_p}(a) \leq n+1$. If $\mathrm{S_p}(a) = n$, then, by induction hypothesis, $X^a \in \Sigma_n \subset \Sigma_{n+1}$. Otherwise, $\mathrm{S_p}(a) = n+1$ and there exists an integer a_i in the p-adic expansion of a such that $a_i \geq 1$. Put $b := a - p^i$. As $\mathrm{S_p}(b) = n$, the hypothesis implies $X^b \in \Sigma_n$, hence $X^a = X^b\, X^{p^i} \in \Sigma_{n+1}$. □

Definition 3.3.6. *Let f be a nonnull polynomial of $k[X]$ such that $f(X) = \sum_{a\in\mathbb{N}} c_a(f)\, X^a$. We define*

$$d_p(f) := \max_{c_a(f)\neq 0} \{\mathrm{S_p}(a)\}.$$

By convenience, put $d_p(0) := -\infty$.

Lemma 3.3.7. *Let f and g be polynomials of $k[X]$. Let $n \in \mathbb{Z}$.*

1. *$f \in \Sigma_n$ if and only if $d_p(f) \leq n$*
   i.e. $f(X) = \sum_{a\in\mathbb{N}} c_a(f)\, X^a \in \Sigma_n$ if and only if, whenever $\mathrm{S_p}(a) > n$, $c_a(f) = 0$.
2. *If f is non identically zero, $d_p(f) = \inf\{n \in \mathbb{Z},\ f \in \Sigma_n\}$.*
3. *$d_p(f) = -\infty$ if and only if $f \in \cap_{n\in\mathbb{Z}}\Sigma_n = \{0\}$.*
4. *$d_p(f\, g) \leq d_p(f) + d_p(g)$.*
5. *$d_p(f + g) \leq \sup\{d_p(f),\, d_p(g)\}$.*
6. *$d_p(F(f)) = d_p(f)$, where F means the Frobenius operator.*
7. *Let $S(X) \in k[X]$ be an additive polynomial. Then $d_p(f(S(X))) = d_p(f(X))$.*

In particular, d_p is the order function of the ring filtration defined by the $(\Sigma_n)_{n\in\mathbb{Z}}$.

Proof : Most of the properties can be deduced from Remark 3.3.4 and Lemma 3.3.5. The last one is left as an exercise to the reader. □

Definition 3.3.8. *Let f be a polynomial of $k[X]$. Let $y \in k$. We define the operator Δ_y as follows : $\Delta_y(f) := f(X + y) - f(X)$.*

One checks that this operator enjoys the following property :

Lemma 3.3.9. *For all y in k and for all $n \in \mathbb{Z}$, $\Delta_y(\Sigma_{n+1}) \subset \Sigma_n$.*

Remark 3.3.10. *Although $d_p(\Delta_y(X^a)) = d_p(X^a) - 1$, for all y in $k - \{0\}$ and all a in $\mathbb{N}^*$, one can find some polynomial f in $k[X]$ and some y in $k - \{0\}$ such that $d_p(\Delta_y(f)) \neq d_p(f) - 1$. It means that for $n \geq 2$ and for y in $k - \{0\}$, $\Delta_y(\Sigma_{n+1} - \Sigma_n)$ is not always included in $\Sigma_n - \Sigma_{n-1}$.*

3.3.2 Notation and preliminary lemmas.

Throughout this section, we keep the notations introduced in 3.2.1 combined with the following

Notation 3.3.11. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$.*

1. *We call condition (N) the inequality satisfied by big actions, namely : $\frac{|G|}{g} > \frac{2\,p}{p-1}$.*
2. *We fix an adapted basis of A : $\{\overline{f_1(X)}, \ldots, \overline{f_n(X)}\}$, as constructed in Definition 3.2.7 and assume that the functions f_i's are reduced mod $\wp(k[X])$ (see definition in Section 3.1). We denote by m_i the degree of $f_i(X)$. From now on, the extension $L/k(X)$ is parametrized by the n Artin-Schreier equations : $W_i^p - W_i = f_i(X)$, with $1 \leq i \leq n$.*
3. *As recalled in Corollary 3.2.15, $f_1(X) = X\, S_1(X) + c_1\, X$, where $S_1 \in k\{F\}$ is an additive polynomial with degree $s_1 \geq 1$ in F. In this case, the palindromic polynomial Ad_{f_1} related to f_1 is defined as in Proposition 3.2.16.*
4. *We denote by ρ the representation from V to $\mathrm{Aut}(A)$ defined in Definition 3.2.4. As seen in Section 3.2.5, when expressed in the adapted basis fixed above, the automorphism $\rho(y)$ is associated with the unipotent matrix :*

$$L(y) := \begin{pmatrix} 1 & \ell_{1,2}(y) & \ell_{1,3}(y) & \ldots & \ell_{1,n}(y) \\ 0 & 1 & \ell_{2,3}(y) & \ldots & \ell_{2,n}(y) \\ 0 & 0 & \ldots & \ldots & \ell_{i,n}(y) \\ 0 & 0 & \ldots & 1 & \ell_{n-1,n}(y) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_p).$$

5. *If ρ is trivial, we use Proposition 3.2.16 to write each f_i as $f_i(X) = X\, S_i(X) + c_i\, X$, where S_i is an additive polynomial of $k[X]$ with degree $s_i \geq 1$ in F. Then we define a palindromic polynomial Ad_{f_i} related to each f_i (see Proposition 3.2.16).*

Lemma 3.3.12. *We keep the notation defined above. The dimension v of the $\mathbb{F}_p$-vector space V satisfies $v \leq 2\, s_1$ and $p^v \geq m_n + 1$. In particular, $2 \leq s_1 + 1 \leq v \leq 2\, s_1$.*

Proof : The inclusion of V in $Z(\mathrm{Ad}_{f_1})$ first requires $v \leq 2\,s_1$. On the one hand, $|G| = p^{n+v}$. On the other hand, Corollary 4.1 implies : $g = \frac{p-1}{2}\sum_{i=1}^{n} p^{i-1}\,(m_i-1) \geq \frac{p-1}{2}\,p^{n-1}\,(m_n-1)$. Thus, $\frac{|G|}{g} \leq \frac{2\,p}{p-1}\,\frac{p^v}{m_n-1}$. The inequality $p^v \leq m_n - 1$ would contradict condition (N). Therefore, since m_n is prime to p, we obtain $p^v \geq m_n + 1$. It follows that $p^v > m_n \geq m_1 = 1 + p^{s_1}$ and $v \geq s_1 + 1$. □

Lemma 3.3.13. *Let $f(X) := \sum_{a \in \mathbb{N}} c_a(f)\,X^a$ be a polynomial in $\wp(k[X])$. Fix $a_0 \in \mathbb{N} - p\,\mathbb{N}$ and define $I_{a_0} := \{a_0\,p^n,\ n \in \mathbb{N}\}$. Then the polynomial $f_{a_0}(X) := \sum_{a \in I_{a_0}} c_a(f)\,X^a$ also lies in $\wp(k[X])$. In particular, if $f_{a_0}(X)$ is non identically zero, then p divides its degree.*

Proof : The Frobenius operator F acts on the basis $(X^a)_{a\in\mathbb{N}}$ of $k[X]$ and this action induces a partition of the monomials of $k[X]$, namely $(X^a)_{a \in I_{a_0}}$, for a_0 running over $\{0\} \cup \{\mathbb{N} - p\,\mathbb{N}\}$. This justifies the first claim. Now, assume that $f_{a_0}(X)$ is non identically zero. If $f = \wp(g)$ with $g \in k[X]$, then $f_{a_0} = \wp(g_{a_0})$, with g_{a_0} defined as for f. It follows that $\deg(f_{a_0}) = p \deg(g_{a_0})$. □

3.3.3 The link with the parametrization of big actions.

Theorem 3.3.14. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$. Then for all i in $\{1, \ldots, n\}$, $f_i(X)$ belongs to Σ_{i+1}.*

Proof : For a fixed n, we proceed by induction on i. As recalled in Section 3.3.2, $f_1(X) = X S_1(X) + c_1\,X$, where S_1 is an additive polynomial. Accordingly, $f_1 \in \Sigma_2$. We now consider some integer i such that $2 \leq i \leq n$ and assume that for all j in $\{1, \ldots, i-1\}$, $f_j(X)$ lies in Σ_{j+1}. From the form of the matrix $L(y)$, we gather :

$$\forall\, y \in V,\ \Delta_y(f_i) := f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y)\,f_j(X) \qquad \mathrm{mod}\ \ (\wp(k[X])),$$

where for all j in $\{1, \ldots, i-1\}$, $\ell_{j,i}$ is a map from V to $\mathbb{F}_p$.

Suppose that $f_i(X)$ does not belong to Σ_{i+1} and call X^a the monomial of $f_i(X)$ with highest degree which does not belong to Σ_{i+1}. Note that, by definition of a, $a > i+1$. Furthermore, as f_i is assumed to be reduced mod $\wp(k[X])$, $a \neq 0$ mod p.

We first prove that p divides $a-1$. Indeed, assume that p does not divide $a-1$ and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)\,f_j(X)$ and $a_0 := a-1 \in \mathbb{N} - p\mathbb{N}$. To construct the polynomial f_{a_0} as defined in Lemma 3.3.13, we first search for the monomials $X^{(a-1)p^r}$, with $r \geq 0$, in $\Delta_y(f_i)$. If $r > 0$, such monomials come from monomials X^b of $f_i(X)$ such that $b > (a-1)\,p^r \geq (a-1)\,p \geq a$, since $a \geq i+1 \geq 2 \geq \frac{p}{p-1}$. By definition of a, such monomials X^b, whose degree is greater than a, lies in Σ_{i+1}. Then by Lemma 3.3.9, they generate in $\Delta_y(f_i)$ polynomials which belongs to Σ_i. But $X^{a-1} \notin \Sigma_i$: otherwise, $X^a \in X\Sigma_i \subset \Sigma_{i+1}$, which contradicts the definition of a. We infer from Lemma 3.3.7.6 that no $X^{(a-1)p^r}$, with $r \geq 0$, lies in Σ_i. It follows that no monomial $X^{(a-1)p^r}$, with $r > 0$, can be found in $\Delta_y(f_i)$. We now search for the monomial X^{a-1}. By the same token, one can check that the only monomial in $f_i(X)$ which generates X^{a-1} in $\Delta_y(f_i)$ is X^a. More precisely, it produces $a\,y\,c_a(f_i)\,X^{a-1}$ in $\Delta_y(f_i)$, where $c_a(f_i) \neq 0$ denotes the coefficient of X^a in f_i. As the induction hypothesis asserts that $\sum_{j=1}^{i-1} \ell_{j,i}(y)\,f_j(X)$ lies in Σ_i, which is the case of none of the $X^{(a-1)p^r}$, we gather that $f_{a_0}(X) = a\,y\,c_a(f_i)\,X^{a-1}$. As p does not divide $a_0 = a-1$, it follows from Lemma 3.3.13 that $f_{a_0}(X)$ is identically zero. Since $a \neq 0$ mod p, this implies that $y = 0$ for all y in V, hence $V = \{0\}$. It means that $G_1 = G_2$, which is impossible for a big action (see Chapter 2 Prop. 2.2.2). Accordingly, p divides $a-1$. Thus, we can write $a = 1 + \lambda\,p^t$ with $t \geq 1$, λ prime to p and $\lambda > i \geq 2$, as X^a does not lie in Σ_{i+1}.

Now, put $j_0 := a - p^t = 1 + (\lambda - 1)\,p^t$ and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)\,f_j(X)$ and $a_0 := j_0 \in \mathbb{N} - p\,\mathbb{N}$. To construct the polynomial f_{a_0}, we first determine the monomials $X^{j_0 p^r}$, with $r \geq 0$, occurring in $\Delta_y(f_i)$. If $r > 0$, such terms come from monomials X^b of $f_i(X)$ such that $b > j_0 p$. But $j_0 p > a$. Indeed,

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

which contradicts $\lambda \geq 2$. As explained above, the monomials X^b of $f_i(X)$, with $b > a$, produce polynomials in $\Delta_y(f_i)$ which belongs to Σ_i, whereas X^{j_0} does not belong to Σ_i. Otherwise, $X^a = X^{p^t} X^{j_0}$ would belong to Σ_{i+1}, hence a contradiction. We gather from Lemma 3.3.7.6 that no $X^{j_0 p^r}$, with $r \geq 0$, lies in Σ_{i+1}. It follows that no monomials $X^{j_0 p^r}$, with $r > 0$, can be found in $\Delta_y(f_i)$. Likewise, for $r = 0$, the only monomials of $f_i(X)$ which generates X^{j_0} in $\Delta_y(f_i)$ are those of the form : X^b, with $j_0 + 1 \leq b \leq a$. For all $b \in \{j_0 + 1, \ldots, a\}$, the monomial X^b of $f_i(X)$ generates some $\binom{b}{j_0}\,y^{b-j_0}\,X^{j_0}$ in $\Delta_y(f_i)$. It follows that the coefficient of X^{j_0} in $\Delta_y(f_i)$ is $T(y)$ with $T(Y) := \sum_{b=j_0+1}^{a} c_b(f_i)\binom{b}{j_0} Y^{b-j_0}$, where $c_b(f_i)$ denotes the coefficient of X^b in $f_i(X)$. As no $X^{j_0 p^r}$, with $r \geq 0$, can be found in $\sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ which lies in Σ_i by induction, the polynomial f_{a_0} eventually reads $f_{a_0}(X) = T(y)\, X^{a_0}$. By Lemma 3.3.13, f_{a_0} is identically zero, which means that for all y in V, $T(y) = 0$. We gather that V is included in the set of zeroes of T. As the coefficient of Y^{a-j_0} in $T(Y)$ is $c_a(f_i)\binom{a}{j_0} = c_a(f_i)\binom{1+\lambda p^t}{1+(\lambda-1)p^t} \equiv c_a(f_i)\lambda \neq 0 \bmod p$, the polynomial $T(Y)$ has degree $a - j_0 = p^t$, hence $v \leq t$. This leads to a contradiction, insofar as Lemma 3.3.12 implies : $p^v \geq m_n - 1 \geq m_i - 1 \geq a - 1 = \lambda\, p^t \geq 2\, p^t > p^t$, which involves : $v > t$. As a consequence, $f_i(X)$ does not have any monomial which does not belong to Σ_{i+1}, which completes both the induction and the proof of the theorem. □

Remark 3.3.15. *The proof is actually self-contained, since the first step of the induction, namely $f_1 \in \Sigma_2$, could be obtained without any hint at Corollary 3.2.15 which requires the use of [LM05]. Indeed, in the case $i = 1$, the sum $\sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ is replaced by 0 which obviously lies in Σ_1. Using the same argument as in the second part of the proof, it enables us to conclude that f_1 belongs to Σ_2.*

3.4 A case where each $f_i \in \Sigma_2$.

This section is devoted to a first special case where each function f_i lies in $\Sigma_2 - \Sigma_1$, or equivalently, the representation ρ is trivial. The difficulty in solving the general case of trivial representation lies in finding the GCD for the family of palindromic polynomials associated to the functions f_i's as defined in Proposition 3.2.16. This could be done by working in the Ore ring of Laurent polynomials $k\{F, F^{-1}\}$ (see [El97], section 3, or [Go96], 1.6). Nevertheless, in what follows, we merely explore the simplest case where all the palindromic polynomials are equal.

Notation. The notations used throughout this section are those established in Sections 3.2.1 and 3.3.2.

Lemma 3.4.1. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$.*

1. *The upper ramification filtration of G' has only one jump.*
2. *The functions f_i's have the same degree, i.e. for all i in $\{1, \dots, n\}$, $m_i = m_1 = 1 + p^{s_1}$.*

In this case, the representation ρ is trivial and each function f_i reads $f_i(X) = X\, S_i(X) + c_i\, X \in \Sigma_2 - \Sigma_1$, where S_i is an additive polynomial with degree s_1 in F. Moreover, $V \subset \cap_{1 \leq i \leq n} Z(\mathrm{Ad}_{f_i})$.

Proof : Assume that there is only one jump in the upper ramification filtration of G' as defined in Section 3.2.4.2, namely $G' = (G')^{\nu_0} \supsetneq (G')^{\nu_0+1} = \{0\}$. The duality between the filtrations of A and G' (cf. Proposition 3.2.9) implies that this is equivalent to $\{0\} = A^{\mu_0} \subsetneq A^{\mu_0+1} = A$. By Remark 3.2.8, this situation occurs if and only if all the functions f_i's have the same degree, namely : $1 + p^{s_1}$. Comparing the degree of each member of equation (3.1), we gather that $\ell_{j,i}$ is zero on V, for all $j < i$ and all $2 \leq i \leq n$. Therefore, the representation ρ is trivial and the following assertions derive from Proposition 3.2.16. □

In what follows, we restrict to the special case : $V = Z(\mathrm{Ad}_{f_1})$, which means that V has maximal cardinality for a given s_1, namely $|V| = p^{2s_1}$.

Proposition 3.4.2. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 2$. Assume that ρ is trivial and that $v = 2\, s_n$.*

1. *Then for all i in $\{1, \dots, n\}$, $s_i = s$ and $V = Z(\mathrm{Ad}_{f_1})$.*
2. *There exists an integer d dividing s and some $\gamma_2, \dots, \gamma_n$ in $\mathbb{F}_{p^d} - \mathbb{F}_p$ such that :*

$$S_1 = \sum_{j=0}^{s/d} a_{jd}\, F^{jd} \qquad \text{and} \qquad \forall\, i \in \{2, \dots, n\} \quad S_i = \gamma_i\, S_1.$$

Moreover, $\{\gamma_1 := 1, \gamma_2, \dots, \gamma_n\}$ are linearly independent over $\mathbb{F}_p$. It follows that $s \geq 2$.

Proof :

1. As $v \leq 2\, s_1 \leq 2\, s_n$, the hypothesis $v = 2\, s_n$ implies that each s_i is equal to s_1. From now on, $s_1 = s_2 = \ldots = s_n$ is denoted by s. By Proposition 3.2.16, $V \subset \cap_{1 \leq i \leq n} Z(\mathrm{Ad}_{f_i}) \subset Z(\mathrm{Ad}_{f_1})$. As the two vector spaces V and $Z(\mathrm{Ad}_{f_1})$ have the same dimension over $\mathbb{F}_p$, namely $v = 2\, s$, we conclude that $Z(\mathrm{Ad}_{f_1}) = V = Z(\mathrm{Ad}_{f_i})$ for all i in $\{1, \dots, n\}$. Since k is algebraically closed and since Ad_{f_1} and Ad_{f_i} are monic, it follows that $\mathrm{Ad}_{f_1} = \mathrm{Ad}_{f_i}$.

2. Let i in $\{2,\dots,n\}$. Write : $S_1 = \sum_{k=0}^{s} a_k\ F^k$ and $S_i = \sum_{k=0}^{s} b_k\ F^k$, with $a_s \neq 0$ and $b_s \neq 0$. Then $\mathrm{Ad}_{f_1} = \frac{1}{a_s}\ F^s\ (\sum_{k=0}^{s}(a_k\ F^k + F^{-k}\ a_k)) = \mathrm{Ad}_{f_i} = \frac{1}{b_s}\ F^s\ (\sum_{k=0}^{s}(b_k\ F^k + F^{-k}\ b_k))$. As for all $\alpha \in k$, $F\ \alpha = \alpha^p\ F$, we obtain : $\gamma_i\ \sum_{k=0}^{s}(a_k^{p^s}\ \ F^{s+k} + a_k^{p^{s-k}}\ \ F^{s-k}) = \sum_{k=0}^{s}(b_k^{p^s}\ \ F^{s+k} + b_k^{p^{s-k}}\ \ F^{s-k})$, with $\gamma_i\, a_k^{p^s} = b_k^{p^s}$ and $\gamma_i\, a_k^{p^{s-k}} = b_k^{p^{s-k}}$, for all $0 \leq k \leq s$. It implies that $\gamma_i^{p^k} = \gamma_i$, for all $0 \leq k \leq s$ such that $a_k \neq 0$. In particular, as $a_s \neq 0$, then $\gamma_i \in \mathbb{F}_{p^s}$. If we denote by d the degree of the minimal polynomial of γ_i over $\mathbb{F}_p$, then $\mathbb{F}_{p^d} := \mathbb{F}_p(\gamma_i) \subset \mathbb{F}_{p^s}$, so d divides s. By the same token, for all $0 \leq k \leq s$ such that $a_k \neq 0$, $\gamma_i \in \mathbb{F}_{p^k}$. Therefore, $\mathbb{F}_{p^d} = \mathbb{F}_p(\gamma_i) \subset \mathbb{F}_{p^k}$, which proves that d divides k, whenever $a_k \neq 0$. It follows that $S_1 = \sum_{j=0}^{s/d} a_{jd}\, F^{jd}$. In addition, as $\gamma_i \in \mathbb{F}_{p^s}$, we gather from $b_k^{p^s} = \gamma_i\, a_k^{p^s}$ for all $0 \leq k \leq s$, that $S_i = \gamma_i\, S_1$.
Note that $\{\gamma_1,\dots,\gamma_n\}$ are linearly independent over $\mathbb{F}_p$. Otherwise, it would contradict the condition (c) imposed in Definition 3.2.7. It follows that none of the γ_i's, for $i \geq 2$, are in $\mathbb{F}_p$. So $s \geq 2$. □

We now display a family of big actions satisfying the conditions described in Proposition 3.4.2.

Proposition 3.4.3. *1. Let $s \in \mathbb{N}^*$, $d \in \mathbb{N}^*$ dividing s and $n \in \mathbb{N}^*$ such that $n \leq d$.
Take $\{\gamma_1 := 1, \gamma_2, \dots, \gamma_n\}$ in $\mathbb{F}_{p^d}$, linearly independent over $\mathbb{F}_p$.
Put $S_1 := \sum_{j=0}^{s/d} a_{jd}\, F^{jd} \in k\{F\}$, with $a_s \neq 0$.
For all i in $\{1,\dots,n\}$, we define $S_i := \gamma_i\, S_1 \in k\{F\}$ and $f_i(X) := X\, S_i(X) + c_i\, X \in k[X]$. Then for all i in $\{1,\dots,n\}$, $Z(\mathrm{Ad}_{f_i}) = Z(\mathrm{Ad}_{f_1})$.*

2. The function field of the curve C parametrized by : $W_i^p - W_i = f_i(X)$ with $1 \leq i \leq n$, is an étale extension of $k[X]$ with Galois group $\Gamma \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Then the group of translations of the affine line : $\{X \to X + y,\ y \in V\}$, where $V := Z(\mathrm{Ad}_{f_1})$, extends to an automorphism p-group of C, say G, such that :

$$0 \longrightarrow \Gamma \simeq (\mathbb{Z}/p\,\mathbb{Z})^n \longrightarrow G \longrightarrow V = Z(\mathrm{Ad}_{f_1}) \longrightarrow 0.$$

3. Thus, we obtain a big action (C,G) whose derived group G' is isomorphic to $(\mathbb{Z}/p\,\mathbb{Z})^n$ and such that the representation ρ is trivial. Moreover, $Z(G) = G' = \mathrm{Fratt}(G) \simeq (\mathbb{Z}/p\mathbb{Z})^n$, where $\mathrm{Fratt}(G)$ denotes the Frattini subgroup of G. Then G is a special group (see [Su86], Def. 4.14). Besides, if $p > 2$, G has exponent p, whereas, if $p = 2$, G has exponent p^2.

Proof :

1. Fix i in $\{1,\dots,n\}$. Then $\gamma_i\,\mathrm{Ad}_{f_1} = \frac{\gamma_i}{a_s^{p^s}}\ F^s\ \sum_{j=0}^{s/d} (a_{jd}\, F^{jd} + F^{-jd}\, a_{jd})$. Since γ_i lies in $\mathbb{F}_{p^d}$, $\gamma_i\,\mathrm{Ad}_{f_1} = \frac{1}{a_s^{p^s}}\ F^s, \sum_{j=0}^{s/d} (a_{jd}\,\gamma_i\, F^{jd} + F^{-jd}\, a_{jd}\gamma_i) = \frac{a_s^{p^s}\ \gamma_i}{a_s^{p^s}}\ \mathrm{Ad}_{f_i} = \gamma_i\,\mathrm{Ad}_{f_i}$. So, $Z(\mathrm{Ad}_{f_i}) = Z(\mathrm{Ad}_{f_1})$.
2. As $Z(\mathrm{Ad}_{f_i}) = \{y \in k,\ \Delta_y(f_i) = 0 \mod \wp(k[X])\}$ (see [LM05], Prop. 5.5), it follows that, for all y in V, $\Delta_y(f_i) = 0 \bmod \wp(k[X])$. So, Galois theory ensures the existence of the group G.
3. We deduce from the first point that $|G| = |G'||V| = p^{n+2\,s}$. We compute the genus of C by means of the formula given in Corollary 4.1. This yields : $g = \frac{(p^n-1)\,p^s}{2}$. Therefore, $\frac{|G|}{g} = \frac{2\,p^{n+s}}{p^n-1}$. So, the pair (C,G) is a big action.
We now show that $Z(G) = G'$. By Proposition 3.2.16, $Z(G)$ contains G'. Conversely, let H be an index p-subgroup of G'. As $H \subset G' \subset Z(G)$, H is normal in G and Lemma 2.2.4.2 in Chapter 2 implies that the pair $(C/H, G/H)$ is a big action. The curve C/H is parametrized by an Artin-Schreier equation : $W^p - W = f(X) := \sum_{i=1}^{n} \lambda_i\, f_i(X)$, with $(\lambda_1,\dots,\lambda_n) \in \mathbb{F}_p^n$ not all zeros. Condition (c) of Definition 3.2.7.4 imposes $\deg(f) = \max_{i=1,\dots,n}\{\deg\,\lambda_i\ f_i(X)\} = 1 + p^{s_1}$. Besides, by Proposition 3.2.14, we get the following exact sequence :
$$0 \longrightarrow (G/H)' \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G/H \longrightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^{2s_1} \longrightarrow 0.$$
In this case, Proposition 8.1 in [LM05] shows that G/H is an extraspecial group, which involves $G'/H = (G/H)' = Z(G/H)$. We denote by $\pi : G \to G/H$ the canonical mapping. Then $\pi(Z(G)) \subset Z(G/H) = G'/H$. As H is included in $Z(G)$, it follows that $Z(G) \subset G'$. Since $Z(G) = G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$ and since $G' = \mathrm{Fratt}(G)$ for any p-group G, we gather that G is a special group. Moreover, if $p > 2$, Proposition 8.1 in [LM05] shows that G/H is an extraspecial group with exponent p. Then $\pi(G)^p = \{e\}$ and G^p is included in H, for any hyperplanes H of G'. It follows that $G^p = \{e\}$. If $p = 2$, the same proposition shows that G/H has exponent p^2. It implies that G also has exponent p^2. □

Remark 3.4.4. *In the situation described in Proposition 3.4.3, $\frac{|G|}{g^2} = \frac{4\,p^n}{(p^n-1)^2}$. Note that the latter quotient does not depend on s any more.*

Corollary 3.4.5. *Let (C,G) be a big action as in Proposition 3.4.3. Let $A_{\infty,1}$ be the wild inertia subgroup of $\mathrm{Aut}_k(C)$ at ∞. Then G is equal to $A_{\infty,1}$.*

Proof : For any big action (C, G), G is included in $A_{\infty,1}$. Furthermore, Corollary 2.2.10 in Chapter 2 shows that the pair $(C, A_{\infty,1})$ is a big action with $A'_{\infty,1} = G'$. Now, assume that (C, G) is a big action as described in Proposition 3.4.3. Then $p^{2s} = \frac{|G|}{|G'|} \leq \frac{|A_{\infty,1}|}{|A'_{\infty,1}|} \leq p^{2\,s}$. It follows that, in this special case, G is equal to $A_{\infty,1}$. □

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

In this section, we define a filtration on the derived group G' of any group G. More specifically, we focus on groups G that are extensions of G' by G/G', both of them being p-elementary abelian, and we investigate the case where the number of jumps in the filtration of G' is maximal. Then we apply these results to the case of big actions with a p-elementary abelian G'. This allows us to give a group-theoretic condition to characterize the big actions such that each function f_i lies in $\Sigma_{i+1} - \Sigma_i$. In this situation, we prove that the filtration on G' actually coincides with its upper ramification filtration as exposed in Section 3.2.4.2. and that, as opposed to the previous case, the number of jumps in the filtration is maximal whereas the cardinality of V is minimal in regard to Lemma 3.3.12, namely : $v = s_1 + 1$.

3.5.1 A filtration on G'.

Definition 3.5.1. *For any group G, we define a sequence of subgroups $(\Lambda_i(G))_{i\geq 0}$ as follows. Put $\Lambda_0(G) := \{e\}$, where e means the identity element of G. For all $i \geq 1$, let $\pi_{i-1} : G \to \frac{G}{\Lambda_{i-1}(G)}$ be the canonical mapping. Then $\Lambda_i(G)$ is the subgroup of G defined by $\pi_{i-1}^{-1}(Z(\frac{G}{\Lambda_{i-1}(G)}) \cap (\frac{G}{\Lambda_{i-1}(G)}))'$. Therefore,*

$$\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = Z(\frac{G}{\Lambda_{i-1}(G)}) \cap (\frac{G}{\Lambda_{i-1}(G)})'.$$

In this way, we get an ascending sequence of subgroups of G' :

$$\{e\} = \Lambda_0(G) \subset \Lambda_1(G) \subset \Lambda_2(G) \subset \ldots \subset G',$$

which are characteristic subgroups of G.

In Section 3.5.3, we shall study the link between this filtration and the upper (resp. lower) central series. In what follows, we study the filtration $(\Lambda_i(G))$ in the special case where G is a p-group with the exact sequence :

$$0 \longrightarrow G' \simeq (\mathbb{Z}/p\,\mathbb{Z})^n \longrightarrow G \xrightarrow{\pi} V \simeq (\mathbb{Z}/\,p\,\mathbb{Z})^v \longrightarrow 0. \tag{3.2}$$

In other words, G is a p-group whose Frattini subgroup is equal to $G' \simeq (\mathbb{Z}/\,p\,\mathbb{Z})^n$, with $n \geq 1$. For convenience, we fix a set theoretical section, i.e. a map $s : G/G' \to G$ such that $\pi \circ s = id_{G/G'}$. We also define a representation $\phi : G/G' \to \mathrm{Aut}(G')$ as follows. For all y in G/G' and all g in G', $\phi(y)(g) = s(y)^{-1}\,g\,s(y)$. As G/G' is a p-group, one can find a basis $\{g_1, \ldots, g_n\}$ of the $\mathbb{F}_p$-vector space G' in which, for all y in G/G', the matrix of the automorphism $\phi(y)$ belongs to the subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ made of the lower triangular matrices with identity on the diagonal, namely :

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

Note that for $n \geq 2$ and for all i in $\{1, \ldots, n-1\}$, $\ell_{i+1,i}$ is a linear form from G/G' to $\mathbb{F}_p$.

Proposition 3.5.2. *Let G be a group satisfying* (3.2)*. We keep the notation defined above. Then the following assertions are equivalent.*

1. *The filtration defined by the $(\Lambda_i(G))_{i\geq 0}$ satisfies :*

$$\{e\} = \Lambda_0(G) \subsetneq \Lambda_1(G) \subsetneq \Lambda_2(G) \subsetneq \ldots \subsetneq \Lambda_n = G',$$

which means, for all i in $\{1, \ldots, n\}$,

$$\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = Z(\frac{G}{\Lambda_{i-1}(G)}) \cap (\frac{G}{\Lambda_{i-1}(G)})' \simeq \mathbb{Z}/p\mathbb{Z}.$$

2. *For all i in $\{1,\dots,n\}$, $\Lambda_i(G)$ is the $\mathbb{F}_p$-vector subspace of G' spanned by $\{g_{n-i+1},\dots,g_n\}$.*
3. *For $n \geq 2$ and for all i in $\{1,\dots,n-1\}$, $\ell_{i+1,i}$ is a nonzero linear form.*

Proof : We prove that the first point implies the second one by induction on i. Assume $i = 1$. By the same argument as in Lemma 3.2.17, one proves that $\Lambda_1(G) = Z(G) \cap G'$ is equal to $\cap_{y\in G/G'} \operatorname{Ker}(\phi(y) - id)$. Then the form of $\Phi(y)$ shows that $\cap_{y\in G/G'} \operatorname{Ker}(\phi(y) - id)$ contains the $\mathbb{F}_p$-vector space spanned by g_n. As $\Lambda_1(G)$ is assumed to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$, it follows that $\Lambda_1(G) = \mathbb{F}_p\, g_n$. Now, take $i \geq 2$ and assume that $\Lambda_{i-1}(G)$ is the $\mathbb{F}_p$-vector subspace of G' spanned by $\{g_{n-i+2},\dots,g_n\}$. Then $\frac{G}{\Lambda_{i-1}(G)}$ is a p-group with the following exact sequence :

$$0 \longrightarrow \frac{G'}{\Lambda_{i-1}(G)} = (\frac{G}{\Lambda_{i-1}(G)})' \simeq (\mathbb{Z}/p\,\mathbb{Z})^{n-i+1} \longrightarrow \frac{G}{\Lambda_{i-1}(G)} \xrightarrow{\pi} G/G' \simeq (\mathbb{Z}/\,p\,\mathbb{Z})^{v} \longrightarrow 0.$$

This exact sequence induces a representation $\phi_{i-1} : G/G' \to \operatorname{Aut}(\frac{G'}{\Lambda_{i-1}(G)})$. Consider the canonical mapping : $\pi_{i-1} : G' \to \frac{G'}{\Lambda_{i-1}(G)}$. In the basis $\{\pi_{i-1}(g_1)\dots,\pi_{i-1}(g_{n-i+1})\}$, the matrix $\Phi_{i-1}(y)$ of the automorphism $\phi_{i-1}(y)$ reads :

$$\Phi_{i-1}(y) := \begin{pmatrix} 1 & 0 & 0 & \dots & 0\\ \ell_{2,1}(y) & 1 & 0 & \dots & 0\\ \ell_{3,1}(y) & \ell_{3,2}(y) & \dots & 0 & 0\\ \ell_{i,1}(y) & \ell_{i,2}(y) & \dots & 1 & 0\\ \ell_{n-i+1,1}(y) & \ell_{n-i+1,2}(y) & \dots & \ell_{n-i+1,n-i}(y) & 1 \end{pmatrix} \in \mathrm{GL}_{n-i+1}(\mathbb{F}_p),$$

where the maps $\ell_{i,j}$ are the same as in $\Phi(y)$. As in the case $i = 1$, $\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = Z(\frac{G}{\Lambda_{i-1}(G)}) \cap (\frac{G}{\Lambda_{i-1}(G)})'$ is equal to $\cap_{y\in G/G'}\operatorname{Ker}(\phi_{i-1}(y) - id)$. The latter is the $\mathbb{F}_p$-vector space of $(\frac{G}{\Lambda_{i-1}(G)})' = \frac{G'}{\Lambda_{i-1}(G)}$ generated by $\pi_{i-1}(g_{n-i+1})$. It follows that $\Lambda_i(G)$ is the $\mathbb{F}_p$-vector subspace of G' spanned by $\{g_{n-i+1},\dots,g_n\}$. As the second assertion trivially implies the first one, the equivalence between 1 and 2 is established.

We now prove that the second assertion implies the third one. Take $i \geq 1$. As seen above, $\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = \cap_{y\in G/G'}\operatorname{Ker}(\phi_{i-1}(y) - id)$ is the $\mathbb{F}_p$-vector space spanned by $\pi_{i-1}(g_{n-i+1})$. From the form of the matrix $\Phi_{i-1}(y)$, we gather that $\ell_{n-i+1,n-i}$ is non identically zero. The proof of the converse works by induction on i. If $i = 1$, the form of the matrix $\Phi(y)$, with each $\ell_{i+1,i}$ non identically zero, implies that $\Lambda_1(G) = \cap_{y\in G/G'}\operatorname{Ker}(\phi(y) - id)$ is the $\mathbb{F}_p$-vector subspace of G' spanned by g_n. Now, take $i \geq 2$ and assume that $\Lambda_{i-1}(G)$ is the $\mathbb{F}_p$-vector subspace of G' spanned by $\{g_{n-i+2},\dots,g_n\}$. By hypothesis, each linear form $\ell_{i+1,i}$ occurring in $\Phi_{i-1}(y)$ is non identically zero. It implies that $\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = \cap_{y\in G/G'}\operatorname{Ker}(\phi_{i-1}(y) - id)$ is the $\mathbb{F}_p$-vector space spanned by $\pi_{i-1}(g_{n-i+1})$. We conclude as above. □

Remark 3.5.3. *Note that the third condition of the Proposition 3.5.2 does not actually depend on the triangularization basis $\{g_1,\dots,g_n\}$ chosen for G'.*

Proposition 3.5.4. *Let G be a group satisfying* (3.2) *and the equivalent properties of Proposition 3.5.2. We assume that $n \geq 2$.*

1. *Then for all i in $\{2,\dots,n\}$, there exists $\lambda_i \in \mathbb{F}_p - \{0\}$ such that $\ell_{i+1,i} = \lambda_i\, \ell_{2,1}$. Therefore, one can choose a basis of G' in which the matrix $\Phi(y)$ reads as follows :*

$$\Phi(y) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0\\ \ell(y) & 1 & 0 & \dots & 0\\ \ell_{3,1}(y) & \ell(y) & \dots & 0 & 0\\ \ell_{i,1}(y) & \ell_{i,2}(y) & \dots & 1 & 0\\ \ell_{n,1}(y) & \ell_{n,2}(y) & \dots & \ell(y) & 1 \end{pmatrix},$$

where ℓ is a nonzero linear form from G/G' to $\mathbb{F}_p$.

2. *Furthermore, $n \leq p$.*

Proof : As G/G' is abelian, for all y and y' in V, $\Phi(y)\Phi(y') = \Phi(y')\Phi(y)$. Then for all i in $\{1,\dots,n-2\}$, the identification of the coefficients situated on the $(i+2)$-th line and the i-th column in the matrices $\Phi(y)\Phi(y')$ and $\Phi(y')\Phi(y)$ reads :

$$\ell_{i+2,i}(y) + \ell_{i+1,i}(y')\,\ell_{i+2,i+1}(y) + \ell_{i+2,i}(y') = \ell_{i+2,i}(y') + \ell_{i+1,i}(y)\,\ell_{i+2,i+1}(y') + \ell_{i+2,i}(y).$$

Therefore, for all y and y' in G/G', $\ell_{i+1,i}(y')\,\ell_{i+2,i+1}(y) = \ell_{i+1,i}(y')\,\ell_{i+2,i+1}(y)$. As $\ell_{i+1,i}$ and $\ell_{i+2,i+1}$ are nonzero linear forms, it follows that $\operatorname{Ker}\ell_{i+1,i} = \operatorname{Ker}\ell_{i+2,i}$. Then $\ell_{i+1,i}$ and $\ell_{i+2,i+1}$ are homothetic. It implies that, for all i in $\{2, \ldots, n\}$, there exists $\lambda_i \in \mathbb{F}_p - \{0\}$ such that $\ell_{i+1,i} = \lambda_i \, \ell_{2,1}$. We eventually replace the basis of G' : $(g_i)_{1 \leq i \leq n}$ with $(\frac{1}{\lambda_i} \, g_i)_{1 \leq i \leq n}$ and denote $\ell_{2,1}$ by ℓ. In this new basis, the matrix $\Phi(y)$ reads as expected and the first point is proved.

We now work with a basis of G' in which the matrix $\Phi(y)$ reads as in the first point. We take some y_0 in G/G' such that $\ell(y_0) \neq 0$. Write I_n for the identity matrix of size n. Then the matrix $\Phi(y_0) - I_n$ is nilpotent, with nilpotency order n, i.e. n is the smallest integer $m \geq 1$ such that $(\Phi(y_0) - I_n)^m = 0$. As G/G' has exponent p, then $(\Phi(y_0) - I_n)^p = \Phi(y_0)^p - I_n = 0$. It follows that $p \geq n$. □

Remark 3.5.5. *In the situation exposed in Proposition 3.5.2, that is to say in the case where each linear form $\ell_{i+1,i}$ in $\Phi(y)$ is non identically zero, the representation ϕ is said to be indecomposable, i.e. if $G' = H_1 \bigoplus H_2$, where H_1 and H_2 are two $\mathbb{F}_p$-subvectors spaces of G' stable by ϕ, then the H_i's are trivial (left as an exercise to the reader). Nevertheless, the converse is false, i.e. the representation ϕ can be indecomposable without the linear forms $\ell_{i+1,i}$'s being all nonzero.*

3.5.2 A group-theoretic characterization for big actions with $f_i \in \Sigma_{i+1} - \Sigma_i$.

In the sequel, we study the filtration defined by the $(\Lambda_i(G))_{i \geq 0}$ in the special case of a big action (C, G) whose G' is p-elementary abelian. Note that such a group G systematically satisfies condition (3.2). We now investigate the case where the group G satisfies the equivalent properties of Proposition 3.5.2. In particular, we show that these group-theoretic conditions characterize the big actions with a p-elementary abelian G' and such that each f_i lies in $\Sigma_{i+1} - \Sigma_i$. The final section will be devoted to explicit families of big actions satisfying these properties.

Notation. The notations used throughout this section are those established in Sections 3.2.1, 3.3.1 and 3.3.2.

Theorem 3.5.6. *Let (C, G) be a big action with $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, for $n \geq 2$.*
Assume that the group G satisfies the equivalent properties of Proposition 3.5.2.

- *Then $p \geq n + 1 \geq 3$.*
- *Furthermore, for all i in $\{1, \ldots, n\}$, $m_i = 1 + i \, p^{s_1}$. In particular, $f_i \in \Sigma_{i+1} - \Sigma_i$.*
- *Moreover, $v = \dim_k V = s_1 + 1$.*
- *In this case, $\frac{|G|}{g} = \frac{2\,p}{p-1} \, \frac{p^n \, (p-1)^2}{n \, p^n \, (p-1) + 1 - p^n} > \frac{2\,p}{p-1}$.*

Proof : For a fixed n, we prove by induction on i that for all i in $\{1, \ldots, n\}$ such that $i \leq p-1$, $m_i = 1 + i \, p^{s_1}$. By the way, we show that $n \leq p - 1$. Indeed, we cannot propagate the induction when $i = p - 1$ and $n = p$.

The first step of the induction derives from the definition of m_1. Then we consider some integer i such that $2 \leq i \leq n$ and $i \leq p - 2$ and assume that the proposition is true for all $j \leq i - 1$. As seen in Section 3.2.5, we can write :

$$\forall\, y \in V, \quad \Delta_y(f_i) := f_i(X + y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y) \, f_j(X) \qquad \mod \wp(k[X]), \tag{3.3}$$

where the maps $\ell_{j,i}$ from V to $\mathbb{F}_p$ refer to the coefficients of the matrix $L(y)$. As the group G satisfies the third condition of Proposition 3.5.2 which does not depend on the basis chosen for G', it follows from Proposition 3.2.12 and Remark 3.2.13 that for all i in $\{1, \ldots, n-1\}$, each $\ell_{i,i+1}$ is a nonzero linear form from V to $\mathbb{F}_p$.

1. *We first prove that the function f_i does not belong to Σ_i.*
   Assume that f_i lies in Σ_i and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y) \, f_j(X)$ and $a_0 := m_{i-1}$. By induction hypothesis, $m_{i-1} = 1 + (i-1) \, p^{s_1} \in \mathbb{N} - p\mathbb{N}$. Note that $X^{a_0} = X^{1+(i-1)\,p^{s_1}}$ lies in $\Sigma_i - \Sigma_{i-1}$. We gather from Lemma 3.7.6 that no $X^{a_0 p^r}$, with $r \geq 0$, belongs to Σ_{i-1}, so none of them can be found in $\Delta_y(f_i)$ which belongs to Σ_{i-1}, as f_i lies in Σ_i (cf. Lemma 3.3.9). Besides, the property (c) imposed on m_i by Definition 3.2.7.4 implies that, for any y in V such that $\ell_{i-1,i}(y) \neq 0$, $a_0 = m_{i-1}$ is the degree of $\sum_{j=1}^{i-1} \ell_{j,i}(y) \, f_j(X)$. Such an element y exists since $\ell_{i-1,i}$ is supposed to be a nonzero linear form. It follows that, when keeping the notation of Lemma 3.3.13, $f_{a_0}(X) = c_{m_{i-1}}(f_{i-1}) \, \ell_{i-1,i}(y) X^{a_0}$, where $c_{m_{i-1}}(f_{i-1}) \neq 0$ denotes the coefficient of $X^{m_{i-1}}$ in f_{i-1}. As p does not divide a_0, we gather from Lemma 3.3.13 that $f_{a_0}(X)$ is identically zero, which contradicts $\ell_{i-1,i}(y) \neq 0$. Therefore f_i does not belong to Σ_i. In particular, as $\Sigma_2 \subset \Sigma_i$, f_i does not belong to Σ_2. Accordingly, we can define an integer $a \leq m_i$ such that X^a is the monomial of f_i with highest degree which does not lie in Σ_2. Since f_i is assumed to be reduced mod $\wp(k[X])$, $a \not\equiv 0 \mod p$.
2. *We now prove that $a - 1 \geq 1 + (i-1) \, p^{s_1}$.*
   Assume that $a - 1 < 1 + (i-1) \, p^{s_1}$ and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y) \, f_j(X)$ and

$a_0 := m_{i-1} = 1+(i-1)\,p^{s_1} \in \mathbb{N} - p\mathbb{N}$. The proof works as above except that we now have to determine the monomials of f_i which could produce some p-powers of X^{a_0} in $\Delta_y(f_i)$. As $a-1 < a_0$, they must be searched for among the monomials of f_i with degree greater than a. But, by definition of a, such monomials belongs to Σ_2, so give monomials in $\Delta_y(f_i)$ which are in Σ_1, whereas $X^{a_0} = X^{1+(i-1)\,p^{s_1}}$ lies in $\Sigma_i - \Sigma_{i-1}$, with $i \geq 2$. Just as in the first point, we can conclude that, for any y in V such that $\ell_{i-1,i}(y) \neq 0$, $f_{a_0}(X) = c_{m_{i-1}}(f_{i-1})\,\ell_{i-1,i}(y) X^{a_0}$, which leads to the same contradiction as above.

3. *We show that p divides $a-1$.*
Assume that p does not divide $a-1$. We first suppose that $a-1 > 1+(i-1)\,p^{s_1}$ and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ and $a_0 := a-1 \in \mathbb{N} - p\mathbb{N}$. As explained above, the monomials in f_i with degree greater than a, produce in $\Delta_y(f_i)$ monomials which are in Σ_1. But, as p does not divide $a-1$, the monomial X^{a-1} cannot belong to Σ_1 : otherwise, $a-1 = 1$, which contradicts $a-1 > 1+(i-1)\,p^{s_1}$, with $i \geq 2$. So the only p-power of X^{a-1} that occur in $\Delta_y(f_i)$ comes from the monomial X^a of f_i : it is $c_a(f_i)\, a\, y\, X^{a-1}$, where $c_a(f_i) \neq 0$ denotes the coefficient of X^a in f_i. Besides, X^{a-1} does not occur in $\sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ whose degree is at most $1+(i-1)\,p^{s_1} < a-1$. We gather from Lemma 3.3.13 that $f_{a_0}(X) = c_a(f_i)\, a\, y\, X^{a_0}$ is identically zero. It implies that $V = \{0\}$, which is excluded for a big action. Accordingly, $a-1 = 1+(i-1)\,p^{s_1}$. The equality of the leading coefficients in (3.3) implies that for all y in V, $\ell_{i-1,i}(y) = \frac{a\, c_a(f_i)}{c_{m_{i-1}}(f_{i-1})}\, y$. So the kernel of the linear form $\ell_{i-1,i}$ is reduced to $\{0\}$ and $v \leq 1$, which contradicts Lemma 3.3.12. Accordingly, p divides $a-1$. Thus, 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.

4. *Put $j_0 := a - p^t = 1 + (\lambda-1)\,p^t$. We prove that $j_0 = 1+(i-1)\,p^{s_1}$.*
Indeed, if $j_0 < 1+(i-1)\,p^{s_1}$, then $a = j_0 + p^t < 1+(i-1)\,p^{s_1} + p^t$. Using the second point, we get : $1+(i-1)\,p^{s_1} < a = 1+\lambda\, p^t < 1+p^t+(i-1)\,p^{s_1}$. If $s_1 - t \geq 0$, it implies $(i-1)\,p^{s_1-t} < \lambda < 1+(i-1)\,p^{s_1-t}$ with $p^{s_1-t} \in \mathbb{N}$, which is impossible. So, $s_1 - t \leq -1$. In this case, as $i-1 < p$, the inequality $1+\lambda\, p^t < 1+(i-1)\,p^{s_1}+p^t$ yields : $\lambda - 1 < (i-1)\,p^{s_1-t} < p^{1+s_1-t} \leq 1$, which contradicts $\lambda \geq 2$. As a consequence, $j_0 \geq 1+(i-1)\,p^{s_1}$.
We now prove that $j_0 = 1+(i-1)\,p^{s_1}$. Assume that $j_0 > 1+(i-1)\,p^{s_1}$ and apply Lemma 3.3.13 to $f(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ and $a_0 := j_0 \in \mathbb{N} - p\mathbb{N}$. No p-power of X^{j_0} can be found in $\sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X)$ whose degree is at most $1+(i-1)\,p^{s_1} < j_0$. It follows that the monomials $X^{j_0 p^r}$ have to be searched for in $\Delta_y(f_i)$. Then the same argument as in the proof of Theorem 3.3.14 allows to write : $f_{a_0}(X) = T(y)\, X^{j_0}$ with $T(y) := \sum_{b=j_0+1}^{a} c_b(f_i)\, \binom{b}{j_0}\, y^{b-j_0}$, where $c_b(f_i)$ denotes the coefficient of X^b in $f_i(X)$. This entails the same contradiction with Lemma 3.3.12 as in the proof of Theorem 3.3.14. Therefore, $j_0 = 1+(i-1)\,p^{s_1}$.

5. *We gather that $v = t+1$.*
Indeed, since $j_0 = 1+(i-1)\,p^{s_1} = \deg f_{i-1}$, the equality of the corresponding coefficients in (3.3) reads : $T(y) = \ell_{i-1,i}(y)\, c_{m_{i-1}}(f_{i-1})$, which holds for all y in V. Put $\tilde{T} := \frac{T}{c_{m_{i-1}}(f_{i-1})}$. It has the same degree as T and satisfies $\tilde{T}(y) = \ell_{i-1,i}(y) \in \mathbb{F}_p$, for all y in V. It follows that $\tilde{T}^p - \tilde{T}$ is identically zero on V, so $v \leq t+1$. Using the same argument as in the proof of Theorem 3.3.14, we prove that $v \leq t$ contradicts Lemma 3.3.12. We gather that $v = t+1$.

6. *We prove that $s_1 = t$. It follows that $v = s_1 + 1$ and $a = 1 + i\, p^{s_1}$, which requires $p > n \geq 2$.*
As $j_0 = 1+(i-1)\,p^{s_1}$, then $a = j_0 + p^t = 1+(i-1)\,p^{s_1} + p^t$. But, $a = 1+\lambda\, p^t \geq 1 + 2\, p^t$. From $i-1 \leq p$, we gather that $p^t \leq (i-1)\,p^{s_1} < p^{s_1+1}$. Therefore, $t \leq s_1$. To prove the equality, we focus on the big action $(C/H_i, G/H_i)$ as defined in Proposition 3.2.14. Since $v = t+1$, then $|G/H_i| = p^{i+v} = p^{i+t+1}$. Besides, as $m_i \geq a = j_0 + p^t = 1+(i-1)\,p^{s_1} + p^t \geq 1 + p^{s_1} + p^t$,

$$g_{C/H_i} \geq \frac{(p-1)}{2}\, p^{i-1}\,(m_i - 1) \geq \frac{(p-1)}{2}\,(p^{i-1+s_1} + p^{i-1+t}).$$

If $u := s_1 - t \geq 1$, the lower bound for the genus becomes :

$$g_{C/H_i} \geq \frac{(p-1)}{2}\, p^{t+i-1}\,(p^u + 1) \geq \frac{(p-1)}{2}\, p^{t+i-1}\,(p+1).$$

This contradicts condition (N) insofar as :

$$\frac{|G/H_i|}{g_{C/H_i}} \leq \frac{2\,p}{p-1}\,\frac{p^{i+t}}{p^{i-1+t}\,(p+1)} = \frac{2\,p}{p-1}\,\frac{p}{p+1} < \frac{2\,p}{p-1}.$$

Therefore, $s_1 = t$, so $v = s_1 + 1$ and $a = 1+(i-1)\,p^{s_1} + p^t = 1 + i\, p^{s_1}$. Note that we find : $\lambda = i$. As λ is supposed to be prime to p and as $2 \leq i \leq n$ and $i \leq p-1$, it requires that $p > n \geq 2$.

7. *We conclude that $m_i = a = 1 + i\,p^{s_1}$.*
Assume $a < m_i$. Then by definition of a, there exists an integer $r \geq 0$ such that $m_i = 1 + p^r$. Thus, we get : $m_i = 1 + p^r > a = 1 + i\,p^{s_1} \geq 1 + 2\,p^{s_1}$. As $p \geq 3$, this implies $r \geq s_1 + 1$. We gather a new lower bound for the genus of C/H_i, namely :

$$g_{C/H_i} \geq \frac{(p-1)}{2}\,(p^{s_1} + p^{i-1}\,(m_i - 1)) = \frac{(p-1)}{2}\,(p^{s_1} + p^{i-1+r}) \geq \frac{(p-1)}{2}\,(1 + p^{i+s_1}).$$

As $|G/H_i| = p^{i+s_1+1}$, it follows that $\frac{|G/H_i|}{g_{C/H_i}} \leq \frac{2\,p}{(p-1)}\,\frac{p^{i+s_1}}{1+p^{i+s_1}} < \frac{2\,p}{(p-1)}$, which contradicts condition (N) for the big action $(C/H_i, G/H_i)$. Accordingly, $m_i = a = 1 + i\,p^{s_1}$, which completes the induction.

To conclude, we compute the genus by means of Corollary 4.1, namely $g = \frac{p-1}{2}\,p^{s_1}\,\frac{n\,p^n\,(p-1)+1-p^n}{(p-1)^2}$. It follows that

$$\frac{|G|}{g} = \frac{2\,p}{p-1}\,\frac{p^n\,(p-1)^2}{n\,p^n\,(p-1)+1-p^n} \geq \frac{2\,p}{p-1}\,\frac{p^n\,(p-1)^2}{p^n\,(p-1)^2+1-p^n} > \frac{2\,p}{p-1}. \qquad \square$$

Corollary 3.5.7. *Let (C, G) be a big action as in Theorem 3.5.6. Let $A_{\infty,1}$ be the wild inertia subgroup of $\mathrm{Aut}_k(C)$ at ∞. Then G is equal to $A_{\infty,1}$.*

Proof : By Chapter 2 (Corollary 2.2.10), the pair $(C, A_{\infty,1})$ is a big action such that $A'_{\infty,1} = G'$. It follows that G/G' is included in $A_{\infty,1}/A'_{\infty,1}$, both of them acting as a group of translations of $\mathrm{Spec}\,k[X]$. In the same way as we define the representation $\phi : G/G' \to \mathrm{Aut}(G')$ in Section 3.2.3 (or more generally in Section 3.6.1), consider a representation ψ from $A_{\infty,1}/A'_{\infty,1}$ to $\mathrm{Aut}(A'_{\infty,1})$. Fix an adapted basis of A (see Definition 3.2.7). By duality (see Remark 3.2.3 and Proposition 3.2.9), this gives a basis of $G' = A'_{\infty,1}$, in which the images of ϕ and ψ are subgroups of triangular matrices of $\mathrm{GL}_n(\mathbb{F}_p)$ (cf. Section 3.2.5). For all y in $A_{\infty,1}/A'_{\infty,1}$ (resp. G/G'), call $\Psi(y)$ (resp. $\Phi(y)$) the matrix of the automorphism $\psi(y)$ (resp. $\phi(y)$) in the previously fixed basis. When restricted to G/G', the two matrices coincide, i.e. if y lies in $G/G' \subset A_{\infty,1}/A'_{\infty,1}$, then $\Phi(y) = \Psi(y)$. As a consequence, the group $A_{\infty,1}$ also satisfies the third condition of Proposition 3.5.2. Therefore, by Theorem 3.5.6, $\frac{|A_{\infty,1}|}{|A'_{\infty,1}|} = s_1 + 1 = \frac{|G|}{|G'|}$. So, $G = A_{\infty,1}$. □

We conclude this section by showing that the big actions (C, G) such that G satisfies the equivalent properties of Proposition 3.5.2 are exactly those with $f_i \in \Sigma_{i+1} - \Sigma_i$.

Theorem 3.5.8. *Let (C, G) be a big action with $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, for $n \geq 2$.*
Then the following assertions are equivalent.

1. *For all i in $\{1, \ldots, n\}$, the function f_i lies in Σ_{i+1}-Σ_i.*
2. *The group G satisfies the equivalent properties of Proposition 3.5.2.*

Assume that these assertions are satisfied.

- *Then $p \geq n + 1 \geq 3$.*
- *For all i in $\{1, \ldots, n\}$, $m_i = 1 + i\,p^{s_1}$.*
- *Moreover, $v = s_1 + 1$ and $\frac{|G|}{g} = \frac{2\,p}{p-1}\,\frac{p^n\,(p-1)^2}{n\,p^n\,(p-1)+1-p^n}$.*
- *Furthermore, the upper ramification groups of G' coincide with the subgroups $\Lambda_i(G)$ studied in Section 3.5.1. More precisely, following the notation of Section 3.2.4.2, $(G')^{\nu_i} = \Lambda_{n-i}(G)$ for all i in $\{0, \ldots, n\}$.*

Proof : The implication from 2 to 1 comes from Theorem 3.5.6 which also shows that, in this case, $n \leq p-1$, $m_i = 1+i\,p^{s_1}$, for all i in $\{1, \ldots, n\}$, $v = s_1+1$ and $\frac{|G|}{g} = \frac{2\,p}{p-1}\,\frac{p^n\,(p-1)^2}{n\,p^n\,(p-1)+1-p^n} > \frac{2\,p}{p-1}$. Conversely, assume that the second assertion is satisfied. We prove by induction on i that, for all i in $\{1, \ldots, n-1\}$, the linear form $\ell_{i,i+1}$ is nonzero. Then by Proposition 3.2.12, Remark 3.2.13 and Remark 3.5.3, we gather that the group G satisfies the third condition of Proposition 3.5.2. We first study the case $i = 1$ and consider the big action $(C/H_2, G/H_2)$, as defined in Proposition 3.2.14, i.e. the big action whose curve C/H_2 is parametrized by $W_j^p - W_j = f_j(X)$, with $1 \leq j \leq 2$. By hypothesis, f_2 does not lie in Σ_2. We infer from Proposition 3.2.16 that the representation ρ associated with $(C/H_2, G/H_2)$ is non trivial. Then the linear form $\ell_{1,2}$ is nonzero. We now take $i \geq 2$ and assume that the property is true for all $j \leq i$. It means that, for all j in $\{1, \ldots, i-1\}$, the linear form $\ell_{j,j+1}$ is nonzero. Then by Theorem 3.5.6, for all j in $\{1, \ldots, i\}$, $m_j = 1+j\,p^{s_1}$ and $v = s_1+1$. We now write condition (N) for the big action $(C/H_{i+1}, G/H_{i+1})$ as defined in Proposition 3.2.14, that is to say the big action parametrized by $W_j^p - W_j = f_j(X)$, with $1 \leq j \leq i+1$. As $|G/H_{i+1}| = p^{v+i+1} = p^{s_1+i+2}$ and $g_{C_{H_{i+1}}} = \frac{p-1}{2}\,\{(\sum_{j=1}^{i} j\,p^{s_1+j-1}) + p^i\,(m_{i+1}-1)\}$, we gather that the inequality $\frac{|G_{H_{i+1}}|}{g_{C_{H_{i+1}}}} > \frac{2\,p}{p-1}$ is equivalent to the following condition on m_{i+1} :

$$m_{i+1} < p^{s_1+1} - (\sum_{j=1}^{i} j\,p^{s_1+j-1-i}) + 1 = p^{s_1}(p-1) + \sum_{j=2}^{i}(p-(j+1))\,p^{s_1+j-i-1} + (p-1)\,p^{s_1-i} + 1. \quad (3.4)$$

We now assume that $\ell_{i,i+1}$ is the null linear form. Then for all y in V, $\Delta_y(f_i) = \sum_{j=1}^{i-1} \ell_{j,i+1}(y)\, f_j(X) \mod \wp(k[X])$. This ensures that the function field of the curve $\mathcal{C} : W_j^p - W_j = f_j(X)$, with $1 \leq j \leq i+1$ and $j \neq i$, is a Galois extension of $k(X)$ whose group $\mathcal{H}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^i$ and, as usual, the group of translations by V extends to an automorphism group of $\mathcal{C}$, say $\mathcal{G}$, with the following exact sequence :

$$0 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G} \longrightarrow V \longrightarrow 0.$$

We compute the quotient $\frac{|\mathcal{G}|}{g_{\mathcal{C}}}$. As $|\mathcal{G}| = p^{s_1+i+1}$ and $g_{\mathcal{C}} = \frac{p-1}{2}\,\{(\sum_{j=1}^{i-1} j\, p^{s_1+j-1}) + p^{i-1}\,(m_{i+1}-1)\}$, one can check that $\frac{|\mathcal{G}|}{g_{\mathcal{C}}} > \frac{2\,p}{p-1}$ if and only if

$$m_{i+1} < p^{s_1+1} - \sum_{j=1}^{i-1} j\, p^{s_1+j-i} + 1 = p^{s_1}\,(p-1) + \sum_{j=1}^{i-2} (p-(j+1))\, p^{s_1+j-i} + (p-1)\, p^{s_1-i+1} + 1. \tag{3.5}$$

The condition (3.5) is verified since it is implied by (3.4). It follows that $(\mathcal{C}, \mathcal{G})$ is a big action. By Theorem 3.3.14, the $i+1$-th function : f_{i+1}, lies in Σ_{i+1}, which contradicts the hypothesis $f_{i+1} \in \Sigma_{i+2} - \Sigma_{i+1}$. Therefore, $\ell_{i,i+1}$ is a nonzero linear form, which completes the induction and prove the equivalence between 1 and 2.

We now prove the last statement on the upper ramification filtration of G'. Starting from a given adapted basis of A : $\{\overline{f_1(X)}, \dots, \overline{f_n(X)}\}$, we get, by duality with respect to the Artin-Schreier pairing, a basis of G', say $\{g_1, \dots, g_n\}$. As proved, for all i in $\{1, \dots, n\}$, $m_i = 1 + i\, p^{s_1}$, the jumps in the filtration of A, as defined in Section 3.2.4.1, are : $\mu_i = m_{i+1} = 1 + (i+1)p^{s_1}$, for all i in $\{0, \dots, n-1\}$. Put $\mu_n := 1 + m_n$. Then $A^{\mu_0} = \{0\}$ and, for all i in $\{1, \dots, n\}$, A^{μ_i} is the $\mathbb{F}_p$-vector subspace of A generated by $\overline{f_1(X)}, \dots, \overline{f_i(X)}$. By duality (see Proposition 3.2.9), $(G')^{\nu_n} = (G')^{\mu_n} = \{e\} = \Lambda_0(G)$ and, for all i in $\{0, \dots, n-1\}$, $(G')^{\nu_i} = (G')^{\mu_i}$ is the $\mathbb{F}_p$-vector subspace of G' generated by $g_{i+1}, \dots, g_n$, which is precisely $\Lambda_{n-i}(G)$, as seen in Proposition 3.5.2. □

3.5.3 The special case : $s_1 = 1$.

In what follows, we exhibit some properties of the group G when (C, G) is a big action satisfying the equivalent conditions of Theorem 3.5.8 with $s_1 = 1$. In particular, we highlight the link with the problem of capable groups, as studied by [Ha40] and [BT82], and with the p-groups of maximal class.

The center of G.

Proposition 3.5.9. *Let $p \geq 3$ and $2 \leq n \leq p-1$.*
Let (C, G) be a big action which satisfies the equivalent conditions of Theorem 3.5.8 with $s_1 = 1$.
Then $Z(G) \subset G'$. It follows that $Z(G)$ is cyclic of order p.

Proof : As G satisfies the conditions of Theorem 3.5.8, and so the third point of Proposition 3.5.2, $\Lambda_{n-1}(G)$ is an index-p subgroup of G'. As $\Lambda_{n-1}(G) = (G')^{\nu_1}$ (cf. Theorem 3.5.8), the quotient curve $C/\Lambda_{n-1}(G)$ is the p-cyclic cover of the affine line parametrized by $W_1^p - W_1 = f_1(X)$. Since $v = s_1 + 1 = 2$, it follows from [LM05] that the group $G/\Lambda_{n-1}(G)$ is the extraspecial group of order p^3 and exponent p. In particular, its center is a p-cyclic group generated by τ such that $\tau(X) = X$ and $\tau(W_1) = W_1 + 1$. Now, take $\sigma \in Z(G)$. Then σ induces $\tilde{\sigma} \in Z(G/\Lambda_{n-1}(G))$. So, $\sigma(X) = X$. As $k(X) = L^{G'}$, it implies that $Z(G)$ is included in G'. Besides, by Theorem 3.5.8, $\Lambda_1(G) = Z(G) \cap G' = Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$, which proves that $Z(G)$ is p-cyclic □

The link with the problem of capable groups.

Definition 3.5.10. *(cf. [Ha40] and [BT82])*
We say that a group G is capable if there exists a group Γ such that $G \simeq \frac{\Gamma}{Z(\Gamma)}$.

Proposition 3.5.11. *Let $p \geq 3$ and $2 \leq n \leq p-1$.*
Let (C, G) be a big action which satisfies the equivalent conditions of Theorem 3.5.8 with $s_1 = 1$.
Then for all i in $\{1, \dots, n\}$, the quotient group $G/\Lambda_i(G)$ is capable.

Proof : Theorem 3.5.8 implies that the cover $C \to C/G'$ is parametrized by n Artin-Schreier equations : $W_j^p - W_j = f_j(X) \in \Sigma_{j+1} - \Sigma_j$, with $1 \leq j \leq n$. Take i in $\{0, \dots, n-1\}$. Then the curve $C/\Lambda_i(G)$ is parametrized by the $n-i$ first equations : $W_j^p - W_j = f_j(X) \in \Sigma_{j+1} - \Sigma_j$, with $1 \leq j \leq n-i$. It follows that the pair $(C/\Lambda_i(G), G/\Lambda_i(G))$ is a big action (cf. Chapter 2 Lemma 2.2.4) which still satisfies Theorem 3.5.8 with $s_1 = 1$. We deduce from Proposition 3.5.9 that $\Lambda_1(G/\Lambda_i(G)) = Z(G/\Lambda_i(G))$. As $\frac{G/\Lambda_i(G)}{\Lambda_1(G/\Lambda_i(G))} \simeq G/\Lambda_{i+1}(G)$, we get the exact sequence :

$$0 \longrightarrow Z(G/\Lambda_i(G)) \longrightarrow G/\Lambda_i(G) \longrightarrow G/\Lambda_{i+1}(G) \longrightarrow 0.$$

The claim follows. □

The link with the central series and with the p-groups of maximal class.

Definition 3.5.12. *(cf. [LGM02] and [Hu67])*

1. *The upper central series of a group G is the ascending series :*

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_2(G) \subset \dots$$

of normal subgroups of G defined inductively by

$$\frac{Z_i(G)}{Z_{i-1}(G)} = Z(\frac{G}{Z_{i-1}(G)}) \quad \textit{for} \quad i \geq 1.$$

2. *The lower central series of a group G is the descending series :*

$$G = C_1(G) \supset C_2(G) \supset C_3(G) \supset \dots$$

of normal subgroups of G defined inductively by

$$C_{i+1}(G) := [C_i(G), G] \quad \textit{for} \quad i \geq 1$$

where $[C_i(G), G]$ denotes the commutator of $C_i(G)$ and G.

3. *A group G is said to be nilpotent if there exists an integer k such that $Z_k(G) = G$. If G is nilpotent, the nilpotency class c of G is the smallest integer $c \geq 1$ such that $Z_c(G) = G$.*
4. *Now, assume that G is a p-group of order p^k, with $k \geq 2$. We say that G is a p-group of maximal class if the nilpotency class of G is $k-1$.*

We first compare the two central series defined above with the filtration $(\Lambda_i(G))_{i\geq 0}$ defined in Section 3.5.1.

Proposition 3.5.13. *Let G be a group such that :*

$$\{e\} = \Lambda_0(G) \subset \Lambda_1(G) \subset \dots \subset \Lambda_{m-1}(G) = G'.$$

and set $\Lambda_m(G) := G$ (cf. Def. 3.5.1).

1. *Then with the notation of Definition 3.5.12,*

$$\forall\, i \in \{0, \dots m\}, \quad C_{m+1-i}(G) \subset \Lambda_i(G) \subset Z_i(G).$$

2. *The group G is nilpotent of nilpotency class $c \leq m$.*

Proof :

1. The definition of the subgroups $\Lambda_i(G)$ shows that $(\Lambda_i(G))_{0\leq i\leq m}$ is an ascending central series of G in the sense of [LGM02] (Def. 1.1.10). The inclusion $\Lambda_i(G) \subset Z_i(G)$ follows. To show the other inclusion, i.e. $C_{m+1-i}(G) \subset \Lambda_i(G)$, use [LGM02] (Lemma 1.1.18). Then the inclusion follows from [LGM02] (Lemma 1.1.19)
2. The previous result applied with $i = m$, shows that $Z_m(G) = G$. □

We now examine the case of a p-group G when (C, G) is a big action satisfying Theorem 3.5.8 with $s_1 = 1$. In this case, G is nilpotent of maximal class and the filtration $(\Lambda_i(G))_{i\geq 0}$ coincides with the two central series of G.

Proposition 3.5.14. *Let (C, G) be a big action with $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.*
Assume that (C, G) satisfies the equivalent properties of Theorem 3.5.8 with $s_1 = 1$.

1. *Then G is a p-group of order p^{n+2} and maximal class $n+1$.*
2. *With the notations of Definitions 3.5.1 and 3.5.12,*

$$\forall\, i \in \{0, \dots, n+1\}, \quad C_{n+2-i}(G) = \Lambda_i(G) = Z_i(G),$$

where $\Lambda_{n+1}(G) := G$.

Proof :

1. The proof works by induction on n. First assume that $n=1$. Proposition 3.5.9 implies : $\{e\} \neq Z(G) \subset G' \simeq \mathbb{Z}/p\mathbb{Z}$. As $v = s_1 + 1 = 2$, we obtain the following exact sequence :

$$0 \longrightarrow Z(G) = G' \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow 0$$

and G is an extraspecial group of order p^3. We deduce from [Hu67] (p. 362) that it has maximal class. Now, assume that $n \geq 2$ and that the property is true for all big actions $(\mathcal{C}, \mathcal{G})$ with $\mathcal{G}' \simeq (\mathbb{Z}/p\mathbb{Z})^{n-1}$ satisfying the equivalent properties of Theorem 3.5.8 with $s_1 = 1$. By Proposition 3.5.9, $\Lambda_1(G) = Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$. As (C,G) satisfies the hypotheses of Theorem 3.5.8, the parametrization of the function field of the curve reads : $W_j^p - W_j = f_j(X) \in \Sigma_{j+1} - \Sigma_j$, with $1 \leq j \leq n$. By Theorem 3.5.8, $Z(G) = \Lambda_1(G) = (G')^{\nu_{n-1}}$. By duality, it follows that $(C/Z(G), G/Z(G))$ is the big action parametrized by the $n-1$ first equations : $W_j^p - W_j = f_j(X) \in \Sigma_{j+1} - \Sigma_j$, with $1 \leq j \leq n-1$. So, the pair $(C/Z(G), G/Z(G))$ still satisfies the equivalent conditions of Theorem 3.5.8 with $s_1 = 1$. As its derived group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{n-1}$, the induction hypothesis implies that $G/Z(G)$ has maximal class $= n$. Moreover, $Z_i(G/Z_1(G)) = Z_{i+1}(G)/Z_i(G)$ for all i in $\{0, \ldots, c-1\}$, where c denotes the niloptency class of G. So, the nilpotency class of $G/Z(G)$ satisfies : $c(G/Z(G)) = c-1$. Therefore, $c = n+1$ and the claim follows.
2. Use [Hu67] (III, 14, Hilfsatz 14.2) together with Proposition 3.5.13. □

3.6 Examples.

We conclude this chapter with some examples illustrating the special case of big actions described in Theorem 3.5.8, namely the big actions (C,G) with a p-elementary abelian G' such that each f_i lies in $\Sigma_{i+1} - \Sigma_i$. Note that Theorem 3.5.8 is twofold : on the one hand, it gives a group-theoretic characterization of G (cf. 3.5.8.2) and, on the other hand, it displays a dual point of view related to the parametrization of the cover (cf. 3.5.8.1). When studying the special family explicitly constructed via equations in Proposition 3.6.1, the second point of view naturally dominates in the proof. On the contrary, when exploring a universal family as in Section 3.6.2, we are lead to combine both aspects.

Notation. The notations concerning big actions are those fixed in Sections 3.2.1 and 3.3.2. Moreover, let $W(k)$ be the ring of Witt vectors with coefficients in k. Then for any $\sigma \in k$, we denote by $\tilde{\sigma}$ the Witt vector $\tilde{\sigma} := (\sigma, 0, 0, \ldots) \in W(k)$. For any $S(X) := \sum_{i=0}^{s} \sigma_i X^i \in k[X]$, we denote by $\tilde{S}(X)$ the polynomial $\sum_{i=0}^{s} \tilde{\sigma_i} X^i \in W(k)[X]$.

3.6.1 A special family.

Case $s_1 = 1$.

Let $p \geq 3$ and $1 \leq n \leq p-1$. We first construct a special family of big actions (C,G) which satisfy the conditions of Theorem 3.5.8 with $s_1 = 1$ and so, $v = \dim_{\mathbb{F}_p} V = 2$. We shall distinguish the cases $n < p-1$ and $n = p-1$.

Proposition 3.6.1. *Let $p \geq 3$. Let $S(X) := \wp(X)$ and $Q(X) := \wp(S(X))$. Call V the $\mathbb{F}_p$-vector space V consisting of the set of zeroes of the polynomial Q.*

1. *Let n in $\{1, \ldots, p-2\}$. For all i in $\{1, \ldots, n\}$, we denote*

$$g_i(X) := \frac{S(X)^{i+1}}{(i+1)!} = \frac{(X^p - X)^{i+1}}{(i+1)!}.$$

Let $f_i := \mathrm{red}(g_i)$ be the reduced representative of g_i, as defined in the introduction. Let $C[n]$ be the curve parametrized by the n Artin-Schreier equations : $W_i^p - W_i = f_i(X)$, for $1 \leq i \leq n$. Then the function field of $C[n]$ is a Galois extension of $k(X)$ with group : $H[n] \simeq (\mathbb{Z}/p\mathbb{Z})^n$ and the group of translations of the affine line : $\{X \to X + y,\ y \in V\}$ extends to an automorphism p-group of $C[n]$, say $G[n]$, such that we get the exact sequence :

$$0 \longrightarrow H[n] \simeq (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow G[n] \longrightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow 0.$$

Such a pair $(C[n], G[n])$ is a big action with $G[n]' \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Moreover, this big action satisfies the conditions of Theorem 3.5.8 with $s_1 = 1$.

2. *Let $n = p-1$. We define $g_{p-1}(X) \in k[X]$ as the reduction mod p of the polynomial*

$$\frac{1}{p!}\left((X^p - X)^p - X^{p^2} + X^p\right) \in W(k)[X].$$

Let f_{p-1} be the reduced representative of g_{p-1}. Let $C[p-1]$ be the curve parametrized by the $p-1$ Artin-Schreier equations : $W_i^p - W_i = f_i(X)$, for $1 \leq i \leq p-1$, where the $p-2$ first f_i's are defined as in the first case. The function field of $C[p-1]$ is a Galois extension of $k(X)$ with group $H[p-1] \simeq (\mathbb{Z}/p\mathbb{Z})^{p-1}$ and the group of translations of the affine line : $\{X \to X+y,\, y \in V\}$ extends to an automorphism p-group of $C[p-1]$, say $G[p-1]$, with the following exact sequence :

$$0 \longrightarrow H[p-1] \simeq (\mathbb{Z}/p\,\mathbb{Z})^{p-1} \longrightarrow G[p-1] \longrightarrow V \simeq (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow 0.$$

Such a pair $(C[p-1], G[p-1])$ is a big action with $G[p-1]' \simeq (\mathbb{Z}/p\,\mathbb{Z})^{p-1}$. Moreover, this big action satisfies the conditions of Theorem 3.5.8 with $s_1 = 1$.

Proof : Using Proposition 3.2.14, we first observe that the second case implies the first one, when excluding the last equation : $W_{p-1}^p - W_{p-1} = f_{p-1}(X)$. Therefore, it is sufficient to prove the second point.

Fix $y \in V$. We begin by calculating $\Delta_y(g_i)$ for $1 \leq i \leq p-2$. So, take i in $\{1, \dots, p-2\}$. One first shows that

$$\Delta_y(g_i) = g_i(X+y) - g_i(X) = \sum_{j=1}^{i-1} \frac{S(y)^{i-j}}{(i-j)!}\, g_j(X) + g_i(y) + \frac{S(y)^i}{i!}\, S(X)$$

where the first sum is empty when $i=1$. Since $S(y)$ lies in $\mathbb{F}_p$ for all y in $Z(Q) = V$, one gets :

$$\Delta_y(g_i) = \sum_{j=1}^{i-1} \frac{S(y)^{i-j}}{(i-j)!}\, g_j(X) + g_i(y) + \wp(\frac{S(y)^i}{i!}\, X).$$

As k is an algebraically closed field, $g_i(y) = 0 \bmod \wp(k[X])$. We gather that $\Delta_y(g_1) = 0 \bmod \wp(k[X])$ and that, for all i in $\{2, \dots, p-2\}$, $\Delta_y(g_i) = \sum_{j=1}^{i-1} \ell_{j,i}(y)\, g_j(X) \bmod \wp(k[X])$ with $\ell_{j,i}(y) := \frac{S(y)^{i-j}}{(i-j)!} \in \mathbb{F}_p$. Since $g_i(X) - f_i(X)$ lies in $\wp(k[X])$ and since each $\ell_{j,i}(y)$ belongs to $\mathbb{F}_p$, it follows that

$$\forall\, i \in \{1, \dots, p-2\}, \quad \Delta_y(f_i) = \sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X) \qquad \bmod\ \wp(k[X]) \quad \text{with} \quad \ell_{j,i}(y) := \frac{S(y)^{i-j}}{(i-j)!}.$$

Now fix y in V and calculate $\Delta_y(g_{p-1})$. As $X^p - X = S(X) \bmod p$, we first notice that $(X^p - X)^p = \tilde{S}(X)^p \bmod p^2 W(k)[X]$. It follows that g_{p-1} can also be seen as the reduction mod p of the polynomial : $\frac{1}{p!}\,(\tilde{S}(X)^p - X^{p^2} + X^p) \in W(k)[X]$. By the same token, from $S(X+y) = S(X) + S(y) \bmod p$, we gather that $\tilde{S}(X+\tilde{y})^p = (\tilde{S}(X) + \tilde{S}(\tilde{y}))^p \bmod p^2 W(k)[X]$. It follows that

$$\tilde{S}(X+\tilde{y})^p - \tilde{S}(X)^p - \tilde{S}(\tilde{y})^p = \sum_{i=1}^{p-1} \binom{p}{i}\, \tilde{S}(X)^i\, \tilde{S}(\tilde{y})^{p-i} \quad \bmod\ p^2 W(k)[X].$$

Likewise,

$$(X+\tilde{y})^p - X^p - \tilde{y}^p - (X+\tilde{y})^{p^2} + X^{p^2} + \tilde{y}^{p^2} = \sum_{i=1}^{p-1} \binom{p}{i}\, (X^i\, \tilde{y}^{p-i} - X^{pi}\, \tilde{y}^{p(p-i)}) \quad \bmod\ p^2\, W(k)[X].$$

Then we obtain the following equalities :

$$\frac{1}{p!}(\tilde{S}(X+\tilde{y})^p - \tilde{S}(X)^p - \tilde{S}(\tilde{y})^p + (X+\tilde{y})^p - X^p - \tilde{y}^p - (X+\tilde{y})^{p^2} + X^{p^2} + \tilde{y}^{p^2})$$

$$= \sum_{i=1}^{p-2} \frac{\tilde{S}(\tilde{y})^{p-i-1}}{(p-i-1)!}\, \frac{\tilde{S}(X)^{i+1}}{(i+1)!} + \frac{\tilde{S}(\tilde{y})^{p-1}}{(p-1)!}\, \tilde{S}(X) + \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p!}\, (X^i\, \tilde{y}^{p-i} - X^{pi}\, \tilde{y}^{p(p-i)}) \quad \bmod\ pW(k)[X]$$

$$= \sum_{i=1}^{p-2} \frac{S(y)^{p-i-1}}{(p-i-1)!}\, \frac{S(X)^{i+1}}{(i+1)!} + \frac{S(y)^{p-1}}{(p-1)!}\, S(X) + \sum_{i=1}^{p-1} \frac{(-1)^i}{i}\, (X^i\, y^{p-i} - X^{ip}\, y^{p(p-i)}) \quad \bmod\ pW(k)[X]$$

since the kernel of the map :$\left\{\begin{array}{l} W(k) \to k \\ (a_0, a_1, \dots) \to a_0 \end{array}\right.$ is $pW(k)$. From $S(y) \in \mathbb{F}_p$, we infer :

$$\Delta_y(g_{p-1}) = \sum_{i=1}^{p-2} \frac{S(y)^{p-i-1}}{(p-i-1)!}\, g_i(X) + \wp(\frac{S(y)^{p-1}}{(p-1)!}\, X) + \wp(\sum_{i=1}^{p-1} \frac{(-1)^{i+1}}{i}\, X^i\, y^{p-i}) + g_{p-1}(y).$$

It follows that $\Delta_y(g_{p-1}) = \sum_{i=1}^{p-2} \ell_{i,p-1}(y)\, g_i(X) \mod \wp(k[X])$, with $\ell_{i,p-1}(y) = \frac{S(y)^{p-1-i}}{(p-1-i)!} \in \mathbb{F}_p$. Since $g_i - f_i \in \wp(k[X])$ and $\ell_{i,p-1}(y) \in \mathbb{F}_p$,

$$\Delta_y(f_{p-1}) = \sum_{i=1}^{p-2} \ell_{i,p-1}(y)\, f_i(X) \qquad \mod \wp(k[X]) \quad \text{with} \quad \ell_{i,p-1}(y) = \frac{S(y)^{p-1-i}}{(p-1-i)!}.$$

By Galois Theory, this ensures that the group $G[p-1]$ is well-defined. Furthermore, it is easy to check that for all i in $\{1, \dots, p-1\}$, $\deg f_i = 1 + i\, p$. In this case, the same computation as in the end of the proof of Theorem 3.5.6 shows that $\frac{|G[p-1]|}{g_{C[p-1]}} = \frac{2\,p}{p-1}\, \frac{p^{p-1}\,(p-1)^2}{(p-1)\,p^{p-1}\,(p-1)+1-p^{p-1}}$, which proves that the pair $(C[p-1], G[p-1])$ is a big action. To conclude, note that for all i in $\{1, \dots, p-2\}$ and for all y in V, $\ell_{i,i+1}(y) = S(y)$, which proves that $\ell_{i,i+1}$ is a nonzero linear form from V to $\mathbb{F}_p$. Therefore, because of Remarks 3.2.13 and 3.5.3, $G[p-1]$ satisfies the third assertion of Proposition 3.5.2 and then the conditions of Theorem 3.5.8. □

Remark 3.6.2. *The preceding proof shows that, in the case of Proposition 3.6.1,*

$$\forall\, y \in V,\ \forall\, i \in \{2, \dots, p-1\} \quad \textit{and} \quad \forall\, j \in \{1, \dots, i-1\}, \quad \ell_{j,i}(y) = \frac{S(y)^{i-j}}{(i-j)!}.$$

It follows that the matrix $L(y)$ defined in Section 3.2.5 now reads :

$$L(y) = \exp(S(y)\, J) = \sum_{i=0}^{n-1} \frac{(S(y) J)^i}{i!}$$

where J is the $n \times n$ nilpotent matrix :

$$J := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

In what follows, we explore the properties of the group $G[n]$ when $(C[n], G[n])$ is a big action as defined in Proposition 3.6.1. To compute the exponent, we still have to distinguish the case $n < p-1$ (Proposition 3.6.3) and the case $n = p-1$ (Proposition 3.6.4).

Proposition 3.6.3. *Let $(C[n], G[n])$ be the big action defined in the first point of Proposition 3.6.1, i.e. with $n < p-1$. The notations are those introduced in Proposition 3.6.1.*

1. *Let σ in $G[n]$. Let y in V such that $y := \sigma(X) - X$. Then*

$$\sigma[W] =^t L(y)[W] + X[\mathcal{R}(y)] + [Z(y)]$$

   where ${}^tL(y)$ denotes the transpose matrix of the upper triangular matrix $L(y)$ defined in Section 3.2.5., $[W] :=^t [W_1, \dots, W_n]$, $[\mathcal{R}(y)] :=^t [\frac{S(y)}{1\,!}, \dots, \frac{S(y)^n}{n\,!}]$, and $[Z(y)] :=^t [Z_1(y), \dots, Z_n(y)]$, where, for all i in $\{1, \dots, n\}$, $Z_i(y)$ is an element of k which satisfies $\wp(Z_i(y)) = g_i(y)$.

2. *The group $G[n]$ has exponent p.*

Proof :

1. For the need of the proof, it is more convenient to work with the non-reduced functions, namely the functions g_i's. However, we still write the equations : $W_i^p - W_i = g_i(X)$, without changing the notation of W_i. As seen in the proof of Proposition 3.6.1,

$$\forall\, y \in V, \quad \forall\, i \in \{1, \dots, n\},\ \Delta_y(g_i) = \sum_{j=1}^{i-1} \ell_{j,i}(y)\, g_j(X) + g_i(y) + \wp(P_i(X, y)),$$

where the sum on j is empty for $i = 1$ and where $P_i(X, y) := \frac{S(y)^i}{i!} X$. From $W_i^p - W_i = g_i(X)$, we infer that $\sigma(W_i^p - W_i) = \sigma(g_i(X)) = \Delta_y(g_i)$, which implies $\wp(\sigma(W_i)) = \wp(W_i + \sum_{j=1}^{i-1} \ell_{j,i}(y)\, W_j + X\, \frac{S(y)^i}{i!} + g_i(y))$. Therefore, for all i in $\{1, \ldots, n\}$,

$$\sigma(W_i) = W_i + \sum_{j=1}^{i-1} \ell_{j,i}(y)\, W_j + X\, \frac{S(y)^i}{i!} + Z_i(y),$$

where $Z_i(y)$ is an element of k such that $\wp(Z_i(y)) = g_i(y)$. Using the vector notations of the proposition, we thus obtain the expected formula.

2. To prove the second assertion, we compute $\sigma^p[W]$. An induction shows that :

$$\sigma^p[W] = ({}^tL(y))^p[W] + X(\sum_{i=0}^{p-1} ({}^tL(y))^i)\, [\mathcal{R}(y)]$$

$$+y\, (\sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i)\, [\mathcal{R}(y)] + (\sum_{i=0}^{p-1} ({}^tL(y))^i)\, [Z(y)].$$

We first notice that $({}^tL(y))^p$ is equal to the identity matrix I, since ${}^tL(y) - I$ is nilpotent of size $n \leq p-2$. Moreover, by Remark 3.6.2, ${}^tL(y) = \exp(J(y)) = \sum_{i=0}^{n-1} \frac{J(y)^i}{i!}$, where $J(y) := S(y)\, {}^tJ$. Accordingly,

$$\begin{aligned}
\textstyle\sum_{i=0}^{p-1} ({}^tL(y))^i &= \textstyle\sum_{i=0}^{p-1} \exp(i\, J(y)) \\
&= I + \textstyle\sum_{i=1}^{p-1} \sum_{j=0}^{n-1} \frac{(i\, J(y))^j}{j!} = I + \sum_{j=0}^{n-1} \frac{J(y)^j}{j!} \sum_{i=1}^{p-1} i^j \\
&= I + (\textstyle\sum_{i=1}^{p-1} i^0)\, I + \sum_{j=1}^{n-1} \frac{J(y)^j}{j!} \sum_{i=1}^{p-1} i^j \\
&= \textstyle\sum_{j=1}^{n-1} \frac{J(y)^j}{j!} \sum_{i=1}^{p-1} i^j \mod p
\end{aligned}$$

But one easily checks that $\mathcal{N}(j) := \sum_{i=1}^{p-1} i^j = 0 \bmod p$ for all j in $\{1, \ldots, p-2\}$. Since $n-1 \leq p-3$, we gather that $\sum_{i=0}^{p-1} ({}^tL(y))^i = 0 \bmod p$.
To conclude, the last sum to compute is $\mathfrak{S} := \sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i$. Likewise, one shows

$$\begin{aligned}
\mathfrak{S} &= \textstyle\sum_{i=0}^{p-2} (p-i-1) \exp(iJ(y)) \\
&= (p-1)\, I + \textstyle\sum_{i=1}^{p-2} (p-i-1) \sum_{j=0}^{n-1} \frac{(iJ(y))^j}{j!} \\
&= (p-1)\, I - \textstyle\sum_{i=1}^{p-2} (i+1)\, I - \sum_{j=1}^{n-1} \frac{J(y)^j}{j!} (\sum_{i=1}^{p-1} (i+1)\, i^j) \qquad \mod p \\
&= (p-1)\, I - (\mathcal{N}(1) - 1)\, I - \textstyle\sum_{j=1}^{n-1} \frac{J(y)^j}{j!} \mathcal{N}(j) - \sum_{j=2}^{n} \frac{J(y)^j}{j!} \mathcal{N}(j) \qquad \mod p
\end{aligned}$$

Since $\mathcal{N}(j) = 0$ when $1 \leq j \leq n \leq p-2$, it follows that $\sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i = 0 \bmod p$. As $\sigma^p(X) = X + p\, y = X \bmod p$, we gather that the order of σ divides p. Therefore, the group $G[n]$ has exponent p. □

Proposition 3.6.4. *Let $(C[p-1], G[p-1])$ be the big action defined in the second point of Proposition 3.6.1, i.e. with $n = p-1$. We keep the notations introduced in Proposition 3.6.1.*

1. *Let σ in $G[p-1]$. Let y in V such that $y := \sigma(X) - X$.*
Put $T(X, y) := \sum_{i=1}^{p-1} \frac{(-1)^{i+1}}{i} X^i\, y^{p-i}$, i.e. the reduction mod p of $\frac{1}{p}\{(X + \tilde{y})^p - X^p - \tilde{y}^p\} \in W(k)[X]$. Then
$$\sigma[W] ={}^t L(y)[W] + X\, [\mathcal{R}(y)] + [Z(y)] + [\mathcal{T}(X, y)],$$
where ${}^tL(y)$ denotes the transpose matrix of the matrix $L(y)$ defined in Section 3.2.5, $[W] :={}^t [W_1, \ldots, W_{p-1}]$, $[\mathcal{R}(y)] :={}^t [\frac{S(y)}{1\,!}, \ldots, \frac{S(y)^{p-1}}{(p-1)\,!}]$, $[\mathcal{T}(X, y)] ={}^t [0, 0, \ldots, 0, T(X, y)]$ and $[Z(y)] :={}^t [Z_1(y), \ldots, Z_{p-1}(y)]$ where, for all i in $\{1, \ldots, n\}$, $Z_i(y)$ is an element of k satisfying $\wp(Z_i(y)) = g_i(y)$.
2. *The group $G[p-1]$ has exponent p^2.*

Proof :

1. The proof of the second point of Proposition 3.6.1 shows that

$$\forall\, y \in V, \quad \Delta_y(g_{p-1}) = \sum_{j=1}^{p-2} \ell_{j,p-1}(y)\, W_j + \wp(P_{p-1}(X,y)) + g_{p-1}(y),$$

   where

$$P_{p-1}(X,y) := \frac{S(y)^{p-1}}{(p-1)!}\, X + \sum_{i=1}^{p-1} \frac{(-1)^{i+1}}{i}\, X^i\, y^{p-i} = \frac{S(y)^{p-1}}{(p-1)!}\, X + T(X,y).$$

   The same calculation as in the proof of Proposition 3.6.3 yields :

$$\sigma(W_{p-1}) = W_{p-1} + \sum_{j=1}^{p-2} \ell_{j,p-1}(y)\, W_j + \frac{S(y)^{p-1}}{(p-1)!}\, X + T(X,y) + Z_{p-1}(y),$$

   where $Z_{p-1}(y)$ is an element of k such that $\wp(Z_{p-1}(y)) = g_{p-1}(y)$. The formula of the first point then derives from the vector notation together with the expression of the others $\sigma(W_i)$, for $1 \leq i \leq p-2$, obtained in Proposition 3.6.3.

2. We now calculate $\sigma^p[W]$. As in the previous proof, an induction shows that :

$$\sigma^p[W] = ({}^tL(y))^p[W] + X(\sum_{i=0}^{p-1} ({}^tL(y))^i)\, [\mathcal{R}(y)] + y\, (\sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i)\, [\mathcal{R}(y)]$$

$$+(\sum_{i=0}^{p-1} ({}^tL(y))^i)\, [Z(y)] + \sum_{i=0}^{p-1} [\mathcal{T}(X+i\,y,y)].$$

   Still as in the proof of Proposition 3.6.3, ${}^tL(y)^p = I$ and $\sum_{i=0}^{p-1} ({}^tL(y))^i = \sum_{j=1}^{p-2} \frac{J(y)^j}{j!}\, \mathcal{N}(j)$, where $\mathcal{N}(j) := \sum_{i=1}^{p-1} i^j = 0 \bmod p$, for j in $\{1,\ldots,p-2\}$. Besides, as previously seen,

$$\begin{aligned} \textstyle\sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i &= -\textstyle\sum_{j=1}^{p-2} \frac{J(y)^j}{j!}\, \{\mathcal{N}(j) + \mathcal{N}(j+1)\} \\ &= -\tfrac{J(y)^{p-2}}{(p-2)!}\, \mathcal{N}(p-1) = \tfrac{J(y)^{p-2}}{(p-2)!} = J(y)^{p-2} \quad \bmod\ p \end{aligned}$$

   Then $y\, (\sum_{i=0}^{p-2} (p-i-1)\, ({}^tL(y))^i)\, [\mathcal{R}(y)] = y\, (S(y)\,{}^tJ)^{p-2}\, [\mathcal{R}(y)] =^t [0,\ldots,0, y\, S(y)^{p-1}] \bmod p$. To complete the calculation, one has to compute $\sum_{i=0}^{p-1} T(X+i\,y,y)$. As T is the reduction mod p of the polynomial $\frac{1}{p}\, \{(X+\tilde{y})^p - X^p - \tilde{y}^p\}$, it follows that

$$\begin{aligned} \textstyle\sum_{i=0}^{p-1} T(X+i\,y,y) &= \tfrac{1}{p} \textstyle\sum_{i=0}^{p-1} \{(X+(1+i)\,\tilde{y})^p - (X+i\,\tilde{y})^p - \tilde{y}^p\} \qquad \bmod\ p \\ &= \tfrac{1}{p}\, \{(X+p\,\tilde{y})^p - X^p - p\,\tilde{y}^p\} = -y^p \qquad \bmod\ p \end{aligned}$$

   Therefore, $\sigma^p[W] = [W] +^t [0,0,0,\ldots,0, y\, S(y)^{p-1} - y^p] \bmod p$. If $y \in \mathbb{F}_p$, or equivalently $S(y) = 0$, then $\sigma^p[W] = [W] +^t [0,0,0,\ldots,0,y] \bmod p$. Otherwise, $S(y) \neq 0$ and, as $S(y)$ lies in $\mathbb{F}_p$, $S(y)^{p-1} = 1 \bmod p$, which implies $\sigma^p[W] = [W] +^t [0,0,0,\ldots,0, y - y^p] = [W] +^t [0,0,0,\ldots,-S(y)] \bmod p$. We gather that if $y = 0$, the order of σ divides p. Otherwise, σ has order p^2. This proves the second assertion. □

We now describe the center of $G[n]$. As an application, we shall see that $G[n]$ is capable (cf. Def. 3.5.10) for all $1 \leq n \leq p-2$.

Proposition 3.6.5. *Let $(C[n], G[n])$ be a big action as defined in the first or the second point of Proposition 3.6.1, i.e. with $n < p-1$ or $n = p-1$. Let σ in $G[n]$. Then σ belongs to the center of $G[n]$ if and only if*

$$\sigma(X) = X \quad \textit{and} \quad \forall\, i \in \{1,\ldots,n-1\},\ \sigma(W_i) = W_i$$

It follows that the center of $G[n]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof : One can use the same method and calculation as in the previous propositions. One can also directly deduce from Proposition 3.5.9 that the center is p-cyclic. □

Corollary 3.6.6. *Let $p \geq 3$. We keep the notation of Proposition 3.6.1.*

1. *The group $G[1]$ is the extraspecial group of order p^3 and exponent p, namely the unique non abelian group of order p^3 and exponent p. Moreover, we get the following exact sequence :*

$$0 \longrightarrow Z(G[1]) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G[1] \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow 0.$$

   It follows that the extraspecial group of order p^3 and exponent p, with $p > 2$, is capable as defined in Definition 3.5.10. More precisely, $G[1] \simeq \frac{\Gamma}{Z(\Gamma)}$ with $\Gamma = G[2]$.

2. *More generally, for all $2 \leq n \leq p-1$, we have the following exact sequence :*

$$0 \longrightarrow Z(G[n]) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow G[n] \longrightarrow G[n-1] \longrightarrow 0.$$

   It follows that the group $G[n-1]$ is capable, namely $G[n-1] \simeq \frac{\Gamma}{Z(\Gamma)}$ with $\Gamma = G[n]$.

Proof :

1. The first assertion derives from [LM05] (Prop. 8.1).
2. Call $K_n := k(C[n]) = k(X, W_1, \ldots, W_n)$ the function field of the curve $C[n]$. Put $k(T) := K_n^{G[n]}$, where $T = Q(X)$, Q being defined as in Proposition 3.6.1. Then Galois theory, combined with Proposition 3.6.5, gives the following exact sequence :

$$0 \longrightarrow Gal(K_n/K_{n-1}) \simeq Z(G[n]) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow Gal(K_n/k(T)) \longrightarrow Gal(K_{n-1}/k(T)) \longrightarrow 0.$$

   The claim directly follows. □

Remark 3.6.7. 1. *Computation using MAGMA package on finite groups shows that, for $n \geq 2$, the group $G[n]$ is, in general, not uniquely determined by the group extension conditions mentioned in Corollary 3.6.6.*

2. *Note that [BT82] (Example 1.12 p.187) gives another proof of the fact that the extraspecial group of order p^3 and exponent p, with $p > 2$, is capable. Nevertheless, this proof uses some group Γ of order p^5 whereas, in our case, $\Gamma = G[2]$ has order p^4.*

General case.

Starting from the big actions defined in Proposition 3.6.1, for which $s_1 = 1$, we use the base change displayed in Chapter 2 (Section 2.3) to obtain new ones which still satisfy the conditions of Theorem 3.5.8 but have arbitrary large s_1.

Proposition 3.6.8. *Let $p \geq 3$, $1 \leq n \leq p-1$ and $s_0 \in \mathbb{N}$. Let $S_0(X)$ be an additive separable polynomial of $k[X]$ with degree p^{s_0}. Let $(C[n], G[n])$ be the big action defined in Proposition 3.6.1. Consider the additive polynomial map $S_0 : \mathbb{P}^1_k \to C[n]/G[n]' \simeq \mathbb{P}^1_k$.*

1. *Let $\tilde{C}[n] := C[n] \times_{\mathbb{P}^1_k} \mathbb{P}^1_k$ be the curve obtained after the base change defined by S_0. Then the cover $\tilde{C}[n] \to C[n]/G[n]$ is Galois with group $\tilde{G}[n] \simeq G[n] \times (\mathbb{Z}/p\mathbb{Z})^{s_0}$. Moreover, the pair $(\tilde{C}[n], \tilde{G}[n])$ is a big action with $\tilde{G}[n]' \simeq G[n]' \times \{0\}$ and $Z(\tilde{G}[n]) \simeq (\mathbb{Z}/p\mathbb{Z})^{s_0+1}$.*
2. *This big action $(\tilde{C}[n], \tilde{G}[n])$ satisfies the conditions of Theorem 3.5.8 with $s_1 = s_0 + 1$.*

Proof :

1. The first assertion derives from Chapter 2 (Prop. 2.3.1). Another proof consists in replacing X with $S_0(X)$ in the proof of Proposition 3.6.1, knowing that the calculation only requires S_0 to be additive.
2. One deduces from Lemmas 3.3.7.2 and 3.3.7.7 that $f_i(X) \in \Sigma_{i+1} - \Sigma_i$ implies $f_i(S_0(X)) \in \Sigma_{i+1} - \Sigma_i$. The claim follows. Another proof consists in considering the filtration $(\Lambda_i(G[n]))_{i \geq 0}$, as defined in Section 3.5.1. By Proposition 3.6.1, this filtration satisfies the first condition of Proposition 3.5.2. Then one concludes by checking that, for all $i \geq 0$, $\Lambda_i(\tilde{G}[n]) \simeq \Lambda_i(G[n])$. □

3.6.2 A universal family.

Under the hypotheses of Theorem 3.5.8, one already knows the form of the functions f_i's, namely their degree $m_i = 1 + i\,p^{s_1}$ and their belonging to $\Sigma_{i+1} - \Sigma_i$. For given p, s_1 and $n \leq p-1$, this naturally yields an algorithmic method to parametrize the functions f_i's. In this way, we obtain a universal family parametrizing the big actions (C, G) that satisfy Theorem 3.5.8 with f_1 monic and $s_1 = 1$. Eventhough it theoretically works for any $p \geq 3$, in what follows, we merely illustrate this method in the special case $p = 5$ and $n \leq p - 1 = 4$. In this case, we also describe the corresponding space of parameters and, when $n = 2$, we give necessary and sufficient conditions on the parameters for two curves of the family to be isomorphic and we characterize the subfamily corresponding to the special curves that are studied in Section 3.6.1.1. In each case, we eventually try to determine the different non-isomorphic models which can occur for the corresponding group G. Following what has been done for the p-cyclic case in Chapter 1 (§ 1.2.10), one should compare the results obtained in this section with the works of Pries ([Pr05]) and Kontogeorgis ([Kon07]).

Notation. The notations used throughout this section are those established in Sections 3.2.1 and 3.3.2.

Proposition 3.6.9. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/5\mathbb{Z})^2$. Assume that (C, G) satisfies the conditions of Theorem 3.5.8 with $s_1 = 1$.*

1. *Then there exists a coordinate X for the projective line $C/G' \simeq \mathbb{P}_1$ and an adapted basis for A such that the functions f_i's read as follows :*

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

$$f_2(X) = b_{11}^5\,X^{11} + 4\,b_{11}^{25}\,X^7 + 2\,(b_{11}^{50} - b_{11}^2)\,b_{11}^{-5}\,X^3 + b_1\,X$$

where $b_{11} \in k - \{0\}$ and $b_1 \in k$ are algebraically independent parameters. In this case,

$$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{25} + 4\,(b_{11}^{125} + b_{11}^5)\,b_{11}^{-25}\,X^5 + X)$$

$$\forall\, y \in V, \quad \ell_{1,2}(y) = 2\,(b_{11}^5\,y^5 - b_{11}^{25}\,y)$$

2. *Two pairs of parameters (b_{11}, b_1) and (b'_{11}, b'_1) in $k^\times \times k$ give isomorphic k-curves C if and only if*

$$(\frac{b'_{11}}{b_{11}})^{24} = 1 \quad \text{and} \quad b'_1 = \pm\,\frac{b'_{11}}{b_{11}}\,b_1.$$

3. *The linear base change : $X \to \lambda\,X$, with $\lambda \in k^\times$, applied to the big action defined in Proposition 3.6.1, gives a subfamily of the universal family $\{f_1, f_2\}$ displayed above if and only if $\lambda \in \mathbb{F}_{25}^\times$. The subfamily obtained in this case is the one characterized by $b_{11}^{24} = 1$ and $b_1 = 0$.*
4. *The group G is isomorphic to the one obtained in Proposition 3.6.1. More precisely,*
   (a) *The group G has order 5^4, exponent 5 and 5-rank 2.*
   (b) *The center of G is cyclic of order 5.*
   (c) *The quotient group $G/Z(G)$ is an extraspecial group of exponent 5.*
   (d) *The group G is nilpotent of maximal class 3.*
   (e) *Call $C_G(G')$ the centralizer of G' in G. Then $C_G(G')/G' \simeq \{y \in V,\ \phi(y) = id\}$, is cyclic of order 5.*

Proof :

1. After an homothety and a translation, one can rigidify the parametrization and fix a coordinate X for the projective line $C/G' \simeq \mathbb{P}_1$ such that f_1 is a monic polynomial with no monomial of degree one (cf. Cor. 3.2.12). Then Theorem 3.5.8 implies that the functions f_i's read as follows :

$$f_1(X) = X^{1+5} + a_2\,X^2$$

$$f_2(X) = b_{11}^5\,X^{1+2.5} + b_7\,X^{2+5} + b_3\,X^3 + b_6\,X^{1+5} + b_2\,X^2 + b_1\,X$$

with $b_{11} \neq 0$. Note that, for convenience of calculation, the coefficient of X^{11} is directly written as a p-power. Following Proposition 3.2.16, we first calculate $\mathrm{Ad}_{f_1}(Y) = Y^{25} + 2\,a_2^5\,Y^5 + Y$. As V is included in $Z(\mathrm{Ad}_{f_1})$ and as these two vector spaces have the same dimension over $\mathbb{F}_p$, namely $s_1 + 1 = 2 = 2\,s_1$, we gather that $V = Z(\mathrm{Ad}_{f_1})$. Now consider the relation :

$$\forall\, y \in V, \qquad \Delta_y(f_2) = \ell_{1,2}(y)\,f_1(X) \qquad \mod\ \wp(k[X]). \tag{3.6}$$

Computations using Maple show that for all y in V, $\ell_{1,2}(y) = 2\,b_7\,y + 2\,b_{11}^5\,y^5$. As $V = Z(\mathrm{Ad}_{f_1})$, we deduce from Proposition 3.2.12 that $\mathrm{Ad}_{f_1}(X)$ divides the polynomial $(2\,b_7\,X + 2\,b_{11}^5\,X^5)^5 - (2\,b_7\,X + 2\,b_{11}^5\,X^5)$. This requires : $b_7 = 4\,b_{11}^{25}$ and $a_2 = 2\,(b_{11}^{25} + b_{11})\,b_{11}^{-5}$. In addition, (3.6) also yields $b_3 = 2\,(b_{11}^{50} - b_{11}^2)\,b_{11}^{-5}$ and $b_6 \in \mathbb{F}_5$. Accordingly, by replacing f_2 with $f_2 - b_6\,f_1$, one can assume that $b_6 = 0$. It follows that $b_2 = 0$, hence the expected formulas.

2. Use [LM05] (Prop. 3.3).

3. This directly comes from calculation.
4. The space of parameters of the universal family is a Zariski open of the linear affine space, which implies that it is irreducible and so connected. It follows from Proposition 4.3.2 (with $s_0 = 0$) combined with the previous point that G is isomorphic to the group obtained in Proposition 3.6.1. Then properties (a) , (b) (c) and (d) respectively derive from Proposition 3.6.3, Proposition 3.6.5, Corollary 3.6.6. and Proposition 3.5.14. We now prove the last point. Consider $W := \{y \in V,\ \phi(y) = id\} \subset V$. Because of the definition of the representation ϕ (cf. Section 3.2.3), we first notice that $C_G(G') = \{g \in G,\ g\, g_2\, g^{-1} = g_2,\ \forall\, g_2 \in G'\} = \pi^{-1}(W)$, where π is defined via the following exact sequence :

$$0 \longrightarrow G' \longrightarrow G \xrightarrow{\pi} V \longrightarrow 0.$$

Then $C_G(G')/G' \simeq W$. As $W := \{y \in V,\ \ell_{1,2}(y) = 0\}$ has dimension 1 over $\mathbb{F}_5$, it follows that $C_G(G')/G' \simeq \mathbb{Z}/5\mathbb{Z}$. □

Remark 3.6.10. *The first property of the fourth point of Proposition 4.3.2 is sufficient to characterize G. Indeed, MAGMA shows that there exists only one group G, up to isomorphism, such that G has order* 5^4*, exponent* 5 *and* 5*-rank* 2.

Proposition 3.6.11. *Let* (C, G) *be a big action such that* $G' \simeq (\mathbb{Z}/5\mathbb{Z})^3$*. Assume that* (C, G) *satisfies the conditions of Theorem 3.5.8 with* $s_1 = 1$.

1. *Then there exists a coordinate* X *for the projective line* $C/G' \simeq \mathbb{P}_1$ *and an adapted basis for* A *such that the functions* f_i*'s read as follows :*

$$\begin{aligned} f_1(X) = &\quad X^6 + 2\,(b_{11}^{25} + b_{11})\, b_{11}^{-5}\, X^2 \\ f_2(X) = &\quad b_{11}^5\, X^{11} + 4\, b_{11}^{25}\, X^7 + 2\,(b_{11}^{50} - b_{11}^2)\, b_{11}^{-5}\, X^3 + 2\,(c_6 - c_6^5)\, b_{11}^{-5}\, X \\ f_3(X) = &\quad 4\, b_{11}^{10}\, X^{16} + 4\, b_{11}^{30}\, X^{12} + c_{11}^5\, X^{11} + 4\, b_{11}^{50}\, X^8 + 4\, c_{11}^{25}\, X^7 + c_6^5\, X^6 \\ &\quad +4\,(b_{11}^{75} + b_{11}^3)\, b_{11}^{-5}\, X^4 + \{(b_{11}^{25} + b_{11})\, c_{11}\, b_{11}^{-5} + 2\,(b_{11}^{25} + b_{11})^2\, c_{11}^5\, b_{11}^{-10}\}\, X^3 \\ &\quad +2\,(c_6^5\, b_{11}^{25} + c_6\, b_{11})\, b_{11}^{-5}\, X^2 + c_1\, X \end{aligned}$$

where $b_{11} \in k - \{0\}$*,* $c_6 \in k$ *and* $c_1 \in k$ *are three algebraically independent parameters whereas* $c_{11} \in k$ *satisfies* $c_{11}^5 \in V$ *, i.e.*

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

In this case,

$$\begin{aligned} &V = Z(\mathrm{Ad}_{f_1}) = Z(X^{25} + 4\,(b_{11}^{125} + b_{11}^5)\, b_{11}^{-25}\, X^5 + X) \\ &\forall\, y \in V, \quad \ell_{1,2}(y) = \ell_{2,3}(y) = 2\,(b_{11}^5\, y^5 - b_{11}^{25}\, y) \\ &\forall\, y \in V, \quad \ell_{1,3}(y) = \tfrac{\ell_{1,2}(y)^2}{2!} + 2\,(c_{11}^5\, y^5 - c_{11}^{25}\, y) \end{aligned}$$

2. *The group* G *satisfies the following properties :*
   (a) *The group* G *has order* 5^5*, exponent* 5 *and* 5*-rank* 2.
   (b) *The center of* G *is cyclic of order* 5.
   (c) *The group* G *is nilpotent of maximal class* 4.
   (d) *Moreover,*

$$C_G(G') \supsetneq G' \quad \Leftrightarrow \quad C_G(G')/G' \simeq \mathbb{Z}/5\mathbb{Z} \quad \Leftrightarrow \quad (\frac{c_{11}}{b_{11}})^5 \in \mathbb{F}_5.$$

Proof :

1. Continue the work begun in the first point of Proposition 4.3.2 and consider the relation

$$\forall\, y \in V, \quad \Delta_y(f_3) = \ell_{1,3}(y)\, f_1(X) + \ell_{2,3}(y)\, f_2(X) \qquad \bmod\ \wp(k[X])$$

with

$$\begin{aligned} f_3(X) = &\quad c_{16}\, X^{1+3.5} + c_{12}\, X^{2+2.5} + c_8\, X^{3+5} + c_4\, X^4 + c_{11}^5\, X^{1+2.5} + c_7\, X^{2+5} \\ &\quad +c_3\, X^3 + c_6\, X^{1+5} + c_2\, X^2 + c_1\, X \quad \text{with} \quad c_16 \neq 0 \end{aligned}$$

Furthermore, following Proposition 3.5.4, one can assume that $\ell_{2,3} = \ell_{1,2}$.

2. The exponent is obtained by computation. The description of the center comes from Proposition 3.5.9. The nilpotency class of G derives from Proposition 3.5.14. To prove the last point, recall that $C_G(G') = \pi^{-1}(W)$ where

$$\begin{aligned} W &= \{y \in V,\, \phi(y) = id\} = \{y \in V,\, \ell_{1,2}(y) = \ell_{1,3}(y) = 0\} \\ &= \{y \in V,\, b_{11}^5\, y^5 - b_{11}^{25}\, y = 0\} \cap \{y \in V,\, c_{11}^5\, y^5 - c_{11}^{25}\, y = 0\} \subsetneq V \end{aligned}$$

As a consequence, W has dimension 1 over $\mathbb{F}_5$ if and only if the linear forms $b_{11}^5\, y^5 - b_{11}^{25}\, y$ and $c_{11}^5\, y^5 - c_{11}^{25}\, y$ are homothetic, i.e. $(\frac{c_{11}}{b_{11}})^5 = (\frac{c_{11}}{b_{11}})^{25}$. The claim follows. □

Remark 3.6.12. *Contrary to the previous case (see Proposition 4.3.2), there are two non isomorphic models for the group G according to whether $c_{11}^5\, b_{11}^{-5} \in \mathbb{F}_5$ or $c_{11}^5\, b_{11}^{-5} \notin \mathbb{F}_5$. But, still as in Proposition 4.3.2, the properties mentioned in the second point of Proposition 3.6.11 are sufficient to characterize each of these two models. Indeed, MAGMA shows that there exists only one group G, up to isomorphism, with order 5^5, exponent 5, 5-rank 2, a center of order 5 and such that $C_G(G') = G'$ (resp. $C_G(G') \supsetneq G'$) .*

Proposition 3.6.13. *Let (C, G) be a big action such that $G' \simeq (\mathbb{Z}/5\mathbb{Z})^4$. Assume that (C, G) satisfies the conditions of Theorem 3.5.8 with $s_1 = 1$.*

1. *Then there exists a coordinate X for the projective line $C/G' \simeq \mathbb{P}_1$ and an adapted basis for A such that the functions f_i's read as follows :*

$$\begin{aligned} f_1(X) = \;& X^6 + 2\,(b_{11}^{25} + b_{11})\, b_{11}^{-5}\, X^2 \\ f_2(X) = \;& b_{11}^5\, X^{11} + 4\, b_{11}^{25}\, X^7 + 2\,(b_{11}^{50} - b_{11}^2)\, b_{11}^{-5}\, X^3 + 2\,(c_6 - c_6^5)\, b_{11}^{-5}\, X \\ f_3(X) = \;& 4\, b_{11}^{10}\, X^{16} + 4\, b_{11}^{30}\, X^{12} + c_{11}^5\, X^{11} + 4\, b_{11}^{50}\, X^8 + 4\, c_{11}^{25}\, X^7 + c_6^5\, X^6 \\ & +4\,(b_{11}^{75} + b_{11}^3)\, b_{11}^{-5}\, X^4 + \{(b_{11}^{25} + b_{11})\, c_{11}\, b_{11}^{-5} + 2\,(b_{11}^{25} + b_{11})^2\, c_{11}^5\, b_{11}^{-10}\}\, X^3 \\ & +2\,(c_6^5\, b_{11}^{25} + c_6\, b_{11})\, b_{11}^{-5}\, X^2 + 2\,\{\,(d_{11} - d_{11}^5)\, b_{11}^{-5} + (c_6^5 - c_6)\, c_{11}^5\, b_{11}^{-10}\}\, X \\ f_4(X) = \;& 2\, b_{11}^{15} X^{21} + b_{11}^{35}\, X^{17} + 3\, b_{11}^5\, c_{11}^5\, X^{16} + 4\, b_{11}^{55}\, X^{13} + 4\,(b_{11}^{25}\, c_{11}^5 + b_{11}^5\, c_{11}^{25})\, X^{12} \\ & +d_{11}^5\, b_{11}^5 X^{11} + 3\, b_{11}^{75}\, X^9 + 3\, b_{11}^{25}\, c_{11}^{25}\, X^8 + (4\, d_{11}^{25}\, b_{11}^{25} + (c_6^{25} - c_6^5)\, b_{11}^{25})\, X^7 \\ & +d_6^5\, X^6 + \{2\, d_{11}^5\, (b_{11}^{50} - b_{11}^2)\, b_{11}^{-5} + (c_6^5 - c_6 + d_{11} - d_{11}^5)\, (b_{11}^{25} + b_{11})\, b_{11}^{-4} \\ & +2\,(c_6^5 - c_6)\, b_{11}^{-3}\}\, X^3 + \{2\,(d_{11}^5\, b_{11}^{25} + d_{11}\, b_{11})\, b_{11}^{-5} \\ & +2\,(c_6^5 - c_6)\,(b_{11}\, c_{11}^5 - b_{11}^5\, c_{11})\, b_{11}^{-10}\}\, X^2 + d_1\, X \end{aligned}$$

where $c_6 \in k$ and d_1 in k are two algebraically independent parameters, $b_{11} \in k^\times$ sastisfies $\frac{b_{11}^{25}}{b_{11}} \in \mathbb{F}_5^\times$, $c_{11} \in k$ satisfies $c_{11}^5 \in V$, i.e.

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

and $d_{11} \in k$ satisfies

$$b_{11}^{25}\,(d_{11} - c_6)^{25} + 4\,(b_{11}^{25} + b_{11})\,(d_{11} - c_6)^5 + b_{11}\,(d_{11} - c_6) = 0.$$

In this case,

$$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{25} + 4\,(b_{11}^{125} + b_{11}^5)\, b_{11}^{-25}\, X^5 + X)$$

and, for all y in V,

$$\begin{aligned} &\ell_{1,2}(y) = \ell_{2,3}(y) = \ell_{3,4}(y) = 2\,(b_{11}^5\, y^5 - b_{11}^{25}\, y) \\ &\ell_{1,3}(y) = \ell_{2,4}(y) = \tfrac{\ell_{1,2}(y)^2}{2!} + 2\,(c_{11}^5\, y^5 - c_{11}^{25}\, y) \\ &\ell_{1,4}(y) = \tfrac{\ell_{1,2}(y)^3}{3\,!} + \ell_{1,2}(y)\,(\ell_{1,3}(y) - \tfrac{\ell_{1,2}(y)^2}{2!}) + 2\,(d_{11}^5 - c_6^5)\, b_{11}^5\, y^5 - 2\,(d_{11}^{25} - c_6^{25})\, b_{11}^{25}\, y \end{aligned}$$

2. *The group G satisfies the following properties :*

(a) The group G has order 5^6, exponent 5^2 and 5-rank 2.

(b) The center of G is cyclic of order 5.

(c) The group G is nilpotent of maximal class 5.

(d) Moreover,

$$C_G(G') \supsetneq G' \quad \Leftrightarrow \quad C_G(G')/G' \simeq \mathbb{Z}/5\mathbb{Z} \quad \Leftrightarrow \quad (\frac{c_{11}}{b_{11}})^5 \in \mathbb{F}_5 \quad \textit{and} \quad (d_{11}^5 - c_6^5) \in \mathbb{F}_5.$$

Proof :

1. Continue the work begun in the two preceding proofs.
2. The exponent is obtained via calculation. The description of the center derives from Proposition 3.5.9. The nilpotency class of G derives from Proposition 3.5.14. The last property is obtained in the same way as in the last point of Proposition 3.6.11. □

Remark 3.6.14. *Contrary to the previous cases, the properties listed in the second point of Proposition 3.6.13 are not sufficient to characterize the group G. Indeed, MAGMA gives 39 models for a group G satisfying (a) and (b).*

We conclude with the following

Problems :

1. For any p, find equations for the universal family (at least for $s_1 = 1$) as we obtained for the special family.
2. Compare the universal family corresponding to a given s_1 with the one obtained after a base change by a generic and additive polynomial map, applied to the universal family with $s_1 = 1$. As shown in Chapter 4 (Rmk. 4.5.7), the universal family is generally larger.

A last interesting question is raised by the following

Remark 3.6.15. *The last three propositions seem to suggest that any p-cyclic étale cover of the affine line given by*

$$W_1^p - W_1 = f_1(X) := X\,S(X) \quad \textit{with} \quad S \in k\{F\}$$

could be embedded in a big action (C, G) where C is parametrized by n Artin-Schreier equations :

$$W_i^p - W_i = f_i(X) \in \Sigma_{i+1} - \Sigma_i \quad \textit{with} \quad 1 \le i \le n < p-1$$

and that without any restriction on the coefficients of f_1. Nevertheless, it is no more true for $n = p-1$ unless the coefficients of $S(X)$ satisfy a specific algebraic condition to be determined (see e.g. $\frac{b_{11}^{25}}{b_{11}} \in \mathbb{F}_5$ in Proposition 3.6.13).

Chapitre 4

Large p-group actions with $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

4.1 Introduction.

Setting. Let k be an algebraically closed field of positive characteristic $p > 0$ and C a connected nonsingular projective curve over k, with genus $g \geq 2$. As in characteristic zero, the k-automorphism group of the curve C, $\mathrm{Aut}_k(C)$, is a finite group whose order is bounded from above by a polynomial in g (cf. [St73] and [Sin74]). But, contrary to the case of characteristic zero, the bound is no more linear but biquadratic, namely : $|\mathrm{Aut}_k(C)| \leq 16\, g^4$, except for the Hermitian curves : $W^q + W = X^{1+q}$, with $q = p^n$ (cf. [St73]). The difference is due to the appearance of wild ramification. More precisely, let G be a subgroup of $\mathrm{Aut}_k(C)$. If the order of G is prime to p, then the Hurwitz bound still holds, i.e. $|G| \leq 84\,(g-1)$. Now, if G is a p-Sylow subgroup of $\mathrm{Aut}_k(C)$, Nakajima (cf. [Na87a]) proves that $|G|$ can be larger according to the value of the p-rank γ of the curve C. Indeed, if $\gamma > 0$, then $|G| \leq \frac{2\,p}{p-1}\, g$, whereas for $\gamma = 0$, $|G| \leq \max\{g, \frac{4\,p}{(p-1)^2}\, g^2\}$, knowing that the quadratic upper bound $\frac{4\,p}{(p-1)^2}\, g^2$ can really be attained. Following Nakajima's work, Lehr and Matignon explore the *big actions*, that is to say the pairs (C, G) where G is a p-subgroup of $\mathrm{Aut}_k(C)$ such that $|G| > \frac{2\,p}{p-1}\, g$ (see [LM05]). In this case, the ramification locus of the cover $\pi : C \to C/G$ is located at one point of C, say ∞. In Chapter 2, we displayed necessary conditions on G_2, the second ramification group of G at ∞ in lower notation, for (C, G) to be a big action. In particular, we showed that G_2 coincides with the derived subgroup G' of G.

Motivation and purpose. The aim of this chapter is to pursue the classification of big actions as initiated in [LM05]. Indeed, when searching for a classification of big actions, it naturally occurs that the quotient $\frac{|G|}{g^2}$ has a *sieve* effect. Lehr and Matignon first prove that the big actions such that $\frac{|G|}{g^2} \geq \frac{4}{(p-1)^2}$ correspond to the p-cyclic étale covers of the affine line parametrized by an Artin-Schreier equation : $W^p - W = f(X) := X\,S(X) + c\,X \in k[X]$, where $S(X)$ runs over the additive polynomials of $k[X]$. In Chapter 2, we showed that the big actions satisfying $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$ correspond to the étale covers of the affine line with Galois group $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \leq 3$. This motivated the study of big actions with a p-elementary abelian G', say $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, which is the main topic of Chapter 3 where we generalized the structure theorem obtained in the p-cyclic case. Namely, we proved that when $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$ with $n \geq 1$, then the function field of the curve is parametrized by n Artin Schreier equations : $W_i^p - W_i = f_i(X) \in k[X]$ where each function f_i can be written as a linear combination over k of products of at most $i+1$ additive polynomials. In this chapter, we display the parametrization of the functions f_i's in the case of the big actions satisfying $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$. In what follows, this condition is called condition $(*)$.

Outline ot the chapter. The chapter falls into two main parts. The first one is focused on finiteness results for big actions (C, G) satisfying $\frac{|G|}{g^2} \geq M$ for a given positive real $M > 0$, called big actions satisfying $\mathcal{G}_M$, whereas the second part is dedicated to the classification of such big actions when $M = \frac{4}{(p^2-1)^2}$. More precisely, we prove in Section 4.4 that, for a given $M > 0$, the order of G' only takes a finite number of values for (C, G) a big action satisfying $\mathcal{G}_M$. When exploring similar finiteness results for g and $|G|$, we are lead to a purely group-theoretic discussion around the inclusion $\mathrm{Fratt}(G') \subset [G', G]$, where $\mathrm{Fratt}(G')$ means the Frattini subgroup of G' and $[G', G]$ denotes the commutator subgroup of G' and G (cf. Section 4.4). When the inclusion is strict, $|G|$ and g also take a finite number of values for (C, G) satisfying $\mathcal{G}_M$. This is no more true when $\mathrm{Fratt}(G') = [G', G]$. In this case, we can only conclude that, for $p > 2$, the quotient $\frac{|G|}{g^2}$ takes a finite number of values for (C, G) satisfying $\mathcal{G}_M$ with an abelian G'. Note that we do not know yet examples of big actions with a nonabelian G'. Another central question is the link between the subgroups G of $\mathrm{Aut}_k(C)$ such that (C, G) is a big action and a p-Sylow subgroup of $\mathrm{Aut}_k(C)$ containing G (Section 4.3). Among other things, we prove that they have the same derived subgroup. This, together with the fact that the order of G' takes a finite number of values for big actions satisfying $\mathcal{G}_M$, implies, on the one hand, that the order of G' is a key criterion to classify big actions and, on the other hand, that we can concentrate on p-Sylow subgroups of $\mathrm{Aut}_k(C)$. In Section 4.5, we eventually display the classification and the parametrization of big actions (C, G) under condition $(*)$ according to the order of G'. Pursuing the preceding discussion, we have to distinguish the cases $[G', G] = \mathrm{Fratt}(G')(= \{e\})$ and $[G', G] \supsetneq \mathrm{Fratt}(G')(= \{e\})$.

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, $P(\alpha + \beta) = P(\alpha) + P(\beta)$. Moreover, a separable polynomial is additive if and only if the set of its roots is a subgroup of k (see [Go96] chap. 1).

Let $f(X)$ be a polynomial of $k[X]$. Then, there is a unique polynomial $\mathrm{red}(f)(X)$ in $k[X]$, called the reduced representative of f, which is p-power free, i.e. $\mathrm{red}(f)(X) \in \bigoplus_{(i,p)=1} k\,X^i$, 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 $\mathrm{Spec}\,k[X]$ corresponds to a curve C_f where f is a polynomial of $k[X]$ (see [Mi80] III.4.12, p. 127). By Artin-Schreier theory, the covers C_f and $C_{\mathrm{red}(f)}$ 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 denotes a connected nonsingular projective curve over k, with genus $g \geq 2$. We denote by $A := \mathrm{Aut}_k C$ the k-automorphism group of the curve C and by $S(A)_p$ any p-Sylow subgroup of A. For any point $P \in C$ and any $i \geq -1$, we denote by $A_{P,i}$ the i-th ramification group of A at P in lower notation, namely

$$A_{P,i} := \{\sigma \in A,\, v_P(\sigma(t_P) - t_P) \geq i + 1\},$$

where t_P denotes a uniformizing parameter at P and v_P means the order function at P.

4.2 The setting : generalities about big actions.

Definition 4.2.1. *Let C be a connected nonsingular projective curve over k, with genus $g \geq 2$. Let G be a subgroup of A. We say that the pair (C, G) is a big action if G is a finite p-group such that*

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

To pinpoint the background of this work, we first recall basic properties of big actions established in [LM05] and Chapter 2.

Recall 4.2.2. *Assume that (C, G) is a big action. 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 ∞ :*

$$G_i := \{\sigma \in G,\, v_\infty(\sigma(t_\infty) - t_\infty) \geq i + 1\},$$

where t_∞ denotes a uniformizing parameter at ∞ and v_∞ means the order function at ∞.

1. *Then, G_2 is non trivial and it is strictly included in G_1.*
2. *The quotient curve C/G_2 is isomorphic to the projective line $\mathbb{P}^1_k$.*
3. *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 $X \to X + y$, 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. This gives the following exact sequence :*

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

where

$$\pi : \left\{ \begin{array}{l} G \to V \\ g \to g(X) - X. \end{array} \right.$$

4. *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_2/H.*

Recall 4.2.3. *(Chapter 2- Thm. 2.2.6.4). Let (C, G) be a big action. Then,*

$$G_2 = G' = \mathrm{Fratt}(G),$$

where G' means the commutator subgroup of G and $\mathrm{Fratt}(G) = G'G^p$ the Frattini subgroup of G.

To conclude this first section, we introduce new definitions used in our future classification.

Definition 4.2.4. *Let C be a connected nonsingular projective curve over k, with genus $g \geq 2$. Let G be a subgroup of A. Let $M > 0$ be a positive real. We say that :*

1. *G satisfies $\mathcal{G}(C)$ (or (C, G) satisfies $\mathcal{G}$) if (C, G) is a big action.*
2. *G satisfies $\mathcal{G}_M(C)$ (or (C, G) satisfies $\mathcal{G}_M$) if (C, G) is a big action with $\frac{|G|}{g^2} \geq M$.*
3. *If (C, G) satisfies $\mathcal{G}_M$ with $M = \frac{4}{(p^2-1)^2}$, we say that (C, G) satisfies condition $(*)$.*

Remark 4.2.5. *There exists big actions (C, G) satisfying $\mathcal{G}_M$ if and only if $M \leq \frac{4\,p}{(p-1)^2}$ (see [St73]).*

4.3 A study on p-Sylow subgroups of $\mathrm{Aut}_k(C)$ inducing big actions.

In this section, we more specifically concentrate on the p-Sylow subgroup(s) of A satisfying $\mathcal{G}(C)$ (resp. $\mathcal{G}_M(C)$).

Remark 4.3.1. *Let C be a connected nonsingular projective curve over k, with genus $g \geq 2$. Assume that there exists a subgroup $G \subset A$ satisfying $\mathcal{G}(C)$.*

1. *Then, every p-Sylow subgroup of A satisfies $\mathcal{G}(C)$.*
2. *Moreover, A has a unique p-Sylow subgroup except in the three following cases (cf. [Han92] and [GK07]) :*

   (a) *The Hermitian curve*

   $$C_H : \quad W^q + W = X^{1+q}$$

   with $p \geq 2$, $q = p^s$, $s \geq 1$. Then, $g = \frac{1}{2}\,(q^2 - q)$ and $A \simeq \mathrm{PGU}_3(\mathbb{F}_{,q^2})$ (cf. [Leo96]). It follows that $|A| = q^3\,(q^2-1)\,(q^3+1)$, so $\frac{|S(A)_p|}{g} = \frac{2q^2}{q-1} > \frac{2\,p}{p-1}$ and $\frac{|S(A)_p|}{g^2} = \frac{4\,q}{(q-1)^2}$, where $S(A)_p$ denotes any p-Sylow subgroup of A. Thus, $(C_H, S(A)_p)$ is a big action with $G' = G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^s$. It satisfies condition $(*)$ if and only if $1 \leq s \leq 3$.

   (b) *The Deligne-Lusztig curve arising from the Suzuki group*

   $$C_S : \quad W^q + W = X^{q_0}\,(X^q + X)$$

   with $p = 2$, $q_0 = 2^s$, $s \geq 1$ and $q = 2^{2s+1}$. In this case, $g = q_0(q-1)$ and $A \simeq Sz(q)$ is the Suzuki group. It follows that $|A| = q^2\,(q-1)\,(q^2+1)$, so $\frac{|S(A)_p|}{g} = \frac{q^2}{q_0(q-1)} > \frac{2\,p}{p-1}$ and $\frac{|S(A)_p|}{g^2} = \frac{q^2}{q_0^2\,(q-1)^2} < \frac{4}{(p^2-1)^2}$, for all $s \geq 1$. Thus, $(C_S, S(A)_p)$ is a big action with $G' = G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^{2s+1}$ but it never satisfies condition $(*)$.

   (c) *The Deligne-Lusztig curve arising from the Ree group*

   $$C_R : \quad W_1^q - W_1 = X^{q_0}\,(X^q + X) \quad \text{and} \quad W_2^q - W_2 = X^{2q_0}\,(X^q + X)$$

   with $p = 3$, $q_0 = 3^s$, $s \geq 1$ and $q = 3^{2s+1}$. Then, $g = \frac{3}{2}\,q_0\,(q-1)\,(q+q_0+1)$ and $A \simeq Ree(q)$ is the Ree group. It follows that $|A| = q^3\,(q-1)\,(q^3+1)$, so $\frac{|S(A)_p|}{g} = \frac{2q^3}{3q_0(q-1)(q+q_0+1)} > \frac{2\,p}{p-1}$ and $\frac{|S(A)_p|}{g^2} = \frac{4q^3}{9q_0^2(q-1)^2(q+q_0+1)^2} < \frac{4}{(p^2-1)^2}$ for all $s \geq 1$. Thus, $(C_R, S(A)_p))$ is a big action with $G' = G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^{2(2s+1)}$ but it never satisfies condition $(*)$.

   In each of these three cases, the group A is simple, so it has more than one p-Sylow subgroups.

Now, fix C a connected nonsingular projective curve over k, with genus $g \geq 2$. We highlight the link between the groups G satisfying $\mathcal{G}(C)$ (resp. $\mathcal{G}_M(C)$) and the p-Sylow subgroup(s) of A.

Proposition 4.3.2. *Let C be a connected nonsingular projective curve over k, with genus $g \geq 2$.*

1. *Let G be a group satisfying $\mathcal{G}(C)$.*
   - (a) *Then, there exists a point of C, say ∞, such that G is included in $A_{\infty,1}$. For all $i \geq 0$, we denote by G_i the i-th ramification group of G at ∞ in lower notation. Then, $A_{\infty,1}$ satisfies $\mathcal{G}(C)$ and $A_{\infty,2} = G_2$, i.e. $(A_{\infty,1})' = G'$. Thus, we obtain the following diagram :*

$$\begin{tikzcd}
0 \arrow[r] & A_{\infty,2} \arrow[r] \arrow[d, equal] & A_{\infty,1} \arrow[r, "\pi"] \arrow[d, phantom, "\cup"] & W \subset k \arrow[r] \arrow[d, phantom, "\cup"] & 0 \\
0 \arrow[r] & G_2 \arrow[r] & G = G_1 \arrow[r, "\pi"] & V \arrow[r] & 0
\end{tikzcd}$$

   In particular, $G = \pi^{-1}(V)$ where V is an $\mathbb{F}_p$-vector subspace of W.
   - (b) *$A_{\infty,1}$ is a p-Sylow subgroup of A. Moreover, except in the three special cases mentionned in Remark 4.3.1, $A_{\infty,1}$ is the unique p-Sylow subgroup of A.*
   - (c) *Let M be a positive real such that G satisfies $\mathcal{G}_M(C)$. Then, $A_{\infty,1}$ also satifies $\mathcal{G}_M(C)$.*
2. *Conversely, let ∞ be a point of the curve C such that $A_{\infty,1}$ satisfies $\mathcal{G}(C)$. Consider V an $\mathbb{F}_p$-vector space of W, defined as above, and put $G := \pi^{-1}(V)$.*
   - (a) *Then, the group G satisfies $\mathcal{G}(C)$ if and only if*

$$|W| \geq |V| > \frac{2p}{p-1} \frac{g}{|A_{\infty,2}|}.$$

   - (b) *Let M be a positive real such that $A_{\infty,1}$ satisfies $\mathcal{G}_M(C)$. Then, G satisfies $\mathcal{G}_M(C)$ if and only if*

$$|W| \geq |V| \geq M \frac{g^2}{|A_{\infty,2}|}.$$

Proof : The first assertion (1.a) derives from [LM05] (Prop 8.5) and Chapter 2 (Cor. 2.2.10). The second point (1.b) comes from Chapter 2 (Rem 2.2.11) together with Remark 4.3.1. The other claims are obtained via calculation. □

Remark 4.3.3. *Except in the three special cases mentionned in Remark 4.3.1, the point ∞ of C defined in Proposition 4.3.2 is uniquely determined. In particular, except for the three special cases, if P is a point of C such that $A_{P,1}$ satisfies $\mathcal{G}(C)$, then $P = \infty$.*

To sum up, if G satisfyies $\mathcal{G}(C)$ (resp. $\mathcal{G}_M(C)$) and if $A_{\infty,1}$ is a (actually "the", in most cases) p-Sylow subgroup of A containing G, then $A_{\infty,1}$ also satisfies $\mathcal{G}(C)$ (resp. $\mathcal{G}_M(C)$) and has the same derived subgroup. So, in our attempt to classify the big actions (C, G) satisfying $\mathcal{G}_M$, this leads us to focus on the derived subgroup G' of G.

4.4 Finiteness results for big actions satisfying $\mathcal{G}_M$.

4.4.1 An upper bound on $|G'|$.

Lemma 4.4.1. *Let $M > 0$ be a positive real such that (C, G) is a big action satisfying $\mathcal{G}_M$. Then, the order of G' is bounded as follows :*

$$p \leq |G'| \leq \frac{4p}{(p-1)^2} \frac{2 + M + 2\sqrt{1+M}}{M^2}.$$

Thus, $|G'|$ only takes a finite number of values for (C, G) a big action satisfying $\mathcal{G}_M$.

Proof : We first recall that $G' = G_2$ is a nontrivial p-group (see e.g. [LM05] Prop. 8.5). Now, let $i_0 \geq 2$ be the integer such that the lower ramification filtration of G at ∞ reads :

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

Put $|G_2/G_{i_0+1}| = p^m$, with $m \geq 1$, and $\mathcal{B}_m := \frac{4}{M} \frac{|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2} = \frac{4}{M} \frac{p^m}{(p^m-1)^2}$. By [LM05] (Thm. 8.6), $M \leq \frac{|G|}{g^2}$ implies $1 < |G_2| \leq \frac{4}{M} \frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}|-1)^2} = p^m \, \mathcal{B}_m$. From $|G_2| = p^m |G_{i_0+1}|$, we infer $1 \leq |G_{i_0+1}| \leq \mathcal{B}_m$. Since $(\mathcal{B}_m)_{m \geq 1}$ is a decreasing sequence which tends to 0 as m grows large, we conclude that m is bounded.

More precisely, $m < m_0$ where m_0 is the smallest integer such that $\mathcal{B}_{m_0} < 1$. As $M \leq \frac{4\,p}{(p-1)^2} \leq 8$ (see Remark 4.2.5), computation shows that $\mathcal{B}_m < 1 \Leftrightarrow p^m > \phi(M) := \frac{2+M+2\,\sqrt{1+M}}{M}$. As $(\mathcal{B}_m)_{m \geq 1}$ is decreasing,

$$|G_2| \leq p^m\,\mathcal{B}_m \leq \phi(M)\,\mathcal{B}_1 = \frac{\phi(M)}{M}\,\frac{4\,p}{(p-1)^2}.$$

The claim follows. □

Next we deduce that, for big actions (C, G) satisfying $\mathcal{G}_M$, an upper bound on $|V|$ induces an upper bound on the genus g of C.

Corollary 4.4.2. *Let $M > 0$ be a positive real such that (C, G) is a big action satisfying $\mathcal{G}_M$. Then,*

$$g < |G'|\,|V|\,\frac{p-1}{2\,p} \leq \frac{2}{p-1}\,\frac{2+M+2\sqrt{1+M}}{M^2}\,|V|.$$

This raises the following question. Let (C, G) be a big action satisfying $\mathcal{G}_M$; in which cases is $|V|$ (and then g) bounded from above ? In other words, in which cases, does the quotient $\frac{|G|}{g}$ take a finite number of values when (C, G) satisfy $\mathcal{G}_M$? We begin with preliminary results on big actions leading to a purely group-theoretic discussion leading to compare the Frattini subgroup of G' with the commutator subgroup of G' and G.

4.4.2 Preliminaries to a group-theoretic discussion.

Lemma 4.4.3. *Let (C, G) be a big action. If $G' \subset Z(G)$, then $G'(= G_2)$ is p-elementary abelian, say $G' \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$. In this case, the function field $L = k(C)$ is parametrized by n equations :*

$$\forall\, i \in \{1, \ldots, n\}, \quad W_i^p - W_i = f_i(X) = X\,S_i(X) + c_i\,X \in k[X],$$

where S_i is an additive polynomial of $k[X]$ with degree $s_i \geq 1$ in F and $s_1 \leq s_2 \ldots \leq s_n$. Moreover, $V \subset \cap_{1 \leq i \leq n} Z(\mathrm{Ad}_{f_i})$ where Ad_{f_i} denotes the palindromic polynomial related to f_i as defined in Chapter 3 (Prop. 3.2.13)

Proof : The hypothesis first requires $G' = G_2$ to be abelian. Now, assume that G_2 has exponent strictly greater than p. Then, there exists a surjective map $\phi : G_2 \to \mathbb{Z}/p^2\mathbb{Z}$. So $H := \mathrm{Ker}\phi \subsetneq G_2 \subset Z(G)$ is a normal subgroup of G. It follows from Chapter 2 (Lemma 2.2.4) that the pair $(C/H, G/H)$ is a big action with second ramification group $(G/H)_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$. This contradicts Chapter 2 (Thm. 2.5.1). The last part of the lemma comes from Chapter 3 (Prop. 3.2.13). □

Corollary 4.4.4. *Let (C, G) be a big action. Let $H := [G', G]$ be the commutator subgroup of G' and G.*

1. *Then, H is trivial if and only if $G' \subset Z(G)$.*
2. *The group H is strictly included in G'.*
3. *The pair $(C/H, G/H)$ is a big action. Moreover, its second ramification group $(G/H)_2 = (G/H)' = G_2/H \subset Z(G/H)$ is p-elementary abelian.*

Proof :

1. The first assertion is clear.
2. As G' is normal in G, then $H \subset G'$. Assume that $G' = H$. Then, the lower central series of G is stationnary, which contradicts the fact that the p-group G is nilpotent (see e.g. [Su86] Chap.4). So $H \subsetneq G'$.
3. As $H \subsetneq G' = G_2$ is normal in G, it follows from Chapter 2 (Lemma 2.2.4 and Thm. 2.2.6) that the pair $(C/H, G/H)$ is a big action with second ramification group $(G/H)_2 = G_2/H$. From $H = [G_2, G]$, we gather that $G_2/H \subset Z(G/H)$. Therefore, we deduce from Lemma 4.4.3 that $(G/H)_2$ is p-elementary abelian. □

Corollary 4.4.5. *Let (C, G) be a big action. Let $F := \mathrm{Fratt}(G')$ be the Frattini subgroup of G'.*

1. *Then, F is trivial if and only if G' is an elementary abelian p-group.*
2. *We have the following inclusions : $F \subset [G', G] \subsetneq G'$.*
3. *The pair $(C/F, G/F)$ is a big action. Moreover, its second ramification group $(G/F)_2 = (G/F)' = G_2/F$ is p-elementary abelian.*
4. *Let M be a positive real. If (C, G) satisfies $\mathcal{G}_M$, then $(C/F, G/F)$ also satisfies $\mathcal{G}_M$.*

Proof :

1. As G' is a p-group, $F = (G')'(G')^p$, where $(G')'$ means the derived subgroup of G' and $(G')^p$ the subgroup generated by the p powers of elements of G' (cf. [LGM02] Prop. 1.2.4). This proves that if G' is p-elementary abelian, then F is trivial. The converse derives from the fact that G'/F is p-elementary abelian (cf. [LGM02] Prop. 1.2.4).
2. Using Corollary 4.4.4, the only inclusion that remains to show is $F \subset [G', G]$. From $[G', G'] \subset [G', G]$, we deduce that $G'/[G', G]$ is abelian. So, $(G')' \subset [G', G]$. Besides, as $G'/[G', G]$ has exponent p, $(G')^p \subset [G', G]$. The claim follows.
3. Since $F \subsetneq G' = G_2$ is normal in G, we deduce from Chapter 2 (Lemma 2.2.4) that the pair $(C/F, G/F)$ is a big action with second ramification group : $(G/F)_2 = G_2/F = (G/F)'$. Furthermore, as G_2 is a p-group, G_2/F is an elementary abelian p-group (see above).
4. This derives from [LM05] (Prop. 8.5 (ii)). □

This leads us to discuss according to whether $\mathrm{Fratt}(G') \subsetneq [G', G]$ or $\mathrm{Fratt}(G') = [G', G]$. We shall start with the special case $\{e\} = \mathrm{Fratt}(G') \subsetneq [G', G]$, i.e. G' is p-elementary abelian and $G' \not\subset Z(G)$ (see Cor. 4.4.1). Before exploring this case, we need to recall some results on big actions with a p-elementary abelian G'.

4.4.3 Preliminaries : big actions with a p-elementary abelian $G'(= G_2)$.

In this section, we fix the notations used throughout this section and recall some necessary results on big actions with a p-elementary abelian G_2 that have been obtained in Chapter 3.

Recall 4.4.6. *Let (C, G) be a big action such that $G'(= G_2) \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$. Write the exact sequence :*

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

1. *We denote by L be the function field of the curve C and by $k(X) := L^{G_2}$ the subfield of L fixed by G_2. Then, the extension $L/k(X)$ can be parametrized by n Artin-Schreier equations : $W_i^p - W_i = f_i(X) \in k[X]$ with $1 \leq i \leq n$. Following Chapter 3 (Def. 3.2.3), one can choose an "adapted basis" $\{f_1(X), \ldots, f_n(X)\}$ with some specific properties :*
   (a) *For all $i \in \{1, \ldots, n\}$, each function f_i is assumed to be reduced mod $\wp(k[X])$*
   (b) *For all $i \in \{1, \ldots, n\}$, put $m_i := \deg f_i$. Then, $m_1 \leq m_2 \leq \ldots \leq m_n$.*
   (c) *$\forall\ (\lambda_1, \ldots \lambda_n) \in \mathbb{F}_p^n$ not all zeros,*
   $$\deg\,(\sum_{i=1}^{n} \lambda_i\, f_i(X)) = \max_{i \in \{1,\ldots,n\}} \{\deg\, \lambda_i\, f_i(X)\}.$$
   In this case, the genus of the curve C is given by the following formula (cf. Chapter 3- Cor. 3.2.7) :
   $$g = \frac{p-1}{2} \sum_{i=1}^{n} p^{i-1}\,(m_i - 1). \tag{4.1}$$
2. *Now, consider the $\mathbb{F}_p$-vector subspace of $k[X]$ generated by the classes of $\{f_1(X), \ldots, f_n(X)\}$ mod $\wp(k[X])$:*
   $$A := \frac{\wp(L) \cap k[X]}{\wp(k[X])}.$$
   Recall that A is isomorphic to the dual of G_2 with respect to the Artin-Schreier pairing (cf. Chapter 3- Section 3.2.1). As seen in Chapter 3 (Section 3.2.2), V acts on G_2 via conjugation. This induces a representation $\phi : V \to \mathrm{Aut}(G_2)$. The representation $\rho : V \to \mathrm{Aut}(A)$, which is dual with respect to the Artin-Schreier pairing, expresses the action of V on A by translation. More precisely, for all y in V, the automorphism $\rho(y)$ is defined as follows :
   $$\rho(y) : \begin{cases} A \to A \\ \overline{f(X)} \to \overline{f(X+y)} \end{cases}$$
   where $\overline{f(X)}$ means the class in A of $f(X) \in k[X]$ For all y in V, the matrix of the automorphism $\rho(y)$ in the adapted basis fixed for A is an upper triangular matrix of $\mathrm{GL}_n(\mathbb{F}_p)$ with identity on the diagonal,

namely

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

where, for all i in $\{1, \dots, n-1\}$, $\ell_{i,i+1}$ is a nonzero linear form from V to $\mathbb{F}_p$ (see Chapter 3 Section 3.2.4). In other words,

$$\forall\, y \in V,\ f_1(X+y) - f_1(X) = 0 \quad \mod \wp(k[X]).$$

$$\forall\, i \in \{2, \dots, n\},\ \forall\, y \in V,\ f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y)\, f_j(X) \qquad \mod \wp(k[X]). \tag{4.2}$$

For all map ℓ, we write $\ell = 0$ if ℓ is identically zero and $\ell \neq 0$ otherwise.

3. *The case of a trivial representation can be characterized by the equivalent assertions (see Chapter 3-Prop. 3.2.13) :*

   (a) *The representation ρ is trivial, i.e.*

   $$\forall\, i \in \{1, \dots, n\}, \quad \forall\, y \in V, \quad f_i(X+y) - f_i(X) = 0 \mod \wp(k[X]).$$

   (b) *The commutator subgroup of G' and G is trivial, i.e. $G' \subset Z(G)$.*

   (c) *For all i in $\{1, \dots, n\}$, $f_i(X) = X\, S_i(X) + c_i\, X \in k[X]$ where each $S_i \in k\{F\}$ is an additive polynomial with degree $s_i \geq 1$ in F. So, write $S_i(F) = \sum_{j=0}^{s_i} a_{i,j}\, F^j$ with $a_{i,s_i} \neq 0$. Then, one defines an additive polynomial related to f_i, called the "palindromic polynomial" of f_i :*

   $$\mathrm{Ad}_{f_i} := \frac{1}{a_{i,s_i}^{p^{s_i}}}\, F^{s_i} (\sum_{j=0}^{s_i} a_{i,j}\, F^j + F^{-j}\, a_{i,j}).$$

   In this case,

   $$V \subset \bigcap_{i=1}^{n} Z(\mathrm{Ad}_{f_i}).$$

   Since, under condition $(*)$, G' is p-elementary abelian, we deduce from point (b) that the case of a trivial representation corresponds to the case $\{e\} = \mathrm{Fratt}(G') = [G', G]$.

4. *To conclude, we recall that for all $t \geq 1$, Σ_t means the k-vector subspace of $k[X]$ generated by 1 and the products of at most t additive polynomials of $k[X]$ (cf. Chapter 3 Def. 3.3.1). As proved in Chapter 3 (Thm. 3.3.13), for all i in $\{1, \dots, n\}$, f_i lies in Σ_{i+1}.*

4.4.4 Case : $\mathrm{Fratt}(G') \subsetneq [G', G]$.

Proposition 4.4.7. *Let $M > 0$ be a positive real such that (C, G) is a big action satisfying $\mathcal{G}_M$. Suppose that $\{e\} = \mathrm{Fratt}(G') \subsetneq [G', G]$. Then, $|V|$ and g are bounded as follows :*

$$|V| \leq \frac{4}{M} \frac{|G_2|}{(p-1)^2} \leq \frac{16\, p}{(p-1)^4}\, \frac{2 + M + 2\sqrt{1+M}}{M^3} \tag{4.3}$$

and

$$\frac{p-1}{2}\, |V| \leq g < \frac{32\, p}{(p-1)^5}\, \frac{(2 + M + 2\sqrt{1+M})^2}{M^5}. \tag{4.4}$$

Thus, under these conditions, g, $|V|$ and so the quotient $\frac{|G|}{g}$ only take a finite number of values.

Proof : Write $G' = G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$. As $G_2 \not\subset Z(G)$, Chapter 3 (Prop. 3.2.13) ensures the existence of a smaller integer $j_0 \geq 1$ such that $f_{j_0+1}(X)$ cannot be written as $c\,X + X S(X)$, with S in $k\{F\}$. If $j_0 \geq 2$, it follows that, for all y in V, the coefficients of the matrix $L(y)$ satisfy $\ell_{j,i}(y) = 0$ for all $2 \leq i \leq j_0$ and $1 \leq j \leq i-1$. Moreover, the matricial multiplication proves that, for all i in $\{1, \dots, j_0\}$, the functions ℓ_{i,j_0+1} are nonzero linear forms from V to $\mathbb{F}_p$. Put $\mathcal{W} := \bigcap_{1 \leq i \leq j_0} \mathrm{Ker}\, \ell_{i,j_0+1}$. Thus, $\mathcal{W}$ is the intersection of j_0 hyperplanes of V. As a consequence, $\dim_k \mathcal{W} \geq \dim_k V - j_0$, which gives :

$$|\mathcal{W}| \geq \frac{|V|}{p^{j_0}}. \tag{4.5}$$

Let $C_{f_{j_0+1}}$ be the curve parametrized by $W^p - W = f_{j_0+1}(X)$. It defines an étale cover of the affine line with group $\Gamma_0 \simeq \mathbb{Z}/p\mathbb{Z}$. Since, for all y in $\mathcal{W}$, $f_{i_0+1}(X+y) = f_{i_0+1}(X) \bmod \wp(k[X])$, the group of translations of the affine line : $\{X \to X+y,\, y \in \mathcal{W}\}$ can be extended to a p-group of automorphisms of the curve $C_{f_{j_0+1}}$, say Γ, with the following exact sequence :

$$0 \longrightarrow \Gamma_0 \simeq \mathbb{Z}/p\,\mathbb{Z} \longrightarrow \Gamma \longrightarrow \mathcal{W} \longrightarrow 0.$$

The pair $(C_{f_{j_0+1}}, \Gamma)$ is not a big action. Otherwise, its second ramification group would be p-cyclic, which contradicts the form of the function $f_{j_0+1}(X)$, as compared with Chapter 2 (Prop. 2.2.5). Thus, $\frac{|\Gamma|}{g_{C_{f_{j_0+1}}}} = \frac{2\,p}{p-1}\,\frac{|\mathcal{W}|}{(m_{j_0+1}-1)} \leq \frac{2\,p}{p-1}$. Using (4.5), we obtain $\frac{|V|}{p^{j_0}} \leq |\mathcal{W}| \leq (m_{j_0+1}-1)$. Combined with the formula given in Chapter 3 (Cor. 3.2.7), this inequality yields a lower bound on the genus, namely :

$$g = \frac{p-1}{2} \sum_{i=1}^{n} p^{i-1}\,(m_i - 1) \geq \frac{p-1}{2}\, p^{j_0}\,(m_{j_0+1} - 1) \geq \frac{p-1}{2}\,|V|.$$

It follows that $M \leq \frac{|G|}{g^2} = \frac{|G_2|\,|V|}{g^2} \leq \frac{4\,|G_2|}{(p-1)^2\,|V|}$. Using Lemma 4.4.1, we gather inequality (4.3). Inequality (4.4) then derives from Corollary 4.4.2. □

The following corollary generalizes the finiteness result of Proposition 4.4.7 to all big actions satisfying $\mathcal{G}_M$ such that $\mathrm{Fratt}(G') \subsetneq [G', G]$.

Corollary 4.4.8. *Let $M > 0$ be a positive real such that (C, G) is a big action satisfying $\mathcal{G}_M$. Suppose that* $\mathrm{Fratt}(G') \subsetneq [G', G]$*. Then, $|V|$ and g are bounded as in Proposition 4.4.7. So the quotients $\frac{|G|}{g}$ and $\frac{|G|}{g^2}$ only take a finite number of values.*

Proof : Put $F := \mathrm{Fratt}(G')$. Corollary 4.4.5 asserts that the pair $(C/F, G/F)$ is a big action satisfying $\mathcal{G}_M$ whose second ramification group : $(G/F)_2 = G_2/F$ is p-elementary abelian. From $F \subsetneq [G_2, G]$, we gather $\{e\} \subsetneq [G_2/F : G/F]$, which implies $(G/F)_2 = (G/F)' \not\subset Z(G/F)$. We deduce that $|V|$ is bounded from above as in Proposition 4.4.7. The claim follows. □

4.4.5 Case : $\mathrm{Fratt}(G') = [G', G]$.

It remains to investigate the case where $\mathrm{Fratt}(G') = [G', G]$. In particular, this equality is satisfied when G' is included in the center of G and so is p-elementary abelian (cf. Lemma 3.3), i.e. $\{e\} = \mathrm{Fratt}(G') = [G', G]$. The finiteness result on g obtained in the preceding section is no more true in this case, as illustrated by the remark below.

Remark 4.4.9. *For any integer $s \geq 1$, Proposition 2.2.5 in Chapter 2 exhibits an example of big actions (C, G) with $C : W^p - W = X\,S(X)$ where S is an additive polynomial of $k[X]$ with degree p^s. In this case, $g = \frac{p-1}{2}\,p^s$, $V = Z(\mathrm{Ad}_f) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}$ and $G' = G_2 \simeq \mathbb{Z}/p\mathbb{Z} \subset Z(G)$. It follows that $\frac{|G|}{g^2} = \frac{4\,p}{(p-1)^2}$. So, for all $M \leq \frac{4\,p}{(p-1)^2}$, (C, G) satisfies $\mathcal{G}_M$, with $\{e\} = \mathrm{Fratt}(G') = [G', G]$, whereas $g = \frac{p-1}{2}\,p^s$ grows arbitrary large with s.*

Therefore, in this case, neither g nor $|V|$ are bounded. Nevertheless, the following section shows that, under these conditions, the quotient $\frac{|G|}{g^2}$ take a finite number of values.

Case : $\mathrm{Fratt}(G') = [G', G] = \{e\}$**.**

Proposition 4.4.10. *Let $M > 0$ be a positive real and (C, G) a big action satisfying $\mathcal{G}_M$. Assume that $[G', G] = \mathrm{Fratt}(G') = \{e\}$. Then the quotient $\frac{|G|}{g^2}$ takes a finite number of values.*

Proof : Write $G' = G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, with $n \geq 1$ and keep the notations of Lemma 4.4.3. First of all, Lemma 4.4.1 implies that p^n can only take a finite number of values. Moreover, as recalled in Lemma 4.4.4, $V \subset \bigcap_{i=1}^n Z(\mathrm{Ad}_{f_i})$. Since Ad_{f_1} has degree p^{2s_1}, $|G| = |G'||V| \leq p^{n+2\,s_1}$. We compute the genus by means of [Ro09] Cor. 3.2.7) :

$$g = \frac{p-1}{2} \sum_{i=1}^{n} p^{i-1}\,(m_i - 1) = \frac{p-1}{2}\, p^{s_1}\,(\sum_{i=1}^{n} p^{i-1} p^{s_i - s_1}).$$

It follows that

$$0 < M \leq \frac{|G|}{g^2} \leq \frac{4\,p^n}{(p-1)^2 (\sum_{i=1}^{n} p^{i-1} p^{s_i - s_1})^2},$$

which implies

$$(\sum_{i=1}^{n} p^{i-1} p^{s_i - s_1})^2 \leq \frac{4\, p^n}{M\,(p-1)^2}.$$

Since p^n is bounded from above (Lemma 4.4.1), the set $\{s_i - s_1, i \in [1,n]\} \subset \mathbb{N}$ is also bounded, and then finite. Thus, the quotient

$$\frac{g^2}{p^{2s_1}} = \frac{(p-1)^2}{4} \, (\sum_{i=1}^{n} p^{i-1} p^{s_i - s_1})^2$$

takes a finite number of values. Moreover, from $M \leq \frac{|G|}{g^2} = \frac{|V|\, p^n}{g^2}$, we infer that $\frac{1}{|V|} \leq \frac{p^n}{M\, g^2}$, which implies

$$1 \leq \frac{p^{2s_1}}{|V|} \leq \frac{p^{2\,s_1}\, p^n}{M\, g^2} = \frac{4\, p^n}{M\,(p-1)^2\, (\sum_{i=1}^{n} p^{i-1} p^{s_i - s_1})^2} \leq \frac{4\, p^n}{M\,(p-1)^2}.$$

It follows that the set $\{\frac{p^{2s_1}}{|V|}\} \subset \mathbb{N}$ is bounded, and then finite, as well as the set $\{\frac{|V|}{p^{2s_1}}\}$. Therefore, the quotient $\frac{|G|}{g^2} = p^n \, \frac{|V|}{p^{2s_1}} \, \frac{p^{2s_1}}{g^2}$ can only take a finite number of values. □

The last remaining case is $\mathrm{Fratt}(G') = [G', G] \neq \{e\}$.

Case : $\mathrm{Fratt}(G') = [G', G] \neq \{e\}$**.**

As shown below, this case can only occur for $G'(= G_2)$ non abelian. Note that we do not know yet examples of big actions with a non abelian $G'(= G_2)$.

Theorem 4.4.11. *Assume that $p > 2$. Let (C, G) be a big action with* $\mathrm{Fratt}(G') = [G', G] \neq \{e\}$*. Then, $G'(= G_2)$ is non abelian.*

We deduce the following

Corollary 4.4.12. *Assume that $p > 2$. Let $M > 0$ be a positive real. Let (C, G) be a big action satisfying $\mathcal{G}_M$ with G' abelian. Then, $\frac{|G|}{g^2}$ only takes a finite number of values.*

Remark 4.4.13. *Theorem 4.4.11 is no more true for $p = 2$. A counterexample is given by Chapter 2 (Prop. 2.6.10) applied with $p = 2$. Indeed, when keeping the notations of Chapter 2 (Prop. 2.6.10), take $q = p^e$ with $p = 2$, $e = 2s-1$ and $s \geq 2$. Put $K = \mathbb{F}_q(X)$. Let $L := \mathbb{F}_q(X, W_1, V_1, W_2)$ be the extension of K parametrized by*

$$W_1^{2^{2s-1}} - W_1 = X^{2^{s-1}}\,(X^{2^{2s-1}} - X) \qquad V_1^{2^{2s-1}} - V_1 = X^{2^{s-2}}\,(X^{2^{2s-1}} - X)$$
$$[W_1, W_2]^2 - [W_1, W_2] = [X^{1+2^s}, 0] - [X^{1+2^{s-1}}, 0].$$

Let G be the p-group of $\mathbb{F}_q$-automorphisms of L constructed as in Chapter 2 (Prop. 2.6.10.3). Then, the formula established for g_L in Chapter 2 (Prop. 2.6.10.4) shows that the pair (C, G) is a big action as soon as $s \geq 4$. In this case, $G' = G_2 \simeq \mathbb{Z}/2^2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{6s-4}$ (cf. Chapter 2 Prop. 2.6.7.2). As the functions $X^{2^{s-1}}\,(X^{2^{2s-1}} - X)$ and $X^{2^{s-2}}\,(X^{2^{2s-1}} - X)$ are products of two additive polynomials, it follows from next proof (cf. point 6) that $[G', G] = \mathrm{Fratt}(G') \neq \{e\}$*.*

Proof of Theorem 4.4.11 :

1. *Preliminary remarks : the link with Theorem 2.5.1 in Chapter 2.*
   (a) One first remarks that Theorem 4.4.11 implies Theorem 2.5.1 in Chapter 2. The latter states that there is no big action (C, G) with G_2 cyclic of exponent strictly greater than p. Indeed, assume that there exists one. Then, $G' = G_2$ is abelian and $\mathrm{Fratt}(G') = (G')^p \neq \{e\}$. To contradict Theorem 4.4.11, it remains to show that $F := \mathrm{Fratt}(G') = [G', G]$. From Corollary 4.4.5, we infer that $(C/F, G/F)$ is a big action whose second ramification group G_2/F is cyclic of order p. Then, $(G/F)' = (G/F)_2 = G_2/F \subset Z(G/F)$ (cf. Chapter 2 Prop. 2.2.5 and Chapter 3 Prop. 3.2.13). It follows that $\mathrm{Fratt}((G/F)') = [(G/F)', G/F] = \{e\}$. As $F \subset G'$, this imposes $F = [G', G]$. Then, Theorem 4.4.11 contradicts the fact that $G' = G_2$ is abelian.

   (b) The object of Theorem 4.4.11 is to prove that there exists no big action (C, G) with $G' = G_2$ abelian of exponent strictly greater than p such that $\mathrm{Fratt}(G') = [G', G]$. The proof follows the same canvas as the proof of Chapter 2 (Thm. 2.5.1). Nevertheless, to refine the arguments, we use the formalism related to the ring filtration of $k[X]$ linked with the additive polynomials as introduced in Chapter 3 (cf. Section 3.3). More precisely, we recall that, for any $t \geq 1$, we define Σ_t as the k-vector subspace of $k[X]$ generated by 1 and the products of at most t additive polynomials of $k[X]$ (cf. Chapter 3, Def. 3.3.1). In what follows, we assume that there exists a big action (C, G) with $G' = G_2$ abelian of exponent strictly greater than p such that $\mathrm{Fratt}(G') = [G', G]$.

2. *One can suppose that* $G' = G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^r$*, with* $r \geq 1$*.*
   Indeed, write $G'/(G')^{p^2} \simeq (\mathbb{Z}/p^2\mathbb{Z})^a \times (\mathbb{Z}/p\mathbb{Z})^b$. By assumption, $a \geq 1$. Using [Su82] (Chap.2, Thm. 19), one can find an index p-subgroup H of $(G')^p$, normal in G, such that $(G')^{p^2} \subset H \subsetneq (G')^p \subsetneq G' = G_2$. Then, we infer from Chapter 2 (Lemma 2.2.4) that $(C/H, G/H)$ is a big action with second ramification group $(G/H)' = (G/H)_2 = G_2/H \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{a+b-1}$. Furthermore, as G' is abelian, $\mathrm{Fratt}(G') = (G')^p$ (resp. $\mathrm{Fratt}((G/H)') = ((G/H)')^p$). From $H \subset (G')^p$ with H normal in G and $\mathrm{Fratt}(G') = [G', G]$, we gather that $\mathrm{Fratt}((G/H)') = (G')^p/H = \mathrm{Fratt}(G')/H = [(G/H)', G/H]$.

3. *Notation.*
   In what follows, 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 as already used in Chapter 2 (proof of Thm. 2.5.1, point 2), we introduce the $W_2(\mathbb{F}_p)$-module

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

   where $W_2(L)$ means the ring of Witt vectors of length 2 with coordinates in L and $\wp = F - id$. One can prove that A is isomorphic to the dual of G_2 with respect to the Artin-Schreier-Witt pairing (cf. [Bour83] Chap. IX, ex. 19). Moreover, as a $\mathbb{Z}$-module, A is generated by the classes mod $\wp(k[X])$ of $(f_0(X), g_0(X))$ and $\{(0, f_i(X))\}_{1 \leq i \leq r}$ in $W_2(k[X])$. In other words, $L = k(X, W_i, V_0)_{0 \leq i \leq r}$ is parametrized by the following system of Artin-Schreier-Witt equations :

$$\wp([W_0, V_0]) = [f_0(X), g_0(X)] \in W_2(k[X])$$

   and

$$\forall\, i \in \{1, \ldots, r\}, \quad \wp(W_i) = f_i(X) \in k[X].$$

   An exercise left to the reader shows that one can choose $g_0(X)$ and each $f_i(X)$, with $0 \leq i \leq r$, reduced mod $\wp(k[X])$.

4. *We prove that* $f_0 \in \Sigma_2$*.*
   As a $\mathbb{Z}$-module, $p\,A$ is generated by the class of $(0, f_0(X))$ in A. By the Artin-Schreier-Witt pairing, $p\,A$ corresponds to the kernel $G_2[p]$ of the map :

$$\begin{cases} G_2 \to G_2 \\ g \to g^p. \end{cases}$$

   Thus, $G_2[p] \subsetneq G_2$ is a normal subgroup of G. Then, it follows from Chapter 2 (Lemma 2.2.4) that the pair $(C/G_2[p], G/G_2[p])$ is a big action parametrized by $W^p - W = f_0(X)$ and with second ramification group $G_2/G_2[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Then, $f_0(X) = X\,S(X) + c\,X \in k[X]$ (cf. Chapter 2, Prop. 2.2.5), where S is an additive polynomial of $k\{F\}$ with degree $s \geq 1$ in F.

5. *The embedding problem.*
   For any $y \in V$, the classes mod $\wp(k[X])$ of $(f_0(X+y), g_0(X+y))$ and $\{(0, f_i(X+y))\}_{1 \leq i \leq r}$ induces a new generating system of A. As in Chapter 2 (proof of Thm 2.5.1, point 3), this is expressed by the following equation :

$$\forall\, y \in V, \quad (f_0(X+y), g_0(X+y)) = (f_0(X), g_0(X) + \sum_{i=0}^{r} \ell_i(y)\, f_i(X)) \quad \mathrm{mod}\ \wp(W_2(k[X])), \qquad (4.6)$$

   where, for all i in $\{0, \ldots, r\}$, ℓ_i is a linear form from V to $\mathbb{F}_p$. On the second coordinate, (4.6) reads :

$$\forall\, y \in V, \quad \Delta_y(g_0) := g_0(X+y) - g_0(X) = \sum_{i=0}^{r} \ell_i(y)\, f_i(X) + c \qquad \mathrm{mod}\ \wp(k[X]), \qquad (4.7)$$

   where

$$c = \sum_{i=1}^{p-1} \frac{(-1)^i}{i}\, y^{p-i}\, X^{i+p^{s+1}} + \text{lower degree terms in X} \qquad (4.8)$$

   For more details on calculation, we refer to Chapter 2 (proof of Thm 2.5.1, point 3 and Lemma 2.5.2).

6. *We prove that* f_i *lies in* Σ_2*, for all* i *in* $\{0, \ldots, r\}$*, if and only if* $\mathrm{Fratt}(G') = [G', G]$.
   Put $F := \mathrm{Fratt}(G')$. We deduce from Corollary 4.4.5 that $(C/F, G/F)$ is a big action whose second ramification group $(G/F)' = (G/F)_2 = G_2/F$ is p-elementary abelian. The function field of the curve C/F is now parametrized by the Artin-Schreier equations :

$$\forall\, i \in \{0, \ldots, r\}, \quad \wp(W_i) = f_i(X) \in k[X].$$

As $F \subset [G', G]$ (cf. Lemma 4.4.5),

$$F = [G', G] = [G_2, G] \Leftrightarrow \{e\} = [G_2/F, G/F] = [(G/F)', G/F] \Leftrightarrow (G/F)' \subset Z(G/F).$$

By Chapter 3 (Prop. 3.2.13), this occurs if and only if for all i in $\{0, \dots, r\}$, $f_i(X) = X\, S_i(X) + c_i\, X \in \Sigma_2$.

7. *We prove that g_0 does not belong to Σ_p.*
We first notice that the right-hand side of (4.7) does not belong to Σ_{p-1} : indeed, the monomial $X^{p-1+p^{s+1}} \in \Sigma_p - \Sigma_{p-1}$ occurs once in c but not in $\sum_{i=0}^{r} \ell_i(y)\, f_i(X)$ which lies in $\Sigma_2 \subset \Sigma_{p-1}$, for $p \geq 3$. Now, assume that $g_0 \in \Sigma_p$. Then, by Chapter 3 (Lemma 3.3.9), the left-hand side of (4.7), namely $\Delta_y(g_0)$, lies in Σ_{p-1}, hence a contradiction. Therefore, one can define an integer a such that X^a is the monomial of $g_0(X)$ with highest degree among those that do not belong to Σ_p. Note that since g_0 is reduced mod $\wp(k[X])$, $a \neq 0 \bmod p$.

8. *We prove that $a - 1 \geq p - 1 + p^{s+1}$.*
We have already seen that the monomial $X^{p-1+p^{s+1}}$ occurs in the right hand side of (4.7). In the left-hand side of (4.7), $X^{p-1+p^{s+1}}$ is produced by monomials X^b of g_0 with $b > p - 1 + p^{s+1}$. If $b > a$, $X^b \in \Sigma_p$, so $\Delta_y(X^b) \in \Sigma_{p-1}$, which is not the case of $X^{p-1+p^{s+1}}$. It follows that $X^{p-1+p^{s+1}}$ comes from monomials X^b with $a \geq b > p - 1 + p^{s+1}$. Hence the expected inequality.

9. *We prove that p divides $a - 1$.*
Assume that p does not divide $a - 1$. In this case, the monomial X^{a-1} is reduced mod $\wp(k[X])$ and (4.7) reads as follows :

$$\forall\, y \in V, \quad c_a(g_0)\, a\, y\, X^{a-1} + S_{p-1}(X) + R_{a-2}(X) = c + \sum_{i=0}^{r} \ell_i(y)\, f_i(X) \quad \bmod\ \wp\,(k[X]),$$

where $c_a(g_0) \neq 0$ denotes the coefficient of X^a in g_0, $S_{p-1}(X)$ is a polynomial in Σ_{p-1} produced by monomials X^b of g_0 with $b > a$ and $R_{a-2}(X)$ is a polynomial of $k[X]$ with degree lower than $a - 2$ produced by monomials X^b of g_0 with $b \leq a$. We first notice that X^{a-1} does not occur in $S_{p-1}(X)$. Otherwise, $X^{a-1} \in \Sigma_{p-1}$ and $X^a = X^{a-1}\, X \in \Sigma_p$, hence a contradiction. Likewise, X^{a-1} does not occur in $\sum_{i=0}^{r} \ell_i(y)\, f_i(X) \in \Sigma_2$. Otherwise, $X^a = X^{a-1}\, X \in \Sigma_3 \subset \Sigma_p$, as $p \geq 3$. It follows that X^{a-1} occurs in c, which requires $a - 1 \leq \deg b = p - 1 + p^{s+1}$. Then, the previous point implies $a - 1 = p - 1 + p^{s+1}$, which contradicts $a \neq 0 \bmod p$.
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 $j_0 := a - p^t = 1 + (\lambda - 1)\, p^t$.

10. *We search for the coefficient of the monomial X^{j_0} in the left-hand side of* (4.7).
Since p does not divide j_0, the monomial X^{j_0} is reduced mod $\wp(k[X])$. In the left-hand side of (4.7), 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 $b \geq j_0 + 1$. However, as seen above, the monomials X^b with $b > a$ produce in $\Delta_y(g_0)$ elements that belong to Σ_{p-1}, whereas $X^{j_0} \notin \Sigma_{p-1}$. Otherwise, $X^a = X^{j_0}\, X^{p^t} \in \Sigma_p$, which contradicts the definition of a. So we only have to consider the monomials X^b of $g_0(X)$ with $b \in \{j_0 + 1, \dots, a\}$. Then, the same arguments as those used in Chapter 2 (proof of Thm. 2.5.1, point 6) allow to conclude that the coefficient of X^{j_0} in the left-hand side of (4.7) is $T(y)$ where $T(Y)$ denotes a polynomial of $k[X]$ with degree p^t.

11. *We identify with the coefficient of X^{j_0} in the right-hand side of* (4.7) *and gather a contradiction.* As mentionned above, the monomial X^{j_0} does not occur in $\sum_{i=0}^{r} \ell_i(y)\, f_i(X) \in \Sigma_2 \subset \Sigma_{p-1}$, for $p \geq 3$. Assume that the monomial X^{j_0} appears in c, which implies that $j_0 \leq p - 1 + p^{s+1}$. Using the same arguments as in Chapter 2 (proof of Thm. 2.5.1, point 7), we gather that $j_0 = 1 + (\lambda - 1)\, p^t = 1 + p^{s+1}$. Then, X^{j_0} lies in Σ_2, which leads to the same contradiction as above. Therefore, the monomial X^{j_0} does not occur in the right-hand side of (4.7). Then, $T(y) = 0$ for all y in V, which means that $|V| \leq p^t$. Call C_0 the curve whose function field is parametrized by $\wp([W_0, V_0]) = [f_0(X), g_0(X)]$. The same calculation as in Chapter 2 (proof of Theorem 2.5.1, point 7) shows that $g_{C_0} \geq p^{t+1}\, (p - 1)$. Furthermore, $g \geq p^r\, g_{C_0}$ (see e.g. [LM05] Prop. 8.5, formula (8)). As $|G| = |G_2||V| \leq p^{2+r+t}$, it follows that $\frac{|G|}{g} = \frac{p}{p-1} < \frac{2\, p}{p-1}$, hence a contradiction. □

4.5 Classification of big actions under condition $(*)$.

We now pursue the classification of big actions initiated by Lehr and Matignon who characterize big actions (C, G) satisfying $\frac{|G|}{g^2} \geq \frac{4}{(p-1)^2}$ (cf. [LM05]). In this section, we exhibit a parametrization for big actions (C,G) satisfying condition $(*)$, namely :

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

As proved in Chapter 2 (Prop. 2.4.1 and Prop. 2.4.2), this condition requires $G'(=G_2)$ to be an elementary abelian p-group with order dividing p^3. Since G_2 cannot be trivial (cf. Chapter 2 Prop. 2.2.2), this leaves three possibilities. This motivates the following

Definition 4.5.1. *Let (C,G) be abig action. Let $i \geq 1$ be an integer. We say that*

1. *(C,G) satisfies $\mathcal{G}_*$ if (C,G) satisfies condition $(*)$*
2. *(C,G) satisfies $\mathcal{G}_*^{p^i}$ if (C,G) satisfies $\mathcal{G}_*$ with $G' \simeq (\mathbb{Z}/p\mathbb{Z})^i$.*

4.5.1 First case : big actions satisfying $\mathcal{G}_*^p$.

Proposition 4.5.2. *We keep the notations of Section 4.4.3.*

1. *(C,G) is a big action with $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ if and only if C is birational to a curve C_f parametrized by $W^p - W = f(X) = X\,S(X) \in k[X]$, where S is a (monic) additive polynomial with degree $s \geq 1$ in F.*
2. *In what follows, we assume that C is birational to a curve C_f as described in the first point.*
   - (a) *If $s \geq 2$, $A_{\infty,1}$ is the unique p-Sylow subgroup of A, where ∞ denotes the point of C corresponding to $X = \infty$.*
   - (b) *If $s = 1$, there exists $r := p^3 + 1$ points of C : $P_0 := \infty, P_1, \ldots, P_r$ such that $(A_{P_i,1})_{0 \leq i \leq r}$ are the p-Sylow subgroups of A. In this case, for all i in $\{1, \ldots, r\}$, there exists $\sigma_i \in A$ such that $\sigma_i(P_i) = \infty$.*

   In both cases, $A_{\infty,1}$ is an extraspecial group (see [Su86] Def. 4.14) with exponent p (resp. p^2) if $p > 2$ (resp. $p = 2$) and order p^{2s+1}. More precisely, $A_{\infty,1}$ is a central extension of its center $Z(A_{\infty,1}) = (A_{\infty,1})'$ by the elementary abelian p-group $Z(\mathrm{Ad}_f)$, i.e.

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

   Furthermore, $(C, A_{\infty,1})$, and so each $(C, A_{P_i,1})$, with $1 \leq i \leq r$, are big actions satisfying $\mathcal{G}_*^p$.
3. *Let V be a vector subspace of $Z(\mathrm{Ad}_f)$ with dimension v over $\mathbb{F}_p$. Then, $(C, \pi^{-1}(V))$ is also a big action satisfying $\mathcal{G}_*^p$ if and only if*

$$\begin{array}{ll} \text{if } p \neq 2, & 2s \geq v \geq \max\{s+1, 2s-3\} \\ \text{if } p = 2, & 2s \geq v \geq \max\{s+1, 2s-4\} \end{array}$$

We collect the different possibilities in the table below :

case	v	s	V	G
1-	$2s$	$s \geq 1^\dagger$	$Z(\mathrm{Ad}_f)^\dagger$	$A_{\infty,1}^\dagger$
2	$2s-1$	$s \geq 2$	index p subgroup of $Z(\mathrm{Ad}_f)$	index p subgroup of $A_{\infty,1}$
3	$2s-2$	$s \geq 3$	index p^2 subgroup of $Z(\mathrm{Ad}_f)$	index p^2 subgroup of $A_{\infty,1}$
4	$2s-3$	$s \geq 4$	index p^3 subgroup of $Z(\mathrm{Ad}_f)$	index p^3 subgroup of $A_{\infty,1}$
5 (p=2)	$2s-4$	$s \geq 5$	index p^4 subgroup of $Z(\mathrm{Ad}_f)$	index p^4 subgroup of $A_{\infty,1}$

case	$\lvert G\rvert/g$	$\lvert G\rvert/g^2$
1	$\frac{2\,p}{p-1}\,p^s$	$\frac{4}{(p^2-1)^2}\,(p+1)^2\,p$
2	$\frac{2\,p}{p-1}\,p^{s-1}$	$\frac{4}{(p^2-1)^2}\,(p+1)^2$
3	$\frac{2\,p}{p-1}\,p^{s-2}$	$\frac{4}{(p^2-1)^2}\,\frac{(p+1)^2}{p}$
4	$\frac{2\,p}{p-1}\,p^{s-3}$	$\frac{4}{(p^2-1)^2}\,\frac{(p+1)^2}{p^2}$
5 (p=2)	$\frac{2\,p}{p-1}\,p^{s-4}$	$\frac{4}{(p^2-1)^2}\,\frac{(p+1)^2}{p^3}$

† *Note :* In the case $s = 1$, this result is true up to conjugation by σ_i as defined in Proposition 4.5.2.

Proof :

1. See [LM05] (Thm. 1.1 I)

2. See Remark 4.3.1, [LM05] (Thm. 3.1) and Chapter 2 (Prop. 2.2.5).
3. This essentially derives from Proposition 4.3.2 which implies $(p+1)^2 \geq p^{2s-v-1}$. If $2s-v-1 \geq 3$, it implies $p^2+2\,p+1 \geq p^3$, which is impossible for $p>2$. Accordingly, if $p>2$, we obtain $2s-v-1 \leq 2$, which means $v \geq 2s-3$. If $p=2$, $(p+1)^2 \geq p^{2s-v-1}$ is satisfied if and only if $2s-v-1 \leq 3$, i.e. $v \geq 2s-4$. The claim follows. □

Remark 4.5.3. *Note that, for $p>2$, the solutions can be parametrized by s algebraically independent variables over $\mathbb{F}_p$, namely the s coefficients of S assumed monic after an homothety on the variable X. Note that $s \sim \log g$.*

4.5.2 Second case : big actions satisfying $\mathcal{G}_*^{p^2}$.

Case : $[G', G] = \mathrm{Fratt}(G') = \{e\}$.

Proposition 4.5.4. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^2}$. Assume that $[G', G] = \{e\}$ and keep the notations of section 4.4.3.*

1. *The pair $(C, A_{\infty,1})$ is a big action satisfying $\mathcal{G}_*^{p^2}$. Moreover, $A_{\infty,1}$ is a special group (see [Su86] Def. 4.14) with exponent p (resp. p^2) (for $p>2$ (resp. $p=2$) and order $p^{2+2\,s_1}$. More precisely, $A_{\infty,1}$ is a central extension of its center $Z(A_{\infty,1}) = (A_{\infty,1})'$ by the elementary abelian p-group $Z(\mathrm{Ad}_{f_1})$, i.e.*

$$0 \longrightarrow Z(A_{\infty,1}) = (A_{\infty,1})' \simeq (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow A_{\infty,1} \xrightarrow{\pi} Z(\mathrm{Ad}_{f_1}) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s_1} \longrightarrow 0.$$

2. *Furthermore, $s_2 = s_1$ or $s_2 = s_1+1$.*
   (a) *If $s_2 = s_1$, $G = \pi^{-1}(V)$, where V is a vector subspace of $Z(\mathrm{Ad}_{f_1})$ with dimension v over $\mathbb{F}_p$ such that $2\,s_1 - 2 \leq v \leq 2\,s_1$. Then, $A_{\infty,1}$ is a p-Sylow subgroup of A. It is normal except if C is birationnal to the Hermitian curve : $W^q - W = X^{1+q}$ with $q = p^2$.*
   (b) *If $s_2 = s_1+1$, $V = Z(\mathrm{Ad}_{f_1})$ and $G = A_{\infty,1}$ is the unique p-Sylow subgroup of A.*

The different possibilities are listed in the table below :

case	s_1	s_2	v	V	G
(a)-1	$s \geq 2$	s	$2s$	$Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2})$	$A_{\infty,1}$
(a)-2	$s \geq 2$	s	$2s-1$	index p subgroup of $Z(\mathrm{Ad}_{f_1})$	index p subgroup of $A_{\infty,1}$
(a)-3	$s \geq 3$	s	$2s-2$	index p^2 subgroup of $Z(\mathrm{Ad}_{f_1})$	index p^2 subgroup of $A_{\infty,1}$
(b)	$s \geq 3$	$s+1$	$2s$	$Z(\mathrm{Ad}_{f_1})$	$A_{\infty,1}$

case	$\lvert G\rvert/g$	$\lvert G\rvert/g^2$
(a)-1	$\frac{2\,p}{p-1}\,\frac{p^{1+s}}{1+p}$	$\frac{4}{(p^2-1)^2}\,p^2$
(a)-2	$\frac{2\,p}{p-1}\,\frac{p^{s}}{1+p}$	$\frac{4}{(p^2-1)^2}\,p$
(a)-3	$\frac{2\,p}{p-1}\,\frac{p^{s-1}}{1+p}$	$\frac{4}{(p^2-1)^2}$
(b)	$\frac{2\,p}{p-1}\,\frac{p^{1+s}}{1+p}$	$\frac{4}{(p^2-1)^2}\,\frac{p^2(p+1)^2}{(1+p^2)^2}$

Proof :

1. Use Proposition 4.3.2 to prove that the pair $(C, A_{\infty,1})$ is a big action satisfying $\mathcal{G}_*^{p^2}$ with the following exact sequence :
$$0 \longrightarrow A_{\infty,2} \longrightarrow A_{\infty,1} \xrightarrow{\pi} Z(\mathrm{Ad}_{f_1}) \simeq (\mathbb{Z}/p\,\mathbb{Z})^{2\,s_1} \longrightarrow 0.$$
The proof to show that $A_{\infty,1}$ is a special group, i.e. satisfies $Z(A_{\infty,1}) = (A_{\infty,1})' = \mathrm{Fratt}(A_{\infty,1}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$, is the same that the one exposed in Chapter 3 (Prop. 3.4.3.3). Nevertheless, one has to choose $\mathcal{H}$ an index p-subgroup of G_2 such that $C/\mathcal{H}$ is the curve parametrized by $W_1^p - W_1 = f_1(X)$.
2. Assume that $s_2 - s_1 \geq 2$. Then, $|G| = p^{2+v} \leq p^{2+2\,s_1}$ and $g = \frac{p-1}{2}\,p^{s_1}\,(1+p^{1+s_2-s_1}) \geq \frac{p-1}{2}\,p^{s_1}\,(1+p^3)$. So, $\frac{|G|}{g^2} \leq \frac{4}{(p^2-1)^2}\,\frac{(1+p)^2\,p^2}{(1+p^3)^2} < \frac{4}{(p^2-1)^2}$, which contradicts condition $(*)$. So, $0 \leq s_2 - s_1 \leq 1$. In each case, the description of $A_{\infty,1}$ and G derive from Proposition 4.3.2 combined with Remark 4.3.1. □

To go further in the description of the functions $f_i's$ in each case, we introduce two additive polynomials $\mathcal{V}$ and T defined as follows :

$$\forall\, i \in \{1,2\}, \quad \mathcal{V} := \prod_{y \in V} (X-y) \quad \text{divides} \quad T := \gcd\{\mathrm{Ad}_{f_1}, \mathrm{Ad}_{f_2}\} \quad \text{divides} \quad \mathrm{Ad}_{f_i}.$$

In what follows, we work in the Ore ring $k\{F\}$ and write the additive polynomials as polynomials in F.

case	$\deg_F \mathcal{V}$	$\deg_F T$	$\deg_F (\mathrm{Ad}_{f_1})$	$\deg_F (\mathrm{Ad}_{f_2})$	T
(a)-1	$2s$	$2s$	$2s$	$2s$	$\mathcal{V} = T = \mathrm{Ad}_{f_1} = \mathrm{Ad}_{f_2}$
(a)-2-i	$2s-1$	$2s$	$2s$	$2s$	$\mathcal{V}$ divides $T = \mathrm{Ad}_{f_1} = \mathrm{Ad}_{f_2}$
(a)-2-ii	$2s-1$	$2s-1$	$2s$	$2s$	$\mathcal{V} = T$ divides Ad_{f_1}
(a)-3-i	$2s-2$	$2s$	$2s$	$2s$	$\mathcal{V}$ divides $T = \mathrm{Ad}_{f_1} = \mathrm{Ad}_{f_2}$
(a)-3-ii	$2s-2$	$2s-1$	$2s$	$2s$	$\mathcal{V}$ divides T divides Ad_{f_1}
(a)-3-iii	$2s-2$	$2s-2$	$2s$	$2s$	$\mathcal{V} = T$ divides Ad_{f_1}
(b)	$2s$	$2s$	$2s$	$2s+2$	$\mathcal{V} = T = \mathrm{Ad}_{f_1}$ divides Ad_{f_2}

The three cases where $\mathrm{Ad}_{f_1} = \mathrm{Ad}_{f_2}$ can be parametrized in the same way as in Chapter 3 (Prop. 3.4.2).

case	S_1 or Ad_{f_1}	S_2 or Ad_{f_2}
(a)-1	$S_1 = \sum_{j=0}^{s/d} \alpha_{jd}\, F^{jd}, \quad \alpha_s = 1$	$S_2 = \gamma\, S_1, \quad \gamma \in \mathbb{F}_{p^d} - \mathbb{F}_p, \quad d \geq 2$
(a)-2-i	$S_1 = \sum_{j=0}^{s/d} \alpha_{jd}\, F^{jd}, \quad \alpha_s = 1$	$S_2 = \gamma\, S_1, \quad \gamma \in \mathbb{F}_{p^d} - \mathbb{F}_p, \quad d \geq 2$
(a)-2-ii	$\mathrm{Ad}_{f_1} = (\alpha_1\, F + \beta_1\, I)\, T, \quad \alpha_1 \neq 0$	$\mathrm{Ad}_{f_2} = (\alpha_2\, F + \beta_2\, I)\, T, \quad \alpha_2 \neq 0$
(a)-3-i	$S_1 = \sum_{j=0}^{s/d} \alpha_{jd}\, F^{jd}, \quad \alpha_s = 1$	$S_2 = \gamma\, S_1, \quad \gamma \in \mathbb{F}_{p^d} - \mathbb{F}_p, \quad d \geq 2$
(a)-3-ii	$\mathrm{Ad}_{f_1} = (\alpha_1\, F + \beta_1\, I)\, T, \quad \alpha_1 \neq 0$	$\mathrm{Ad}_{f_2} = (\alpha_2\, F + \beta_2\, I)\, T, \quad \alpha_2 \neq 0$
(a)-3-iii	$\mathrm{Ad}_{f_1} = (\alpha_1\, F^2 + \beta_1\, F + \delta_1\, I)\, T, \quad \alpha_1 \neq 0$	$\mathrm{Ad}_{f_2} = (\alpha_2\, F^2 + \beta_2\, F + \delta_2\, I)\, T, \quad \alpha_2 \neq 0$
(b)	$\mathrm{Ad}_{f_1} = \prod_{v \in V}(X-v)$	$\mathrm{Ad}_{f_2} = (\alpha_2\, F^2 + \beta_2\, F + \delta_2\, I)\, \mathrm{Ad}_{f_1}, \quad \alpha_2 \neq 0$

We display the parametrization of the functions f_i's in the case (a)-2-ii for the smallest values of s, namely $s=2$ and $s=3$.

Cas (a)-2-ii with $s = 2$ for $p > 2$.

f_1	$f_1(X) = X^{1+p^2} + a_{1+p}\, X^{1+p} + \frac{1}{2}\, a_2\, X^2$
a_{1+p}	$a_{1+p} \in k$
a_2	$a_2 \in k$
f_2	$f_2(X) = b_{1+p^2}^{p^2}\, X^{1+p^2} + b_{1+p}\, X^{1+p} + b_2\, X^2 + b_1\, X$
b_{1+p^2}	$b_{1+p^2} \in Z(w^{p^2}\, X^{p^3} + w^{p}_{,}(-a_2^p + a_{1+p}^p\, w^{p^2} - w^{p^2+p^3})\, X^{p^2} + (a_{1+p} - w^{p^2})\, X^p - w^{-1}\, X)$ with $\quad b_{1+p^2} \notin \mathbb{F}_{p^2}.$
w	$w \in Z(X^{1+p+p^2+p^3} - a_{1+p}^p\, X^{1+p+p^2} + a_2^p\, X^{1+p} - a_{1+p}\, X + 1)$
b_{1+p}	$b_{1+p} = w^{p^2}\, (b_{1+p^2}^{p^2} - b_{1+p^2})^p + b_{1+p^2}^p\, a_{1+p}$
b_2	$2\, b_2 = w^p\, (b_{1+p^2}^{p^2} - b_{1+p^2})\, (a_{1+p} - w^{p^2}) + b_{1+p^2\; 2}$
b_1	$b_1 \in k$

Case (a)-2-ii with $s = 3$ for $p > 2$.

f_1	$f_1(X) = X^{1+p^3} + a_{1+p^2}\, X^{1+p^2} + a_{1+p}\, X^{1+p} + \frac{1}{2}\, a_2\, X^2$
a_{1+p^2}	$a_{1+p^2} \in k$
a_{1+p}	$a_{1+p} \in k$
a_2	$a_2 \in k$

f_2	$f_2(X) = b_{1+p^3}^{p^3}\, X^{1+p^3} + b_{1+p^2}\, X^{1+p^2} + b_{1+p}\, X^{1+p} + b_2\, X^2 + b_1\, X$
w	$w \in Z(X^{1+p+p^2+p^3+p^4+p^5} - a_{1+p^2}^{p^2} X^{1+p+p^2+p^3+p^4}$ $+a_{1+p}^{p^2} X^{1+p+p^2+p^3} - a_2^{p^2}\, X^{1+p+p^2} + a_{1+p}^{p} X^{1+p} - a_{1+p^2} X + 1)$
b_{1+p^3}	$b_{1+p^3} \in Z(P_1) \cap Z(P_2) - \mathbb{F}_{p^3}$ with $P_1(X) = w^{p^3+1}\, X^{p^5} + (1 - w\, a_{1+p^2}) X^{p^3} + (w\, a_{1+p^2} - w^{p^3+1})\, X^{p^2} - X$ with $P_2(X) = w^{p^2} (a_{1+p^2} - w^{p^3})\, X^{p^4} + w^p(-a_2^p + a_{1+p}^p\, w^{p^2} - a_{1+p^2}^p w^{p^2+p^3} + w^{p^2+p^3+p^4})\, X^{p^3}$ $+(a_{1+p} + w^{p^2+p^3} - a_{1+p^2} w^{p2})\, X^p$ $+(-a_{1+p} + a_2^p w^p - a_{1+p}^p w^{p+p^2} + a_{1+p^2}^p w^{p+p^2+p^3} - w^{p+p^2+p^3+p^4})\, X$
b_{1+p^2}	$b_{1+p^2} = w^{p^3}\, (b_{1+p^3}^{p^3} - b_{1+p^3})^{p^2} + b_{1+p^3}^{p^2}\, a_{1+p^2}$
b_{1+p}	$b_{1+p} = w^{p^2}\, (b_{1+p^3}^{p^3} - b_{1+p^3})^p\, (a_{1+p^2} - w^{p^3}) + b_{1+p^3}^{p}\, a_{1+p}$
b_2	$2\, b_2 = w^p\, (b_{1+p^3}^{p^3} - b_{1+p^3})\, (a_{1+p} - a_{1+p^2}\, w^{p^2} + w^{p^2+p^3}) + b_{1+p^3}\, a_2$
b_1	$b_1 \in k$

The calculation of the case $s = 3$ already raises a problem as the parameter b_{1+p^3} has to lie in the set of zeroes of two polynomials.

For the remaining last two cases (a)-3-iii and (b), we merely display examples of realization so as to prove the effectiveness of these cases.

An example of realization for the case (a)-3-iii.

T	$T = F^{2s-2} + I$
V	$V = Z(F^{2s-2} + I)$
Ad_{f_1}	$\mathrm{Ad}_{f_1} = (F^2 + I)\, T$
f_1	$f_1(X) = X^{1+p^s} + X^{1+p^{s-2}}$
Ad_{f_2}	$\mathrm{Ad}_{f_2} = (F^2 + F + I)\, T$
f_2	$f_2(X) = X^{1+p^s} + X^{1+p^{s-1}} + X^{1+p^{s-2}}$

An example of realization for the case (b).

f_1	$f_1(X) = X^{1+p^s}$
f_2	$f_2(X) = \alpha_2\, X^{1+p^{s+1}} + \beta_2\, X^{1+p^s} + \delta_2\, X^{1+p^{s-1}}$
α_2	$\alpha_2 \in \mathbb{F}_{p^{2s}}$
β_2	$\beta_2 \in \mathbb{F}_{p^s}$
δ_2	$\delta_2 \in \mathbb{F}_{p^{2s}}$

Case : $[G', G] \supsetneq \mathrm{Fratt}(G') = \{e\}$.

Proposition 4.5.5. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^2}$ such that $[G', G] \neq \{e\}$. We keep the notations introduced in Section 4.4.3.*

1. *(a) Then, $G = A_{\infty,1}$ is the unique p-Sylow subgroup of A.*
   (b) For all i in $\{1, 2\}$, $f_i \in \Sigma_{i+1} - \Sigma_i$ and $m_i = 1 + i\, p^s$, with $p \geq 3$ and $s \in \{1, 2\}$.
   (c) Moreover, $v = s + 1$. More precisely, $y \in V$ if and only if $\ell_{1,2}(y)^p - \ell_{1,2}(y) = 0$.
2. *There exists a coordinate X for the projective line C/G_2 such that the functions f_i's are parametrized as follows :*

(a) If $s = 1$,

	$p > 3$	$p = 3$
f_1	$f_1(X) = X^{1+p} + a_2\, X^2$	$f_1(X) = X^4 + a_2\, X$
V	$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{p^2} + 2\, a_2^p\, X^p + X)$	$V = Z(\mathrm{Ad}_{f_1}) = Z(X^9 + 2\, a_2^3\, X^3 + X)$
f_2	$f_2(X) = b_{1+2\,p}\, X^{1+2\,p} + b_{2+p}\, X^{2+p} + b_3\, X^3 + b_1\, X$	$f_2(X) = b_7\, X^7 + b_5\, X^5 + b_1\, X$
$b_{1+2\,p}$	$b_{1+2\,p} \in k^\times$	$b_7^{16} = 1$
a_2	$2\, a_2^p = -b_{1+2\,p}^{-p}(b_{1+2\,p}^{p^2} + b_{1+2\,p}) \Leftrightarrow b_{1+2\,p} \in V$	$2\, a_2^3 = -b_7^6 - b_7^{-2}$
b_{2+p}	$b_{2+p} = -b_{1+2\,p}^p$	$b_5 = -b_7^3$
b_3	$3\, b_3^p = b_{1+2\,p}^{-p}\, (b_{1+2\,p}^{2\,p^2} - b_{1+2\,p}^2)$	
b_1	$b_1 \in k$	$b_1 \in k$
$\ell_{1,2}$	$\ell_{1,2}(y) = 2\, (b_{1+2\,p}\, y^p - b_{1+2\,p}^p\, y)$	$\ell_{1,2}(y) = 2\, (b_7\, y^3 - b_7^3\, y)$

Therefore, for $p > 3$, the solutions are parametrized by 2 algebraically independent variables over $\mathbb{F}_p$, namely $b_{1+2\,p} \in k^\times$ and $b_1 \in k$. For $p = 3$, as the monomial X^3 can be reduced mod $\wp(k[X])$, the parameter $b_{1+2\,p}$ satisfies an additional algebraic relation : $b_7^{16} = 1$. Then, b_7 takes a finite number of values.

In both cases ($p = 3$ or $p > 3$),

$$\frac{|G|}{g} = \frac{2\,p}{p-1}\,\frac{p^2}{1+2\,p} \qquad \textit{and} \qquad \frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^2\,(p+1)^2}{(1+2\,p)^2}.$$

(b) If $s = 2$ and $p > 3$,

f_1	$f_1(X) = X^{1+p^2} + a_{1+p}\, X^{1+p} + a_2\, X^2$
Ad_{f_1}	$X^{p^4} + a_{1+p}^{p^2}\, X^{p^3} + 2\, a_2^{p^2}\, X^{p^2} + a_{1+p}^p\, X^p + X$
f_2	$f_2(X) = b_{1+2\,p^2}\, X^{1+2\,p^2} + b_{1+p+p^2}\, X^{1+p+p^2} + b_{2+p^2}\, X^{2+p^2} + b_{1+p^2}\, X^{1+p^2} + b_{1+2\,p}\, X^{1+2\,p}$ $+ b_{2+p} X^{2+p} + b_{1+p} X^{1+p} + b_3\, X^3 + b_2\, X^2 + b_1\, X$
$b_{1+2\,p}$	$b_{1+2\,p} \in k^\times$
b_{2+p^2}	$b_{2+p^2} \in k^\times$
b_{1+p+p^2}	$b_{1+p+p^2}^p = -2\, b_{1+2\,p}^p\, (b_{2+p^2}^p\, b_{1+2\,p}^{-p^2} + b_{2+p^2}^{p-1})$
$\ell_{1,2}$	$\forall\, y \in V, \quad \ell_{1,2}(y) = 2\, b_{1+2\,p}\, y^{p^2} + b_{1+p+p^2}\, y^p + 2\, b_{2+p^2}\, y$
V	V *is an index p-subgroup of* $Z(\mathrm{Ad}_{f_1})$ $V = Z(2\, b_{1+2\,p}^p\, X^{p^3} + (b_{1+p+p^2}^p - 2\, b_{1+2\,p})\, X^{p^2} + (2b_{2+p^2}^p - b_{1+p+p^2})X^p - 2b_{2+p^2} X)$
a_{1+p}	$a_{1+p}^{p^2} = -b_{1+2\,p}^{p-p^2} - b_{1+2\,p}^p\, b_{2+p^2}^{-1} - b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^3} - b_{2+p^2}^{p^2-p}$
a_2	$2\, a_2^{p^2} = b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^2} + b_{1+2\,p}\, b_{2+p^2}^{-1} + b_{2+p^2}^p\, b_{1+2\,p}^{p-2\,p^2} + 2\, b_{2+p^2}^{p-1}\, b_{1+2\,p}^{p-p^2} + b_{1+2\,p}^p b_{2+p^2}^{p-2}$
$b_{1+2\,p}$	$b_{1+2\,p}^{p^2} = -b_{1+2\,p}^{2\,p-p^2} - b_{1+2\,p}^{2\,p}\, b_{2+p^2}^{-1} + b_{2+p^2}^{2\,p^2}\, b_{1+2\,p}^{p^2-2\,p^3} + 2\, b_{2+p^2}^{2\,p^2-p}\, b_{1+2\,p}^{p^2-p^3} + b_{1+2\,p}^{p^2}\, b_{2+p^2}^{2\,p^2-2\,p}$
b_{2+p}	$b_{2+p}^{p^2} = b_{2+p^2}^p\, b_{1+2\,p}^{2\,p-2\,p^2} + 2\, b_{2+p^2}^{p-1}\, b_{1+2\,p}^{2\,p-p^2} + b_{1+2\,p}^{2\,p}\, b_{2+p^2}^{p-2} - b_{2+p^2}^{2\,p^2}\, b_{1+2\,p}^{-p^3} - b_{2+p^2}^{2\,p^2-p}$
b_3	$3\, b_3^{p^2} = b_{2+p^2}^{2\,p^2}\, b_{1+2\,p}^{-p^2} - b_{2+p^2}^{2\,p}\, b_{1+2\,p}^{2\,p-3p^2} - 3\, b_{2+p^2}^{2\,p-2}\, b_{1+2\,p}^{2\,p-p^2} - 3\, b_{2+p^2}^{2\,p-1}\, b_{1+2\,p}^{2\,p-2\,p^2} - b_{1+2\,p}^{2\,p} b_{2+p^2}^{2\,p-3} + b_{1+2\,p}^2\, b_{2+p^2}^{-1}$
b_{1+p^2}	$b_{1+p^2} \in Z(b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^3}\, X^{p^3} - (b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^3} + b_{1+2\,p}^{p-p^2} + b_{2+p^2}^{p^2-p})\, X^{p^2} +$ $(b_{1+2\,p}^{p-p^2} + b_{1+2\,p}^p\, b_{2+p^2}^{-1} + b_{2+p^2}^{p^2-p})\, X^p - b_{1+2\,p}^p\, b_{2+p^2}^{-1}\, X)$
b_{1+p}	$b_{1+p}^{p^2} = -(b_{1+2\,p}^{p-p^2} + b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^3} + b_{2+p^2}^{p^2-p})\, b_{1+p^2}^{p^2} - b_{1+2\,p}^p\, b_{2+p^2}^{-1}\, b_{1+p^2}$
b_2	$2\, b_2^{p^2} = (b_{2+p^2}^p\, b_{1+2\,p}^{p-2\,p^2} + b_{2+p^2}^{p-1}\, b_{1+2\,p}^{p-p^2-p} + b_{2+p^2}^{p^2}\, b_{1+2\,p}^{-p^2}) b_{1+p^2}^{p^2} +$ $(b_{1+2\,p}^p b_{2+p^2}^{p-2} + b_{2+p^2}^{p-1}\, b_{1+2\,p}^{p-p^2} + b_{1+2\,p}\, b_{2+p^2}^{-1})\, b_{1+p^2}$
b_1	$b_1 \in k$

Therefore, for $p > 3$, the solutions can be parametrized by 3 algebraically independent variables over $\mathbb{F}_p$, namely $b_{1+2\,p^2} \in k^\times$, $b_{2+p^2} \in k^\times$ and $b_1 \in k$. One also finds a fourth parameter b_{1+p^2} which runs over an $\mathbb{F}_p$-vector subspace of k, namely the set of zeroes of an additive separable polynomial whose coefficients are rational functions in $b_{1+2\,p^2}$ and b_{2+p^2}. So, for given $b_{1+2\,p}$ and b_{2+p^2}, the parameter b_{1+p^2} takes a finite number of values.

For $p = 3$,

$f_1(X) =$	$X^{10} + a_4\, X^4 + a_2\, X^2$
$f_2(X) =$	$b_{19}\, X^{19} + b_{13}\, X^{13} + b_{11}\, X^{11} + b_{10}\, X^{10} + b_7\, X^7 + b_5\, X^5 +$ $b_4\, X^4 + b_2\, X^2 + b_1\, X$

with a_4, a_2, b_{13}, b_7, b_5, b_3 and b_2 satisfying the same relations as above. But, this time, the parameters b_{19} and b_{11} are linked through an algebraic relation, namely :

$$b_{11}^{18}\, b_{19}^{-9} - b_{11}^{6}\, b_{19}^{-21} - b_{19}^{6}\, b_{11}^{3} + b_{19}^{2}\, b_{11}^{-1} = 0.$$

In both cases ($p = 3$ or $p > 3$),

$$\frac{|G|}{g} = \frac{2\,p}{p-1}\,\frac{p^2}{1+2\,p} \qquad \textit{and} \qquad \frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p\,(p+1)^2}{(1+2\,p)^2}.$$

Remark 4.5.6. *One can now answer the second problem raised in Chapter 3 (Section 3.6). Indeed, one notices that the family obtained for $s = 2$ is larger than the one obtained after the additive base change : $X = Z^p + c\,Z$, $c \in k - \{0\}$ (see Chapter 2 Prop. 2.3.1) applied to the case $s = 1$. Indeed, such a base change does not produce any monomial Z^{1+p^2} in $f_2(Z)$.*

A few special cases.

1. When $s = 1$ and $p > 3$, the special case $a_2 = 0$ corresponds to the parametrization of the extension K_S^m/K given by Auer (cf . [Au99] Prop. 8.9 or Chapter 2 Section 2.6), namely
   $f_1(X) = a\,X^{1+p}$ with $a^p + a = 0$, $a \neq 0$.
   $f_2(X) = a^2\,X^{2\,p}\,(X - X^{p^2})$.
2. When $s = 2$, the special case $b_{1+p^2} \in \mathbb{F}_p$ leads to $b_{1+p} = b_{1+p^2}\,a_{1+p}$ and $b_2 = b_{1+p^2}\,a_2$. So, one can replace f_2 by $f_2(X) - b_{1+p^2}\,f_1(X)$, which eliminates the monomials X^{1+p^2}, X^{1+p} and X^2.

Proof of Proposition 4.5.5 :

1. As $\ell_{1,2} \neq 0$, the group G satisfies the third condition of Chapter 3 (Prop. 3.5.2). Then, the equality $G = A_{\infty,1}$ derives from Chapter 3 (Cor. 3.5.7). The unicity of the p-Sylow subgroup is explained in Remark 4.3.1. The second and third assertions come from Chapter 3 (Thm. 3.5.6). Moreover, the description of V displayed in (c) is due toChapter 3 (Prop 3.2.9.2). It remains to show that $s = 1$ or $s = 2$. Using formula (4.1), we compute $g = \frac{(p-1)}{2}\,(p^s + p\,(m_2 - 1)) = \frac{(p-1)}{2}\,p^s(1 + 2\,p)$. As $|G| = p^{3+s}$, condition $(*)$ requires : $\frac{4}{(p^2-1)^2} \leq \frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{(p+1)^2}{p^{s-3}\,(1+2\,p)^2}$. It follows that $3 - s > 0$, i.e. $1 \leq s \leq 2$.
2. We merely explain the case $s = 1$. One can find a coordinate X of the projective line C/G_2 such that $f_1(X) = X\,S_1(X) = X\,(X^p + a_2\,X)$ (cf. Chapter 3 Cor. 3.2.12). Then, $\mathrm{Ad}_{f_1} = F^2 + 2\,a_2^p\,F + I$ (cf. Chapter 3 Prop. 3.2.13). As $V \subset Z(\mathrm{Ad}_{f_1})$ and $\dim_{\mathbb{F}_p} Z(\mathrm{Ad}_{f_1}) = 2 = s + 1 = v$, we deduce that $V = Z(\mathrm{Ad}_{f_1})$. As $f_2 \in \Sigma_3 - \Sigma_2$ with $\deg f_2 = 1 + 2\,p^s$ and as the functions f_i's are supposed to be reduced mod $\wp(k[X])$, equation (4.2) reads :

$$\forall\, y \in V, \qquad f_2(X+y) - f_2(X) = \ell_{1,2}(y)\,f_1(X) \qquad \bmod\ \wp(k[X])$$

$$\begin{array}{lll}
\text{with} & f_1(X) = X^{1+p} + a_2\,X^2 & \\
\text{and} & f_2(X) = b_{1+2\,p}\,X^{1+2\,p} + b_{2+p}\,X^{2+p} + b_{1+p}\,X^{1+p} + b_3\,X^3 + b_2\,X^2 + b_1\,X & \text{for } p > 3 \\
\text{(resp.} & f_2(X) = b_{1+2\,p}\,X^{1+2\,p} + b_{2+p}\,X^{2+p} + b_{1+p}\,X^{1+p} + b_2\,X^2 + b_1\,X & \text{for } p = 3)
\end{array}$$

Then, calculation gives the relations gathered in the table. In particular, we find : $f_2(X) = b_{1+2\,p}X^{1+2\,p} + b_{2+p}\,X^{2+p} + b_3\,X^3 + b_1\,X + b_{1+p}\,f_1(X)$ with $b_{1+p} \in \mathbb{F}_p$. Since we are working in the $\mathbb{F}_p$-space generated by $f_1(X)$ and $f_2(X)$, we can replace $f_2(X)$ with $f_2(X) - b_{1+p}\,f_1(X)$, hence the expected formula. We solve the case $s = 2$ in the same way. □

4.5.3 Third case : big actions satisfying $\mathcal{G}_*^{p^3}$.

Preliminaries.

The idea is to use, as often as possible, the results obtained in the preceding section.

Remark 4.5.7. *Let (C, G) be a big action with $G'(= G_2) \simeq (\mathbb{Z}/p\mathbb{Z})^3$. We keep the notations introduced in Section 4.4.3.*

1. *Let $C_{1,2}$ be the curve parametrized by the two equations : $W_i^p - W_i = f_i(X)$, with $i \in \{1, 2\}$, and let $K_{1,2} := k(C_{1,2})$ be the function field of this curve. Then, $K_{1,2}/k(X)$ is a Galois extension with group $\Gamma_{1,2} \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Moreover, the group of translations by V : $\{X \to X + y, y \in V\}$ extends to an automorphism p-group of $C_{1,2}$ say $G_{1,2}$, with the following exact sequence :*

$$0 \longrightarrow \Gamma_{1,2} \longrightarrow G_{1,2} \longrightarrow V \longrightarrow 0.$$

Let $A_{1,2}$ be the $\mathbb{F}_p$-vector subspace of A generated by the classes of $f_1(X)$ and $f_2(X)$. Let $H_{1,2} \subsetneq G_2$ be the orthogonal of $A_{1,2}$ with respect to the Artin-Schreier pairing. Then, $C_{1,2} = C/H_{1,2}$ and $G_{1,2} = G/H_{1,2}$. Furthermore, as $A_{1,2}$ is stable under the action of ρ, its dual $H_{1,2}$ is stable by the dual representation ϕ, i.e. by conjugation by the elements of G (see Section 4.4.3). It follows that $H_{1,2} \subsetneq G_2$ is a normal subgroup in G. So, by Chapter 2 (Lemma 2.2.4), the pair $(C_{1,2}, G_{1,2})$ is a big action with second ramification group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.

2. *Likewise, if $\ell_{2,3} = 0$, the $\mathbb{F}_p$-vector subspace of A generated by the classes of $f_1(X)$ and $f_3(X)$ is also stable by ρ (see matrix $L(y)$ in Section 4.4.3). So, the two equations : $W_i^p - W_i = f_i(X)$, with $i \in \{1, 3\}$, also parametrize a big action, say $(C_{1,3}, G_{1,3})$, with second ramification group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.*
3. *Similarly, if $\ell_{1,2} = \ell_{1,3} = 0$, the $\mathbb{F}_p$-vector subspace of A generated by the classes of $f_2(X)$ and $f_3(X)$ is stable by ρ (see matrix $L(y)$ in Section 4.4.3). So, the two equations : $W_i^p - W_i = f_i(X)$, with $i \in \{2, 3\}$, also parametrize a big action, say $(C_{2,3}, G_{2,3})$, with second ramification group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.*

Lemma 4.5.8. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$. Let $(C_{1,2}, G_{1,2})$ be defined as in Remark 4.5.7. We keep the notations introduced in Section 4.4.3.*

1. *Then, $(C_{1,2}, G_{1,2})$ is a big action satisfying $\mathcal{G}_*^{p^2}$.*
2. *If $\ell_{1,2} = 0$, then $m_1 = m_2 = 1 + p^s$, with $s \geq 2$.*
3. *If $\ell_{1,2} \neq 0$, then $m_1 = 1 + p^s$, $m_2 = 1 + 2\,p^s$, with $s \in \{1, 2\}$ and $p \geq 3$. In this case, $v = s + 1$.*

Proof :

1. Use Remark 4.5.7 and [LM05] (Prop. 8.5 (ii)) to see that condition $(*)$ is still satisfied.
2. We deduce from Proposition 4.5.4 that $m_1 = 1 + p^{s_1}$ and $m_2 = 1 + p^{s_2}$ with $s_2 = s_1$ or $s_2 = s_1 + 1$. Assume that $s_2 = s_1 + 1$. Then, $m_3 \geq m_2 = 1 + p^{s_1+1}$. We compute the genus by means of (4.1) : $g = \frac{p-1}{2}\,(p^{s_1} + p^{1+s_2} + p^2\,(m_3 - 1)) \geq \frac{p-1}{2}\,p^{s_1}\,(1 + p^2 + p^3)$. Besides, by Chapter 2 (Thm. 2.2.6), $V \subset Z(\mathrm{Ad}_{f_1})$, so $|G| = p^{3+v} \leq p^{3+2s_1}$. Thus, $\frac{|G|}{g^2} \leq \frac{4}{(p^2-1)^2}\,\frac{p^3\,(p+1)^2}{(1+p^2+p^3)^2} < \frac{4}{(p^2-1)^2}$, which contradicts condition $(*)$. It follows that $s_2 = s_1 \geq 2$.
3. Apply Proposition 4.5.5 to (C_{12}, G_{12}). □

Remark 4.5.9. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$. Assume that $\ell_{1,2} = \ell_{1,3} = 0$. Then, the results of Lemma 4.5.8 also hold for the big action $(C_{2,3}, G_{2,3})$ as defined in Remark 4.5.7.*

Lemma 4.5.10. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$. We keep the notations introduced in Section 4.4.3. Assume that $\ell_{2,3} = 0$. Let $(C_{1,3}, G_{1,3})$ be defined as in Remark 4.5.7.*

1. *Then, $(C_{1,3}, G_{1,3})$ is a big action satisfying $\mathcal{G}_*^{p^2}$.*
2. *If $\ell_{1,3} = 0$, then $\ell_{1,2} = 0$ and $m_1 = m_2 = m_3 = 1 + p^s$ with $s \geq 2$. In this case, $v = 2\,s$.*
3. *If $\ell_{1,3} \neq 0$, then $m_1 = 1 + p^s$, $m_3 = 1 + 2\,p^s$, with $s \in \{1, 2\}$ and $p \geq 3$. In this case, $v = s + 1$.*

Proof :

1. Use Remark 4.5.7 and [LM05] (Prop. 8.5 (ii)).
2. As $\ell_{1,3} = 0$, we deduce from Proposition 4.5.4 that $m_1 = 1 + p^s$ and $m_3 = 1 + p^{s_3}$ with $s_3 = s$ or $s_3 = s + 1$.
   (a) *We show that $\ell_{1,2} = 0$.*
   Assume that $\ell_{1,2} \neq 0$. Then, Lemma 4.5.8 applied to $(C_{1,2}, G_{1,2})$ implies $m_2 = 1 + 2\,p^s$ with $s \in \{1, 2\}$ and $p \geq 3$. Moreover, $v = s + 1$. As $m_2 \leq m_3$, there are two possibilities :
      i. $s = 1$ *and* $s_3 = s + 1 = 2.$, i.e. $m_1 = 1 + p$, $m_2 = 1 + 2\,p$, $m_3 = 1 + p^2$ and $v = 2$. Then, $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^3\,(p+1)^2}{(1+2\,p+p^3)^2} < \frac{4}{(p^2-1)^2}$, which contradicts condition $(*)$.
      ii. $s = 2$ *and* $s_3 = s + 1 = 3$. i.e. $m_1 = 1 + p^2$, $m_2 = 1 + 2\,p^2$, $m_3 = 1 + p^3$ and $v = 3$. Then, $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^2\,(p+1)^2}{(1+2\,p+p^3)^2} < \frac{4}{(p^2-1)^2}$, which also contradicts condition $(*)$.

   As a consequence, $\ell_{1,2} = 0$.
   (b) *We deduce that $m_1 = m_2 = 1 + p^s$ with $s \geq 2$.*
   Lemma 4.5.8 applied to $(C_{1,2}, G_{1,2})$ implies $m_1 = m_2 = 1 + p^s$ with $s \geq 2$. In particular, $g = \frac{p-1}{2}\,p^s\,(1 + p + p^{2+s_3-s})$ and $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^{3+v-2s}\,(p+1)^2}{(1+p+p^{2+s_3-s})^2}$.

(c) *We show that $v = 2\,s_3$ and conclude that $s_3 = s$.*
Assume that $v \leq 2\,s_3 - 3$. Then, $\frac{|G|}{g^2} < \frac{4}{(p^2-1)^2} \frac{p^{2s_3-2s}\,(p+1)^2}{p^{4+2s_3-2s}} < \frac{4}{(p^2-1)^2}$ which contradicts condition $(*)$. Therefore, $2\,s_3 - 2 \leq v \leq 2\,s \leq 2\,s_3$. Assume that $v \leq 2\,s_3 - 3$. Then, $\frac{|G|}{g^2} < \frac{4}{(p^2-1)^2} \frac{p^{2s_3-2s}\,(p+1)^2}{p^{4+2s_3-2s}} < \frac{4}{(p^2-1)^2}$ which contradicts condition $(*)$. Assume that $v = 2\,s_3 - 1$. So, v is odd and $2\,s_3 - 2 < v \leq 2s \leq 2\,s_3$ implies $s_3 = s$ and $v = 2s - 1$. Then, $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2} \frac{p^2\,(p+1)^2}{(1+p+p^2)^2} < \frac{4}{(p^2-1)^2}$, which is excluded. Now, assume that $v = 2\,s_3 - 2$. Then, $2\,s_3 - 2 = v \leq 2s \leq 2\,s_3$ implies $s_3 = s$ or $s_3 = s + 1$. In the first case, $v = 2s - 2$ and $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2} \frac{p\,(p+1)^2}{(1+p+p^2)^2} < \frac{4}{(p^2-1)^2}$. In the second case, $v = 2s$ and $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2} \frac{p^3\,(p+1)^2}{(1+p+p^3)^2} < \frac{4}{(p^2-1)^2}$. In both cases, we obtain a contradiction. We gather that $v = 2\,s_3$. Applying Chapter 3 (Prop. 3.4.2), we conclude that $s = s_3$.

3. Apply Proposition 4.5.5 to (C_{13}, G_{13}). □

Case : $[G', G] = \mathrm{Fratt}(G') = \{e\}$**.**

Proposition 4.5.11. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$ such that $[G', G] = \{e\}$. We keep the notations introduced in Section 4.4.3.*

1. *Then, $G = A_{\infty,1}$ is a special group of exponent p (resp. p^2) for $p > 2$ (resp. $p = 2$) and order $p^{3+2\,s_1}$. More precisely, G is a central extension of its center $Z(G) = G'$ by the elementary abelian p-group $V = Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2}) = Z(\mathrm{Ad}_{f_3})$:*

$$0 \longrightarrow Z(G) = G' \simeq (\mathbb{Z}/p\mathbb{Z})^3 \longrightarrow G \xrightarrow{\pi} Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2}) = Z(\mathrm{Ad}_{f_3}) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s_1} \longrightarrow 0.$$

Furthermore, G is a p-Sylow subgroup of A, which is normal except when C is birational to the Hermitian curve : $W^q - W = X^{1+q}$, with $q = p^3$.

2. *There exists a coordinate X for the projective line C/G_2, $s \geq 2$, $d \geq 2$ dividing s, and γ_2, γ_3 in $\mathbb{F}_{p^d} - \mathbb{F}_p$ linearly independent over $\mathbb{F}_p$, $b_1 \in k$, $c_1 \in k$ such that :*

f_1	$f_1(X) = X\,S_1(X)$	*with*	$S_1(F) = \sum_{j=0}^{s/d} a_{jd}\,F^{jd} \in k\{F\}$	$a_s = 1$
f_2	$f_2(X) = X\,S_2(X) + b_1\,X$	*with*	$S_2 = \gamma_2\,S_1$	
f_3	$f_3(X) = X\,S_3(X) + c_1\,X$	*with*	$S_3 = \gamma_3\,S_1$	
V	$V = Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2}) = Z(\mathrm{Ad}_{f_3})$			

Therefore, the solutions can be parametrized by $s+4$ algebraically independent variables over $\mathbb{F}_p$, namely the s coefficients of S, $\gamma_2 \in \mathbb{F}_{p^d} - \mathbb{F}_p$, $\gamma_3 \in \mathbb{F}_{p^d} - \mathbb{F}_p$, $b_1 \in k$ and $c_1 \in k$.

Moreover,

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

Proof : As $\ell_{1,2} = \ell_{2,3} = \ell_{1,3} = 0$, the second point of Lemma 4.5.10 first implies $v = 2\,s_3$. Applying Chapter 3 (Prop. 3.4.2), we gather that $s_1 = s_2 = s_3$, that $V = Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2}) = Z(\mathrm{Ad}_{f_3})$ and we get the expected formulas for the functions $f_i's$. Moreover, it follows from Chapter 3 (Prop. 3.4.3 and Rem. 3.4.5) that $G = A_{\infty,1}$ is a special group. The unicity of the p-Sylow subgroup is discussed in Remark 4.3.1. □

Case : $[G', G] \supsetneq \mathrm{Fratt}(G') = \{e\}$**.**

Lemma 4.5.12. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$ such that $[G', G] \neq \{e\}$. We keep the notations introduced in Section 4.4.3. Then, one cannot have $\ell_{1,2} = \ell_{2,3} = 0$.*

Proof : Assume that $\ell_{1,2} = 0$ and $\ell_{2,3} = 0$. Since the representation ρ is non trivial, $\ell_{1,3} \neq 0$. The second point of Lemma 4.5.8 shows that $m_1 = m_2 = 1 + p^s$ with $s \geq 2$. The third point of Lemma 4.5.10 implies that $m_3 = 1 + 2p^s$ with $p \geq 3$ and $s \in \{1, 2\}$. Moreover, $v = s + 1$. As $s \geq 2$, we obtain : $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2} \frac{(p+1)^2\,p^2}{(1+p+2\,p^2)^2} < \frac{4}{(p^2-1)^2}$, hence a contradiction. As a conclusion, either $\ell_{1,2} \neq 0$ or $\ell_{2,3} \neq 0$. □

As a consequence, there are 3 cases to study :

$\ell_{1,2} \neq 0$ and $\ell_{2,3} = 0$ (cf. Proposition 4.5.13).

$\ell_{1,2} = 0$ or $\ell_{2,3} \neq 0$ (cf. Proposition 4.5.14).

$\ell_{1,2} \neq 0$ or $\ell_{2,3} \neq 0$ (cf. Proposition 4.5.15).

Proposition 4.5.13. *Let (C,G) be a big action satisfying $\mathcal{G}_*^{p^3}$ such that $[G',G] \neq \{e\}$. We keep the notations introduced in Section 4.4.3. Assume that $\ell_{1,2} \neq 0$ and $\ell_{2,3} = 0$.*

1. *Then, $p \geq 5$ and there exists a coordinate X for the projective line C/G_2 such that the functions f_i's can be parametrized as follows :*

f_1	$f_1(X) = X^{1+p} + a_2\, X^2$
V	$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{p^2} + 2\, a_2^p\, X^p + X)$

f_2	$f_2(X) = b_{1+2\,p}\, X^{1+2\,p} + b_{2+p}\, X^{2+p} + b_3\, X^3 + b_1\, X$
$b_{1+2\,p}$	$b_{1+2\,p} \in k^\times$
a_2	$2\, a_2^p = -b_{1+2\,p}^{-p}\, (b_{1+2\,p} + b_{1+2\,p}^{p^2}) \Leftrightarrow b_{1+2\,p} \in V$
V	$V = Z(X^{p^2} - b_{1+2\,p}^{-p}\, (b_{1+2\,p} + b_{1+2\,p}^{p^2})\, X^p + X)$
b_{2+p}	$b_{2+p} = -b_{1+2\,p}^p$
b_3	$3\, b_3^p = b_{1+2\,p}^{-p}\, (b_{1+2\,p}^{2\,p^2} - b_{1+2\,p}^2)$
b_1	$b_1 \in k$
$\ell_{1,2}$	$\ell_{1,2}(y) = 2\, (b_{1+2\,p}\, y^p - b_{1+2\,p}^p\, y)$

f_3	$f_3(X) = c_{1+2\,p}\, X^{1+2\,p} + c_{2+p}\, X^{2+p} + c_3\, X^3 + c_1\, X$
$c_{1+2\,p}$	$c_{1+2\,p} \in k^\times$
$c_{1+2\,p}$	$c_{1+2\,p} \in V$, $c_{1+2\,p}$ *and* $b_{1+2\,p}$ $\mathbb{F}_p$*-independent*
c_{2+p}	$c_{2+p} = -c_{1+2\,p}^p$
c_3	$3\, c_3^p = -c_{1+2\,p}^{-p}\, (c_{1+2\,p}^{2\,p^2} + c_{1+2\,p}^2)$
c_1	$c_1 \in k$
$\ell_{1,3}$	$\ell_{1,3}(y) = 2\, (c_{1+2\,p}\, y^p - c_{1+2\,p}^p\, y)$
$\ell_{2,3}$	$\ell_{2,3}(y) = 0$

Therefore, the solutions are parametrized by 4 algebraically independent variables over $\mathbb{F}_p$, namely $b_{1+2\,p} \in k^\times$, $c_{1+2\,p} \in k^\times$, $b_1 \in k$ and $c_1 \in k$.
Moreover,

$$\frac{|G|}{g} = \frac{2\,p}{p-1}\;\frac{p^3}{1+2\,p+2\,p^2} \quad \textit{and} \quad \frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\;\frac{p^3(p+1)^2}{(1+2\,p+2\,p^2)^2}.$$

2. *In this case, $G = A_{\infty,1}$ is the unique p-Sylow subgroup of A.*

Proof :

1. Lemma 4.5.8 first shows that $m_1 = 1 + p^s$, $m_2 = 1 + 2\,p^s$, with $p \geq 3$ and $s \in \{1,2\}$. Moreover, $v = s+1$. As $\ell_{1,2} \neq 0$ and $\ell_{2,3} = 0$, the second point of Lemma 4.5.10 imposes $\ell_{1,3} \neq 0$. Then, Lemma 4.5.10 shows that $m_3 = 1 + 2\,p^s$. If $s = 2$, $m_1 = 1 + p^2$, $m_2 = m_3 = 1 + 2\,p^3$ and $v = 3$. So $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^2\,(p+1)^2}{(1+2\,p+2\,p^2)^2} < \frac{4}{(p^2-1)^2}$, which contradicts condition $(*)$. It follows that $s = 1$. In this case, $m_1 = 1 + p$, $m_2 = m_3 = 1 + 2\,p$, $v = 2$ and $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^3\,(p+1)^2}{(1+2\,p+2\,p^2)^2}$. Therefore, condition $(*)$ is satisfied as soon as $p \geq 5$. The parametrization of the functions f_i's then derives from Proposition 4.5.5. Furthermore, the third condition (cf. Recall 4.2.1-c) imposed on the degree of the functions f_i's requires that the parameters $b_{1+2\,p}$ and $c_{1+2\,p}$ are linearly independent over $\mathbb{F}_p$.
2. The equality $G = A_{\infty,1}$ derives from the maximality of $V = Z(\mathrm{Ad}_{f_1})$ (see Proposition 4.3.2). The unicity of the p-Sylow subgroup is due to Remark 4.3.1. □

Proposition 4.5.14. *Let (C,G) be a big action satisfying $\mathcal{G}_*^{p^3}$ such that $[G',G] \neq \{e\}$. We keep the notations introduced in Section 4.4.3. Assume that $\ell_{1,2} = 0$ and $\ell_{2,3} \neq 0$.*

1. *Then, $p \geq 5$ and there exists a coordinate X for the projective line C/G_2 such that the functions f_i's can be parametrized as follows :*

f_1	$f_1(X) = X^{1+p^2} + a_2\, X^2$

f_2	$f_2(X) = \gamma_2\, (\, X^{1+p^2} + a_2\, X^2) + b_1\, X$
b_1	$b_1 \in k$
γ_2	$\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$
V	$V = Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2}) = Z(X^{p^4} + 2\, a_2^{p^2}\, X^{p^2} + X)$

<u>*First case : $b_1 \neq 0$*</u>

f_3	$f_3(X) = c_{1+2\,p^2}\,X^{1+2\,p^2} + c_{2+p^2}\,X^{2+p^2} + c_{1+p^2}\,X^{1+p^2}$ $+c_{1+p}\,X^{1+p} + c_3\,X^3 + c_2 X^2 + c_1\,X$
$c_{1+2\,p^2}$	$c_{1+2\,p^2} \in k^\times$
a_2	$2\,a_2^{p^2} = -c_{1+2\,p^2}^{-p^2}\,(c_{1+2\,p^2}^{p^4} + c_{1+2\,p^2}) \Leftrightarrow c_{1+2\,p^2} \in V$
V	$V = Z(X^{p^2} - c_{1+2\,p^2}^{-p}\,(c_{1+2\,p^2} + c_{1+2\,p^2}^{p^2})\,X^p + X)$
c_{2+p^2}	$c_{2+p^2} = -c_{1+2\,p^2}^{p^2}$
c_3	$3\,c_3^{p^2} = -c_{1+2\,p^2}^{p^2}\,(3\,c_{1+2\,p^2}^{2\,p^4} + 4\,c_{1+2\,p^2}^{1+p^4} + c_{1+2\,p^2}^2)$
$e := c_{1+p^2} - c_{1+p^2}^{p^2}$	$e \in Z\,((c_{1+2\,p^2}^{p^7-p^3} + 1 + c_{1+2\,p^2}^{p-p^5} + c_{1+2\,p^2}^{p^7+p-p^5-p^3})\,X^{1+p^4}$ $-X^{1+p^2} - X^{p^2} - X - 1)$
b_1	$b_1^{p^5-p^4+p^3-p^2} = -e^{p^3-1}$
c_{1+p}	$c_{1+p}^{p+p^3} = -e^{1+p}$
c_2	$4\,c_2^{p^3\,(p-1)^2\,(p^2+1)} = c_{1+p^2}^{p^3\,(p^2+1)}$ $+(c_{1+2\,p^2}^{p^7-p^3} + 1 + c_{1+2\,p^2}^{p-p^5} + c_{1+2\,p^2}^{p^7+p-p^5-p^3})\,(c_{1+p^2} - c_{1+p^2}^{p^2})^{p^3+p^2+p-1}$
c_1	$c_1 \in k$

Therefore, the solutions can be parametrized by 3 algebraically independent variables over $\mathbb{F}_p$, namely $c_{1+2\,p^2} \in k^\times$, $c_1 \in k$ and $\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$. One also finds a fourth parameter $e := c_{1+p^2} - c_{1+p^2}^{p^2}$ which runs over the set of zeroes of a polynomial whose coefficients are rational functions in $c_{1+2\,p^2}$. So, for a given $c_{1+2\,p^2}$, the parameter e takes a finite number of values.

Second case : $b_1 = 0$

f_3	$f_3(X) = c_{1+2\,p^2}\,X^{1+2\,p^2} + c_{2+p^2}\,X^{2+p^2} + c_3\,X^3$
$c_{1+2\,p^2}$	$c_{1+2\,p^2} \in k^\times$
a_2	$2\,a_2^{p^2} = -c_{1+2\,p^2}^{-p^2}\,(c_{1+2\,p^2}^{p^4} + c_{1+2\,p^2}) \Leftrightarrow c_{1+2\,p^2} \in V$
V	$V = Z(X^{p^2} - c_{1+2\,p^2}^{-p}\,(c_{1+2\,p^2} + c_{1+2\,p^2}^{p^2})\,X^p + X)$
c_{2+p^2}	$c_{2+p^2} = -c_{1+2\,p^2}^{p^2}$
c_3	$3\,c_3^{p^2} = -c_{1+2\,p^2}^{p^2}\,(3\,c_{1+2\,p^2}^{2\,p^4} + 4\,c_{1+2\,p^2}^{1+p^4} + c_{1+2\,p^2}^2)$
c_1	$c_1 \in k$

In this case, the solutions can be parametrized by 3 algebraically independent variables over $\mathbb{F}_p$, namely $c_{1+2\,p^2} \in k^\times$, $c_1 \in k$ and $\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$.

In both cases,

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

2. *Moreover, $G = A_{\infty,1}$ is the unique p-Sylow subgroup of A.*

Proof :

1. (a) *We describe f_1, f_2 and V.*
   Lemma 4.5.8 first implies that $m_1 = m_2 = 1 + p^s$, with $s \geq 2$. More precisely, we deduce from Proposition 4.5.4 that $f_1(X) = X\,S_1(X)$ and $f_2(X) = \gamma_2\,X\,S_1(X) + b_1\,X$, where S_1 is a monic additive polynomial with degree s in F, $b_1 \in k$ and $\gamma_2 \in \mathbb{F}_{p^d} - \mathbb{F}_p$ with d an integer dividing s. Moreover, $v = 2\,s$ and $V = Z(\mathrm{Ad}_{f_1}) = Z(\mathrm{Ad}_{f_2})$.

   (b) *We show that $\ell_{1,3} \neq 0$.*
   Indeed, assume that $\ell_{1,3} = 0$. Then, we deduce from Remark 4.5.9 that $m_3 = 1 + 2\,p^s$, with $s \in \{2, 3\}$ and $p \geq 3$. Moreover, $v = s+1$. As $s \neq 1$, it follows that $s = 2$ and $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\,\frac{p^2\,(p+1)^2}{(1+p+2\,p^2)^2} < \frac{4}{(p^2-1)^2}$, which contradicts condition $(*)$.

   (c) *We show that $f_3 \notin \Sigma_2$.*
   If $f_3 \in \Sigma_2$, the representation ρ is trivial, hence a contradiction. Therefore, $f_3 \notin \Sigma_2$ and one can define an integer $a \leq m_3$ such that X^a is the monomial of f_3 with highest degree among those that do not belong to Σ_2. Since f_3 is assumed to be reduced mod $\wp(k[X])$, then $a \neq 0$ mod p.

(d) *We show that p divides $a-1$.*
Consider the equation :

$$\forall\, y \in V, \quad \Delta_y(f_3) = \ell_{1,3}(y)\, f_1(X) + \ell_{2,3}(y)\, f_2(X) \qquad \mathrm{mod}\ \wp(k[X]), \tag{4.9}$$

where $\ell_{1,3}$ and $\ell_{2,3}$ are non zero linear forms from V to $\mathbb{F}_p$. The monomials of f_3 with degree strictly lower than a belong to Σ_2. So they give linear contributions in $\Delta_y(f_3)$ mod $\wp(k[X])$ (cf. Chapter 3 Lemma 3.3.9). Assume that p does not divide $a-1$. Then, for all y in V, equation (4.9) gives the following equality mod $\wp(k[X])$:

$$c_a(f_3)\, a\, X^{a-1} + \text{lower degree terms} = (\ell_{1,3}(y) + \gamma_2\, \ell_{2,3}(y))\, X^{1+p^s} + \text{lower degree terms}.$$

where $c_a(f_3) \neq 0$ denotes the coefficient of X^a in f_3. If $a-1 > 1+p^s$, then $y=0$ for all y in V and $V = \{0\}$ which is excluded for a big action (cf. Chapter 2 Prop. 2.2.2). If $a-1 < 1+p^s$, then, $\ell_{1,3}(y) + \gamma_2\, \ell_{2,3}(y) = 0$, for all y in V. It follows that $\gamma_2 \in \mathbb{F}_p$, which is another contradiction. So, $a-1 = 1+p^s$ and by equating the corresponding coefficients in (4.9), one gets : $a\, y = \ell_{1,3}(y) + \gamma_2\, \ell_{2,3}(y)$, for all y in V. So, $V \subset \mathbb{F}_p + \gamma_2\, \mathbb{F}_p$ and $v \leq 2$. As $v = 2\, s$, we deduce that $s = 1$, which is a contradiction. Thus, p divides $a-1$ and one can write $a = 1 + \lambda\, p^t$ with $t \geq 1$ and $\lambda \geq 2$, because of the definition of a. We also define $j_0 := a - p^t$.

(e) *We show that $v \geq t+1$.*
By Chapter 3 (Lemma 3.3.11), $p^v \geq m_3 + 1 > m_3 - 1 \geq a - 1 = \lambda\, p^t \geq 2\, p^t$. This implies $v \geq t+1$.

(f) *We show that $j_0 = 1 + p^s$.*
If $j_0 < 1 + p^s$, we gather the same contradiction as the one found in Chapter 3 [proof of Theorem 3.5.6, point 4, with $i = 2$]. Now, assume that $j_0 > 1 + p^s$. As in Chapter 2 [proof of Theorem 2.5.1, point 6], we prove that the coefficient of X^{j_0} in the left-hand side of (4.9) is $T(y)$, where T is a polynomial of $k[X]$ with degree p^t. If $j_0 > 1 + p^s$, then $T(y) = 0$, for all y in V. This implies $V \subset Z(T)$ and $v \leq t$, which contradicts the previous point.

(g) *We show that either $v = t+1$ or $v = t+2$.*
We have already seen that $v \geq t$. As $j_0 = 1 + p^s$, we equate the corresponding coefficients in (4.9) and obtain $T(y) = \ell_{1,3}(y) + \gamma_2\, \ell_{2,3}(y)$, for all y in V. As $\ell_{1,3}(y) \in \mathbb{F}_p$ and $\ell_{2,3}(y) \in \mathbb{F}_p$, we get $T(y)^p - T(y) = \ell_{2,3}(y)\, (\gamma_2^p - \gamma_2)$, with $\gamma_2 \notin \mathbb{F}_p$. Then, for all y in V, $R(y) := \frac{T(y)^p - T(y)}{\gamma_2^p - \gamma_2} = \ell_{2,3}(y) \in \mathbb{F}_p$ and $V \subset Z(R^p - R)$. In particular, $v \leq t+2$.

(h) *We show that $m_3 = a = 1 + p^s + p^t$.*
Assume that $m_3 > a$. Then, by definition of a, $m_3 = 1 + p^{s_3}$ with $s_3 \geq s$. Note that $s_3 \geq s+1$. Otherwise, $m_3 = 1 + p^s = j_0 < a$. On the one hand, $|G| = p^{3+v} = p^{3+2s}$. On the other hand,

$$g = \frac{p-1}{2}\, (p^s + p^{s+1} + p^2(m_3 - 1)) = \frac{p-1}{2}\, p^s\, (1 + p + p^{2+s_3-s}) \geq \frac{p-1}{2}\, p^s\, (1 + p + p^3).$$

Thus, $\frac{|G|}{g^2} \leq \frac{4}{(p^2-1)^2}\, \frac{p^3\, (p+1)^2}{(1+p+p^3)^2} < \frac{4}{(p^2-1)^2}$. This contradicts condition $(*)$, so $m_3 = a$.

(i) *We show that $s = 2$ and $v = 4$. In particular, $\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$.*
We already know that $s \geq 2$ and $v = 2\, s \geq 4$. So, $|G| = p^{3+v} \leq p^7$. Assume that $s \geq 3$. Then, as $t \geq 1$, we get : $g = \frac{p-1}{2}\, (p^s + p^{s+1} + p^2(m_3 - 1)) = \frac{p-1}{2}\, (p^s + p^{s+1} + p^{s+2} + p^{t+2}) \geq \frac{p-1}{2}\, (2\, p^3 + p^4 + p^5)$. It follows that $\frac{|G|}{g^2} \leq \frac{4}{(p^2-1)^2}\, \frac{p\, (p+1)^2}{(2+p+p^2)^2} < \frac{4}{(p^2-1)^2}$, which is a contradiction. So $s = 2$ and $v = 4$. We have previously mentionned that $\gamma_2 \in \mathbb{F}_{p^d} - \mathbb{F}_p$, where d is an integer dividing s. As $s = 2$, the only possibility is $d = 2$.

(j) *We deduce that $t = s = 2$, so $m_3 = 1 + 2\, p^2$ and $p \geq 5$.*
We have seen $v = t+1$ or $v = t+2$, with $t \geq 1$. As $v = 4$, there are two possibilities either $t = 2$ or $t = 3$. If $t = 3$, $|G| = p^7$ and $g = \frac{p-1}{2}\, p^2\, (1 + p + 2\, p^3)$. So, $\frac{|G|}{g^2} \leq \frac{4}{(p^2-1)^2}\, \frac{p^3\, (p+1)^2}{(1+p+2\, p^3)^2} < \frac{4}{(p^2-1)^2}$. Therefore, $t = 2 = s$. In this case, $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\, \frac{p^3\, (p+1)^2}{(1+p+2\, p^2)^2}$ and condition $(*)$ requires $p \geq 5$.

(k) *We gather the parametrization of f_1, f_2 and V.*
As $s = d = 2$, f_1 reads $f_1(X) = X\, S_1(X)$ with $S_1(F) = \sum_j^{s/d} a_{jd}\, F^{jd} = a_0\, I + F^2$, since S_1 is assumed to be monic. Then,

$$f_1(X) = X\, (X^{p^2} + a_2\, X^2) \quad \text{and} \quad f_2(X) = \gamma_2\, X\, (X^{p^2} + a_2\, X^2) + b_1\, X$$

with $a_2 \in k$, $b_1 \in k$ and $\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$. In this case,

$$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{p^4} + +2\, a_2^{p^2}\, X^{p^2} + X).$$

(l) *We show that $f_3 \in \Sigma_4$ but $f_3 \notin \Sigma_4 - \Sigma_3$.*
By Chapter 3 (Thm. 3.3.13), $f_3 \in \Sigma_4$. We now show that f_3 does not have any monomial in $\Sigma_4 - \Sigma_3$. Indeed, as $m_3 = 1 + 2\,p^2$, the possible monomials of f_3 in $\Sigma_4 - \Sigma_3$ are $X^{1+2\,p+p^2}$, X^{2+p+p^2}, X^{3+p^2}, $X^{1+3\,p}$, $X^{2+2\,p}$, X^{3+p} and X^4. Now, equate the coefficients of the monomial $X^{1+p+p^2} \in \Sigma_3$ in each side of (4.9). In the left-hand side, i.e. in $\Delta_y(f_3) \bmod \wp(k[X])$, X^{1+p+p^2} is produced by monomials X^b of f_3 that belong to $\Sigma_4 - \Sigma_3$ and satisfy $b > 1 + p + p^2$. This leaves only two possibilities : $X^{1+2\,p+p^2}$ and X^{2+p+p^2}. In the right-hand side of (4.9), $X^{1+p+p^2} \in \Sigma_3 - \Sigma_2$ does not occur since $\ell_{1,3}(y)\, f_1(X) + \ell_{2,3}(y)\, f_2(X)$ lies in Σ_2. It follows that, for all y in V, $2\, c_{2+p+p^2}\, y^p + 2\, c_{1+2\,p+p^2}\, y = 0$, where c_t denotes the coefficient of the monomial X^t in f_3. As $v = \dim_{\mathbb{F}_p} V = 4$, we deduce that $c_{2+p+p^2} = c_{1+2\,p+p^2} = 0$. We go on this way and equate successively the coefficients of X^{2+p^2}, $X^{1+2\,p}$, X^{2+p} and X^3 to prove that f_3 does not contain any monomial in $\Sigma_4 - \Sigma_3$. Therefore, f_3 reads as follows :

$$f_3(X) = c_{1+2\,p^2}\, X^{1+2\,p^2} + c_{1+p+p^2}\, X^{1+p+p^2} + c_{2+p^2}\, X^{2+p^2} + c_{1+p^2}\, X^{1+p^2} +$$

$$c_{1+2\,p^2}\, X^{1+2\,p} + c_{2+p}\, X^{2+p} + c_{1+p}\, X^{1+p} + c_3\, X^3 + c_2 X^2 + c_1\, X.$$

(m) *We determine f_3.*
We finally have to solve (4.9) with f_1, f_2 and f_3 as described above. Calculation show that $c_{1+p+p^2} = c_{1+2\,p^2} = c_{2+p} = 0$ and that the coefficients a_2, c_{2+p^2} and c_3 can be expressed as rational functions in $c_{1+2\,p^2}$ (see formulas in the table given in the proposition). To conclude, one has to distinguish the cases $b_1 \neq 0$ and $b_1 = 0$. In the first case, b_1, c_{1+p} and c_2 can be expressed as rational functions in c_{1+p^2} whereas $e := c_{1+p^2} - c_{1+p^2}^{p^2}$ belongs to the set of zeroes of a polynomial whose coefficients are rational functions in $c_{1+2\,p^2}$ (see table). When $b_1 = 0$, then $c_{1+p} = 0$, $c_1 = c_{1+p^2}\, a_2$ and $c_{1+p^2} \in \mathbb{F}_{p^2}$. It follows that $f_3(X) = c_{1+2\,p^2}\, X^{1+2\,p^2} + c_{2+p^2}\, X^{2+p^2} + c_3\, X^3 + c_1\, X + c_{1+p^2}\, f_1(X)$. As $\gamma_2 \in \mathbb{F}_{p^2} - \mathbb{F}_p$, $\{1, \gamma_2\}$ is a basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. Write $\epsilon = \epsilon_1 + \epsilon_2\, \gamma_2$, with ϵ_1 and ϵ_2 in $\mathbb{F}_p$. By replacing f_3 with $f_3 - (\epsilon_1\, f_1 + \epsilon_2\, f_2)$, one obtains the expected formula.

2. The equality $G = A_{\infty,1}$ derives from the maximality of $V = Z(\mathrm{Ad}_{f_1})$ (see Proposition 4.3.2). The unicity of the p-Sylow subgroup is due to Remark 4.3.1. □

The last case : $\ell_{1,2} \neq 0$ and $\ell_{2,3} \neq 0$, generalizes the results obtained in Chapter 3 (Section 3.6.2).

Proposition 4.5.15. *Let (C, G) be a big action satisfying $\mathcal{G}_*^{p^3}$ such that $[G', G] \neq \{e\}$. We keep the notations introduced in Section 4.4.3. Assume that $\ell_{1,2} \neq 0$ and $\ell_{2,3} \neq 0$.*

1. *Then, $p \geq 11$ and there exists a coordinate X for the projective line C/G_2 such that the functions f_i's can be parametrized as follows :*

f_1	$f_1(X) = X^{1+p} + a_2\, X^2$
V	$V = Z(\mathrm{Ad}_{f_1}) = Z(X^{p^2} + 2\, a_2^p\, X^p + X)$
f_2	$f_2(X) = b_{1+2\,p}\, X^{1+2\,p} + b_{2+p}\, X^{2+p} + b_3\, X^3 + b_1\, X$
$b_{1+2\,p}$	$b_{1+2\,p} \in k^\times$
a_2	$2\, a_2^p = -b_{1+2\,p}^{-p}\, (b_{1+2\,p} + b_{1+2\,p}^{p^2}) \Leftrightarrow b_{1+2\,p} \in V$
V	$V = Z(X^{p^2} - b_{1+2\,p}^{-p}\, (b_{1+2\,p} + b_{1+2\,p}^{p^2})\, X^p + X)$
b_{2+p}	$b_{2+p} = -b_{1+2\,p}^p$
b_3	$3\, b_3^p = b_{1+2\,p}^{-p}\, (b_{1+2\,p}^{2\,p^2} - b_{1+2\,p}^2)$
$\ell_{1,2}$	$\ell_{1,2}(y) = 2\, (b_{1+2\,p}\, y^p - b_{1+2\,p}^p\, y)$
f_3	$f_3(X) = c_{1+3\,p}\, X^{1+3\,p} + c_{2+2\,p}\, X^{2+2\,p} + c_{1+2\,p}\, X^{1+2\,p} + c_{3+p}\, X^{3+p}$ $+c_{2+p}\, X^{2+p} + c_{1+p}\, X^{1+p} + c_4\, X^4 + c_3\, X^3 + c_2\, X^2 + c_1\, X$
$c_{1+3\,p}$	$3\, c_{1+3\,p} = 2\, b_{1+2\,p}^2$
$c_{2+2\,p}$	$c_{2+2\,p} = -b_{1+2\,p}^{1+p}$
c_{3+p}	$3\, c_{3+p} = 2\, b_{1+2\,p}^{2\,p}$
c_4	$6\, c_4^p = -b_{1+2\,p}^{-p}\, (b_{1+2\,p}^3 + b_{1+2\,p}^{3\,p^2})$
$c_{1+2\,p}$	$c_{1+2\,p} \in V$
c_{2+p}	$c_{2+p} = -c_{1+2\,p}^p$
c_3	$3\, c_3^p = b_{1+2\,p}^{-p}\, (b_{1+2\,p} + b_{1+2\,p}^{p^2})\, (c_{1+2\,p}^{p^2} - c_{1+2\,p})$
c_{1+p}	$c_{1+p} \in k$
b_1	$2\, b_1^p = b_{1+2\,p}^{-p}\, (c_{1+p}^p - c_{1+p})$
c_2	$2\, c_2^p = -b_{1+2\,p}^{-p}\, (c_{1+p}^p\, b_{1+2\,p}^{p^2} + c_{1+p}\, b_{1+2\,p})$
c_1	$c_1 \in k$
$\ell_{1,3}$	$\ell_{1,3}(y) = 2\, (c_{1+2\,p}\, y^p\, c_{1+p}^p - y) + 2\, b_{1+2\,p}^2\, y^{2\,p} - 4\, b_{1+2\,p}^{1+p}\, y^{1+p} + 2\, b_{1+2\,p}^{2\,p}\, y^2$ $= 2\, (c_{1+2\,p}\, y^p - c_{1+p}^p\, y) + \ell_{1,2}^2(y)/2$
$\ell_{2,3}$	$\ell_{2,3}(y) = 2\, (b_{1+2\,p}\, y^p - b_{1+2\,p}^p\, y)$

Therefore, the solutions can be parametrized by 3 algebraically independent variables over $\mathbb{F}_p$, namely $b_{1+2\,p} \in k^\times$, $c_{1+p} \in k$ and $c_1 \in k$. One also finds a fourth parameter $c_{1+2\,p}$ which runs over V. So, for a given $b_{1+2\,p}$, the parameter $c_{1+2\,p}$ takes a finite number of values.
Moreover,

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

2. *$G = A_{\infty,1}$ is the unique p-Sylow subgroup of A. Furthermore, $Z(G)$ is cyclic of order p.*

Proof :

1. In this case, the group G satisfies the third condition of Chapter 3 (Prop. 3.5.2). So, we deduce from Chapter 3 (Thm. 3.5.6) that $m_1 = 1 + p^s$, $m_2 = 1 + 2\,p^s$, $m_3 = 1 + 3\,p^s$ with $p \geq 5$ and $v = s + 1$. Furthermore, it follows from Lemma 4.5.8 that $s \in \{1, 2\}$. Assume that $s = 2$. Then, $|G| = p^6$, $g = \frac{p-1}{2}\, p^2\,(1+2\,p+3\,p^2)$, so $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\, \frac{p^2\,(p+1)^2}{(1+2\,p+3\,p^2)^2} < \frac{4}{(p^2-1)^2}$. This is a contradiction, hence $s = 1$. In this case, $\frac{|G|}{g^2} = \frac{4}{(p^2-1)^2}\, \frac{p^3\,(p+1)^2}{(1+2\,p+3\,p^2)^2}$ and condition $(*)$ is satisfied as soon as $p \geq 11$. Then, we deduce from Proposition 4.5.5 the parametrization of f_1, V and f_2 mentionned in the table. Besides, we deduce from Chapter 3 (Thm. 3.5.6) that f_3 is in $\Sigma_4 - \Sigma_3$ with $m_3 = 1 + 3\,p$. This means that f_3 reads as follows :
$$f_3(X) = c_{1+3\,p}\, X^{1+3\,p} + c_{2+2\,p}\, X^{2+2\,p} + c_{1+2\,p}\, X^{1+2\,p} + c_{3+p}\, X^{3+p}$$
$$+c_{2+p}\, X^{2+p} + c_{1+p}\, X^{1+p} + c_4\, X^4 + c_3\, X^3 + c_2\, X^2 + c_1\, X.$$
We determine the expressions of the coefficient by solving the equation :
$$\forall\, y \in V, \quad \Delta_y(f_3) = \ell_{1,3}(y)\, f_1(X) + \ell_{2,3}\, f_2(X) \qquad \mathrm{mod}\ \wp(k[X])$$
with $\ell_{1,2}(y) = \ell_{2,3}(y) = 2\,(b_{1+2\,p}\, y^p - b_{1+2\,p}^p\, y)$ (cf. Chapter 3, Prop. 3.5.4.1). The results are gathered in the table above.
2. The equality $G = A_{\infty,1}$ derives from Chapter 2 (Cor. 2.5.7). The unicity of the p-Sylow subgroup comes from Remark 4.3.1. The description of the center is due to Chapter 2 (Prop. 2.6.15). □

Bibliographie

[Ab57] S. Abhyankar, *Coverings of algebraic curves.* Amer. J. Math. **79**, (1957), 825–856.

[Au99] R. Auer, *Ray Class Fields of Global Function Fields with Many Rational Places.* Dissertation at the University of Oldenburg, (1999), disponible à `http ://www.bis.uni-oldenburg.de/dissertation/fb06.html`

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

[Be96] J. Bertin, *Compactification des schémas de Hurwitz.* C. R. Acad. Sci. Paris Sér. I Math. **322**, no. 11, (1996), 1063–1066.

[BeMe00] J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques.* Invent. Math. **141**, no. 1, (2000), 195–238.

[BeRo08] J. Bertin, M. Romagny, *Champs d'Hurwitz*, (2008), disponible à `http ://www.math.jussieu.fr/` $\sim$ `romagny/`

[Bor01] N. Borne, *Modules galoisiens sur les courbes : une introduction.* Arithmétique de revêtements algébriques (Saint-Étienne, 2000), 147–159, Sémin. Congr. 5, Soc. Math. France, Paris, (2001).

[Bor06] N. Borne, *Cohomology of G-sheaves in positive characteristic.* Adv. Math. **201**, no. 2, (2006), 454–515.

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

[Bour83] N. Bourbaki, *Algèbre commutative.* Eléments de Mathématiques, Masson, Paris, (1983)

[Br00] T. Breuer, *Characters and automorphism groups of compact Riemann surfaces.* London Mathematical Society Lecture Note Series, 280. Cambridge University Press, Cambridge, (2000).

[BT82] F. R. Beyl, J. Tappe, *Group extensions, representations, and the Schur multiplicator.* Lecture Notes in Mathematics, 958. Springer-Verlag, Berlin-New York, (1982).

[ByCo08] J. Byszewski, G. Cornelissen, *Which weakly ramified group actions admit a universal formal deformation ?* (2008), arXiv :0708.3279, disponible à `http ://front.math.ucdavis.edu/0708.3279`

[Con90] M. Conder, *Hurwitz groups : a brief survey.* Bull. Amer. Math. Soc. (N.S.) **23**, no. 2, (1990), 359-370.

[CoKa03] G. Cornelissen, F. Kato, *Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic*, Duke Math. J. **116**, no. 3, (2003) 431–470.

[CoMe06] G. Cornelissen, A. Mézard, *Relèvements des revêtements de courbes faiblement ramifiés.* Math. Z. **254** no. 2, (2006), 239–255.

[DeMu69] P. Deligne, D. Mumford, *The irreducibility of the space of curves of given genus.* Inst. Hautes Études Sci. Publ. Math. no. **36** (1969), 75–109.

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

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

[FaKa92] H. Farkas, I. Kra, *Riemann surfaces.* Second edition. Graduate Texts in Mathematics, 71. Springer-Verlag, New York, (1992).

[Ga99] M. Garuti, *Linear systems attached to cyclic inertia.* Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., **70**, Amer. Math. Soc., Providence, RI, (2002), 377–386.

[Gi00] P. Gille, *Le groupe fondamental sauvage d'une courbe affine en caractéristique* $p > 0$. Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., 187, Birkhäuser, Basel, (2000), 217–231.

[GK07] M. Giulietti, G. Korchmáros, *On large automorphism groups of algebraic curves in positive characteristic* (2007), arXiv :0706.2320, disponible à `http ://front.math.ucdavis.edu/0706.2320`

[GK08] M. Giulietti, G. Korchmáros, *Nakajima's remark on Henn's proof* (2008), arXiv :0808.4029, disponible à `http ://front.math.ucdavis.edu/0808.4029`

[Go96] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol.35, (Springer, Berlin, 1996)

[GrMa98] B. Green, M. Matignon *Liftings of Galois covers of smooth curves.* Compositio Math. **113**, no. 3, (1998) 237–272.

[Gro57] A. Grothendieck, *Sur quelques points d'algèbre homologique* Tôhoku Math. J. (2) **9** , (1957), 119–221.

[Gro63] A. Grothendieck, *Revêtements étales et groupe fondamental. Fasc. I : Exposés 1 à 5. Séminaire de Géométrie Algébrique, 1960/61.* Troisième édition, corrigée Institut des Hautes Études Scientifiques, Paris (1963).

[GS91] A. Garcia, H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields.* Manuscripta Mat. **72**, no. 1, (1991),67–79.

[Ha40] P. Hall, *The classification of prime-power groups.* J. Reine Angew. Math. **182** (1940), 130–141.

[Han92] J. Hansen, *Deligne-Lusztig varieties and group codes.* Coding theory and algebraic geometry (Luminy, 1991), 63–81, Lecture Notes in Math., 1518, Springer, Berlin, (1992).

[HaPe93] J. P. Hansen, J. P. Pedersen *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields.* J. Reine Angew. Math. **440**, (1993), 99–109.

[Har94] D. Harbater, *Abhyankar's conjecture on Galois groups over curves.* Invent. Math. **117**, no. 1, (1994), 1–25.

[Har03] D. Harbater, *Patching and Galois theory.* Galois groups and fundamental groups, 313–424, Math. Sci. Res. Inst. Publ. 41, Cambridge Univ. Press, Cambridge, (2003).

[HarSt99] D. Harbater, K. Stevenson, *Patching and thickening problems.* J. Algebra **212** no. 1, (1999), 272–304.

[Hen78] H. W. Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew Math **302** (1978), 96–115.

[HKT08] J. Hirschfeld, G. Korchmáros, F.Torres, *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[Hu67] B. Huppert, *Endliche Gruppen. I.*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York (1967)

[Hur92] A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich.* Math. Ann. **41**, no. 3, (1892), 403–442

[Ka86] N. Katz, *Local-to-global extensions of representations of fundamental groups.* Ann. Inst. Fourier (Grenoble) **36**, no. 4, (1986), 69-106.

[KaMa85] N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves. Annals of Mathematics Studies,* 108. Princeton University Press, Princeton, NJ, (1985).

[Kl79] F. Klein, *Über die Transformationen siebenter Ordnung der elliptischen Functionen.* Math. Annalen **14**, (1879), 428-471.

[Kon06] A. Kontogeorgis, *Polydifferentials and the deformation functor of curves with automorphisms.* J. Pure Appl. Algebra **210** , no. 2, (2007), 551–558.

[Kon07] A. Kontogeorgis, *On the tangent space of the deformation functor of curves with automorphisms.* Algebra & Number Theory **1** , no. 2, (2007) 119–161.

[Ku91] R. Kulkarni, *Riemann surfaces admitting large automorphism groups.* Extremal Riemann surfaces (San Francisco, CA, 1995), 63–79, Contemp. Math., 201, Amer. Math. Soc., Providence, RI, (1997).

[KuKi90] A. Kuribayashi, H. Kimura, *Automorphism groups of compact Riemann surfaces of genus five,* J. Algebra **134** , no. 1, (1990), 80–103.

[Lar01] M. Larsen, Michael, *How often is* $84(g-1)$ *achieved ?*, Israel J. Math. **126**, (2001), 1–16.

[Lau99] K. Lauter, *A Formula for Constructing Curves over Finite Fields with Many Rational Points*, Journal of Number Theory **74**, no. 1, (1999), 56–72.

[LGM02] C.R. Leedham-Green, S. McKay, *The structure of groups of prime power order.* London Mathematical Society Monographs. New Series, 27. Oxford Science Publications. Oxford University Press, Oxford, (2002).

[Leo96] H-W Leopoldt, *Über die Automorphismengruppe des Fermatkörpers,* J. Number Theory **56**, no. 2, (1996), 256–282.

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, (2002).

[LM05] C. Lehr, M. Matignon, *Automorphism groups for p-cyclic covers of the affine line.* Compositio Math. **141** , no. 5,(2005), 1213–1237.

[LM06a] C. Lehr, M. Matignon, *Wild monodromy and automorphisms of curves.* Duke Math. J. **135**, no. 3, (2006), 569–586.

[LM06b] C. Lehr, M. Matignon, *Maximal wild monodromy in unequal characteristic*, (2006) preprint disponible à `http ://www.math.u-bordeaux1.fr/∼ matignon/`

[Ma06] M. Matignon, *Semi-stable reduction and wild monodromy*, beamer slides version of a lecture given for MariusFest (Groningen, April 2007), availabale at `http ://www.math.u-bordeaux1.fr/ ∼ matignon/`

[Mar71] M. Marshall, *Ramification groups of abelian local field extensions.* Canad. J. Math. **23** (1971), 271–281

[Mau08] S. Maugeais, *Espaces des modules des courbes équivariantes et torseurs*, (2008), arXiv :0803.4399, disponible à `http ://front.math.ucdavis.edu/0803.4399`

[Mc61] A.M. Macbeath, *On a theorem of Hurwitz.* Proc. Glasgow Math. Assoc. **5** 90-96 (1961).

[Mc65] A.M. Macbeath, *On a curve of genus* 7. Proc. London Math. Soc. (3) **15** (1965), 527-542 .

[Mi80] J. S. Milne, *Etale cohomology*, Princeton Mathematical Series, 33, Princeton University Press, (Princeton, N.J., 1980)

[MR08] M. Matignon, M. Rocher, *On smooth curves endowed with a large automorphism p-group in characteristic* $p > 0$ Algebra Number Theory 2, n° 8, (2008), 887–926

[MSSV02] K. Magaard, T. Shaska, S. Shpectorov, H. Völklein, *The locus of curves with prescribed automorphism group.* Communications in arithmetic fundamental groups (Kyoto, 1999/2001). Sūrikaisekikenkyūsho Kōkyūroku no. 1267 (2002), 112–141, disponible à `http ://arxiv.org/abs/math/0205314`

[Na87a] S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. **303**, no. 2, (1987), 595–607.

[Na87b] S. Nakajima, *On abelian automorphism groups of algebraic curves.* J. London Math. Soc. (2) **36**, no. 1, (1987) 23–32.

[Oo85] F. Oort, *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero.* Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), 165–195, Proc. Sympos. Pure Math., 46, Part 2, Amer. Math. Soc., Providence, RI, 1987.

[OSS89] F. Oort, T. Sekiguchi, N. Suwa, *On the deformation of Artin-Schreier to Kummer.* Ann. Sci. École Norm. Sup. (4) **22**, no. 3, (1989), 345–375.

[PaSt00] A. Pacheco, K. Stevenson, *Finite quotients of the algebraic fundamental group of projective curves in positive characteristic.* Pacific J. Math. **192** , no. 1, (2000), 143–158.

[Pr02] R. Pries, *Families of wildly ramified covers of curves.* Amer. J. Math. **124** , no. 4, (2002), 737–768.

[Pr05] R. Pries, *Equiramified deformations of covers in positive characteristic*, math.AG/0403056, (2005), disponible à http ://front.math.ucdavis.edu/0403.5056

[Pr06] R. Pries, *Wildly ramified covers with large genus.* J. Number Theory **119** , no. 2, (2006), 194–209.

[PrOb08] R. Pries, A. Obus, *Wild cyclic-by-tame extensions.* (2008), arXiv :0807.4790 , disponible à `http ://front.math.ucdavis.edu/0807.4790`

[Ray94] M. Raynaud, *Revêtements de la droite affine en caractéristique* $p > 0$ *et conjecture d'Abhyankar.* Invent. Math. **116** , no. 1-3, (1994), 425–462

[Ro08] M. Rocher, *Large p-group actions with $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$*, arXiv :0804.3494, (2008)

[Ro09] M. Rocher, *Large p-group actions with a p-elementary abelian derived group.* Journal of Algebra **321** (2009), 704–740

[Roq70] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik.* Math. Z. **117**, (1970), 157–163.

[Sch38] H. L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharacteristik*, J. Reine Angew. Math. **179**, (1938), 5–15

[Se60] J-P. Serre, *Rigidité du foncteur de Jacobi d'échelon $n \geq 3$*, appendice à l'exposé 17 du séminaire Cartan (1960-1961).

[Se68] J-P. Serre, *Corps locaux.* Deuxième édition. Hermann, Paris, (1968).

[Se92] J-P. Serre, *Topics in Galois theory.* Lecture notes prepared by Henri Darmon. With a foreword by Darmon and the author. Research Notes in Mathematics, 1. Jones and Bartlett Publishers, Boston, MA, (1992.)

[Si86] J. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[SiZa05] A. Silverberg, Y. Zarhin, *Inertia groups and abelian surfaces.* J. Number Theory **110**, no. 1, (2005), 178–198.

[Sin74] B. Singh, *On the group of automorphisms of function field of genus at least two*, J. Pure Appl. Algebra **4**, (1974), 205–229.

[St73] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionkorpers von Primzahlcharakteristik I, II*, Arch. Math. (Basel) **24** (1973), 527–544, 615–631.

[St93] H. Stichtenoth, *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, (1993).

[Su82] M. Suzuki, *Group Theory I.* Grundlehren der Mathematischen Wissenschaften , 247. (Springer-Verlag, Berlin-New York, 1982.)

[Su86] M. Suzuki, *Group theory. II.* Grundlehren der Mathematischen Wissenschaften, 248. Springer-Verlag, New York, (1986)

[Tu93] S. Tufféry, *Déformations de courbes avec action de groupe.* Forum Math. **5**, no. 3, (1993), 243–259.