Inertia Groups and Jacobian Varieties

Pierre Chrétien

UNIVERSITÉ DE BORDEAUX

Université de Bordeaux
École doctorale EDMI de Bordeaux

Groupes d'Inertie et Variétés Jacobiennes

Inertia Groups and Jacobian Varieties

THÈSE

soutenue publiquement le 13 Juin 2013

pour l'obtention du

Doctorat de l'Université de Bordeaux
(spécialité mathématiques pures)

par

Pierre CHRÉTIEN

Rapporteurs :

BOUW Irene	Professeur
PERRET Marc	Professeur

Composition du jury :

COUVEIGNES Jean-Marc	Professeur (Président)
MATIGNON Michel	Professeur (Directeur)
PERRET Marc	Professeur
ROMAGNY Matthieu	Professeur

Numéro d'ordre : 4875

Institut de Mathématiques de Bordeaux UMR 5251

Inertia Groups and Jacobian Varieties

Groupes d'Inertie et Variétés Jacobiennes

Thèse de Mathématiques pures
13 Juin 2013

RÉSUMÉ

Soient k un corps algébriquement clos de caractéristique $p > 0$ et C/k une courbe projective, lisse, intègre de genre $g > 1$ munie d'un p-groupe d'automorphismes G tel que $|G| > \frac{2p}{p-1}g$. Le couple (C, G) est appelé *grosse action*. Si (C, G) est une grosse action, alors $|G| \leqslant \frac{4p}{(p-1)^2}g^2$ (*). Dans cette thèse, nous étudions les répercussions arithmétiques des propriétés géométriques de grosses actions. Nous étudions d'abord l'arithmétique de l'extension de monodromie sauvage maximale de courbes sur un corps local K d'inégale caractéristique p à corps résiduel algébriquement clos, de genre arbitrairement grand ayant pour potentielle bonne réduction une grosse action satisfaisant le cas d'égalité de (*). On étudie en particulier les conducteurs de Swan attachés à ces courbes. Nous donnons ensuite les premiers exemples, à notre connaissance, de grosses actions (C, G) telles que le groupe dérivé $D(G)$ soit non abélien. Ces courbes sont obtenues comme revêtements de S-corps de classes de rayons de $\mathbb{P}^1_{\mathbb{F}_q}$ pour $S \neq \emptyset$ un sous-ensemble fini de $\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q)$. Enfin, on donne une méthode de calcul des S-corps de classes de Hilbert de revêtements abéliens de la droite projective d'exposant p et supersinguliers que l'on illustre pour des courbes de Deligne-Lusztig.

Mots-clés : Réduction semi-stable, exposant du conducteur, corps de classes de rayons, automorphismes.

ABSTRACT

Let k be an algebraically closed field of characteristic $p > 0$ and C/k be a projective, smooth, integral curve of genus $g > 1$ endowed with a p-group of automorphisms G such that $|G| > \frac{2p}{p-1}g$. The pair (C, G) is called *big action*. If (C, G) is a big action, then $|G| \leqslant \frac{4p}{(p-1)^2}g^2$ (*). In this thesis, one studies arithmetical repercussions of geometric properties of big actions. One studies the arithmetic of the maximal wild monodromy extension of curves over a local field K of mixed characteristic p with algebraically closed residue field, with arbitrarily high genus having for potential good reduction a big action achieving equality in (*). One studies the associated Swan conductors. Then, one gives the first examples, to our knowledge, of big actions (C, G) with non abelian derived group $D(G)$. These curves are obtained as coverings of S-ray class fields of $\mathbb{P}^1_{\mathbb{F}_q}$ where $S \neq \emptyset$ is a finite subset of $\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q)$. Finally, one describes a method to compute S-Hilbert class fields of supersingular abelian covers of the projective line having exponent p and one illustrates it for some Deligne-Lusztig curves.

Keywords : Semi-stable reduction, conductor exponent, ray class fields, automorphisms.

Institut de Mathématiques de Bordeaux, UMR 5251
351, cours de la Libération - F 33405 TALENCE cedex

À mes parents.

"Le plus grand dérèglement de l'esprit, c'est de croire les choses parce qu'on veut qu'elles soient, et non parce qu'on a vu qu'elles sont en effet."
J. Bossuet

REMERCIEMENTS

Ma gratitude va tout d'abord à Michel Matignon grâce à qui j'ai pu faire les mathématiques que j'aime pendant ces années sous sa direction. Sa disponibilité et sa culture mathématique inépuisables ont été pour moi le soutien indispensable au bon déroulement de mes premières armes dans le monde de la recherche. La confiance sans bornes que j'ai en lui n'a jamais été déçue, pour cela aussi je tiens à le remercier.

Mes remerciements vont ensuite à Irene Bouw et Marc Perret qui ont bien voulu être les rapporteurs de cette thèse en dépit de leurs obligations respectives. Je remercie également Jean-Marc Couveignes et Matthieu Romagny qui m'ont fait le plaisir d'accepter d'être membre de mon jury.

Je voudrais remercier les enseignants-chercheurs de l'institut de mathématiques de Bordeaux que j'ai rencontrés à l'occasion des séminaires et ceux avec qui j'ai travaillé à la préparation d'enseignements. Merci à Andreas Enge grâce à qui j'ai pu assister à un des fameux séminaires d'Oberwolfach et à tous les membres de l'équipe LFANT. J'aimerais aussi remercier Jean Fresnel pour son aide continue durant mes années d'études.

Merci aux doctorants de l'institut que j'ai côtoyés pendant ces années de thèse. Merci à Pierre, Zoé, Aurel, Nicolas, Bruno, Nicola, Samuel, Giovanni, Andrea, Sophie, Raphael, Enea, Alan et à tous ceux que j'aurais oubliés. J'ai une pensée particulière pour Aurélien, Nicolas, Arthur et Louis avec qui j'ai passé de nombreuses années à Bordeaux et qui sont des amis fidèles entre tous.

Je remercie chaleureusement mes amis proches en dehors du laboratoire avec lesquels j'ai d'excellents souvenirs. Merci donc à Vincent, Yannick, Charles, Diane, Cécile et Véronique.

Je voudrais remercier le docteur Clément Tournier grâce à qui je marche à nouveau aujourd'hui. Les mots ne peuvent que me manquer pour exprimer ma gratitude envers lui.

Je remercie mes parents pour leur amour et leur soutien indéfectibles et inconditionnels. J'ai mis toute ma confiance en vous, j'espère que vous êtes fiers de moi parce que moi, je suis fier de vous avoir à mes côtés.

PLAN DE LA THÈSE

Les chapitres de cette thèse sont présentés dans l'ordre logique et chronologique où les différents centres d'intérêt sont apparus. On y aborde différents thèmes de géométrie arithmétique, avec des colorations plus ou moins arithmétiques ou géométriques, tous étant liés à l'étude de p-groupes d'automorphismes de courbes en caractéristique $p > 0$. Soient k un corps algébriquement clos de caractéristique $p > 0$ et C/k une courbe projective, lisse, intègre de genre $g > 1$ munie d'un p-groupe d'automorphismes G tel que $|G| > \frac{2p}{p-1}g$. Le couple (C, G) est appelé *grosse action*. En particulier, nous étudions les répercussions arithmétiques des propriétés géométriques de grosses actions.

Dans les paragraphes suivants, on présente le contenu des différents chapitres de cette thèse.

Prérequis.

Ce chapitre est une compilation de résultats nécessaires à la lecture de la thèse mais n'est en aucun cas une introduction aux différents domaines mis en jeu. On a préféré donner systématiquement des références bibliographiques.

Monodromie maximale sauvage en inégale caractéristique.

Ce chapitre reprend le contenu de [CM13], paru au Journal of Number Theory.

Le théorème de réduction semi-stable des courbes dit que pour une courbe C projective, lisse, intègre de genre $\geqslant 2$ sur un corps local K d'inégale caractéristique p et à corps résiduel k algébriquement clos, il existe une unique extension finie M/K minimale pour l'inclusion sur laquelle C acquiert réduction semi-stable. L'extension M/K est appelée *extension de monodromie* de C/K et $\mathrm{Gal}(M/K)$ agit fidèlement sur la réduction stable de $C_M := C \times_K M$. En particulier, on voit $\mathrm{Gal}(M/K)$ comme groupe d'automorphismes d'une courbe semi-stable en caractéristique p. Il existe des bornes en fonction du genre sur la taille d'un p-groupe d'automorphismes d'une courbe projective, lisse, intègre en caractéristique $p > 0$. Quand on considère la partie *sauvage* de l'extension de monodromie, ces bornes induisent des majorations sur le degré de l'extension de monodromie sauvage d'une courbe projective, lisse, intègre C/K ayant potentiellement bonne réduction.

Dans ce chapitre on s'intéresse à la réalisation de courbes projectives, lisses, intègres C/K, pour un corps local K d'inégale caractéristique p bien choisi, de genre arbitrairement grand, telles que la réduction stable de C_M soit lisse, munie d'un p-groupe d'automorphismes aussi gros que possible pour son genre et telles que le groupe de Galois de l'extension de monodromie sauvage soit égal à ce p-groupe d'automorphismes. Autrement dit, dans le cas de potentielle bonne réduction, on réalise les plus grosses monodromies sauvages possibles pour les genres considérés.

Plus précisément, soit k un corps algébriquement clos de caractéristique $p > 0$ et $W(k)$ son anneau des vecteurs de Witt. On étudie le cas où K est une extension finie modérée de $\mathrm{Frac}(W(k))$ et la courbe projective, lisse, intègre C/K est un revêtement p-cyclique $\phi : C \to \mathbb{P}^1_K$ de $\mathbb{P}^1_K$ dont le lieu de branchement est K-rationnel avec *géométrie équidistante*. Dans le cas p-cyclique, cette condition de géométrie équidistante est l'hypothèse sur le

diviseur de branchement du Théorème 1′ de [Ray90] qui assure que le graphe dual de la réduction stable de C_M est un arbre. La géométrie équidistante du branchement a aussi des conséquences sur l'action du groupe de Galois de l'extension de monodromie M/K de C/K sur la réduction stable de C_M. Soient $\mathcal{C}$ le modèle stable de C_M/M et $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ le sous-groupe de $\mathrm{Aut}_k(\mathcal{C}_k)$ des automorphismes agissant trivialement sur la réduction dans $\mathcal{C}_k$ du lieu de branchement de $\phi_M = \phi \times \mathrm{Id}_M : C_M \to \mathbb{P}^1_M$. On montre qu'on a une injection

$$\mathrm{Gal}(M/K) \hookrightarrow \mathrm{Aut}_k(\mathcal{C}_k)^\#.$$

Soit v_p la valuation p-adique sur $\mathbb{Z}$. Quand $v_p(|\mathrm{Gal}(M/K)|) = v_p(|\mathrm{Aut}_k(\mathcal{C}_k)^\#|)$, on dit que C/K *a monodromie sauvage maximale*. Quand C_M a bonne réduction, le lieu de branchement de ϕ_M se spécialise en un unique point de $\mathcal{C}_k$ noté ∞ et $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ est le sous-groupe de $\mathrm{Aut}_k(\mathcal{C}_k)$ des automorphismes fixant ∞. La courbe $\mathcal{C}_k$ est alors un revêtement p-cyclique de $\mathbb{P}^1_k$ de genre $g(C) = g(\mathcal{C}_k)$, ramifié en un point ∞ et étale en dehors de ∞.

Soit X/k un revêtement p-cyclique de $\mathbb{P}^1_k$ de genre $g(X)$, ramifié en un point ∞ et étale en dehors de ∞. D'après [Sti73], le p-sous-groupe de Sylow $G_{\infty,1}(X)$ du sous-groupe des k-automorphismes de X fixant ∞ vérifie $|G_{\infty,1}(X)| \leqslant \frac{4p}{(p-1)^2} g(X)^2$. La courbe projective, lisse X/k d'équation $w^p - w = t^{1+q}$ avec $q = p^n$, $n \geqslant 1$, munie du p-groupe d'automorphismes $G_{\infty,1}(X)$ est telle que $|G_{\infty,1}(X)| = \frac{4p}{(p-1)^2} g(X)^2$.

Nous étudions donc des courbes projectives, lisses, intègres C/K avec K extension finie modérée de $\mathrm{Frac}(W(k))$, ayant monodromie sauvage maximale, telles que $C \to \mathbb{P}^1_K$ soit un revêtement p-cyclique dont le lieu de branchement est K-rationnel avec géométrie équidistante qui ont potentielle bonne réduction $\mathcal{C}_k$ donnée par $w^p - w = t^{1+q}$ pour un certain $q = p^n$, $n \geqslant 1$. Ainsi, dans le cas de potentielle bonne réduction, on réalise les plus grosses monodromies sauvages possibles pour les genres g arbitrairement grands considérés, i.e. $g \in \frac{p-1}{2} p^{\mathbb{N}}$.

Comme corollaire de ces résultats, on construit des familles d'extensions galoisiennes de corps locaux d'inégale caractéristique p de groupe un p-groupe extra-spécial. En effet, le p-sous-groupe de Sylow $G_{\infty,1}(\mathcal{C}_k)$ de $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ où $\mathcal{C}_k$ est donnée par $w^p - w = t^{1+q}$ pour un certain $q = p^n$, $n \geqslant 1$, est un p-groupe extra-spécial d'ordre pq^2.

Un autre point développé dans ce chapitre est l'étude de l'arithmétique de l'extension de monodromie M/K des exemples considérés. Soit $G := \mathrm{Gal}(M/K)$ le *groupe de monodromie* de C/K, il existe une suite décroissante de sous-groupes G_i de G, $i \geqslant 0$ appelée *filtration de ramification inférieure de* G. Dans les situations que nous considérons, la jacobienne $J := \mathrm{Jac}(C)$ de C/K a potentielle bonne réduction et dans ce cas $M = K(J[\ell])$ pour $\ell \geqslant 3$ premier et distinct de p. On définit *le conducteur de Swan de* J/K par

$$\mathrm{sw}(J/K) = \sum_{i \geqslant 1} \frac{|G_i|}{|G_0|} \dim_{\mathbb{F}_\ell} J[\ell]/J[\ell]^{G_i},$$

et *l'exposant du conducteur de* J/K défini, pour ℓ suffisament grand, par

$$f(J/K) = \mathrm{sw}(J/K) + \dim_{\mathbb{F}_\ell} J[\ell]/J[\ell]^G.$$

On détermine la filtration de ramification des extensions de monodromie rencontrées ainsi que les exposants du conducteur et les conducteurs de Swan correspondants.

Dans la seconde partie de ce chapitre, on s'intéresse à la réduction stable des courbes hyperelliptiques C/K de genre 2 en inégale caractéristique 2, toujours sous la condition de géométrie équidistante K-rationnelle, mais non nécessairement avec potentielle bonne réduction. Dans ce cadre, il y a trois types de géométrie pour le modèle semi-stable de C_M déployant le lieu de branchement de ϕ_M. Pour chacun de ces types, on donne un exemple de courbe hyperelliptique ayant ce type de réduction avec monodromie sauvage maximale et, quand cela est possible, on étudie l'arithmétique de son extension de monodromie.

Comme corollaires, on obtient des familles d'extensions galoisiennes de corps locaux d'inégale caractéristique 2 de groupe un 2-groupe. On construit des solutions au problème inverse de Galois pour le 2-groupe extra-spécial $D_8 * Q_8$, pour $Q_8 \times Q_8$ et pour $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ où Q_8 est le groupe des quaternions, D_8 est le groupe dihédral et où $\mathbb{Z}/2\mathbb{Z}$ agit sur $Q_8 \times Q_8$ par permutation des facteurs.

Relèvements de revêtements p-cycliques avec monodromie sauvage maximale.

Ce chapitre reprend le contenu de [Chr13], à paraître à Manuscripta Mathematica.

Les résultats du chapitre précédent peuvent être vus comme solutions d'un raffinement du problème de relèvement d'une courbe projective, lisse en caractéristique $p > 0$. Plus précisément, soient k un corps algébriquement clos de caractéristique $p > 0$ et C/k une courbe projective, lisse, intègre munie d'un p-groupe d'automorphismes G, peut-on trouver une extension finie K de $\mathrm{Frac}(W(k))$ et une courbe projective, lisse, intègre $\mathcal{C}/K$ ayant potentielle bonne réduction isomorphe à C/k avec un groupe de monodromie sauvage isomorphe à G ? Avec ce point de vue, le chapitre précédent donne une réponse positive quand C/k est la courbe projective, lisse d'équation $w^p - w = t^{1+q}$ où $q = p^n$, $n \geqslant 1$ et G est le p-sous-groupe de Sylow du sous-groupe de $\mathrm{Aut}_k(C)$ des automorphismes laissant fixe le point au-dessus de $t = \infty$.

D'après [Sti73], pour C/k une courbe projective, lisse, intègre et pour tout point x de C, l'ordre du p-sous-groupe de Sylow $G_1(x)$ du groupe d'inertie $G(x)$ en x satisfait $|G_1(x)| \leqslant \frac{4p}{(p-1)^2} g(C)^2$. D'après [LM05], les grosses actions (C, G) telles que $|G| = \frac{4p}{(p-1)^2} g(C)^2$ sont données par $w^p - w = tR(t)$ avec $R(t) \in k[t]$ additif et G est le p-sous-groupe de Sylow $G_{\infty,1}(C)$ du sous-groupe des k-automorphismes de C fixant le point au-dessus de $t = \infty$. La réduction stable obtenue au chapitre précédent correspond donc à une courbe particulière de cette famille et il est alors naturel de se demander si on peut étendre les résultats qu'on a montré dans le premier chapitre à toutes les courbes de cette famille.

On montre dans ce chapitre que pour toute courbe projective, lisse C/k définie par $w^p - w = tR(t)$ où $R(t)$ est un polynôme additif, en notant G le p-sous-groupe de Sylow du sous-groupe de $\mathrm{Aut}_k(C)$ des automorphismes laissant fixe le point au-dessus de $t = \infty$, il existe une extension finie modérée K de $\mathrm{Frac}(W(k))$ et une courbe $\mathcal{C}/K$ ayant potentielle bonne réduction isomorphe à C/k avec un groupe de monodromie sauvage isomorphe à G. De plus, on détermine la filtration de ramification de l'extension de monodromie sauvage de $\mathcal{C}/K$ et on calcule les exposants du conducteur et les conducteurs de Swan qui lui sont attachés.

Grosses actions ayant un groupe dérivé non abélien.

Le contenu de ce chapitre a donné lieu a un article soumis.

Les grosses actions ont été étudiées par C. Lehr et M. Matignon puis par M. Matignon et M. Rocher, voir [LM05], [MR08] et [Roco9]. Les exemples de grosses actions (C, G) qui sont présentés dans ces articles sont tous tels que le groupe dérivé de G est abélien. Une des méthodes utilisées pour produire de telles grosses actions est de les construire comme p-groupes d'automorphismes associés à des corps de classes de rayons.

Dans ce chapitre on construit les premiers exemples, à notre connaissance, de grosses actions avec un groupe dérivé non abélien. Ces exemples sont obtenus comme revêtements explicites de corps de classes de rayons de $\mathbb{P}^1_{\mathbb{F}_q}$ qui sont des généralisations des équations de la courbe de Ree.

S-Corps de classes de rayons des courbes de Deligne-Lusztig.

Le contenu de ce chapitre est une présentation de travaux en cours.

Les courbes hermitiennes, de Suzuki et de Ree sont les trois familles de courbes de Deligne-Lusztig. Ce sont toutes des S-corps de classes de rayons de $\mathbb{P}^1_{\mathbb{F}_q}$ pour q convenable avec $S \neq \emptyset$, un sous-ensemble de $\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q)$. En particulier la courbe de Ree est un S-corps de classes de rayons de $\mathbb{P}^1_{\mathbb{F}_q}$ d'équations

$$X_R/\mathbb{F}_q : \begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x), \end{cases}$$

avec $q_0 := 3^s$, $q := 3q_0^2$ et $S = \{(x - a), a \in \mathbb{F}_q\}$. De plus $\mathbb{F}_q(x, y_1)$ est un S-corps de classes de rayons de $\mathbb{P}^1_{\mathbb{F}_q}$.

On aimerait savoir si $\mathbb{F}_q(x, y_1, y_2)$ est un S-corps de classes de rayons de $\mathbb{F}_q(x, y_1)$. Cela soulève donc la question de calculer des S-corps de classes de Hilbert de courbes de genre élevé. D'une part, il existe des méthodes pour produire des S-corps de classes de rayons de genre arbitrairement grand de $\mathbb{P}^1_{\mathbb{F}_q}$ et d'autre part on a des algorithmes pour calculer des S-corps de classes de rayons de courbes $C/\mathbb{F}_q$ qui restent valides quand le genre $g(C)$ de C est non nul. Néanmoins, les seuls résultats pour $g(C) > 0$ sont, à notre connaissance, tels que $g(C) \leqslant 5$ pour $q = p^s$ avec $s \leqslant 4$ et $p \leqslant 3$ ou bien pour $q = 2$ auquel cas on peut produire des exemples avec $g(C) \leqslant 50$. En particulier, les méthodes existantes étaient inadaptées au calcul de S-corps de classes de Hilbert des courbes de Deligne-Lusztig.

Dans ce chapitre on décrit une méthode de calcul des S-corps de classes de Hilbert de courbes de genre non nul et on l'applique à différentes courbes de Deligne-Lusztig pour lesquelles on calcule des S-corps de classes de Hilbert et des S-corps de classes de rayons. Cette méthode couvre en fait les revêtements supersinguliers de $\mathbb{P}^1_{\mathbb{F}_q}$ de groupe un p-groupe abélien élémentaire.

De nombreux points de ce chapitre recouvrent des travaux en cours. En particulier, les aspects algorithmiques et les problèmes de comptage de points sont en cours de développement.

TABLE OF CONTENTS

0 BACKGROUND MATERIAL.

"La géométrie est une harmonie."
V. Hugo in *Notre-Dame de Paris*

Table of Contents

Notations : Let p be a prime number and $q = p^n$ for some $n \in \mathbb{N} - \{0\}$. Let (K, v_K) be a local field of mixed characteristic $(0, p)$ with uniformizing parameter π_K such that $v_K(\pi_K) = 1$. Let R be the ring of integers of K. Let L/K be an algebraic extension with separable residual extension, we will denote by π_L(resp. v_L, resp. L°) a uniformizing parameter for L (resp. the prolongation of v to L such that $v_L(\pi_L) = 1$, resp. the ring of integers of L). If there is no possible confusion we note v for the prolongation of v_K to an algebraic closure K^{alg} of K.

0.1 STABLE REDUCTION OF VARIETIES.

Denote by k the residue field of K and assume that k is algebraically closed.

0.1.1 Stable reduction of curves.

The first result is due to Deligne and Mumford (see for example [Liu02] for a presentation following Artin and Winters).

Theorem 0.1.1 (Stable reduction theorem)**.** *Let C/K be a smooth, projective, geometrically connected curve over K of genus $g(C) \geqslant 2$. There exists a unique finite Galois extension M/K*

minimal for the inclusion relation such that $C_M := C \times_K M$ *has a stable model over* M°. *The stable model* $\mathcal{C}/M^\circ$ *of* C_M/M *is unique up to isomorphism. One has a canonical injective morphism*

$$\mathrm{Gal}(M/K) \overset{i}{\hookrightarrow} \mathrm{Aut}_k(\mathcal{C}_k). \tag{0.1}$$

Remarks :

1. Let's explain the action of $\mathrm{Gal}(K^{alg}/K)$ on $\mathcal{C}_k/k$. The group $\mathrm{Gal}(K^{alg}/K)$ acts on $C_M = C \times M$ on the right. By unicity of the stable model, this action extends to $\mathcal{C}$

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\sigma} & \mathcal{C} \\ \downarrow & & \downarrow \\ M^\circ & \xrightarrow{\sigma} & M^\circ \end{array}$$

   Since $k = k^{alg}$ one gets $\sigma \times k = \mathrm{Id}_k$, whence the announced action. The last assertion of the theorem characterizes the elements of $\mathrm{Gal}(K^{alg}/M)$ as the elements of $\mathrm{Gal}(K^{alg}/K)$ that trivially act on $\mathcal{C}_k/k$.

2. If $p > 2g(C)+1$, then C/K has stable reduction over a tamely ramified extension of K. We will study examples of covers with $p \leqslant 2g(C)+1$.

3. Our results will cover the elliptic case. Let E/K be an elliptic curve with additive reduction. If its modular invariant is integral, then there exists a smallest extension M of K over which E/K has good reduction. Otherwise E/K obtains split multiplicative reduction over a unique quadratic extension of K (see [Kra90]).

Definition 0.1.1. *The extension* M/K *is the monodromy extension of* C/K. *We call* $\mathrm{Gal}(M/K)$ *the monodromy group of* C/K. *It has a unique* p*-Sylow subgroup* $\mathrm{Gal}(M/K)_1$ *called the wild monodromy group. The extension* $M/M^{\mathrm{Gal}(M/K)_1}$ *is the wild monodromy extension.*

From now on we consider smooth, projective, geometrically integral curves C/K of genus $g(C) \geqslant 2$ birationally given by

$$Y^p = f(X) := \prod_{i=0}^{t} (X - x_i)^{n_i},\ \forall\, 0 \leqslant i \leqslant t,\ x_i \in R^\times,$$

with $(p, \sum_{i=0}^{t} n_i) = 1$ and $(p, n_i) = 1$. Moreover, we assume that $\forall i \neq j,\ v(x_i - x_j) = 0$, that is to say, the branch locus $B = \{x_0, \ldots, x_t, \infty\}$ of the cover has *equidistant geometry*. We denote by Ram the ramification locus of the cover.

Remark : We only ask p-cyclic covers to satisfy Raynaud's theorem 1' [Ray90] condition, that is the branch locus is K-rational with equidistant geometry. This has consequences on the image of (0.1), see Proposition 0.1.1.

Proposition 0.1.1. *Let* $\mathcal{T} = \mathrm{Proj}(M^\circ[X_0, X_1])$ *with* $X = X_0/X_1$. *The normalization* $\mathcal{Y}$ *of* $\mathcal{T}$ *in* $K(C_M)$ *admits a blowing-up* $\tilde{\mathcal{Y}}$ *which is a semi-stable model of* C_M/M. *The dual graph of* $\tilde{\mathcal{Y}}_k/k$

is a tree and the points in $\mathfrak{Ram}$ *specialize in a unique irreducible component* $D_0 \simeq \mathbb{P}^1_k$ *of* $\tilde{\mathcal{Y}}_k/k$. *There exists a contraction morphism* $h : \tilde{\mathcal{Y}} \to \mathcal{C}$, *where* $\mathcal{C}$ *is the stable model of* C_M/M *and*

$$\mathrm{Gal}(M/K) \hookrightarrow \mathrm{Aut}_k(\mathcal{C}_k)^{\#}, \tag{0.2}$$

where $\mathrm{Aut}_k(\mathcal{C}_k)^{\#}$ *is the subgroup of* $\mathrm{Aut}_k(\mathcal{C}_k)$ *of elements inducing the identity on* $h(D_0)$.

Proof. Let $f(X) = (X - x_0)^{n_0} S(X)$ and $an_0 + bp = 1$. Using [Liu02] 4.1.18, one shows that above $\mathcal{T}\backslash B = \operatorname{Spec} A$, the equation of $\mathcal{Y}$ is

$$A[Y]/(Y^p - f(X)),$$

and above $\mathcal{T}\backslash\{B\backslash x_0\} = \operatorname{Spec} A_0$, the equation of $\mathcal{Y}$ is

$$A_0[Y]/(Y^p - (X - x_0)S(X)^a).$$

From the equation of $\mathcal{Y}$ above $\mathcal{T}\backslash\{B\backslash x_0\}$ and since $v(S(x_0)) = 0$, one sees that $\mathcal{Y}_k$ is smooth at the reduction of x_0, thus the ramification locus $\mathfrak{Ram}$ specialize in a unique component D_0 of $\tilde{\mathcal{Y}}_k$. Using [Ray90] theorem 2, one sees that the dual graph of $\tilde{\mathcal{Y}}_k$ is a tree. It implies that there exists a contraction morphism $h : \tilde{\mathcal{Y}} \to \mathcal{X}$ of the components of $\tilde{\mathcal{Y}}_k$ isomorphic to $\mathbb{P}^1_k$ meeting $\tilde{\mathcal{Y}}_k$ in at most 2 points ([Liu02] 7.5.4 and 8.3.36). The scheme $\mathcal{X}$ is seen to be stable ([Liu02] 10.3.31), so $\mathcal{X} \simeq \mathcal{C}$.

The irreducible component D_0 is a smooth curve of genus 0, since it is birational to a curve with function field a purely inseparable extension of $k(\mathbb{P}^1_k)$, so $D_0 \simeq \mathbb{P}^1_k$. Then, B having K-rational equidistant geometry with $|B| \geqslant 3$, any element of $\mathrm{Gal}(M/K)$ induces the identity on D_0, giving (0.2). □

Remark : The component D_0 is the so-called *original component*.

Definition 0.1.2. *If the morphism* (0.2) *is surjective, one says that the curve* C/K *has maximal monodromy. Denote by* v_p *the* p*-adic valuation on* $\mathbb{Z}$. *If* $v_p(|\mathrm{Gal}(M/K)|) = v_p(|\mathrm{Aut}_k(\mathcal{C}_k)^{\#}|)$, *we say that the curve* C/K *has maximal wild monodromy.*

Definition 0.1.3. *The valuation on* $K(X)$ *corresponding to the discrete valuation ring* $R[X]_{(\pi_K)}$ *is called the Gauss valuation* v_X *with respect to* X. *We then have*

$$v_X\left(\sum_{i=0}^{m} a_i X^i\right) = \min\{v(a_i),\ 0 \leqslant i \leqslant m\}.$$

Remark : Note that a change of variables $T = \frac{X-y}{\rho}$ for $y, \rho \in R$ induces a Gauss valuation v_T. These valuations are exactly those that come from the local rings at generic points of components in the semi-stable models of $\mathbb{P}^1_K$.

0.1.2 Stable reduction of abelian varieties.

See [Gro72], [DK73] or [BLR90] for a complete account on stable reduction of abelian varieties and how it is related to semi-stable reduction of curves. The case of good reduction of abelian varieties is detailled in [ST68].

Definition 0.1.4. *1. Let* G/R *be a smooth, connected group scheme of finite type. We say that* G *has abelian reduction (resp. semi-abelian reduction) if the connected component* G^0_k *of* G_k *is an abelian variety (resp. an extension of an abelian variety by an affine torus).*

2. *Let* A_K/K *be an abelian variety, then* A_K *has potential abelian reduction (resp. potential semi-abelian reduction) if there exists a finite Galois extension* L/K *such that the Néron model of* A_L *over the normalization of* R *in* L *has abelian reduction (resp. semi-abelian reduction).*

Theorem 0.1.2 (Semi-abelian reduction theorem)**.** *Every abelian variety* A_K/K *has potential semi-abelian reduction.*

Theorem 0.1.3. *Let* C/K *be a smooth, projective curve such that* $C(K) \neq \emptyset$ *with regular model* $\mathcal{C}/R$ *and let* $\mathcal{A}$ *be the Néron model of* $\mathrm{Jac}(C)$*. Then,* $\mathcal{A}^0_k(k) \simeq \mathrm{Pic}^0(\mathcal{C}_k)$*.*

Theorem 0.1.4. *Let* C/K *be a smooth, projective, geometrically connected curve of genus* $g \geqslant 2$ *such that* $C(K) \neq \emptyset$*, then* C *has stable reduction if and only if* $\mathrm{Jac}(C)$ *has semi-abelian reduction.*

Remarks :

1. One also talks about *good reduction* of abelian varieties instead of abelian reduction of abelian varieties.

2. Let C/K be a stable curve, from the above and the description of $\mathrm{Pic}^0(X)$ where X/k is a connected, projective curve, one shows that the dual graph of the stable reduction of C is a tree if and only if $\mathrm{Jac}(C)$ has good reduction.

3. Theorem 0.1.4 remains true without the hypothesis $C(K) \neq \emptyset$ but the proof is then more difficult, see [DM69] Theorem 2.4.

0.2 EXTRA-SPECIAL p-GROUPS.

Some of the Galois groups and automorphism groups that we will have to consider are p-groups with peculiar group theoretic properties (see for example [Hup67], [Gor80] or [Suz86] for an account on extra-special p-groups). Let G be a finite group, we will denote by $Z(G)$ (resp. $D(G)$, resp. $\Phi(G)$) the center (resp. the derived subgroup, resp. the Frattini subgroup) of G. If G is a p-group, one has $\Phi(G) = D(G)G^p$.

Definition 0.2.1. *An extra-special* p*-group is a non-abelian* p*-group* G *such that*

$$D(G) = Z(G) = \Phi(G),$$

has order p*.*

Proposition 0.2.1. *Let* G *be an extra-special* p*-group.*

1. *Then* $|G| = p^{2n+1}$ *for some* $n \in \mathbb{N} - \{0\}$*.*

2. *One has the exact sequence*

$$0 \to Z(G) \to G \to (\mathbb{Z}/p\mathbb{Z})^{2n} \to 0.$$

3. *The group* G *has an abelian subgroup* J *such that* $Z(G) \subseteq J$ *and* $|J/Z(G)| = p^n$*.*

Proof. 1. See [Gor80] Theorem 5.5.2.

2. Since $D(G) = Z(G) = D(G)G^p$, the quotient $G/Z(G)$ is an abelian p-group of exponent p, thus $G/Z(G) \simeq (\mathbb{Z}/p\mathbb{Z})^{2n}$.

3. One proves this in the case $p = 2$ because it will only be used in this setting, nonetheless the result remains true for any prime p. Actually the case $p = 2$ needs a little more attention since symmetric forms have a special behavior in characteristic 2.

   Let $\bar{x}, \bar{y} \in G/Z(G)$ and $< \rho >= Z(G) \simeq \mathbb{Z}/2\mathbb{Z}$, then the commutator $[x, y]$ does not depend on the choice of the liftings x and y, moreover $[x, y] \in D(G) = Z(G)$, whence $[x, y] = \rho^\epsilon$ with $\epsilon \in \{0, 1\}$. One defines

$$\begin{array}{ccc} G/Z(G) \times G/Z(G) & \to & \mathbb{F}_2 \\ (\bar{x}, \bar{y}) & \mapsto & < \bar{x}, \bar{y} >:= \epsilon. \end{array}$$

   One easily checks that $< ., . >$ is a non-degenerate alternating bilinear form. Let $\bar{x} \in G/Z(G) - \{0\}$ and $\bar{y} \in G/Z(G)$ such that $< \bar{x}, \bar{y} >= 1$, then $P := \mathbb{F}_2\bar{x} \oplus \mathbb{F}_2\bar{y}$ is the hyperbolic plane. Since $< ., . >$ is a symmetric bilinear form and $< ., . > |_{P\times P}$ is non-degenerate, one has the decomposition $G/Z(G) = P \oplus P^\perp$. By induction one may write $G/Z(G) = \oplus_{i=1}^n P_i$ where the P_i's are hyperbolic planes and the direct sum is an orthogonal sum. Then, there exists an $\mathbb{F}_2$-subspace $J/Z(G)$ of dimension n of $G/Z(G)$ such that

$$\forall \bar{x}, \bar{y} \in J/Z(G), < \bar{x}, \bar{y} >= 0,$$

   that is, the group J is abelian.

□

0.3 GALOIS EXTENSIONS OF COMPLETE DISCRETE VALUATION FIELDS.

See [Ser79] for a complete presentation. Let L/K be a finite Galois extension with separable residual extension and group G. Then G is endowed with a *lower ramification filtration* $(G_i)_{i\geqslant -1}$ where G_i is the i-*th lower ramification group* defined by

$$G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geqslant i + 1\}.$$

The integers i such that $G_i \neq G_{i+1}$ are called *lower breaks*. For $\sigma \in G - \{1\}$, let

$$i_G(\sigma) := v_L(\sigma(\pi_L) - \pi_L).$$

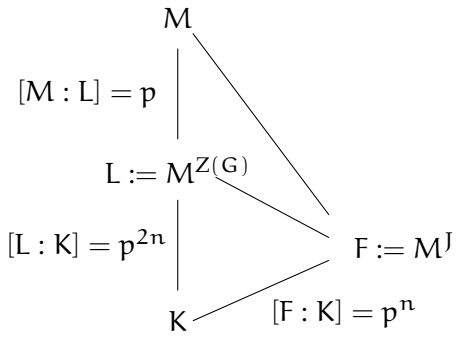
The group G is also endowed with a *higher ramification filtration* $(G^i)_{i\geqslant -1}$ which can be computed from the G_i's by means of the *Herbrand's function* $\varphi_{L/K}$. The real numbers t such that $\forall \epsilon > 0$, $G^{t+\epsilon} = G^t$ are called *higher breaks*. The least integer $m \geqslant 0$ such that $G^m = \{1\}$ is called the *conductor of* L/K.

Lemma 0.3.1 (see [Hyo87]). *Let* L/K *be defined by* $X^p = 1 + w\pi_K^s$ *with* $0 < s < \frac{p}{p-1}v_K(p)$, $(s, p) = 1$ *and* $w \in R^\times$. *The different ideal* $\mathcal{D}_{L/K}$ *satisfies*

$$v_K(\mathcal{D}_{L/K}) = v_K(p) + \frac{p-1}{p}(1 - s).$$

Lemma 0.3.2. *Let* M/K *be a Galois extension such that* $G := \mathrm{Gal}(M/K)$ *is an extra-special* p*-group of order* p^{2n+1}*. Assume that* $\mathrm{Gal}(M^{Z(G)}/K)_2 = \{1\}$*, then the break* t *of* $M/M^{Z(G)}$ *is such that* $t \in 1 + p^n\mathbb{N}$.

Proof. According to Proposition 0.2.1 3, there exists an abelian subgroup J of G such that $Z(G) \subseteq J$ and $|J/Z(G)| = p^n$. Thus, one has the following diagram



Let t be the lower break of M/L, then t is a lower break of M/F and

$$\varphi_{M/F}(t) = \varphi_{L/F}(\varphi_{M/L}(t)),$$

is a higher break of M/F. Since $\varphi_{M/L}(t) = t$, one has $\varphi_{M/F}(t) = \varphi_{L/F}(t)$. Since $\mathrm{Gal}(L/K)_2 = \{1\}$, one has $\mathrm{Gal}(L/F)_2 = \{1\}$ and $\varphi_{L/F}(t) = 1 + \frac{t-1}{p^n}$. The Hasse-Arf Theorem applied to the abelian extension M/F implies that $1 + \frac{t-1}{p^n} \in \mathbb{N} - \{0\}$, thus $t \in 1 + p^n\mathbb{N}$. □

Proposition 0.3.1 (see [GS91])**.** *Let* K *be a perfect field of characreristic* $p > 0$*. Let* F/K *be an algebraic function field of one variable with full constant field* K *and genus* $g(F)$*. Consider an elementary abelian extension* E/F *of degree* p^n *such that* K *is the constant field of* E*. Denote by* $E_1, \ldots, E_t$*, where* $t = (p^n - 1)/(p - 1)$*, the intermediate fields* $F \subsetneq E_i \subsetneq E$ *with* $[E_i : F] = p$ *and by* $g(E)$ *(resp.* $g(E_i)$*), the genus of* E/K *(resp.* E_i/K*). Then*

$$g(E) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1} - 1)g(F).$$

0.4 SOME REPRESENTATION THEORY OF FINITE GROUPS.

Let G be a finite group and k be a field of characteristic 0 or $p > 0$ such that $p \nmid |G|$. For a representation ρ, one denotes by χ_ρ the corresponding character. In the following, we restrict to finite-dimensional representations. One starts by recalling usual constructions of $k[G]$-modules and their properties that will be used in the course of the proof of Proposition 0.5.1.

Definition 0.4.1. *Let* V, W *be* $k[G]$*-modules, one denotes* $\mathrm{Hom}_G(V, W) := \mathrm{Hom}_{k[G]}(V, W)$.

1. *The* k*-module* $\mathrm{Hom}_k(V, W)$ *acquires an action of* G *by*

$$\forall f \in \mathrm{Hom}_k(V, W),\ \forall g \in G,\ \forall v \in V,\ g.f(v) = g.f(g^{-1}v).$$

One has $\mathrm{Hom}_k(V, W)^G = \mathrm{Hom}_G(V, W)$.

2. *Denote by* V^* *the* $k[G]$*-module* $\mathrm{Hom}_k(V,k)$ *where* k *is the* $k[G]$*-module with action*

$$\forall g \in G,\ \forall \lambda \in k,\ g.\lambda = \lambda.$$

Then $\chi_{V^*}(g) = \chi_V(g^{-1})$.

3. *One defines the* $k[G]$*-module* $V \otimes_k W$ *as the* k*-vector space* $V \otimes_k W$ *with the action of* G *given by*

$$\forall g \in G,\ \forall (v,w) \in V \times W,\ g.(v \otimes w) = (g.v) \otimes (g.w),$$

thus $\chi_{V\otimes_k W} = \chi_V.\chi_W$. *Moreover, one has an isomorphism of* $k[G]$*-modules*

$$\mathrm{Hom}_k(V,W) \simeq V^* \otimes_k W.$$

Proposition 0.4.1. *Let* ρ, τ *be finite-dimensional representations of* G *over* k *and* V, W *be the* $k[G]$*-modules afforded by* ρ *and* τ*, then*

$$< \chi_\rho, \chi_\tau > := \frac{1}{|G|} \sum_{g\in G} \chi_\rho(g^{-1})\chi_\tau(g) = \dim_k \mathrm{Hom}_G(V,W) =: < V, W > .$$

Proof. Let V be a finite k-vector space and $\pi : G \to \mathrm{Gl}(V)$ be a representation, then

$$e^V : \frac{1}{|G|} \sum_{g\in G} \pi(g) : V \to V,$$

is such that

$$\mathrm{Tr}(e^V) = \frac{1}{|G|} \sum_{g\in G} \chi_\pi(g) = \dim_k V^G. \tag{0.3}$$

Indeed, there exists a G-stable k-vector space W such that $V = V^G \bigoplus W$, moreover $\mathrm{Im}\ e^V \subseteq V^G$ and $e^V|_{V^G} = \mathrm{Id}\,|_{V^G}$. From $e^V(W) \subseteq W$, one gets $e^V(W) \subseteq W \cap V^G = \{0\}$, whence $\mathrm{Tr}(e^V) = \dim_k V^G$. From this one may compute

$$\begin{aligned}
\dim_k \mathrm{Hom}_G(V,W) &= \dim_k \mathrm{Hom}_k(V,W)^G \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_{\mathrm{Hom}_k(V,W)}(g), \quad \text{according to equation 0.3} \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_{V^*\otimes_k W}(g) \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_{V^*}(g)\chi_W(g) \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_V(g^{-1})\chi_W(g).
\end{aligned}$$

□

0.5 TORSION POINTS OF ABELIAN VARIETIES.

Denote by k the residue field of K and assume that k is algebraically closed. Let A/K be an abelian variety over K of dimension d with potential good reduction and $\ell \neq p$ be a prime number. One denotes by $A[\ell]$ the ℓ-torsion subgroup of $A(K^{alg})$ and by $T_\ell(A) = \varprojlim A[\ell^n]$ (resp. $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$) the Tate module (resp. ℓ-adic Tate module) of A. The following result may be found in [Gur03] paragraph 3. We recall it for the convenience of the reader.

Lemma 0.5.1. *Let k be an algebraically closed field. Let C/k be a smooth, projective, integral curve, $\ell \in \mathbb{N}$ such that $\gcd(\ell, p) = 1$ and H be a finite subgroup of $\mathrm{Aut}_k(C)$ such that $\gcd(|H|, \ell) = 1$. Let $\pi : C \to C/H$, then π induces a group isomorphism*

$$\mathrm{Jac}(C/H)[\ell] \simeq \mathrm{Jac}(C)[\ell]^H.$$

In particular, if $\ell \neq p$ is prime, one has

$$2g(C/H) = \dim_{\mathbb{F}_\ell} \mathrm{Jac}(C/H)[\ell] = \dim_{\mathbb{F}_\ell} \mathrm{Jac}(C)[\ell]^H.$$

Proof. Put $d := |H|$, the morphism $\pi : C \to C/H$ is finite, dominant of degree d. Moreover, C/H is a smooth integral curve, thus one may consider the Weil divisors groups $Z^1(C)$ and $Z^1(C/H)$ and one defines

$$Z^1(C)^H := \{D \in Z^1(C) / \ \sigma(D) = D, \ \forall \sigma \in H\}.$$

Using [Liu02] 7.2.17 and [Liu02] Exercice 7.2.3, one has

$$\pi_* \pi^* D = dD, \ D \in Z^1(C/H),$$
$$\pi^* \pi_* D = dD, \ D \in Z^1(C)^H.$$

Then, since $\gcd(d, \ell) = 1$, the multiplication by d on $\mathrm{Jac}(C)[\ell]$ and $\mathrm{Jac}(C/H)[\ell]$ are isomorphisms, thus

$$\pi_* : \mathrm{Jac}(C)[\ell]^H \to \mathrm{Jac}(C/H)[\ell],$$
$$\pi^* : \mathrm{Jac}(C/H)[\ell] \to \mathrm{Jac}(C)[\ell]^H,$$

are isomorphisms.

□

If $\ell \geqslant 3$, then $L = K(A[\ell])$ is the minimal extension over which A/K has good reduction, it is a Galois extension with group G (see [ST68]). We denote by r_G (resp. 1_G) the character of the regular (resp. unit) representation of G. We denote by I the inertia group of K^{alg}/K. For further explanations about conductor exponents see [Ser67], [Ogg67] and [ST68].

Definition 0.5.1. *1. Let*

$$a_G(\sigma) := -i_G(\sigma), \quad \sigma \neq 1,$$
$$a_G(1) := \sum_{\sigma \neq 1} i_G(\sigma),$$

and $sw_G := a_G - r_G + 1_G$. Then, a_G is the character of a $\mathbb{Q}_\ell[G]$-module and there exists a projective $\mathbb{Z}_\ell[G]$-module Sw_G such that $Sw_G \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has character sw_G.

2. *We still denote by* $T_\ell(A)$ *(resp.* $A[\ell]$*) the* $\mathbb{Z}_\ell[G]$*-module (resp.* $\mathbb{F}_\ell[G]$*-module) afforded by* $G \to \mathrm{Aut}(T_\ell(A))$ *(resp.* $G \to \mathrm{Aut}(A[\ell])$*). Let*

$$\mathrm{sw}(A/K) := \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathbb{Z}_\ell[G]}(\mathrm{Sw}_G, A[\ell]),$$
$$\epsilon(A/K) := \dim_{\mathbb{Q}_\ell} V_\ell(A)/V_\ell(A)^I.$$

The integer $f(A/K) := \epsilon(A/K) + \mathrm{sw}(A/K)$ *is the so-called conductor exponent of* A/K *and* $\mathrm{sw}(A/K)$ *is the Swan conductor of* A/K.

Proposition 0.5.1. *Let* $\ell \neq p$ *be a prime number such that* $\ell \geqslant 3$.

1. *The integers* $\mathrm{sw}(A/K)$ *and* $\epsilon(A/K)$ *are independent of* ℓ.

2. *One has*

$$\mathrm{sw}(A/K) = \sum_{i \geqslant 1} \frac{|G_i|}{|G_0|} \dim_{\mathbb{F}_\ell} A[\ell]/A[\ell]^{G_i}.$$

Moreover, for ℓ *large enough,* $\epsilon(A/K) = \dim_{\mathbb{F}_\ell} A[\ell]/A[\ell]^{G_0}$.

Proof. Let $\mathcal{A}/R$ be the Néron model of A/K, denote by a (resp. u, resp. t) the abelian rank (resp. unipotent rank, resp. toric rank) of $\mathcal{A}_k^0$.

1. According to [ST68] Theorem 4, $\mathrm{sw}(A/K)$ is independent of ℓ and from [ST68] §3 Remark (1), one has

$$\epsilon(A/K) = 2u,$$

thus it is independent of ℓ.

2. One recalls the construction of Sw_G from [Ser67] and one gives some more details in order to prove the statement about $\mathrm{sw}(A/K)$. Put $g := |G|$ and $g_i := |G_i|$, note that $g = g_0$. Let u_G be the character of the augmentation representation of G over $\mathbb{Q}_\ell$, then $u_G = r_G - 1_G$. Recall that for P a projective $\mathbb{Z}_\ell[G]$-module, the module

$$\overline{P} := P/lP,$$

is a projective $\mathbb{F}_\ell[G]$-module. Since $A[\ell]$ is of ℓ-torsion, one has a group isomophism

$$\mathrm{Hom}_{\mathbb{Z}_\ell[G]}(\mathrm{Sw}_G, A[\ell]) \simeq \mathrm{Hom}_{\mathbb{F}_\ell[G]}(\overline{\mathrm{Sw}_G}, A[\ell]),$$

thus

$$\mathrm{sw}(A/K) = \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathbb{F}_\ell[G]}(\overline{\mathrm{Sw}_G}, A[\ell]) =< \overline{\mathrm{Sw}_G}, A[\ell] > .$$

For $i \geqslant 1$, denote by u_i the character of the augmentation representation of G_i over $\mathbb{Q}_\ell$ and u_i^* its induced character to G. One defines the $\mathbb{Z}_\ell[G_i]$-module U_i as the kernel of the surjective morphism of $\mathbb{Z}_\ell[G_i]$-modules

$$\begin{array}{ccc} \mathbb{Z}_\ell[G_i] & \to & \mathbb{Z}_\ell \\ \sum_i \lambda_i g_i & \mapsto & \sum_i \lambda_i. \end{array}$$

Thus $U_i \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has character u_i and U_i is a free $\mathbb{Z}_\ell$-module. Since $\gcd(\ell, |G_i|) = 1$ for $i \geqslant 1$, then U_i is a pojective $\mathbb{Z}_\ell[G_i]$-module (see [Ser67] III.2.5). In particular one may realize u_i^* as a projective $\mathbb{Z}_\ell[G]$-module, more precisely $U_i^* \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has character u_i^* where $U_i^* = U_i \otimes_{\mathbb{Z}_\ell[G_i]} \mathbb{Z}_\ell[G]$. In our setting, one has $u_0^* = u_0 = u_G$, then according to [Ser79] VI §2 Proposition 2 (the proof is done when viewing a_G and the u_i's as characters of $\mathbb{C}[G]$-modules but still holds when viewing them as characters of $\mathbb{Q}_\ell[G]$-modules), one has

$$\begin{aligned} g a_G &= \sum_{i \geqslant 0} g_i u_i^* = g u_G + \sum_{i \geqslant 1} g_i u_i^*, \\ \text{and } g a_G &= g(r_G - 1_G + \mathrm{sw}_G) = g u_G + g\,\mathrm{sw}_G\,. \end{aligned}$$

Thus $g\,\mathrm{sw}_G = \sum_{i \geqslant 1} g_i u_i^*$ and taking the direct sum of g_i times each U_i^*, one obtains the projective $\mathbb{Z}_\ell[G]$-module Sw_G, whence

$$g\overline{\mathrm{Sw}_G} = \sum_{i \geqslant 1} g_i \overline{U_i^*}.$$

Moreover, $\overline{U_i^*} = \overline{U_i}^*$ and $\overline{U_i}$ is the augmentation representation of G_i over $\mathbb{F}_\ell$. Finally, for any $\mathbb{F}_\ell[G]$-module V one denotes by $V|_{G_i}$ its restriction to G_i and if χ_V is the character of a $\mathbb{F}_\ell[G]$-module V, one sets

$$\chi_V(G_i) := \frac{1}{g_i} \sum_{g \in G_i} \chi_V(g),$$

then

$$\begin{aligned} < \chi_V|_{G_i}, \overline{U_i} > &= \chi_V(1) - \chi_V(G_i) \\ &= \dim_{\mathbb{F}_\ell} V - \dim_{\mathbb{F}_\ell} V^{G_i}, \quad \text{see equation (0.3).} \end{aligned}$$

It implies that

$$\begin{aligned} g < \overline{\mathrm{Sw}_G}, V > &= \sum_{i \geqslant 1} g_i < \overline{U_i}^*, V > \\ &= \sum_{i \geqslant 1} g_i < \overline{U_i}, V|_{G_i} > \\ &= \sum_{i \geqslant 1} g_i \dim_{\mathbb{F}_\ell} V/V^{G_i}. \end{aligned}$$

Applying this last relation with $V = A[\ell]$ yields the result.

Then one proves the statement about $\epsilon(A/K)$. Since $G = G_0$ and $L = K(A[\ell])$, one has $A(K)[l] = A[l]^{G_0} = A[l]^I$. Recall that $d = t + u + a$ and that in our setting $t = 0$ and $\epsilon(A/K) = 2u$. Thus one wants to prove the following equality

$$\begin{aligned} 2u &= \dim_{\mathbb{F}_\ell} A[l] - \dim_{\mathbb{F}_\ell} A[l]^I \\ &= 2d - \dim_{\mathbb{F}_\ell} A[l]^I \\ &= 2u + 2a - \dim_{\mathbb{F}_\ell} A[l]^I. \end{aligned} \tag{0.4}$$

According to [ST68] §1 Lemma 1 and Lemma 2 one knows that $\dim_{\mathbb{F}_\ell} \mathcal{A}_k^0[l] = 2a$ and $A[l]^I \simeq \mathcal{A}_k[\ell]$, thus equality (0.4) will hold if and only if $\mathcal{A}_k[\ell] = \mathcal{A}_k^0[\ell]$. Denote by $\Phi(\mathcal{A}_k)$ the group of components of $\mathcal{A}_k$. Since $\mathcal{A}_k[\ell]/\mathcal{A}_k^0[\ell]$ is a finite dimensional $\mathbb{F}_\ell$-vector space of order dividing $|\Phi(\mathcal{A}_k)|$, if one choses ℓ prime to $|\Phi(\mathcal{A}_k)|$ then $\mathcal{A}_k[\ell]/\mathcal{A}_k^0[\ell] = \{0\}$.

□

Remarks :

1. It follows from the definition that $sw(A/K) = 0$ if and only if $G_1 = \{1\}$. The Swan conductor is a measure of the wild ramification.

2. In [LRS93] equation (13) of §1, the authors claim that one may compute $\epsilon(A/K)$ by means of the formula of Proposition 0.5.1 2 when $\ell \neq 2$ without giving proof. Here is an example in the elliptic case showing that it is not correct.

   Let k be an algebraically closed field of characteristic 2 and $K = \mathrm{Frac}(W(k))$. The elliptic curve E/K with equation $y^2 = x^3 - 1296x - 15552$ has potential good reduction and has additive reduction, whence $\epsilon(E/K) = 2$. Moreover, the curve E/K has Kodaira type IV, thus the group of components of the special fiber of its Néron model is $\mathbb{Z}/3\mathbb{Z}$. In particular, one may compute $\epsilon(E/K)$ using the formula of Proposition 0.5.1 for $\ell \geqslant 5$ prime.

0.6 AUTOMORPHISMS OF CURVES OF CHARACTERISTIC p.

Let k be an algebraically closed field of characteristic $p > 0$. See [LM05], [MR08] and [Roc09] for a complete account on big actions.

0.6.1 Big actions.

Definition 0.6.1. *A big action is a pair (X, G) where X/k is a smooth, projective, geometrically connected curve of genus $g(X) \geqslant 2$ and G is a finite p-group, $G \subseteq \mathrm{Aut}_k(X)$, such that*

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

The following result may be found in [MR08] Proposition 2.2 and Lemma 2.4.

Proposition 0.6.1. *Let (X, G) be a big action and $H \subseteq G$ be a subgroup.*

1. *There exists a point of X, say ∞, such that G is the wild inertia group G_1 of G at ∞ and $D(G)$ is the second ramification subgroup G_2.*

2. *One has $g(X/H) = 0$ if and only if $D(G) \subseteq H$.*

0.6.2 Automorphisms of Artin-Schreier covers.

Let $R(t) \in k[t]$ be a monic additive polynomial and A_R/k be the smooth, projective, geometrically irreducible curve birationally given by $w^p - w = tR(t)$. Denote by $G_{1,\infty}(R)$ the p-Sylow subgroup of the subgroup of $\mathrm{Aut}_k(A_R)$ of automorphisms fixing ∞. There is a so-called Artin-Schreier morphism $\pi : A_R \to \mathbb{P}^1_k$. The automorphism t_a of $\mathbb{P}^1_k$ given by $t \mapsto t + a$ with $a \in k$ has a prolongation $\tilde{t}_a$ to A_R if there is a commutative diagram

$$\begin{array}{ccc} A_R & \xrightarrow{\tilde{t}_a} & A_R \\ \pi \downarrow & & \pi \downarrow \\ \mathbb{P}^1_k & \xrightarrow{t_a} & \mathbb{P}^1_k \end{array}$$

Proposition 0.6.2. *Let* $n \geqslant 1$, $q = p^n$, $R(t) = \sum_{k=0}^{n-1} \bar{u}_k t^{p^k} + t^q \in k[t]$ *and* $a \in k$. *Let*

$$Q(a) := a^{q^2} + (2\bar{u}_0 a)^q + \sum_{k=1}^{n-1} (\bar{u}_k^q a^{qp^k} + (\bar{u}_k a)^{q/p^k}) + a,$$

Then, the automorphism of $\mathbb{P}^1_k$ *given by* $t \mapsto t + a$ *has a prolongation to* A_R/k *as an element of* $G_{1,\infty}(R)$ *if and only if* $Q(a) = 0$.

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{P}^1_k)$ defined by $t \mapsto t + a$ and

$$\begin{aligned} \mathrm{Frob}_p : k(t) &\longrightarrow k(t) \\ x &\longmapsto x^p. \end{aligned}$$

From the equation of A_R/k, one has

$$\sigma(w)^p - \sigma(w) = (t + a)(R(t) + R(a)),$$

and an easy computation shows that

$$(\sigma(w) - w)^p - (\sigma(w) - w) = tR(a) + aR(t) + aR(a) = t^q Q(a) \bmod (\mathrm{Frob}_p - \mathrm{Id})(k[t]).$$

Thus, if $Q(a) = 0$, then $\sigma(w) = w + P(t) \in k(w, t)$ for some $P(t) \in k[t]$, then according to [LM05] Corollary 3.4 one has $\sigma \in G_{1,\infty}(R)$. Conversely, if σ has a prolongation as an element of $G_{1,\infty}(R)$, then $\sigma(w) = w + P(t)$ for some $P(t) \in k[t]$. Thus

$$t^q Q(a) = 0 \bmod \ (\mathrm{Frob}_p - \mathrm{Id})(k[t]),$$

implying that $Q(a) = 0$. □

The following result may be found in [LM05] Proposition 8.1.

Proposition 0.6.3. *Let* $R(t) \in k[t]$ *be an additive polynomial of degree* p^n, *then* $G_{1,\infty}(R)$ *is an extra-special* p*-group and one has the exact sequence*

$$0 \to Z(G_{1,\infty}(R)) \simeq \mathbb{Z}/p\mathbb{Z} \to G_{1,\infty}(R) \to (\mathbb{Z}/p\mathbb{Z})^{2n} \to 0,$$

where $(\mathbb{Z}/p\mathbb{Z})^{2n}$ *is identified with the group of translations* $t \mapsto t + a$ *of* $\mathbb{P}^1_{\mathbb{F}_q}$ *extending to elements of* $G_{1,\infty}(R)$.

The elliptic curve over $\mathbb{F}_2^{\mathrm{alg}}$ birationally given by $w^2 - w = t^3$ will be of particular interest in Chapter 1. The following group theoretical result may be found in [Ser72], II Proposition 15.

Proposition 0.6.4. *Let* G *be a subgroup of* $Gl_2(\mathbb{F}_3)$ *such that* 3 *divides* $|G|$. *Then* $|G| \leqslant 12$ *or* $Sl_2(\mathbb{F}_3) \subseteq G$.

Proposition 0.6.5. *Let* $k = \mathbb{F}_2^{alg}$, E/k *be an elliptic curve and* $m \geqslant 3$, *then the natural map*

$$Aut_k(E) \to Aut(E(k)[m]),$$

is injective.

Proof. Let $\sigma \in Aut_k(E) - \{Id\}$ and $P \in E(k)$ such that $\sigma(P) \neq P$. According to the Riemann-Roch theorem $l(2P) \geqslant 2$. Since $l(0) = 1$ and $\mathcal{L}(0) \subseteq \mathcal{L}(2P)$, there exist $1 \leqslant r \leqslant 2$ and $f \in k(E)$ such that $(f)_\infty = r(P)$.

Then, $h := f - f \circ \sigma \in k(E)$ is such that $(h)_\infty = r(P) + r(\sigma^{-1}(P))$, thus h has at most $2r$ zeroes. On the one hand, fixed points of σ being zeroes of h, there are at most 4 of them, one the other hand $|E(k)[m]| = m^2 \geqslant 9 > 4$. Thus if $\sigma \in Aut_k(E)$ acts trivially on $E(k)[m]$, then $\sigma = Id$. □

Proposition 0.6.6. *Let* $k = \mathbb{F}_2^{alg}$ *and* E/k *be the elliptic curve given by* $w^2 - w = t^3$. *Then,* $Aut_k(E) \simeq Sl_2(\mathbb{F}_3)$.

Proof. According to [Sil09] III.3 Proposition 3.1, $|Aut_k(E)| = 24$. The previous Proposition implies that $Aut_k(E)$ is isomorphic to a subgroup of $Aut(E(k)[m]) \simeq Gl_2(\mathbb{F}_3)$ of order 24, whence $Aut_k(E) \simeq Sl_2(\mathbb{F}_3)$. □

0.7 RAY CLASS FIELDS.

See [Aue99] for a detailed account. Let $K/\mathbb{F}_q$ be a function field of one variable with full constant field $\mathbb{F}_q$ and fix an algebraic closure K^{alg} in which all extensions of K are assumed to lie. Thus K is a finite extension of $\mathbb{F}_q(x)$. In this Section, we consider only Galois extensions of function fields of one variable with full constant field $\mathbb{F}_q$ that are totally ramified over the place $(\frac{1}{x})$ of $\mathbb{F}_q(x)$, denoted ∞, and unramified outside ∞. In this setting, the definition of the conductor given in Section 0.3 coincides with that given in [Aue99] I.3.

Definition 0.7.1. *Let* S *be a non-empty set of finite* $\mathbb{F}_q$*-rational places of* K *and* $m \in \mathbb{N}$. *One defines the* S*-ray class field mod* $m\infty$ *of* K, *denoted by* $K_S^{m\infty}$, *as the largest abelian extension* L/K *with conductor* $\leqslant m\infty$ *such that every place in* S *splits completely in* L.

Definition 0.7.2. *For a place* $\mathfrak{p}$ *of* K, *let* $\mathcal{O}_\mathfrak{p}$ *be the corresponding discrete valuation ring of* K. *Let* $\mathcal{O}_S := \cap_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}$ *be the group of* S*-regular functions. Let* $Cl(\mathcal{O}_S)$ *be the class group of the Dedekind ring* $\mathcal{O}_S$ *and* $h_S := |Cl(\mathcal{O}_S)|$.

The field extension $K_S^{m\infty}/K$ is finite Galois and the field K_S^0 is the so-called S*-Hilbert Class field of* K, then K_S^0/K is finite Galois and

$$Gal(K_S^0/K) \simeq Cl(\mathcal{O}_S).$$

Proposition 0.7.1 (see [Aue99] II.5.3.)**.** *If* $S \supseteq T$ *and* $m \leqslant n$, *then* $K_S^{m\infty} \subseteq K_T^{n\infty}$.

In particular, for $m \geqslant 0$ one has the following inclusions

$$K \subseteq K_S^0 \subseteq K_S^\infty \subseteq K_S^{m\infty}.$$

Let $C/\mathbb{F}_q$ be the smooth, projective and irreducible curve with function field $K/\mathbb{F}_q$. One defines the map

$$\begin{aligned} \theta : C(\mathbb{F}_q) &\to \mathrm{Jac}(C)(\mathbb{F}_q) \\ P &\mapsto [P - \infty]. \end{aligned}$$

Let J_S be the subgroup of $\mathrm{Jac}(C)(\mathbb{F}_q)$ generated by $\theta(S)$. One has the following well known result, see [Aue99] I.2.1.

Proposition 0.7.2. *There is an exact sequence*

$$0 \to J_S \to \mathrm{Jac}(C)(\mathbb{F}_q) \to Cl(\mathcal{O}_S) \to 0.$$

Remark : According to Proposition 0.7.2, if $< \theta(S) >= J_S = \mathrm{Jac}(C)(\mathbb{F}_q)$, then $K_S^0 = K$.

0.8 DELIGNE–LUSZTIG CURVES.

There are three types of irreducible curves arising as the Deligne-Lusztig variety associated to a connected, reductive, algebraic group, these are the Hermitian curves, the Suzuki curves and the Ree curves (see [Han92], [Ped92], [Lau99b] and [HP93]).

Let $C/\mathbb{F}_q$ be a smooth, projective, irreducible curve, one denotes by $L(C, \mathbb{F}_q, t)$ its L-polynomial, i.e. the numerator of its zeta function $Z(C, \mathbb{F}_q, t)$. One has the relation

$$Z(C, \mathbb{F}_q, t) = \frac{L(C, \mathbb{F}_q, t)}{(1-t)(1-qt)}.$$

Proposition 0.8.1. *Let $s \in \mathbb{N} - \{0\}$ and $q := p^s$. The Hermitian curve $X_H/\mathbb{F}_{q^2}$ is the smooth, projective, irreducible curve birationally given by*

$$X_H : y^q + y = x^{1+q}.$$

Let $K := \mathbb{F}_{q^2}(x)$ and $S := \{(x-a), a \in \mathbb{F}_{q^2}\}$, then $\mathbb{F}_{q^2}(X_H) = K_S^{(q+2)\infty}$. One has

$$L(X_H, \mathbb{F}_{q^2}, t) = (1+qt)^{q(q-1)}.$$

Proposition 0.8.2. *Let $s \in \mathbb{N}$, $q_0 := 2^s$ and $q := 2q_0^2$. The Suzuki curve $X_S/\mathbb{F}_q$ is the smooth, projective, irreducible curve birationally given by*

$$X_S : y^q - y = x^{q_0}(x^q - x).$$

Let $K := \mathbb{F}_q(x)$ and $S := \{(x-a), a \in \mathbb{F}_q\}$, then $\mathbb{F}_q(X_S) = K_S^{(2q_0+2)\infty}$. One has

$$L(X_S, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{q_0(q-1)}.$$

Proposition 0.8.3. *Let $s \in \mathbb{N}$, $q_0 := 3^s$ and $q := 3q_0^2$. The Ree curve $X_R/\mathbb{F}_q$ is the smooth, projective, irreducible curve birationally given by*

$$X_R : \begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x). \end{cases}$$

Let $K := \mathbb{F}_q(x)$ and $S := \{(x-a), a \in \mathbb{F}_q\}$, then $\mathbb{F}_q(X_R) = K_S^{(3q_0+3)\infty}$ and $\mathbb{F}_q(x, y_1) = K_S^{(3q_0+2)\infty}$. One has

$$L(X_R, \mathbb{F}_q, t) = (1 + 3q_0 t + qt^2)^a (1 + qt^2)^b,$$

where $a = q_0(q^2-1)$ and $b = \frac{1}{2}(q_0 - 1)(q + 3q_0 + 1)$.

R. Auer proved the following generalization about ray class fields.

Proposition 0.8.4 ([Aue99] III. Prop. 8.9 b) and Lemma 8.7 c)). *Let $K := \mathbb{F}_q(x)$ and $S := \{(x-a), a \in \mathbb{F}_q\}$, assume that $r := \sqrt{pq} \in \mathbb{N}$ and let $y_1, \dots, y_{p-1} \in K^{alg}$ satisfy $y_i^q - y_i = x^{ir/p}(x^q - x)$. Then $K_S^{i\infty} = K$ for $1 \leqslant i \leqslant p$ and*

$$K_S^{(r+i+1)\infty} = K(y_1, \dots, y_i) \text{ for } i \in \{1, \dots, p-1\}.$$

Moreover, $[K_S^{(r+i+1)\infty} : K] = q^i$ for $1 \leqslant i \leqslant p-1$.

0.9 SUPERSINGULAR VARIETIES.

We recall some well-known facts about supersingularity, see [LO03] for a complete account.

Definition 0.9.1. 1. *Let $E/\mathbb{F}_q$ be an elliptic curve. If for one $r \geqslant 1$, $E[p^r] = \{0\}$, then the elliptic curve $E/\mathbb{F}_q$ is said to be supersingular.*

2. *Let $A/\mathbb{F}_q$ be an abelian variety of dimension d, then A is supersingular if there exists a supersingular elliptic curve $E/\mathbb{F}_q^{alg}$ and an isogeny $A \otimes \mathbb{F}_q^{alg} \sim E^d$.*

3. *Let $C/\mathbb{F}_q$ be a curve such that $C(\mathbb{F}_q) \neq \emptyset$, then C is supersingular if its jacobian is a supersingular abelian variety.*

Definition 0.9.2. *A curve $C/\mathbb{F}_q$ such that $C(\mathbb{F}_q) \neq \emptyset$ is superspecial if there exists a supersingular elliptic curve $E/\mathbb{F}_q^{alg}$ such that one has an isomorphism $\mathrm{Jac}(C) \otimes \mathbb{F}_q^{alg} \simeq E^{g(C)}$.*

Proposition 0.9.1. *A curve $C/\mathbb{F}_q$ given by $w^p - w = xR(x)$, where $R(x) = \sum_{k=0}^n a_k x^{p^k}$, is supersingular. In particular, the Deligne-Lusztig curves are supersingular.*

Proof. According to [Bla12] Corollary 3.7 (ii), a curve $C/\mathbb{F}_q$ given by $w^p - w = xR(x)$, where $R(x) = \sum_{k=0}^n a_k x^{p^k}$, is supersingular. We show that the jacobian of a Deligne-Lusztig curve is isogenous to a product of jacobians of curves given by $w^p - w = xR(x)$, for various $R(x) = \sum_{k=0}^n a_k x^{p^k}$.

In order to prove that the Suzuki curve is supersingular, we use the notations of Proposition 0.8.2 and Proposition 0.3.1. We apply Proposition 0.3.1 with $E = \mathbb{F}_q(X_S)$,

$F = \mathbb{F}_q(x)$ and $t = q - 1$. In particular, there are t intermediate fields E_i such that $F \subseteq E_i \subseteq E$ with $[E_i : F] = p$. It yields condition (10) of [KR89], i.e.

$$g(E) = \sum_{i=1}^{t} g(E_i),$$

whence, relation (11) of [KR89] reads (one denotes by $\mathrm{Jac}(E_i)$ the jacobian of the curve with function field E_i)

$$\mathrm{Jac}(X_S) \sim \mathrm{Jac}(E_1) \times \cdots \times \mathrm{Jac}(E_t).$$

According to [GS91], the E_i's are the function fields of curves given by

$$w^p - w = \gamma_i x^{q_0}(x^q - x), \gamma_i \in \mathbb{F}_q,$$

thus, the $\mathrm{Jac}(E_i)$'s are supersingular and X_S is a supersingular curve.

A straightforward transposition of this proof yields the analogous result for the Hermitian curve since it is a $\mathbb{F}_q$-cover of $\mathbb{P}^1_{\mathbb{F}_q^2}$ and for the Ree curve since it is $\mathbb{F}_q^2$-cover of $\mathbb{P}^1_{\mathbb{F}_q}$.

□

1 MAXIMAL WILD MONODROMY IN UNEQUAL CHARACTERISTIC.

"La mesure d'aimer, c'est d'aimer sans mesure."
St Bernard

Table of Contents

1.1 INTRODUCTION.

Let (R, v) be a complete discrete valuation ring of mixed characteristic $(0, p)$ with fraction field K containing a primitive p-th root of unity ζ_p and algebraically closed residue field k. The stable reduction theorem states that given a smooth, projective, geometrically connected curve C/K of genus $g(C) \geqslant 2$, there exists a unique minimal Galois extension M/K called *the monodromy extension of* C/K such that $C_M := C \times M$ has stable reduction over M. The group $G = \mathrm{Gal}(M/K)$ is the *monodromy group of* C/K. In one of their papers, C. Lehr and M. Matignon [LM06] gave an algorithm to determine the stable reduction of p-cyclic covers of $\mathbb{P}^1_K$ under the extra assumption of *equidistant geometry* of the branch locus and obtain information about the monodromy extension M/K of C/K. This makes effective a theorem of Raynaud [Ray90] in the case of p-cyclic covers of $\mathbb{P}^1_K$. In this chapter, one studies examples of such p-cyclic covers but is independent of their work and develops specific methods to treat our special covers.

Let $C \to \mathbb{P}^1_K$ be a p-cyclic cover with K-rational equidistant geometry. Let $\mathcal{C}$ be the stable model of C_M/M and $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ the subgroup of $\mathrm{Aut}_k(\mathcal{C}_k)$ of elements acting trivially on the reduction in $\mathcal{C}_k$ of the ramification locus of $C_M \to \mathbb{P}^1_M$ (see [Liu02] 10.1.3 for the definition of the reduction map of C_M). One derives from the stable reduction theorem the following injection

$$\mathrm{Gal}(M/K) \hookrightarrow \mathrm{Aut}_k(\mathcal{C}_k)^\#. \tag{1.1}$$

When the p-Sylow subgroups of these groups are isomorphic, one says that the *wild monodromy is maximal*. We are interested in realization of covers such that the p-adic valuation of $|\mathrm{Aut}_k(\mathcal{C}_k)^\#|$ is large compared to $g(\mathcal{C}_k)$ and having maximal wild monodromy. We will study ramification filtrations and Swan conductors of their monodromy extensions.

In Section 1.2, we consider examples of covers of arbitrarily high genus having potential good reduction. Let k be an algebraically closed field of characteristic $p > 0$ and

$K_p := \mathrm{Frac}(W(k))$. Let $n \in \mathbb{N}^\times$, $q = p^n$, ζ_p be a primitive p-th root of unity, $\lambda = \zeta_p - 1$ and $K = K_p(\lambda^{1/(1+q)})$. We study covers C_c/K of $\mathbb{P}^1_K$ defined by $Y^p = 1 + cX^q + X^{1+q}$ with $c \in K^\circ$, $v(\lambda^{p/(1+q)}) > v(c)$ and $v(c^p - c) \geqslant v(p)$.

Theorem 1.1.1. *The stable reduction $\mathcal{C}_k/k$ is canonically a p-cyclic cover of $\mathbb{P}^1_k$. It is smooth, ramified at one point ∞ and étale outside ∞. The ramification locus of $C_M \to \mathbb{P}^1_M$ reduces in ∞ and the group $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ has a unique p-Sylow subgroup $\mathrm{Aut}_k(\mathcal{C}_k)^\#_1$. Moreover, the curve C_c/K has maximal wild monodromy M/K. The extension M/K is the decomposition field of an explicitly given polynomial and $\mathrm{Gal}(M/K) \simeq \mathrm{Aut}_k(\mathcal{C}_k)^\#_1$ is an extra-special p-group of order pq^2.*

Let X/k be a p-cyclic cover of $\mathbb{P}^1_k$ of genus $g(X)$, ramified at one point ∞ and étale outside ∞. According to [LM05], the p-Sylow subgroup $G_{\infty,1}(X)$ of the subgroup of $\mathrm{Aut}_k(X)$ of automorphisms leaving ∞ fixed satisfies $|G_{\infty,1}(X)| \leqslant \frac{4p}{(p-1)^2} g(X)^2$. The stable reduction $\mathcal{C}_k/k$ of Theorem 1.1.1 is such that $G_{\infty,1}(\mathcal{C}_k) = \mathrm{Aut}_k(\mathcal{C}_k)^\#_1$ and satisfies $|G_{\infty,1}(\mathcal{C}_k)| = \frac{4p}{(p-1)^2} g(\mathcal{C}_k)^2$. So we obtain the largest possible maximal wild monodromy for curves over some finite extension of K_p with genus in $\frac{p-1}{2} p^{\mathbb{N}}$ in the good reduction case.

The group $G_{\infty,1}(\mathcal{C}_k) = \mathrm{Aut}_k(\mathcal{C}_k)^\#_1$ is endowed with the natural ramification filtration $(G_{\infty,i}(\mathcal{C}_k))_{i\geqslant 0}$. Let $Z := Z(G_{\infty,1}(\mathcal{C}_k))$ be the center of $G_{\infty,1}(\mathcal{C}_k)$, it is a cyclic group of order p generated by the Artin-Schreier morphism, see [LM05]. Applying the Riemann-Hurwitz formula and the Different formula (see [Ser79] IV §2 Proposition 4) to the Galois covers

$$\mathcal{C}_k \to \mathcal{C}_k/Z \simeq \mathbb{P}^1_k \text{ and } \mathcal{C}_k/Z \simeq \mathbb{P}^1_k \to \mathcal{C}_k/G_{\infty,1}(\mathcal{C}_k) \simeq \mathbb{P}^1_k,$$

one shows that

$$G_{\infty,0}(\mathcal{C}_k) = G_{\infty,1}(\mathcal{C}_k) \supsetneq Z(G_{\infty,0}(\mathcal{C}_k)) = G_{\infty,2}(\mathcal{C}_k) = \cdots = G_{\infty,1+q}(\mathcal{C}_k) \supsetneq \{1\}.$$

Moreover, the group $G := \mathrm{Gal}(M/K)$ being the Galois group of a finite extension of K_p, it is endowed with the ramification filtration $(G_i)_{i\geqslant 0}$ of an arithmetic nature. Since $G \simeq G_{\infty,1}(\mathcal{C}_k)$ it is natural to ask for the behavior of $(G_i)_{i\geqslant 0}$ under (1.1), that is to compare $(G_i)_{i\geqslant 0}$ and $(G_{\infty,i}(\mathcal{C}_k))_{i\geqslant 0}$. One shows that they actually coincide and we compute the conductor exponent $f(\mathrm{Jac}(C_c)/K)$ of $\mathrm{Jac}(C_c)/K$ and its Swan conductor $\mathrm{sw}(\mathrm{Jac}(C_c)/K)$.

Theorem 1.1.2. *Under the hypotheses of Theorem 1.1.1, the lower ramification filtration of G is*

$$G = G_0 = G_1 \supsetneq Z(G) = G_2 = \cdots = G_{1+q} \supsetneq \{1\}.$$

Then, $f(\mathrm{Jac}(C_c)/K) = (2q+1)(p-1)$ and, in the case where $c \in K_p^\circ$, $\mathrm{sw}(\mathrm{Jac}(C_c)/K_p) = 1$.

The value $\mathrm{sw}(\mathrm{Jac}(C_c)/K_p) = 1$ is the smallest one among abelian varieties over K_p with non-tame monodromy extension. That is, in some sense, a counterpart of [BK05] and [LRS93] where an upper bound for the conductor exponent is given and it is shown that this bound is actually achieved.

In Section 1.3, one considers the case $p = 2$ and genus 2. In this situation there are three possible types of geometry for the stable reduction. In each case, one gives a family of curves with the prescribed degeneration type such that the wild monodromy is maximal. This has applications to the Inverse Galois Problem. For example, we have the following

Proposition 1.1.1. *Let* $K = K_2(2^{1/15})$ *and* C_0/K *the smooth, projective, geometrically integral curve given by* $Y^2 = 1 + 2^{3/5}X^2 + X^3 + 2^{2/5}X^4 + X^5$. *The irreducible components of its stable reduction* $\mathcal{C}_k/k$ *are elliptic curves. The monodromy extension* M/K *of* C_0/K *is the decomposition field of an explicitly given polynomial. The curve* C_0/K *has maximal wild monodromy and* $G := \mathrm{Gal}(M/K) \simeq Q_8 \times Q_8$. *Moreover, we have*

$$G_i \simeq \begin{cases} Q_8 \times Q_8, & -1 \leqslant i \leqslant 1, \\ Z(Q_8) \times Q_8, & 2 \leqslant i \leqslant 3, \\ \{1\} \times Q_8 & 4 \leqslant i \leqslant 31, \\ \{1\} \times Z(Q_8), & 32 \leqslant i \leqslant 543, \\ \{1\} \times \{1\}, & 544 \leqslant i. \end{cases}$$

and $\mathrm{sw}(\mathrm{Jac}(C_0)/K) = 45$.

Remark : Throughout this chapter, one describes monodromy extensions as decomposition fields of explicitly given polynomials being p-adic approximations of the so-called *monodromy polynomial* of [LM06]. The point is that the roots of the monodromy polynomial are the centers of the blowing-ups giving the stable reduction of a p-cyclic cover of $\mathbb{P}^1_K$ with equidistant geometry. For a given genus, the expression of the monodromy polynomial is somehow generic meaning that it is a polynomial in the coefficients of the polynomial $f(X)$ where $Y^p = f(X)$ is the equation of the p-cyclic covering that we consider. That is why dealing directly with the monodromy polynomial is far too complicated. Since p-adically close polynomials with same degrees define the same extensions, it was natural to drop terms having a small p-adic contribution in our examples to obtain modified monodromy polynomials easier to handle than the actual monodromy polynomial.

1.2 COVERS WITH POTENTIAL GOOD REDUCTION.

We start by fixing notations that will be used throughout this Section.

Notations : Let $n \in \mathbb{N}^\times$, $q = p^n$ and $a_n = (-1)^q(-p)^{p+p^2+\cdots+q}$. Let k be an algebraically closed field of characteristic $p > 0$, $K_p = \mathrm{Frac}(W(k))$ and $K = K_p(\lambda^{1/(1+q)})$. We denote by $\mathfrak{m}$ the maximal ideal of $(K^{alg})^\circ$. Let $R = K^\circ$, for $c \in R$ let

$$f_{q,c}(X) = 1 + cX^q + X^{1+q}.$$

One defines the *modified monodromy polynomial* by

$$L_c(X) = X^{q^2} - a_n(c + X)f_{q,c}(X)^{q-1}.$$

Let C_c/K and A_q/k be the smooth projective integral curves birationally given respectively by $Y^p = f_{q,c}(X)$ and $w^p - w = t^{1+q}$.

First of all, one gives an easy technical lemma that will be used in the proof of the main theorem of Section 1.2.

Lemma 1.2.1. *For* $s \in \mathbb{N} - \{0\}$, $A \in K^{alg}$ *with* $v(A) > 0$ *and* $B \in (K^{alg})^\circ[T]$

$$(A + B)^{p^s} \equiv (A^{p^{s-1}} + B^{p^{s-1}})^p \bmod p^2\mathfrak{m}[T], \tag{1.2}$$

Proof. The proof goes by induction on s. For $s = 1$, the equation 1.2 is an equality, let's do the case $s = 2$.

$$(A+B)^{p^2} = ((A+B)^p)^p = (A^p + B^p + R)^p = (A^p + B^p)^p + R^p + \tilde{\Sigma},$$

where

$$R := \sum_{k=1}^{p-1} \binom{p}{k} A^k B^{p-k} \in p\mathfrak{m}[T],$$
$$\tilde{\Sigma} := \sum_{k=1}^{p-1} \binom{p}{k} (A^p + B^p)^k R^{p-k}.$$

So $R^p \in p^p\mathfrak{m}[T]$ and $\tilde{\Sigma} \in p^2\mathfrak{m}[T]$. Let $s \geqslant 3$ and assume that equation 1.2 is true for $s-1$, then one writes

$$(A+B)^{p^s} = ((A+B)^{p^{s-1}})^p \equiv (A^{p^{s-2}} + B^{p^{s-2}})^{p^2} \bmod p^2\mathfrak{m}[T],$$

and one concludes as in the case $s = 2$. □

Theorem 1.2.1. *The curve C_c/K has potential good reduction isomorphic to A_q/k.*

1. *If $v(c) \geqslant v(\lambda^{p/(1+q)})$, then the monodromy extension of C_c/K is trivial.*
2. *If $v(c) < v(\lambda^{p/(1+q)})$, let y be a root of $L_c(X)$ in K^{alg}. Then C_c has good reduction over $K(y, f_{q,c}(y)^{1/p})$. If $L_c(X)$ is irreducible over K, then C_c/K has maximal wild monodromy. The monodromy extension of C_c/K is $M = K(y, f_{q,c}(y)^{1/p})$ and $G = \mathrm{Gal}(M/K)$ is an extra-special p-group of order pq^2.*
3. *If $c \in R$ with $v(c) = 0$ and $v(c^p - c) \geqslant v(p)$, then $L_c(X)$ is irreducible over K, the lower ramification filtration of G is*

$$G = G_0 = G_1 \supsetneq G_2 = \cdots = G_{1+q} = Z(G) \supsetneq \{1\},$$

and $f(\mathrm{Jac}(C_c)/K) = (2q+1)(p-1)$. If, moreover, $c \in K_p$ then $\mathrm{sw}(\mathrm{Jac}(C_c)/K_p) = 1$.

Proof. 1. Assume that $v(c) \geqslant v(\lambda^{p/(1+q)})$. Set $\lambda^{p/(1+q)}T = X$ and $\lambda W + 1 = Y$. Then, the equation defining C_c/K becomes

$$(\lambda W + 1)^p = \sum_{i=0}^{p} \binom{p}{i} \lambda^i W^i = 1 + c\lambda^{pq/(1+q)} T^q + \lambda^p T^{1+q}.$$

After simplification by λ^p and reduction modulo π_K this equation gives

$$w^p - w = at^q + t^{1+q},\ a \in k. \tag{1.3}$$

By Riemann-Hurwitz formula the genus of the curve defined by (1.3) is seen to be that of C_c/K . Applying [Liu02] 10.3.44, there is a component in the stable reduction birationally given by (1.3). The stable reduction being a tree, the curve C_c/K has good reduction over K.

2. The proof of the first part is divided into six steps. **Step I** is a technical prerequisite, in **Step II** and **Step III** one writes a stable model of C_c/K over a finite extension of K and under the extra assumption that $L_c(X)$ is irreducible over K, we will prove in **Step VI** that this is the wild monodromy extension. Let y be a root of $L_c(X)$.

Step I : *One has* $v(y) = v(a_n c)/q^2$.

Since y is a root of $L_c(X)$, one has

$$y^{q^2} = a_n(c+y)f_{q,c}(y)^{q-1},$$

so $v(y) > 0$. Assume that $v(c+y) \geqslant v(y)$. Then, $q^2 v(y) \geqslant v(a_n) + v(y)$ and

$$v(c) \geqslant v(y) \geqslant \frac{v(a_n)}{q^2-1} = \frac{p}{q+1}v(\lambda),$$

which is a contradiction. So $v(c+y) < v(y)$ thus $v(c+y) = v(c)$.

Step II : *Define* S *and* T *by* $\lambda^{p/(1+q)}T = (X-y) = S$. *Then,*

$$f_{q,c}(S+y) \equiv f_{q,c}(y) + y^q S + (c+y)S^q + S^{1+q} \bmod \lambda^p \mathfrak{m}[T].$$

Using the following formula for $A \in K^{alg}$ with $v(A) > 0$ and $B \in (K^{alg})^\circ[T]$

$$(A+B)^q \equiv (A^{q/p} + B^{q/p})^p \bmod p^2\mathfrak{m}[T],$$

one computes $\bmod \lambda^p\mathfrak{m}[T]$

$$\begin{aligned} f_{q,c}(y+S) &= 1 + c(y+S)^q + (y+S)^{1+q} \\ &\equiv 1 + c(y^{q/p} + S^{q/p})^p + (y+S)(y^{q/p} + S^{q/p})^p \\ &\equiv f_{q,c}(y) + (y^q + \Sigma)S + (c+y)S^q + S^{1+q} + (c+y)\Sigma, \end{aligned}$$

where $\Sigma = \sum_{k=1}^{p-1} \binom{p}{k} y^{kq/p} S^{(p-k)q/p}$. Using **Step I**, one checks that $\Sigma \in \lambda^p\mathfrak{m}[T]$.

Step III : *Let* $R_1 := K[y]^\circ$. *For all* $0 \leqslant i \leqslant n$, *there exist* $B_i \in R_1$ *and* $A_i(S) \in R_1[S]$ *such that* $\bmod \lambda^p\mathfrak{m}[T]$ *one has*

$$f_{q,c}(S+y) \equiv f_{q,c}(y)(1 + SA_i(S))^p + y^q S + B_i S^{q/p^i} + S^{1+q}. \tag{1.4}$$

One defines the $A_i(S)$'s and the B_i's by induction. For all $0 \leqslant i \leqslant n-1$, let

$$\begin{aligned} B_n &:= -y^q \qquad &&\text{and} \quad B_i := f_{q,c}(y)\frac{B_{i+1}^p}{(-pf_{q,c}(y))^p}, \\ A_0(S) &:= 0 \qquad &&\text{and} \quad SA_{i+1}(S) := SA_i(S) - p^{-1}f_{q,c}(y)^{-1}B_{i+1}S^{q/p^{i+1}}. \end{aligned}$$

One checks that for all $0 \leqslant i \leqslant n$

$$B_i/f_{q,c}(y) = (-p)(-p)^{-1-p-\cdots-p^{n-i}}(-y^q/f_{q,c}(y))^{p^{n-i}},$$

and

$$v(B_i) \geqslant (1 + \frac{1}{p} + \cdots + \frac{1}{p^{i-1}})v(p), \ \forall 1 \leqslant i \leqslant n. \tag{1.5}$$

It follows that $\forall\ 1 \leqslant i \leqslant n$, $p^{-1}B_i \in R_1$, $\forall\ 0 \leqslant i \leqslant n$ $A_i(S) \in R_1[S]$ and $B_0 = c + y$ since $L_c(y) = 0$.

One proves this step by induction on i. According to **Step II**, the equation (1.4) holds for $i = 0$. Assume that equation (1.4) is satisfied for i. From the definition of $SA_i(S)$, one has

$$SA_i(S) = SA_{i+1}(S) + p^{-1}f_{q,c}(y)^{-1}B_{i+1}S^{q/p^{i+1}},$$

one has that $f_{q,c}(S+y)$ is congruent mod $\lambda^p\mathfrak{m}[T]$ to

$$\begin{aligned}
&f_{q,c}(y)\big[1+SA_i(S)\big]^p + B_iS^{q/p^i} + y^qS + S^{1+q}\\
\equiv&f_{q,c}(y)\big[1+SA_{i+1}(S)\big]^p + f_{q,c}(y)\Sigma + f_{q,c}(y)\frac{B_{i+1}^pS^{q/p^i}}{p^pf_{q,c}(y)^p} + B_iS^{q/p^i} + y^qS + S^{1+q},
\end{aligned}$$

where

$$\Sigma := \sum_{k=1}^{p-1}\binom{p}{k}\Big(\frac{B_{i+1}}{pf_{q,c}(y)}S^{q/p^{i+1}}\Big)^k(1+SA_{i+1}(S))^{p-k}.$$

We will use the fact that

$$\begin{aligned}
&f_{q,c}(y)(1+(-1)^p)\frac{B_{i+1}^p}{p^pf_{q,c}(y)^p}S^{q/p^i},\\
&\sum_{k=2}^{p-1}\binom{p}{k}\Big(\frac{B_{i+1}}{pf_{q,c}(y)}S^{q/p^{i+1}}\Big)^k(1+SA_{i+1}(S))^{p-k},\\
&B_{i+1}S^{q/p^{i+1}}\sum_{k=1}^{p-1}\binom{p-1}{k}S^kA_{i+1}(S)^k,
\end{aligned}$$

are in $\lambda^p\mathfrak{m}[T]$. Recall that

$$B_i := f_{q,c}(y)\frac{B_{i+1}^p}{(-pf_{q,c}(y))^p},$$

thus

$$\begin{aligned}
f_{q,c}(y)\frac{B_{i+1}^pS^{q/p^i}}{p^pf(y)^p} + B_iS^{q/p^i} =&f_{q,c}(y)(1+(-1)^p)\frac{B_{i+1}^p}{p^pf_{q,c}(y)^p}S^{q/p^i}\\
\equiv&0 \mod \lambda^p\mathfrak{m}[T].
\end{aligned}$$

Then one computes

$$\begin{aligned}
f_{q,c}(y)\Sigma =&f_{q,c}(y)\sum_{k=1}^{p-1}\binom{p}{k}\Big(\frac{B_{i+1}}{pf_{q,c}(y)}S^{q/p^{i+1}}\Big)^k(1+SA_{i+1}(S))^{p-k}\\
\equiv&pf_{q,c}(y)(1+SA_{i+1}(S))^{p-1}\frac{B_{i+1}}{pf_{q,c}(y)}S^{q/p^{i+1}}\\
\equiv&(1+SA_{i+1}(S))^{p-1}B_{i+1}S^{q/p^{i+1}}\\
\equiv&B_{i+1}S^{q/p^{i+1}} \mod \lambda^p\mathfrak{m}[T],
\end{aligned}$$

giving the equation (1.4) for $i+1$.

Step IV : *The curve* C_c/K *has good reduction over* $K(y, f_{q,c}(y)^{1/p})$.

Applying **Step III** for $i = n$, one gets

$$f_{q,c}(y+S) \equiv f_{q,c}(y)(1+SA_n(S))^p + S^{1+q} \bmod \lambda^p \mathfrak{m}[T],$$

then the change of variables in $K(y, f_{q,c}(y)^{1/p})$

$$X = \lambda^{p/(1+q)}T + y = S + y \text{ and } \frac{Y}{f_{q,c}(y)^{1/p}} = \lambda W + 1 + SA_n(S),$$

induces in reduction $w^p - w = t^{1+q}$ with genus $g(C_c)$. So [Liu02] 10.3.44 implies that the above change of variables gives the stable model.

Step V : *For any distinct roots* y_i, y_j *of* $L_c(X)$, $v(y_i - y_j) = v(\lambda^{p/(1+q)})$.

The changes of variables

$$T = (X - y_i)/\lambda^{p/(1+q)} \text{ and } T = (X - y_j)/\lambda^{p/(1+q)},$$

induce equivalent Gauss valuations of $K(C_c)$ else applying [Liu02] 10.3.44 would contradict the uniqueness of the stable model. In particular

$$v(y_i - y_j) \geqslant v(\lambda^{p/(1+q)}).$$

Using **Step I**, one checks that $v(q^2 y^{q^2-1}) > v(a_n)$ and $v(f'_{q,c}(y)) > 0$, so

$$v(L'_c(y)) = v(a_n) = (q^2-1)v(\lambda^{p/(1+q)}).$$

Taking into account that $L'_c(y_i) = \prod_{j \neq i}(y_i - y_j)$ and $\deg L_c(X) = q^2$, one obtains that $v(y_i - y_j) = v(\lambda^{p/(1+q)})$.

Step VI : *If* $L_c(X)$ *is irreducible over* K, *then* C_c/K *has maximal wild monodromy, the extension* $K(y, f_{q,c}(y)^{1/p})/K$ *is the monodromy extension* M *of* C_c/K *and* $G := \mathrm{Gal}(M/K)$ *is an extraspecial* p*-group of order* pq^2.

Let $(y_i)_{i=1,\dots,q^2}$ be the roots of $L_c(X)$, $L := K(y_1, \dots, y_{q^2})$ and M/K be the monodromy extension of C_c/K. Any $\tau \in \mathrm{Gal}(L/K) - \{1\}$ is such that $\tau(y_i) = y_j$ for some $i \neq j$. Thus, the change of variables

$$X = \lambda^{p/(1+q)}T + y_i \text{ and } \frac{Y}{f_{q,c}(y_i)^{1/p}} = \lambda W + 1 + SA_n(S),$$

induces the stable model and τ acts on it by

$$\tau(T) = \frac{X - y_j}{\lambda^{p/(1+q)}}, \quad \text{hence} \quad T - \tau(T) = \frac{y_j - y_i}{\lambda^{p/(1+q)}}. \tag{1.6}$$

According to **Step V** and equations (1.6), τ acts non-trivially on the stable reduction, it follows that $L \subseteq M$. Indeed if $\mathrm{Gal}(K^{alg}/M) \not\subseteq \mathrm{Gal}(K^{alg}/L)$ it would exist $\sigma \in \mathrm{Gal}(K^{alg}/M)$

inducing $\bar{\sigma} \neq \mathrm{Id} \in \mathrm{Gal}(L/K)$, this would contradict the characterization of $\mathrm{Gal}(K^{alg}/M)$ (see remark after Theorem 0.1.1).

According to Proposition 0.6.3 , the p-Sylow subgroup $\mathrm{Aut}_k(\mathcal{C}_k)_1^\#$ of $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ is an extra-special p-group of order pq^2. Moreover, one has the exact sequence

$$0 \to Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^\#) \to \mathrm{Aut}_k(\mathcal{C}_k)_1^\# \to (\mathbb{Z}/p\mathbb{Z})^{2n} \to 0,$$

where $(\mathbb{Z}/p\mathbb{Z})^{2n}$ is identified with the group of translations $t \mapsto t + a$ extending to elements of $\mathrm{Aut}_k(\mathcal{C}_k)_1^\#$. Therefore we have morphisms

$$\mathrm{Gal}(M/K) \overset{i}{\hookrightarrow} \mathrm{Aut}_k(\mathcal{C}_k)_1^\# \overset{\varphi}{\to} \mathrm{Aut}_k(\mathcal{C}_k)_1^\#/Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^\#).$$

The composition is seen to be surjective since the image contains the q^2 translations

$$t \mapsto t + \overline{(y_i - y_1)/\lambda^{p/(1+q)}},\ 1 \leqslant i \leqslant q^2.$$

Consequently, $i(\mathrm{Gal}(M/K))$ is a subgroup of $\mathrm{Aut}_k(\mathcal{C}_k)_1^\#$ of index at most p. So it contains

$$\Phi(\mathrm{Aut}_k(\mathcal{C}_k)_1^\#) = Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^\#) = \mathrm{Ker}\,\varphi.$$

It implies that i is an isomorphism. Thus $[M : K] = pq^2$. According to **Step IV**, one has $M \subseteq K(y, f_{q,c}(y)^{1/p})$, hence $M = K(y, f_{q,c}(y)^{1/p})$.

We show, for later use, that $K(y_1)/K$ is Galois and that $\mathrm{Gal}(M/K(y_1)) = Z(G)$. Indeed, $M/K(y_1)$ is p-cyclic and generated by σ defined by

$$\sigma(y_1) = y_1 \text{ and } \sigma(f_{q,c}(y_1)^{1/p}) = \zeta_p^{-1} f_{q,c}(y_1)^{1/p}.$$

According to **Step IV**, σ acts on the stable model by

$$\sigma(S) = S, \quad \sigma\Big(\frac{Y}{f_{q,c}(y_1)^{1/p}}\Big) = \frac{Y}{\zeta_p^{-1} f_{q,c}(y_1)^{1/p}} = \lambda\sigma(W) + 1 + SA_n(S).$$

Hence

$$\frac{\lambda W + 1 + SA_n(S)}{\zeta_p^{-1}} = \lambda\sigma(W) + 1 + SA_n(S),$$

$$\text{thus,} \quad \sigma(W) = \zeta_p W + 1 + SA_n(S).$$

It follows that σ acts on the stable reduction as the Artin-Schreier morphism that generates $Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^\#)$. It implies that $\mathrm{Gal}(M/K(y_1)) = Z(G)$, thus the extension $K(y_1)/K$ is Galois and

$$\mathrm{Gal}(K(y_1)/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{2n}.$$

3. We now prove the statements concerning the arithmetic of M/K. We assume that $c \in R$ with $v(c^p - c) \geqslant v(p)$ and we split the proof into 5 steps. Let y be a root of $L_c(X)$, let $G := \mathrm{Gal}(M/K)$ and $L := K(y)$. One puts

$$b_n := (-1)(-p)^{1+p+\cdots+p^{n-1}}.$$

Note that $b_n^p = a_n$ and $b_n^p = a_n$. Moreover since $v(c^p - c) \geqslant v(p)$, the condition $v(\lambda^{p/(1+q)}) > v(c)$ implies $v(c) = 0$.

Step A : *The polynomial* $L_c(X)$ *is irreducible over* K.

One computes

$$\begin{aligned}(y^{q^2/p} - cb_n)^p &= y^{q^2} + (-c)^p a_n + \Sigma \\ &= a_n(1 + y^q(c+y))^{q-1}(c+y) + (-c)^p a_n + \Sigma \\ &= a_n \sum_{k=0}^{q-1} \binom{q-1}{k} y^{kq}(c+y)^{1+k} + (-c)^p a_n + \Sigma \\ &= a_n y + a_n(c + (-c)^p) + a_n \Sigma' + \Sigma,\end{aligned}$$

where $\Sigma := \sum_{k=1}^{p-1} \binom{p}{k} y^{kq^2/p}(-cb_n)^{p-k}$ and $\Sigma' := \sum_{k=1}^{q-1} \binom{q-1}{k} y^{kq}(c+y)^{1+k}$.

Using **Step I** one checks that

$$v(\Sigma) > v(a_n y) \text{ and } v(\Sigma') \geqslant v(y^q) > v(y).$$

By assumption $v(c^p - c) \geqslant v(p)$ and $v(p) > v(y)$, thus

$$v(y^{q^2/p} - cb_n) = \frac{v(a_n y)}{p},$$

and $t := p^{q^2}(y^{q^2/p} - cb_n)^{-(p-1)(q+1)} \in L$ has valuation $v_L(p)/q^2 = [L : K_p]/q^2$. So q^2 divides $[L : K]$. It implies that $L_c(X)$ is irreducible over K. In particular

$$L = K(y) = K(y_1, \ldots, y_{q^2}),$$

where $(y_i)_{i=1\ldots q^2}$ are the roots of $L_c(X)$.

Step B : *Reduction step.*

The last non-trivial group G_{i_0} of the lower ramification filtration $(G_i)_{i\geqslant 0}$ of G is a subgroup of $Z(G)$ ([Ser79] IV §2 Corollary 2 of Proposition 9) and as $Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$, it follows that $G_{i_0} = Z(G)$.

According to **Step VI** the group $H := \mathrm{Gal}(M/L)$ is $Z(G)$. Consequently, the filtration $(G_i)_{i\geqslant 0}$ can be deduced from that of M/L and L/K (see [Ser79] IV §2 Proposition 2 and Corollary of Proposition 3).

Step C : *The ramification filtration of* L/K *is*

$$(G/H)_0 = (G/H)_1 \supsetneq (G/H)_2 = \{1\}.$$

Since K/K_p is tamely ramified of degree $(p-1)(q+1)$, one has $K = K_p(\pi_K)$ with $\pi_K^{(p-1)(q+1)} = p$ for some uniformizer π_K of K. In particular

$$z := \frac{\pi_K^{q^2}}{y^{q^2/p} - cb_n},$$

is such that $t = z^{(p-1)(q+1)}$. Then, following the proof of **Step A**, z is a uniformizer of L. Let y and y' be two distinct roots of $L_c(X)$. Let $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(y) = y'$. Then

$$\begin{aligned}\sigma(z) - z &= \frac{\pi_K^{q^2}}{y'^{q^2/p} - cb_n} - \frac{\pi_K^{q^2}}{y^{q^2/p} - cb_n} \\ &= \pi_K^{q^2} \frac{y^{q^2/p} - y'^{q^2/p}}{(y^{q^2/p} - cb_n)(y'^{q^2/p} - cb_n)},\end{aligned}$$

so $v(\sigma(z)-z) = 2v(z) - q^2 v(\pi_K) + v(y'^{q^2/p} - y^{q^2/p})$. It follows from

$$(y-y')^{q^2/p} = y^{q^2/p} + (-y')^{q^2/p} + \sum_{k=1}^{\frac{q^2}{p}-1} \binom{q^2/p}{k} y^k (-y')^{\frac{q^2}{p}-k},$$

and $v(y) = v(y')$, $v(p) + \frac{q^2}{p} v(y) > \frac{q^2}{p} v(y-y')$ (use **Step I** and **Step V**) that

$$v(y^{q^2/p} - y'^{q^2/p}) = \frac{q^2}{p} v(y-y') = q^2 v(\pi_K).$$

Hence $v(\sigma(z)-z) = 2v(z)$. This means that $(G/H)_2 = \{1\}$.

Step D : *Let* $s := (q+1)(pq^2-1)$. *There exist* $u \in L$, $r \in \pi_L^s \mathfrak{m}$ *such that*

$$f_{q,c}(y)u^p = 1 + py^{q/p}\left(\frac{y^{q^2/p}}{b_n} - c\right) + r,$$

and $v_L\left(py^{q/p}\left(\frac{y^{q^2/p}}{b_n} - c\right)\right) = s$.

To prove the second statement, we note that

$$\left(\frac{y^{q^2/p}}{b_n}\right)^p = f_{q,c}(y)^{q-1}(c+y) = \sum_{k=0}^{q-1} \binom{q-1}{k} y^{kq}(c+y)^{1+k} = c + y + \Sigma,$$

with $\Sigma := \sum_{k=1}^{q-1} \binom{q-1}{k} y^{kq}(c+y)^{1+k}$. We set $h := \frac{y^{q^2/p}}{b_n} - c$ and compute

$$\begin{aligned} h^p &= \left(\frac{y^{q^2/p}}{b_n}\right)^p + (-c)^p + \sum_{k=1}^{p-1} \binom{p}{k} \left(\frac{y^{q^2/p}}{b_n}\right)^k (-c)^{p-k} \\ &= c + (-c)^p + y + \Sigma + \sum_{k=1}^{p-1} \binom{p}{k} \left(\frac{y^{q^2/p}}{b_n}\right)^k (-c)^{p-k}. \end{aligned}$$

Since $v(c^p - c) \geqslant v(p) > v(y)$, $v(\Sigma) > v(y)$ and $v\left(\frac{y^{q^2/p}}{b_n}\right) \geqslant 0$, one gets

$$v_L(h) = v_L(y)/p = q^2 - 1,$$

and $v_L(py^{q/p}h) = s$.

In order to prove the first claim, if $n \geqslant 2$ we put

$$u := 1 - cy^{q/p} + \sum_{k=0}^{n-2} \frac{y^{(1+q)p^k}}{(-p)^{1+p+\cdots+p^k}} = 1 + w.$$

Then, $f_{q,c}(y)u^p - 1 = 1 + cy^q + y^{1+q} + \Sigma_1 + cy^q\Sigma_1 + y^{1+q}\Sigma_1 - 1$ with

$$\begin{aligned} \Sigma_1 &:= \sum_{k=1}^{p-1} \binom{p}{k} w^k + w^p = pw + \sum_{k=2}^{p-1} \binom{p}{k} w^k + w^p = pw + \Sigma' + w^p \\ &= p\left[-cy^{q/p} - \frac{y^{1+q}}{p} + \sum_{k=1}^{n-2} \frac{y^{(1+q)p^k}}{(-p)^{1+p+\cdots+p^k}}\right] + \Sigma' + w^p, \end{aligned}$$

and $\Sigma' := \sum_{k=2}^{p-1} \binom{p}{k} w^k$, where sums are eventually empty if $n = 2$ or $p = 2$. So

$$f_{q,c}(y)u^p - 1 = cy^q - pcy^{q/p} + \sum_{k=1}^{n-2} \frac{py^{(1+q)p^k}}{(-p)^{1+p+\cdots+p^k}} + \Sigma' + w^p + cpy^q w + cy^q \Sigma' + cy^q w^p + y^{1+q} pw + y^{1+q}\Sigma' + y^{1+q} w^p.$$

Computation shows that $v(w) = v(y^{q/p})$ and we deduce that

$$w^p = (-c)^p y^q + \sum_{k=0}^{n-2} \frac{y^{(1+q)p^{1+k}}}{(-p)^{p+\cdots+p^{1+k}}} \bmod \pi_L^s \mathfrak{m}.$$

One checks that $v_L(y^q p) > s$, $v_L(y^q w^p) > s$ and $v_L(\Sigma') > s$. Hence

$$f_{q,c}(y)u^p - 1 = (c + (-c)^p)y^q - pcy^{q/p} + \sum_{k=1}^{n-2} \frac{py^{(1+q)p^k}}{(-p)^{1+\cdots+p^k}} + \sum_{k=0}^{n-2} \frac{y^{(1+q)p^{1+k}}}{(-p)^{p+\cdots+p^{1+k}}}$$
$$= -pcy^{q/p} + \frac{y^{q/p(1+q)}}{(-p)^{p+\cdots+q/p}} = py^{q/p}\left(\frac{y^{q^2/p}}{b_n} - c\right) \bmod \pi_L^s \mathfrak{m}.$$

If $n = 1$, one puts $u := 1 - cy$ and check that the statement is still true.

Step E : *Computation of conductors.*

From **Step D**, one deduces that the extension M/L is defined by $X^p = 1 + phy^{q/p} + r$ with $r \in \pi_L^s \mathfrak{m}$. From lemma 0.3.1, one gets that $v_M(\mathcal{D}_{M/L}) = (p-1)(q+2)$. Hence

$$\mathbb{Z}/p\mathbb{Z} \simeq H_0 = H_1 = \cdots = H_{1+q} \supsetneq \{1\},$$

and according to **Step B** and **Step C** one has

$$G = G_0 = G_1 \supsetneq Z(G) = G_2 = \cdots = G_{1+q} \supsetneq \{1\}.$$

Let $\ell \neq p$ be a prime number. Since the G-modules $\mathrm{Jac}(C)[\ell]$ and $\mathrm{Jac}(\mathcal{C}_k)[\ell]$ are isomorphic (see [ST68] paragraph 2) one has that for $i \geqslant 0$

$$\dim_{\mathbb{F}_\ell} \mathrm{Jac}(C)[\ell]^{G_i} = \dim_{\mathbb{F}_\ell} \mathrm{Jac}(\mathcal{C}_k)[\ell]^{G_i}.$$

Moreover, for $0 \leqslant i \leqslant 1 + q$ one has $\mathrm{Jac}(\mathcal{C}_k)[\ell]^{G_i} \subseteq \mathrm{Jac}(\mathcal{C}_k)[\ell]^{Z(G)}$.

Then, from $\mathcal{C}_k/Z(G) \simeq \mathbb{P}^1_k$ (see end of **StepVI**) and Lemma 0.5.1, it follows that for $0 \leqslant i \leqslant 1 + q$

$$\dim_{\mathbb{F}_\ell} \mathrm{Jac}(\mathcal{C}_k)[\ell]^{G_i} = 0.$$

According to the Riemann-Hurwitz formula $g(C) = q(p-1)/2$, thus applying Proposition 0.5.1 with ℓ large enough, one gets

$$f(\mathrm{Jac}(C)/K) = (2q+1)(p-1).$$

Moreover, if $c \in K_p$, an easy computation shows that $\mathrm{sw}(\mathrm{Jac}(C)/K_p) = 1$. □

Remark : If $c \in R$ with $v(c) = (a/b)v(p) < v(\lambda^{p/(1+q)})$ and a and b both prime to p, then $L_c(X)$ is irreducible over K. Indeed, the expression of the valuation of any root y of $L_c(X)$ shows that the ramification index of $K(y)/K$ is q^2.

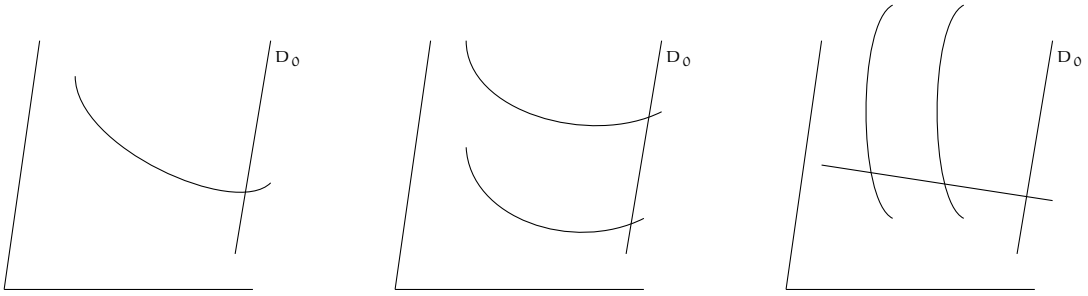
1.3 MONODROMY OF GENUS 2 HYPERELLIPTIC CURVES.

We restrict to the case $p = 2$ and $\deg f(X) = 5$ of the introduction. In this situation, there are three types of geometry for the stable reduction (see Figure 1). For each type of degeneration, we will give an example of cover C/K with maximal wild monodromy and birationally given by

$$Y^2 = f(X) = 1 + b_2X^2 + b_3X^3 + b_4X^4 + X^5 \in R[X],$$

over some R. Define $\mathcal{X}$ to be the R-model of C/K given by $Y^2 = f(X)$ and let's describe each degeneration type.

The Jacobian criterion shows that $\mathcal{X}_k/k$ has two singularities if and only if $\overline{b_3} \neq 0$. Then, type I occurs when $\mathcal{X}_k/k$ has two singularities and by blowing-up $\mathcal{X}$ at these points one obtains two elliptic curves. Type II (resp. type III) occurs in the one singularity case when there are two (resp. one) irreducible components of non 0 genus in the stable reduction. The elliptic curves E/k that we will encounter are birationally given by $w^2 - w = t^3$. We showed in Section 0.6.2 that they are such that $\mathrm{Aut}_k(E) \simeq \mathrm{Sl}_2(\mathbb{F}_3)$ has a unique 2-Sylow subgroup isomorphic to Q_8. We denote by D_0 the *original component* defined in Proposition 0.1.1.



Type III Type I Type II

Figure 1

Notations : For $f(X) \in R[X]$, let

$$f(X + x) = s_0(x) + s_1(x)X + s_2(x)X^2 + s_3(x)X^3 + s_4(x)X^4 + X^5,$$

be the Taylor expansion of f and define

$$T_f(Y) := s_1(Y)^2 - 4s_0(Y)s_2(Y).$$

Degeneration type III

This is the case of potential good reduction. For example, using notations of the previous Section, let $K := K_2((-2)^{1/5})$ and C_1/K be the smooth, projective, geometrically integral curve birationally given by

$$Y^2 = 1 + X^4 + X^5 = f_{4,1}(X).$$

Then, according to Theorem 1.2.1 the curve C_1/K has potential good reduction with maximal wild monodromy M/K, the group $\mathrm{Gal}(M/K)$ is an extra-special of order 2^5, $f(\mathrm{Jac}(C_1)/K) = 9$ and $\mathrm{sw}(\mathrm{Jac}(C_1)/K_2) = 1$.

Degeneration type I

Proposition 1.3.1. *Let* $\rho := 2^{2/3}$, $b_2, b_3, b_4 \in {K_2}^{alg}$, $K := K_2(b_2, b_3, b_4)$ *and* C/K *be the smooth, projective, geometrically integral curve birationally given by*

$$Y^2 = f(X) = 1 + b_2X^2 + b_3X^3 + b_4X^4 + X^5,$$

with $v(b_i) \geqslant 0$ *and* $v(b_3) = 0$. *Assume that* $1 + b_3b_2 + b_3^2b_4 \not\equiv 0 \bmod \pi_K$. *Then* C *has stable reduction of type I and*

$$T_f(Y) = T_{1,f}(Y)T_{2,f}(Y) \text{ with } T_{i,f}(Y) \in K[Y],$$

are such that

$$\overline{T_{1,f}}(Y) = Y^4 \in k[Y], \text{ and } \overline{T_{2,f}}(Y) = Y^4 + \overline{b_3}^2 \in k[Y].$$

Assume moreover that $T_{1,f}(Y)$ *and* $T_{2,f}(Y)$ *are irreducible over* K *and define linearly disjoint extensions of* K, *then* C/K *has maximal wild monodromy* M/K *with group* $\mathrm{Gal}(M/K) \simeq Q_8 \times Q_8$.

Proof. Using Maple, one computes $T_f(Y)$ and reduces it mod 2. The statement about $T_f(Y)$ follows from Hensel's lemma.

Let y be a root of $T_f(Y)$. Define $\rho T = S = X - y$ and choose $s_0(y)^{1/2}$ and $s_2(y)^{1/2}$ such that $2s_0(y)^{1/2}s_2(y)^{1/2} = s_1(y)$. Then

$$\begin{aligned} f(S+y) &= s_0(y) + s_1(y)S + s_2(y)S^2 + s_3(y)S^3 + s_4(y)S^4 + S^5 \\ &= (s_0(y)^{1/2} + s_2(y)^{1/2}S)^2 + s_3(y)S^3 + s_4(y)S^4 + S^5 \\ &= (s_0(y)^{1/2} + s_2(y)^{1/2}\rho T)^2 + s_3(y)\rho^3T^3 + s_4(y)\rho^4T^4 + \rho^5T^5. \end{aligned}$$

The change of variables

$$\rho T = S = X - y \text{ and } Y = 2W + (s_0(y)^{1/2} + s_2(y)^{1/2}S),$$

induces

$$W^2 + (s_0(y)^{1/2} + s_2(y)^{1/2}S)W = s_3(y)T^3 + s_4(y)\rho T^4 + \rho^2T^5,$$

which is an equation of a quasi-projective flat scheme over $K(y, f(y)^{1/2})^\circ$ with special fiber given by $w^2 - w = t^3$.

Let $(y_i)_{i=1,\dots,4}$ (resp. $(y_i)_{i=5,\dots,8}$) be the roots of $T_{1,f}(Y)$ (resp. $T_{2,f}(Y)$). Then, for any $i \in \{1,\dots,4\}$ and $j \in \{5,\dots,8\}$, the above computations show that C has stable reduction over $L := K(y_i, y_j, f(y_i)^{1/2}, f(y_j)^{1/2})$i, use [Liu02] 10.3.44. Moreover two distinct roots of $T_{1,f}(Y)$ (resp. $T_{2,f}(Y)$) induce equivalent Gauss valuations on $K(C)$ by means of the above change of variables, else it would contradict the uniqueness of the stable model. In particular,

$$\begin{aligned} &v(y_i - y_j) \geqslant v(\rho), \ i \neq j \in \{1,2,3,4\} \text{ or } i \neq j \in \{5,6,7,8\}, \\ &v(y_i - y_j) = 0, \ i \in \{1,2,3,4\} \text{ and } j \in \{5,6,7,8\}, \end{aligned} \tag{7}$$

which implies that $v(\mathrm{disc}(T_{1,f}(Y))) + v(\mathrm{disc}(T_{2,f}(Y))) = v(\mathrm{disc}(T_f(Y)))$. In particular, for $i = 1, 2$

$$v(\mathrm{disc}(T_{i,f}(Y))) \geqslant 12v(\rho) = 8v(2).$$

These are equalities if and only if (7) are all equalities. Using Maple, one has

$$2^{-16}\,\mathrm{disc}(T_f(Y)) = b_3^8(1 + b_3b_2 + b_3^2b_4)^4 \bmod 2,$$

thus one gets that (7) are all equalities, therefore

$$0, \frac{y_2 - y_1}{\rho}, \frac{y_3 - y_1}{\rho}, \frac{y_4 - y_1}{\rho},$$

are all distinct mod π_K. Applying Hensel's lemma to $T_{1,f}(\rho Y + y_1)$ shows that $K(y_1)/K$ is Galois. The same holds for $K(y_5)/K$.

Let's denote by E_1/k and E_2/k (resp. ∞_1 and ∞_2) the genus 1 curves in the stable reduction of C (resp. their crossing points with D_0). The group

$$\mathrm{Aut}_k(\mathcal{C}_k)^{\#} \simeq \mathrm{Aut}_{k,\infty_1}(E_1) \times \mathrm{Aut}_{k,\infty_2}(E_2),$$

has a unique 2-Sylow subgroup isomorphic to

$$\mathrm{Syl}_2(\mathrm{Aut}_{k,\infty_1}(E_1)) \times \mathrm{Syl}_2(\mathrm{Aut}_{k,\infty_2}(E_2)),$$

where $\mathrm{Aut}_{k,\infty_i}(E_i) \simeq \mathrm{Sl}_2(\mathbb{F}_3)$ denotes the subgroup of $\mathrm{Aut}_k(E_i)$ leaving ∞_i fixed.

First, we show that L/K is the monodromy extension M/K of C/K. Let $\sigma \in \mathrm{Gal}(L/K)$ inducing the identity on $\mathcal{C}_k/k$. We show that $\forall i \in \{1, \ldots, 8\}$, $\sigma(y_i) = y_i$. Otherwise, since σ is an isometry, $\sigma(y_1) \notin \{y_5, \ldots, y_8\}$ and we can assume that $\sigma(y_1) = y_2$. So

$$\sigma\left(\frac{X - y_1}{\rho}\right) = \frac{X - y_1}{\rho} + \frac{y_1 - y_2}{\rho},$$

so σ does not induce the identity on $\mathcal{C}_k/k$. If $\sigma(s_0(y_i)^{1/2}) = -s_0(y_i)^{1/2}$ for some i then $\sigma(s_2(y_i)^{1/2}) = -s_2(y_i)^{1/2}$ and

$$\sigma(W) - W = s_0(y_i)^{1/2} + s_2(y_i)^{1/2}\rho T,$$

therefore σ acts non-trivially on $\mathcal{C}_k/k$. Thus, $\forall\ i \in \{1, \ldots, 8\}$, $\sigma(s_0(y_i)^{1/2}) = s_0(y_i)^{1/2}$ and $\sigma = \mathrm{Id}$. Since $M \subseteq L$, this shows that $L = M$.

Now, we show that the wild monodromy is maximal assuming that $T_{1,f}(Y)$ and $T_{2,f}(Y)$ are irreducible over K and define linearly disjoint extensions. One has natural morphisms

$$\mathrm{Gal}(M/K) \xhookrightarrow{i} Q_8 \times Q_8 \xrightarrow{p} Q_8 \times Q_8/Z(Q_8) \xrightarrow{q} Q_8/Z(Q_8) \times Q_8/Z(Q_8).$$

For any $i \in \{1, \ldots, 4\}$ and $j \in \{5, \ldots, 8\}$, $(i, j) \neq (1, 5)$, there exists $\sigma_{i,j} \in \mathrm{Gal}(M/K)$ such that

$$\sigma_{i,j}(y_1) = y_i \quad \text{and} \quad \sigma_{i,j}(y_5) = y_j,$$

which is seen to act non-trivially on $\mathcal{C}_k/k$. The composition $q \circ p \circ i$ is then surjective, it implies that $p \circ i(\mathrm{Gal}(M/K))$ is a subgroup of $Q_8 \times Q_8/Z(Q_8)$ of index at most 2 so it contains

$$\Phi(Q_8 \times Q_8/Z(Q_8)) = Z(Q_8) \times \{1\} = \mathrm{Ker}\, q.$$

It follows that $p \circ i$ is onto and $i(\mathrm{Gal}(M/K))$ is a subgroup of $Q_8 \times Q_8$ of index at most 2 so it contains

$$\Phi(Q_8 \times Q_8) = Z(Q_8) \times Z(Q_8) \supseteq \mathrm{Ker}\, p.$$

Finally, one has $i(\mathrm{Gal}(M/K)) = Q_8 \times Q_8$. □

Example : Let $f_0(X) := 1 + 2^{3/5}X^2 + X^3 + 2^{2/5}X^4 + X^5$ and $K := K_2(2^{\frac{1}{15}})$. With the notations of Proposition 1.3.1, one has

$$1 + b_3b_2 + b_3^2b_4 \not\equiv 0 \bmod \pi_K.$$

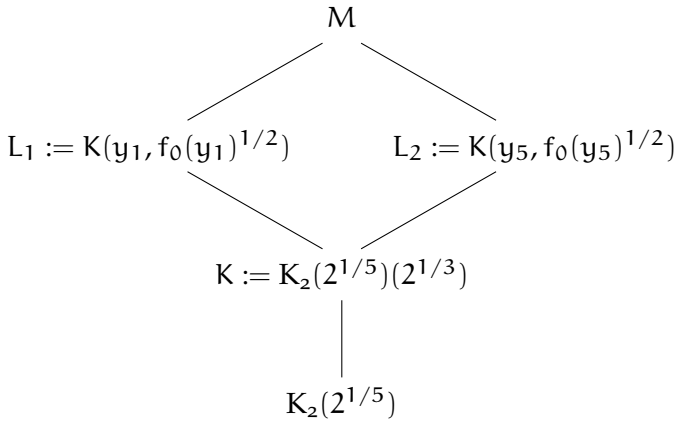
Then, one checks using Magma that $T_{f_0}(Y) = T_{1,f_0}(Y)T_{2,f_0}(Y)$ where $T_{1,f_0}(Y)$ and $T_{2,f_0}(Y)$ are irreducible polynomials over K and $T_{2,f_0}(Y)$ is irreducible over the decomposition field of $T_{1,f_0}(Y)$. So, the curve C_0/K defined by $Y^2 = f_0(X)$ has maximal wild monodromy M/K with group $\mathrm{Gal}(M/K) \simeq Q_8 \times Q_8$.

```
q2:= pAdicField(2,8);
q2x<x>:=PolynomialRing(q2);
k<pi>:=TotallyRamifiedExtension(q2,x^15-2);
K<rho>:=UnramifiedExtension(k,8);
Ky<y>:=PolynomialRing(K);
b3:=1;
b2:=pi^9;
b4:=pi^6;
T:=(2*b2*y+3*b3*y^2+4*b4*y^3+5*y^4)^2-
4*(1+b2*y^2+b3*y^3+b4*y^4+y^5)*(b2+3*b3*y+6*b4*y^2+10*y^3);
F,a,A:=Factorization(T: Extensions:= true);
Degree(F[1][1]);Degree(F[2][1]);
L1:=A[1]‘Extension;
L1Y<Y>:=PolynomialAlgebra(L1);
TY:=L1Y!Eltseq(T);
G:=Factorization(TY);
G[1][2];G[2][2];G[3][2];G[4][2];G[5][2];
Degree(G[5][1]);
```

This has the following consequence for the Inverse Galois Problem.

Corollary 1.3.1. *With the notations of the above example, let* $(y_i)_{i=1,\dots,8}$ *be the roots of* $T_{f_0}(Y)$ *and* $M = K(y_1, \dots, y_8, f_0(y_1)^{1/2}, \dots, f_0(y_8)^{1/2})$. *Then* M/K *is Galois with Galois group isomorphic to* $Q_8 \times Q_8 \simeq \mathrm{Syl}_2(\mathrm{Aut}_k(\mathcal{C}_k)^{\#})$.

We now give results about the arithmetic of the monodromy extension of the previous example.



First of all, $M/K_2(2^{1/5})$ is the monodromy extension of $C_0/K_2(2^{1/5})$. Indeed, let θ be a primitive cube root of unity. The curve C_0 has a stable model over M and let $\sigma \in \mathrm{Gal}(K/K_2(2^{1/5}))$ defined by $\sigma(2^{1/3}) = \theta 2^{1/3}$ acts non-trivially on the stable reduction by $t \mapsto \bar{\theta} t$. It implies that

$$\mathrm{Gal}(M/K_2(2^{1/5})) \hookrightarrow \mathrm{Sl}_2(\mathbb{F}_3) \times \mathrm{Sl}_2(\mathbb{F}_3).$$

Moreover, M/L_1 is Galois with group isomorphic to Q_8. Indeed, from the proof of proposition 1.3.1, since $\mathrm{Gal}(M/L_1)$ acts trivially on one of the two elliptic curves of the stable reduction, one has the injection

$$\mathrm{Gal}(M/L_1) \hookrightarrow Q_8 \times \{\mathrm{Id}\}.$$

Moreover, the previous corollary shows that $[M : L_1] = 8$, so $\mathrm{Gal}(M/L_1) \simeq Q_8 \times \{\mathrm{Id}\}$, thus

$$\mathrm{Gal}(L_1/K_2(2^{1/5})) \overset{i}{\hookrightarrow} \mathrm{Sl}_2(\mathbb{F}_3)/Q_8 \times \mathrm{Sl}_2(\mathbb{F}_3) \xrightarrow{p} \mathrm{Sl}_2(\mathbb{F}_3),$$

where p is the projection on the second factor. From the description of the action of the monodromy on the stable reduction, the morphism $p \circ i$ is seen to be onto, thus

$$\mathrm{Gal}(L_1/K_2(2^{1/5})) \simeq \mathrm{Sl}_2(\mathbb{F}_3).$$

One shows in the same way that $\mathrm{Gal}(L_2/K_2(2^{1/5})) \simeq \mathrm{Sl}_2(\mathbb{F}_3)$.

This has consequences on the possible ramification subgroups arising in the ramification filtrations of ${}_1G := \mathrm{Gal}(L_1/K)$ and ${}_2G := \mathrm{Gal}(L_2/K)$. Since ${}_1G$ is the wild ramification group of $\mathrm{Gal}(L_1/K_2(2^{1/5}))$, if there was a ramification subgroup of L_1/K of order 4, there would be a normal subgroup of order 4 in $\mathrm{Sl}_2(\mathbb{F}_3)$, which do not exist. So the only possible subgroups arising in the ramification filtrations of ${}_1G$ and ${}_2G$ are Q_8, $Z(Q_8)$ and $\{1\}$.

Using Magma one computes the lower ramification filtrations

$$\begin{aligned} {}_1G = ({}_1G)_0 = ({}_1G)_1 \supsetneq Z({}_1G) = ({}_1G)_2 = ({}_1G)_3 \supsetneq \{1\}, \\ {}_2G = ({}_2G)_0 = \cdots = ({}_2G)_5 \supsetneq Z({}_2G) = ({}_2G)_6 = \cdots = ({}_2G)_{69} \supsetneq \{1\}. \end{aligned}$$

In order to compute the lower ramification filtration of $\mathrm{Gal}(M/K)$, we now determine its upper ramification filtration since it enjoys peculiar arithmetic properties. Using lemma

3.5 of [Kido3] and the expressions of $\varphi_{L_1/K}$ and $\varphi_{L_2/K}$, one sees that L_1/K and L_2/K are *arithmetically disjoint*. According to [Yam68] theorem 3, one has for any $u \in \mathbb{R}$

$$\mathrm{Gal}(M/K)^u \simeq {}_1G^u \times {}_2G^u.$$

So one gets

$$\mathrm{Gal}(M/K)^u \simeq \begin{cases} {}_1G \times {}_2G, & -1 \leqslant u \leqslant 1, \\ Z({}_1G) \times {}_2G, & 1 < u \leqslant 3/2, \\ \{1\} \times {}_2G, & 3/2 < u \leqslant 5, \\ \{1\} \times Z({}_2G), & 5 < u \leqslant 21, \\ \{1\} \times \{1\}, & 21 < u. \end{cases}$$

One deduces the lower ramification filtration of $\mathrm{Gal}(M/K)$

$$\mathrm{Gal}(M/K)_i \simeq \begin{cases} {}_1G \times {}_2G, & -1 \leqslant i \leqslant 1, \\ Z({}_1G) \times {}_2G, & 2 \leqslant i \leqslant 3, \\ \{1\} \times {}_2G, & 4 \leqslant i \leqslant 31, \\ \{1\} \times Z({}_2G), & 32 \leqslant i \leqslant 543, \\ \{1\} \times \{1\}, & 544 \leqslant i. \end{cases}$$

Let denote the genus 1 irreducible components of $\mathcal{C}_k/k$ by E_1 and E_2. Let H_1 (resp. H_2) be a finite subgroup of $\mathrm{Syl}_2(\mathrm{Aut}_{k,\infty_1}(E_1))$ (resp. $\mathrm{Syl}_2(\mathrm{Aut}_{k,\infty_2}(E_2))$) and $\ell \neq 2$ be a prime number. One has

$$\mathrm{Pic}^\circ(\mathcal{C}_k)[\ell]^{H_1 \times H_2} = \mathrm{Pic}^\circ(E_1)[\ell]^{H_1} \times \mathrm{Pic}^\circ(E_2)[\ell]^{H_2}.$$

According to lemma 0.5.1 one has $\dim_{\mathbb{F}_\ell} \mathrm{Pic}^\circ(E_i)[\ell]^{H_i} = 2g(E_i/H_i)$, thus applying Proposition 0.5.1 with ℓ large enough, one gets

$$\mathrm{sw}(\mathrm{Jac}(C_0)/K) = 45.$$

Degeneration type II

Proposition 1.3.2. *Let* $a^9 = 2$, $K := K_2(a)$, $\rho := a^4$ *and* C/K *be the smooth, projective, geometrically integral curve birationally given by*

$$Y^2 = f(X) = 1 + a^3X^2 + a^6X^3 + X^5.$$

Then, C *has stable reduction of type II and* C/K *has maximal wild monodromy* M/K *with group* $\mathrm{Gal}(M/K) \simeq (Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$.

Proof. Using Magma, one determines the Newton polygon of $T_f(Y)$. Let $(y_i)_{i=1,\dots,8}$ be the roots of $T_f(Y)$. Then

$$\forall 1 \leqslant i \leqslant 8,\ v(y_i) = \frac{7}{24}v(2).$$

By considering the Newton polygon of

$$\Delta(Z) = (T_f(Z + y_1) - T_f(y_1))/Z,$$

one shows that $\Delta(Z)$ has 3 roots (say $y_2 - y_1$, $y_3 - y_1$ and $y_4 - y_1$) of valuation $v(\rho)$ and 4 roots of valuation $v(2)/3$.

Let y be a root of $T_f(Y)$. Define $\rho T = S = X - y$ and choose $s_0(y)^{1/2}$ and $s_2(y)^{1/2}$ such that $2s_0(y)^{1/2}s_2(y)^{1/2} = s_1(y)$. Then the change of variables

$$\rho T = S = X - y \text{ and } Y = 2W + (s_0(y)^{1/2} + s_2(y)^{1/2}S),$$

induces

$$W^2 + (s_0(y)^{1/2} + s_2(y)^{1/2}S)W = \frac{s_3(y)\rho^3}{4}T^3 + \frac{s_4(y)\rho^4}{4}T^4 + \frac{\rho^5}{4}T^5,$$

which is an equation of a quasi-projective flat scheme over $K(y, f(y)^{1/2})$ with special fiber given by $w^2 - w = t^3$. The same argument as in the degeneration type I shows that C has stable reduction of type II over $L = K(y_1, \dots, y_8, f(y_1)^{1/2}, \dots, f(y_8)^{1/2})$.

We first show that L/K is the monodromy extension M/K of C/K. Let $\sigma \in \mathrm{Gal}(L/K)$ inducing the identity on $\mathcal{C}_k/k$. We show that $\forall i \in \{1, \dots, 8\}$, $\sigma(y_i) = y_i$. Else, for example, $\sigma(y_1) = y_2$ or $\sigma(y_1) = y_5$. It follows from the properties of the roots of $\Delta(Z)$ that, if $\sigma(y_1) = y_2$ then σ acts by non-trivial translation on $\mathcal{C}_k/k$ and if $\sigma(y_1) = y_5$ then σ acts on $\mathcal{C}_k/k$ by permuting the genus 1 components. Once again, the same computations as in the degeneration type I show that $\forall i \in \{1, \dots, 8\}$, $\sigma(f(y_i)^{1/2}) = f(y_i)^{1/2}$. Since $M \subseteq L$, one gets $M = L$.

Now, we show that the wild monodromy is maximal. Let's consider the canonical morphism

$$\mathrm{Gal}(M/K) \overset{i}{\hookrightarrow} \mathrm{Syl}_2(\mathrm{Aut}_k(\mathcal{C}_k)^{\#}) \simeq (Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

One sees $Q_8 \times Q_8$ as the subgroup $(Q_8 \times Q_8) \rtimes \{1\}$ of $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ and put

$$H := i(\mathrm{Gal}(M/K)) \cap (Q_8 \times Q_8).$$

One has natural morphisms

$$H \xrightarrow{p} Q_8 \times Q_8/Z(Q_8) \xrightarrow{q} Q_8/Z(Q_8) \times Q_8/Z(Q_8).$$

Using Magma one shows that $T_f(Y)$ is irreducible over K and over $K(y_1)$ one has the following decomposition in irreducible factors

$$T_f(Y) = \prod_{i=1}^{4}(Y - y_i)T_2(Y),$$

and $T_2(Y)$ decomposes over $K(y_1, y_5)$. It implies that $q \circ p \circ i$ is surjective and $p(H)$ is a subgroup of index at most 2 so it contains $\Phi(Q_8 \times Q_8/Z(Q_8))$ and as for type I, one has $p(H) = Q_8 \times Q_8/Z(Q_8)$. It implies that H is a subgroup of $Q_8 \times Q_8$ of index at most 2 and again $H = Q_8 \times Q_8$, that is $Q_8 \times Q_8 \subseteq i(\mathrm{Gal}(M/K))$. Finally on has a natural morphism

$$(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{r} (Q_8/Z(Q_8) \times Q_8/Z(Q_8)) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

The composition $r \circ i$ is surjective since there exist $\sigma, \tau \in \mathrm{Gal}(M/K)$ such that for all $i \in \{1, \dots, 4\}$ and $j \in \{5, \dots, 8\}$

$$\sigma(y_1) = y_i \text{ and } \sigma(y_5) = y_j,$$
$$\tau(y_1) = y_5.$$

Since the index of $i(\mathrm{Gal}(M/K))$ in $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ is at most 2, this group contains

$$\Phi((Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}) \supseteq \operatorname{Ker} r,$$

so $i(\mathrm{Gal}(M/K)) = (Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$. □

Again we derive the following result for the Inverse Galois Problem.

Corollary 1.3.2. *With the notations of Proposition 1.3.2, let* $(y_i)_{i=1,\dots,8}$ *be the roots of* $T_f(Y)$ *and* $M = K(y_1, \dots, y_8, f(y_1)^{1/2}, \dots, f(y_8)^{1/2})$. *Then* M/K *is Galois with Galois group isomorphic to* $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Syl}_2(\mathrm{Aut}_k(\mathcal{C}_k)^{\#})$.

2 LIFTING p-CYCLIC COVERS WITH MAXIMAL MONODROMY.

"Ce n'est pas parce que les choses sont difficiles que nous n'osons pas, mais parce que nous n'osons pas qu'elles sont difficiles."
Sénèque

Table of Contents

2.1 INTRODUCTION.

Let (R, v) be a complete discrete valuation ring of mixed characteristic $(0, p)$ with fraction field K containing a primitive p-th root of unity ζ_p and algebraically closed residue field k. The stable reduction theorem states that given a smooth, projective, geometrically connected curve C/K of genus $g(C) \geqslant 2$, there exists a unique minimal Galois extension M/K called *the monodromy extension of* C/K such that $C_M := C \times M$ has stable reduction over M. The group $G = \mathrm{Gal}(M/K)$ is the *monodromy group of* C/K.

Let us consider the case where $\phi : C \to \mathbb{P}^1_K$ is a p-cyclic cover with K-rational equidistant geometry. Let $\mathcal{C}$ be the stable model of C_M/M and $\mathrm{Aut}_k(\mathcal{C}_k)^\#$ be the subgroup of $\mathrm{Aut}_k(\mathcal{C}_k)$ of elements acting trivially on the reduction in $\mathcal{C}_k$ of the ramification locus of $\phi \times \mathrm{Id}_M : C_M \to \mathbb{P}^1_M$ (see [Liu02] 10.1.3 for the definition of the reduction map of C_M). One derives from the stable reduction theorem the following injection

$$\mathrm{Gal}(M/K) \hookrightarrow \mathrm{Aut}_k(\mathcal{C}_k)^\#. \tag{2.1}$$

When the p-Sylow subgroups of these groups are isomorphic, one says that the *wild monodromy is maximal*. We are interested in realization of smooth covers as above such that the p-adic valuation of $|\mathrm{Aut}_k(\mathcal{C}_k)^\#|$ is large compared to the genus of $\mathcal{C}_k$ and having maximal wild monodromy. Moreover, we will study the ramification filtration and the Swan conductor of their monodromy extension.

Recall that a big action is a pair (X, G) where X/k is a smooth, projective, geometrically connected curve of genus $g(X) \geqslant 2$ and G is a finite p-group of k-automorphisms of X/k such that $|G| > \frac{2p}{p-1} g(X)$. According to [LM05], if (X, G) is a big action, then one has that $|G| \leqslant \frac{4p}{(p-1)^2} g(X)^2$ with equality if and only if X/k is birationally given by $w^p - w = tR(t)$ where $R(t) \in k[t]$ is an additive polynomial and G is the p-Sylow subgroup $G_{\infty,1}(X)$ of the subgroup of $\mathrm{Aut}_k(X)$ leaving $t = \infty$ fixed. In this case, G is an extra-special p-group.

This motivates the following question, with the above notations, given a big action (X, G) such that $|G| = \frac{4p}{(p-1)^2} g(X)^2$ and $G = G_{\infty,1}(X)$, is it possible to find a finite extension K of $\mathrm{Frac}(W(k))$ and a a p-cyclic cover C/K of $\mathbb{P}^1_K$ such that $\mathcal{C}_k \simeq X$, that $G \simeq \mathrm{Aut}(\mathcal{C}_k)^{\#}_1$ is a p-Sylow subgroup of $\mathrm{Aut}(\mathcal{C}_k)^{\#}$ and the curve C/K has maximal wild monodromy ?

Let k be an algebraically closed field of characteristic $p > 0$ and $K_p := \mathrm{Frac}(W(k))$. Let $n \in \mathbb{N}^\times$, $q = p^n$, ζ_p be a primitive p-th root of unity, $\lambda = \zeta_p - 1$ and $K = K_p(\lambda^{1/(1+q)})$. For any additive polynomial $R(t) \in k[t]$ of degree q, let X/k be curve defined by $w^p - w = tR(t)$. In Section 2.2, we will prove the following

Theorem 2.1.1. *There exists a p-cyclic cover C/K of $\mathbb{P}^1_K$ such that $\mathcal{C}_k \simeq X$, one has $G_{\infty,1}(X) \simeq \mathrm{Aut}(\mathcal{C}_k)^{\#}_1$ and the curve C/K has maximal wild monodromy M/K. The extension M/K is the decomposition field of an explicitly given polynomial and the group $\mathrm{Gal}(M/K) \simeq \mathrm{Aut}_k(\mathcal{C}_k)^{\#}_1$ is an extra-special p-group of order pq^2.*

The group $G_{\infty,1}(\mathcal{C}_k) = \mathrm{Aut}_k(\mathcal{C}_k)^{\#}_1$ is endowed with the lower ramification filtration $(G_{\infty,i}(\mathcal{C}_k))_{i\geqslant 0}$. Let $Z := Z(G_{\infty,1}(\mathcal{C}_k))$ be the center of $G_{\infty,1}(\mathcal{C}_k)$, it is a cyclic group of order p generated by the Artin-Schreier morphism, see [LM05]. Applying the Riemann-Hurwitz formula and the Different formula (see [Ser79] IV §2 Proposition 4) to the Galois covers $\mathcal{C}_k \to \mathcal{C}_k/Z \simeq \mathbb{P}^1_k$ and $\mathcal{C}_k/Z \simeq \mathbb{P}^1_k \to \mathcal{C}_k/G_{\infty,1}(\mathcal{C}_k) \simeq \mathbb{P}^1_k$ one shows that

$$G_{\infty,1}(\mathcal{C}_k) \supsetneq Z = G_{\infty,2}(\mathcal{C}_k) = \cdots = G_{\infty,1+q}(\mathcal{C}_k) \supsetneq \{1\}.$$

Moreover, $G := \mathrm{Gal}(M/K)$ being the Galois group of a finite extension of K, it is endowed with the ramification filtration $(G_i)_{i\geqslant 0}$. Since $G \simeq G_{\infty,1}(\mathcal{C}_k)$ it is natural to ask for the behavior of $(G_i)_{i\geqslant 0}$ under (2.1), that is to compare $(G_i)_{i\geqslant 0}$ and $(G_{\infty,i}(\mathcal{C}_k))_{i\geqslant 0}$. In the general case, the arithmetic is quite tedious due to the expression of the lifting of X/k. Actually we could not obtain a numerical example for the easiest case when $p = 3$. Nonetheless, when $p = 2$, one computes the conductor exponent $f(\mathrm{Jac}(C)/K)$ of $\mathrm{Jac}(C)/K$ and its Swan conductor $\mathrm{sw}(\mathrm{Jac}(C)/K)$

Theorem 2.1.2. *Under the hypotheses of Theorem 2.1.1, if $p = 2$ the lower ramification filtration of G is :*

$$G = G_0 = G_1 \supsetneq Z(G) = G_2 = \cdots = G_{1+q} \supsetneq \{1\}.$$

Then, $f(\mathrm{Jac}(C)/K) = 2q + 1$ and $\mathrm{sw}(\mathrm{Jac}(C)/K_2) = 1$.

Remarks :

1. In Theorem 2.1.1, one actually obtains a family of liftings C/K of X/k with the announced properties. It is worth noting that there are finitely many additive polynomials $R_0(t) \in k[t]$ such that $w^p - w = tR(t)$ is k-isomorphic to $w^p - w = tR_0(t)$ (see [LM05] 8.2), so we have to solve the problem in a somehow generic way. In [CM13], we obtain the analogs of Theorem 2.1.1 and Theorem 2.1.2 for $p \geqslant 2$ in the easier case $R(t) = t^q$.

2. For $p = 3$, the easiest non-trivial case is such that $[M : K] = 243$, that is why we could not even do computations using Magma to guess the behavior of the ramification filtration of the monodromy extension for $p > 2$. Nonetheless, one shows that if $p \geqslant 3$, the lower ramification filtration of G is

   $$G = G_0 = G_1 \supsetneq G_2 = \cdots = G_u = Z(G) \supsetneq \{1\},$$

   where $u \in 1 + q\mathbb{N}$.

3. The value $\mathrm{sw}(\mathrm{Jac}(C)/K_2) = 1$ is the smallest one among abelian varieties over K_2 with non tame monodromy extension. That is, in some sense, a counterpart of [BK05] and [LRS93] where an upper bound for the conductor exponent is given and it is shown that this bound is actually achieved.

2.2 LIFTINGS AND STUDY OF THEIR ARITHMETIC.

We start by fixing notations that will be used throughout this Section.

Notations : Let $n \in \mathbb{N}^\times$, $q := p^n$, $a_n := (-1)^q(-p)^{p+p^2+\cdots+q}$ and

$$\forall\, 0 \leqslant i \leqslant n-1,\ d_i := p^{n-i+1} + \cdots + q.$$

Let k be an algebraically closed field of characteristic $p > 0$, let $K_p := \mathrm{Frac}(W(k))$ and put $K := K_p(\lambda^{1/(1+q)})$. Let $\underline{\rho} := (\rho_0, \ldots, \rho_{n-1})$ where $\forall\ 0 \leqslant k \leqslant n-1$, $\rho_k \in K$, $\rho_k = u_k\lambda^{p(q-p^k)/(1+q)}$ and $v(u_k) = 0$ or $u_k = 0$. We denote by $\mathfrak{m}$ the maximal ideal of $(K^{\mathrm{alg}})^\circ$. Let $R = K^\circ$, for $c \in R$ let

$$f_{c,\rho}(X) := 1 + \sum_{k=0}^{n-1} \rho_k X^{1+p^k} + cX^q + X^{1+q},$$

$$\text{and } s_{1,\rho}(X) := 2\rho_0 X + \sum_{k=1}^{n-1} \rho_k X^{p^k} + X^q.$$

One defines the *modified monodromy polynomial* $L_{c,\rho}(X)$ by

$$s_{1,\rho}(X)^q - a_n f_{c,\rho}(X)^{q-1}(c+X) - (-1)^q \sum_{k=1}^{n-1} (\rho_k X)^{q/p^k}(-p)^{d_k} f_{c,\rho}(X)^{q(p^k-1)/p^k}.$$

Let $C_{c,\rho}/K$ and A_u/k be the smooth projective integral curves birationally given respectively by $Y^p = f_{c,\rho}(X)$ and $w^p - w = \sum_{k=0}^{n-1} \bar{u}_k t^{1+p^k} + t^{1+q}$.

Remark : The ρ_k's are chosen such that a suitable change of variables on X and Y induces the good reduction A_u/k. This is detailed in **Step VI** of proof of Theorem 2.2.1.

Theorem 2.2.1. *The curve $C_{c,\rho}/K$ has potential good reduction isomorphic to A_u/k.*

1. *If $v(c) \geqslant v(\lambda^{p/(1+q)})$, then the monodromy extension of $C_{c,\rho}/K$ is trivial.*
2. *If $v(c) < v(\lambda^{p/(1+q)})$, let y be a root of $L_{c,\rho}(X)$ in K^{alg}. Then $C_{c,\rho}$ has good reduction over $K(y, f_{c,\rho}(y)^{1/p})$. If $L_{c,\rho}(X)$ is irreducible over K, then $C_{c,\rho}/K$ has maximal wild monodromy. The monodromy extension of $C_{c,\rho}/K$ is $M = K(y, f_{c,\rho}(y)^{1/p})$ and $G = \mathrm{Gal}(M/K)$ is an extra-special p-group of order pq^2.*
3. *Assume that $c = 1$. The polynomial $L_{1,\rho}(X)$ is irreducible over K. The lower ramification filtration of G is*

$$G = G_0 = G_1 \supsetneq G_2 = \cdots = G_u = Z(G) \supsetneq \{1\},$$

with $u \in 1 + q\mathbb{N}$. Moreover, if $p = 2$, then $u = 1 + q$, one has $f(\mathrm{Jac}(C_{1,\rho})/K) = 2q + 1$ and $\mathrm{sw}(\mathrm{Jac}(C_{1,\rho})/K_2) = 1$.

Proof. 1. Assume that $v(c) \geqslant v(\lambda^{p/(1+q)})$. Set $\lambda^{p/(1+q)}T = X$ and $\lambda W + 1 = Y$. Then, the equation defining $C_{c,\rho}/K$ becomes

$$(\lambda W+1)^p = 1 + \sum_{k=0}^{n-1} \rho_k \lambda^{p(1+p^k)/(1+q)} T^{1+p^k} + c\lambda^{pq/(1+q)} T^q + \lambda^p T^{1+q}.$$

After simplification by λ^p and reduction modulo π_K this equation gives

$$w^p - w = \sum_{k=0}^{n-1} \bar{u}_k t^{1+p^k} + at^q + t^{1+q},\ a \in k. \tag{2.2}$$

By Hurwitz formula the genus of the curve defined by (2.2) is seen to be that of $C_{c,\rho}/K$. Applying [Liu02] 10.3.44, there is a component in the stable reduction birationally given by (2.2). The stable reduction being a tree, the curve $C_{c,\rho}/K$ has good reduction over K.

2. The proof is divided into eight steps. **Step I** and **Step II** are similar to the first two steps of the proof of Theorem 1.2.1. In **Step III**, **Step IV** and **Step V** one writes a stable model of $C_{c,\rho}/K$ over a finite extension of K and under the extra assumption that $L_{c,\rho}(X)$ is irreducible over K, we will prove in **Step VIII** that this is the wild monodromy extension. The first seven steps are much more difficult to handle than their analogos in proof of Theorem 1.2.1 due to the more complicated expression of $C_{c,\rho}/K$ while **Step VIII** is similar to **Step VI** of the proof of Theorem 1.2.1. Let y be a root of $L_{c,\rho}(X)$.

Step I : *One has* $v(y) = v(a_n c)/q^2$.

By expanding $L_{c,\rho}(X)$, one shows that its Newton polygon has a single slope $v(a_n c)/q^2$. The polynomial $L_{c,\rho}(X)$ has degree q^2 and its leading (resp. constant) coefficient has valuation 0 (resp. $v(a_n c)$). One examines monomials from $a_n f_{c,\rho}^{q-1}(X)(c+X)$. Since $v(c) < v(\lambda^{p/(1+q)})$, one checks that

$$\forall 1 \leqslant i \leqslant q^2-1,\ \frac{v(a_n)}{q^2-i} \geqslant \frac{v(a_n c)}{q^2}.$$

Then one examines monomials from $(\rho_i X)^{q/p^i} p^{d_i} f_{c,\rho}(X)^{q(p^i-1)/p^i}$. They have degree at least q/p^i, thus one checks that

$$\forall\ 1 \leqslant i \leqslant n-1,\ \frac{q/p^i v(\rho_i) + d_i v(p)}{q^2 - q/p^i} \geqslant \frac{v(a_n c)}{q^2}.$$

The monomial X^{q^2} in $s_{1,\rho}(X)^q$ corresponds to the point $(0,0)$ in the Newton polygon of $L_{c,\rho}(X)$, the other monomials of $s_{1,\rho}(X)^q$ produce a slope greater than $v(\rho_i)/(q-p^i)$ and one checks that

$$\forall\ 0 \leqslant i \leqslant n-1,\ \frac{v(\rho_i)}{q-p^i} \geqslant \frac{v(a_n c)}{q^2}.$$

Note that **Step I** implies that $v(f_{c,\rho}(y)) = 0$, we will use this remark throughout this proof.

Step II : *Define* S *and* T *by* $\lambda^{p/(1+q)}T = (X-y) = S$. *Then* $f_{c,\rho}(S+y)$ *is congruent modulo* $\lambda^p\mathfrak{m}[T]$ *to*

$$f_{c,\rho}(y) + s_{1,\rho}(y)S + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + \sum_{k=1}^{n-1} \rho_k y S^{p^k} + (c+y)S^q + S^{1+q}.$$

Using the following formula for $A \in K^{alg}$ with $\nu(A) > 0$ and $B \in (K^{alg})^\circ[T]$

$$k \geqslant 1,\ (A+B)^{p^k} \equiv (A^{p^{k-1}} + B^{p^{k-1}})^p \bmod p^2\mathfrak{m}[T],$$

one computes mod $\lambda^p\mathfrak{m}[T]$

$$f_{c,\rho}(y+S) = 1 + \sum_{k=0}^{n-1} \rho_k (y+S)^{1+p^k} + (y+S)^{1+q} + c(y+S)^q$$

$$\equiv 1 + \rho_0(y+S)^2 + \sum_{k=1}^{n-1} \rho_k (y+S)(y^{p^{k-1}} + S^{p^{k-1}})^p + (y+S+c)(y^{q/p} + S^{q/p})^p.$$

Using **Step I**, one checks that for all $1 \leqslant k \leqslant n-1$

$$\rho_k(y^{p^{k-1}} + S^{p^{k-1}})^p \equiv \rho_k(y^{p^k} + S^{p^k}) \bmod \lambda^p\mathfrak{m}[T],$$

and $(y^{q/p} + S^{q/p})^p \equiv y^q + S^q \bmod \lambda^p\mathfrak{m}[T]$. It follows that

$$f_{c,\rho}(y+S) \equiv 1 + \rho_0(y+S)^2 + \sum_{k=1}^{n-1} \rho_k (y+S)(y^{p^k} + S^{p^k}) + (y+c+S)(y^q + S^q).$$

One easily concludes from this last expression.

Step III : *Let* $R_1 := K[y]^\circ$. *For all* $0 \leqslant i \leqslant n$, *one defines* $A_i(S) \in R_1[S]$ *and* $B_i \in R_1$ *by induction :*

$$B_n := -s_{1,\rho}(y),\ \forall\, 1 \leqslant i \leqslant n-1,\ B_i := \frac{f_{c,\rho}(y)B_{i+1}^p}{(-pf_{c,\rho}(y))^p} - y\rho_{n-i},$$

$$\text{and } B_0 := \frac{f_{c,\rho}(y)B_1^p}{(-pf_{c,\rho}(y))^p},$$

$$A_0(S) := 0 \text{ and } \forall\, 0 \leqslant i \leqslant n-1\ \ SA_{i+1}(S) := SA_i(S) - \frac{B_{i+1}S^{q/p^{i+1}}}{pf_{q,c}(y)^{(p-1)/p}}.$$

Then for all $0 \leqslant i \leqslant n-1$, $\nu(B_{i+1}) = (1+\cdots+p^i)\nu(p)/p^i + \nu(c)/p^{i+1}$ *and modulo* $\lambda^{\frac{pq^2}{q+1}}\mathfrak{m}$ *one has*

$$B_n^q \equiv \frac{a_n}{(-1)^q} f_{c,\rho}(y)^{q-1}B_0 + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k}(-p)^{d_k} f_{c,\rho}(y)^{q(p^k-1)/p^k}. \tag{2.3}$$

We prove the claim about $\nu(B_{i+1})$ by induction on i. Using **Step I**, one checks that

$$\forall\, 0 \leqslant k \leqslant n-1,\ \nu(\rho_k y^{p^k}) > \nu(y^q),$$

so $v(B_n) = v(y^q)$. Assume that we have shown the claim for i, then one checks that $v((B_{i+1}/p)^p) < v(y\rho_{n-i})$ and one deduces $v(B_i)$ from the definition of B_i. According to the expression of $v(B_i)$, one has $\forall\ 0 \leqslant i \leqslant n, A_i(S) \in R_1[S]$.

Then we prove the second part of **Step III**. From the definition of the B_i's one obtains that for all $1 \leqslant i \leqslant n-1$

$$B_{n-i+1}^{q/p^{i-1}} = (-p)^{q/p^{i-1}} f_{c,\rho}(y)^{q(p-1)/p^i} (y\rho_i + B_{n-i}(y))^{q/p^i}. \tag{2.4}$$

Using **Step I** and $v(B_{n-1})$ one checks that $\forall\ 1 \leqslant k \leqslant q/p-1$

$$p^q \binom{q/p}{k} (y\rho_1)^k B_{n-1}^{q/p-k} \equiv 0 \bmod \lambda^{pq^2/(1+q)}\mathfrak{m},$$

so $p^q(y\rho_1 + B_{n-1})^{q/p} \equiv p^q((y\rho_1)^{q/p} + B_{n-1}^{q/p}) \bmod \lambda^{pq^2/(1+q)}\mathfrak{m}$. Thus, applying equation (2.4) with $i = 1$, one gets

$$\begin{aligned} B_n^q &= (-p)^q f_{c,\rho}(y)^{q(p-1)/p} (y\rho_1 + B_{n-1})^{q/p} \\ &\equiv (-p)^q f_{c,\rho}(y)^{q(p-1)/p} ((y\rho_1)^{q/p} + B_{n-1}^{q/p}) \bmod \lambda^{pq^2/(1+q)}\mathfrak{m}. \end{aligned}$$

One checks using **Step I** and $v(B_{n-i})$ that $\forall\ 1 \leqslant i \leqslant n-1$ and $1 \leqslant k \leqslant q/p^i - 1$

$$p^{q+\cdots+q/p^{i-1}} \binom{q/p^i}{k} B_{n-i}^{q/p^i-k} (y\rho_i)^k \equiv 0 \bmod \lambda^{pq^2/(1+q)}\mathfrak{m},$$

then by induction on i, using equation (2.4), one shows that modulo $\lambda^{pq^2/(1+q)}\mathfrak{m}$

$$B_n^q \equiv (-p)^{p+\cdots+q} f_{c,\rho}(y)^{q-1} B_0 + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} f_{c,\rho}(y)^{q(p^k-1)/p^k}.$$

Step IV : *One has modulo* $\lambda^p\mathfrak{m}[T]$

$$f_{c,\rho}(S+y) \equiv f_{c,\rho}(y) + s_{1,\rho}(y)S + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + \sum_{k=1}^{n-1} y\rho_k S^{p^k} + B_0 S^q + S^{1+q}.$$

Since $L_{c,\rho}(y) = 0$, one has

$$s_{1,\rho}(y)^q = a_n f_{c,\rho}(y)^{q-1}(c+y) + (-1)^q \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} f_{c,\rho}(y)^{q(p^k-1)/p^k}. \tag{2.5}$$

Using $B_n := -s_{1,\rho}(y)$, equations (2.3) and (2.5) one gets

$$a_n f_{c,\rho}(y)^{q-1}(c + y - B_0) \equiv 0 \bmod \lambda^{pq^2/(q+1)}\mathfrak{m}.$$

which is equivalent to $S^q(y + c - B_0) \equiv 0 \bmod \lambda^p\mathfrak{m}[T]$. Then, **Step IV** follows from **Step II**.

Step V : *One has*

$$f_{c,\rho}(S+y) \equiv (f_{c,\rho}(y)^{1/p} + SA_n(S))^p + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q} \bmod \lambda^p\mathfrak{m}[T].$$

Let $R := \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q} + s_{1,\rho}(y)S$. Since $B_n = -s_{1,\rho}(y)$ one has

$$\begin{aligned}
&(f_{c,\rho}(y)^{1/p} + SA_n(S))^p + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q} \\
&= (f_{c,\rho}(y)^{1/p} + SA_n(S))^p + B_n S + R \\
&= \Big(f_{c,\rho}(y)^{1/p} + SA_{n-1}(S) - \frac{B_n S}{p f_{q,c}(y)^{(p-1)/p}}\Big)^p + B_n S + R \\
&= (f_{c,\rho}(y)^{1/p} + SA_{n-1}(S))^p + \Big(\frac{-B_n S}{p f_{q,c}(y)^{(p-1)/p}}\Big)^p + B_n S + R + \Sigma, \qquad (2.6)
\end{aligned}$$

where

$$\Sigma = \sum_{k=1}^{p-1} \binom{p}{k} (f_{c,\rho}(y)^{1/p} + SA_{n-1}(S))^{p-k} \Big(\frac{-B_n S}{p f_{q,c}(y)^{(p-1)/p}}\Big)^k. \qquad (2.7)$$

Using the expression of $\nu(B_n)$ computed in **Step III**, one checks that the terms with $k \geqslant 2$ in (2.7) are zero modulo $\lambda^p \mathfrak{m}[T]$. It implies the following relations

$$\begin{aligned}
\Sigma + B_n S &\equiv B_n S \Big[1 - \frac{(f_{c,\rho}(y)^{1/p} + SA_{n-1}(S))^{p-1}}{f_{c,\rho}(y)^{(p-1)/p}}\Big] \\
&\equiv \frac{B_n S}{f_{c,\rho}(y)^{(p-1)/p}} \Big[f_{c,\rho}(y)^{(p-1)/p} - (f_{c,\rho}(y)^{1/p} + SA_{n-1}(S))^{p-1}\Big] \\
&\equiv \frac{B_n S}{f_{c,\rho}(y)^{(p-1)/p}} \Big[-\sum_{k=1}^{p-1} \binom{p-1}{k} f_{c,\rho}(y)^{(p-1-k)/p} (SA_{n-1}(S))^k\Big] \\
&\equiv 0 \bmod \lambda^p \mathfrak{m}[T], \text{ since for } k \geqslant 1,\ B_n S^{k+1} \equiv 0 \bmod \lambda^p \mathfrak{m}[T].
\end{aligned}$$

According to the definition of B_{n-1} (see **Step III**) one obtains

$$(2.6) \equiv (f_{c,\rho}(y)^{1/p} + SA_{n-1}(S))^p + R + B_{n-1} S^p + y\rho_1 S^p \bmod \lambda^p \mathfrak{m}[T]. \qquad (2.8)$$

Using the same process, one shows by induction on i that (2.6) is congruent to

$$(f_{c,\rho}(y)^{1/p} + SA_{i+1}(S))^p + B_{i+1} S^{p^{n-i-1}} + \sum_{k=1}^{n-i-1} y\rho_k S^{p^k} + R \bmod \lambda^p \mathfrak{m}[T]. \qquad (2.9)$$

Thus, one applies equation (2.9) with $i = 0$

$$(2.6) \equiv (f_{c,\rho}(y)^{1/p} + SA_1(S))^p + B_1 S^{q/p} + \sum_{k=1}^{n-1} y\rho_k S^{p^k} + R \bmod \lambda^p \mathfrak{m}[T].$$

One defines Σ' by $(f_{c,\rho}(y)^{1/p} + SA_1(S))^p = f_{c,\rho}(y) + (SA_1(S))^p + \Sigma'$. From

$$p f_{c,\rho}(y)^{(p-1)/p} SA_1(S) = -B_1 S^{q/p}, \text{ see the definition of } SA_1(S),$$

one gets

$$\Sigma' + B_1 S^{q/p} = \sum_{k=2}^{p-1} \binom{p}{k} f_{c,\rho}(y)^{(p-k)/p} (SA_1(S))^k,$$

so using the expression of $v(B_1)$ computed in **Step III**, one checks that

$$\Sigma' + B_1 S^{q/p} \equiv 0 \bmod \lambda^p \mathfrak{m}[T].$$

From the definition of $SA_1(S)$ and B_0 one has $(SA_1(S))^p = B_0 S^q$, thus

$$(2.6) \equiv f_{c,\rho}(y) + B_0 S^q + \sum_{k=1}^{n-1} y\rho_k S^{p^k} + R \bmod \lambda^p \mathfrak{m}[T].$$

Then, **Step V** follows from **Step IV** and this last relation.

Step VI : *The curve* $C_{c,\rho}/K$ *has good reduction over* $K(y, f_{c,\rho}(y)^{1/p})$.

According to **Step V**, the change of variables in $K(y, f_{c,\rho}(y)^{1/p})$

$$X = \lambda^{p/(1+q)} T + y = S + y \quad \text{and} \quad Y = \lambda W + f_{c,\rho}(y)^{1/p} + SA_n(S),$$

induces in reduction $w^p - w = \sum_{k=0}^{n-1} \bar{u}_k t^{1+p^k} + t^{1+q}$ with genus $g(C_{c,\rho})$. So [Liu02] 10.3.44 implies that this change of variables gives the stable model. Note that the ρ_k's were chosen to obtain this equation for the special fiber of the stable model.

Step VII : *For any distinct roots* y_i, y_j *of* $L_{c,\rho}(X)$, $v(y_i - y_j) = v(\lambda^{p/(1+q)})$.

The changes of variables $\lambda^{p/(1+q)} T = X - y_i$ and $\lambda^{p/(1+q)} T = X - y_j$ induce equivalent Gauss valuations of $K(C_{c,\rho})$, else applying [Liu02] 10.3.44 would contradict the uniqueness of the stable model. Thus $v(y_i - y_j) \geqslant v(\lambda^{p/(1+q)})$.

One checks that $v(f'_{c,\rho}(y)) > 0$, $v(s'_{1,\rho}(y)) > 0$, $v(s_{1,\rho}(y)) = v(y^q)$

$$v(q s_{1,\rho}(y)^{q-1} s'_{1,\rho}(y)) > v(a_n) \text{ and } \forall\, 0 \leqslant k \leqslant n-1, \quad v(\rho_k^{q/p^k} p^{d_k} q/p^k) > v(a_n).$$

Then one computes $L'_{c,\rho}(X)$ and from these relations one deduces

$$v(L'_{c,\rho}(y)) = v(a_n) = (q^2 - 1) v(\lambda^{p/(1+q)}).$$

Taking into account that $L'_{c,\rho}(y_i) = \prod_{j \neq i} (y_i - y_j)$ and $\deg L_{c,\rho}(X) = q^2$, one obtains $v(y_i - y_j) = v(\lambda^{p/(1+q)})$.

Step VIII : *If* $L_{c,\rho}(X)$ *is irreducible over* K, *then* $K(y, f_{c,\rho}(y)^{1/p})$ *is the monodromy extension* M *of* $C_{c,\rho}/K$ *and* $G := \mathrm{Gal}(M/K)$ *is an extra-special* p*-group of order* pq^2.

Let $(y_i)_{i=1,\dots,q^2}$ be the roots of $L_{c,\rho}(X)$, $L := K(y_1, \dots, y_{q^2})$ and M/K be the monodromy extension of $C_{c,\rho}/K$. Any $\tau \in \mathrm{Gal}(L/K) - \{1\}$ is such that $\tau(y_i) = y_j$ for some $i \neq j$. Thus, the change of variables

$$X = \lambda^{p/(1+q)} T + y_i \quad \text{and} \quad Y = \lambda W + f_{c,\rho}(y)^{1/p} + SA_n(S),$$

induces the stable model and τ acts on it by

$$\tau(T) = \frac{X - y_j}{\lambda^{p/(1+q)}}, \quad \text{hence} \quad T - \tau(T) = \frac{y_j - y_i}{\lambda^{p/(1+q)}}. \tag{2.10}$$

According to **Step VII** and equation (2.10), τ acts non-trivially on the stable reduction. It follows that $L \subseteq M$. Indeed if $\mathrm{Gal}(K^{alg}/M) \nsubseteq \mathrm{Gal}(K^{alg}/L)$ it would exist $\sigma \in \mathrm{Gal}(K^{alg}/M)$ inducing $\bar{\sigma} \neq \mathrm{Id} \in \mathrm{Gal}(L/K)$, which would contradict the characterization of $\mathrm{Gal}(K^{alg}/M)$ (see remark after Theorem 0.1.1) .

According to [LM05], the p-Sylow subgroup $\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}$ of $\mathrm{Aut}_k(\mathcal{C}_k)^{\#}$ is an extra-special p-group of order pq^2. Moreover, one has

$$0 \to Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}) \to \mathrm{Aut}_k(\mathcal{C}_k)_1^{\#} \to (\mathbb{Z}/p\mathbb{Z})^{2n} \to 0,$$

where $(\mathbb{Z}/p\mathbb{Z})^{2n}$ is identified with the group of translations $t \mapsto t + a$ extending to elements of $\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}$. Therefore we have morphisms

$$\mathrm{Gal}(M/K) \overset{i}{\hookrightarrow} \mathrm{Aut}_k(\mathcal{C}_k)_1^{\#} \overset{\varphi}{\to} \mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}/Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}).$$

The composition is seen to be surjective since the image contains the q^2 translations $t \mapsto t + \overline{(y_i - y_1)/\lambda^{p/(1+q)}}$. Consequently, $i(\mathrm{Gal}(M/K))$ is a subgroup of $\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}$ of index at most p. So it contains $\Phi(\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}) = Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#}) = \mathrm{Ker}\,\varphi$. It implies that i is an isomorphism and $[M : K] = pq^2$. By **Step VI**, one has $M \subseteq K(y, f_{q,c}(y)^{1/p})$, hence $M = K(y, f_{q,c}(y)^{1/p})$.

We show that $K(y_1)/K$ is Galois and that $\mathrm{Gal}(M/K(y_1)) = Z(G)$. Indeed, $M/K(y_1)$ is p-cyclic and generated by σ defined by

$$\sigma(y_1) = y_1 \text{ and } \sigma(f_{c,\rho}(y_1)^{1/p}) = \zeta_p f_{c,\rho}(y_1)^{1/p}.$$

According to **Step VI**, σ acts on the stable model by

$$\sigma(S) = S, \quad \sigma(Y) = Y = \lambda\sigma(W) + \zeta_p f_{c,\rho}(y_1)^{1/p} + SA_n(S).$$

Hence

$$\sigma(W) = W - f_{c,\rho}(y_1)^{1/p}.$$

It follows that, in reduction, σ induces a morphism that generates $Z(\mathrm{Aut}_k(\mathcal{C}_k)_1^{\#})$. It implies that $K(y_1)/K$ is Galois, $\mathrm{Gal}(M/K(y_1)) = Z(G)$ and $\mathrm{Gal}(K(y_1)/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{2n}$.

3. Let $L_\rho(X) := L_{1,\rho}(X)$, $f_\rho(X) := f_{1,\rho}(X)$, y be a root of $L_\rho(X)$, $s_\rho(y) := s_{1,\rho}(y)$ and $b_n := (-1)(-p)^{1+p+\cdots+p^{n-1}}$. Note that $b_n^p = a_n$. One puts $L := K(y)$ and we do not assume $p = 2$ until **Step E**.

Step A : *The polynomial* $L_\rho(X)$ *is irreducible over* K.

Let $\tilde{s} := s_\rho(y) - y^q$, $\sigma := \sum_{k=1}^{q} \binom{q}{k} \tilde{s}^k y^{q(q-k)}$ and $R_1 := \sum_{k=1}^{p-1} \binom{p}{k} y^{kq^2/p} (-b_n)^{p-k}$. Since $L_\rho(y) = 0$ one has

$$y^{q^2} + \sigma = s_\rho(y)^q = a_n f_\rho(y)^{q-1}(1+y) + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k}.$$

It implies that $(y^{q^2/p} - b_n)^p$ equals

$$a_n\left[f_\rho(y)^{q-1}(1+y) + (-1)^p\right] + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k} + R_1 - \sigma.$$

We are going to remove monomials with valuation greater than $v(a_n y)$ in the above expression by taking p-th roots. Note that if $\forall i \geqslant 1$, $\rho_i = 0$, then one could skip most of **Step A** (see equation (2.13)). Assume that $\rho_i \neq 0$ for some $i \geqslant 1$, let

$$j := \max\{1 \leqslant i \leqslant n-1,\ \rho_i \neq 0\} \text{ and } l := \min\{1 \leqslant i \leqslant n-1, \rho_i \neq 0\}.$$

The following relations are straightforward computations using **Step I** :

$$v(f_\rho(y)(1+y) + (-1)^p) = v(y),\ \ v(\tilde{s}) = v(\rho_j y^{p^j}),\ \ v(\sigma) = qv(\tilde{s}), \tag{2.11}$$
$$v\Big(\sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k}\Big) = v((\rho_l y)^{p^{n-l}} p^{d_l}).$$

Then one checks that

$$v(R_1) > v(a_n y) > v((\rho_l y)^{p^{n-l}} p^{d_l}) > v(\sigma). \tag{2.12}$$

It implies that $v((y^{q^2/p} - b_n)^p) = qv(\tilde{s})$, so one considers $(y^{q^2/p} - b_n + \tilde{s}^{q/p})^p$. By expanding this last expression, using (2.11), (2.12) and taking into account

$$v(\sum_{k=1}^{q-1} \binom{q}{k} \tilde{s}^k y^{q(q-k)}) > v(a_n y),\ \ v(\sum_{k=1}^{p-1} \binom{p}{k} (y^{q^2/p} - b_n)^k \tilde{s}^{(p-k)q/p}) > v(a_n y),$$

one obtains that $pv(y^{q^2/p} - b_n + \tilde{s}^{q/p}) = v((\rho_l y)^{p^{n-l}} p^{d_l})$, leading us to consider

$$(y^{q^2/p} - b_n + \tilde{s}^{q/p} + (\rho_l y)^{q/p^{l+1}} (-p)^{d_l/p} f_\rho(y)^{q(p^l-1)/p^{l+1}})^p.$$

By expanding this expression and using (2.11) and (2.12) one checks that it has valuation $v((\rho_{l_1} y)^{p^{n-l_1}} p^{d_{l_1}})$ where $l_1 := \min\{l+1 \leqslant i \leqslant n-1, \rho_i \neq 0\}$. By induction one shows that

$$t := y^{q^2/p} - b_n + \tilde{s}^{q/p} + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^{k+1}} (-p)^{d_k/p} f_\rho(y)^{q(p^k-1)/p^{k+1}}, \tag{2.13}$$

satisfies $pv(t) = v(a_n y)$. Then $v_L(p^{q^2} t^{-(p-1)(q+1)}) = v_L(p)/q^2 = [L : K_p]/q^2$, so q^2 divides $[L : K]$. It implies that $L_\rho(X)$ is irreducible over K. In particular

$$L = K(y) = K(y_1, \ldots, y_{q^2}),$$

where $(y_i)_{i=1\ldots q^2}$ are the roots of $L_\rho(X)$.

Step B : *Reduction step.*

Put $G := \mathrm{Gal}(M/K)$, then the last non-trivial group G_{i_0} of the lower ramification filtration $(G_i)_{i\geqslant 0}$ of G is a subgroup of $Z(G)$ ([Ser79] IV §2 Corollary 2 of Proposition 9) and as $Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$, it follows that $G_{i_0} = Z(G)$.

According to **Step VIII** the group $H := \mathrm{Gal}(M/L)$ is $Z(G)$. Consequently, the filtration $(G_i)_{i\geqslant 0}$ can be deduced from that of M/L and L/K (see [Ser79] IV §2 Proposition 2 and Corollary of Proposition 3).

Step C : *Let* $\sigma \in \mathrm{Gal}(L/K) - \{1\}$, *then* $v(\sigma(t) - t) = q^2 v(\pi_K)$.

Let $y' := \sigma(y)$, one deduces the following easy lemma from **Step VII**.

Lemma 2.2.1. *For any* $m \geqslant 0$, $v(y^m - y'^m) \geqslant mv(y)$.

Recall that from the definition of $\tilde{s}$ one has

$$\tilde{s} = 2\rho_0 y + \sum_{k=1}^{n-1} \rho_k y^{p^k}.$$

First one shows that modulo $(y-y')^{q^2/p}\mathfrak{m}$ one has

$$\sigma(\tilde{s})^{q/p} - \tilde{s}^{q/p} \equiv (2\rho_0)^{q/p}(y'^{q/p} - y^{q/p}) + \sum_{k=1}^{n-1} \rho_k^{q/p}(y'^{qp^k/p} - y^{qp^k/p}). \tag{2.14}$$

Indeed, let $(m_i)_{i=0,\dots,n-1} \in \mathbb{N}^n$ be such that $m_0 + m_1 + \cdots + m_{n-1} = q/p$ and put $t := m_0 + m_1 p + \cdots + m_{n-1}p^{n-1}$, then using lemma 2.2.1 one checks that

$$v(p\rho_0^{m_0}\rho_1^{m_1}\dots\rho_{n-1}^{m_{n-1}}(y^t - y'^t)) > \frac{q^2}{p}v(y-y').$$

This inequality implies (2.14).

Let $1 \leqslant k \leqslant n-1$ and write $f_\rho(y)^{(p^k-1)q/p^{k+1}} = 1 + \sum_{i\in I_k} \alpha_{i,k}y^i$, for some set I_k. Then

$$\begin{aligned} &y'^{q/p^{k+1}} f_\rho(y')^{(p^k-1)q/p^{k+1}} - y^{q/p^{k+1}} f_\rho(y)^{(p^k-1)q/p^{k+1}} \\ &= y'^{q/p^{k+1}} - y^{q/p^{k+1}} + \sum_{i\in I_k} \alpha_{i,k}(y'^i - y^i). \end{aligned}$$

Let $i \in I_k$. Consider the case when $v(\alpha_{i,k}) \geqslant v(\rho_h)$ for some $0 \leqslant h \leqslant n-1$, then using **Step VII**, one checks that $\forall\ 1 \leqslant k \leqslant n-1$, $v(\alpha_{i,k}) \geqslant v(\rho_h) > qv(y'-y)/p^{k+1}$. If this case does not occur, then according to the expression of $f_\rho(y)$ one has $i \geqslant q/p^{k+1} + q$ and using lemma 2.2.1 one checks that $v(y'^i - y^i) > qv(y'-y)/p^{k+1}$. In any case $v(\alpha_{i,k}(y'^i - y^i)) > qv(y'-y)/p^{k+1}$ and one checks that

$$v(p^{d_k/p}\rho_k^{q/p^{k+1}}\alpha_{i,k}(y'^i - y^i)) > q^2 v(y'-y)/p. \tag{2.15}$$

Taking into account (2.13), (2.14) and (2.15), one gets mod $(y'-y)^{q^2/p}\mathfrak{m}$

$$\begin{aligned} \sigma(t) - t \equiv\ & y'^{q^2/p} - y^{q^2/p} + (2\rho_0)^{q/p}(y'^{q/p} - y^{q/p}) \\ &+ \sum_{k=1}^{n-1} \rho_k^{q/p}(y'^{qp^k/p} - y^{qp^k/p}) + \sum_{k=1}^{n-1} (-p)^{d_k/p}\rho_k^{q/p^{k+1}}(y'^{q/p^{k+1}} - y^{q/p^{k+1}}). \end{aligned} \tag{2.16}$$

Using lemma 2.2.1, it is now straightforward to check the following relations modulo $(y'-y)^{q^2/p}\mathfrak{m}$.

$$\begin{aligned} y'^{q^2/p} - y^{q^2/p} &\equiv (y'-y)^{q^2/p}, \\ \rho_k^{q/p}(y'^{qp^k/p} - y^{qp^k/p}) &\equiv \rho_k^{q/p}(y'-y)^{qp^k/p}, \\ (-p)^{d_k/p}\rho_k^{q/p^{k+1}}(y'^{q/p^{k+1}} - y^{q/p^{k+1}}) &\equiv (-p)^{d_k/p}\rho_k^{q/p^{k+1}}(y'-y)^{q/p^{k+1}}. \end{aligned}$$

Using **Step VII**, one sees that each of these three elements has valuation $q^2\nu(y'-y)/p$, thus one gets

$$(\sigma(t)-t)^p \equiv (y'-y)^{q^2} + (2\rho_0)^q(y'-y)^q + \sum_{k=1}^{n-1} \rho_k^q (y'-y)^{qp^k} + \sum_{k=1}^{n-1} (-p)^{d_k} \rho_k^{q/p^k} (y'-y)^{q/p^k} \mod (y'-y)^{q^2}\mathfrak{m}. \tag{2.17}$$

Now recall **Step VII**, the definitions of the ρ_k's and of λ, then for some $\nu \in R^\times$ and $\Sigma \in R$

$$\rho_k = u_k \lambda^{p(q-p^k)/(1+q)}, \quad y'-y = \nu\lambda^{p/(1+q)} \text{ and } -p = \lambda^{p-1} + p\lambda\Sigma.$$

Since $q^2\nu(y'-y) = \frac{pq^2}{1+q}\nu(\lambda)$, equation (2.17) becomes

$$(\sigma(t)-t)^p \equiv \lambda^{\frac{q^2p}{1+q}} \left[\nu^{q^2} + (2u_0\nu)^q + \sum_{k=1}^{n-1} (u_k^q \nu^{qp^k} + (u_k\nu)^{q/p^k})\right] \mod \lambda^{\frac{q^2p}{1+q}}\mathfrak{m}.$$

From the action of σ on the stable reduction (see **Step VIII**), one has that the automorphism of $\mathbb{P}^1_k$ given by $t \mapsto t+\bar{\nu}$ has a prolongation to A_u/k, so Proposition 0.6.2 implies that

$$\bar{\nu}^{q^2} + (2\bar{u}_0\bar{\nu})^q + \sum_{k=1}^{n-1} (\bar{u}_k^q \bar{\nu}^{qp^k} + (\bar{u}_k\bar{\nu})^{q/p^k}) + \bar{\nu} = 0. \tag{2.18}$$

Assume that $\bar{\nu}^{q^2} + (2\bar{u}_0\bar{\nu})^q + \sum_{k=1}^{n-1}(\bar{u}_k^q\bar{\nu}^{qp^k} + (\bar{u}_k\bar{\nu})^{q/p^k}) = 0$, then from (2.18) one has $\bar{\nu} = 0$, which contradicts $\nu \in R^\times$. It implies that

$$\nu(\sigma(t)-t) = q^2\nu(\lambda)/(1+q) = q^2\nu(y-y')/p = q^2\nu(\pi_K).$$

Step D : *The ramification filtration of* L/K *is*

$$(G/H)_0 = (G/H)_1 \supsetneq (G/H)_2 = \{1\}.$$

Since K/K_p is tamely ramified of degree $(p-1)(q+1)$, one has $K = K_p(\pi_K)$ with $\pi_K^{(p-1)(q+1)} = p$ for some uniformizer π_K of K. In particular $z := \pi_K^{q^2}/t$, is a uniformizer of L. Let $\sigma \in \mathrm{Gal}(L/K) - \{1\}$, then

$$\sigma(z) - z = \frac{t-\sigma(t)}{\sigma(t)t}\pi_K^{q^2} = \frac{t-\sigma(t)}{\pi_K^{q^2}} \frac{\pi_K^{q^2}}{t} \frac{\pi_K^{q^2}}{\sigma(t)}.$$

Using **Step C** one obtains $\nu(\sigma(z)-z) = 2\nu(z)$, i.e. $(G/H)_2 = \{1\}$.

Step E : *From now on, we assume* $p = 2$. *Let* $s := (q+1)(2q^2-1)$. *There exist* $u, h \in L$ *and* $r \in \pi_L^s\mathfrak{m}$ *such that* $v_L(2y^{q/2}h) = s$ *and*

$$f_\rho(y)u^2 = 1 + \rho_{n-1}y^{1+q/2} + 2y^{q/2}h + r.$$

To prove the first statement we note that, from the definition of $f_\rho(y)$, one has $f_\rho(y) = 1+T$ with $v(T) = qv(y)$ and $L_\rho(y) = 0$, thus

$$\Big(\frac{s_\rho^{q/2}(y)}{b_n}\Big)^2 = f_\rho(y)^{q-1}(1+y) + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^k}}{2^{2+\cdots+2^{n-k}}} f_\rho(y)^{q(2^k-1)/2^k},$$

$$\text{and } f_\rho(y)^{q-1}(1+y) = 1+y+\sum_{k=1}^{q-1}\binom{q-1}{k}T^k(1+y).$$

Then, we put $\tilde{\Sigma} := \sum_{k=1}^{q-1}\binom{q-1}{k}T^k(1+y)$ and

$$h := \frac{s_\rho^{q/2}(y)}{b_n} + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^{k+1}}}{2^{1+\cdots+2^{n-k-1}}} f_\rho(y)^{q(2^k-1)/2^{k+1}} - 1.$$

Then one computes

$$\begin{aligned} h^2 &= \Big[\frac{s_\rho^{q/2}(y)}{b_n} + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^{k+1}}}{2^{1+\cdots+2^{n-k-1}}} f_\rho(y)^{q(2^k-1)/2^{k+1}}\Big]^2 + 1 - 2(h+1) \\ &= (\frac{s_\rho^{q/2}(y)}{b_n})^2 + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^k}}{2^{2+\cdots+2^{n-k}}} f_\rho(y)^{q(2^k-1)/2^k} + \Sigma_1 + 1 - 2(h+1) \\ &= 2+y+2\sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^k}}{2^{2+\cdots+2^{n-k}}} f_\rho(y)^{q(2^k-1)/2^k} + \Sigma_1 + \tilde{\Sigma} - 2(h+1). \end{aligned}$$

In **Step III**, we proved that $v(B_n) = qv(y) = 2v(b_n)/q$ where $B_n = -s_\rho(y)$, it implies that $v(\frac{s_\rho^{q/2}(y)}{b_n}) = 0$ and one checks using **Step I** that

$$v(2) > v(y), \text{ and } \forall\ 1 \leqslant k \leqslant n-1,\ v\Big(\frac{(\rho_k y)^{q/2^{k+1}}}{2^{1+\cdots+2^{n-k-1}}}\Big) \geqslant 0, \tag{2.19}$$

thus $v(h+1) \geqslant 0$ and $v(2(h+1)) \geqslant v(2) > v(y)$. One checks in the same way that $v(\Sigma_1) > v(y)$. One has $v(\tilde{\Sigma}) \geqslant v(T) > v(y)$, so $v(h^2) = v(y)$ and $v_L(2y^{q/2}h) = s$.

To prove the second statement of **Step E**, we first remark that

$$\forall i \geqslant 1,\ f_\rho(y)^i = 1 + \sum_{k=1}^{i}\binom{i}{k}T^k = 1+\Sigma_i,$$

whence $v(\Sigma_i) \geqslant v(T)$. Since, for all $0 \leqslant k \leqslant n-1$, $v(\rho_k y^{p^k}) > qv(y)$ one has mod $\pi_L^s\mathfrak{m}$

$$\frac{s_\rho^{q/2}(y)}{b_n} 2y^{q/2} \equiv \big[(2\rho_0 y)^{q/2} + \sum_{k=1}^{n-1}(\rho_k y^{2^k})^{q/2} + y^{q^2/2}\big]\frac{y^{q/2}}{2^{2+\cdots+2^{n-1}}}. \tag{2.20}$$

One also checks that $\forall i \geqslant 1$, $v_L(2y^{q/2}\Sigma_i) > s$, then according to (2.19), $\forall\ i \geqslant 1$ and $1 \leqslant k \leqslant n-1$

$$v_L\Big(\frac{(\rho_k y)^{q/2^{k+1}}}{2^{1+\cdots+2^{n-k-1}}} 2y^{q/2}\Sigma_i\Big) > s \text{ and one checks that } v_L\Big(\frac{(2\rho_0)^{q/2}y^q}{2^{2+\cdots+2^{n-1}}}\Big) > s. \tag{2.21}$$

Thus, applying relations (2.20), (2.21) and the definition of h, one has

$$2hy^{q/2} \equiv \Big[\sum_{k=1}^{n-1}(\rho_k y^{2^k})^{q/2} + y^{q^2/2}\Big]\frac{y^{q/2}}{2^{2+\cdots+2^{n-1}}} + \sum_{k=1}^{n-1}\frac{(\rho_k y)^{q/2^{k+1}}}{2^{1+\cdots+2^{n-k-1}}}2y^{q/2} - 2y^{q/2} \bmod \pi_L^s\mathfrak{m}. \tag{2.22}$$

Finally one puts

$$u := 1 - y^{q/2} - \sum_{k=0}^{n-2}\frac{y^{2^k(1+q)}}{2^{1+\cdots+2^k}} + \sum_{i=1}^{n-1}\sum_{k=n-i-1}^{n-2}\frac{\rho_i^{2^k}}{2^{1+\cdots+2^k}}y^{2^k(1+2^i)} = 1+\tilde{u},$$

and one checks that $v(\tilde{u}) = v(y^{q/2})$. From the equality

$$f_\rho(y)u^2 - 1 = \sum_{k=0}^{n-1}\rho_k y^{1+2^k} + y^q + y^{1+q} + (1+T)2\tilde{u} + (1+T)\tilde{u}^2,$$

taking into account that $v_L(2T\tilde{u}) > s$, $v_L(T\tilde{u}^2) > s$, $\forall\ 0 \leqslant k \leqslant n-2$, $v_L(\rho_k y^{1+2^k}) > s$ and expanding $\tilde{u}$ and $\tilde{u}^2$ one gets modulo $\pi_L^s\mathfrak{m}$

$$f_\rho(y)u^2 - 1 \equiv \rho_{n-1}y^{1+q/2} - 2y^{q/2} + 2y^q - \sum_{k=1}^{n-2}\frac{2y^{2^k(1+q)}}{2^{1+\cdots+2^k}} + \sum_{k=1}^{n-1}\frac{y^{2^k(1+q)}}{2^{2+\cdots+2^k}} + \sum_{i=1}^{n-1}\sum_{k=n-i-1}^{n-2}\frac{2\rho_i^{2^k}y^{2^k(1+2^i)}}{2^{1+\cdots+2^k}} + \sum_{i=1}^{n-1}\sum_{k=n-i}^{n-1}\frac{\rho_i^{2^k}y^{2^k(1+2^i)}}{2^{2+\cdots+2^k}}. \tag{2.23}$$

Arranging the terms of (2.23) , taking into account that $v_L(2y^q) > s$ and

$$\forall\ 1 \leqslant i \leqslant n-1,\ \forall\ n-i \leqslant k \leqslant n-2,\ v_L\Big(\rho_i^{2^k}y^{2^k(1+2^i)}\frac{2}{2^{2+\cdots+2^k}}\Big) > s,$$

then comparing with (2.22), one obtains $f_\rho(y)u^2 - 1 \equiv \rho_{n-1}y^{1+q/2} + 2hy^{q/2} \bmod \pi_L^s\mathfrak{m}$.

Step F: *The ramification filtration of* M/L *is*

$$H_0 = H_1 = \cdots = H_{1+q} \supsetneq \{1\}.$$

One has to show that $v_M(\mathcal{D}_{M/L}) = q+2$, we will use freely results from [Ser79] IV. If $\rho_{n-1} = 0$, then according to **Step E**, one has

$$f_\rho(y)u^2 = 1 + 2y^{q/2}h + r,$$

and one concludes using Lemma 0.3.1 Lemma 2.1. Otherwise, if $\rho_{n-1} \neq 0$, one has

$$\max_{u\in L^\times} v_L(f_\rho(y)u^2 - 1) \geqslant v_L(\rho_{n-1}y^{1+q/2}),$$

then [LRS93] Lemma 6.3 implies that $v_M(\mathcal{D}_{M/L}) \leqslant q+3$. Using **Step B**, **Step D** and [Ser79] IV §2 Proposition 11, one has that the break in the ramification filtration of M/L is congruent to $1 \bmod 2$, i.e. $v_M(\mathcal{D}_{M/L}) \leqslant q+2$. According to **Step D** and lemma 0.3.2,

the break t of M/L is in $1+q\mathbb{N}$. If $t=1$ then $G_2=\{1\}$ and $G_1/G_2=G/G_2\simeq G$ would be abelian, so $t\geqslant 1+q$, i.e. $v_M(\mathcal{D}_{M/L})\geqslant q+2$.

Step G : *Computations of conductors.*

For $l\neq 2$ a prime number, the G-modules $\mathrm{Jac}(C)[l]$ and $\mathrm{Jac}(\mathcal{C}_k)[l]$ being isomorphic one has that for $i\geqslant 0$

$$\dim_{\mathbb{F}_l}\mathrm{Jac}(C)[l]^{G_i}=\dim_{\mathbb{F}_l}\mathrm{Jac}(\mathcal{C}_k)[l]^{G_i}.$$

Moreover, for $0\leqslant i\leqslant 1+q$ one has $\mathrm{Jac}(\mathcal{C}_k)[l]^{G_i}\subseteq\mathrm{Jac}(\mathcal{C}_k)[l]^{Z(G)}$, then according to the end of **Step VIII** one has $\mathcal{C}_k/Z(G)\simeq\mathbb{P}^1_k$ and lemma 0.5.1 implies that

$$\forall\, 0\leqslant i\leqslant 1+q,\ \dim_{\mathbb{F}_l}\mathrm{Jac}(\mathcal{C}_k)[l]^{G_i}=0.$$

Since $g(C)=q/2$ one gets $f(\mathrm{Jac}(C)/K)=2q+1$ and $\mathrm{sw}(\mathrm{Jac}(C)/K_2)=1$. □

Example : Magma codes are available on the author webpage. Let $K:=K_2(2^{1/5})$ and $f(X):=1+2^{6/5}X^2+2^{4/5}X^3+X^4+X^5\in K[X]$, one checks that the smooth, projective, integral curve birationally given by $Y^2=f(X)$ has the announced properties, that is the wild monodromy M/K has degree 32 and one can describe its ramification filtration. The first program checks that **Step A** and **Step D** hold for this example. The second program checks **Step F** and is due to Guardia, J., Montes, J. and Nart, E. (see [GMN11]) and computes $v_M(\mathcal{D}_{M/K_2})=194$. Using [Ser79] III §4 Proposition 8, one finds that $v_M(\mathcal{D}_{M/K})=66$, which was the announced result in Theorem 2.2.1 3.

Remarks :

1. The above example was the main motivation for **Step F** since it shows that one could expect the correct behavior for the ramification filtration of $\mathrm{Gal}(M/K)$ when $p=2$.
2. The naive method to compute the ramification filtration of M/K in the above example fails. Indeed, in this case Magma needs a huge precision when dealing with 2-adic expansions to get the correct discriminant.

3 BIG ACTIONS WITH NON-ABELIAN DERIVED SUBGROUP.

"Si vous voulez n'être jamais effrayé par la multitude de vos travaux et de vos peines, attendez-vous toujours à tout ce qu'il y aura de plus dur et de plus pénible."
Sun Tzu in *L'art de la guerre*

Table of Contents

3.1 INTRODUCTION

Let k be an algebraically closed field of characteristic $p > 0$. A *big action* is a pair (X, G) where X/k is a smooth, projective, integral curve of genus $g(X) \geqslant 2$ and G is a finite p-group, $G \subseteq \mathrm{Aut}_k(X)$, such that $|G| > \frac{2p}{p-1} g(X)$. Big actions were studied by Lehr and Matignon [LM05] then by Matignon and Rocher [MR08] and Rocher [Roc09]. The examples of big actions (X, G) appearing in these papers have an abelian derived group $D(G)$. The main goal of this chapter is to give the first example, to our knowledge, of big action (X, G) with a non-abelian $D(G)$.

The approach in [MR08] to construct big actions (X, G) with an abelian $D(G)$ is to consider ray class fields of function fields. One puts $n \in \mathbb{N} - \{0\}$, $q := p^n$, $m \in \mathbb{N}$, $K := \mathbb{F}_q(x)$, $S := \{(x - a), a \in \mathbb{F}_q\}$ be the set of finite $\mathbb{F}_q$-rational places of K and ∞ be the place $(\frac{1}{x})$. One defines the *S-ray class field mod* $m\infty$, denoted by $K_S^{m\infty}$, as the largest abelian extension L/K with conductor $\leqslant m\infty$ such that every place in S splits completely in L.

Denote by $G_S(m) := \mathrm{Gal}(K_S^{m\infty}/K)$ and let $C_S(m)/\mathbb{F}_q$ be the smooth, projective, integral curve with function field $K_S^{m\infty}/\mathbb{F}_q$ and denote by $g(C_S(m))$ its genus. Then, the group of $\mathbb{F}_q$-automorphisms of $\mathbb{P}^1_{\mathbb{F}_q}$ given by $x \mapsto x + a$ with $a \in \mathbb{F}_q$ has a prolongation to a p-group $G(m) \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C_S(m))$ with an exact sequence

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

Moreover, one has

$$\text{if } m > \sqrt{pq} + 2, \text{ then } |G(m)| > \frac{q}{-1 + m/2} g(C_S(m)).$$

The crucial point is that one may choose q and m such that $\frac{q}{-1+m/2} \geqslant \frac{2p}{p-1}$, thus one has $|G(m)| > \frac{2p}{p-1} g(C_S(m))$, in particular the pair $(C_S(m), G(m))$ is a big action. It follows from Proposition 0.6.1 2 and Proposition 0.8.4 that $D(G(m)) = G_S(m)$ which is an abelian p-group having arbitrarily large exponent.

In order to produce big actions with non-abelian derived subgroup, we are going to mimic this construction in a slightly different context. Assume that $q = pq_0^2$ with $q_0 = p^s$, $s \in \mathbb{N}$. Let $K_1 := K_S^{m\infty}$ where $m = pq_0 + 3$, then according to [Aueoo], one has $K_1 = K(y_1, y_2)$ with

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x), \end{cases}$$

and $[K_1 : K] = q^2$. In the spirit of [Abr95] example page 48, we will consider for $p > 2$ the K_1-algebra $K_2 := K_1[W]/(P(W)) = K_1[w]$ where

$$P(W) := W^q - W - \frac{1}{2}(y_2^q y_1 - y_1^q y_2).$$

The set of transformations $\sigma_{a,b,c}$ with $(a, b, c) \in \mathbb{F}_q^3$ such that

$$\begin{aligned} \sigma_{a,b,c}(y_1) &= y_1 + a \\ \sigma_{a,b,c}(y_2) &= y_2 + b \\ \sigma_{a,b,c}(w) &= w + \frac{1}{2}(-by_1 + ay_2) + c. \end{aligned}$$

defines a group of K-automorphisms of the K-algebra K_2. An exercise shows that this automorphism group is isomorphic to the unipotent linear group $UL_3(\mathbb{F}_q)$ of 3-dimensional upper triangular matrices with entries in $\mathbb{F}_q$. This group is, in particular, a non-abelian p-group. We will prove that the K-algebra K_2 is a field by exhibiting a uniformization at $x = \infty$ of the curve defined by $y_1^q - y_1 = f_1(x)$; moreover, one computes the genus of K_2. Actually, in order to produce a big action, we need to consider a cover of K_2 obtained by extending the monomorphisms $K_2 \hookrightarrow K^{alg}$ induced by the automorphisms of K given by $x \mapsto x + a$, $a \in \mathbb{F}_q$. More precisely, we will prove the following

Theorem 3.1.1. *Let $p > 2$ be a prime number, $s \in \mathbb{N} - \{0, 1\}$, $q_0 = p^s$ and $q = pq_0^2$. Let $K = \mathbb{F}_q(x)$ and put $F := K[y_1, y_2, v_1, v_2, w]$ where*

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x) \\ v_1^q - v_1 &= y_1^q x - x^q y_1 \\ v_2^q - v_2 &= y_2^q x - x^q y_2 \\ w^q - w &= f_2(x)y_1 - f_1(x)y_2 = y_2^q y_1 - y_1^q y_2. \end{cases}$$

Then F is a field extension of K of degree q^5 and $\mathbb{F}_q^{alg} \cap F = \mathbb{F}_q$. Let $X/\mathbb{F}_q$ be the smooth projective integral curve with function field $F/\mathbb{F}_q$. Let $H \subseteq Aut_{\mathbb{F}_q}(K)$ be the subgroup of translations $x \mapsto x + a$, $a \in \mathbb{F}_q$, then any $h \in H$ has q^5 prolongations to F, the extension F/K^H is Galois, the group $G := Gal(F/K^H)$ has order q^6, the pair (X, G) is a big action and $D(G) = Gal(F/K)$ is a non-abelian group.

3.2 A TOWER.

Notations : Let $p > 2$ be a prime number, $s \in \mathbb{N} - \{0, 1\}$, $q_0 := p^s$ and $q := pq_0^2$. Let

$$\begin{aligned} Frob_p : K^{alg} &\longrightarrow K^{alg} \\ x &\longmapsto x^p, \end{aligned}$$

then $\mathrm{Frob}_q := \mathrm{Frob}_p^{2s+1}$ and $\wp = \mathrm{Frob}_p - \mathrm{Id}$. Then one puts $K := \mathbb{F}_q(x)$ and $F := K(y_1, y_2, v_1, v_2, w)$ where $y_1, y_2, v_1, v_2, w \in K^{alg}$ satisfy

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x) \\ v_1^q - v_1 &= y_1^q x - x^q y_1 \\ v_2^q - v_2 &= y_2^q x - x^q y_2 \\ w^q - w &= f_2(x)y_1 - f_1(x)y_2 = y_2^q y_1 - y_1^q y_2. \end{cases}$$

We will make extensive use of the following consequence of the *Artin-Schreier theory*, see for instance [Neu99].

Proposition 3.2.1. *Let $\wp : K^{alg} \to K^{alg}$, $z \mapsto z^p - z$. Let $U \subseteq K$ be a finite set and put $L := K(\wp^{-1}(U)) \subseteq K^{alg}$. One puts $V := \sum_{u \in U} \mathbb{F}_p u$, then $\wp K$ is a subgroup of finite index of $V + \wp K$ and L/K is an elementary abelian extension of degree*

$$[L : K] = (V + \wp K : \wp K).$$

Remark : The previous system of equations is equivalent to

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x) \\ v_1'^q - v_1' &= x^{q_0}(x^{2q} - x^2) =: g_1(x) \\ v_2'^q - v_2' &= x^{2q_0}(x^{2q} - x^2) =: g_2(x) \\ w'^q - w' &= 2y_1 f_2(x) + f_1(x)f_2(x), \end{cases}$$

Theorem 3.2.1. *One has $[F : K] = q^5$ and $\mathbb{F}_q^{alg} \cap F = \mathbb{F}_q$. Let $X/\mathbb{F}_q$ be the smooth, projective, integral curve with function field $F/\mathbb{F}_q$. Let $H \subseteq \mathrm{Aut}_{\mathbb{F}_q}(K)$ be the subgroup of translations $x \mapsto x + a$, $a \in \mathbb{F}_q$, then any $h \in H$ has q^5 prolongations to F, the extension F/K^H is Galois, the group $G := \mathrm{Gal}(F/K^H)$ has order q^6, the pair (X, G) is a big action and $D(G) = \mathrm{Gal}(F/K)$ is a non-abelian group.*

Proof. First of all, the extension $K(y_1) = K(\wp^{-1}(U))$ is the compositum of extensions of degree p of K given by

$$y_{1,i}^p - y_{1,i} = \alpha_i f_1(x),$$

where $\alpha_i \in \mathbb{F}_q^\times$ and the set $U := \{\alpha_i f_1(x), \alpha_i \in \mathbb{F}_q^\times\}$ spans an $\mathbb{F}_p$-vector space modulo $\wp K$ of dimension $2s+1$.

Following [Aueoo], let $\gamma_j \in \mathbb{F}_q^\times$ and $y_1, y_{2,j} \in K^{alg}$ satisfy

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ y_{2,j}^p - y_{2,j} &= \gamma_j f_2(x). \end{cases}$$

Note that

$$\begin{aligned} \alpha_i f_1(x) &= \alpha_i^{q/q_0} x^{1+q/q_0} - \alpha_i x^{1+q_0} \bmod \wp K, \\ \text{and } \gamma_j f_2(x) &= \gamma_j^{q/q_0} x^{2+q/q_0} - \gamma_j x^{1+2q_0} \bmod \wp K. \end{aligned} \tag{3.1}$$

Thus $U_j := \{\gamma_j f_2(x), \alpha_i f_1(x), \alpha_i \in \mathbb{F}_q^\times\}$ spans an $\mathbb{F}_p$-vector space modulo $\wp K$ of dimension $2s+2$. According to Proposition 3.2.1, one has

$$K(y_1, y_{2,j}) = K(\wp^{-1}(U_j)) \text{ and } [K(y_1, y_{2,j}) : K] = qp.$$

Applying Proposition 0.3.1, one obtains

$$g(K(y_1, y_{2,j})) = \frac{q}{2q_0}\big[qp + q_0 p - q_0 - 1\big].$$

Note that equation (3.1) implies that $\{\gamma_j f_2(x), \gamma_j \in \mathbb{F}_q^\times\}$ spans an $\mathbb{F}_p$-vector space modulo $\wp K(y_1)$ of dimension $2s+1$.

Let $\gamma_j \in \mathbb{F}_q^\times$ and $y_1, v'_{1,j}, v'_{2,j} \in K^{alg}$ such that

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ v_{1,j}'^p - v'_{1,j} &= \gamma_j g_1(x), \end{cases} \qquad \begin{cases} y_1^q - y_1 &= f_1(x) \\ v_{2,j}'^p - v'_{2,j} &= \gamma_j g_2(x). \end{cases}$$

As above, one shows that $[K(y_1, v'_{1,j}) : K] = qp$ and $[K(y_1, v'_{2,j}) : K] = qp$ and one computes their genera

$$g(K(y_1, v'_{1,j})) = \frac{q}{2q_0}\big[2qp - q - 1\big],$$
$$g(K(y_1, v'_{2,j})) = \frac{q}{2q_0}\big[2qp + q_0 p - q_0 - q - 1\big].$$

Moreover, the set $\{\gamma_j g_1(x), \gamma_j \in \mathbb{F}_q^\times\}$ (resp. $\{\gamma_j g_2(x), \gamma_j \in \mathbb{F}_q^\times\}$) spans an $\mathbb{F}_p$-vector space modulo $\wp K(y_1)$ of dimension $2s+1$.

Let $\gamma_j \in \mathbb{F}_q^\times$ and $y_1, w'_j \in K^{alg}$ satisfy

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ w_j'^p - w'_j &= \gamma_j\big[2y_1 f_2(x) + f_1(x) f_2(x)\big] = \gamma_j F(x, y_1). \end{cases}$$

One needs an expression of y_1 and x in terms of a uniformizing parameter z of $K(y_1)$ at infinity, this is the crucial point of the proof and it is detailed in the following Proposition.

Proposition 3.2.2. *One has* $[K(y_1, w'_j) : K] = qp$ *and* $K(y_1, w'_j)$ *has genus*

$$g(K(y_1, w'_j)) = \frac{q}{2q_0}\big[2pq + 2pq_0 - 2q_0 - q - 1\big].$$

Proof. One defines $z \in K^{alg}$ by

$$x = z^{-q} + z^{a_1} - z^{a_2},$$
$$\text{with } a_1 := \frac{q^2 - qq_0 - q}{q_0},\ a_2 := \frac{q^2 - q_0 - q}{q_0}.$$

Then, one shows that this change of variable splits completely the place $x = \infty$ in $K(y_1)$. One writes T for an indeterminate and one puts

$$b_1 := a_1 - qq_0, \quad b_2 := a_2 - qq_0,$$
$$y_T := \frac{1}{z^{q+q_0}} + z^{b_1} - z^{b_2} + z^{a_1 q_0 - q} - z^{a_2 q_0 - q} + z^{a_1(1+q_0)} + z^{a_2(1+q_0)} - z^{a_1 + a_2 q_0} - z^{a_1 q_0 + a_2} + T.$$

By expanding $y_T^q - y_T - f_1(x)$, a tedious computation left to the reader shows that for some $G(z) \in \mathbb{F}_q[[z]]$

$$y_T^q - y_T - f_1(x) = z^{qb_1}(1 + zG(z)) + T^q - T.$$

Denote by ν_z the discrete valuation of $\mathbb{F}_q[[z]]$ such that $\nu_z(z) = 1$. According to Hensel's lemma, the equation $T^q - T + z^{qb_1}(1 + zG(z)) = 0$ in $\mathbb{F}_q[[z]][T]$ has a solution $T_0 \in \mathbb{F}_q[[z]]$ such that $\nu_z(T_0) > 0$, thus $\nu_z(T_0) = qb_1$. So one has a solution $y_{T_0} \in \mathbb{F}_q[[z]]$ to the equation $Y^q - Y = f_1(x)$. Hence, one has the following diagram

$$\begin{array}{ccc} \mathbb{F}_q((z)) & \supseteq & \mathbb{F}_q((\frac{1}{x}))[y_{T_0}] \\ & \searrow \quad \swarrow & \\ & \mathbb{F}_q((\frac{1}{x})) & \end{array}$$

One has $[\mathbb{F}_q((z)) : \mathbb{F}_q((\frac{1}{x}))] = q$. According to Proposition 0.8.4, the extension $K(y_1)/K$ has degree q and is totally ramified above ∞, thus one has $[\mathbb{F}_q((\frac{1}{x}))[y_{T_0}] : \mathbb{F}_q((\frac{1}{x}))] = q$. It follows that $\mathbb{F}_q((\frac{1}{x}))[y_{T_0}] = \mathbb{F}_q((z))$, i.e. z is a uniformizing parameter of $K(y_1)$ at infinity.

Remark : Note that letting $y_T := \frac{1}{z^{q+q_0}} + z^{b_1} + T$ and using the same process as above, one still obtains that z is a uniformizing parameter of $K(y_1)$ at infinity, but in this case one has $\nu(T_0) = b_2$ and one needs a much more accurate expansion of y_1 in order to show that $K(y_1, w_j')$ is a field extension of K of degree qp and to compute its genus, see below.

Then, one expands $\gamma_j F(x, y_1) \in \mathbb{F}_q((z))$ in terms of z and T_0 and one reads its principal part $P_j(z)$. Note that $\nu_z(T_0) = qb_1$ implies that the terms in $\gamma_j F(x, y_1)$ where T_0 appears do not disturb $P_j(z)$. One has

$$P_j(z) = \gamma_j \Big[\frac{1}{z^{3q_0q+2q^2}} + \frac{1}{z^{q^2+q+3q_0q}} - \frac{1}{z^{q_0+q+qq_0-a_2q_0+q^2}} - \frac{1}{z^{q_0+q+2qq_0+q^2}} \Big],$$

and mod $\wp(\mathbb{F}_q((z)))$ one has

$$P_j(z) \equiv \frac{\gamma_j^{q/q_0}}{z^{3+2pq_0}} + \frac{\gamma_j}{z^{1+3q_0+q}} - \frac{\gamma_j^{q/q_0}}{z^{1+pq_0+q-a_2+pq_0q}} - \frac{\gamma_j^{q/q_0}}{z^{1+pq_0+2q+pq_0q}}. \tag{3.2}$$

It follows that the conductor of the extension $K(y_1, w_j')/K(y_1)$ is $2 + pq_0 + 2q + pq_0q$, in particular one has $[K(y_1, w_j') : K(y_1)] = p$, whence $[K(y_1, w_j') : K] = qp$. Thus applying the Riemann-Hurwitz formula, one obtains

$$g(K(y_1, w_j')) = \frac{q}{2q_0}\big[2pq + 2pq_0 - 2q_0 - q - 1\big].$$

Note that equation (3.2) implies that $\{\gamma F(x, y_1), \gamma \in \mathbb{F}_q^\times\}$ spans an $\mathbb{F}_p$-vector space modulo $\wp K(y_1)$ of dimension $2s + 1$.

□

One comes back to the proof of Theorem 3.2.1. Let

$$U := \{\gamma f_2(x), \gamma \in \mathbb{F}_q^\times\} \cup \{\gamma g_1(x), \gamma \in \mathbb{F}_q^\times\} \cup \{\gamma g_2(x), \gamma \in \mathbb{F}_q^\times\} \cup \{\gamma F(x, y_1), \gamma \in \mathbb{F}_q^\times\}.$$

One has proven that, modulo $\wp K(y_1)$, each set

$$\{\gamma f_2(x), \gamma \in \mathbb{F}_q^\times\}, \{\gamma g_1(x), \gamma \in \mathbb{F}_q^\times\}, \{\gamma g_2(x), \gamma \in \mathbb{F}_q^\times\}, \{\gamma F(z), \gamma \in \mathbb{F}_q^\times\},$$

spans an $\mathbb{F}_p$-vector space of dimension $2s+1$ and the corresponding extensions have distinct conductors since their genera are distinct. It implies that, modulo $\wp K(y_1)$, the set U spans an $\mathbb{F}_p$-vector space of dimension $4(2s+1)$. Thus, according to Proposition 3.2.1, one has $[F : K(y_1)] = q^4$.

Applying Proposition 0.3.1, since one has shown that

$$g(K(y_1, w_j')),\ g(K(y_1, v_{2,j}')),\ g(K(y_1, v_{1,j}'))\ \text{ and } g(K(y_1, y_{2,j})),$$

are independent of j, one obtains

$$g(F) = \frac{q-1}{p-1}\big[q^3 g(K(y_1, w_j')) + q^2 g(K(y_1, v_{2,j}')) + q g(K(y_1, v_{1,j}')) + g(K(y_1, y_{2,j}))\big] - \frac{q-1}{p-1}\frac{q}{2q_0}(q-1). \tag{3.3}$$

Then, one shows that the group $\mathrm{Gal}(F/K)$ is non-abelian. One defines K-automorphisms of F/K by

$$\begin{cases} \sigma_i(y_1) &= y_1 + \gamma_i \\ \sigma_i(y_2) &= y_2 \\ \sigma_i(v_1') &= v_1' + \gamma_i \\ \sigma_i(v_2') &= v_2' \\ \sigma_i(w) &= w + \gamma_i y_2 \end{cases} \quad \text{and} \quad \begin{cases} \tau_i(y_1) &= y_1 \\ \tau_i(y_2) &= y_2 + \gamma_i \\ \tau_i(v_1') &= v_1' + \gamma_i \\ \tau_i(v_2') &= v_2' \\ \tau_i(w) &= w - \gamma_i y_1 \end{cases}$$

are such that τ_i and σ_j do not commute since $p > 2$.

Let $a \in \mathbb{F}_q$ and $t_a \in \mathrm{Aut}_{\mathbb{F}_q}(K)$ given by $x \mapsto x + a$. Let $\sigma : F \hookrightarrow K^{\mathrm{alg}}$ be a morphism such that $\sigma|_K = t_a$, an easy computation shows that

$$\begin{gathered}(\sigma(y_1)^q - \sigma(y_1)) - (y_1^q - y_1),\ (\sigma(y_2)^q - \sigma(y_2)) - (y_2^q - y_2),\\ (\sigma(v_1')^q - \sigma(v_1')) - (v_1'^q - v_1'),\ (\sigma(v_2')^q - \sigma(v_2')) - (v_2'^q - v_2'),\\ (\sigma(w')^q - \sigma(w')) - (w'^q - w'),\end{gathered}$$

are in $\mathrm{Frob}_q(F)$, thus the elements of H have q^5 prolongations to F and F/K^H is a Galois extension of degree q^6.

Using equation (3.3), an easy computation shows that (X, G) is a big action. Actually, the leading term in equation (3.3) is $\frac{q-1}{p-1}q^3 g(K(y_1, w_j'))$ which, surprisingly, is not too large compared to $|G|$, that is why (X, G) is a big action

Remark : Note that equation (3.3) implies that $\lim_{p\to\infty} \frac{|G|}{q_0 g(F)} = 1$, checking the inequality $|G| > \frac{2p}{p-1} g(F)$ being left to the reader.

One shows that $D(G) = \mathrm{Gal}(F/K)$. Let $L := F^{D(G)}$, according to Proposition 0.6.1 2, one has $D(G) \subseteq \mathrm{Gal}(F/K)$, whence $K \subseteq L$ and the function field L has genus 0, so the

Riemann-Hurwitz formula implies that the conductor of L/K is $\leqslant 2\infty$. Let S be the set of finite $\mathbb{F}_q$-rational places of K, i.e. $S := \{(x-a), a \in \mathbb{F}_q\}$. Then L/K is an abelian extension with conductor $\leqslant 2\infty$ such that every place in S completely split splits in L, then $L \subseteq K_S^{2\infty}$. According to Proposition 0.8.4, one has $K_S^{2\infty} = K$, it implies that $L = K$ and $D(G) = \mathrm{Gal}(F/K)$.

□

Remark : Let $k = \mathbb{F}_q^{alg}$ and $X_k = X \times_{\mathbb{F}_q} k$. The group G may be seen as a subgroup of $\mathrm{Aut}_k(X_k)$. Moreover, it fixes a point, say ∞. As $\frac{|G|}{g(X_k)} > \frac{p}{p-1}$, it follows from [GK10] that the full group $\mathrm{Aut}_k(X_k)$ fixes the point ∞. This is a good reason for expecting that $\mathrm{Aut}_k(X_k) = G$.

4 S-RAY CLASS FIELDS OF NONZERO GENUS CURVES.

"Ils passent en un éclair devant les yeux de sa mémoire, devant les yeux de son âme.
Ils habitent sa mémoire et son coeur et son âme et les yeux de son âme.
Ils habitent son regard."
C. Péguy in *Le porche du mystère de la deuxième vertu*

Table of Contents

4.1 INTRODUCTION

Deligne-Lusztig varieties are of particular interest, see [Lus77], among them the Deligne-Lusztig curves enjoy peculiar properties and have been extensively studied (see [HP93], [Han92], [Lau99b], [Ped92]). Especially, these curves turn out to have many points, more precisely, they have the maximum number of $\mathbb{F}_q$-rational points for their genus and they are maximal over a suitable extension of $\mathbb{F}_q$, in the sense that they reach the Hasse-Weil bound after a suitable extension of the field of constants. It was one of the reasons for investigating the relation between these curves and class field theory. In [Lau99b] the Deligne-Lusztig curves are described as S-ray class fields of $\mathbb{P}^1_{\mathbb{F}_q}$ where $S = \{(x-a), a \in \mathbb{F}_q\}$, in particular the Ree curve $X_R/\mathbb{F}_q$ defined by the equations

$$X_R : \begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x), \end{cases}$$

where $q = 3q_0^2 = 3^{2s+1}$, is such that $\mathbb{F}_q(x, y_1, y_2)$ and $\mathbb{F}_q(x, y_1)$ are S-ray class fields of $\mathbb{F}_q(x)$. Thus, one asks the following question

(Q1) Is $\mathbb{F}_q(x, y_1, y_2)$ an S-ray class field of $\mathbb{F}_q(x, y_1)$ for some S ?

This raises the question of computing S-ray class fields of a nonzero genus curve $C/\mathbb{F}_q$. In [Lau99a], the author gives a general result making it possible to compute S-ray class fields of $\mathbb{P}^1_{\mathbb{F}_q}$ having arbitrarily high genus, see also [Aue99], [Aue00]. In his thesis, R. Auer (see [Aue99]) describes an algorithm to compute S-ray class fields of a non necessarily genus zero curve, however the only tables of such ray class fields

are, to our knowledge, for $C/\mathbb{F}_q$ of genus $g(C) \leqslant 5$ with $q = p^s$ such that $s \leqslant 4$ and C has gonality less than 2 except over $\mathbb{F}_2$ where curves of genus up to 50 are studied, see for example [Aue99], [Aue00], [Lau96], [FD12] and [Rok]. In particular, it makes this approach ineffective in order to answer question **(Q1)** as soon as $s \geqslant 1$ since $\mathbb{F}_q(x, y_1)/\mathbb{F}_q$ has genus $\frac{3}{2}q_0(q-1)$ and has degree q over $\mathbb{F}_q(x)$.

In this chapter, one gives a method to compute the S-Hilbert class field of a non zero genus curve by studying its automorphism group. This method applies to supersingular abelian covers of the projective line having exponent p and thus to the Deligne-Lusztig curves, in particular one has a partial answer to **(Q1)** (see Proposition 4.2.1). Tables of results may be found in Section 4.4.

4.2 S-HILBERT CLASS FIELDS

The following result is the technical heart of our construction, it will be applied in several explicit situations later on.

Theorem 4.2.1. *Let $C/\mathbb{F}_q$ be a smooth, projective, irreducible curve. Let $\infty \in C(\mathbb{F}_q)$, let $S \subseteq C(\mathbb{F}_q) - \{\infty\}$ be non-empty and let*

$$\begin{aligned} \theta : C(\mathbb{F}_q) &\to \mathrm{Jac}(C)(\mathbb{F}_q) \\ P &\mapsto [P - \infty]. \end{aligned}$$

Let $n \geqslant 1$ and for $1 \leqslant i \leqslant n$ let H_i be a finite subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(C)$. Put $C_i := C/H_i$, the quotient morphism $\pi_i : C \to C_i$, $S_i := \pi_i(S)$, $\infty_i := \pi_i(\infty)$ and

$$\begin{aligned} \theta_i : C_i(\mathbb{F}_q) &\to \mathrm{Jac}(C_i)(\mathbb{F}_q) \\ P &\mapsto [P - \infty_i]. \end{aligned}$$

Assume that

1. *One has $H_i(S) \subseteq S$ for $1 \leqslant i \leqslant n$.*
2. *The morphism π_i totally splits over S_i and is totally ramified over ∞_i for $1 \leqslant i \leqslant n$.*
3. *One has $[H_i, H_j] = \{1\}$ for $1 \leqslant i, j \leqslant n$.*
4. *One has $\mathrm{Jac}(C)(\mathbb{F}_q)^{<H_i, H_j>} = \{0\}$ for $1 \leqslant i \neq j \leqslant n$.*
5. *One has $\gcd(p, |\mathrm{Jac}(C)(\mathbb{F}_q)|) = 1$ and $\gcd(|H_i|, |\mathrm{Jac}(C)(\mathbb{F}_q)|) = 1$ for $1 \leqslant i \leqslant n$.*
6. *One has $|\mathrm{Jac}(C)(\mathbb{F}_q)| = \prod_{i=1}^{n} |\mathrm{Jac}(C_i)(\mathbb{F}_q)|$.*

If $\forall i \in [\![1, n]\!]$, $< \theta_i(S_i) >= \mathrm{Jac}(C_i)(\mathbb{F}_q)$ then $< \theta(S) >= \mathrm{Jac}(C)(\mathbb{F}_q)$.

Proof. For the sake of simplicity we give the proof for $n = 2$, the general case is then a straightforward generalization. Put $h_i = |H_i|$ and

$$\begin{aligned} \pi_* : \mathrm{Jac}(C) &\to \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2) \\ D &\mapsto (\pi_{1*}D, \pi_{2*}D). \end{aligned}$$

Let $P_1 \in S_1$, one shows that $\pi_*(\pi_1^*(P_1 - \infty_1)) = (h_1(P_1 - \infty_1), 0)$. It is well-known that $\pi_{1*}\pi_1^*(P_1 - \infty_1) = h_1(P_1 - \infty_1)$, see for instance [Liu02] Theorem 7.2.8. According to *1.* and *2.* one has

$$\pi_1^{-1}(P_1) = \{Q_1, \dots, Q_{h_1}\} \subseteq S, \tag{4.1}$$

thus

$$\pi_1^*(P_1 - \infty_1) = [Q_1 + \cdots + Q_{h_1} - h_1\infty] \in < \theta(S) > .$$

Put $D := \pi_{2*}\pi_1^*(P_1 - \infty_1)$, one shows that $\pi_2^*D \in \mathrm{Jac}(C)^{H_1}$. Let $g_1 \in H_1$ and $P \in \mathrm{Supp}\,\pi_2^*D - \{\infty\}$, then there exists $g_2 \in H_2$ such that $P = g_2Q_i$ for some i. Then, according to *3.* one has $g_1g_2 = g_2g_1$ and (4.1) implies that $g_1Q_i = Q_j$ for some j, whence

$$g_1P = g_1g_2Q_i = g_2g_1Q_i = g_2Q_j \in \mathrm{Supp}\,\pi_2^*D.$$

Let n_P be the order of P in π_2^*D, then

$$\begin{aligned} n_P &= |\{Q = P,\ Q \in \mathrm{Orb}_{H_2}(Q_j),\ 1 \leqslant j \leqslant h_1\}|, \\ n_{g_1P} &= |\{Q = g_1P,\ Q \in \mathrm{Orb}_{H_2}(Q_j),\ 1 \leqslant j \leqslant h_1\}|. \end{aligned}$$

Thus $n_P = n_{g_1P}$. So we proved that $g_1\pi_2^*D = \pi_2^*D$, whence

$$\pi_2^*D \in \mathrm{Jac}(C)(\mathbb{F}_q)^{H_1} \cap \mathrm{Jac}(C)(\mathbb{F}_q)^{H_2} \subseteq \mathrm{Jac}(C)(\mathbb{F}_q)^{<H_1,H_2>} = \{0\}.$$

According to Proposition 0.5.1 applied with $\ell = |\mathrm{Jac}(C)(\mathbb{F}_q)|$, it implies that $D = 0$. Whence

$$(h_1(P_1 - \infty_1), 0) = \pi_*(\pi_1^*(P_1 - \infty_1)) \in \pi_*(< \theta(S) >),$$

and according to *5.* and *6.*, one has $\gcd(h_1, |\mathrm{Jac}(C_1)(\mathbb{F}_q)|) = 1$, thus

$$(P_1 - \infty_1, 0) \in \pi_*(< \theta(S) >).$$

One proves similarly that

$$(0, P_2 - \infty_2) \in \pi_*(< \theta(S) >).$$

Let $(D_1, D_2) \in \mathrm{Jac}(C_1)(\mathbb{F}_q) \times \mathrm{Jac}(C_2)(\mathbb{F}_q)$. Since $< \theta_i(S_i) >= \mathrm{Jac}(C_i)(\mathbb{F}_q)$ there exist $\tilde{D}_1, \tilde{D}_2 \in \pi_*(< \theta(S) >)$ such that

$$(D_1, 0) = \pi_*(\tilde{D}_1) \text{ and } (0, D_2) = \pi_*(\tilde{D}_2),$$

whence

$$(D_1, D_2) = \pi_*(\tilde{D}_1 + \tilde{D}_2) \in \pi_*(< \theta(S) >).$$

One has shown that

$$\pi_*(< \theta(S) >) = \mathrm{Jac}(C_1)(\mathbb{F}_q) \times \mathrm{Jac}(C_2)(\mathbb{F}_q),$$

and *6.* implies that $< \theta(S) >= \mathrm{Jac}(C)(\mathbb{F}_q)$. □

Remark : During the course of proof of Theorem 4.2.1, one showed that

$$\mathrm{Jac}(C)(\mathbb{F}_q) \simeq \prod_{i=1}^{n} \mathrm{Jac}(C_i)(\mathbb{F}_q).$$

Let us explain how we use Theorem 4.2.1 in order to compute some ray class fields of Deligne-Lusztig curves. One gives details in the case of the Suzuki curve and we use the notations of Proposition 0.8.2.

Let $s \in \mathbb{N}$ and $q := 2q_0^2 = 2^{2s+1}$, the Suzuki curve $X_S/\mathbb{F}_q$ is a Galois cover of $\mathbb{P}^1_{\mathbb{F}_q}$ with group

$$\mathrm{Gal}(\mathbb{F}_q(X_S)/\mathbb{F}_q(x)) \simeq \mathbb{F}_q \simeq (\mathbb{Z}/2\mathbb{Z})^{2s+1}.$$

One uses the notations of Theorem 4.2.1 with $S = X_S(\mathbb{F}_q) - \{\infty\}$, $n = q-1$, $G = \mathrm{Gal}(\mathbb{F}_q(X_S)/\mathbb{F}_q(x))$ and the H_i's are the n subgroups of G of index 2. The equation of $C_i/\mathbb{F}_q$ is

$$C_i : w^2 - w = \gamma_i x^{q_0}(x^q - q),$$

for some $\gamma_i \in \mathbb{F}_q$, one has

$$\begin{aligned} \pi_i : C(\mathbb{F}_q) &\to C_i(\mathbb{F}_q) \\ (x, w) &\mapsto (x, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\gamma_i w)), \end{aligned}$$

and $S_i = C_i(\mathbb{F}_q) - \{\infty_i\}$. One checks each point of Theorem 4.2.1.

1. Every element of G is $\mathbb{F}_q$-rational and fixes ∞, so any element of G sends a finite $\mathbb{F}_q$-rational point to a finite $\mathbb{F}_q$-rational point, i.e. $H_i(S) \subseteq S$.
2. From the equation of $C_i/\mathbb{F}_q$, one has that the extension $\mathbb{F}_q(C_i)/\mathbb{F}_q(x)$ is totally split over the finite $\mathbb{F}_q$-rational points of $\mathbb{F}_q(x)$ and is totally ramified at infinity. Since the same holds for $\mathbb{F}_q(X_R)/\mathbb{F}_q(x)$, it also holds for $\mathbb{F}_q(X_R)/\mathbb{F}_q(C_i)$.
3. The group G is abelian and $H_i \subseteq G$.
4. The subgroups H_i's are maximal subgroups of G, so $< H_i, H_j >= G$ for $i \neq j$ and $\mathbb{F}_q(X_S)^G = \mathbb{F}_q(x)$ has genus 0, one concludes by using Proposition 0.5.1.
5. According to Proposition 0.8.2, one has $L(X_S, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{q_0(q-1)}$. The curve $C_i/\mathbb{F}_q$ being a quotient of $X_S/\mathbb{F}_q$, the polynomial $L(C_i, \mathbb{F}_q, t)$ divides $L(X_S, \mathbb{F}_q, t)$. Since $|H_i| = 2^{2s}$, one has $\gcd(|H_i|, \mathrm{Jac}(C_i)(\mathbb{F}_q)) = 1$.
6. Since $g(C_i) = q_0$, one has $L(C_i, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{q_0}$.

Then, according to Theorem 4.2.1 and remark after Proposition 0.7.2, one may show that the S-Hilbert class field of the Suzuki curve is trivial by showing that the S_i-Hilbert class field of C_i is trivial for every i. This might be much easier since $\mathrm{Jac}(C_i)(\mathbb{F}_q)$ is much smaller than $\mathrm{Jac}(C)(\mathbb{F}_q)$. See the next Section for an algorithm computing this S-Hilbert class field for the first values of s.

The previous paragraph about the Suzuki curve may be applied to the Hermitian curve and the Ree curve since they are G-covers of $\mathbb{P}^1_{\mathbb{F}_q}$ where G is a p-elementary abelian group, one has an analogous description of the C_i's, the π_i's and the S_i's. Moreover the L-polynomials of these curves are known so one proves that the six assumptions of Theorem 4.2.1 are satisfied in the same way as above.

We now give a criterion to answer question **(Q1)**.

Proposition 4.2.1. *With the notations of Proposition 0.8.3, let* $L := \mathbb{F}_q(x, y_1)$ *and let* S' *be the set of finite* $\mathbb{F}_q$*-rational places of* L *. If* $L^0_{S'} = L$ *then* $\mathbb{F}_q(X_R)$ *is a* S'*-ray class field over* L*. More precisely, let* $m = q + 3q_0 + 2$*, then*

$$\mathbb{F}_q(X_R) = \mathbb{F}_q(x, y_1, y_2) = L^{m\infty}_{S'}.$$

Proof. We use the notations of Proposition 0.8.3 and one starts by giving some properties of $\mathbb{F}_q(X_R)/L$ and $L/\mathbb{F}_q(x)$. The extension $L/\mathbb{F}_q(x)$ is totally ramified above ∞ and unramified outside ∞. Since $\mathrm{Gal}(L/\mathbb{F}_q(x)) \simeq \mathbb{F}_q$, Theorem 2.1 of [GS91] yields

$$g(L) = \sum_{i=1}^{n} g(L_i),$$

where $n = (q-1)/2$ and the L_i's are the subfields of L such that $[L_i : \mathbb{F}_q(x)] = 3$. An equation defining $L_i/\mathbb{F}_q(x)$ is

$$y_i^3 - y_i = \gamma_i x^{q_0}(x^q - x), \tag{4.2}$$

where $\gamma_i \in \mathbb{F}_q$, so one reads the conductor of $L_i/\mathbb{F}_q(x)$ on the equation (4.2), and the Riemann-Hurwitz genus formula gives $g(L_i)$, whence

$$g(L) = \frac{3}{2} q_0(q-1).$$

From the equations of $X_R/\mathbb{F}_q$ one sees that every place of S' totally splits in $\mathbb{F}_q(X_R)$ and one shows that the conductor of $\mathbb{F}_q(X_R)/L$ equals m by means of [Ser79] III, §4 Proposition 8 and IV §2 Proposition 4. Thus, according to the definition of $L^{m\infty}_{S'}$, one has

$$\mathbb{F}_q(X_R) = L(y_2) \subseteq L^{m\infty}_{S'}.$$

Since $[\mathbb{F}_q(X_R) : L] = q$, in order to prove the Proposition one shows that $[L^{m\infty}_{S'} : L] = q$. According to Proposition 0.7.1 and [Aue99] II.6, one has

$$[L^{m\infty}_{S'} : L] = [L^{m\infty}_{S'} : L^{\infty}_{S'}][L^{\infty}_{S'} : L^0_{S'}][L^0_{S'} : L] = [L^{m\infty}_{S'} : L^{\infty}_{S'}] \in 3^{\mathbb{N}}.$$

Let $r \in \mathbb{N}$ such that $[L^{m\infty}_{S'} : L] = q3^r$. The Riemann-Hurwitz genus formula yields

$$2(g(L^{\infty}_{S'}) - 1) = 2(g(L) - 1)q3^r + \deg \mathcal{D}_{L^{\infty}_{S'}/L},$$

where $\mathcal{D}_{L^{\infty}_{S'}/L}$ is the different divisor of the function field extension $L^{\infty}_{S'}/L$. Denote by $\mathfrak{p}_\infty$ the place of L corresponding to the point ∞, the Discriminant-Conductor formula (see [Ser79] VI §4 Corollary 2) reads

$$\mathfrak{d}_{L^{\infty}_{S'}/L} = \prod_{\chi} \mathfrak{p}_\infty^{f(\chi, \mathfrak{p}_\infty)},$$

where $\mathfrak{d}_{L^{\infty}_{S'}/L}$ is the discriminant divisor of the function field extension $L^{\infty}_{S'}/L$, the product being taken over the non-trivial irreducible characters of G and $f(\chi, \mathfrak{p}_\infty)$ denotes the Artin conductor of χ at ∞. For every such character one has

$$f(\chi, \mathfrak{p}_\infty) \leqslant m,$$

see [Ser79] VI §4. Since there are $q3^r - 1$ such characters of G and $L^{\infty}_{S'}/L$ is totally ramified

$$2(g(L^{\infty}_{S'}) - 1) \leqslant 2(g(L) - 1)q3^r + (q3^r - 1)m,$$

thus

$$2g(L^{\infty}_{S'}) \leqslant (q^2 3^r - 1)(3q_0 + 1) - q + 1.$$

Since $L^{\infty}_{S'}$ has $1 + q^3 3^r$ $\mathbb{F}_q$-rational points, the Oesterlé bound for the number of $\mathbb{F}_q$-rational points of $L^{\infty}_{S'}$ with a suitable trigonometric polynomial yields a contradiction with $r \geqslant 1$ (see [Lau99b] Theorem 3 for the details of this last computation). □

4.3 ALGORITHMS

The previous Section shows how one may compute Hilbert class fields by splitting the problem into smaller ones. One gives two approaches that were used in order to compute Hilbert class fields of p-abelian elementary covers of $\mathbb{P}^1_{\mathbb{F}_q}$ using Theorem 4.2.1.

Let $s \in \mathbb{N}$, $q := p^s$, $G \simeq (\mathbb{F}_q, +)$ and $C/\mathbb{F}_q$ be the G-cover of $\mathbb{P}^1_{\mathbb{F}_q}$ birationally given by

$$w^q - w = f(x) \in \mathbb{F}_q[x],$$

Let $n := \frac{q-1}{p-1}$, then the n subgroups of index p of G give rise to p-cyclic covers $C_i/\mathbb{F}_q$ of $\mathbb{P}^1_{\mathbb{F}_q}$ birationally given by

$$C_i : w^p - w = \gamma_i f(x),$$

with $\gamma_i \in \mathbb{F}_q$ and the morphism $\pi_i : C \to C_i$ satisfies

$$\begin{aligned} \pi_i : C(\mathbb{F}_q) &\to C_i(\mathbb{F}_q) \\ (x, w) &\mapsto (x, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\gamma_i w)). \end{aligned}$$

From the explicit description of the π_i's and the C_i's one may describe the S_i's. Assume that the hypotheses of Theorem 4.2.1 are satisfied, i.e. one may check that $< \theta(S) >= \mathrm{Jac}(C)(\mathbb{F}_q)$ by checking that $< \theta_i(S_i) >= \mathrm{Jac}(C_i)(\mathbb{F}_q)$ for all i, then one has the following naive algorithm

Algorithm 1: Class group based method

Data: p, s, f, S
Result: Returns **true** if the S-Hilbert class field of $\mathbb{F}_q(C)$ is $\mathbb{F}_q(C)$
for *each quotient* C_i *of* C *as above* **do**
  Compute the jacobian $J_i(\mathbb{F}_q)$ of $C_i/\mathbb{F}_q$ and the set S_i;
  Compute the subgroup J_{S_i} of $J_i(\mathbb{F}_q)$ generated by $\theta_i(S_i)$;
end
if $|J_{S_i}| = |J_i(\mathbb{F}_q)|$ *for all* i **then**
  Return **true**;
end

The main problem with this method is that one has to compute the J_i's. Actually we are interested in computing ray class fields of curves having many $\mathbb{F}_q$-rational points, so the J_i's have a large cardinality, that is why this method is not adapted to our purpose. For example, the case $s = 2$ for the Ree curve gives rise to $n = 121$ curves defined by

$$w^3 - w = \gamma(x^{252} - x^{10}),\ \gamma \in \mathbb{F}_q,$$

having genus 27 with class number $\simeq 5.10^{21}$. Nonetheless, it is a work in progress, when $C_i/\mathbb{F}_q$ is given by

$$C_i : w^p - w = xR(x) \in \mathbb{F}_q[x],$$

where $R(x) = \sum_{i=0}^{d} a_i x^{p^i}$ is an additive polynomial, to split up to isogeny $\mathrm{Jac}(C_i)(\mathbb{F}_q)$ as the product of supersingular elliptic curves, so one has only to compute small class groups, see Section 4.5 for more details.

We expose a second method based on the computation of Weil pairings, one describes this method for the Suzuki curve for the sake of ease of comprehension. Recall that $g(C_i) = q_0$ and

$$L(C_i, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{q_0}, \tag{4.3}$$

so, $|\mathrm{Jac}(C_i)(\mathbb{F}_q)| = n^{q_0}$ and one wants to know if $< \theta_i(S_i) >= \mathrm{Jac}(C_i)(\mathbb{F}_q)$. Basically, one may hope that the matrix of the Weil pairings of q_0 points of $< \theta_i(S_i) >$ has rank q_0, proving $< \theta_i(S_i) >= \mathrm{Jac}(C_i)(\mathbb{F}_q)$. Unfortunatly in the examples we considered (i.e. $s \leqslant 5$) the points of $\theta_i(S_i)$ are contained in a totally isotropic subspace for the Weil pairing.

According to equation (4.3), not all the n-torsion of $\mathrm{Jac}(C_i)$ will be $\mathbb{F}_q$-rational, the idea is then to pick q_0 random points in a finite extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ and to try to construct a basis $\mathcal{B}$ of the free $\mathbb{Z}/n\mathbb{Z}$-module $\mathrm{Jac}(C_i)(\mathbb{F}_q^{alg})[n]$ from these random points and q_0 points of $\theta_i(S_i)$. If the matrix of the Weil pairings of the elements of $\mathcal{B}$ has rank $2q_0$, then $\mathcal{B}$ generates $\mathrm{Jac}(C_i)(\mathbb{F}_q^{alg})[n]$, thereby $\theta_i(S_i)$ will generate the whole $\mathrm{Jac}(C_i)(\mathbb{F}_q)$.

Algorithm 2: Weil pairing based method.

```
Data: p, s, f, S
Result: The S-Hilbert class field of F_q(C) is F_q(C) if the program terminates
Put n = 1 + 2q_0 + q ;
for each quotient C_i of C as above do
    for each prime factor ℓ of n put n_ℓ = ν_ℓ(n) do
        Put J_i = Jac(C_i), B = ∅ and Rk = 0;
        while Rk ⩽ 2q_0 do
            while Rk ≠ |B| + 2 do
                Take random points P ∈ θ_i(S_i) and Q ∈ J_i(F_{q^k})[ℓ^{n_ℓ}];
                Compute the rank Rk of the matrix of the Weil pairings of
                B ∪ {n/ℓ^{n_ℓ} P, Q};
            end
            Put B = B ∪ {n/ℓ^{n_ℓ} P, Q};
        end
    end
end
```

Remarks :

1. One chooses k to be the smallest integer such that $q^k \equiv 1 \bmod n$.
2. Note that, according to remark after Theorem 4.2.1, one restricts ourselves to the ℓ^{n_ℓ}-torsion instead of studying the $\ell^{q_0 n_\ell}$-torsion.

4.4 TABLES

The algorithms have been implemented using Magma. Since the Weil pairing is only available for elliptic and hyperelliptic curves in Magma, it was not immediatly possible to implement the Weil pairing based algorithm for the Hermitian curve when $p \geqslant 3$, neither for the Ree curve. One only gives here some examples for $p = 2$ in the Hermitian case but one may produce tables for larger p. The table for the first stage of the Ree curve (resp. the Ree curve) only gives the cases $s \leqslant 1$ since for $s = 2$ one has to compute class groups of order $\simeq 5.10^{21}$ (resp. $\simeq 7.10^{7898}$) when using the class group based algorithm.

Recall that for a non-empty set of places S of a function field $K/\mathbb{F}_q$, one denotes by $Cl(\mathcal{O}_S)$ the S-class group and one has

$$h_S = |Cl(\mathcal{O}_S)| = \mathrm{Gal}(K_S^0/K).$$

For $K/\mathbb{F}_q$ a function field of one variable, let $g(K)$ be its genus and $N_q(K)$ be the number of $\mathbb{F}_q$-rational points of the corresponding smooth, projective, irreducible curve. We specify the algorithm we used in the last column, CG stands for the Class group based algorithm and WP for the Weil pairing based algorithm.

We use the notations of Proposition 0.8.2, we denote by S' the set of finite $\mathbb{F}_q$-rational points of X_S.

Suzuki curve					
s	q	$g(K)$	$N_q(K)$	$h_{S'}$	Note
0	2	1	5	1	
1	8	14	65	1	CG, WP
2	32	124	1025	1	WP
3	128	1016	16385	1	WP
4	512	8176	262145	1	WP

We use the notations of Proposition 0.8.3, we denote by S' the set of finite $\mathbb{F}_q$-rational places of $\mathbb{F}_q(x, y_1)$. Recall that according to Proposition 4.2.1, if $h_{S'} = 1$ then $\mathbb{F}_q(X_R)$ is a ray class field over $\mathbb{F}_q(x, y_1)$.

First stage of the Ree curve					
s	q	$g(K)$	$N_q(K)$	$h_{S'}$	Note
0	3	3	10	1	CG
1	27	117	730	1	CG

One keeps the same notations, except that S' is the set of finite $\mathbb{F}_q$-rational places of $\mathbb{F}_q(X_R)$.

Ree curve					
s	q	g(K)	$N_q(K)$	$h_{S'}$	Note
0	3	15	28	1	CG
1	27	3627	19684	1	CG

Put $p := 2$, we use the notations of Proposition 0.8.1, we denote by S' the set of finite $\mathbb{F}_{q^2}$-rational places of $\mathbb{F}_{q^2}(X_H)$.

Hermitian curve, $p = 2$					
s	q^2	g(K)	$N_{q^2}(K)$	$h_{S'}$	Note
1	4	1	9	1	GG
2	16	6	65	1	CG
3	64	28	513	1	CG,WP
4	256	120	4097	1	CG,WP
5	1024	496	32769	1	WP

4.5 FURTHER DEVELOPMENTS

In this Section, one describes further material in order to explain how one may improve the algorithms presented in Section 4.3.

In order to produce a more efficient algorithm for computing ray class fields of the Deligne-Lusztig curves one would like to continue the process of splitting up to isogeny explicitly over $\mathbb{F}_q$ the jacobians of the curves A_R birationally given by $w^p - w = xR(x)$ where $R(x) = \sum_{i=0}^{n} a_i x^{p^i} \in \mathbb{F}_q[x]$. First of all, recall that Proposition 0.9.1 implies that $\mathrm{Jac}(A_R)$ is isogenous over $\mathbb{F}_q^{alg}$ to a product of supersingular elliptic curves.

In the case of the Suzuki curve $X_S/\mathbb{F}_q$, one has an algorithm to describe the morphisms that split $\mathrm{Jac}(X_S)$ up to isogeny in a product of elliptic curves over $\mathbb{F}_q$. This is done by studying the automorphism group of these curves. This follows from [dGdV92].

Denote by $G_R(\mathbb{F}_q)$ the p-Sylow subgroup of the group of $\mathbb{F}_q$-rational automorphisms of $A_R/\mathbb{F}_q$ fixing ∞ and recall (see Proposition 0.6.3) that $G_R(\mathbb{F}_q)$ is a subgroup of an extra-special p-group with center generated by the Artin-Schreier morphism

$$\begin{aligned} \rho : A_R &\to A_R \\ (x, w) &\mapsto (x, w + 1). \end{aligned}$$

Proposition 4.5.1 and Lemma 4.5.1 may be found in [dGdV92] §5 and §9.

Proposition 4.5.1. *Assume that* $p = 2$ *and there exists* $t_a \in G_R(\mathbb{F}_q) - < \rho >$, *then the curve* $A_R/ < t_a >$ *is birationnaly given by*

$$w^p - w = x\tilde{R}(x),\ \tilde{R}(x) = \sum_{i=0}^{n-1} a_i x^{p^i} \in \mathbb{F}_q[x].$$

One may compute explicitely $\tilde{R}(x)$ *from* $R(x)$ *and the equation of* t_a.

Let

$$W_R = \{x \in \mathbb{F}_q, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(y) + yR(x)) = 0 \ \forall y \in \mathbb{F}_q\},$$
$$V_R = \{x \in W_R, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(x)) = 0\}.$$

Then $\dim V_R = \dim W_R - 1$ or $V_R = W_R$, depending on whether the linear map

$$\varphi : W_R \to \mathbb{F}_p$$
$$x \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(x)),$$

is onto or not. Put $d_R := \dim W_R$.

Lemma 4.5.1. *Assume that* $p = 2$.

1. *One has* $|G_R(\mathbb{F}_q)| = 2^{d_R}$ *or* $|G_R(\mathbb{F}_q)| = 2^{d_R+1}$, *depending on whether the map* φ *is onto or not.*
2. *One has either* $|A_R(\mathbb{F}_q)| = q + 1$ *or* $|A_R(\mathbb{F}_q)| = 1 + q \pm \sqrt{q2^d}$.
3. *If* $\dim V_R = \dim W_R - 1$, *then* $|A_R(\mathbb{F}_q)| = q + 1$.

From now on, one focus on the case of the Suzuki curve. One assumes that $A_R/\mathbb{F}_q$ is a quotient of

$$C_i : w^2 - w = \gamma_i x^{q_0}(x^q - x),$$

where $q_0 = 2^s$, $q = 2q_0^2$ and $\gamma_i \in \mathbb{F}_q^\times$. Let us explain how we split $\mathrm{Jac}(A_R)$ up to isogeny as a product of supersingular elliptic curves. One knows that

$$L(C_i, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{q_0},$$

whence

$$L(A_R, \mathbb{F}_q, t) = (1 + 2q_0 t + qt^2)^{g(A_R)}.$$

and according to Lemma 4.5.1 one knows that $|G_R(\mathbb{F}_q)| > 2$. In particular, there exists $t_a \in G_R(\mathbb{F}_q) - < \rho >$. One considers the subgroup of $G_R(\mathbb{F}_q)$

$$H := < t_a, \rho > \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

it has 3 subgroups of order 2, namely

$$H_1 = < t_a >,\ H_2 = < t_a \rho > \text{ and } H_3 = < \rho > .$$

If $g(A_R) > 1$, one may write an equation for the quotient of A_R by H_1 and H_2 as an $A_{\tilde{R}}$ and $\mathrm{Jac}(A_R)$ is isogenous to the jacobians of these quotients. One continues this process until one gets elliptic curves. In particular, assumptions *2* to *6* of Theorem 4.2.1 are satisfied in this setting. So in order to compute S-ray class fields of the Suzuki curve, one has to get some insight on the behavior of S under the succesive quotients.

Remarks :

1. If one does not put conditions on the set S, one may already compute S-ray class fields of the Suzuki curve by taking S sufficiently large so that assumption *1* of Theorem 4.2.1 holds.

2. Finding an explicit $t_a \in G_R(\mathbb{F}_q)$ amounts to find a root of a polynomial in $\mathbb{F}_q[t]$ and to reduce an explicit polynomial modulo $\wp\mathbb{F}_q[t]$. Since Proposition 4.5.1 is also effective, one may explicit every quotient, curve and subset arising in Theorem 4.2.1.

When dealing with the other Deligne-Lusztig curves, some new difficulties appear. Indeed, one may first prove an analogous for Proposition 4.5.1 and Lemma 4.5.1 when $p > 2$. Moreover, if the L-polynomial of the initial curve has more than one irreducible factor, then it is not easy from a theoretical point of view to count $\mathbb{F}_q$-rational points on the quotient curve.

Remark : The analogous for Proposition 4.5.1 when $p > 2$ announced in [dGdV92] §13 Proposition (13.5) is not correct. Here is a counter-example. The supersingular curve $C/\mathbb{F}_3$ defined by $w^3 - w = x(x^3 - x)$ has genus 3 and the morphism $x \mapsto x + 1$ of $\mathbb{P}^1_{\mathbb{F}_3}$ has an $\mathbb{F}_3$-rational prolongation t_1 to C. The group $H :=< \rho, t_1 >$ has 4 subgroups of order 3 giving rise to an isogeny over $\mathbb{F}_3$

$$\mathrm{Jac}(C) \sim E_1 \times E_2 \times E_3,$$

where the E_i's are supersingular elliptic curves defined over $\mathbb{F}_3$. Since

$$L(C, \mathbb{F}_3, t) = (1 + 3t^2)(1 + 3t + 3t^2)^2,$$

one has for instance $L(E_1, \mathbb{F}_3, t) = 1 + 3t + 3t^2$. Thus, the equation of $E_1/\mathbb{F}_3$ is not of the form $w^3 - w = xS(x)$ with $S(x) \in \mathbb{F}_3[x]$ an additive polynomial.

The general case of Proposition 4.5.1 is somehow tedious but is not a big deal. Counting points on the successive quotients might be much more tricky. Namely, by means of Proposition 0.5.1, since the elements of the H_i's are quite simple, one has some control on the action of Frobenius on the quotient curve. It is a work in progress to understand the behavior of the factors of the L-polynomial of the Ree curve when taking quotients by groups of translations.

Remark : In order to give extended tables in the case $p \geqslant 3$ it would be desirable to have an efficient way of computing Weil pairings for curves birationally given by $w^p - w = xR(x)$ where $R(x)$ is an additive polynomial.

Example : One shows how these improvements of the algorithm may be used. One considers the Suzuki curve $X_S/\mathbb{F}_q$ with $q_0 = 2$ and $q = 8$ given by

$$X_S : w^8 - w = x^2(x^8 - x),$$

it has 7 quotients $C_i/\mathbb{F}_q$, corresponding to the index 2 subgroups of $\mathbb{F}_q$, given by

$$C_i : w^2 - w = \gamma_i x^2(x^8 - x),$$

for some $\gamma_i \in \mathbb{F}_q$. Let $S := X_S(\mathbb{F}_q) - \{\infty\}$, $\pi_i : X_S \to C_i$, $\infty_i := \pi_i(\infty)$ and $S_i := \pi_i(S)$. Then, $S_i = C_i(\mathbb{F}_q) - \{\infty_i\}$. According to Section 4.2, if the S_i-Hilbert class field of $C_i/\mathbb{F}_q$ is trivial for each i, so is the S-Hilbert class field of $X_S/\mathbb{F}_q$.

Fix some i_0, an easy computation shows that, for any $a \in \mathbb{F}_q^\times$, the translation t_a by a on $\mathbb{P}^1_{\mathbb{F}_q}$ has a prolongation, still denoted by t_a, has an automorphism of $C_{i_0}/\mathbb{F}_q$. The group $< t_a, \rho >$ has 3 subgroups of index 2 denoted by H_1, H_2 and H_3. Denote by

D_j the quotients of C_{i_0} by the H_j's. The D_j's are respectively two elliptic curves with 13 $\mathbb{F}_q$-rational points and a projective line. Since C_{i_0} has genus 2, every assumption of Theorem 4.2.1 is satisfied. The image of S_{i_0} under each morphism $C_{i_0} \to D_j$ generates $\mathrm{Jac}(D_j)(\mathbb{F}_q)$, thus the S_{i_0}-Hilbert class field of $C_{i_0}/\mathbb{F}_q$ is trivial.

Example : The Suzuki curve $X_S/\mathbb{F}_q$ with $q_0 = 4$ and $q = 32$ is given by

$$X_S : w^{32} - w = x^4(x^{32} - x),$$

and has genus 124. By weakening condition *1* of Theorem 4.2.1 and splitting $\mathrm{Jac}(X_S)$ up to isogeny in a product of supersingular elliptic curves, one shows that $X_S/\mathbb{F}_q$ has a trivial S-Hilbert class field where $S := X_S(\mathbb{F}_q) - \{\infty\}$.

BIBLIOGRAPHY

[Abr95] V. A. Abrashkin. A ramification filtration of the Galois group of a local field. In *Proceedings of the St. Petersburg Mathematical Society, Vol. III*, volume 166 of *Amer. Math. Soc. Transl. Ser. 2*, pages 35–100, Providence, RI, 1995. Amer. Math. Soc. (Cited on page 54.)

[Aue99] R. Auer. *Ray Class Fields of Global Function Fields with Many Rational Places*. PhD thesis, Lindau/ Bodensee, 1999. (Cited on pages 13, 14, 15, 61, 62, and 65.)

[Aue00] Roland Auer. Ray class fields of global function fields with many rational places. *Acta Arith.*, 95(2):97–122, 2000. (Cited on pages 54, 55, 61, and 62.)

[BK05] A. Brumer and K. Kramer. The conductor of an abelian variety. *Compositio mathematica*, 2(92), 2005. (Cited on pages 18 and 39.)

[Bla12] R. Blache. Valuation of exponential sums and the generic first slope for Artin–Schreier curves. *Journal of Number Theory*, 10(132), 2012. (Cited on page 15.)

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. (Cited on page 3.)

[Chr13] P. Chrétien. Lifting artin-schreier covers with maximal wild monodromy. *Manuscripta Math.*, 2013. (Cited on page xiii.)

[CM13] P. Chrétien and M. Matignon. Maximal wild monodromy in unequal characteristic. *J. Number Theory*, 133(4):1389–1408, 2013. (Cited on pages xi and 38.)

[dGdV92] G. Van der Geer and M. Van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Mathematica*, 84, 1992. (Cited on pages 69 and 71.)

[DK73] P. Deligne and N. Katz. *Groupes de monodromie en géométrie algébrique. II*. Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz. (Cited on page 3.)

[DM69] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, 36:75–109, 1969. (Cited on page 4.)

[FD12] C. Fieker and V. Ducet. Computing equations of curves with many points. *Proceedings of the ANTS X conference*, 2012. (Cited on page 62.)

[GK10] M. Giulietti and G. Korchmáros. Algebraic curves with a large non-tame automorphism group fixing no point. *Trans. Amer. Math. Soc.*, 362(11):5983–6001, 2010. (Cited on page 59.)

[GMN11] J. Guardia, J. Montes, and E. Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *Journal de théorie des nombres de Bordeaux*, 2, 2011. (Cited on page 51.)

[Gor80] D. Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980. (Cited on page 4.)

[Gro72] A. Grothendieck. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par P. Deligne et N. Katz. (Cited on page 3.)

[GS91] A. Garcia and H. Stichtenoth. Elementary abelian p-extensions of algebraic function fields. *Manuscripta Mathematica*, 72, 1991. (Cited on pages 6, 16, and 65.)

[Gur03] R. Guralnick. Monodromy groups of coverings of curves. In *Galois groups and fundamental groups*, volume 41. MSRI Publications, 2003. (Cited on page 8.)

[Han92] Johan P. Hansen. Deligne-Lusztig varieties and group codes. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.* Springer, Berlin, 1992. (Cited on pages 14 and 61.)

[HP93] J.P Hansen and J.P. Pedersen. Automorphism groups of Ree type, Deligne-Lusztig curves and function fields. *J. reine angew. Math.*, 440, 1993. (Cited on pages 14 and 61.)

[Hup67] B. Huppert. Endliche gruppen i. *Grundlehren der Mathematischen Wissenschaften*, 134, 1967. (Cited on page 4.)

[Hyo87] O. Hyodo. Wild ramification in imperfect residue field case. *Advanced Studies in Pure Mathematics*, 12, 1987. (Cited on page 5.)

[Kid03] M. Kida. Variation of the reduction type of elliptic curves under small base change with wild ramification. *Central European science journals*, 4, 2003. (Cited on page 33.)

[KR89] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284, 1989. (Cited on page 16.)

[Kra90] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Mathematica*, 69, 1990. (Cited on page 2.)

[Lau96] Kristin Lauter. Ray class field constructions of curves over finite fields with many rational points. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1996. (Cited on page 62.)

[Lau99a] K. Lauter. A formula for constructing curves over finite fields with many rational points. *J. Number Theory*, 74, 1999. (Cited on page 61.)

[Lau99b] K. Lauter. Deligne-Lusztig curves as ray class fields. *Manuscripta Mathematica*, 98, 1999. (Cited on pages 14, 61, and 66.)

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002. (Cited on pages 1, 3, 8, 17, 20, 23, 29, 37, 40, 44, and 63.)

[LM05] C. Lehr and M. Matignon. Automorphism groups for p-cyclic covers of the affine line. *Compositio Mathematica*, 5(141), 2005. (Cited on pages xiii, xiv, 11, 12, 18, 37, 38, 45, and 53.)

[LM06] C. Lehr and M. Matignon. Wild monodromy and automorphisms of curves. *Duke Math. Journal*, 5(141), 2006. (Cited on pages 17 and 19.)

[LO03] K.-Z. Li and F. Oort. *Moduli of Supersingular Abelian Varieties*, volume 1680. Lecture Notes in Mathematics, 2003. (Cited on page 15.)

[LRS93] P. Lockhart, M.I. Rosen, and J. Silverman. An upper bound for the conductor of an abelian variety. *Journal of algebraic geometry*, 2, 1993. (Cited on pages 11, 18, 39, and 50.)

[Lus77] G. Lusztig. Coxeter orbits and eigenspaces of Frobenius. *Invent. Math.*, 38, 1977. (Cited on page 61.)

[MR08] M. Matignon and M. Rocher. Smooth curves having a large automorphism p-group in characteristic $p > 0$. *Algebra and Number Theory*, 2(8), 2008. (Cited on pages xiv, 11, and 53.)

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. (Cited on page 55.)

[Ogg67] A.P. Ogg. Elliptic curves and wild ramification. *American Journal of Mathematics*, 89(1), 1967. (Cited on page 8.)

[Ped92] J. P. Pedersen. A function field related to the Ree group. In H. Stichtenoth and M. A. Tsfasman, editors, *Coding Theory and Algebraic Geometry, Proceedings, Luminy 1991*. Springer, Berlin, 1992. (Cited on pages 14 and 61.)

[Ray90] M. Raynaud. p-groupes et réduction semi-stable des courbes . In Birkhäuser, editor, *The Grothendieck Festschrift, Vol. III*, 1990. (Cited on pages xii, 2, 3, and 17.)

[Roc09] M. Rocher. Large p-group actions with a p-elementary abelian derived group. *Journal of Algebra*, 321, 2009. (Cited on pages xiv, 11, and 53.)

[Rok] K. Rokaeus. New curves with many points over small finite fields. `http://arxiv.org/abs/1204.4355`. (Cited on page 62.)

[Ser67] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, 1967. (Cited on pages 8, 9, and 10.)

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae* , 15, 1972. (Cited on page 12.)

[Ser79] J.-P. Serre. *Local Fields*, volume 67. Graduate Texts in Mathematics, Springer, 1979. (Cited on pages 5, 10, 18, 25, 38, 46, 50, 51, 65, and 66.)

[Sil09] J. Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Graduate Texts in Mathematics, Springer, 2009. (Cited on page 13.)

[ST68] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88, 1968. (Cited on pages 3, 8, 9, 11, and 27.)

[Sti73] Henning Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I,II. Eine Abschätzung der Ordnung der Automorphismengruppe. *Arch. Math. (Basel)*, 24:527–544, 1973. (Cited on pages xii and xiii.)

[Suz86] M. Suzuki. *Group Theory II*, volume 248. Grundlehren der Mathematischen Wissenschaft, Springer - Verlag, 1986. (Cited on page 4.)

[Yam68] S. Yamamoto. On a property of the Hasse's function in the ramification theory. *Memoirs of the Faculty of Science, Kyushu University*, 22(4), 1968. (Cited on page 33.)