THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

Spécialité : Mathématiques

Arrêté ministériel : 25 mai 2016

Présentée par

Séverin PHILIP

Thèse dirigée par **Gaël REMOND**,DR

préparée au sein du **Laboratoire Institut Fourier**
dans **l'École Doctorale Mathématiques, Sciences et technologies de l'information, Informatique**

Réduction semi-stable des variétés abéliennes

Semi-stable reduction of abelian varieties

Thèse soutenue publiquement le **4 octobre 2021**,
devant le jury composé de :

Monsieur GAEL REMOND
DIRECTEUR DE RECHERCHE, CNRS DELEGATION ALPES, Directeur de thèse
Monsieur PASCAL AUTISSIER
PROFESSEUR DES UNIVERSITES, UNIVERSITE DE BORDEAUX, Rapporteur
Monsieur PIERRE DèBES
PROFESSEUR DES UNIVERSITES, UNIVERSITE DE LILLE, Rapporteur
Monsieur ERIC GAUDRON
PROFESSEUR DES UNIVERSITES, UNIVERSITE CLERMONT AUVERGNE, Examinateur
Monsieur SAMUEL LE FOURN
MAITRE DE CONFERENCE, UNIVERSITE GRENOBLE ALPES, Examinateur
Madame SARA CHECCOLI
MAITRE DE CONFERENCE, UNIVERSITE GRENOBLE ALPES, Examinatrice

Résumé. Dans cette thèse, on s'intéresse à la propriété de semi-stabilité des variétés abéliennes sur les corps de nombres. Plus précisément, on étudie le degré minimal d'une extension de corps nécessaire pour qu'une variété abélienne de dimension fixée sur un corps de nombres atteigne réduction semi-stable. On note d_g ce degré, qui ne dépend que de la dimension g, et on note $d(A)$ le degré minimal pour une variété abélienne A sur un corps de nombres K donnée, celui-ci ne dépend que de A. Les objets principaux de notre étude sont les groupes de monodromie finie de A, introduits par Grothendieck. Ces groupes, notés $\Phi_{A,v}$ pour les places non archimédiennes v de K, représentent l'obstruction locale à la semi-stabilité. On relie dans un premier temps le cardinal de ces groupes aux différentes places de mauvaise réduction à l'entier $d(A)$. Ceci, avec les travaux de Silverberg et Zarhin, donne que d_g divise la borne de Minkowski $M(2g)$. On poursuit par une étude du comportement géométrique de ces groupes, c'est-à-dire dans les fibres d'un schéma abélien. En considérant un schéma abélien universel fourni par Mumford, on en déduit l'existence de variétés abéliennes avec groupes de monodromie finie prescrits relativement à un corps de nombres sous quelques conditions techniques. On termine en construisant pour chaque premier impair (par torsion en cohomologie galoisienne) des variétés abéliennes avec multiplication complexe qui ont monodromie finie maximale en ce nombre premier sur un même corps de nombres (en toute dimension). On en déduit, pour tout entier naturel non nul g, l'inégalité

$$\frac{M(2g)}{2^{g-1}} \leq d_g \leq M(2g).$$

Abstract. In this thesis, we study the semi-stable property of abelian varieties over number fields. More precisely, we study the minimal degree of a field extension that is necessary for an abelian variety of fixed dimension over a number field to obtain semi-stable reduction. We denote by d_g this degree, which depends only on the dimension g, and by $d(A)$ the minimal degree for a given abelian variety A over a number field, which depends only on A. The principal objects of our study are the finite monodromy groups of A which were introduced by Grothendieck. These groups that we denote by $\Phi_{A,v}$ for non archimedean places v of K represent the local obstruction to semi-stability. We start by linking the cardinals of these groups at the places of bad reduction and the integer $d(A)$. This, with the work of Silverberg and Zarhin, gives that the Minkowski bound $M(2g)$ is divisible by d_g. We continue by studying the geometric behaviour of these groups, i.e. their behaviour in the fibers of abelian schemes. By considering a universal abelian scheme provided by Mumford we deduce the existence of abelian varieties with prescribed finite monodromy groups relative to a number field under some technical conditions. We finish by building for every odd prime (by torsion in Galois cohomology) abelian varieties with complex multiplication that have maximal finite monodromy at that prime over a same number field (in arbitrary dimension). We deduce, for any nonzero integer g, the inequality

$$\frac{M(2g)}{2^{g-1}} \leq d_g \leq M(2g).$$

À mon père,

Remerciements

Je remercie avant tout mon directeur Gaël Rémond pour m'avoir dirigé au cours de ces 3 années et m'avoir formé au métier de chercheur de la meilleure façon possible mais aussi pour m'avoir amené dans le monde merveilleux de la géométrie arithmétique et des variétés abéliennes. Ces quelques lignes ne sont qu'un modeste acompte de la reconnaissance que j'ai pour lui.

Je remercie les membres du jury Eric Gaudron, Samuel Le Fourn, Sara Checcoli et particulièrement les rapporteurs Pierre Dèbes et Pascal Autissier d'avoir accepté de lire en détail mon travail.

Merci à toute l'équipe de l'institut Fourier d'avoir créé le cadre idéal pour travailler les mathématiques aussi bien pour ma thèse que pour mes années d'études depuis la licence.

Je remercie les membres du bureau 307 : Antoine, Rodolfo et Loïs avec qui j'ai appris la géométrie algébrique et un peu de théorie des catégories.

Je tiens à remercier particulièrement Benjamin Collas pour toutes les discussions mathématiques ou non ainsi que son soutien. Merci d'avoir répondu à mon mail jeté comme une bouteille à la mer dans l'espoir d'en apprendre plus sur les champs.

Merci à Michel Brion pour ses excellents cours en géométrie algébrique ainsi que ses conseils.

Finalement je tiens à remercier mon père pour m'avoir appris la force de la volonté et du travail, ma mère pour son soutien depuis toujours et Ludivine pour m'avoir accompagné au cours de ces 3 années, dans les hauts et les bas.

Table des matières

Chapitre 1

Introduction

Les variétés abéliennes sur les corps de nombres sont des objets de nature arithmétique et géométrique. Une extension du corps de base peut modifier leur structure. Dans cette thèse, on s'intéresse au degré minimal d'une extension sur laquelle une variété abélienne sur un corps de nombres atteint réduction semi-stable. On commence par énoncer succinctement notre résultat principal (les notions de réduction et de semi-stabilité seront rappelées dans la suite).

Définition 1.0.1. Pour une variété abélienne A sur un corps de nombres K, on pose

$$d(A) = \min\{[L : K] \mid L/K \text{ finie telle que } A_L \text{ a réduction semi-stable}\}.$$

Pour un entier naturel non nul g, on note d_g le supremum des entiers $d(A)$ pour les variétés abéliennes A de dimension g sur tout corps de nombres K.

On appelle borne de Minkowski l'entier

$$M(n) = \prod_p p^{r(n,p)}$$

où $r(n,p) = \sum_{i \geq 0} \left\lfloor \frac{n}{p^i(p-1)} \right\rfloor$ pour tout entier naturel non nul n et tout nombre premier p. Cette borne est le résultat du calcul par Minkowski du ppcm des cardinaux des sous-groupes finis de $\mathrm{GL}_n(\mathbf{Q})$. Le résultat principal de cette thèse s'énonce alors comme suit.

Résultat 1. *Pour tout entier naturel non nul g, on a les inégalités*

$$\frac{M(2g)}{2^{g-1}} \leq d_g \leq M(2g)$$

et les égalités $d_1 = M(2) = 24$ et $d_2 = M(4) = 5760$.

Ce résultat s'obtiendra par une construction explicite pour chaque nombre premier $p \mid M(2g)$ faite dans le chapitre 4 ainsi que d'une forme de principe local-global pour la quantité $d(A)$ obtenue en chapitre 3. L'écart à la borne de Minkowski pour $p = 2$ est dû à notre construction utilisant la théorie de la multiplication complexe et sera expliqué dans la partie 5 du chapitre 4.

Dans le paragraphe suivant, on présente de manière élémentaire les notions de réduction et de semi-stabilité dans le cas des courbes elliptiques. On présentera ensuite plus en détail les résultats de cette thèse.

1.1 Courbes elliptiques, réduction et semi-stabilité

Une courbe elliptique sur $\mathbf{Q}$ est donnée par une équation de Weierstrass, c'est-à-dire une équation cubique

$$y^2 = x^3 + Ax + B,\ A, B \in \mathbf{Z}$$

avec un discriminant

$$\Delta = -16(4A^3 + 27B^2)$$

non nul. Par exemple l'équation

$$E\colon y^2 = x^3 + 1$$

définit une courbe elliptique sur $\mathbf{Q}$. Son discriminant Δ_E est $-16 \cdot 27$. Une équation de la même forme avec un discriminant nul donne une courbe singulière avec par exemple un point double ou une pointe. A contrario les courbes elliptiques sont donc lisses et elles sont également projectives : elles sont compactes en ajoutant un point à l'infini. Une autre caractéristique remarquable des courbes elliptiques est que l'on peut munir les points de la courbe d'une loi naturelle de groupe commutative.

L'équation de la courbe E ci-dessus est à coefficients entiers et il est habituel pour un arithméticien de s'intéresser aux réductions modulo un nombre premier de cette équation. On obtient ainsi les réductions de E que l'on note provisoirement E_p. Par définition E_p est la courbe sur le corps fini $\mathbf{F}_p$ définie par l'équation $y^2 = x^3 + 1$. Les courbes E_p sont encore des courbes algébriques, cubiques et, la réduction ayant de bonnes propriétés, le discriminant Δ_{E_p} de la courbe réduite modulo p est $\Delta_E \mod p$. On voit que si p divise Δ_E alors E_p est singulière. Ce n'est plus une courbe elliptique. Ce phénomène se produit pour E avec $p = 2$ et $p = 3$. Il s'avère que si l'on retire le point singulier, la courbe réduite $E_3 \setminus \{\text{sing}\}$ possède encore une loi de groupe. La connaissance des groupes algébriques en dimension 1

donne deux possibilités pour $E_3 \setminus \{\text{sing}\}$. Cette courbe est isomorphe soit au groupe additif soit au groupe multiplicatif. Dans le premier cas on parle de mauvaise réduction additive et dans le deuxième de mauvaise réduction multiplicative ou de réduction semi-stable en 3. Cette situation se généralise à tous les nombres premiers de mauvaise réduction d'une courbe elliptique, en particulier pour $p = 2$ pour la courbe E. Pour les nombres premiers qui ne divisent pas le discriminant, la courbe réduite est une courbe elliptique et on parle de bonne réduction en p. Toutes ces notions s'étendent sans difficulté aux équations de Weierstrass à coefficients dans un corps de nombres.

On peut de plus vérifier que l'extension des scalaires de la courbe E au corps $K = \mathbf{Q}(\sqrt[4]{3})$ a bonne réduction en la place au-dessus de 3. La subtilité cachée est que pour calculer les courbes réduites il faut d'abord obtenir une équation de Weierstrass dite minimale pour la valuation considérée. Ce sont les extensions de $\mathbf{Q}$ que l'on obtient de cette manière et particulièrement leur degré que l'on veut mieux comprendre. On peut par ailleurs se demander si la courbe E a bonne réduction en 3 sur une extension intermédiaire $\mathbf{Q} \subset L \subset K$ et si cette extension est unique. La réponse est non aux deux questions, ce qui nécessitera plus de travail.

Dans un cas de mauvaise réduction multiplicative, la réduction est inchangée par extension de corps ce qui justifie la terminologie. La réduction n'est pas bonne mais elle est devenue stable. Le comportement des deux types de réduction vis-à-vis des extensions est essentiellement différent, l'une disparaît et devient bonne ou multiplicative et l'autre reste.

Il y a une dernière particularité remarquable de la courbe E qui jouera un rôle dans notre étude. La courbe E a une structure de groupe commutatif et son anneau d'endomorphismes contient les multiplications par n que l'on note $[n]$ et donc $\mathbf{Z}$. C'est généralement là toute l'histoire. Mais ici pour E, on peut remarquer que

$$(x, y) \mapsto (jx, y)$$

laisse E invariant et que c'est en fait un endomorphisme. On le note $[j]$ car on peut vérifier que $[j]^3 = [1] = \mathrm{id}$ et on obtient $\mathrm{End}\, E = \mathbf{Z}[j]$ (en fait ce sont les endomorphismes seulement d'une extension de E à un surcorps). L'anneau des endomorphismes de E a pour rang sur $\mathbf{Z}$ deux fois la dimension de E, on parle de multiplication complexe. Il serait trop long d'expliquer en détail comment la multiplication complexe interagit avec la semi-stabilité, mais il s'avère qu'une courbe avec multiplication complexe a bonne réduction potentielle et que son obstruction à la bonne réduction est liée à ses endomorphismes. Ceci sera particulièrement utile par la suite à cause de la

construction suivante. On considère les deux courbes elliptiques

$$\begin{aligned} E_1 &: y^2 = x^3 + 3x - 2, & \Delta_{E_1} &= -2^7 \cdot 3^3; \\ E_1' &: y^2 = x^3 + 3p^2x - 2p^3, & \Delta_{E_1'} &= -2^7 \cdot 3^3 \cdot p^6 \end{aligned}$$

où $p > 3$ est un nombre premier. Comme p divise le discriminant de E_1' on sait que celle-ci a mauvaise réduction en p ce qui n'est pas le cas de E_1. Sur le corps $\mathbf{Q}(\sqrt{p})$ on peut effectuer le changement de variable

$$x' = px,\ y' = p\sqrt{p}y$$

qui donne

$$E_1' : y'^2 = x'^3 + 3p^2x' - 2p^3$$

et donc

$$\begin{aligned} E_1' : p^3y^2 &= p^3x^3 + 3p^3x - 2p^3 \\ y^2 &= x^3 + 3x - 2. \end{aligned}$$

Sur $\mathbf{Q}(\sqrt{p})$ les courbes E_1 et E_1' sont isomorphes et E_1' atteint bonne réduction en p. On dit que E_1' est une tordue de E_1. La construction générale se fait dans le cadre de la cohomologie galoisienne où le groupe des automorphismes de la courbe que l'on veut tordre intervient. C'est ici que se trouve l'intérêt de considérer des courbes avec multiplication complexe. Leur groupe d'automorphismes plus gros leur permet d'avoir des tordues plus riches.

On reprend le vocabulaire. On dit que E a bonne réduction en p si E_p est une courbe elliptique, réduction semi-stable en p si $E_p \setminus \{\text{sing}\}$ est isomorphe à $\mathbf{G}_m$ et mauvaise réduction additive si $E_p \setminus \{\text{sing}\}$ est isomorphe à $\mathbf{G}_a$. Si E a bonne réduction ou réduction semi-stable pour tous les nombres premiers on dit que E a réduction semi-stable. Comme on l'a vu sur l'exemple la mauvaise réduction additive disparaît après une extension finie. Les premiers de mauvaise réduction divisent le discriminant. Celui-ci n'ayant qu'un nombre fini de diviseurs premiers on obtient l'existence d'une extension finie sur laquelle l'extension des scalaires de E a réduction semi-stable. On peut donc définir le degré minimal $d(E)$ d'une extension sur laquelle E atteint réduction semi-stable. On cherche en fait à majorer de façon optimale $d(E)$ indépendamment de E. Il est remarquable que le supremum

$$d_1 = \sup_E d(E)$$

est fini, c'est-à-dire est un maximum. On obtiendra que $d_1 = 24$ est atteint pour la courbe

$$E^{\max} : y^2 = x^3 - 2x^2 - x.$$

Ce sont ces nombres, $d(E)$ et plus particulièrement d_1, que l'on cherche à étudier aussi bien pour les courbes elliptiques que pour leurs analogues en dimensions supérieures : les variétés abéliennes. Pour ces dernières la situation est plus compliquée. Il faut généraliser les concepts intuitifs tels que la réduction, que l'on a introduit ici grâce aux équations de Weierstrass, en dimension supérieure ce qui se fait par la géométrie algébrique.

Les références pour la réduction semi-stable des courbes elliptiques sont [Si] chapitre 7 paragraphe 5-7, [Se1] partie 5.6 et [Kr].

1.2 Motivation et objectifs

On s'intéresse maintenant aux variétés abéliennes sur un corps de nombres, notre objet d'étude. Soit A une variété abélienne sur un corps de nombres K. La notion de réduction se définit grâce à un modèle canonique de A sur le spectre de l'anneau des entiers $\mathcal{O}_K$ de K. Un modèle de A est un schéma $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ dont la fibre générique est A. Parmi ces modèles, il en existe un, appelé modèle de Néron et noté

$$\mathcal{A} \longrightarrow \operatorname{Spec} \mathcal{O}_K$$

qui est canonique au sens où il vérifie la propriété universelle suivante : pour tout schéma Y lisse sur $\operatorname{Spec} \mathcal{O}_K$, on a l'égalité

$$\operatorname{Hom}(Y, \mathcal{A}) = \operatorname{Hom}(Y_K, A).$$

La construction d'un tel modèle est difficile et fait l'objet du livre [BLR].

On note $k(\mathfrak{p})$ le corps résiduel du point $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$. Les composantes neutres des fibres de $\mathcal{A}$ aux points fermés $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ sont appelées les réductions de A et on les note $A_{k(\mathfrak{p})}$. Pour une courbe elliptique E sur $\mathbf{Q}$ et un nombre premier p on a $E_{k(p)} = E_p \setminus \{\text{sing}\}$, donnant ainsi une définition intrinsèque au groupe $E_p \setminus \{\text{sing}\}$, indépendante du choix d'une équation de Weierstrass. Les variétés $A_{k(\mathfrak{p})}$ sont des groupes algébriques connexes et le théorème de Chevalley donne une suite exacte

$$1 \longrightarrow G_{\mathfrak{p}} \longrightarrow A_{k(\mathfrak{p})} \longrightarrow B_{\mathfrak{p}} \longrightarrow 1$$

où $G_{\mathfrak{p}}$ est un groupe algébrique linéaire commutatif et $B_{\mathfrak{p}}$ une variété abélienne. On dit que A a réduction semi-stable en $\mathfrak{p}$ si $G_{\mathfrak{p}}$ est un tore ou encore si $A_{k(\mathfrak{p})}$ est une variété semi-abélienne. Cela généralise bien le cas des courbes. En effet, en dimension 1 la suite exacte de Chevalley impose $E_{k(p)} = B_p$

ou $E_{k(p)} = G_p$. Si A a réduction semi-stable en $\mathfrak{p}$ pour tout $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ fermé on dit que A a réduction semi-stable ou A est semi-stable. Le point de départ de cette thèse est le théorème fondamental dit « de réduction semi-stable » dû à Grothendieck.

Théorème 1.2.1. *(de réduction semi-stable) Soit A une variété abélienne sur un corps de nombres K. Alors il existe une extension finie L de K telle que A_L ait réduction semi-stable.*

Ce théorème découle du critère galoisien suivant basé sur la notion de module de Tate. Soient A une variété abélienne sur un corps p-adique K de dimension g et $\ell \neq p$ un nombre premier. La limite projective des groupes des points de ℓ^n-torsion $A(\overline{K})[\ell^n] \simeq (\mathbf{Z}/\ell^n\mathbf{Z})^{2g}$ de A

$$\mathrm{T}_\ell A = \varprojlim_n A[\ell^n]$$

est un $\mathbf{Z}_\ell$-module libre de rang $2g$ appelé module de Tate de A. Le groupe de Galois absolu de K agit sur les points de torsion de façon compatible ce qui définit ainsi une représentation ℓ-adique

$$\rho_{A,\ell} \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_{2g}(\mathbf{Q}_\ell).$$

Théorème 1.2.2. *Soit A une variété abélienne sur un corps p-adique K. Alors A a réduction semi-stable si et seulement si l'action de l'inertie sur le module de Tate $\mathrm{T}_\ell A$ de A est unipotente d'échelon 2 où $\ell \neq p$ est un nombre premier.*

Ces deux théorèmes sont démontrés dans [SGA7] exposé IX.

Le théorème de réduction semi-stable assure que l'entier $d(A)$ de la définition 1.0.1 est bien défini et ne dépend que de A. L'objectif de cette thèse est d'obtenir une majoration optimale de $d(A)$ qui ne dépend que de la dimension g de A. On cherche la valeur de

$$d_g = \sup_{A,\ \dim A = g} d(A)$$

où A varie parmi toutes les variétés abéliennes de dimension g sur un corps de nombres. Il est bien connu que d_g est un entier (c'est en fait un maximum) pour tout $g \in \mathbf{N} \setminus \{0\}$. On sait par exemple que A atteint réduction semi-stable sur le corps de rationalité $K(A[12])$ des points de 12-torsion de A grâce au critère galoisien (voir la proposition 4.7 de [SGA7] exposé IX). Cela conduit à la majoration

$$d_g \leq \operatorname{Card} \mathrm{GL}_{2g}(\mathbf{Z}/12\mathbf{Z})$$

ce qui donne $d_1 \leq 4608$ par exemple.

Beaucoup de résultats théoriques sur les variétés abéliennes sur un corps de nombres utilisent une extension préalable finie pour se ramener au cas semi-stable grâce au théorème de Grothendieck. On peut par exemple citer la hauteur de Faltings qui ne devient stable qu'à partir d'une extension où A a réduction semi-stable. Le degré de cette extension préalable intervient alors dans les calculs effectifs ce qui explique l'intérêt de connaître la valeur exacte de d_g.

1.3 Énoncé des résultats et panorama de la thèse

L'obtention du résultat principal (résultat 1) se fait par le biais de trois théorèmes, résultats principaux de chacun des chapitres qui composent ce manuscrit. Pour plus de détails sur les techniques et objets utilisés pour les obtenir on renvoie le lecteur aux introductions des chapitres concernés. Ces résultats nécessitent des approches et théories différentes mais tous sont reliés par l'objet central de notre étude : les groupes de monodromie finie.

Les groupes de monodromie finie d'une variété abélienne sont d'abord introduits par Serre dans [Se1] dans le cas des courbes elliptiques et ensuite par Grothendieck dans [SGA7] pour les dimensions supérieures. La définition suivante est donnée par Silverberg et Zarhin dans [SZ2].

Définition. Soit A une variété abélienne sur un corps de nombres K et v une place non archimédienne de K de caractéristique résiduelle p et $\ell \neq p$ un nombre premier. On note $\overline{v}$ une extension de v à $\overline{K}$ et $I(\overline{v}/v)$ le groupe d'inertie associé. Soit G le groupe algébrique sur $\mathbf{Q}_\ell$ défini par l'adhérence de Zariski de l'image $\rho_{A,\ell}(I(\overline{v}/v))$.

Alors le groupe de monodromie finie de A en v est le groupe des composantes G/G° noté $\Phi_{A,v}$ où G° est la composante neutre de G.

Ces groupes, qui ne dépendent pas du choix de ℓ, représentent l'obstruction à la réduction semi-stable comme on le montre dans le chapitre 2 suivant Grothendieck. Dans ce chapitre on reprend la construction de Grothendieck de $\Phi_{A,v}$ dans le but d'obtenir le premier résultat de cette thèse. Pour un corps de nombres K on note Σ_K l'ensemble des places non archimédiennes de K.

Résultat 2. *Pour une variété abélienne A sur K on a l'égalité*

$$d(A) = \operatorname*{ppcm}_{v \in \Sigma_K} \operatorname{Card} \Phi_{A,v}.$$

Cette égalité lie les groupes de monodromie finie de A et l'entier $d(A)$ et on en déduit avec le corollaire 6.3 de [SZ2] les relations de divisibilité

$$d(A) \mid M(2g) \text{ et } d_g \mid M(2g).$$

En particulier on a l'inégalité $d_g \leq M(2g)$ annoncée dans le résultat 1. Pour comparer cette borne à celle rappelée dans la partie précédente voici les premières valeurs de chacune dans un tableau.

g	$M(2g)$	$\operatorname{Card} \mathrm{GL}_{2g}(\mathbf{Z}/12\mathbf{Z})$
1	24	4608
2	5760	32053931488051200
3	2903040	1.2×10^{38}
4	1393459200	1.9×10^{68}

Par ailleurs, une étude asymptotique de $M(n)$ a été faite par Katznelson dans [Ka], on a

$$\lim_{n\to\infty} \left(\frac{M(n)}{n!}\right)^{\frac{1}{n}} \simeq 3.4109.$$

On en déduit $d_1 = 24$ du fait que le groupe de monodromie finie en 2 de la courbe $E^{\max}$ est $\mathrm{SL}_2(\mathbf{F}_3)$ (d'ordre 24) d'après le paragraphe 5.9.1 de [Se1].

Le chapitre 3 consiste en une étude du comportement géométrique des groupes de monodromie finie, c'est-à-dire dans les fibres d'un schéma abélien $A \to S$ avec S sur un corps de nombres. On construit des recouvrements analytiques de la base $S(K_v)$ du schéma abélien à partir du revêtement fini étale de la ℓ-torsion de ce schéma pour chaque place $v \in \Sigma_K$. Ces recouvrements sont tels que les groupes de monodromie finie des fibres sont constants sur les ouverts du recouvrement. Avec un résultat de type approximation faible sur l'espace des modules des variétés abéliennes principalement polarisées de dimension g et linéairement rigidifiées construit dans le chapitre 7 de [GIT] on obtient notre deuxième résultat.

Résultat 3. *Soit K un corps de nombres. Il existe une extension finie L de K et une variété abélienne A de dimension g sur L telle que*

$$d(A) = \operatorname*{ppcm}_{B/K,\ p.p.,\ \dim B=g} d(B).$$

Grâce au résultat 2 cette dernière égalité peut se réécrire

$$d(A) = \operatorname{ppcm} \operatorname{Card} \Phi_{B,v}$$

où le ppcm est pris sur tous les groupes de monodromie finie des variétés abéliennes principalement polarisées de dimension g sur K et toutes les places $v \in \Sigma_K$. En particulier dans le but de construire une variété abélienne A avec $d(A)$ maximal il suffit de construire des variétés abéliennes sur un même corps de nombres avec monodromie finie sauvage maximale en une unique place $v \in \Sigma_K$ de caractéristique résiduelle $p \mid M(2g)$ et ceci pour tous les facteurs premiers de $M(2g)$.

On met en place cette stratégie dans le chapitre 4 en utilisant la théorie des variétés abéliennes avec multiplication complexe (CM). On rappelle l'égalité

$$M(n) = \prod_p p^{r(n,p)}$$

où $r(n,p) = \sum_{i \geq 0} \left\lfloor \frac{n}{p^i(p-1)} \right\rfloor$.

Résultat 4. *Soient g un entier naturel non nul et K un corps de nombres non ramifié en 2. On note $p_1, \ldots, p_n$ les diviseurs premiers impairs de $M(2g)$. Alors il existe une extension finie L de K telle que pour chaque $i \in \{1, \ldots, n\}$ il existe une variété abélienne A_i de dimension g principalement polarisée sur L et une place v_i de L avec*

$$\operatorname{Card} \Phi_{A_i, v_i} = p_i^{r(2g, p_i)}$$

et il existe une variété abélienne principalement polarisée A de dimension g sur L et une place v de L telles que

$$\operatorname{Card} \Phi_{A,v} = 2^{r(2g,2)+1-g}.$$

Même si le résultat n'est a priori pas optimal pour la 2-partie, il l'est lorsque l'on se restreint aux variétés abéliennes sur un corps de nombres qui sont géométriquement CM. Cela est démontré en fin de chapitre 4.

Le résultat 1 se déduit du résultat 4 en appliquant le résultat 3 au corps de nombres obtenu par le résultat 4. La robustesse du résultat 4 permettrait de démontrer l'égalité $d_g = M(2g)$ si l'on savait montrer l'existence d'une variété abélienne principalement polarisée sur un corps de nombres qui vérifie $v_2(\operatorname{Card} \Phi_{A,v}) = v_2(M(2g))$ pour une place $v \in \Sigma_K$. Le cas particulier de la dimension 2 s'obtient de cette façon. La construction d'une surface abélienne S sur $\mathbf{Q}(\sqrt[9]{2})$, jacobienne d'une courbe hyperelliptique, qui vérifie $\operatorname{Card} \Phi_{S,2} = 128 = 2^{v_2(M(4))}$ est faite par Chrétien et Matignon dans la proposition 12 de [CM] (voir aussi la définition 1).

Chapitre 2

Les groupes de monodromie finie

2.1 Introduction

Dans ce chapitre, on introduit les groupes de monodromie finie $\Phi_{A,v}$ d'une variété abélienne A sur un corps de nombres K et on étudie leur relation avec l'entier $d(A)$. Cette relation se concrétise par l'égalité

$$d(A) = \operatorname*{ppcm}_{v \in \Sigma_K} \operatorname{Card} \Phi_{A,v} \tag{2.1}$$

obtenue en partie 2.3.

Pour construire les groupes de monodromie finie on étudie d'abord le cas local, c'est-à-dire que l'on ne travaille qu'avec une seule place v et un corps p-adique K_v. Dans ce contexte, on montre, suivant Grothendieck, l'existence d'une plus petite extension $(K_v^{\mathrm{nr}})_{A,s}$ de l'extension maximale non ramifiée K_v^{nr} de K_v sur laquelle A atteint réduction semi-stable. Cette extension est galoisienne et on note $\Phi_{A,v}$ son groupe de Galois. On montre ensuite que cette extension descend à K_v sans perte de degré, c'est-à-dire qu'il existe une extension L/K_v de degré $\operatorname{Card} \Phi_{A,v}$ qui a même groupe d'inertie absolu que $(K_v^{\mathrm{nr}})_{A,s}$. Le critère galoisien de réduction semi-stable assure que A atteint réduction semi-stable sur L et donc l'égalité

$$d(A_{K_v}) = \operatorname{Card} \Phi_{A,v}$$

où $d(A_{K_v})$ est défini de façon analogue à $d(A)$ mais dans le cas des corps locaux. On termine l'étude du cas local par quelques propriétés des groupes

de monodromie finie dont la relation de divisibilité

$$\operatorname{Card}\Phi_{A,v} \mid M(2g)$$

où $g = \dim A$ ainsi que leur relation à la ℓ-torsion de A.

Pour obtenir l'égalité 2.1 à partir du cas local, on commence par des résultats sur la continuité des racines des polynômes sur les corps p-adiques qui permettent, avec le lemme de Krasner, de démontrer un résultat d'approximation faible pour les corps de nombres. On en déduit grâce à l'existence d'extensions locales de degré minimal le théorème suivant, but principal du chapitre.

Théorème 2.1.1. *Soit A une variété abélienne sur un corps de nombres K. Il existe une extension L de K de degré $\operatorname{ppcm}_{v\in\Sigma_K} \operatorname{Card}\Phi_{A,v}$ telle que A ait réduction semi-stable sur L. De plus, une telle extension est de degré minimal parmi celles sur lesquelles A atteint réduction semi-stable. En particulier on obtient la divisibilité*

$$d(A) \mid M(2g).$$

La connaissance des groupes $\Phi_{A,v}$ possibles pour les courbes elliptiques avec le théorème 2.1.1 permet de conclure à la valeur de d_1.

Corollaire 2.1.2. *Soit E une courbe elliptique sur un corps de nombres K. Il existe une extension L de K de degré au plus 24 telle que E ait réduction semi-stable sur L. De plus, il existe une courbe E sur $\mathbf{Q}$ telle qu'il n'y a aucune extension de $\mathbf{Q}$ de degré strictement inférieur à 24 avec cette propriété. Autrement dit, on a*

$$d_1 = \max_{A,\ \dim A=1} d(A) = 24.$$

On termine le chapitre par une digression sur la notion de corps de stabilité pour un ensemble fini $S \subset \Sigma_K$ et un entier non nul g.

2.2 L'obstruction à la réduction semi-stable dans le cas local

On considère dans cette partie un corps p-adique K de valuation v et de corps résiduel k de caractéristique $p > 0$. On note G_K le groupe de Galois absolu de K et G_k celui de son corps résiduel. On note I_K le groupe

d'inertie de G_K et P_K le groupe d'inertie sauvage (ce dernier est le groupe de Galois absolu de l'extension maximale modérément ramifiée de K). On a $G_K/I_K = \mathrm{Gal}(\overline{k}/k) = G_k$. On note de plus K^{nr} l'extension maximale non ramifiée de K et K^{mr} l'extension maximale modérément ramifiée sur K^{nr}. On rappelle que l'on a des isomorphismes canoniques

$$G_k \simeq \widehat{\mathbf{Z}} \simeq \mathrm{Gal}(K^{\mathrm{nr}}/K)$$

et le résultat suivant.

Proposition 2.2.1. *Soit n un entier naturel non nul premier à p. Il existe une unique extension de degré n de K^{nr}. De plus cette extension est galoisienne de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$.*

Pour plus de détails sur les corps complets voir l'annexe de [FO].

Dans cette partie, on introduit dans un premier temps les notations et résultats nécessaires à la définition du groupe de monodromie finie $\Phi_{A,v}$ d'une variété abélienne A sur K. On montre ensuite l'égalité $d(A) = \mathrm{Card}\,\Phi_{A,v}$ ainsi que des propriétés du groupe $\Phi_{A,v}$.

2.2.1 Le théorème de réduction semi-stable

On considère $\rho_{A,\ell}\colon G_K \to \mathrm{GL}_{2g}(\mathbf{Q}_\ell)$ la représentation ℓ-adique obtenue par l'action de G_K sur le module de Tate $\mathrm{T}_\ell A$ de A pour un nombre premier $\ell \neq p$. Le but de ce paragraphe est de démontrer que l'image de $\rho_{A,\ell}$ est formée de matrices quasi-unipotentes et seulement unipotentes après une extension finie du corps de base. Ce résultat est bien connu mais la démonstration que l'on en fait ici, suivant [FO], introduit des objets utiles à la suite de cette partie.

On commence par définir un nouveau sous-groupe de I_K dont l'image par $\rho_{A,\ell}$ sera finie. On note $\mathbf{Z}_\ell(1)$ le module de Tate du groupe multiplicatif, c'est-à-dire $\mathbf{Z}_\ell(1) = \varprojlim_{n\in\mathbf{N}} \mu_{\ell^n}$ où μ_{ℓ^n} est le groupe des racines ℓ^n-èmes de l'unité. C'est un $\mathbf{Z}_\ell$-module libre de rang 1 naturellement muni d'une action de G_K par le caractère cyclotomique. Ce dernier est défini comme suit. On considère

$$\begin{array}{rccc} \chi^{(n)}\colon & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^\times \\ & \sigma & \longmapsto & \chi^{(n)}(\sigma) \end{array}$$

où, si ζ_n est une racine primitive n-ème de l'unité, $\chi^{(n)}(\sigma)$ est défini par $\sigma(\zeta_n) = \zeta_n^{\chi^{(n)}(\sigma)}$. Cela définit un système compatible de morphismes continus

d'où l'existence du caractère cyclotomique

$$\begin{array}{rccc} \chi\colon & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \widehat{\mathbf{Z}}^\times \\ & \sigma & \longmapsto & (\chi^{(n)}(\sigma)). \end{array}$$

Par projection sur le ℓ-ème facteur de $\widehat{\mathbf{Z}}^\times$ on obtient le morphisme $\chi_\ell\colon G_K \to \mathbf{Z}_\ell^\times = \mathrm{Aut}_{\mathbf{Z}_\ell} \mathbf{Z}_\ell(1)$ de l'action de G_K sur $\mathbf{Z}_\ell(1)$. On a un isomorphisme canonique

$$I_K/P_K \simeq \prod_{\ell \neq p \text{ premier}} \mathbf{Z}_\ell(1).$$

Soit $P_{K,\ell}$ le sous-groupe de I_K image réciproque de $\prod_{\ell' \neq \ell, p \text{ premier}} \mathbf{Z}_{\ell'}(1)$. On note de plus $G_{K,\ell}$ le quotient $G_K/P_{K,\ell}$. On a les suites exactes

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow G_k \longrightarrow 1$$

$$1 \longrightarrow \mathbf{Z}_\ell(1) \longrightarrow G_{K,\ell} \longrightarrow G_k \longrightarrow 1.$$

On renvoie au livre [W] chapitre 1 et 2 pour les résultats sur les groupes profinis et entiers de Steinitz (ou entiers surnaturels).

Par définition de $P_{K,\ell}$ on a un isomorphisme

$$P_{K,\ell}/P_K \simeq \prod_{\ell' \neq \ell, p} \mathbf{Z}_{\ell'}(1)$$

et celui-ci montre que l'ordre du quotient est $\prod_{\ell' \neq \ell, p} \ell'^\infty$. Par le théorème de Lagrange pour les groupes profinis on a

$$[P_{K,\ell} : 1] = [P_{K,\ell} : P_K][P_K : 1].$$

On en déduit que l'ordre du groupe $P_{K,\ell}$ est $\prod_{\ell' \neq \ell} \ell'^\infty$.

On peut par ailleurs vérifier que l'action par conjugaison de $G_{K,\ell}$ sur $I_K/P_{K,\ell} \simeq \mathbf{Z}_\ell(1)$ coïncide avec l'action naturelle.

La proposition suivante donne une caractérisation par le caractère cyclotomique des corps vérifiant la propriété

(*) Aucune extension finie de K ne contient toutes les racines de l'unité d'ordre une puissance de ℓ.

Cette condition est automatiquement vérifiée si K est un corps p-adique.

Proposition 2.2.2. *Aucune extension finie de K ne contient toutes les racines de l'unité d'ordre une puissance de ℓ si et seulement si* $\operatorname{Im}\chi_\ell$ *est un sous-groupe ouvert de* $\mathbf{Z}_\ell^\times$.

Démonstration. Tout d'abord, s'il existe une extension L/K finie qui contient toutes les racines de l'unité d'ordre une puissance de ℓ, alors χ_ℓ se factorise par $\mathrm{Gal}(L/K)$ qui est fini donc a une image finie.

Pour la réciproque, on suppose la propriété (*). L'image $\operatorname{Im}\chi_\ell$ est fermée car le groupe G_K est compact. Il suffit donc de montrer que c'est un sous-groupe d'indice fini dans $\mathbf{Z}_\ell^\times$. Cela revient à montrer que pour n assez grand $1+\ell^n\mathbf{Z}_\ell \subset \operatorname{Im}\chi_\ell$.

Pour cela on utilise le lemme suivant.

Lemme 2.2.3. *Pour $n \geq 1$ les degrés $[K(\mu_{\ell^{n+1}}) : K(\mu_{\ell^n})]$ sont ℓ ou 1.*

Démonstration. L'extension $K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n})$ est galoisienne en tant que corps de décomposition du polynôme $X^\ell - \xi$ où ξ est une racine primitive ℓ^n-ème de l'unité. Le corps K est la complétion en un idéal premier $\mathfrak{p}$ d'un corps de nombres L. Comme $[\mathbf{Q}(\mu_{\ell^{n+1}}) : \mathbf{Q}(\mu_{\ell^n})] = \ell$ ou 1 il en est de même pour $[L(\mu_{\ell^{n+1}}) : L(\mu_{\ell^n})]$. Le groupe de Galois de cette extension de corps globaux est d'ordre ℓ ou 1 et les groupes de Galois des localisés sont des sous-groupes de celui-ci donc d'ordre ℓ ou 1 aussi. □

Par l'hypothèse sur K, il existe $n \geq 1$ tel que $[K(\mu_{\ell^{n+1}}) : K(\mu_{\ell^n})] = \ell$. On montre par l'absurde que $[K(\mu_{\ell^{n+2}}) : K(\mu_{\ell^{n+1}})] = \ell$. On suppose $K(\mu_{\ell^{n+2}}) = K(\mu_{\ell^{n+1}})$.

L'extension $K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n})$ est galoisienne de groupe de Galois $\mathbf{Z}/\ell\mathbf{Z}$. On note ξ une racine primitive ℓ^n-ème de l'unité, w_i les racines de $X^\ell - \xi$ et $\varepsilon_{i,j}$ les racines ℓ^{n+2}-èmes de l'unité tels que $\varepsilon_{i,j}^\ell = w_i$. Le groupe de Galois agit transitivement sur les w_i et si $\sigma(w_i) = w_j$ alors $\sigma(\varepsilon_{i,k}) \in \{\varepsilon_{j,m}\}$ pour $\sigma \in \mathrm{Gal}(K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n}))$. On obtient que l'orbite de $\varepsilon_{i,j}$ sous l'action de $\mathrm{Gal}(K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n}))$ est donnée par les ε_{i,n_i} où $1 \leq i \leq \ell$. Il suit que le polynôme minimal sur $K(\mu_{\ell^n})$ de $\varepsilon_{i,j}$ est $\prod_{i=1}^{\ell}(X - \varepsilon_{i,n_i})$. Le coefficient constant de ce polynôme est $\zeta = \prod_{i=1}^{\ell}\varepsilon_{i,n_i}$. On a

$$\zeta^\ell = \prod_{i=1}^{\ell}(\varepsilon_{i,n_i})^\ell = \prod_{i=1}^{\ell} w_i = \xi$$

donc $\zeta \in K(\mu_{\ell^n})$ est une racine de $X^\ell - \xi$ ce qui est une contradiction par choix de n.

On a obtenu que pour tout $m \geq n$, $[K(\mu_{\ell^{m+1}}) : K(\mu_{\ell^m})] = \ell$. On considère le sous-groupe $H \subset G_K$ défini comme le groupe de Galois $\mathrm{Gal}(\overline{K}/K(\mu_{\ell^n}))$. Soit $(\lambda_i) \in 1 + \ell^n \mathbf{Z}_\ell$. Soit $(\varepsilon_i) \in \mathbf{Z}_\ell(1)$ qui engendre $\mathbf{Z}_\ell(1)$ en tant que $\mathbf{Z}_\ell$-module. Pour tout $\sigma \in H$ on a pour $i \leq n$, $\sigma(\varepsilon_i) = \varepsilon_i$ par définition de H. On a

$$\lambda_{n+1} = \overline{1 + \ell^n k} \in \mathbf{Z}/\ell^{n+1}\mathbf{Z}$$

avec $k \in \mathbf{Z}$. Le groupe de Galois $\mathrm{Gal}(K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n}))$, au travers duquel H agit, agit transitivement sur les racines de $X^\ell - \varepsilon_n$. Autrement dit, il existe $\sigma \in \mathrm{Gal}(K(\mu_{\ell^{n+1}})/K(\mu_{\ell^n}))$ tel que $\sigma(\varepsilon_{n+1}) = \varepsilon_{n+1}^{\lambda_{n+1}}$. Chaque extension successive est galoisienne de degré ℓ donc il y a ℓ choix pour étendre σ à chaque étape qui correspondent aux choix possibles pour étendre λ_{n+1} en un élément de $\mathbf{Z}_\ell$. On obtient par extension un élément $\sigma \in H$ tel que $\chi_\ell(\sigma) = \lambda$. □

Définition 2.2.4. On note K^ℓ l'extension modérément ramifiée ℓ-maximale, c'est-à-dire

$$K^\ell = \bigcup_{n=1}^{\infty} L_n$$

où L_n est l'extension de degré ℓ^n de K^{nr}.

Théorème 2.2.5. *Soient g un entier naturel non nul et $\rho\colon G_K \to \mathrm{GL}_{2g}(\mathbf{Z}_\ell)$ une représentation continue ℓ-adique de G_K. Alors il existe une extension finie L de K telle que la représentation de G_L induite par ρ vérifie pour tout $\sigma \in I_L$, $\rho(\sigma)$ est unipotente. Dans cette situation l'action est donnée par un générateur topologique τ de $\mathbf{Z}_\ell(1)$ au travers duquel elle se factorise.*

Démonstration. On montre d'abord que l'on peut se ramener au cas où $P_{K,\ell}$ agit trivialement par une extension finie.

Soit N le noyau de la réduction $\bmod \ell$, on a une suite exacte

$$0 \longrightarrow N \longrightarrow \mathrm{GL}_{2g}(\mathbf{Z}_\ell) \longrightarrow \mathrm{GL}_{2g}(\mathbf{F}_\ell)\ .$$

Le groupe N est un groupe profini car c'est la limite projective des quotients N/N_n où N_n consiste en les matrices qui se réduisent à l'identité $\bmod \ell^n$. Ces quotients sont tous d'ordre une puissance de ℓ donc N est un pro-ℓ groupe. Comme $P_{K,\ell}$ est un groupe profini d'ordre premier à ℓ, par construction, son image $\rho(P_{K,\ell})$ aussi et par le théorème de Lagrange l'intersection

$\rho(P_{K,\ell}) \cap N$ est réduite à $\{1\}$. Il suit que $\rho(P_{K,\ell})$ s'identifie à un sous-groupe de $\mathrm{GL}_{2g}(\mathbf{F}_\ell)$ donc est fini. Une extension de degré fini permet alors de se ramener au cas où l'action se factorise par $G_{K,\ell}$.

Soit $t \in \mathbf{Z}_\ell(1) \subset G_{K,\ell}$ un générateur topologique de $\mathbf{Z}_\ell(1)$. Quitte à considérer ρ à valeurs dans $\mathrm{GL}_{2g}(\overline{\mathbf{Q}_\ell})$ on considère a une valeur propre de $\rho(t)$ et v un vecteur propre associé. L'action par conjugaison de $G_{K,\ell}$ sur $\mathbf{Z}_\ell(1)$ est donnée par le caractère cyclotomique, on a donc, pour $g \in G_{K,\ell}$,

$$\rho(gtg^{-1})(v) = \rho(t^{\chi_\ell(g))})(v) = a^{\chi_\ell(g)} \cdot v.$$

Il suit

$$\rho(t)\big(\rho(g^{-1})(v)\big) = \rho(tg^{-1})(v) = \rho(g^{-1})\big(a^{\chi_\ell(g)} \cdot v\big) = a^{\chi_\ell(g)}\rho(g^{-1})(v).$$

Ainsi $a^{\chi_\ell(g)}$ est valeur propre de $\rho(t)$ pour tout $g \in G_{K,\ell}$. Par la proposition 2.2.2, $\operatorname{Im}\chi_\ell$ est ouvert donc contient un sous-groupe ouvert de la forme $1 + \ell^n\mathbf{Z}_\ell$ et donc une infinité de $n \in \mathbf{N}$ tel que a^n est valeur propre de $\rho(t)$. Ceci implique que a est une racine de l'unité et donc que $\rho(t)$ est quasi-unipotent. Soit donc $N \in \mathbf{N} \setminus \{0\}$ tel que t^N agit de façon unipotente. Le sous-groupe de $\mathbf{Z}_\ell(1)$ engendré par t^N est d'indice N et son image réciproque par la surjection $I \to \mathbf{Z}_\ell(1)$ donne un sous-groupe d'indice N de I. □

La proposition 3.5 et le corollaire 3.8 de [SGA7] exposé IX donnent en fait que l'action de I est unipotente d'échelon 2 suite à ces extensions.

La démonstration précédente définit un sous-groupe fini $\rho_{A,\ell}(P_{K,\ell})$ et on note K_2 l'extension finie de K^ℓ déterminée par le noyau de la restriction de $\rho_{A,\ell}$ à $P_{K,\ell}$.

2.2.2 Définition des groupes de monodromie finie

Théorème 2.2.6. *Soit $I_{A,v} = \{\sigma \in I_K \mid \rho_{A,\ell}(\sigma)$ est unipotent$\}$. L'ensemble $I_{A,v}$ est un sous-groupe distingué et ouvert de I_K. Il est de plus distingué dans G_K.*

Démonstration. Par le théorème 2.2.5, il existe un sous-groupe ouvert I' de I_K qui agit de façon unipotente sur le module de Tate $U = T_\ell(A)$ de la variété abélienne A sur K. On montre dans un premier temps que le sous-module $U^{I'}$ de U des éléments fixés par l'action de I' est indépendant de I'. Il suffit de le prouver pour $I'' \subset I'$ sous-groupe ouvert de I_K car si J

est un autre sous-groupe ouvert qui agit de façon unipotente l'intersection $I' \cap J$ est un sous-groupe ouvert contenu dans chacun d'eux. Soit $V = U^{I''}$; on a $U^{I'} \subset V$ par construction. De plus, comme l'action de I' est unipotente d'échelon 2, pour $x \in V$ et $\tau, \sigma \in I'$ on a $(\tau - \mathrm{id})(\sigma - \mathrm{id})(x) = 0$ d'où $(\sigma - \mathrm{id})(x) \in U^{I'} \subset V$. Il suit que $\sigma(x) \in V$. Autrement dit, V est stable par I' et l'action de I' sur V se factorise par I'/I'' donc est donnée par l'action d'un groupe fini G. La représentation induite est unipotente et semi-simple car G est fini donc triviale. Il suit que $U^{I'} = V$.

On obtient un sous-module $U^{\mathrm{ef}} = U^{I'}$ indépendant de I'. Le noyau de la représentation induite par I_K sur U^{ef} est donc $I_{A,v}$. Il suit que celui-ci est un sous-groupe ouvert distingué de I_K. Comme le fait d'être unipotent est stable par conjugaison et que I_K est distingué dans G_K, on en déduit directement que $I_{A,v}$ est de plus distingué dans G_K. □

Le critère galoisien ([SGA7] exposé IX 3.5) permet d'assurer que le corps défini par $I_{A,v}$ est la plus petite extension galoisienne $K^{\mathrm{nr}}_{A,s}$ de K^{nr} telle que A ait réduction semi-stable sur $K^{\mathrm{nr}}_{A,s}$. En effet, une extension de K^{nr} a réduction semi-stable si et seulement si son groupe d'inertie agit de façon unipotente donc si et seulement s'il est inclus dans $I_{A,v}$. Comme $I_{A,v}$, l'extension $K^{\mathrm{nr}}_{A,s}$ ne dépend pas du choix de ℓ.

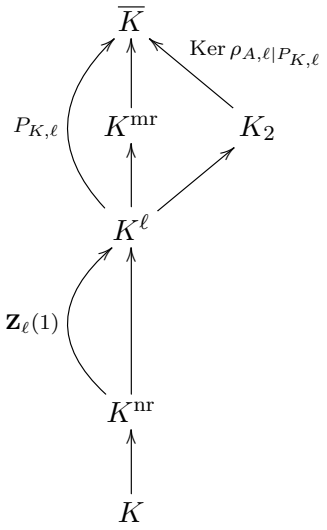
On obtient finalement la définition des groupes de monodromie finie.

Définition 2.2.7. On appelle groupe de monodromie finie de A en v le groupe de Galois de l'extension $K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}$ et on le note $\Phi_{A,v}$. On a $\Phi_{A,v} = I_K/I_{A,v}$.

L'équivalence de cette définition avec celle donnée dans l'introduction est démontrée par le théorème 4.2 de [SZ2]. Le groupe $\Phi_{A,v}$ est un groupe d'inertie par construction donc s'écrit comme un produit semi-direct $G \rtimes \mathbf{Z}/n\mathbf{Z}$ pour un certain entier naturel n et p-groupe fini G.

On continue par une description utilisant $\rho_{A,\ell}$ de $\Phi_{A,v}$ qui permettra une première majoration de son cardinal dans la suite. On suppose maintenant ℓ fixé assez grand de sorte que ℓ ne divise pas $\mathrm{Card}\,\Phi_{A,v}$. Il résulte de cette hypothèse que $K^{\ell} \cap K^{\mathrm{nr}}_{A,s} = K^{\mathrm{nr}}$.

On a le diagramme d'extensions de corps suivant



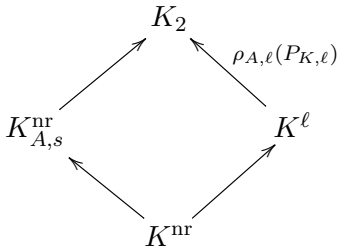
où K_2 est l'extension de K^{ℓ} déterminé par le sous-groupe $\operatorname{Ker}\rho_{A,\ell|P_{K,\ell}}$.

Proposition 2.2.8. *L'extension K_2 est le compositum $K^{\mathrm{nr}}_{A,s}K^{\ell}$ et le groupe de Galois de l'extension $K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}$ est $\rho_{A,\ell}(P_{K,\ell})$.*

Démonstration. On montre d'abord l'égalité $\operatorname{Ker}\rho_{A,\ell|P_{K,\ell}} = I_{A,v} \cap P_{K,\ell}$ qui par correspondance de Galois assure le premier point.

L'inclusion $I_{A,v} \cap P_{K,\ell} \supset \operatorname{Ker}\rho_{A,\ell|P_{K,\ell}}$ est claire, pour l'inclusion réciproque il suffit de remarquer qu'une matrice unipotente d'ordre fini est nécessairement l'identité en caractéristique nulle.

Le groupe de Galois de l'extension K_2/K^{ℓ} est $\rho_{A,\ell}(P_{K,\ell})$ par construction. On a un diagramme d'extensions



Comme l'extension $K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}$ est galoisienne, on obtient par décalage un isomorphisme

$$\mathrm{Gal}(K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}) \simeq \rho_{A,\ell}(P_{K,\ell}).$$

□

On termine cette partie par quelques propriétés des groupes de monodromie finie qui se déduisent directement de leur définition.

Proposition 2.2.9. *Soient A, B des variétés abéliennes sur K qui sont isogènes. Alors on a*

$$\Phi_{A,v} \simeq \Phi_{B,v}.$$

Démonstration. L'isomorphisme découle du fait qu'une isogénie induit un isomorphisme entre les modules de Tate. □

On introduit la notion de type d'obstruction qui sera à nouveau utile en partie 2.3.3.

Définition 2.2.10. Soit A une variété abélienne sur un corps local K. On définit le type d'obstruction à la réduction semi-stable de A comme l'extension galoisienne $K_{A,s}^{\mathrm{nr}}/K^{\mathrm{nr}}$.

Il est clair que c'est un invariant plus fin que le groupe de monodromie finie car plusieurs extensions galoisiennes peuvent avoir le même groupe de Galois. On verra un exemple de cette situation en partie 2.3.3.

Proposition 2.2.11. *Soient A, B des variétés abéliennes sur un corps local K. Alors le type d'obstruction à la réduction semi-stable de $A \times B$ est le compositum $K_{A,s}^{\mathrm{nr}} K_{B,s}^{\mathrm{nr}}$. En particulier $\Phi_{A\times B}$ est un sous-groupe du produit $\Phi_A \times \Phi_B$. Si $B \simeq A$ alors on a $\Phi_{A^2,v} = \Phi_{A,v}$.*

Démonstration. Le module de Tate du produit est le produit des modules de Tate. L'assertion s'en déduit directement. □

2.2.3 Descente sur K

On montre ici que l'ordre du groupe $\Phi_{A,v}$ est bien l'ordre à majorer pour notre problème. Pour cela, on descend l'extension $K_{A,s}^{\mathrm{nr}}/K^{\mathrm{nr}}$ en une extension $K_{A,s}$ de K sur laquelle il y a réduction semi-stable sans perte de degré. On traite d'abord le cas d'une extension modérément ramifiée qui se déduit facilement des rappels sur les corps p-adiques.

Proposition 2.2.12. *Soit L une extension de degré n premier à p de K^{nr}. Alors toute extension modérément et totalement ramifiée M de degré n de K vérifie $I_M = I_L$.*

Démonstration. Soit M/K une telle extension. Le compositum MK^{nr} est une extension de degré n de K^{nr} par le degré de ramification et donc l'unicité d'une telle extension donne $MK^{\mathrm{nr}} = L$ et l'égalité des groupes d'inertie. □

Il suffit maintenant de voir qu'une telle extension de K existe. On peut prendre par exemple $K(\pi^{1/n})$ où π est une uniformisante de l'anneau $\mathcal{O}_K$. On a prouvé le résultat suivant.

Corollaire 2.2.13. *Si l'extension $K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}$ est de degré n premier à p il existe une extension $K_{A,s}$ de K totalement et modérément ramifiée de degré n sur laquelle il y a réduction semi-stable.*

Pour traiter le cas général, on rappelle que l'extension $K^{\mathrm{nr}}_{A,s}/K$ est galoisienne car le groupe $I_{A,v}$ est distingué dans G_K. On a donc une extension de groupes

$$1 \to \Phi_{A,v} \to E \to \widehat{\mathbf{Z}} \to 1.$$

Le résultat suivant généralise le théorème 7.2 de [SZ3].

Théorème 2.2.14. *Il existe une extension $K_{A,s}$ de K de degré* $\operatorname{Card}\Phi_{A,v}$ *telle que A ait réduction semi-stable sur $K_{A,s}$. De plus une telle extension est de degré minimal parmi celles ayant cette propriété. Plus précisément, si L est une extension de K telle que A ait réduction semi-stable sur L alors on la divisibilité*

$$\operatorname{Card}\Phi_{A,v} \mid e(L/K)$$

où $e(L/K)$ est l'indice de ramification.

Démonstration. On est dans la situation d'une extension du groupe $\widehat{\mathbf{Z}}$ (le groupe de Galois de K^{nr}/K) par $\Phi_{A,v}$. D'après la proposition 5.2.2 de [W] le groupe $\widehat{\mathbf{Z}}$ est projectif dans la catégorie des groupes profinis donc il existe un morphisme continu $s\colon \widehat{\mathbf{Z}} \to E$. Le sous-groupe $H = s(\widehat{\mathbf{Z}})$ de E vérifie $H \cap \Phi_{A,v} = \{1\}$, est fermé comme image d'un compact et l'ordre de l'ensemble quotient E/H est $\operatorname{Card}\Phi_{A,v}$. Le sous-groupe H d'indice fini est donc ouvert d'où l'existence d'une extension M répondant au problème par correspondance de Galois. On a $MK^{\mathrm{nr}} = K^{\mathrm{nr}}_{A,s}$ et

$$[M : K] = \operatorname{Card}\Phi_{A,v}.$$

Il reste à prouver la propriété de minimalité. Soit une extension L de K sur laquelle il y a réduction semi-stable alors par critère galoisien on a $I_L \subset I_{A,v}$ et donc LK^{nr} est une extension de $K^{\mathrm{nr}}_{A,s}$. On a donc $\operatorname{Card}\Phi_{A,v}$ divise $[LK^{\mathrm{nr}} : K^{\mathrm{nr}}]$. Le résultat vient alors de la décomposition de l'extension

L/K en une tour

$$\begin{array}{c} L \\ \uparrow \\ L^{\mathrm{non}} \\ \uparrow \\ K \end{array}$$

où L^{non}/K est non ramifiée et L/L^{non} est totalement ramifiée. Il suit que $[LK^{\mathrm{nr}} : K^{\mathrm{nr}}] = [L : L^{\mathrm{non}}]$ et le fait que $\mathrm{Card}\,\Phi_{A,v}$ divise $e(L/K)$. □

Dans la suite, on notera $K_{A,s}$ une extension vérifiant la proposition. On a montré l'existence d'une extension réalisant le degré minimum sans unicité a priori. On a tout de même le résultat suivant.

Proposition 2.2.15. *Soit L/K une extension telle que L est K-isomorphe à $K_{A,s}$. Alors il y a réduction semi-stable sur L.*

Démonstration. L'extension $K_{A,s}/K$ est totalement ramifiée ; c'est donc le cas de L/K aussi. Il suit que $L \cap K^{\mathrm{nr}} = K$ et que l'on peut étendre l'isomorphisme $L \simeq K_{A,s}$ en un isomorphisme $LK^{\mathrm{nr}} \simeq K_{A,s}^{\mathrm{nr}}$. Comme l'extension $K_{A,s}^{\mathrm{nr}}$ est galoisienne, ce dernier est en fait une égalité et donc $I_L = I_{A,v}$. Le critère galoisien assure alors qu'il y a réduction semi-stable sur L. □

2.2.4 Une majoration des cardinaux des groupes $\Phi_{A,v}$

On introduit les notations

$$F^{(p)} = F \cap \mathbf{Q}(\mu_{p^\infty}),\ m(F,p) = \inf\{m \geq 1 \mid F^{(p)} \subset \mathbf{Q}(\mu_{p^m}),\ p^m \neq 2\}$$

et $t(F,p) = [\mathbf{Q}(\mu_{p^{m(F,p)}}) : F^{(p)}]$ où F est un corps de nombres, μ_{p^m} le groupe des racines p^m-èmes de l'unité et $\mathbf{Q}(\mu_{p^\infty})$ la réunion des $\mathbf{Q}(\mu_{p^m})$ pour $m \geq 1$. La borne de Schur est alors donnée, pour un entier naturel non nul s et un corps de nombres F, par

$$S(s,F) = 2^{s-\lfloor s/t(F,2)\rfloor} \prod_{p \text{ premier}} p^{m(F,p)\lfloor s/t(F,p)\rfloor} \Big(\Big\lfloor \frac{s}{t(F,p)} \Big\rfloor ! \Big)_p,$$

où $\lfloor x \rfloor$ est la partie entière de x et $m_p = p^{v_p(m)}$. On retrouve la borne de Minkowski par l'égalité $M(2g) = S(2g, \mathbf{Q})$ (voir [Ré2] introduction de la partie 4).

Proposition 2.2.16. *On a la borne de divisibilité*

$$\operatorname{Card}\Phi_{A,v} | 2^g S(2g, \mathbf{Q}).$$

Démonstration. La démonstration du théorème 2.2.5 donne des injections

$$\rho_{A,\ell}(P_{K,\ell}) \longrightarrow \mathrm{GL}_{2g}(\mathbf{F}_\ell)$$

et pour tout ℓ assez grand on a un isomorphisme $\rho_{A,\ell}(P_{K,\ell}) \simeq \Phi_{A,v}$. Le théorème de Lagrange assure donc que $\operatorname{Card}\Phi_{A,v}$ divise le pgcd des ordres des groupes $\mathrm{GL}_{2g}(\mathbf{F}_\ell)$ pour ℓ grand. Ce dernier est connu et le résultat se déduit directement de [Ré2] proposition 4.9. □

Cette borne n'est pas optimale, on peut en effet montrer la divisibilité $\operatorname{Card}\Phi_{A,v} \mid S(2g, \mathbf{Q})$ en utilisant le fait que le groupe $\Phi_{A,v}$ s'injecte dans le groupe des automorphismes de la variété réduite d'une extension des scalaires de A qui soit semi-stable, ce qui constitue le théorème suivant dans le cas de bonne réduction potentielle. Le cas général est traité dans [SZ2] aux théorèmes 5.2 et 5.3.

Théorème 2.2.17. *Dans le cas de bonne réduction potentielle, le groupe $\Phi_{A,v}$ est isomorphe à un sous-groupe du groupe des automorphismes de $A'^{\circ}_{k'}$ la partie connexe de la réduction de $A_{K_{A,s}} = A'$.*

Démonstration. Comme le modèle de Néron est invariant par extension non ramifiée, on peut supposer $K = K^{\mathrm{nr}}$. On considère $A' = A \times_K K_{A,s}$. Le groupe de Galois $\mathrm{Gal}(K_{A,s}/K) = \Gamma$ agit sur A' par son action sur $K_{A,s}$. Pour $\sigma \in \Gamma$ on a un diagramme commutatif

$$\begin{array}{ccc} A' & \xrightarrow{(id\times\sigma)} & A' \\ \downarrow & & \downarrow \\ \operatorname{Spec} K_{A,s} & \xrightarrow[\sigma]{} & \operatorname{Spec} K_{A,s} \end{array}$$

qui permet de voir A' comme schéma sur $K_{A,s}$ par la composée du morphisme structurel avec σ. On note ce schéma A'_σ. On note $\mathcal{A}'$ le modèle de Néron de A'. Le modèle de Néron de A'_σ est $\mathcal{A}'_\sigma$, c'est-à-dire $\mathcal{A}'$ vu comme $\operatorname{Spec}\mathcal{O}_{K_{A,s}}$ schéma par la composée avec l'action de σ sur $\operatorname{Spec}\mathcal{O}_{K_{A,s}}$. La propriété de Néron donne alors un morphisme qui relève $(\mathrm{id} \times \sigma)$ en une flèche faisant

commuter le diagramme

$$\begin{array}{ccc} A' & \xrightarrow{(\mathrm{id}\times\sigma)} & A' \\ \downarrow & & \downarrow \\ \mathcal{A}' & \longrightarrow & \mathcal{A}' \\ \downarrow & & \downarrow \\ \operatorname{Spec}\mathcal{O}_{K_{A,s}} & \longrightarrow & \operatorname{Spec}\mathcal{O}_{K_{A,s}} \end{array}$$

On a de plus un carré commutatif

$$\begin{array}{ccc} \mathcal{O}_{K_{A,s}} & \xrightarrow{\sigma} & \mathcal{O}_{K_{A,s}} \\ \downarrow & & \downarrow \\ k' & \xrightarrow[\overline{\sigma}]{} & k' \end{array}$$

où $\overline{\sigma}$ est l'identité car σ est dans le groupe d'inertie. On en déduit un k'-isomorphisme faisant commuter le diagramme

$$\begin{array}{ccc} \mathcal{A}' & \xrightarrow{\sigma} & \mathcal{A}' \\ \uparrow & & \uparrow \\ A'_{k'} & \longrightarrow & A'_{k'} \end{array}$$

Dans tout ce qui précède on peut se restreindre à $\mathcal{A}'^{\circ}$, ce qui donne un automorphisme de $A'^{\circ}_{k'}$.

Ce groupe agit sur le module de Tate $\mathrm{T}_\ell(A'_{\overline{k}})$. Comme le morphisme d'action

$$\Gamma \longrightarrow \operatorname{Aut} T_\ell(A)^{I_{A,v}}$$

est injectif et qu'il est obtenu par la composition $\Gamma \to \operatorname{Aut} A'^{\circ}_{k'} \to \operatorname{Aut} T_\ell(A)^{I_{A,v}}$ alors $\Gamma \to \operatorname{Aut} A'^{\circ}_{k'}$ est injectif ce qui donne le théorème car $\Gamma \simeq \Phi_{A,v}$. L'isomorphisme $T_\ell(A)^{I_{A,v}} \simeq T_\ell(A'_{k'})$ est démontré dans [SGA7] exposé IX p. 331–332. □

On sait de plus que le groupe des automorphismes d'une variété abélienne est une algèbre de dimension au plus $4g^2$ sur $\mathbf{Q}$ (voir [Mu] corollaire 1 p. 178) ce qui donne la borne de divisibilité annoncée avec le théorème 4.1 de [Ré2] et le fait que $S(g,F) \mid S(dg,\mathbf{Q})$ pour F un corps de nombres de degré d sur $\mathbf{Q}$. On obtient ainsi le théorème suivant dans le cas de bonne réduction potentielle qui est le corollaire 6.3 de [SZ2] en toute généralité.

Théorème 2.2.18. *Soit A une variété abélienne de dimension g sur un corps local K. On a la borne de divisibilité*

$$\operatorname{Card}\Phi_{A,v} \mid M(2g).$$

Corollaire 2.2.19. *Soit A une variété abélienne de dimension g sur un corps local K. Les diviseurs premiers de* $\operatorname{Card}\Phi_{A,v}$ *sont inférieurs à $2g+1$.*

Démonstration. Cela est direct par la formule donnant $M(2g) = S(2g, \mathbf{Q})$. En effet, on a $t(\mathbf{Q}, p) = p-1$ pour $p > 2$ donc les équivalences

$$p \mid M(2g) \iff \left\lfloor \frac{2g}{p-1} \right\rfloor \neq 0 \iff p \leq 2g+1.$$

□

2.2.5 Lien avec la ℓ-torsion

Il est bien connu que pour un entier m (qui n'est pas une puissance de 2) assez grand le corps de définition $K(A[m])$ de la m-torsion de A est un corps de stabilité pour A. Ceci est en particulier étudié en détail par Silverberg et Zahrin dans [SZ1]. On démontre une version faible de leur résultat ici. Dans le théorème suivant uniquement K est un corps de nombres.

Théorème 2.2.20. *Soient v une place de K, p la caractéristique du corps résiduel k_v et ℓ un nombre premier différent de p. On suppose les points de ℓ-torsion de A définis sur une extension non ramifiée de K. Alors A a réduction semi-stable en v si $\ell \neq 2$ et sur une extension quadratique ramifiée de K en v si $\ell = 2$.*

Démonstration. Soient $\sigma \in I(\overline{v}/v)$ où $\overline{v}$ est une extension de v à $\overline{\mathbf{Q}}$ et I le groupe d'inertie associé. Il faut montrer que σ ou σ^2 agit de façon unipotente sur $T_\ell(A)$. On sait que σ^m agit de façon unipotente d'échelon 2 pour un $m \in \mathbf{N}\setminus\{0\}$ par le théorème de réduction semi-stable. Soit donc a une racine du polynôme caractéristique de $\rho_{A,\ell}(\sigma)$, où $\rho_{A,\ell}\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(T_\ell(A))$ est la représentation ℓ-adique associée.

Le nombre a est une racine m-ième de l'unité. L'hypothèse sur les points de torsion assure de plus que $\rho_{A,\ell}(\sigma)$ agit trivialement sur $T_\ell(A)/\ell T_\ell(A) \simeq \mathbf{Z}_\ell^{2g}/\ell\mathbf{Z}_\ell^{2g}$ donc $\rho_{A,\ell}(\sigma)-1 \in \ell \mathrm{M}_{2g}(\mathbf{Z}_\ell)$. Il suit que $\frac{a-1}{\ell}$ est racine du polynôme caractéristique de $\frac{\rho_{A,\ell}(\sigma)-1}{\ell}$. On sait aussi que le polynôme caractéristique χ_σ de $\rho_{A,\ell}(\sigma)$ est à coefficients entiers par le théorème 4.3 de l'exposé IX de [SGA7], $\chi_\sigma \in \mathbf{Z}[X]$. On en déduit

$$\ell^{-2g}\chi_\sigma(1+\ell X) = \chi_{\frac{\rho_{A,\ell}(\sigma)-1}{\ell}} \in \big(\mathbf{Z}[\tfrac{1}{\ell}] \cap \mathbf{Z}_\ell\big)[X].$$

Comme ℓ n'est pas inversible dans $\mathbf{Z}_\ell$ on a $\mathbf{Z}[\frac{1}{\ell}] \cap \mathbf{Z}_\ell = \mathbf{Z}$ et $\frac{a-1}{\ell} \in \overline{\mathbf{Z}}$, $a - 1 \in \ell\overline{\mathbf{Z}}$.

Soit M l'ordre de a, si $M = 1$ alors $a = 1$. Sinon, soit q un nombre premier tel que q^r divise exactement M. Alors $a^{\frac{M}{q^r}} = w$ est une racine primitive q^r-ème de l'unité et $w - 1 \in \ell\overline{\mathbf{Z}}$ par le binôme de Newton. On a de plus par un calcul classique de théorie des nombres

$$q = \phi_{q^r}(1) = \prod_{i \wedge q^r = 1} (1 - w^i) \in \ell^{\varphi(q^r)}\overline{\mathbf{Z}}.$$

Donc $\frac{q}{\ell^{\varphi(q^r)}} \in \overline{\mathbf{Z}}$ ce qui est impossible sauf si $q = \ell = 2$. On a donc $M = 1$ ou $M = 2$ et $\rho_{A,\ell}(\sigma)^2$ agit de façon unipotente. □

L'argument présenté dans [SZ1] est un raffinement de celui-ci en ne considérant qu'un sous-groupe isotrope maximal du groupe des points de n-torsion défini sur une extension non ramifiée de K.

On considère à nouveau que K est un corps p-adique. On reprend les notations de la partie 2 et on se place sur K^{nr}. Le résultat précédent se traduit par le fait que le groupe $I_{A[\ell]} = \mathrm{Gal}\big(\overline{K}/K^{\mathrm{nr}}(A[\ell])\big)$ est un sous-groupe de $I_{A,v}$ nécessairement distingué ou encore qu'on a l'inclusion $K^{\mathrm{nr}}_{A,s} \subset K^{\mathrm{nr}}(A[\ell])$. On se fixe alors ℓ suffisamment grand ($\ell > 2\dim A + 1$ suffit) de manière à ce que $\Phi_{A,v}$ soit d'ordre premier à ℓ.

On énonce un autre résultat bien connu, voir par exemple [BK] partie 2.

Proposition 2.2.21. *L'extension $K^{\mathrm{nr}}(A[\ell])/K^{\mathrm{nr}}_{A,s}$ est triviale ou l'unique extension modérément ramifiée d'ordre ℓ.*

Démonstration. Soit $\sigma \in I_{A,v}$. Alors σ agit de façon unipotente d'échelon 2 sur $A[\ell]$. Pour $x \in A[\ell]$ on a

$$\sigma^2(x) = 2 \cdot \sigma(x) - x$$

et par une récurrence immédiate $\sigma^\ell(x) = \ell \cdot \sigma(x) - (\ell - 1) \cdot x = x$.

Il suit que $\mathrm{Gal}(K^{\mathrm{nr}}(A[\ell])/K^{\mathrm{nr}}_{A,s})$ a pour exposant ℓ ce qui conclut. □

On peut finalement décrire le groupe de Galois de l'extension $K^{\mathrm{nr}}(A[\ell])/K^{\mathrm{nr}}$.

Proposition 2.2.22. *L'extension $K^{\mathrm{nr}}(A[\ell])/K^{\mathrm{nr}}$ a pour groupe de Galois $\Phi_{A,v}$ ou $\Phi_{A,v} \times \mathbf{Z}/\ell\mathbf{Z}$.*

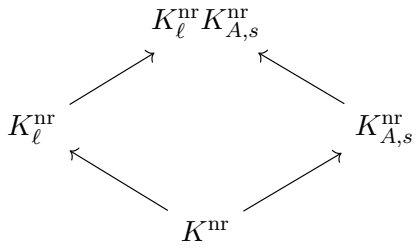
Démonstration. Soit G le groupe de Galois en question.

D'après ce qui précède, on a un diagramme d'extensions galoisiennes

$$K^{\mathrm{nr}} \longrightarrow K^{\mathrm{nr}}_{A,s} \longrightarrow K^{\mathrm{nr}}(A[\ell])$$

où $K^{\mathrm{nr}}(A[\ell])/K^{\mathrm{nr}}_{A,s}$ est triviale ou l'unique extension de degré ℓ. Si cette extension est triviale alors $G = \Phi_{A,v}$.

Sinon, l'unique extension K^{nr}_{ℓ} de degré ℓ de K^{nr} est linéairement disjointe de $K^{\mathrm{nr}}_{A,s}$ par choix de ℓ. Il suit que le compositum $K^{\mathrm{nr}}_{\ell}K^{\mathrm{nr}}_{A,s}$ s'insère dans le diagramme suivant



et par décalage l'extension $K^{\mathrm{nr}}_{\ell}K^{\mathrm{nr}}_{A,s}/K^{\mathrm{nr}}_{A,s}$ est encore de degré ℓ. Finalement on obtient par unicité l'égalité $K^{\mathrm{nr}}_{\ell}K^{\mathrm{nr}}_{A,s} = K^{\mathrm{nr}}(A[\ell])$ et G est le produit direct annoncé.

□

L'intérêt de cette proposition vient du fait que le groupe $\Phi_{A,v}$ est entièrement connu par l'action de l'inertie sur la ℓ-torsion pourvu que ℓ soit assez grand, c'est-à-dire plus grand que $2\dim A + 1$ ce qui sera utile dans le chapitre suivant.

2.3 Le cas des corps de nombres

2.3.1 Préliminaires d'analyse p-adique

Les premiers énoncés sont des résultats standard et traitent de la continuité des racines dans le cas non archimédien. Le théorème 2.3.4 qui en résulte est notre outil pour construire des extensions de corps globaux avec des comportements locaux prescrits. Dans cette sous-partie, le corps K est toujours p-adique sauf mention du contraire.

Lemme 2.3.1. *Soit $(f_j)_{j\geq 0}$ une suite de polynômes de $K[X]$ unitaires de degré n. On note*

$$f_j = X^n + \sum_{i=0}^{n-1} a_{ij} X^i.$$

On suppose que les coefficients a_{ij} convergent vers des éléments $a_i \in K$ pour chaque i. Soit $r_j \in \overline{K}$ une racine de f_j pour chaque j. Dans ces conditions il existe une sous-suite de $(r_j)_{j\geq 0}$ qui converge vers une racine $r \in \overline{K}$ de $f = X^n + \sum_{i=0}^{n-1} a_i X^i$.

Démonstration. On note C la constante $\max_k |a_k|^{\frac{1}{n-k}}$.

La distance est ultramétrique donc pour j assez grand et $a_i \neq 0$ on a l'égalité $|a_{ij}| = |a_i|$ en regardant le triangle $(a_{ij}, a_i, 0)$. Dans le cas où $a_i = 0$ la suite $(a_{ij})_{j\geq 0}$ converge vers 0 donc pour j assez grand $|a_{ij}|^{\frac{1}{n-i}} \leq \max_k |a_k| = C$ s'il existe un i tel que $a_i \neq 0$. Dans ces deux cas, on a $|a_{ij}|^{\frac{1}{n-i}} \leq C$ et on en déduit l'inégalité

$$|r_j^n| \leq \max_i C^{n-i} |r_j|^i$$

pour j assez grand et par suite $|r_j| \leq C$.

On a alors

$$|f(r_j)| = |f(r_j) - f_j(r_j)| = |\sum_{i=0}^{n-1} (a_i - a_{ij}) r_j^i| \leq \max_i |a_i - a_{ij}| \max(1, C^{n-1}).$$

On déduit de l'hypothèse que $(|f(r_j)|)_{j\geq 0}$ converge vers 0 dans tous les cas (si tous les a_i sont nuls aussi). Soient L le corps de décomposition de f et ρ_k les racines de f sur L. On a

$$\lim_{j\to\infty} \prod_{k=1}^{n} (r_j - \rho_k) = 0$$

et donc il existe une sous-suite $(r_{\varphi(j)})_{j\geq 0}$ de $(r_j)_{j\geq 0}$ qui converge vers ρ_k pour un certain k. □

Théorème 2.3.2. *(Continuité des racines) Soit $r \in \overline{K}$ une racine de $f = \sum_{i=0}^{n} a_i X^i$ avec $a_n = 1$. On note μ la multiplicité de r en tant que racine de f. Soit $\eta > 0$ tel que toutes les autres racines de f sont à distance au moins η*

de r. Alors pour tout $0 < \varepsilon < \eta$ il existe $\delta > 0$ tel que si $g = \sum_{i=0}^{n} b_i X^i$ unitaire de degré n vérifie

$$|a_i - b_i| < \delta$$

pour tout i alors g a exactement μ racines comptées avec multiplicité dans la boule

$$B_\varepsilon(r) = \{x \in \overline{K},\ |x - r| < \varepsilon\}.$$

Démonstration. Soit $0 < \varepsilon < \eta$ et on suppose par l'absurde qu'il n'existe pas de tel δ. Cela revient à supposer l'existence d'une suite de polynômes unitaires $f_j = \sum_{i=0}^{n} a_{ij} X^i$ avec

$$|a_{ij} - a_i| \underset{j\to\infty}{\longrightarrow} 0$$

et f_j n'a pas μ racines dans la boule $B_\varepsilon(r)$.

On note ρ_{jk} les racines de f_j. Par le lemme précédent il existe une sous-suite de $(\rho_{j1})_{j\geq 0}$ qui converge vers une racine ρ_1 de f et quitte à extraire n fois on obtient une suite $(f_j)_{j\geq 0}$ telle que $\rho_{jk} \to \rho_k$.

Dans l'espace vectoriel des polynômes de degré inférieur à n sur $\overline{K}$ muni de la norme infinie, $(f_j)_{j\geq 0}$ converge vers $\prod_{k=1}^{n}(X - \rho_k)$ par ce qui précède et les formules coefficients-racines. Or par hypothèse $(f_j)_{j\geq 0}$ converge vers f. On en déduit que l'ensemble $\{\rho_k\}$ est l'ensemble des racines de f. En particulier $r = \rho_k$ pour μ indices. Quitte à renuméroter on peut supposer que ce sont les indices $1 \leq k \leq \mu$. Quitte à extraire à nouveau une sous-suite de $(f_j)_{j\geq 0}$ on peut de plus supposer que pour tout j on a

$$|\rho_{jk} - \rho_k| < \varepsilon$$

et en particulier $|\rho_{jk} - r| < \varepsilon$ pour $1 \leq k \leq \mu$. Pour les autres indices, on a par définition de η

$$|\rho_{jk} - r| = | = |r'_k - r| \geq \eta > \varepsilon$$

pour une racine r'_k de f distincte de r.

On a montré que tous les f_j ont exactement μ racines dans $B_\varepsilon(r)$ ce qui est une contradiction. □

Corollaire 2.3.3. *Soit $f \in K[X]$ unitaire à racines simples. Soit $\varepsilon > 0$ assez petit. Pour tout polynôme unitaire $g \in K[X]$ dont les coefficients sont assez proches de ceux de f, chaque racine de g est à distance au plus ε d'une*

unique racine de f. De plus, la factorisation de g dans $K[X]$ correspond à celle de f, c'est-à-dire si $f = \prod_{k=1}^{s} f_i$ où les f_i sont des polynômes irréductibles de degré n_i alors $g = \prod_{k=1}^{s} g_i$ où les g_i sont des polynômes irréductibles de degré n_i.

Démonstration. On applique le théorème précédent avec $\mu = 1$ et ε par hypothèse sur g. L'action du groupe de Galois absolu G_K se fait par isométries donc les orbites des racines de f sous cette action correspondent aux orbites des racines de g par unicité. □

Théorème 2.3.4. *Soient K un corps de nombres et $v_1, \ldots, v_n$ des places distinctes de K. Soient K_i'/K_{v_i} des extensions finies ayant même degré d. Alors il existe une extension K'/K avec une unique place $v_i'|v_i$ pour chaque i telle que $K'_{v_i'} \simeq K_i'$ et $[K' : K] = d$.*

Démonstration. Les extensions K_i'/K_{v_i} sont données par des polynômes unitaires $g_i = \sum_{j=0}^{d} b_{ij} X^j$ de degré d par le théorème de l'élément primitif. Par approximation faible quelque soit $\varepsilon > 0$ il existe un polynôme $f = \sum_{j=0}^{d} a_j X^j \in K[X]$ tel que $|a_j - b_{ij}|_{v_i} < \varepsilon$ et ce pour tout i, j. Par le corollaire précédent on déduit que f est irréductible dans $K_{v_i}[X]$ donc dans $K[X]$ pour ε assez petit. Soit $K' = K[X]/(f)$. Par construction il n'y a qu'une seule place v_i' de K' au-dessus de v_i pour chaque i. De plus pour tout i on a

$$K_{v_i} \otimes_K K' = K_{v_i}[X]/(f) \simeq K_i'.$$

L'isomorphisme de droite s'obtient, lorsque ε est assez petit, par [N] proposition 5.9 page 207. □

La démonstration montre que l'on peut ajouter un nombre fini de places S de K sur lesquelles on peut prescrire un certain comportement local comme par exemple choisir un ensemble de places inertes dans K'.

Dans le cas où les extensions locales sont galoisiennes de groupe de Galois abélien on a le théorème suivant.

Théorème 2.3.5. *Soient K un corps de nombres et $v_1, \ldots, v_n$ des places distinctes de K. Soient L_i/K_{v_i} des extensions locales abéliennes. Alors il existe une extension abélienne L de K telle que pour toute place w_i au dessus de v_i on ait $L_{w_i} \simeq L_i$. Autrement dit l'extension L réalise les extensions abéliennes locales.*

Démonstration. Voir [AT] chapitre X théorème 4 p. 102. □

Si les groupes locaux sont cycliques le théorème est celui de Grunwald-Wang et on a de plus une majoration du degré de l'extension globale. Ce théorème intervient pour les variétés abéliennes à multiplication complexe. On obtient un résultat presque optimal en terme de degré. La situation est décrite dans [ST], en particulier le théorème 7.

2.3.2 L'entier $d(A)$ et les groupes $\Phi_{A,v}$

On considère maintenant une variété abélienne A sur un corps de nombres K. On note $v_1, \ldots, v_n$ les places de K pour lesquelles il n'y a pas réduction semi-stable. D'après la partie précédente il existe des groupes Φ_{A,v_i} qui donnent le degré minimal d'une extension de K_{v_i} ayant réduction semi-stable.

On en déduit en corollaire du théorème 2.3.4 le résultat d'existence que l'on veut, qui généralise à A quelconque le théorème 7 de [ST] sans toutefois obtenir une extension galoisienne.

Théorème 2.3.6. *Soit A une variété abélienne sur un corps de nombres K. Il existe une extension $K_{A,s}$ de K de degré $\operatorname{ppcm}_{v\in\Sigma_K} \operatorname{Card}\Phi_{A,v}$ telle que A atteint réduction semi-stable sur $K_{A,s}$. De plus, si L est une extension finie de K telle que A_L ait réduction semi-stable alors on a*

$$\operatorname*{ppcm}_{v\in\Sigma_K} \operatorname{Card}\Phi_{A,v} \mid [L:K].$$

Démonstration. Soit $d = \operatorname{ppcm}_{v\in\Sigma_K} \operatorname{Card}\Phi_{A,v}$. Soient $v_1, \ldots, v_n$ les places de K telles que $\Phi_{A,v_i} \neq \{1\}$ et soit d_i tel que $\operatorname{Card}\Phi_{A,v_i} d_i = d$. Par le théorème 2.2.14 pour chaque corps local K_{v_i} il existe une extension L_i/K_{v_i} de degré $\operatorname{Card}\Phi_{A,v_i}$ telle que A ait réduction semi-stable sur L_i. On note M_i l'extension de L_i non ramifiée de degré d_i. Les extensions $M_1/K_{v_1}, \ldots, M_n/K_{v_n}$ sont de même degré d. Le théorème 2.3.4 appliqué avec ces extensions locales donne une extension L/K de degré d et telle que A atteint réduction semi-stable sur L.

On montre maintenant la propriété de minimalité. Soit L une extension de K telle que A_L ait réduction semi-stable. Soient $w_{i1}, \ldots, w_{im}$ les places de L au dessus de v_i. Par définition il y a réduction semi-stable sur les localisés $L_{w_{ij}}$ pour tout j donc par le théorème 2.2.14 l'ordre de Φ_{A,v_i} divise l'indice de ramification $e(w_{ij}/v_i)$. Par la formule classique de théorie algébrique des nombres

$$\sum_j e(w_{ij}/v_i) f(w_{ij}/v_i) = [L:K]$$

on obtient que $\mathrm{Card}\,\Phi_{A,v_i}$ divise $[L : K]$. Ceci étant valable pour tous les indices i le résultat sur le ppcm s'en déduit directement. □

Le résultat est optimal en terme du degré de l'extension obtenue. On ne peut néanmoins pas garantir que l'extension est galoisienne comme c'est le cas pour une variété abélienne CM.

On peut finalement revenir au cas des courbes elliptiques et démontrer le corollaire 2.1.2. Les groupes $\Phi_{A,v}$ possibles dans le cas des courbes elliptiques sont décrits dans [Se1] page 312.

Corollaire 2.3.7. *Soit E une courbe elliptique sur un corps de nombres K. Il existe une extension L de K de degré au plus 24 telle que E ait réduction semi-stable sur L. De plus, il existe une courbe E sur $\mathbf{Q}$ telle qu'il n'y a aucune extension de $\mathbf{Q}$ de degré strictement inférieur à 24 avec cette propriété. Autrement dit, on a*

$$d_1 = \max_{A,\ \dim A=1} d(A) = 24.$$

Démonstration. Soit E une courbe elliptique sur un corps de nombres K. La borne de divisibilité pour $g = 1$ obtenue avec le théorème 2.2.18 est 24. On sait donc par le théorème 2.3.6 qu'il existe une extension L de K de degré divisant 24 telle que E atteigne réduction semi-stable sur L.

En particulier la courbe sur $\mathbf{Q}$

$$E\colon y^2 = x^3 - 2x^2 - x$$

atteint cette borne, ayant $\mathrm{SL}_2(\mathbf{F}_3)$ pour groupe $\Phi_{E,2}$ d'après le paragraphe 5.9.1 de [Se1]. □

2.3.3 Corps de stabilité

Le but de cette digression est de renverser le point de vue. On ne considère plus une variété abélienne dont on veut connaître un corps de degré minimal où elle atteindrait réduction semi-stable en une ou plusieurs places mais les corps qui stabilisent toutes les variétés abéliennes de dimension fixée en des places données. On montre qu'il existe des extensions de corps de degré fini sur lesquels toutes les variétés abéliennes de dimension fixée ont réduction semi-stable en un nombre fini de places. On se restreint à $K = \mathbf{Q}$ dans cette partie pour simplifier l'écriture.

On commence par un lemme sur les ensembles d'extensions locales qui sont des types d'obstruction.

Lemme 2.3.8. *Soient p un nombre premier et g un entier naturel non nul. L'ensemble*

$$\mathcal{S}_{p,g} = \{L/\mathbf{Q}_p^{\mathrm{nr}} \mid \exists A \text{ variété abélienne sur } \mathbf{Q}_p, \dim A = g, \text{ avec } L = (\mathbf{Q}_p^{\mathrm{nr}})_{A,s}\}$$

est fini.

Démonstration. En effet, par le théorème 2.2.14, ces extensions sont toutes obtenues par compositum d'une extension de degré fini borné par $M(2g)$ de $\mathbf{Q}_p$ et de $\mathbf{Q}_p^{\mathrm{nr}}$. Comme il n'existe qu'un nombre fini d'extensions de $\mathbf{Q}_p$ de degré borné, on en déduit immédiatement le lemme. □

Il est notable de voir que l'ensemble des extensions de degré borné par $M(2g)$ de $\mathbf{Q}_p^{\mathrm{nr}}$ est lui de cardinal infini, cela peut se démontrer par la formule de masse de Serre.

Proposition 2.3.9. *Soient p un nombre premier et g un entier naturel non nul. Il existe une extension $K_{p,g}$ de degré fini de $\mathbf{Q}$ telle que si A est une variété abélienne de dimension g sur $\mathbf{Q}$ alors $A_{K_{p,g}}$ a réduction semi-stable en p.*

Démonstration. On considère l'extension $L_p/\mathbf{Q}_p^{\mathrm{nr}}$ obtenue par compositum de tous les éléments de $\mathcal{S}_{p,g}$, qui est galoisienne finie sur $\mathbf{Q}_p^{\mathrm{nr}}$. C'est encore une extension galoisienne de $\mathbf{Q}_p$ par construction et donc le théorème 2.2.14 assure qu'elle descend à une extension finie L' de $\mathbf{Q}_p$. Il suffit alors de prendre $K_{p,g}$ telle que $(K_{p,g})_p = L'$. □

L'extension $K_{p,g}$ est découpée par le sous-groupe ouvert de I_K qui est l'intersection des sous-groupes définissant les éléments de $\mathcal{S}_{p,g}$.

Si A est une courbe elliptique et si $p > 3$ on peut choisir $K_{p,1}$ de degré 6.

On a en fait un résultat plus précis.

Théorème 2.3.10. *Soient S un ensemble fini de places de $\mathbf{Q}$ et g un entier naturel non nul. Alors il existe une extension finie $K_{S,g}/\mathbf{Q}$ telle que si A est une variété abélienne sur $\mathbf{Q}$ de dimension g dont l'ensemble des places de mauvaise réduction est inclus dans S alors $A_{K_{S,g}}$ a réduction semi-stable.*

Démonstration. Pour chaque place $p \in S$ on considère $L_p/\mathbf{Q}_p^{\mathrm{nr}}$ l'extension obtenue par compositum de tous les éléments de $\mathcal{S}_{p,g}$. C'est une extension

galoisienne de $\mathbf{Q}_p$ par construction et donc la preuve du théorème 2.2.14 assure qu'elle descend à une extension finie L'_p de $\mathbf{Q}_p$. Quitte à faire des extensions non ramifiées (comme dans le théorème 2.3.6) on peut supposer que les L'_p ont même degré. Le théorème 2.3.4 donne alors l'existence de $K_{S,g}$. □

Comme précédemment on peut remarquer que pour $g = 1$ si de plus l'ensemble S ne contient ni 2 ni 3 on peut choisir $K_{S,1}$ de degré 6.

Définition 2.3.11. Soient S un ensemble de places de $\mathbf{Q}$ et g un entier naturel non nul. On appelle corps de stabilité pour S d'ordre g une extension $K_{S,g}/\mathbf{Q}$ de degré fini telle que toute variété abélienne A de dimension g sur $\mathbf{Q}$ dont les places de mauvaise réduction sont dans S atteint réduction semi-stable sur $K_{S,g}$.

On peut remarquer qu'une extension de stabilité pour S un ensemble de places fixé et g un entier naturel non nul est une extension de stabilité pour $S' \subset S$ et $g' \leq g$ un entier naturel non nul.

Exemple 2.3.12. On étudie le cas des courbes elliptiques sur $\mathbf{Q}$ ayant $\mathbf{Z}/3\mathbf{Z}$ pour groupe de monodromie finie en 3. On cherche d'abord le nombre de types d'obstruction possibles. Soit E une telle courbe. Il existe une extension K de degré 3 de $\mathbf{Q}_3$ telle que E_K a réduction semi-stable. Une telle extension doit de plus vérifier que $K\mathbf{Q}_3^{\mathrm{nr}}$ est galoisienne de groupe $\mathbf{Z}/3\mathbf{Z}$. Soit L la clôture galoisienne de K alors L/K est galoisienne de degré 1 ou 2 et par décalage $L^{\mathrm{nr}}/K^{\mathrm{nr}}$ aussi. Toujours par décalage $L^{\mathrm{nr}}/\mathbf{Q}_3^{\mathrm{nr}}$ est galoisienne de groupe isomorphe au groupe d'inertie de l'extension $L/\mathbf{Q}_3$. On en déduit que $\mathrm{Gal}(L^{\mathrm{nr}}/\mathbf{Q}_3^{\mathrm{nr}})$ est un sous-groupe de $\mathfrak{S}_3$ qui admet un quotient d'ordre 3 ce qui impose que c'est $\mathbf{Z}/3\mathbf{Z}$ et $L^{\mathrm{nr}} = K^{\mathrm{nr}}$. On a donc deux cas. Le premier cas est celui où $L = K$ et le second où $L/\mathbf{Q}_3$ est galoisienne de groupe $\mathfrak{S}_3$ avec $\mathbf{Z}/3\mathbf{Z}$ comme groupe d'inertie. La liste des extensions de degré 3 de $\mathbf{Q}_3$ étant connue on a les quatre possibilités suivantes, données par un polynôme générateur :

$$\text{Premier cas} \begin{cases} K_1 \colon X^3 - 3X^2 + 21 \\ K_2 \colon X^3 - 3X^2 + 3 \\ K_3 \colon X^3 - 3X^2 + 12 \end{cases} \qquad \text{Second cas} \begin{cases} K_4 \colon X^3 + 3X^2 + 3. \end{cases}$$

On peut d'ailleurs remarquer qu'il y a 2 autres extensions dans le second cas mais qu'elles sont isomorphes à K_4.

On montre maintenant que K_1, K_2 et K_3 ont même extension maximale non ramifiée. Le compositum K_1K_2 est galoisien sur $\mathbf{Q}_3$ de groupe $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$. Ce dernier possède 4 sous-groupes distingués d'ordre 3 donc 4 quotients d'ordre 3. Or d'après la liste il n'y a que 3 extensions totalement ramifiés et galoisienne d'ordre 3 de $\mathbf{Q}_3$. L'unique extension non ramifiée K_u de degré 3 de $\mathbf{Q}_3$ est donc un sous-corps de K_1K_2 ce qui donne $K_1K_2 = K_1K_u$. Il en résulte que

$$K_1^{\mathrm{nr}}K_2^{\mathrm{nr}} = K_1K_2\mathbf{Q}_3^{\mathrm{nr}} = K_1^{\mathrm{nr}}$$

et de même pour K_1K_3 et K_2K_3.

Il reste à voir que $K_4^{\mathrm{nr}} \neq K_1^{\mathrm{nr}}$ pour comprendre la situation entièrement. Soit L la clôture galoisienne de K_4. On suppose que $K_4^{\mathrm{nr}} = K_1^{\mathrm{nr}}$ donc que $LK_1^{\mathrm{nr}} = K_1^{\mathrm{nr}}$. Cela implique que LK_1 est ramifié de degré 3 donc contient l'unique extension de $\mathbf{Q}_3$ non ramifiée de degré 6 notée K_{u_6}. Le groupe de Galois de $LK_1/\mathbf{Q}_3$ est $\mathbf{Z}/3\mathbf{Z}\times\mathfrak{S}_3$ or l'unique quotient isomorphe à $\mathbf{Z}/6\mathbf{Z}$ de ce groupe est obtenu comme groupe de Galois du compositum $K_1K_{u_2}$ avec K_{u_2} l'extension non ramifiée de degré 2 qui est incluse dans L. Cette dernière extension n'est pas non ramifiée ce qui est absurde. Le groupe d'inertie de LK_1 est donc $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ et $K_4^{\mathrm{nr}}K_1^{\mathrm{nr}}$ est une extension de degré 9 de $\mathbf{Q}_3^{\mathrm{nr}}$.

Cette étude donne avec le théorème 2.3.4 qu'il existe une extension K de $\mathbf{Q}$ de degré 9 telle que toute courbe elliptique E avec $\Phi_{E,3} = \mathbf{Z}/3\mathbf{Z}$ vérifie E_K est semi-stable.

On peut de plus vérifier que les courbes

$$E_1\colon y^2 + xy + y = x^3 - x^2 + 4x - 1,\ \Delta = -1\cdot 2^6\cdot 3^4$$

et

$$E_2\colon y^2 + xy + y = x^3 - x^2 + 5x + 5,\ \Delta = -1\cdot 2^3\cdot 3^4$$

ont pour type respectivement K_1^{nr} et K_4^{nr} en 3 ce qui assure que cette extension est de degré minimal.

Chapitre 3

Variétés abéliennes principalement polarisées avec $d(A)$ maximal

3.1 Introduction

Dans le chapitre précédent, on a relié les groupes de monodromie finie d'une variété abélienne A sur un corps de nombres K à la valeur de $d(A)$. On va ici s'intéresser au comportement géométrique de ces groupes, c'est-à-dire leur comportement dans les fibres d'un schéma abélien. On considère pour cela le revêtement fini étale $A[\ell] \to S$ donné par la ℓ-torsion d'un schéma abélien. On montre d'abord par une construction directe, puis par la théorie du groupe fondamental étale l'existence de recouvrements analytiques des K_v-points de S pour toute place $v \in \Sigma_K$ pour lesquels les groupes de monodromie finie des fibres de $A \to S$ sont constants sur les ouverts du recouvrement. En particulier pour une base S qui vérifie l'approximation faible, on peut trouver des fibres avec monodromie finie prescrite en un nombre fini de places. L'existence de tels recouvrements pour les topologies p-adiques de la base d'un schéma abélien constitue le théorème suivant.

Théorème 3.1.1. *Soient $A \to S$ un schéma abélien avec S de type fini sur un corps de nombres K et $v \in \Sigma_K$. Alors il existe des groupes finis $G_1, \ldots, G_n$ et un recouvrement fini de $S(K_v)$ par des ouverts disjoints $U_1, \ldots, U_n$ tels que pour tout $s \in S(K_v)$ on a*

$$s \in U_i \iff \Phi_{A_s,v} \simeq G_i.$$

En particulier, si L/K est une extension finie et $w \mid v$ une place de L telle que $L_w \simeq K_v$ alors pour un point $s \in S(L)$ on a

$$s \in U_i \iff \Phi_{A_s,w} \simeq G_i.$$

Pour utiliser ce théorème et en déduire le résultat 3 de l'introduction, l'objet naturel à considérer serait un espace des modules des variétés abéliennes de dimension g fixée. Comme un tel objet n'existe pas dans la catégorie des schémas, on utilise l'espace des modules des variétés abéliennes de dimension g principalement polarisées et linéairement rigidifiées H_g dont on rappelle la construction en partie 3.3. Une autre approche consiste à considérer le champ $\mathcal{A}_g$ des variétés abéliennes principalement polarisées de dimension g ce que l'on fait en partie 3.5.

Comme l'approximation faible n'est connue pour aucun de ces deux espaces, on utilise un lemme qui donne une sorte d'approximation faible à extension finie près se reposant sur un résultat d'Ekedahl pour pallier ce défaut, ce qui explique la présence d'une extension finie L/K non contrôlée dans l'énoncé du résultat 3. La démonstration de ce lemme et du théorème principal de ce chapitre font l'objet de la partie 3.4. Ce dernier donne l'existence de variétés abéliennes avec $d(A)$ maximal relativement à un corps de nombres K. Pour cela on introduit la notation

$$d_g(K) = \operatorname*{ppcm}_{B/K,\ p.p.,\ \dim B=g} d(B).$$

On est finalement en mesure d'énoncer le théorème principal de ce chapitre, qui correspond au résultat 3 de l'introduction.

Théorème 3.1.2. *Pour tout corps de nombres K et tout entier non nul g, il existe une extension finie L/K et une variété abélienne A principalement polarisée de dimension g sur L telle que*

$$d(A) = d_g(K).$$

3.2 Des recouvrements analytiques d'un schéma abélien

3.2.1 Une construction directe

Dans cette partie, K est un corps de caractéristique nulle fixé. Le but est d'obtenir un raffinement du lemme de Krasner pour les revêtements finis étales énoncé dans [Po], proposition 3.5.74. On commence par rappeler la

construction de la clôture galoisienne d'un revêtement fini étale d'un schéma connexe.

Proposition 3.2.1. *Soient $S' \to S$ un revêtement fini étale de schémas sur K avec S connexe. Alors il existe un revêtement galoisien $T \to S$ tel que pour tout point $s \in S(L)$ pour un corps L contenant K et $\overline{s} \in S(\overline{L})$ point géométrique au-dessus de s on ait les propriétés suivantes.*

(i) L'ensemble $\mathrm{Hom}_S(T, S')$ s'identifie à la fibre géométrique $S' \times_S \overline{s}$ par tout choix de point dans cette fibre.

(ii) L'action naturelle de $\mathrm{Aut}_S T$ sur $S' \times_S \overline{s}$ induite par tout choix comme dans (i) est fidèle.

(iii) L'action de G_L sur $S' \times_S \overline{s}$ se factorise par $\mathrm{Aut}_S T$ par tout choix comme dans (i), c'est-à-dire elle est donnée par un morphisme

$$\varphi_s \colon G_L \to \mathrm{Aut}_S T$$

et différents choix de points dans la fibre donnent des morphismes conjugués.

Démonstration. Soient $s \in S(L)$ et $\overline{s} \in S(\overline{L})$ comme dans l'énoncé. On note $a_1, \ldots, a_n$ les points de la fibre géométrique $S' \times_S \overline{s}$. Soit Y le produit fibré de S' avec lui-même sur S pris n fois muni des projections $p_1, \ldots, p_n \colon Y \to S'$. Le point géométrique $\overline{a} = (a_1, \ldots, a_n) \in Y \times_S \overline{s}$ définit un point $a \in Y$ dont on note C la composante connexe et $\iota \colon C \to Y$ l'inclusion. Les morphismes $p_1 \circ \iota, \ldots, p_n \circ \iota$ définissent tous des éléments de l'ensemble $\mathrm{Hom}_S(C, S')$ et vérifient de plus $p_i \circ \iota(\overline{a}) = a_i$ ce qui fait que l'application d'évaluation

$$\begin{array}{rccc} ev_{\overline{a}} \colon & \mathrm{Hom}_S(C, S') & \longrightarrow & S' \times_S \overline{s} \\ & f & \longmapsto & f(\overline{a}) \end{array}$$

est surjective. Par ailleurs on sait par la théorie générale que deux morphismes de revêtements finis étales qui coïncident en un point géométrique sont égaux sur une composante connexe ce qui assure que $ev_{\overline{a}}$ est aussi injective donc bijective.

On va maintenant montrer que le revêtement $C \to S$ est galoisien, c'est-à-dire que l'action de $\mathrm{Aut}_S C$ sur la fibre $C \times_S \overline{s}$ est libre et transitive. Du fait que C est connexe, la remarque précédente assure que l'action est libre. On montre qu'elle est transitive. Soit $\overline{a'} \in C \times_S \overline{s}$. L'application d'évaluation

$$\begin{array}{rccc} ev_{\overline{a'}} \colon & \mathrm{Hom}_S(C, S') & \longrightarrow & S' \times_S \overline{s} \\ & f & \longmapsto & f(\overline{a'}) \end{array}$$

est injective pour les mêmes raisons que précédemment donc bijective car entre ensembles de même cardinal. Comme on sait de plus que $\mathrm{Hom}_S(C, S') = \{p_1 \circ \iota, \ldots, p_n \circ \iota\}$ on a $\overline{a'} = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ pour une permutation $\sigma \in \mathfrak{S}_n$. Cette permutation σ définit un automorphisme de Y par permutation des facteurs et comme $\overline{a'} \in \sigma(C)$ on a $\sigma(C) = C$. Il suit que σ se restreint à un automorphisme $\sigma \in \mathrm{Aut}_S C$ qui vérifie $\sigma(\overline{a}) = \overline{a'}$ et l'action est transitive.

On montre maintenant la propriété (ii). Soit $g \in \mathrm{Aut}_S C$ qui agit trivialement sur $\mathrm{Hom}_S(C, S')$. Alors pour tout $i \in \{1, \ldots, n\}$ on a

$$p_i \circ \iota(g(\overline{a})) = a_i$$

d'où $g(\overline{a}) = \overline{a}$ et $g = \mathrm{id}_C$.

Pour la propriété (iii), l'action galoisienne de G_L sur $C \times_S \overline{s}$ se fait sur le deuxième facteur donc commute à celle de $\mathrm{Aut}_S C$ qui se fait sur le premier facteur. Comme cette dernière est libre et transitive, le choix du point $\overline{a} \in C \times_S \overline{s}$ induit un morphisme $\varphi_s \colon G_L \to \mathrm{Aut}_S C$ qui factorise l'action galoisienne. Précisément, pour $\sigma \in G_L$ et $b \in C \times_S \overline{s}$ on a

$$\sigma \cdot b = \varphi_s(\sigma) \cdot b$$

où dans le terme de gauche l'action est galoisienne et dans le terme de droite l'action naturelle provient de $\mathrm{Aut}_S C$. Par construction différents choix de points induisent des morphismes conjugués.

Maintenant pour $f \in \mathrm{Hom}_S(C, S')$ et $\sigma \in G_L$ le diagramme suivant commute

$$\begin{array}{ccc} C \times_S \overline{s} & \xrightarrow{\sigma} & C \times_S \overline{s} \\ \downarrow f & & \downarrow f \\ S' \times_S \overline{s} & \xrightarrow{\sigma} & S' \times_S \overline{s}. \end{array}$$

ce qui s'écrit $\sigma(f(\overline{a})) = f(\sigma(\overline{a}))$ ou encore $\varphi_s(\sigma)(f)(\overline{a}) = \sigma(f(\overline{a}))$ par définition de φ_s.

Il reste à vérifier que cette construction est indépendante du choix des points $s \in S(L)$ et $\overline{s} \in S(\overline{L})$. On considère pour cela des points $t \in S(L)$ et $\overline{t} \in S(\overline{L})$ comme dans l'énoncé. La même construction donne un revêtement galoisien $T \to S$ qui vérifie les propriétés $(i), (ii)$ et (iii) vis-à-vis de t et $\overline{t}$. Le fait que S est connexe assure que le cardinal de la fibre $S' \times_S \overline{t}$ est encore n et que toute composante connexe de S' s'envoie surjectivement sur S. On pose $S' \times_S \overline{t} = \{b_1, \ldots, b_n\}$ et on suppose, quitte à renuméroter, que b_1 est dans la même composante connexe de S' que a_1. Soit $\pi_1 \in \mathrm{Hom}_S(T, S')$ tel que $\pi_1(\overline{b}) = b_1$ pour un $\overline{b} \in T(\overline{L})$ et soient $\pi_2, \ldots, \pi_n$ les autres éléments de $\mathrm{Hom}_S(T, S')$. Le morphisme π_1 est une surjection de T sur la composante

connexe de S' contenant b_1 donc il existe $\overline{c} \in T(\overline{L})$ tel que $\pi_1(\overline{c}) = a_1$. Comme précédemment l'application d'évaluation

$$\begin{array}{rccc} ev_{\overline{c}}\colon & \mathrm{Hom}_S(T, S') & \longrightarrow & S' \times_S \overline{s} \\ & f & \longmapsto & f(\overline{c}) \end{array}$$

est bijective. Quitte à renuméroter, les morphismes $\pi_1, \ldots, \pi_n$ définissent un morphisme $\eta\colon T \to Y$ tel que $p_i \circ \eta = \pi_i$ et

$$\pi_i \circ \eta(\overline{c}) = a_i.$$

On en déduit que $\eta(\overline{c}) = \overline{a}$ et que $\eta(T) = C$. Réciproquement on obtient un morphisme $C \to T$ et donc $T \simeq C$. □

Dans la suite, pour un revêtement fini étale $S' \to S$ avec S connexe on notera $T \to S$ un revêtement galoisien vérifiant les propriétés de la proposition et pour tout L-point s de S on dispose du morphisme φ_s. Pour un sous-groupe $H \subset \mathrm{Aut}_S T$ on note $\pi_H\colon T_H \to S$ le revêtement quotient associé à H par correspondance de Galois. Les deux lemmes suivants permettent de définir un recouvrement analytique de la base S avec de bonnes propriétés à partir d'ouverts obtenus des morphismes π_H pour H variant.

Lemme 3.2.2. *Soient $S' \to S$ un revêtement fini étale de schémas sur K avec S connexe et L/K une extension de corps. Alors pour tout $s \in S(L)$ on a un isomorphisme*

$$G_L/\operatorname{Ker}\varphi_s \simeq \mathrm{Gal}(L(S'_s(\overline{L}))/L).$$

Démonstration. Par définition le groupe de Galois $\mathrm{Gal}(L(S'_s(\overline{L}))/L)$ est le quotient $G_L/\operatorname{Ker}\rho_s$ où $\rho_s\colon G_L \to \mathrm{Aut}\, S' \times_s \overline{s}$ est l'action de Galois. Par la propriété (iii) de T cette action se factorise par $\varphi_s\colon G_L \to \mathrm{Aut}_S T$ et par (ii) l'action de $\mathrm{Aut}_S T$ sur $S' \times_s \overline{s}$ est fidèle. Il suit l'égalité $\operatorname{Ker}\rho_s = \operatorname{Ker}\varphi_s$ et donc l'isomorphisme annoncé. □

Lemme 3.2.3. *Soient $S' \to S$ un revêtement fini étale de schémas sur K et L/K une extension de corps. Soient $s \in S(L)$ et $H \subset \mathrm{Aut}_S T$ un sous-groupe. Alors, la fibre $T_H \times_S s$ a un L-point si et seulement s'il existe $g \in \mathrm{Aut}_S T$ tel que $\operatorname{Im}\varphi_s \subset gHg^{-1}$.*

Démonstration. On commence par identifier la fibre $T_H \times \overline{s}$ et $\mathrm{Hom}_S(T, T_H)$. L'action de G_L sur cette fibre se fait par φ_s par (iii) et le stabilisateur du morphisme canonique $p_H\colon T \to T_H$ sous l'action naturelle de $\mathrm{Aut}_S T$ est H par construction. Comme cette action est transitive (T_H étant connexe) le

stabilisateur de tout élément de la fibre géométrique est conjugué à H. On peut maintenant démontrer l'équivalence.

Un L-point de $T_H \times_S s$ correspond à un élément de $\mathrm{Hom}_S(T_H, T)$ stable sous l'action de G_L. Cela donne que l'image de φ_s est contenue dans le stabilisateur de cet élément donc dans un conjugué de H. Réciproquement, si l'image de φ_s est incluse dans un conjugué gHg^{-1} de H pour un $g \in \mathrm{Aut}_S T$ alors $g \cdot p_H$ donne un élément de la fibre géométrique fixé par l'action de Galois donc un L-point. □

On peut maintenant construire les revêtements analytiques qui constituent le résultat principal de cette partie.

Théorème 3.2.4. *Soient $S' \to S$ un revêtement fini étale de schémas de type fini sur K et L/K un corps local. Alors il existe des groupes finis $H_1, \ldots, H_n$ et un recouvrement fini de $S(L)$ par des ouverts disjoints $U_1, \ldots, U_n$ tels que pour tout $i \in \{1, \ldots, n\}$ et tout $s \in S(L)$*

$$s \in U_i \iff \mathrm{Gal}(L(S'_s(\overline{L}))/L) \simeq H_i.$$

Démonstration. Il suffit de démontrer le théorème pour chaque composante connexe de S (quitte éventuellement à regrouper certains ouverts) donc on suppose S connexe et on utilise les notations précédentes.

Pour un sous-groupe $H \subset \mathrm{Aut}_S T$ on définit le sous-ensemble

$$\widetilde{U}_H = \pi_H(T_H(L)) \setminus \bigcup_{G \subsetneq H} \pi_G(T_G(L))$$

de $S(L)$. Comme les morphismes π_H pour $H \subset \mathrm{Aut}_S T$ sont finis étales, ils induisent des applications ouvertes et fermées pour les topologies analytiques sur $T_H(L)$ et $S(L)$. Les ensembles $\widetilde{U}_H$ sont donc ouverts et la famille obtenue en considérant tous les sous-groupes de $\mathrm{Aut}_S T$ est un recouvrement par construction.

On choisit maintenant des représentants $H_1, \ldots, H_n$ des classes d'isomorphismes des sous-groupes de $\mathrm{Aut}_S T$ et on pose

$$U_i = \bigcup_{\substack{H' \subset \mathrm{Aut}_S T \\ H' \simeq H_i}} \widetilde{U}_{H'}.$$

On démontre maintenant l'équivalence

$$s \in U_i \iff \mathrm{Im}\, \varphi_s \simeq H_i$$

pour $s \in S(L)$. Par définition si $s \in U_i$ alors $s \in \widetilde{U}_H$ pour un sous-groupe $H \subset \mathrm{Aut}_S T$ isomorphe à H_i. Le lemme 3.2.3 assure alors que $\mathrm{Im}\,\varphi_s \subset gHg^{-1}$ pour un $g \in \mathrm{Aut}_S T$ car la fibre $T_H \times_S s$ a un L-point. Par l'absurde, si on a une inclusion $\mathrm{Im}\,\varphi_s \subset gGg^{-1}$ pour un sous-groupe $G \subsetneq H$ alors le même lemme donne que la fibre $T_G \times_S s$ a un L-point et donc $s \in \pi_G(T_G(L))$ ce qui est exclu par définition de $\widetilde{U}_H$. Inversement, on suppose $\mathrm{Im}\,\varphi_s \simeq H_i$. On note H l'image de φ_s. À nouveau par le lemme 3.2.3 la fibre $T_H \times_S s$ a un L-point et s n'est l'image d'aucun L-point provenant d'un revêtement T_G pour $G \subsetneq H$ ce qui donne $s \in \widetilde{U}_H \subset U_i$.

L'équivalence montre par ailleurs que les ouverts U_i sont disjoints.

On conclut la preuve par le lemme 3.2.2 qui donne

$$\mathrm{Im}\,\varphi_s \simeq H_i \iff G_L/\mathrm{Ker}\,\varphi_s \simeq H_i \iff \mathrm{Gal}(L(S'_s(\overline{L}))/L) \simeq H_i.$$

□

On termine cette partie par un raffinement qui consiste à remplacer le recouvrement précédent par un recouvrement qui n'est plus nécessairement fini mais pour lequel les fibres ont des corps de définition constants et pas seulement leur groupe de Galois.

Théorème 3.2.5. *Soient $S' \to S$ un revêtement fini étale de schémas de type fini sur K et L/K un corps local. Alors il existe un recouvrement par des ouverts disjoints $(U_{L'})_{L'/L galoisienne}$ de $S(L)$ tel que si $s \in U_{L'}$ alors les points de la fibre S'_s sont définis sur L'.*

Démonstration. Soit L'/L une extension galoisienne. Soit $H \subset \mathrm{Aut}_S T$ un sous-groupe. On note V_H l'ouvert de $S(L')$ correspondant à la classe d'isomorphie de ce sous-groupe par le théorème 3.2.4. Comme $\iota_{L'} \colon L \hookrightarrow L'$ est une injection continue, l'ouvert $\iota_{L'}^{-1}(V_{\{1\}})$ de $S(L)$ est tel que si $s \in \iota_{L'}^{-1}(V_{\{1\}})$ alors $L(S'_s) \subset L'$.

Pour $L' = L$ on pose

$$U_L = V_{\{1\}}$$

et, par récurrence,

$$U_{L'} = \iota_{L'}^{-1}(V_{\{1\}}) \setminus \bigcup_{K \subsetneq M \subsetneq L} U_M$$

sinon.

Par une récurrence directe on obtient que $U_{L'}$ est ouvert et fermé dans $S(L)$. □

3.2.2 Par la théorie du groupe fondamental étale

La théorie du groupe fondamental étale est développée dans [SGA1]. On va montrer que l'on retrouve naturellement le théorème 3.2.4 dans ce cadre. Ceci sera utile en partie 5. Pour un schéma quasi-compact et géométriquement connexe S sur un corps K il est démontré l'existence de la suite exacte d'homotopie, pour un choix $\overline{x}$ de point géométrique de S

$$1 \longrightarrow \pi_1^{\text{ét}}(S_{\overline{K}}, \overline{x}) \longrightarrow \pi_1^{\text{ét}}(S, \overline{x}) \longrightarrow G_K \longrightarrow 1.$$

La fonctorialité de la construction donne, pour une extension de corps L/K et un L-point $s \in S(L)$, un diagramme commutatif

$$\begin{array}{ccccccccc} & & & & \pi_1^{\text{ét}}(S_L, \overline{s}) & \longleftarrow & G_L & & \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pi_1^{\text{ét}}(S_{\overline{K}}, \overline{x}) & \longrightarrow & \pi_1^{\text{ét}}(S, \overline{x}) & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

On note $s_* \colon G_L \to \pi_1^{\text{ét}}(S, \overline{x})$ le morphisme obtenu ainsi.

On fixe maintenant un revêtement fini étale $S' \to S$, un point $s \in S(L)$ et un point géométrique $\overline{s} \in S(\overline{L})$. Par définition $\pi_1^{\text{ét}}(S, \overline{x})$ agit sur la fibre géométrique $S' \times_S \overline{s}$ par un morphisme $\varphi \colon \pi_1^{\text{ét}}(S, \overline{x}) \to \operatorname{Aut}_S T$. On retrouve alors le morphisme φ_s de la partie précédente par l'égalité $\varphi_s = \varphi \circ s_*$.

On pourrait donc considérer l'application $S(L) \to \operatorname{Hom}(G_L, \operatorname{Aut}_S T)$ qui associe à un point $s \in S(L)$ le morphisme φ_s mais pour notre propos il suffit de montrer la continuité de l'application $S(L) \to \operatorname{Sub} \operatorname{Aut}_S T$ à valeurs dans l'ensemble des sous-groupes de $\operatorname{Aut}_S T$ à conjugaison près qui à s associe l'image de φ_s. On va préciser cette construction en commençant par définir une topologie sur l'espace des sous-groupes fermés d'un groupe profini.

Soit G un groupe profini. On note $\operatorname{Sub} G$ l'ensemble des sous-groupes fermés de G (pouvant être à conjugaison par un sous-groupe fermé près). Cet ensemble est muni naturellement d'une structure d'espace profini par la bijection

$$\operatorname{Sub} G \simeq \varprojlim_{\varphi \colon G \to H} \operatorname{Sub} H$$

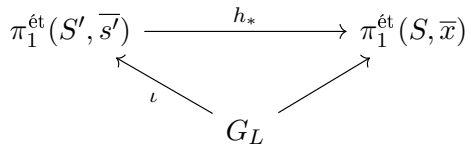
où φ est une surjection sur un groupe fini H et les ensembles $\operatorname{Sub} H$ sont munis de la topologie discrète.

Dans le but d'obtenir la proposition 3.2.8, on rappelle la démonstration du fait que le morphisme de Kummer profini

$$\kappa \colon S(L) \to \operatorname{Sub} \pi_1^{\text{ét}}(S_L, \overline{s})$$

est continu pour un corps local L (voir le paragraphe 16.2 de [St]).

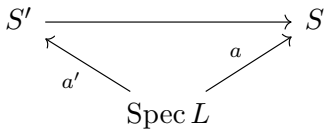
Pour cela on introduit l'espace des sections de la suite exacte $\mathcal{S}_{\pi_1^{\text{ét}}}(S/L)$, sous-espace de l'espace profini des fermés de $\pi_1^{\text{ét}}(S_L, \overline{s})$ à conjugaison près par $\pi_1^{\text{ét}}(S_{\overline{L}}, \overline{x})$ composé des fermés images d'une section $G_L \to \pi_1^{\text{ét}}(S_L, \overline{s})$. Cet espace est muni de la topologie induite dont on a une description plus concrète dans [St]. Une base d'ouverts est donnée par les images des morphismes h_* induits sur les espaces de sections pour un revêtement fini étale géométriquement connexe $h\colon S' \to S$. Le diagramme est le suivant.



La continuité se déduira du lemme suivant.

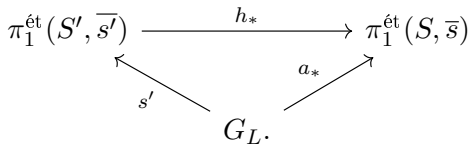
Lemme 3.2.6. *Soient $a \in S(L)$ et $U_h \subset \mathcal{S}_{\pi_1^{ét}}(S/L)$ un ouvert correspondant à $h\colon S' \to S$. Alors on a $a_* \in U_h$ si et seulement s'il existe $a' \in S'(L)$ avec $h(a') = a$.*

Démonstration. Le sens réciproque est clair par le triangle commutatif



et la fonctorialité de la construction.

Maintenant si $a_* \in U_h$ alors il existe une section s' telle que le triangle suivant commute



De plus h_* est un isomorphisme sur un sous-groupe ouvert $U \subset \pi_1^{\text{ét}}(S, \overline{s})$ qui contient l'image de a_*. Le revêtement étale h correspond au $\pi_1^{\text{ét}}(S, \overline{s})$-ensemble $\pi_1^{\text{ét}}(S, \overline{s})/U$ et la fibre de h en a est un revêtement étale de $\operatorname{Spec} L$ déduit de S' par tiré en arrière par $a\colon \operatorname{Spec} L \to S$. Il suit que cette fibre est donnée par le $\operatorname{Gal}(\overline{L}/L)$-ensemble $\pi_1^{\text{ét}}(S, \overline{s})/U$ où $\operatorname{Gal}(\overline{L}/L)$ agit par a_*. L'élément $\overline{1}$ de cet ensemble est donc fixé par cette action ce qui correspond à un point L-rationnel dans la fibre $h^{-1}(a)$, donc l'existence de a'. □

Corollaire 3.2.7. *L'application de Kummer profini*

$$\kappa\colon S(L) \longrightarrow \mathcal{S}_{\pi_1^{\acute{e}t}}(S/L)$$

est continue.

Démonstration. Soient $a \in S(L)$ et a_* son image par κ. Soit $h\colon S' \to S$ un revêtement étale fini géométriquement connexe tel que U_h est un voisinage ouvert de a_*. Alors par définition on a

$$\kappa^{-1}(U_h) = \{s \in S(L) \mid s_* \in U_h\}$$

et par le lemme

$$\begin{aligned}\kappa^{-1}(U_h) &= \{s \in S(L) \mid \exists s' \in S'(L),\ h(s') = s\} \\ &= h(S'(L)).\end{aligned}$$

Or h est étale donc ouverte sur les L-points, voir par exemple [Po] proposition 3.5.73. □

Le passage de $\mathcal{S}_{\pi_1^{\acute{e}t}}(S/L)$ à $\operatorname{Sub}\pi_1^{\text{ét}}(S_L, \overline{s})$ se déduit simplement du fait que l'application quotient des fermés à conjugaison près par $\pi_1^{\text{ét}}(S_{\overline{L}}, \overline{s})$ sur $\operatorname{Sub}\pi_1^{\text{ét}}(S_L, \overline{s})$ est continue.

Proposition 3.2.8. *Pour un corps local L/K, l'application*

$$S(L) \longrightarrow \operatorname{Sub}\operatorname{Aut}_S T$$

est continue.

Démonstration. D'après ce qui précède le morphisme de Kummer profini $\kappa\colon S(L) \to \operatorname{Sub}\pi_1^{\text{et}}(S_L, \overline{s})$ est continu. Or notre application est donnée par la composition de κ et des flèches naturelles et continues

$$\operatorname{Sub}\pi_1^{\text{ét}}(S_L, \overline{s}) \to \operatorname{Sub}\pi_1^{\text{ét}}(S, \overline{x}) \to \operatorname{Sub}\operatorname{Aut}_S T.$$

□

Le théorème 3.2.4 se déduit directement de cette proposition. En effet, un ouvert du recouvrement donné par le théorème est simplement l'image réciproque par $S(L) \to \operatorname{Sub}\operatorname{Aut}_S T$ d'une partie correspondant à tous les points d'une même classe d'isomorphisme.

3.3 Conséquences pour un schéma abélien

Pour un schéma abélien $A \to S$ donné, on dispose de revêtements finis étales de la base donnés par la n-torsion du schéma abélien notés $A[n] \to S$. La proposition 2.2.22 permet de retrouver le groupe de monodromie finie d'une fibre du schéma abélien à partir du revêtement de la ℓ-torsion pourvu que ℓ soit assez grand à partir du théorème 3.2.4.

Théorème 3.3.1. *Soient $A \to S$ un schéma abélien avec S sur un corps de nombres K et $v \in \Sigma_K$. Alors il existe des groupes finis $G_1, \ldots, G_n$ et un recouvrement fini de $S(K_v)$ par des ouverts disjoints $U_1, \ldots, U_n$ tels que pour tout $s \in S(K_v)$ on a*

$$s \in U_i \iff \Phi_{A_s,v} \simeq G_i.$$

En particulier, si L/K est une extension finie et $w \mid v$ une place de L telle que $L_w \simeq K_v$ alors pour un point $s \in S(L)$ on a

$$s \in U_i \iff \Phi_{A_s,w} \simeq G_i.$$

Démonstration. On note p la caractéristique résiduelle de v. Le théorème 3.2.4 appliqué au revêtement de la ℓ-torsion $A[\ell] \to S$ avec $\ell > \max(2\dim A + 1, p)$ et le corps local K_v^{nr} donne des groupes finis $H_1, \ldots, H_n$ ainsi qu'un recouvrement ouvert $(V_i)_{1 \leq i \leq n}$ de $S(K_v^{\mathrm{nr}})$ tel que

$$s \in V_i \iff \mathrm{Gal}(K_v^{\mathrm{nr}}(A_s[\ell])/K_v^{\mathrm{nr}}) \simeq H_i.$$

Par la proposition 2.2.22 le groupe de Galois $\mathrm{Gal}(K_v^{\mathrm{nr}}(A_s[\ell])/K_v^{\mathrm{nr}})$ est isomorphe à $\Phi_{A_s,v}$ ou $\Phi_{A_s,v} \times \mathbf{Z}/\ell\mathbf{Z}$ et ℓ ne divise pas $\mathrm{Card}\,\Phi_{A,v}$. Pour les $i \in \{1, \ldots, n\}$ tels que $\mathbf{Z}/\ell\mathbf{Z}$ est un facteur direct de H_i on pose $G_i = H_i/(\mathbf{Z}/\ell\mathbf{Z})$ et on pose $G_i = H_i$ pour les indices restants. De plus, on pose

$$U_i^{\mathrm{nr}} = \bigcup_{G_j \simeq G_i} V_j$$

et on considère la famille d'ouverts $(U_i)_{1 \leq i \leq r}^{\mathrm{nr}}$ où les redondances sont retirées de manière à ce qu'on ait

$$s \in U_i^{\mathrm{nr}} \iff \Phi_{A_s,v} \simeq G_i$$

pour tout $s \in S(K_v^{\mathrm{nr}})$.

Comme l'injection $S(K_v) \hookrightarrow S(K_v^{\mathrm{nr}})$ est continue, le recouvrement donné par $U_i = U_i^{\mathrm{un}} \cap S(K_v)$ est un recouvrement ouvert et celui-ci convient. □

Une conséquence est que pour un schéma abélien de base S vérifiant l'approximation faible on peut choisir des fibres avec monodromie finie prescrite en un nombre fini de places.

Corollaire 3.3.2. *Soient $A \to S$ un schéma abélien de type fini sur K avec S vérifiant l'approximation faible et $v_1, \ldots, v_n \in \Sigma_K$ des places distinctes. Soient $s_i \in S(K_{v_i})$ des K_{v_i}-points de S. Alors il existe un point $s \in S(K)$ tel que pour tout i on a un isomorphisme*

$$\Phi_{A_s, v_i} \simeq \Phi_{A_{s_i}, v_i}.$$

Le théorème 3.2.5 donne de la même façon (avec la proposition 2.2.22) le théorème suivant dans le contexte d'un schéma abélien.

Théorème 3.3.3. *Soient $A \to S$ un schéma abélien sur un corps de nombres K et v une place non archimédienne de K. Alors il existe un recouvrement par des ouverts disjoints $(U_L)_{L/K_v^{\mathrm{nr}} \text{ finie galoisienne}}$ de $S(K_v^{\mathrm{nr}})$ tels que si $s \in U_L$ alors la plus petite extension de K_v^{nr} sur laquelle A_s atteint réduction semi-stable est L.*

Par la digression en fin du chapitre 2 on retrouve un recouvrement fini au niveau des complétions d'un corps de nombres.

Corollaire 3.3.4. *Soient $A \to S$ un schéma abélien sur un corps de nombres K et v une place non archimédienne de K. Alors il existe un recouvrement fini par des ouverts disjoints $(U_L)_{L/K_v^{\mathrm{nr}} \text{ finie galoisienne}}$ de $S(K_v)$ tels que si $s \in U_L$ alors la plus petite extension de K_v^{nr} sur laquelle A_s atteint réduction semi-stable est L.*

Démonstration. On considère le recouvrement de $S(K_v)$ obtenu par tiré en arrière de celui obtenu par le théorème 3.3.3 par l'inclusion continue $S(K_v) \hookrightarrow S(K_v^{\mathrm{nr}})$. C'est un recouvrement de $S(K_v)$ par des ouverts disjoints vérifiant la propriété voulue. Il suffit de voir que seul un nombre fini des ouverts obtenus ainsi sont non vides. Cela vient du fait vu au chapitre 2 qu'il n'existe qu'un nombre fini d'extensions de K_v^{nr} qui sont le type d'obstruction à la réduction semi-stable d'une variété abélienne de dimension donnée sur K_v. □

On termine cette partie par un exemple de schéma elliptique sur la droite affine privée de 0.

Exemple 3.3.5. On considère le schéma abélien de dimension 1 sur $\mathbf{A}^1_{\mathbf{Q}} \setminus \{0\}$ donné par l'équation

$$E\colon y^2 = x^3 + t.$$

Le schéma $\mathbf{A}^1_{\mathbf{Q}} \setminus \{0\} = S$ est connexe et de type fini. Soit $\overline{s}\colon \overline{\mathbf{Q}} \to S$ un point géométrique au dessus d'un $\mathbf{Q}$-point $s \in S$. La suite exacte d'homotopie donne

$$0 \longrightarrow \widehat{\mathbf{Z}} \longrightarrow \pi_1(S, \overline{s}) \longrightarrow \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow 1$$

et on a de plus une section de cette suite par le morphisme induit par $s\colon \operatorname{Spec}\mathbf{Q} \to S$. Le groupe fondamental $\pi_1(S, \overline{s})$ est isomorphe au produit semi-direct

$$\widehat{\mathbf{Z}} \rtimes \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}).$$

On peut alors vérifier que l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $\widehat{\mathbf{Z}}$ se fait par le caractère cyclotomique χ.

Pour tout point $s \in S(\mathbf{Q})$ la courbe elliptique E_s fibre de E en s a pour équation de Weierstrass

$$y^2 = x^3 + s$$

d'où un discriminant $\Delta_{E_s} = -16 \cdot 27 \cdot s^2 = -2^4 \cdot 3^3 s^2$ et un j-invariant nul. On a de plus les invariants standards $c_4 = 0$ et $c_6 = 2^5 \cdot 3^3 \cdot s$.

On s'intéresse à la réduction en 2 et 3 des courbes elliptiques de la famille E. Le fait que $j = 0$ assure qu'il y a bonne réduction potentielle en 2 et 3. On commence par la réduction en 3. La table page 356 de [Kr] donne le groupe de monodromie finie de E_s en fonction des valuations 3-adiques de Δ_{E_s}, c_4 et c_6 ainsi que de certaines congruences modulo 9. Plus précisément, si $v_3(s) = 0$ on a $\Phi_{E_s,3} = \mathbf{Z}/4\mathbf{Z}$ si $s \equiv 1$ ou $8 \mod 9$ et $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$ sinon. Si $1 \leq v_3(s) \leq 4$ on a $\Phi_{E_s,3} = \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$ sauf si $v_3(s) = 3$. Dans ce dernier cas on a $\Phi_{E_s,3} = \mathbf{Z}/4\mathbf{Z}$ si, en notant $s = u3^3$, on a $u \equiv 1$ ou $8 \mod 9$. L'ouvert correspondant à $\mathbf{Z}/4\mathbf{Z}$ par le théorème 3.3.1 contient les boules ouvertes $1 + 9\mathbf{Z}_3$, $8 + 9\mathbf{Z}_3$, $3^3 + 3^5\mathbf{Z}_3$ et $8 \cdot 3^3 + 3^5\mathbf{Z}_3$. Pour s de valuations plus grandes (ou négatives) l'équation n'est plus minimale de Weierstrass et il faut d'abord trouver un modèle minimal ce qui n'est pas l'objet ici.

Pour la réduction en 2 on regarde le tableau page 358–359 de [Kr]. L'équation est minimale si $-2 \leq v_2(s) \leq 4$. On traite quelques unes des possibilités.

$v_2(s) = 0$: $\Phi_{E_s,2} = \mathbf{Z}/3\mathbf{Z}$ si $s \equiv 1 \mod 4$ et $\Phi_{E_s,2} = \mathbf{Z}/6\mathbf{Z}$ sinon.

$v_2(s) = 1$: $\Phi_{E_s,2} = \mathbf{Z}/2\mathbf{Z}$.

$v_2(s) = 2$: $\Phi_{E_s,2} = \mathbf{Z}/3\mathbf{Z}$ si $\frac{s}{2^2} \equiv -1 \mod 4$ et $\Phi_{E_s,2} = \mathrm{SL}_2(\mathbf{F}_3)$ sinon.

De la même manière que pour $p = 3$ ces conditions donnent des boules ouvertes incluses dans les ouverts du recouvrement obtenu par le théorème 3.3.1.

On peut alors directement choisir des courbes elliptiques avec monodromie finie en 2 et 3 prescrite dans la liste des possibilités. Par exemple la courbe

$$E_4 \colon y^2 = x^3 + 4$$

a monodromie finie maximale en 2 et 3, i.e. $\Phi_{E_4,2} = \mathrm{SL}_2(\mathbf{F}_3)$ et $\Phi_{E_4,3} = \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$.

3.4 Construction d'un schéma abélien universel

Pour déduire de la partie précédente le théorème principal de ce chapitre on a besoin d'un schéma abélien universel. Un tel schéma qui convient pour nous est construit dans [GIT] au chapitre 7, on discutera en partie 5 de ce chapitre de l'idée, plus naturelle, de considérer l'espace des modules des variétés abéliennes principalement polarisées de dimension fixée. On rappelle ici la construction de ce schéma par Mumford pour obtenir un espace des modules des schémas abéliens principalement polarisés avec rigidification linéaire. Ce dernier terme sera défini après quelques lemmes préliminaires sur les schémas abéliens et leurs faisceaux amples.

On commence par rappeler des résultats sur les polarisations et faisceaux bien connus (voir [GIT], [Mu] et [MGE] pour les preuves). Ceux-ci permettent l'obtention d'un faisceau très ample associé à une polarisation d'un schéma abélien. Pour cela on considère une variété abélienne X sur un corps K.

Théorème 3.4.1. *Pour tout faisceau L ample sur X, $L^{\otimes n}$ est très ample pour $n \geq 3$.*

Pour une polarisation $\lambda \colon X \to \widehat{X}$ on définit un faisceau inversible sur X par

$$L^{\Delta}(\lambda) = (1_X, \lambda)^* \mathcal{P}$$

où $\mathcal{P}$ est le faisceau de Poincaré sur $X \times_K \widehat{X}$.

Pour un faisceau ample L on note ϕ_L la polarisation associée. On a le résultat suivant

Proposition 3.4.2. *Soit λ une polarisation sur X. Alors $\phi_{L^{\Delta}(\lambda)} = 2\lambda$.*

Proposition 3.4.3. *Soit λ une polarisation sur X. Alors il existe une extension finie séparable K'/K et un faisceau ample M sur $X_{K'}$ tel que $\phi_M = \lambda_{K'}$.*

On déduit des propositions précédentes que si λ est une polarisation sur X alors $L^{\Delta}(\lambda)^{\otimes 2}$ est très ample. En effet, après extension des scalaires à une

extension finie séparable K' de K, par la proposition précédente, il existe un N ample tel que $\phi_N = \lambda_{K'}$. Quitte à faire une extension finie supplémentaire on peut choisir N de manière à ce que l'on ait $L^\Delta(\lambda)_{K'} \simeq N^{\otimes 2}$. Il suit

$$L^\Delta(\lambda)_{K'}^{\otimes 2} \simeq N^{\otimes 4}$$

est très ample.

Proposition 3.4.4. *Soit $X \to S$ un schéma abélien projectif. Soit L un faisceau inversible sur X et relativement ample. Alors*

(i) $R^i\pi_*(L) = (0)$ pour $i > 0$.

(ii) $\pi_*(L)$ est localement libre sur S.

(iii) Le degré de la polarisation ϕ_L définie par L est r^2 où r est le rang de $\pi_*(L)$.

Finalement on a besoin du théorème plus difficile suivant.

Théorème 3.4.5. *Soit S un schéma connexe localement noethérien. Soient $\pi\colon X \to S$ un morphisme projectif lisse et $\varepsilon\colon S \to X$ une section de π. Si pour un point géométrique $\overline{s}$ de S la fibre géométrique $X_{\overline{s}}$ de π est une variété abélienne avec unité $\varepsilon(s)$ alors X est un schéma abélien sur S avec unité ε.*

Notre but est de construire un schéma qui serait un espace de modules pour des variétés abéliennes munies d'une structure supplémentaire qui permet de se ramener à un schéma de Hilbert classique. La notion de rigidification linéaire va jouer ce rôle.

Définition 3.4.6. Une rigidification linéaire d'un schéma abélien principalement polarisé (X, λ), $\pi\colon X \to S$ est un S-isomorphisme

$$\phi\colon \mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2})) \simeq \mathbf{P}^{4^g} \times S.$$

Pour que l'association

$$S \longmapsto \{X \to S \text{ p.p. de dimension } g \text{ et linéairement rigidifié}\}$$

soit fonctorielle il suffit de vérifier que la rigidification est stable par changement de base. Cela résulte d'abord du fait que si $T \to S$ est un morphisme alors $\lambda \times 1$ est une polarisation principale sur $X \times_S T$ et on a

$$L^\Delta(\lambda)^{\otimes 2} \otimes_{\mathcal{O}_S} \mathcal{O}_T = L^\Delta(\lambda \times 1)^{\otimes 2}.$$

Pour passer à la rigidification on utilise un lemme de géométrie algébrique qui, du fait que $R^1\pi_*(L^\Delta(\lambda)) = 0$, donne un isomorphisme canonique

$$f^*(\pi_*(L^\Delta(\lambda)^2)) \simeq \pi_{T*}(f_X^*(L^\Delta(\lambda)^2))$$

où les morphismes π, π_T, f et f_X proviennent du carré cartésien

$$\begin{array}{ccc} X \times_S T & \xrightarrow{\pi_T} & T \\ \downarrow{\scriptstyle f_X} & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{\pi} & S \end{array}$$

On en déduit un isomorphisme $\mathbf{P}(\pi_{T*}(f_X^*(L^\Delta(\lambda)^{\otimes 2})) \simeq \mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2})) \times_S T$ et donc $\phi \times 1 \colon \mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2})) \times_S T \to \mathbf{P}^{4g} \times T$ est une rigidification linéaire du schéma abélien principalement polarisé $(X \times_S T, \lambda \times 1)$.

On dispose donc d'un foncteur

$$\mathcal{H}_g \colon S \longmapsto \{X \to S \text{ p.p. de dimension } g \text{ et linéairement rigidifié}\}.$$

On va maintenant construire une transformation naturelle

$$\Phi \colon \mathcal{H}_g \longrightarrow \mathcal{H}\mathrm{ilb}^P_{\mathbf{P}^{4g}}$$

pour un polynôme P bien choisi dont on montre qu'elle est injective. On obtient donc $\mathcal{H}_g$ comme sous-foncteur du foncteur de points d'un schéma de Hilbert et il suffit alors de trouver un sous-schéma de celui-ci dont le foncteur de points coïncide avec $\mathcal{H}_g$ pour conclure quant à l'existence de l'espace de modules que l'on veut.

La transformation naturelle Φ vient du fait que $L^\Delta(\lambda)^{\otimes 2}$ étant relativement très ample, il induit une immersion fermée $X \hookrightarrow \mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2}))$ et la rigidification linéaire donne un diagramme commutatif

$$\begin{array}{ccccc} X & \xhookrightarrow{\iota} & \mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2})) & \xrightarrow{\phi} & \mathbf{P}^{4g} \times S \\ & {\scriptstyle \varepsilon}\nwarrow \quad \searrow{\scriptstyle \pi} & & \swarrow{\scriptstyle p_2} & \downarrow{\scriptstyle p_1} \\ & & S & & \mathbf{P}^{4g} \end{array}$$

On obtient un sous-schéma fermé de $\mathbf{P}^{4g} \times S$ plat sur S de polynôme de Hilbert $4^g X^g$ et ainsi le morphisme Φ. Dans la suite on note Y le schéma $\mathbf{P}(\pi_*(L^\Delta(\lambda)^{\otimes 2}))$ pour simplifier l'écriture.

Proposition 3.4.7. *La transformation naturelle Φ est injective.*

Démonstration. Il faut voir que la structure de schéma abélien linéairement rigidifié est uniquement déterminée à partir de l'immersion fermée $j \colon X \hookrightarrow \mathbf{P}^{4g} \times S$, du morphisme $\pi \colon X \to S$ et de sa section ε.

On utilise pour cela le lemme de la balançoire (corollaire 6 p. 51 de [Mu]) appliqué au produit $\mathbf{P}^{4^g} \times S$ et au faisceau inversible $(\phi_* \mathcal{O}_Y(1))^{-1} \otimes \mathcal{O}_{\mathbf{P}^{4^g}_S}(1)$. La restriction de ce dernier aux fibres géométriques de la projection p_2 est triviale ce qui assure qu'il provient d'un faisceau inversible $\mathcal{F}'$ sur S. Après tiré en arrière sur X cela donne

$$(\iota^* \mathcal{O}_Y(1))^{-1} \otimes (p_1 \circ \phi \circ \iota)^* \mathcal{O}_{\mathbf{P}^{4^g}}(1) = \pi^* \mathcal{F}'.$$

On note $\mathcal{F}$ le faisceau $(p_1 \circ \phi \circ \iota)^* \mathcal{O}_{\mathbf{P}^{4^g}}(1) = j^* \mathcal{O}_{\mathbf{P}^{4^g}_S}(1)$. Or on a $\iota^* \mathcal{O}_Y(1) = L^\Delta(\lambda)^{\otimes 2}$ et un isomorphisme canonique $\varepsilon^* L^\Delta(\lambda) = \mathcal{O}_S$ donc on obtient

$$\varepsilon^*((L^\Delta(\lambda)^{\otimes 2})^{-1} \otimes \mathcal{F}) = \mathcal{F}'$$

d'où $\varepsilon^* \mathcal{F} = \mathcal{F}'$ ce qui donne finalement

$$L^\Delta(\lambda)^{\otimes 2} \simeq \mathcal{F} \otimes \pi^* \varepsilon^* \mathcal{F}^{-1}$$

et on obtient que $L^\Delta(\lambda)^{\otimes 2}$ est déterminé par cette structure. Il suit que $4\lambda = \varphi_{L^\Delta(\lambda)^{\otimes 2}}$ est déterminé mais comme le groupe des S-morphismes $X \to X^\vee$ est sans torsion cela détermine λ.

On va maintenant retrouver la rigidification linéaire ϕ. Comme $\mathcal{F} = j^* \mathcal{O}_{\mathbf{P}^{4^g}_S}(1)$ on a un morphisme naturel $\Gamma(\mathbf{P}^{4^g}, \mathcal{O}_{\mathbf{P}^{4^g}}(1))_S \to \pi_* \mathcal{F}$ par adjonction. Maintenant la formule de projection avec $(\varepsilon^*(\mathcal{F}))^{-1}$ et $\mathcal{F}$ donne un isomorphisme

$$\pi_*(\mathcal{F} \otimes \pi^*(\varepsilon^* \mathcal{F})^{-1}) \simeq \pi_* \mathcal{F} \otimes (\varepsilon^* \mathcal{F})^{-1}.$$

Or d'après l'isomorphisme précédent $\pi_*(\mathcal{F} \otimes \pi^*(\varepsilon^* \mathcal{F})^{-1}) \simeq \pi_* L^\Delta(\lambda)^{\otimes 2}$.

On en déduit donc un morphisme naturel

$$\Gamma(\mathbf{P}^{4^g}, \mathcal{O}_{\mathbf{P}^{4^g}}(1))_S \otimes (\varepsilon^* \mathcal{F})^{-1} \longrightarrow \pi_* L^\Delta(\lambda)^{\otimes 2}$$

qui induit la rigidification linéaire

$$\mathbf{P}(\pi_* L^\Delta(\lambda)^2) \simeq \mathbf{P}(\Gamma(\mathbf{P}^{4^g}, \mathcal{O}_{\mathbf{P}^{4^g}}(1))_S \otimes (\varepsilon^* \mathcal{F})^{-1}) = \mathbf{P}^{4^g} \times S.$$

□

Il résulte de cette étude que $\mathcal{H}_g$ est un sous-foncteur de $\mathcal{H}\mathrm{ilb}^{4^g X^g}_{\mathbf{P}^{4^g}}$. On a besoin d'un dernier résultat avant de montrer que $\mathcal{H}_g$ est représentable.

Proposition 3.4.8. *Soient $\pi\colon X \to S$ un schéma abélien projectif et L un faisceau inversible sur X et π-ample sur S tel que $\varepsilon^*(L) = \mathcal{O}_S$. Pour un changement de base $f\colon T \to S$ on note L_T le faisceau sur $X_T = X \times_S T$ déduit de L. Alors pour tout entier non nul k il y a au plus un morphisme $\lambda\colon X_T \to X_T^\vee$ tel que $L_T = L^\Delta(k\lambda)$. De plus, il existe un sous-schéma fermé $S_0 \subset S$ tel qu'un tel λ existe si et seulement si f se factorise par S_0.*

Le résultat fondamental est le suivant.

Théorème 3.4.9. *Il existe un sous-schéma H_g localement fermé dans* $\mathrm{Hilb}^{(4X)^g}_{\mathbf{P}^{4^g}}$ *qui représente $\mathcal{H}_g$.*

Démonstration. On procède par réductions successives. On note H_0 le schéma $\mathrm{Hilb}^{4^g X^g}_{\mathbf{P}^{4^g}}$. D'après la démonstration de la proposition 5.1 de [GIT] il existe un sous-schéma ouvert $H_1 \subset H_0$ qui factorise les morphismes $S \to H_0$ où $X \to S$ est à fibres lisses et géométriquement connexes. L'ouvert H_1 est muni d'un schéma universel $Z_1 \to H_1$ et d'une section canonique. La restriction à ce H_1 permet d'utiliser le théorème 3.4.5 sur les composantes connexes de H_1. On note $H_1 = \coprod_i H_{1,i}$ où $H_{1,i}$ est une composante connexe de H_1. Alors si $\overline{x}\colon \operatorname{Spec}\overline{k} \to H_1$ est un point géométrique de H_1 qui induit par produit fibré une variété abélienne alors le théorème 3.4.5 donne que la composante connexe de H_1 contenant l'image de $\overline{x}$ est un schéma abélien. On note H_2 l'union des composantes connexes de H_1 qui sont des schémas abéliens. Par construction H_2 factorise les morphismes $S \to H_1$ où $X \to S$ est un schéma abélien et on dispose d'un schéma abélien $Z_2 \to H_2$.

On s'intéresse maintenant à la polarisation et la rigidification linéaire. Par construction Z_2 est un sous-schéma de $\mathbf{P}^{4^g} \times H_2$ donc on peut considérer le faisceau

$$L_2 = \mathcal{O}_{Z_2} \otimes p_1^*(\mathcal{O}_{\mathbf{P}^{4^g}}(1)).$$

Soient $\pi\colon Z_2 \to H_2$ le morphisme structurel et ε la section identité. Alors le faisceau $L_2' = L_2 \otimes \pi^*\varepsilon^* L_2^{-1}$ est trivial suivant la section identité. Si S est un schéma tel que le schéma abélien $Z_2 \times_{H_2} S$ avec son immersion dans un espace projectif provient d'un schéma abélien principalement polarisé et linéairement rigidifié alors la polarisation λ_S doit vérifier

$$L_2' \otimes \mathcal{O}_S = L^{\Delta}(\lambda)^{\otimes 2}.$$

Alors par la proposition 3.4.8 il existe un sous-schéma fermé $H_3 \subset H_2$ tel que $L_2' \otimes \mathcal{O}_S$ est de la forme $L^{\Delta}(\lambda)^{\otimes 2}$ si et seulement si $S \to H_2$ se factorise par H_3. On pose $Z_3 = Z_2 \times_{H_2} H_3$. Alors $Z_3 \to H_3$ est un schéma abélien avec une polarisation principale $\lambda\colon Z_3 \to Z_3^{\vee}$ tel que si $L_3 = L_2' \otimes \mathcal{O}_{Z_3}$ alors $L_3 = L^{\Delta}(\lambda)^{\otimes 2}$. On en déduit un morphisme

$$H^0(\mathcal{O}_{\mathbf{P}^{4^g}}(1)) \otimes (\varepsilon^* L_3)^{-1} \longrightarrow \pi_* L^{\Delta}(\lambda)^{\otimes 2}.$$

Il suffit alors de considérer le sous-schéma H_4 déterminé par le fait que le noyau et conoyau de ce morphisme sont triviaux.

□

On termine par rappeler deux propriétés du schéma abélien $Z_g \to H_g$. La théorie complexe développée dans [BL] paragraphe 8.1 donne une description des points complexes de H_g. On en déduit en particulier que H_g est géométriquement irréductible. De plus par la proposition 7.4 de [GIT] les schémas Z_g et H_g sont quasi-projectifs.

3.5 Existence de variétés abéliennes avec $d(A)$ maximal relatif à un corps de nombres

On dispose maintenant d'un schéma abélien universel $Z_g \to H_g$ pour les variétés abéliennes de dimension g principalement polarisées et linéairement rigidifiées. Il reste le problème de ce que l'approximation faible n'est pas connue pour H_g. Pour pallier ce problème on utilise le lemme suivant, déduit d'un résultat d'Ekedahl.

Lemme 3.5.1. *Soit $\varphi\colon X \to Y$ un revêtement fini étale de schémas de type fini sur un corps de nombres K avec X géométriquement irréductible et Y vérifiant l'approximation faible. Soient $v_1, \dots, v_n \in \Sigma_K$ des places distinctes et $U_i \subset X(K_{v_i})$ un ouvert non vide pour chaque $i \in \{1, \dots, n\}$. Alors il existe une extension finie L/K avec des places $w_i \mid v_i$ telles que $L_{w_i} \simeq K_{v_i}$ pour chaque $i \in \{1, \dots, n\}$ et un point $x \in X(L)$ tel que $x_{L_{w_i}} \in U_i$ pour chaque $i \in \{1, \dots, n\}$.*

Démonstration. On considère les ensembles $\varphi(U_i)$ de $Y(K_{v_i})$ qui sont ouverts et non vides car ce sont les images par φ qui est étale. Par hypothèse Y vérifie l'approximation faible et X est géométriquement irréductible donc par le théorème 1.3 de [Ek] il existe un point $y \in Y(K)$ tel que $y_{K_{v_i}} \in \varphi(U_i)$ pour tout $i \in \{1, \dots, n\}$ et y a une fibre connexe par φ. Cette fibre est donc le spectre d'un corps L et comme φ est un morphisme fini, L est une extension finie de K.

Pour tout $i \in \{1, \dots, n\}$ la fibre de $y_{K_{v_i}}$ par φ est $\operatorname{Spec} L \otimes K_{v_i} = \bigoplus_{w \mid v_i} L_w$. De plus, par construction $y_{K_{v_i}}$ est l'image d'un point $x_i \in U_i$. Un tel point correspond à une place $w_i \mid v_i$ de L telle que $L_{w_i} = K_{v_i}$. Finalement, si $x = \varphi^{-1}(y)$ on a $x_{L_{w_i}} = x_i$ et donc $x \in X(L)$ vérifie l'énoncé. □

On est finalement en mesure de démontrer le résultat 4 de l'introduction de cette thèse.

Théorème 3.5.2. *Pour tout corps de nombres K et tout entier non nul g, il existe une extension finie L/K et une variété abélienne A principalement*

polarisée de dimension g sur L telle que

$$d(A) = d_g(K).$$

Démonstration. Soient $p_1, \ldots, p_n$ les diviseurs premiers de $d_g(K)$. Par le théorème 2.3.6 il existe des variétés abéliennes $B_1, \ldots, B_n$ principalement polarisées de dimension g sur K et des places $v_1, \ldots, v_n \in \Sigma_K$ telles que

$$v_{p_i}(\mathrm{Card}\, \Phi_{B_i,v_i}) = v_{p_i}(d_g(K)).$$

Quitte à faire une extension préliminaire non ramifiée en les v_i et avec suffisamment de places au-dessus de celles-ci (par le théorème 4 du chapitre 6 de [Ri]) on peut supposer les places v_i distinctes.

Soient $b_i \in H_g(K)$ des points de fibre B_i pour tout $i \in \{1, \ldots, n\}$. Par le théorème 3.3.1 appliqué à $Z_g \to H_g$ et les places v_i on obtient des ouverts $U_i \subset H_g(K_{v_i})$ qui vérifient la propriété suivante, pour $s \in H_g(K_{v_i})$,

$$s \in U_i \iff \Phi_{A_s,v_i} \simeq \Phi_{B_i,v_i}$$

où l'on note A_s la variété abélienne donnée par la fibre de $Z_g \to H_g$ en s.

Maintenant, comme H_g est une variété quasi-projective et géométriquement irréductible, on dispose d'un ouvert affine géométriquement irréductible $U \subset H_g$ qui contient les points $b_1, \ldots, b_n \in U$. Soit $\varphi\colon U \to \mathbf{A}^m_K$ le morphisme obtenu par le lemme de normalisation de Noether. Le morphisme φ est fini et génériquement étale donc il existe un ouvert affine géométriquement irréductible $V \subset U$ tel que $\varphi_{|V}$ est étale et a pour image un ouvert $Y \subset \mathbf{A}^m_K$ de manière à ce que

$$\varphi_{|V}\colon V \to Y$$

est fini étale et Y vérifie l'approximation faible. Soit $F = U \setminus V$ le fermé complémentaire. Comme U est irréductible, F est de codimension non nulle et il suit que les ensembles $U_i \cap V(K_{v_i})$ sont ouverts et non vides. En effet, $U_i \cap U(K_{v_i})$ est non vide par construction et $F(K_{v_i})$ est d'intérieur vide par sa codimension. Le lemme 3.5.1 appliqué à $\varphi_{|V}$ donne alors un point $s \in V(L)$ pour une extension finie L/K et des places $w_i \in \Sigma_L$ avec $L_{w_i} \simeq K_{v_i}$ tels que $s_{L_{w_i}} \in U_i$. La variété abélienne A_s donnée par le point $s \in H_g(L)$ vérifie

$$\Phi_{A_s,w_i} = \Phi_{B_i,v_i}$$

pour chaque $i \in \{1, \ldots, n\}$ par le théorème 3.3.1. Finalement le théorème 2.3.6 donne $d_g(K) \mid d(A_s)$. Pour obtenir l'égalité on reprend les arguments développés dans le chapitre 2. Pour toute place $w \in \Sigma_L \setminus \{w_1, \ldots, w_n\}$ de

mauvaise réduction pour A_s on considère l'extension M_w de L_w de degré $\operatorname{Card}\Phi_{A_s,w}$ donnée par le théorème 2.2.14. Soit d le plus petit commun multiple des degrés des extensions M_w/L_w obtenues de cette manière et soit M'_w/L_w l'extension non ramifiée de M_w de manière à ce que $[M'_w : L_w] = d$. Par construction les extensions M'_w/L_w sont de même degré et $(A_s)_{M'_w}$ est semi-stable. Soit M/L l'extension obtenue par le théorème 2.3.4 appliquée aux extensions locales M'_w/L_w des places w de mauvaise réduction où M'_w est l'extension non ramifiée de degré d si w est l'une des w_i. Alors la variété abélienne $(A_s)_M$ vérifie $d((A_s)_M) = d_g(K)$ par construction.

□

Avec la même démonstration on obtient l'énoncé de principe local-global pour les groupes de monodromie finie suivant ainsi qu'un lemme d'approximation faible à extension finie près pour les variétés quasi-projectives.

Théorème 3.5.3. *Soient K un corps de nombres et g un entier non nul. Soient $G_1, \dots G_n$ des groupes finis tels qu'il existe des places $v_1, \dots, v_n \in \Sigma_K$ et des variétés abéliennes principalement polarisées A_i de dimension g sur K_{v_i} pour $1 \leq i \leq n$ telles que*

$$\Phi_{A_i,v_i} = G_i.$$

Alors il existe une extension finie L de K et des places $w_1, \dots, w_n \in \Sigma_L$ ainsi qu'une variété abélienne principalement polarisée A de dimension g sur L telle que pour tout i on a

$$\Phi_{A,w_i} = G_i.$$

Lemme 3.5.4. *Soit X une variété quasi-projective et géométriquement irréductible sur un corps de nombres K. Soient $v_1, \dots, v_n \in \Sigma_K$ et des ouverts non vide $U_i \subset X(K_{v_i})$ pour $1 \leq i \leq n$.*

Alors il existe une extension finie L/K avec des places $w_i \mid v_i$ telles que $L_{w_i} \simeq K_{v_i}$ pour chaque $i \in \{1, \dots, n\}$ et un point $x \in X(L)$ tel que $x_{L_{w_i}} \in U_i$ pour chaque $i \in \{1, \dots, n\}$.

3.6 Complément : une version champêtre

Dans le but d'obtenir le théorème 3.1.2 l'objet naturel à considérer est l'espace des modules $\mathcal{A}_g$ des variétés abéliennes de dimension g principalement polarisées qui n'est plus un schéma mais un champ de Deligne-Mumford. Celui-ci est construit en prenant le quotient de H_g par l'action

naturelle de PGL_{4^g}. L'unicité du modèle de Néron assure que c'est un champ séparé et on peut vérifier que c'est un champ de Deligne-Mumford. En particulier H_g est un atlas de $\mathcal{A}_g$.

Dans cette partie on montre que l'on peut obtenir des résultats similaires aux parties 3.2 et 3.3 dans ce nouveau cadre. Une topologie analytique sur les points à valeurs dans un corps topologique d'un champ qui généralise le cas des schémas est donnée dans [Mo]. Les morphismes étales induisent des homéomorphismes locaux pour cette topologie. La théorie du groupe fondamental étale des champs de Deligne-Mumford est traité dans [No] et correspond essentiellement à celle des schémas. En particulier on dispose sous certaines conditions (remplies ici) d'une suite exacte d'homotopie.

Théorème 3.6.1. *Soit S un champ de Deligne-Mumford sur un corps topologique k. On suppose que le centre de G_k est trivial. Alors l'application de Kummer profini induit une application continue*

$$\kappa\colon S(k)/\sim_k \longrightarrow \mathcal{S}_{\pi_1}(S/k).$$

Démonstration. On montre d'abord que si $a, b \in S(k)$ sont tels qu'il existe un morphisme $\gamma\colon a \to b$ dans $S(k)$ alors a et b induisent des sections conjuguées par un élément $g \in \pi_1(S_{\overline{k}}, \overline{a})$. On note $\overline{a}, \overline{b}$ les points géométriques correspondants et $\overline{\gamma}$ l'isomorphisme de $S(\overline{k})$ déduit de γ, c'est-à-dire $\overline{\gamma} = \mathrm{Pt}^*\,\gamma$. De ce dernier point on déduit que l'action de $\sigma \in \mathrm{Gal}(\overline{k}/k)$ sur $S(\overline{k})$ laisse $\overline{\gamma}$ invariant. En effet, σ agit par tiré en arrière par le morphisme $\sigma\colon \operatorname{Spec}\overline{k} \to \operatorname{Spec}\overline{k}$ et

$$\sigma^*\overline{\gamma} = \sigma^*\,\mathrm{Pt}^*\,\gamma = (\mathrm{Pt}\circ\sigma)^*\gamma = \mathrm{Pt}^*(\gamma) = \overline{\gamma}.$$

Soit X un revêtement fini étale de S. On a un carré commutatif

$$\begin{array}{ccc} (x,\phi) & \overline{a}(X) \xrightarrow{\overline{\gamma}} \overline{b}(X) & (x, \phi\circ\overline{\gamma}^{-1}) \\ \big\downarrow & \big\downarrow p_{\sigma,\overline{a}} \qquad \big\downarrow p_{\sigma,\overline{b}} & \big\downarrow \\ (\sigma(x),\sigma(\phi)) & \overline{a}(X) \xrightarrow{\overline{\gamma}} \overline{b}(X) & (\sigma(x), \sigma(\phi)\circ\overline{\gamma}^{-1}) \end{array}$$

On en déduit directement le fait que $\overline{\gamma}\circ p_{\sigma,\overline{b}}\circ\overline{\gamma}^{-1} = p_{\sigma,\overline{a}} \in \pi_1(S,\overline{a})$.

Il reste à voir que $p_*(\overline{\gamma}) = \mathrm{id}$ pour obtenir le résultat. Cela découle à nouveau du carré commutatif, en effet on en déduit par ailleurs que

$$p_{\sigma,\overline{b}}\circ\overline{\gamma}\circ p_{\sigma,\overline{a}}^{-1} = \overline{\gamma}$$

et comme p_* respecte la composition des chemins il suit que $p_*(\overline{\gamma})$ est dans le centre de G_k.

Finalement, $\overline{\gamma}$ induit un morphisme des suites exactes d'homotopies qui envoie la section s_a sur s_b.

L'application de Kummer se factorise donc par $S(k)/\sim_k$ et l'application induite est continue par les mêmes arguments que dans la partie 3.2.2 adapté au cas des champs. □

On obtient donc un analogue du théorème 3.2.4 pour les revêtement finis étales de champs de Deligne-Mumford géométriquement connexes et quasi-compacts.

Remarque 3.6.2. L'application de Kummer qui nous intéresse n'est pas constante sur les classes d'équivalences $S(k)/\sim_{\overline{k}}$ comme le montre l'exemple 3.3.5. En effet, on trouve différentes courbes elliptiques de j-invariant nul dont les groupes de monodromie finie en (3) sont $\mathbf{Z}/4\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$. Ces courbes sont donc dans des ouverts analytiques différents de $\mathcal{M}_{1,1}(\mathbf{Q}_3)/\sim$ mais sont confondues dans $\mathcal{M}_{1,1}(\mathbf{Q}_3)/\sim_{\overline{\mathbf{Q}_3}}$.

La discussion de la partie 2.2 s'applique donc au cas du champ $\mathcal{A}_g$ des variétés abéliennes principalement polarisées avec son revêtement fini étale $A_g[\ell]$ des variétés abéliennes principalement polarisées avec structure de niveau ℓ.

Proposition 3.6.3. *Le revêtement fini étale $\mathcal{A}_g[\ell] \to \mathcal{A}_g$ est de groupe $\mathrm{GL}_{2g}(\mathbf{F}_\ell)$.*

Démonstration. Il suffit de voir que pour tout schéma abélien (principalement polarisé mais ceci n'interviendra pas) A/S le changement de base de $\mathcal{A}_g[\ell] \to \mathcal{A}_g$ par $S \to \mathcal{A}_g$ est un revêtement fini étale de groupe $\mathrm{GL}_{2g}(\mathbf{F}_\ell)$.

On remarque d'abord que s'il existe une structure de niveau ℓ sur A alors toutes les structures de niveau ℓ sur A sont définies et un isomorphisme de telles structures est donné par un élément de $\mathrm{GL}_{2g}(\mathbf{F}_\ell)$. Ceci donne, dans ce cas, un isomorphisme

$$\mathrm{GL}_{2g}(\mathbf{F}_\ell) \times S \simeq S \times_{\mathcal{A}_g} \mathcal{A}_g[\ell].$$

Il reste à voir dans le cas général qu'il existe un revêtement fini étale $S' \to S$ tel que $A \times_S S'$ a une structure de niveau ℓ.

Soit T_ℓ un revêtement galoisien de S tel que toutes les composantes connexes du revêtement fini étale $A[\ell] \to S$ sont des quotients de T_ℓ. Alors $A[\ell] \times_S T_\ell$ est $A'[\ell]$ où $A' = A \times_S T_\ell$. Par choix de T_ℓ on a de plus que $A'[\ell]$ est un revêtement étale trivial de T_ℓ. Par définition ces sections forment une structure de niveau ℓ sur A' ce qui conclut. □

On peut remplacer $\mathcal{A}_g[\ell]$ par le même espace de modules mais avec la condition que la structure de niveau respecte la structure symplectique.

Proposition 3.6.4. *Soit A sur K une variété abélienne principalement polarisée. L'action de $\mathrm{Gal}(\overline{K}/K)$ sur le revêtement étale $K \times_{\mathcal{A}_g} \times \mathcal{A}_g[\ell]$ de K donné par l'ensemble des structures de niveaux ℓ de A coïncide avec son action sur la ℓ-torsion de A.*

Démonstration. Une structure de niveau ℓ sur A correspond au choix d'une base du $\mathbf{F}_\ell$-espace vectoriel $A[\ell]$. L'ensemble des structures de niveau est en bijection avec les bases de cette espace. Soit $\mathcal{B} = (a_1, \ldots, a_n)$ une telle base. On a par définition de l'action de $\sigma \in \mathrm{Gal}(\overline{K}/K)$ l'égalité

$$\sigma(\mathcal{B}) = (\sigma(a_1), \ldots, \sigma(a_n)).$$

□

Comme cela on retrouve la réduction modulo ℓ de l'image de l'inertie $I_{\overline{v}}$ par la représentation ℓ-adique associé au module de Tate d'une variété abélienne A sur K comme image de la composée

$$I_{\overline{v}} \xrightarrow{s_*} \pi_1(\mathcal{A}_g, \overline{s}) \longrightarrow \mathrm{GL}_{2g}(\mathbf{F}_\ell),$$

le morphisme $s\colon \operatorname{Spec} K \to \mathcal{A}_g$ étant celui donnée par A comme élément de $\mathcal{A}_g(K)$.

Il suit que l'on a un analogue du théorème 3.3.1 obtenu du revêtement fini étale $\mathcal{A}_g[\ell] \to \mathcal{A}_g$. Une étude de la propriété d'approximation faible sur cet espace permettrait alors d'obtenir des résultats semblables au résultat 3.

Chapitre 4

Construction de variétés abéliennes CM avec grosse monodromie finie sauvage [1].

4.1 Introduction

Dans le but d'utiliser le théorème 3.1.2 on va s'intéresser à la construction de variétés abéliennes de toutes dimensions sur des corps de nombres dont la p-partie des groupes de monodromie finie est maximale. Cette étude nous amène à montrer une nouvelle borne pour la 2-partie du cardinal d'un groupe de monodromie finie d'une variété abélienne potentiellement CM.

Théorème 4.1.1. *Soient g un entier naturel non nul et K un corps de nombres non ramifié en 2. On note $p_1, \ldots, p_n$ les diviseurs premiers impairs de $M(2g)$. Alors il existe une extension finie L de K telle que pour chaque $i \in \{1, \ldots, n\}$ il existe une variété abélienne A_i de dimension g principalement polarisée sur L et une place v_i de L avec*

$$\operatorname{Card} \Phi_{A_i, v_i} = p_i^{r(2g, p_i)}$$

et il existe une variété abélienne principalement polarisée A de dimension g sur L et une place v de L telles que

$$\operatorname{Card} \Phi_{A,v} = 2^{r(2g,2)+1-g}.$$

La p-partie des groupes de monodromie finie dont le théorème assure l'existence est donc maximale, sauf lorsque p est pair. La construction des

1. Ce chapitre correspond dans sa quasi-totalité à la prépublication [Ph]

variétés abéliennes A_i repose sur la théorie de la multiplication complexe et le manque, lorsque $p = 2$, s'explique par le théorème suivant, résultat principal de la partie 5 qui avec le théorème 4.4.5 donne l'égalité

$$\operatorname{Card} \Phi_{A,v} = 2^{r(2g,2)+1-g}$$

dans l'énoncé précédent.

Théorème 4.1.2. *Soit A une variété abélienne de dimension g sur un corps de nombres K telle que $A_{\overline{K}}$ est CM. Alors on a*

$$v_2(\operatorname{Card} \Phi_{A,v}) \leq r(2g,2) + 1 - g$$

pour toute place ultramétrique v de K. De plus, l'égalité ne peut intervenir que lorsque une composante isotypique de $A_{\overline{K}}$ est isogène à une puissance de la courbe elliptique $y^2 = x^3 - x$.

Lorsque A est isotypique et que A a multiplication complexe par Z, il est connu depuis [ST] que $\Phi_{A,v}$ est un sous-groupe du groupe des racines de l'unité de Z. Si l'on ne suppose plus que A est CM mais seulement que $A_{\overline{K}}$ l'est alors le degré $[K_A : K]$ intervient dans la majoration où K_A est le corps de définition des endomorphismes de $A_{\overline{K}}$. Ce degré est étudié dans [Ré2] et [GK] ; ces derniers obtiennent

$$v_2([K_A : K]) \leq r(2g,2) - g - 1.$$

On obtient alors la borne en combinant les deux approches de façon adaptée à notre contexte.

La construction des variétés abéliennes de l'énoncé du théorème 4.1.1 se fait par une adaptation aux corps de nombres des techniques de [SZ4] qui sont utilisées dans le cas de corps locaux d'égales caractéristiques p. Précisément on construit ces variétés abéliennes comme formes tordues de variétés abéliennes avec multiplication complexe (CM). Pour cela on effectue deux généralisations du théorème 4.3 de torsion de [SZ4], l'une aux corps de nombres et l'autre avec des hypothèses réduites, qui permettent de construire des variétés abéliennes avec des groupes de monodromie finie prescrits. Pour déduire de ces théorèmes le résultat principal on a besoin d'une part de l'existence de variétés abéliennes avec des gros groupes d'automorphismes et d'autre part de l'existence d'extensions galoisiennes de corps de nombres avec des gros groupes d'inertie en des places choisies.

En partie 2 on montre l'existence de variétés abéliennes CM qui ont $\mathbf{Z}[\zeta_p]$ pour anneaux d'endomorphismes ainsi que les autres énoncés sur les variétés

abéliennes CM et polarisations utiles à la suite du texte. L'obstruction à cette approche, pour $p = 2$, vient du fait que l'on ne dispose pas, en caractéristique nulle, d'une courbe supersingulière.

La partie 3 est consacrée aux résultats d'arithmétique des corps de nombres nécessaires pour appliquer les théorèmes de torsion. On commence pour cela de manière analogue à [SZ4] en établissant l'existence d'extensions locales pour des p-groupes prescrits. On résout ensuite des problèmes de Grunwald pour des produits en couronne de la forme $\mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$. On traite à part la construction pour $p = 2$ qui nécessite une attention particulière. Dans tous les cas, bien qu'on cherche à produire des groupes de monodromie finie qui sont des p-Sylow des groupes concernés, on travaille avec les groupes complets pour permettre la résolution du problème de Grunwald qui se pose (i.e. le passage d'extensions locales à une extension d'un corps de nombres).

4.1.1 Rappels sur les groupes de monodromie finie

Soient A une variété abélienne de dimension g sur un corps de nombres K et v une place non archimédienne de K de caractéristique résiduelle p. On note I le groupe d'inertie d'une extension $\overline{v}$ de v à $\overline{K}$. Soit $\ell \neq p$ un nombre premier. L'action du groupe de Galois absolu $\mathrm{Gal}(\overline{K}/K)$ sur le module de Tate $\mathrm{T}_\ell A$ de A induit une représentation ℓ-adique

$$\rho_{A,\ell} \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_{2g}(\mathbf{Q}_\ell).$$

On note G le groupe algébrique linéaire obtenu comme adhérence pour la topologie de Zariski de l'image de $\rho_{A,\ell}$ restreinte à I dans GL_{2g}.

Définition 4.1.3. Le groupe de monodromie finie de A en v noté $\Phi_{A,v}$ est le groupe des composantes G/G°.

On note $I_{A,v}$ le noyau du morphisme naturel, surjectif $I \to G/G^\circ$. On a donc $\Phi_{A,v} = I/I_{A,v}$ par définition.

Il est démontré dans [SZ2] (théorème 4.2) que cette définition est équivalente à celle de Grothendieck et en particulier

$$I_{A,v} = \{\sigma \in I \mid \rho_{A,\ell}(\sigma) \text{ est unipotent}\}.$$

Dans le cas où A a bonne réduction potentielle cette égalité devient

$$I_{A,v} = \mathrm{Ker}\, \rho_{A,\ell}.$$

Le résultat fondamental sur les groupes de monodromie finie est le suivant.

Théorème 4.1.4. *(Grothendieck) La variété abélienne A a réduction semi-stable en v si et seulement si $\Phi_{A,v} = \{1\}$.*

Il suit de la définition et du résultat fondamental les propriétés suivantes :

(i) Le sous-groupe $I_{A,v}$ de I définit une extension galoisienne $(K_v^{\mathrm{nr}})_{A,s}$ de K_v^{nr} qui est la plus petite extension sur laquelle $A_{K_v^{\mathrm{nr}}}$ atteint réduction semi-stable. Autrement dit, si L est une extension de K_v^{nr} telle que A_L a réduction semi-stable alors $(K_v^{\mathrm{nr}})_{A,s} \subset L$. En particulier on a

$$\mathrm{Card}\, \Phi_{A,v} = [(K_v^{\mathrm{nr}})_{A,s} : K_v^{\mathrm{nr}}].$$

(ii) Les groupes de monodromie finie sont invariants par isogénie et puissance. De plus, si B est une variété abélienne sur K on a l'inclusion

$$(K_v^{\mathrm{nr}})_{A\times B,s} \subset (K_v^{\mathrm{nr}})_{A,s}(K_v^{\mathrm{nr}})_{B,s}.$$

(iii) Si L est une extension de K et $w \mid v$ est une place de L non ramifiée alors

$$\Phi_{A_L,w} = \Phi_{A,v}.$$

Comme on l'a vu dans le premier chapitre et utilisé dans le chapitre précédent, suite au résultat fondamental et à la propriété (i) on peut toujours, par un résultat d'approximation faible (voir par exemple le théorème 2.3.4 vu en chapitre 2), construire une extension finie L de K ramifiée seulement en v et des places de caractéristiques résiduelles arbitrairement grandes telle que A_L a réduction semi-stable aux places de L au-dessus de v.

4.2 Existence de variétés abéliennes CM principalement polarisées

On rappelle au préalable la convention pour les variétés abéliennes CM que l'on utilise ici.

Définition 4.2.1. Soit A une variété abélienne de dimension g sur K. On dit que A est CM s'il existe une $\mathbf{Q}$-algèbre commutative semi-simple F de dimension $2g$ et une injection

$$F \to \mathbf{Q} \otimes \mathrm{End}\, A.$$

On dit dans ce cas que A a multiplication complexe par F.

Dans le cas où $A_{\overline{K}}$ est CM on dit que A est potentiellement CM.

On commence par la proposition d'existence des variétés abéliennes CM qui nous intéressent dans la suite.

Proposition 4.2.2. *Soient p un nombre premier impair, ζ_p une racine primitive p-ième de l'unité et $\ell > p$ un nombre premier. Il existe un corps de nombres K et une variété abélienne A sur K de sorte que*

(i) $\dim A = \frac{p-1}{2}$;

(ii) $\operatorname{End} A \simeq \mathbf{Z}[\zeta_p]$;

(iii) *A admet une polarisation principale.*

De plus on peut choisir K ramifié seulement au-dessus de p et des places de caractéristiques résiduelles supérieures à ℓ avec A de bonne réduction sur K.

Démonstration. On commence par trouver une variété abélienne A sur $\mathbf{C}$ qui vérifie (i), (ii) et (iii).

On note $\alpha = \frac{\zeta_p - \zeta_p^{-1}}{p} \in \mathbf{Q}(\zeta_p)$. Pour tout plongement $\tau\colon \mathbf{Q}(\zeta_p) \to \mathbf{C}$ l'image $\tau(\alpha)$ de α est un imaginaire pur que l'on note $\mathrm{i}\beta_\tau$. Alors

$$\Phi = \{\tau\colon \mathbf{Q}(\zeta_p) \to \mathbf{C} \mid \beta_\tau > 0\}$$

définit un type CM de $\mathbf{Q}(\zeta_p)$ qui est primitif. Il suffit de voir pour cela que

$$G = \{\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \mid \Phi\sigma = \Phi\} = \{\mathrm{id}\}$$

par la proposition 26 de [Sh]. Si l'on fait correspondre à chaque élément de ce groupe de Galois son image de ζ_p, Φ correspond aux racines primitives p-èmes de l'unité sur le demi-cercle supérieur. On vérifie qu'un élément σ non trivial ne laisse pas stable le demi-cercle supérieur ce qui donne bien $G = \{\mathrm{id}\}$.

Le type CM primitif Φ définit une structure complexe sur $\mathbf{Q}(\zeta_p) \otimes \mathbf{R}$. On va maintenant montrer que le tore complexe $A = \mathbf{Q}(\zeta_p) \otimes \mathbf{R}/\mathbf{Z}[\zeta_p]$ a les propriétés voulues. La dimension de A est bien $\frac{p-1}{2}$ ce qui donne (i). Pour $(x, y) \in (\mathbf{Q}(\zeta_p) \otimes \mathbf{R})^2$ on pose

$$H(x, y) = 2 \sum_{\tau \in \Phi} \beta_\tau \tau(x) \overline{\tau(y)}.$$

On vérifie suivant [Mu] p. 212 que H est une forme de Riemann avec

$$\operatorname{Im} H(\mathbf{Z}[\zeta_p], \mathbf{Z}[\zeta_p]) = \mathbf{Z}.$$

Plus précisément on calcule la matrice de $\operatorname{Im} H$ dans la base $(1, \zeta_p, \ldots, \zeta_p^{p-2})$. On a

$$\operatorname{Im} H(\zeta_p^m, \zeta_p^n) = \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\alpha \zeta_p^{m-n})$$

ce qui vaut 0 si $|m-n| \neq 1$, 1 si $m = n+1$ et -1 sinon. Cela donne pour matrice de $\operatorname{Im} H$

$$\begin{pmatrix} 0 & -1 & & 0 \\ 1 & 0 & \ddots & \\ & \ddots & \ddots & -1 \\ 0 & & 1 & 0 \end{pmatrix}$$

qui a donc déterminant 1. On obtient que le tore complexe A est une variété abélienne et H définit une polarisation principale. Pour (ii) on a l'inclusion $\mathbf{Z}[\zeta_p] \hookrightarrow \operatorname{End} A$ et l'égalité vient du fait que A est simple car Φ est primitif.

Le corps réflexe de $(\mathbf{Q}(\zeta_p), \Phi)$ est encore $\mathbf{Q}(\zeta_p)$ car $\mathbf{Q}(\zeta_p)$ est une extension abélienne et Φ est un type primitif. Par le théorème p. 112 de [Sh] le corps des modules de A muni de ses endomorphismes et de sa polarisation est une extension de $\mathbf{Q}(\zeta_p)$ incluse dans son corps de classes de Hilbert. De la même façon le théorème 2 p. 118 de [Sh] permet de calculer le corps des modules K de cette structure à laquelle on a rajouté la p-torsion de A comme corps de classes sur le corps réflexe et de borner son conducteur. On peut alors vérifier que K n'est ramifié qu'en l'unique idéal au-dessus de p de $\mathbf{Z}[\zeta_p]$. Finalement, le théorème principal 1 p. 112 de [Sh] assure que K est un corps de définition de A.

La variété abélienne A a sa p-torsion définie sur K donc par la proposition 4.7 de l'exposé IX de [SGA7] elle a réduction semi-stable en toutes les places non archimédiennes de K qui ne sont pas au-dessus de p. Par ailleurs comme A est CM, par le théorème 6. a) de [ST] elle a bonne réduction potentielle donc bonne réduction en ces places. Quitte à faire une extension finie L/K ramifiée seulement en les places au-dessus de p et des places de caractéristiques résiduelles supérieures à ℓ la variété abélienne A_L a bonne réduction sur L (voir paragraphe 4.1.1). □

Remarque 4.2.3. En particulier la variété abélienne A du lemme précédent est CM et a multiplication complexe par $\mathbf{Q}(\zeta_p)$.

Soit (A, λ) une variété abélienne principalement polarisée sur un corps K. Soit B une variété abélienne sur K telle qu'il existe une extension finie galoisienne L et un isomorphisme $\varphi\colon B_L \to A_L$. Alors, comme la construction de la variété duale est fonctorielle, on a un isomorphisme $\varphi^\vee\colon A_L^\vee \to B_L^\vee$. Il suit que B_L a une polarisation principale $\varphi^*\lambda$, i.e. un isomorphisme $B_L \simeq B_L^\vee$ donné par $(\varphi^\vee) \circ \lambda \circ \varphi$. On dispose par ailleurs de l'involution de Rosati correspondant à λ sur $\operatorname{End} A_L \otimes \mathbf{Q}$ définie par $^\dagger\colon f \mapsto \lambda^{-1} \circ f^\vee \circ \lambda$. On donne maintenant un critère pour que $\varphi^*\lambda$ provienne d'une polarisation

principale de B. On note c le cocycle qui représente la classe de B dans $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}\, A_L)$, c'est-à-dire

$$\begin{array}{rccc} c: & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Aut}\, A_L \\ & \sigma & \longmapsto & \varphi \circ \sigma(\varphi)^{-1}. \end{array}$$

Lemme 4.2.4. *La polarisation principale $\varphi^*\lambda$ provient de B si et seulement pour tout $\sigma \in \mathrm{Gal}(L/K)$ l'égalité*

$$c(\sigma)^\dagger c(\sigma) = \mathrm{id}$$

est vérifiée.

Démonstration. On remarque d'abord que $\varphi^*\lambda$ provient de B si et seulement si elle est fixée par l'action de Galois, c'est-à-dire si et seulement si

$$\sigma(\varphi^*\lambda) = \varphi^*\lambda$$

pour tout $\sigma \in \mathrm{Gal}(L/K)$.

Or pour $\sigma \in \mathrm{Gal}(L/K)$, on a

$$\begin{aligned} \sigma(\varphi^*\lambda) &= \sigma(\varphi^\vee \circ \lambda \circ \varphi) \\ &= \sigma(\varphi^\vee) \circ \sigma(\lambda) \circ \sigma(\varphi). \end{aligned}$$

L'égalité $\sigma(\varphi^*\lambda) = \varphi^*\lambda$ est donc équivalente à

$$\sigma(\varphi^\vee) \circ \sigma(\lambda) \circ \sigma(\varphi) = \varphi^\vee \circ \lambda \circ \varphi$$

soit à

$$\lambda = c(\sigma)^\vee \circ \lambda \circ c(\sigma)$$

et finalement à

$$c(\sigma)^\dagger c(\sigma) = \mathrm{id}.$$

□

On termine cette partie par un lemme sur les variétés abéliennes isotypiques qui sera utile en partie 5.

Lemme 4.2.5. *Soit A une variété abélienne sur un corps de nombres K telle que $A_{\overline{K}}$ est isotypique et CM . Soit K_A le corps de définition des endomorphismes de $A_{\overline{K}}$. Alors la variété abélienne $A' = A_{K_A}$ est isotypique. Il existe une variété abélienne B de dimension d sur K_A telle que A' est isogène à B^h pour un entier $h \geq 0$. De plus on a*

$$\mathbf{Q} \otimes \mathrm{End}\, B \simeq Z$$

où Z est un corps CM de dimension $2d$ sur $\mathbf{Q}$ avec $2dh = 2g$.

Démonstration. Comme $A_{\overline{K}}$ est isotypique l'algèbre $\mathrm{End}\, A_{\overline{K}} \otimes \mathbf{Q} = \mathrm{End}\, A' \otimes \mathbf{Q}$ est simple ce qui montre que A' est isotypique. Il existe donc une variété abélienne simple B sur K_A telle que A est isogène à B^h pour un certain $h \geq 0$. La proposition 1.3.2.1 et le théorème 1.3.4 de [CCO] donnent le résultat. □

4.3 Le problème de Grunwald pour certains produits en couronne

Soient G un groupe fini, k un corps de nombres et S un ensemble fini de places de k. Le problème de Grunwald consiste à trouver une extension galoisienne L/k de groupe G et de comportement local prescrit aux places de S. Pour plus de détails à ce sujet, on renvoie le lecteur à la partie 2 de [Ch].

Notre but est de montrer que certains problèmes de Grunwald pour les groupes $\mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$, où p, m et n varient, sont résolubles quitte à grossir le corps de base k dans un premier temps. Dans un second temps, on s'intéressera au cas, plus difficile, du groupe $(\mathbf{Z}/4\mathbf{Z} \wr \mathfrak{S}_n) \rtimes \mathbf{Z}/2\mathbf{Z}$.

On commence pour cela par rappeler la notion de produit en couronne de groupes.

Définition 4.3.1. Soient G un groupe fini et n un entier naturel. On note $G \wr \mathfrak{S}_n$ le produit semi-direct de G^n et $\mathfrak{S}_n$ où le groupe symétrique $\mathfrak{S}_n$ agit par permutations sur G^n.

Pour un groupe fini G, on a par définition

$$\mathrm{Card}\, G \wr \mathfrak{S}_n = n!(\mathrm{Card}\, G)^n.$$

Lemme 4.3.2. *Soient p un nombre premier impair et n un entier naturel. On a*

$$v_p(\mathrm{Card}\, \mathbf{Z}/p\mathbf{Z} \wr \mathfrak{S}_n) = n + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

et

$$v_2(\mathrm{Card}\, \mathbf{Z}/4\mathbf{Z} \wr \mathfrak{S}_n) = 2n + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor.$$

Démonstration. Cela découle directement de la définition et de la formule de Legendre

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

pour tout nombre premier p. □

Remarque 4.3.3. On remarque que si, pour un entier naturel non nul g fixé et un nombre premier impair p, on choisit $n = \lfloor \frac{2g}{p-1} \rfloor$, alors

$$v_p(\mathrm{Card}\, \mathbf{Z}/p\mathbf{Z} \wr \mathfrak{S}_n) = r(2g, p).$$

Pour le nombre premier 2, on a seulement

$$v_2(\mathrm{Card}\, \mathbf{Z}/4\mathbf{Z} \wr \mathfrak{S}_g) = r(2g, 2) - g$$

en prenant $n = g$.

Les groupes $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/4\mathbf{Z}$ correspondent aux groupes des racines de l'unité dans $\mathbf{Z}[\zeta_p]$ et $\mathbf{Z}[\mathrm{i}]$ respectivement. Si l'on disposait d'une courbe elliptique avec le groupe des quaternions comme groupe d'automorphismes alors le calcul serait ici

$$v_2(\mathrm{Card}\, Q_8 \wr \mathfrak{S}_g) = r(2g, 2).$$

4.3.1 Les groupes $\mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$

Dans cette sous-partie, on traite le cas des groupes $\mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$, où p, n et m varient. La résolution du problème de Grunwald pour ces groupes découlera des travaux de Saltman dans [Sa] après quelques propositions de préparation. On construit dans un premier temps, pour un corps de nombres k, une extension K de k sur laquelle on montrera que le problème est résoluble.

Lemme 4.3.4. *Soient K un corps de nombres et v une place finie de K au-dessus de p. Le pro-p quotient maximal H du groupe de Galois absolu G de K_v^{nr} est un pro-p groupe libre de rang infini dénombrable.*

Démonstration. Par les théorèmes 9.3 et 9.7 de [Ko] le groupe H est pro-p libre. Par ailleurs, la suite spectrale d'Hochschild-Serre donne un isomorphisme

$$H^1(H, \mathbf{F}_p) \simeq H^1(G, \mathbf{F}_p)$$

avec $H^1(G, \mathbf{F}_p) = \varinjlim H^1(G_n, \mathbf{F}_p)$ où G_n est le groupe de Galois absolu de l'unique extension non ramifiée de degré n de K_v. Par les théorèmes 3.9.1 et 7.5.11 de [NSW] on a de plus $\dim H^1(G_n, \mathbf{F}_p) \geq n$ ce qui donne que la dimension de $H^1(H, \mathbf{F}_p)$ est infinie dénombrable. Le théorème 3.9.1 de [NSW] permet alors de conclure que H est de rang infini dénombrable. □

Ce lemme et sa preuve nous ont été communiqués par Akio Tamagawa, ce qui permet, avec la maîtrise de la ramification locale, une présentation plus élégante de nos résultats.

Lemme 4.3.5. *Soit G un p-groupe fini. Alors pour tout corps de nombres k et toute place v de corps résiduel de caractéristique p de k, il existe une extension finie non ramifiée $K^{(v)}$ de k_v telle que G est le groupe de Galois d'une extension totalement ramifiée $L^{(v)}/K^{(v)}$.*

Démonstration. Par le lemme 4.3.4, on dispose d'une extension galoisienne de k_v^{nr} de groupe de Galois H un pro-p groupe libre de rang infini dénombrable. Soit $(s_n)_{n\in\mathbf{N}}$ une base de ce groupe. On définit un morphisme surjectif $H \to G$ en choisissant des images presque toutes égales à 1_G des s_n. Ceci détermine une extension galoisienne de k_v^{nr} de groupe G. Cette extension descend en une extension galoisienne $L^{(v)}/K^{(v)}$ de même groupe pour un choix convenable de $K^{(v)} \subset k_v^{\mathrm{nr}}$ extension finie de k_v. □

Le résultat de préparation avant de résoudre notre problème de Grunwald peut alors s'énoncer comme suit.

Lemme 4.3.6. *Soient G un groupe fini, k un corps de nombres et S un ensemble fini de places ultramétriques de k. Il existe une extension finie K/k telle que pour toute place v de S*

(1) il existe une unique place w de K au-dessus de v ;
(2) l'extension K_w/k_v est non ramifiée ;
(3) il existe une extension galoisienne $L^{(v)}/K_w$ totalement ramifiée ;
(4) le groupe $\mathrm{Gal}(L^{(v)}/K_w)$ est isomorphe à un p-Sylow de G où p est la caractéristique résiduelle de v.

Démonstration. Par le lemme 4.3.5 on obtient des extensions finies non ramifiées $K^{(v)}/k_v$ pour les places v de S et des extensions $L^{(v)}/K^{(v)}$ totalement ramifiées galoisiennes de groupes un p-Sylow de G. Quitte à faire des extensions non ramifiées des $K^{(v)}$, et donc linéairement disjointes des $L^{(v)}$, on peut supposer que les degrés $[K^{(v)} : k_v]$ sont égaux. Le théorème 2.3.4 appliqué à cette situation donne l'existence de K. □

Proposition 4.3.7. *Soient k un corps de nombres, p un nombre premier et m, n des entiers naturels non nuls. Si $p = 2$ on suppose que $m = 1$ ou $m = 2$. On note G le groupe $\mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$. Soit S un ensemble fini de places ultramétriques de k contenant une place v au-dessus de p. Alors il existe une extension finie K/k et une extension L/K galoisienne de groupe G telles que*

(1) au-dessus de chaque place de S, il existe une unique place de K et elle est non ramifiée ;
(2) le groupe d'inertie de $\mathrm{Gal}(L/K)$ en l'unique place w de K au-dessus de v est un p-Sylow de G.

Démonstration. On peut supposer sans perte de généralité que S contient des places au-dessus de tous les diviseurs premiers de $\operatorname{Card} G$. Le lemme 4.3.6 appliqué avec k, G et S fournit une extension K/k et des extensions locales. Les résultats de Saltman dans [Sa] permettent de réaliser ces extensions comme complétés d'une extension L/K. En effet d'après les théorèmes 2.1 et 5.1 de [Sa], les groupes $\mathbf{Z}/p^m\mathbf{Z}$ et $\mathfrak{S}_n$ admettent des extensions galoisiennes génériques sur K (par choix de m pour $p = 2$) et donc le produit en couronne $G = \mathbf{Z}/p^m\mathbf{Z} \wr \mathfrak{S}_n$ aussi par le théorème 3.3 de [Sa]. Le théorème 5.9 de [Sa] s'applique donc avec des sous-groupes H_i qui sont des sous-groupes de Sylow de G et pour tout nombre premier ℓ au moins un ℓ-Sylow fait partie des H_i par choix de S.

□

4.3.2 Le groupe $(\mathbf{Z}/4\mathbf{Z} \wr \mathfrak{S}_n) \rtimes \mathbf{Z}/2\mathbf{Z}$

On fixe pour cette partie un entier naturel non nul n. On voit le produit en couronne $G = \mathbf{Z}/4\mathbf{Z} \wr \mathfrak{S}_n$ comme un groupe de matrices (voir [ShTo] et le lemme 2.3 de [Ré2]) plongé dans $\mathrm{GL}_n(\mathbf{Q}(\mathrm{i}))$ et $H = G \rtimes \mathbf{Z}/2\mathbf{Z}$ est obtenu par l'action de la conjugaison complexe sur G. On a le diagramme d'inclusions

$$\begin{array}{ccc} H & \subset & \mathrm{Aut}_{\mathbf{Q}}\, \mathbf{Q}(\mathrm{i})^n \\ \cup & & \cup \\ G & \subset & \mathrm{GL}_n(\mathbf{Q}(\mathrm{i})). \end{array}$$

Cela permet de voir H comme le produit direct d'ensembles $G \times \{\mathrm{id}, \gamma\}$ où $\gamma \in \mathrm{Aut}_{\mathbf{Q}}\, \mathbf{Q}(\mathrm{i})$ est la conjugaison complexe et on note un élément de H par un couple (g, γ) ou (g, id) avec $g \in G$. Pour $g \in G$ on utilise la notation

$$\overline{g} = \gamma \cdot g = (1, \gamma)(g, \mathrm{id})(1, \gamma).$$

Notre but est ici de résoudre un problème de Grunwald pour H sur un corps de nombres K de manière à ce que $K(\mathrm{i}) = L^G$ où L/K est galoisienne de groupe H et un 2-Sylow de H est un groupe d'inertie de L. L'action de la conjugaison complexe sur G est d'ordre 2 et donc il existe un 2-Sylow de G stabilisé par celle-ci. On peut donc choisir H_2, un 2-Sylow de H, de la forme $G_2 \rtimes \mathbf{Z}/2\mathbf{Z}$ où G_2 est un 2-Sylow de G.

On commence par un lemme technique qui correspond au lemme 4.3.5 dans le cas particulier que l'on traite ici.

Lemme 4.3.8. *Soit $M/\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$ une extension galoisienne finie totalement sauvagement ramifiée. Il existe une extension finie $K_2/\mathbf{Q}_2$ non ramifiée et*

une extension galoisienne totalement ramifiée L_2/K_2 de groupe H_2 vérifiant $L_2^{G_2} = K_2(\mathrm{i})$ et $L_2\mathbf{Q}_2^{\mathrm{nr}} \cap M = \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$.

Démonstration. Par le lemme 4.3.4 on dispose d'une extension galoisienne $L/\mathbf{Q}_2^{\mathrm{nr}}$ de groupe de Galois V un pro-2 groupe libre de rang infini dénombrable. L'extension $\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$ définit un sous-groupe $\widetilde{V}$ d'indice 2 de V. Soit $(s_k)_{k\in\mathbf{N}}$ une base de V. Le groupe $V_{\mathrm{lib}} =< s_k \mid k \in \mathbf{N} >$ est un groupe libre inclus dans V dont l'adhérence est V et $\widetilde{V} \cap V_{\mathrm{lib}} = \widetilde{V}_{\mathrm{lib}}$ est un sous-groupe d'indice 2 de V_{lib} dont l'adhérence est $\widetilde{V}$. Il existe donc $i \in \mathbf{N}$ tel que $s_i \notin \widetilde{V}_{\mathrm{lib}}$. Quitte à renuméroter on peut supposer $i = 0$. Pour $k \geq 1$, si $s_k \notin \widetilde{V}_{\mathrm{lib}}$ alors $s_k s_0 \in \widetilde{V}_{\mathrm{lib}}$ et donc quitte à remplacer s_k par $s_k s_0$ on peut supposer que $s_k \in \widetilde{V}_{\mathrm{lib}}$ pour $k \geq 1$. On vérifie alors que la famille $\{s_0^2, s_k, s_0 s_k s_0^{-1} \mid k \geq 1\}$ est une base de $\widetilde{V}_{\mathrm{lib}}$, ce qui peut aussi se déduire du théorème de Nielsen-Schreier. En raisonnant comme dans la preuve du théorème 5.4.4 de [W] on obtient de plus que $\widetilde{V}$ est un pro-2 groupe libre sur la même base.

On est maintenant en mesure de construire l'extension L_2. Comme M est galoisienne elle est donnée par un morphisme surjectif $f\colon \widetilde{V} \to F$ dont les images de la base $\{s_0^2, s_k, s_0 s_k s_0^{-1} \mid k \geq 1\}$ sont presque toutes égales à 1_F. Soit N un entier tel que pour tout $k \geq N$, $f(s_k) = f(s_0 s_k s_0^{-1}) = 1_F$. On définit alors un morphisme surjectif $\psi\colon \widetilde{V} \to G_2$ en choisissant des images de la base $\{s_0^2, s_k, s_0 s_k s_0^{-1} \mid k \geq 1\}$ de la façon suivante. On choisit pour chaque élément de $g \in G_2 \backslash \{1_{G_2}\}$ un antécédent s_k avec $k > N$ et on impose $\psi(s_0^2) = \psi(s_m) = 1_{G_2}$ pour les autres. On impose de plus $\psi(s_0 s_k s_0^{-1}) = \overline{\psi(s_k)}$ pour tout $k \geq 1$. On étend ce morphisme en un morphisme surjectif $\varphi\colon V \to H_2$ en choisissant des images de la base $\{s_k \mid k \in \mathbf{N}\}$ de façon compatible. Pour cela on pose $\varphi(s_0) = (1_G, \gamma)$ et $\varphi(s_k) = (\psi(s_k), \mathrm{id})$ si $k \geq 1$. Le morphisme φ définit une extension $L_2^{\mathrm{nr}}/\mathbf{Q}_2^{\mathrm{nr}}$ galoisienne de groupe H_2 dont le corps fixé par G_2 est $\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$ par construction et qui vérifie $L_2^{\mathrm{nr}} \cap M = \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$ car $(f, \psi)\colon \widetilde{V} \to F \times G_2$ est surjectif.

À nouveau on peut descendre cette extension en une extension galoisienne totalement ramifiée L_2 de K_2, une extension finie non ramifiée de $\mathbf{Q}_2$, telle que $L_2^{G_2} = K_2(\mathrm{i})$ et $L_2\mathbf{Q}_2^{\mathrm{nr}} = L_2^{\mathrm{nr}}$. □

Par le théorème 2.3.4 on dispose alors pour tout choix de M comme dans l'énoncé d'une extension $K/\mathbf{Q}$ non ramifiée en 2 et avec une unique place v au-dessus de 2 telle qu'on ait une extension galoisienne L_2/K_v totalement ramifiée de groupe H_2 et dont le corps fixé par G_2 est $K_v(\mathrm{i})$. Ceci sera utilisé pour le résultat principal de cette partie avec le lemme de géométrie algébrique suivant qui permet de remplacer les résultats de Saltman.

Lemme 4.3.9. *Soit K un corps de nombres ne contenant pas* i. *On fait agir le groupe H par K-automorphismes sur $R = K(\mathrm{i})[(X_g)_{g\in G}]$ de manière à avoir $(h,\gamma)\cdot aX_g = \overline{a}X_{h\overline{g}}$ pour $h,g \in G$ et $a \in K(\mathrm{i})$. Alors il existe des polynômes algébriquement indépendants $(P_a)_{a\in\mathcal{A}}$ de R et un polynôme $P \in K[(P_a)_{a\in\mathcal{A}}] \setminus \{0\}$ tels que*

$$R\big[\frac{1}{P}\big]^H = K\big[(P_a)_{a\in\mathcal{A}}, \frac{1}{P}\big].$$

De plus, on peut choisir P de manière à ce que l'extension $R[\frac{1}{P}]/R[\frac{1}{P}]^H$ soit étale.

Démonstration. On considère la représentation régulière de G sur $K(\mathrm{i})$ donnée par

$$\mathrm{Reg} = \bigoplus_{g\in G} K(\mathrm{i})X_g.$$

Le sous-espace V engendré par la famille de vecteurs $Y_i = \sum_{g\in G} \overline{g_{i,1}}X_g$, $1 \le i \le n$ est une sous-représentation de Reg isomorphe à la représentation standard (donnée par $G \subset \mathrm{GL}_n(K(\mathrm{i}))$). En effet, pour $h \in G$ on a

$$\begin{aligned} h\cdot Y_i &= \sum_{g\in G} \overline{g_{i,1}}X_{hg} \\ &= \sum_{g\in G} \overline{(h^{-1}g)_{i,1}}X_g. \end{aligned}$$

Or la matrice de h^{-1} est la conjuguée de la transposée de h d'où

$$\begin{aligned} h\cdot Y_i &= \sum_{g\in G}\sum_{j=1}^{n} h_{j,i}\overline{g_{j,1}}X_g \\ &= \sum_{j=1}^{n} h_{j,i}Y_j. \end{aligned}$$

Soient W un supplémentaire de V dans Reg et $L = K(\mathrm{i})(Y_1,\dots,Y_n)$. Par le lemme 3.5 de [CTS] on a

$$W\otimes L = (W\otimes L)^G \otimes_{L^G} L.$$

Soit $(\widetilde{F}_j)_{j\in J}$ une base de $(W\otimes L)^G$ sur L^G. Comme on a une injection

$$(W\otimes L)^G \longrightarrow (\mathrm{Reg}\otimes L)^G$$

on peut écrire $\widetilde{F}_j = \sum_{g\in G} g(P_j)\otimes X_g$ avec $P_j \in L$.

Maintenant on a $K(\mathrm{i})((X_g)_{g\in G}) = L(W\otimes L) = L((F_j)_{j\in J})$ avec F_j l'image de $\widetilde{F}_j$ par $P\otimes X_g \mapsto PX_g$. Il suit l'égalité $K(\mathrm{i})((X_g)_{g\in G})^G = L^G(F_j)$. On peut par ailleurs vérifier que L^G est engendré par les fonctions symétriques en les $Y_1^4,\dots,Y_n^4$. D'après le théorème 1(c) de [Bo] IV.6.1 la famille $\{Y_1^{4b_1}\cdots Y_n^{4b_n} \mid 0\le b_i\le n-i\}$ est une base de $K(\mathrm{i})(Y_i^4)$ sur L^G donc la famille $\{Y_1^{a_1}\cdots Y_n^{a_n} \mid a\in\mathcal{A}\}$ avec $\mathcal{A} = \{a\in\mathbf{N}^n \mid a_i\le 4(n-i)+3\}$ est une base de L sur L^G. Il suit que chaque F_j est une combinaison linéaire sur L^G des éléments de la famille

$$\{P_a = \sum_{g\in G} g(Y_1^{a_1}\cdots Y_n^{a_n})X_g\}_{a\in\mathcal{A}}.$$

Ces éléments étant stables par G on a des inclusions

$$K(\mathrm{i})((X_g)_{g\in G})^G = L^G(F_j)\subset L^G(P_a)\subset K(\mathrm{i})((X_g)_{g\in G})^G$$

d'où l'égalité $K(\mathrm{i})((X_g)_{g\in G})^G = L^G((P_a)_{a\in\mathcal{A}})$.

De plus, le calcul suivant montre que les $P_{(4k-1,0,\dots,0)}$ pour $1\le k\le n$ engendrent $K(\mathrm{i})[Y_i]^G$ par les formules de Newton :

$$\begin{aligned}
P_{(4k-1,0,\dots,0)} &= \sum_{g\in G} g\cdot(Y_1^{4k-1})X_g \\
&= \sum_{g\in G}(\sum_{i=1}^n g_{i,1}Y_i)^{4k-1}X_g \\
&= \sum_{g\in G}\sum_{i=1}^n \overline{g_{i,1}}Y_i^{4k-1}X_g \\
&= \sum_{i=1}^n Y_i^{4k-1}\sum_{g\in G}\overline{g_{i,1}}X_g \\
&= \sum_{i=1}^n Y_i^{4k}.
\end{aligned}$$

Il suit $K(\mathrm{i})((X_g)_{g\in G})^G = K(\mathrm{i})((P_a)_{a\in\mathcal{A}})$ et on en déduit l'indépendance algébrique de la famille $(P_a)_{a\in\mathcal{A}}$ car $\operatorname{degtr} K(\mathrm{i})((X_g)_{g\in G}) = \operatorname{Card} G = \operatorname{Card}\mathcal{A}$. Finalement, il existe $P\in K(\mathrm{i})[(P_a)_{a\in\mathcal{A}}]\setminus\{0\}$, que l'on peut choisir stable par conjugaison, tel que

$$R[\frac{1}{P}]^G = K(\mathrm{i})[(P_a)_{a\in\mathcal{A}},\frac{1}{P}]$$

et comme les P_a sont stables par conjugaison on a même

$$R[\frac{1}{P}]^H = K[(P_a)_{a\in\mathcal{A}}, \frac{1}{P}].$$

Quitte à rajouter des facteurs à P de manière à ce que l'extension soit étale on a le résultat annoncé. □

On peut finalement déduire des propositions précédentes le résultat de type Grunwald que l'on veut.

Théorème 4.3.10. *Soit $M/\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$ une extension galoisienne finie totalement sauvagement ramifiée. Il existe un corps de nombres K non ramifié en 2 et une extension galoisienne L/K de groupe H telle que*

(1) le groupe d'inertie en une place w de L au-dessus de 2 est H_2 ;
(2) $L_w^{G_2} = K_v(\mathrm{i})$ où $v = w_{|K}$;
(3) $L_w\mathbf{Q}_2^{\mathrm{nr}} \cap M = \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$.

Démonstration. Par le lemme 4.3.8 appliqué avec M on dispose d'une extension locale L_2/K_2 telle que $L_2^{G_2} = K_2(\mathrm{i})$ et par le théorème 2.3.4 d'un corps de nombres K et d'une place v de K au-dessus de 2 telle que $K_v = K_2$.

Maintenant, le lemme 4.3.9 appliqué avec K fournit un morphisme fini étale galoisien de groupe H

$$\pi\colon W \longrightarrow U$$

où $W = \operatorname{Spec} K(\mathrm{i})[(X_g)_{g\in G}, \frac{1}{P}]$ et $U = \operatorname{Spec} K[(P_a)_{a\in\mathcal{A}}, \frac{1}{P}]$ avec les notations du lemme.

On pose $\mathbf{L}_2 = \operatorname{Ind}_{H_2}^H L_2$ la K_2-algèbre galoisienne de groupe H produit de $[H : H_2]$ copies de L_2 et vérifiant

$$\mathbf{L}_2^G = L_2^{G_2} = K_2(\mathrm{i}).$$

Par le lemme 5.2 de [Sa] appliqué au polynôme $\widetilde{P} \in K[(X_h)_{h\in H}]$ déduit de P par la substitution $X_g = X_{g,\mathrm{id}} + X_{g,\gamma}$ il existe une base normale $(\xi_h)_{h\in H}$ de $\mathbf{L}_2$ sur K_2 qui n'annule pas $\widetilde{P}$. La famille $(w_g)_{g\in G}$ définie par

$$w_g = \xi_{g,\mathrm{id}} + \xi_{g,\gamma}$$

est alors une base normale de $\mathbf{L}_2$ sur $K_2(\mathrm{i})$ qui vérifie de plus

$$\overline{w_g} = w_{\overline{g}}.$$

En effet on a, pour $g \in G$, $\overline{\xi_{g,\mathrm{id}}} = \xi_{\overline{g},\gamma}$, $\overline{\xi_{g,\gamma}} = \xi_{\overline{g},\mathrm{id}}$ par définition du produit semi-direct et du fait que les $(\xi_h)_{h\in H}$ forment une base normale de $\mathbf{L}_2$ sur K_2. Par construction on a de plus $P((w_g)_{g\in G}) = \widetilde{P}((\xi_h)_{h\in H}) \neq 0$. On définit donc une spécialisation qui respecte l'action de H par $X_g \mapsto w_g$ de manière à ce que $P(w_g) \neq 0$. Cela induit un diagramme commutatif

$$\begin{array}{ccc} K(\mathrm{i})[(X_g)_{g\in G}, \frac{1}{P}] & \longleftarrow & K[(P_a)_{a\in\mathcal{A}}, \frac{1}{P}] \\ \downarrow & & \downarrow{\scriptstyle \varphi_2} \\ \mathbf{L}_2 & \longleftarrow & K_2. \end{array}$$

Le morphisme φ_2 détermine ainsi un K_2-point z_2 de U. La fibre de $z_2 \in U(K_2)$ est $\operatorname{Spec}\mathbf{L}_2$ par construction.

Il reste à voir qu'un point K-rationnel de U assez proche de z_2 a une fibre connexe qui donne une extension de corps qui convient. Comme U vérifie l'approximation faible on peut, par le théorème 1.3 de [Ek], choisir un K-point $z \in U$ suffisamment proche de z_2 pour la topologie analytique sur $U(K_2)$ dont la fibre est connexe et assez proche de manière à avoir l'égalité $\pi^{-1}(\iota_2^* z) = \pi^{-1}(z_2)$ par le lemme 3.5.74 de [Po], avec $\iota_2 \colon \operatorname{Spec} K_2 \to \operatorname{Spec} K$. Soit L le corps tel que $\pi^{-1}(z) = \operatorname{Spec} L$. C'est une extension galoisienne de groupe H. Par ce qui précède on a un isomorphisme de K_2-algèbres galoisiennes

$$L \otimes K_2 \simeq \mathbf{L}_2$$

ce qui assure le comportement local de L. □

4.4 Variétés abéliennes tordues

On va maintenant utiliser les résultats des deux parties précédentes pour construire les variétés abéliennes de l'énoncé du théorème 4.1.1. Notre méthode consiste à tordre une variété abélienne A, c'est-à-dire la remplacer par une variété abélienne B sur K telle que $B_L \simeq A_L$ pour une extension galoisienne finie L/K (on dit que B est une L/K-forme de A). On commence par étudier l'effet de ce procédé sur les groupes de monodromie finie.

4.4.1 Les résultats de torsion

On généralise le théorème 4.3 de [SZ4] énoncé pour les corps locaux dans deux directions différentes. Tout d'abord on obtient une généralisation directe aux corps de nombres et dans un second temps on donne une version avec des hypothèses réduites.

Dans la suite de cette partie, pour un corps de nombres K et une place non archimédienne v de K, on fixe un choix de plongement $\overline{K} \hookrightarrow \overline{K_v}$ et donc une place $\overline{v}$ de $\overline{K}$ au-dessus de v. On note $I(\overline{v}/v)$ le groupe d'inertie de $\overline{K_v}/K_v$ vu comme sous-groupe du groupe de décomposition de $\mathrm{Gal}(\overline{K}/K)$ associé à $\overline{v}$.

Théorème 4.4.1. *Soient A une variété abélienne de dimension g sur un corps de nombres K ayant bonne réduction et L/K une extension galoisienne finie. Pour toute place finie v de K, on note I_v le sous-groupe d'inertie de la place $\overline{v}_{|L}$ de L au-dessus de v. Soit*

$$c\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}A_L$$

un morphisme injectif. Alors il existe une variété abélienne B de dimension g sur K telle qu'on ait des isomorphismes $\Phi_{B,v} \simeq I_v$ pour toute place finie v de K.

Démonstration. On considère le morphisme

$$\tilde{c}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}A_L$$

obtenu en composant c et la surjection $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K)$.

Soient B la variété abélienne obtenue en tordant A par le cocycle $\tilde{c}$ et φ l'isomorphisme $B_L \to A_L$ qui vérifie $\varphi\sigma(\varphi)^{-1} = \tilde{c}(\sigma)$ pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K)$ (ce procédé est décrit page 131 de [Se2]).

Soient v une place finie de K et $w = \overline{v}_{|L}$ la place de L au-dessus de v définie par $\overline{v}$. On a $\Phi_{B,v} = I(\overline{v}/v)/I_{B,v}$ où $I_{B,v} = \{\sigma \in I(\overline{v}/v) \mid \rho_{B,\ell}(\sigma) = 1\}$ avec ℓ un nombre premier distinct de la caractéristique p du corps résiduel de v. On obtient

$$\rho_{B,\ell}(\sigma) = \sigma(\varphi^{-1})\rho_{A,\ell}(\sigma)\varphi = \varphi^{-1}\tilde{c}(\sigma)\rho_{A,\ell}(\sigma)\varphi.$$

Il suit

$$I_{B,v} = \{\sigma \in I(\overline{v}/v) \mid \tilde{c}(\sigma)\rho_{A,\ell}(\sigma) = 1\}.$$

Comme A a bonne réduction on a $\rho_{A,\ell}(\sigma) = 1$ ce qui donne $I_{B,v} = \mathrm{Ker}\,\tilde{c}_{|I(\overline{v}/v)}$. On montre maintenant l'égalité $\mathrm{Ker}\,\tilde{c}_{|I(\overline{v}/v)} = I(\overline{v}/w)$. Par définition de $\tilde{c}$ on a $\mathrm{Ker}\,\tilde{c} = \mathrm{Gal}(\overline{K}/L)$ car $\mathrm{Ker}\,c = \{1\}$. Il suit $\mathrm{Ker}\,\tilde{c}_{|I(\overline{v}/v)} = \mathrm{Gal}(\overline{K}/L) \cap I(\overline{v}/v) = I(\overline{v}/w)$. On en déduit

$$\Phi_{B,v} = I(\overline{v}/v)/I(\overline{v}/w) = I_v.$$

□

L'énoncé précédent ne suffit pas pour construire des variétés abéliennes CM avec monodromie finie sauvage maximale en une place résiduelle de caractéristique 2. Pour ce faire on s'affranchit de l'hypothèse de bonne réduction. Dans le cas d'une variété abélienne sur un corps local on utilise des notations analogues à celles introduites dans le paragraphe 4.1.1 sans la mention de la place en indice.

Théorème 4.4.2. *Soient A une variété abélienne sur un corps local K à corps résiduel algébriquement clos et L/K une extension galoisienne finie. On suppose que le corps K_A de définition des endomorphismes de $A_{\overline{K}}$ est un sous-corps de L et que A a bonne réduction potentielle. On suppose de plus que $L \cap K_{A,s} = K_A$. Soit*

$$c\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut} A_L$$

un cocycle tel que $c_{|\mathrm{Gal}(L/K_A)}$ est injectif. Alors la L/K-forme de A associée au cocycle c est une variété abélienne B sur K telle que

$$[L : K_A][K_{A,s} : K] \mid [K_{B,s} : K] \operatorname{Card} \mathcal{C} \mid [LK_{A,s} : K] \operatorname{Card} \mathcal{C}$$

où $\mathcal{C}$ est le centralisateur de $\mathrm{Gal}(K_{A,s}/K_A)$ dans $\Phi_A = \mathrm{Gal}(K_{A,s}/K)$.

Démonstration. On considère le morphisme

$$\tilde{c}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut} A_L$$

obtenu en composant c et la surjection $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K)$.

Soient B la variété abélienne obtenue en tordant A par le cocycle $\tilde{c}$ et φ l'isomorphisme $B_L \to A_L$ qui vérifie $\varphi\sigma(\varphi)^{-1} = \tilde{c}(\sigma)$ pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

On a $\Phi_B = \mathrm{Gal}(\overline{K}/K)/I_B$ où $I_B = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid \rho_{B,\ell}(\sigma) = 1\}$ avec ℓ un nombre premier distinct de la caractéristique p du corps résiduel. On obtient par la formule de torsion, pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\rho_{B,\ell}(\sigma) = \sigma(\varphi^{-1})\rho_{A,\ell}(\sigma)\varphi = \varphi^{-1}\tilde{c}(\sigma)\rho_{A,\ell}(\sigma)\varphi.$$

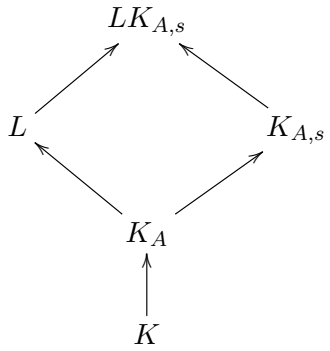
Il suit

$$I_B = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid \tilde{c}(\sigma)\rho_{A,\ell}(\sigma) = 1\}.$$

Soit $\sigma \in I_{B,v}$. L'action de $\tilde{c}(\sigma)$ sur le module de Tate $\mathrm{T}_\ell A$ se fait par K_A-automorphismes. Il suit que $\tilde{c}(\sigma)$ vu comme automorphisme de $\mathrm{T}_\ell A$ commute aux éléments de $\mathrm{Gal}(K_{A,s}/K_A) \subset \mathrm{Aut}\, \mathrm{T}_\ell A$. La dernière inclusion vient de ce que $\rho_{A,\ell}$ induit une injection $\mathrm{Gal}(K_{A,s}/K) \subset \mathrm{Aut}\, \mathrm{T}_\ell A$ par définition

de $K_{A,s}$. Il suit que $\rho_{A,\ell}(\sigma)$ commute aux éléments de $\mathrm{Gal}(K_{A,s}/K_A)$ car $\rho_{A,\ell}(\sigma) = \tilde{c}(\sigma)^{-1}$ et est donc dans $\mathcal{C}$.

Les hypothèses donnent le diagramme d'extensions suivant



On considère maintenant la restriction $(\rho_{A,\ell})_{|I_B} : I_B \to \mathrm{Gal}(K_{A,s}/K)$. Par ce qui précède son image est dans $\mathcal{C}$ et son noyau est par construction $I_B \cap \mathrm{Ker}\,\rho_{A,\ell}$. On montre que cette intersection est égale à $\mathrm{Gal}(\overline{K}/LK_{A,s})$. Soit donc $\sigma \in I_B \cap \mathrm{Ker}\,\rho_{A,\ell}$. Comme $\mathrm{Ker}\,\rho_{A,\ell} = \mathrm{Gal}(\overline{K}/K_{A,s})$ on a $\sigma_{|K_{A,s}} = \mathrm{id}$ et en particulier $\sigma_{|K_A} = \mathrm{id}$. La description de I_B assure par ailleurs que $\tilde{c}(\sigma) = c(\sigma_{|L}) = 1$. Or $\sigma_{|L} \in \mathrm{Gal}(L/K_A)$ par ce qui précède et l'hypothèse sur c donne $\sigma_{|L} = \mathrm{id}$. Il suit $\sigma_{|LK_{A,s}} = \mathrm{id}$ comme annoncé.

On a

$$[K_{B,s} : K] = \mathrm{Card}\,\mathrm{Gal}(LK_{A,s}/K)/(I_B/\mathrm{Gal}(\overline{K}/LK_{A,s}))$$

et on déduit de l'étude précédente

$$\mathrm{Card}\,I_B/\mathrm{Gal}(\overline{K}/LK_{A,s}) \mid \mathrm{Card}\,\mathcal{C}.$$

Finalement on obtient

$$[L : K_A][K_{A,s} : K] \mid [K_{B,s} : K]\,\mathrm{Card}\,\mathcal{C}$$

comme annoncé. □

4.4.2 Les résultats d'existence

Le théorème 4.1.1 est obtenu à partir des constructions suivantes. La première donne pour chaque premier impair l'existence de variétés abéliennes avec grosse monodromie finie sauvage.

Proposition 4.4.3. *Soient K un corps de nombres et g un entier non nul. On note p un diviseur premier impair de $M(2g)$. On suppose qu'il existe une variété abélienne A sur K vérifiant*

(i) $\dim A = \frac{p-1}{2}$;

(ii) $\operatorname{End} A \simeq \mathbf{Z}[\zeta_p]$;

(iii) A admet une polarisation principale ;

(iv) A a bonne réduction.

Soit S un ensemble fini de places ultramétriques de K contenant une place v au-dessus de p. Alors il existe une extension finie L de K telle que,

(1) au-dessus de chaque place de S il existe une unique place de L et elle est non ramifiée ;

(2) si w est la place de L au-dessus de v il existe une variété abélienne B principalement polarisée de dimension g sur L vérifiant

$$\operatorname{Card} \Phi_{B,w} = p^{r(2g,p)}.$$

Démonstration. On note G le groupe $\mathbf{Z}/p\mathbf{Z} \wr \mathfrak{S}_n$ avec $n = \lfloor \frac{2g}{p-1} \rfloor$. La proposition 4.3.7 assure l'existence d'une extension L de K vérifiant la propriété (1) et qui admet de plus une extension galoisienne M/L de groupe G dont le groupe d'inertie au-dessus de w est un p-Sylow de G.

Par les hypothèses sur A on a $\operatorname{Aut} A^n \simeq \mathrm{GL}_n(\mathbf{Z}[\zeta_p])$. Le groupe G s'identifie alors à un sous-groupe unitaire de $\operatorname{Aut}(A^n)$ en considérant les matrices ayant exactement un élément de $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ par ligne et par colonne (voir la proposition 4 de [GL] pour plus de détails). On obtient une injection

$$c\colon \operatorname{Gal}(M/L) \longrightarrow \operatorname{Aut}(A^n_M).$$

Le théorème 4.4.1 donne alors l'existence d'une variété abélienne B', M/L-forme de A^n_L avec pour groupe de monodromie finie en w un p-Sylow de G qui d'après le lemme 4.3.2 est de cardinal $p^{r(2g,p)}$. Soit une telle variété abélienne B'. On peut choisir une polarisation principale de A^n par produit d'une polarisation principale sur A qui donne la conjugaison complexe comme involution de Rosati sur $\operatorname{End} A$. La polarisation produit est principale et son involution de Rosati est la composition de la transposition et de la conjugaison complexe sur les coefficients des matrices. Comme le cocycle que l'on considère a pour image un groupe de matrices unitaires la condition du lemme 4.2.4 est vérifiée et B' admet une polarisation principale.

La dimension de B' est $b = \dim A^n = \frac{p-1}{2} \cdot \lfloor \frac{2g}{p-1} \rfloor \leq g$. Soit $k = g - b$. On considère $B = B' \times C^k$ où C est une courbe elliptique CM sur L ayant bonne réduction en v_1. Alors B est une variété abélienne de dimension g qui admet une polarisation principale et avec $\Phi_{B,w} \simeq \Phi_{B',w}$ par construction. Il suit que L vérifie aussi (2). □

La situation pour $p = 2$ est plus délicate. On va construire des formes tordues de puissances de la courbe elliptique $E\colon y^2 = x^3 - x$ sur $\mathbf{Q}$. L'application du théorème 4.4.2 avec un corps L bien choisi va permettre de gagner un facteur 2 par rapport à la construction générale utilisée pour les premiers impairs. Un corps L qui convient est bien sûr donné par le théorème 4.3.10.

Théorème 4.4.4. *Soit g un entier naturel non nul. Il existe une variété abélienne A principalement polarisée de dimension g sur un corps de nombres K telle que $A_{\overline{K}}$ est CM et* $\operatorname{Card}\Phi_{A,v} = 2^\alpha$ *avec $\alpha \geq r(2g,2) + 1 - g$ pour une place v de K de corps résiduel de caractéristique* 2.

Démonstration. Soit E la courbe elliptique donnée par l'équation $y^2 = x^3 - x$ sur $\mathbf{Q}$. Le corps de définition des endomorphismes de $E_{\overline{\mathbf{Q}}}$ est $\mathbf{Q}(\mathrm{i})$ et E a bonne réduction potentielle en 2 avec pour groupe de monodromie finie $\Phi_{E,2} = Q_8$ le groupe des quaternions d'ordre 8, comme le montre le tableau p. 358 de [Kr] (on a $\Delta = 2^6$ et $c_4 = 2^4 \cdot 3$). Sur $\mathbf{Q}_2^{\mathrm{nr}}$ on a une tour $\mathbf{Q}_2^{\mathrm{nr}} \subset \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i}) \subset (\mathbf{Q}_2^{\mathrm{nr}})_{E,s}$ où $\mathrm{Gal}((\mathbf{Q}_2^{\mathrm{nr}})_{E,s}/\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i}))$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ et est son propre centralisateur dans $\Phi_{E,2}$. Soit $A = E^g$. Le théorème 4.3.10 appliqué avec $M = (\mathbf{Q}_2^{\mathrm{nr}})_{A,s}$ fournit un corps de nombres K non ramifié en 2 et une extension galoisienne L de K de groupe H telle que

(1) H_2 est le groupe d'inertie d'une place w au-dessus de 2;
(2) $L_w^{G_2} = K_v(\mathrm{i})$ où $v = w_{|K}$;
(3) $L_w\mathbf{Q}_2^{\mathrm{nr}} \cap (\mathbf{Q}_2^{\mathrm{nr}})_{A,s} = L_w^{\mathrm{nr}} \cap (\mathbf{Q}_2^{\mathrm{nr}})_{A,s} = (\mathbf{Q}_2^{\mathrm{nr}})_A = \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})$.

On note $\widetilde{G}$ le sous-groupe $\mathrm{Gal}(L/K(\mathrm{i}))$ de $\mathrm{Gal}(L/K)$. L'injection $L \hookrightarrow L_w$ donne une inclusion $G_2 \subset \widetilde{G}$ et le fait que $(1,\gamma) \in H_2$ agit non trivialement sur i. Comme $\widetilde{G}$ est d'indice 2 il est distingué et la suite exacte

$$1 \longrightarrow \widetilde{G} \longrightarrow H \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 1$$

est scindée par le choix de l'élément $(1,\gamma) \in H$. On a donc une écriture de H comme produit semi-direct de $\widetilde{G}$ et $\{(1,\mathrm{id}),(1,\gamma)\}$ ce qui permet de définir un cocycle

$$c\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}\, A_L$$

comme dans la démonstration de la proposition 2.2 de [Ré2]. Par construction ce cocycle vérifie que la restriction $c_{|\widetilde{G}}$ est injective.

Soit B la variété abélienne obtenue comme L/K-forme de A associée au cocycle c. Alors $B_{\mathbf{Q}_2^{\mathrm{nr}}}$ est la $L_w^{\mathrm{nr}}/\mathbf{Q}_2^{\mathrm{nr}}$-forme de $A_{\mathbf{Q}_2^{\mathrm{nr}}}$ associée à ce même cocycle restreint à H_2. De plus, la restriction $c_{|G_2}$ est injective du fait que $c_{|\widetilde{G}}$ l'est et $G_2 \subset \widetilde{G}$. Les hypothèses du théorème 4.4.2 sont vérifiées et celui-ci

montre que B vérifie l'énoncé. En effet on obtient les divisibilités

$$[L_w^{\mathrm{nr}} : \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})][\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i}) : \mathbf{Q}_2^{\mathrm{nr}}][(\mathbf{Q}_2^{\mathrm{nr}})_{A,s} : \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})] \mid [(\mathbf{Q}_2^{\mathrm{nr}})_{B,s} : \mathbf{Q}_2^{\mathrm{nr}}] \cdot \operatorname{Card} \mathcal{C}$$

et

$$[(\mathbf{Q}_2^{\mathrm{nr}})_{B,s} : \mathbf{Q}_2^{\mathrm{nr}}] \mid [L_w^{\mathrm{nr}}(\mathbf{Q}_2^{\mathrm{nr}})_{A,s} : \mathbf{Q}_2^{\mathrm{nr}}]$$

où $\mathcal{C}$ est le centralisateur de $\mathrm{Gal}((\mathbf{Q}_2^{\mathrm{nr}})_{A,s}/\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i}))$ dans $\mathrm{Gal}((\mathbf{Q}_2^{\mathrm{nr}})_{A,s}/\mathbf{Q}_2^{\mathrm{nr}})$. Cela donne $\operatorname{Card} \Phi_{B,v} = [(\mathbf{Q}_2^{\mathrm{nr}})_{B,s} : \mathbf{Q}_2^{\mathrm{nr}}] = 2^\alpha$ pour un entier α. De plus on a par construction $[L_w^{\mathrm{nr}} : \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})][\mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i}) : \mathbf{Q}_2^{\mathrm{nr}}] = \operatorname{Card} H_2 = 2^{r(2g,2)-g+1}$ et $[(\mathbf{Q}_2^{\mathrm{nr}})_{A,s} : \mathbf{Q}_2^{\mathrm{nr}}(\mathrm{i})] = \operatorname{Card} \mathcal{C} = 4$. On en déduit l'inégalité

$$\alpha \geq r(2g,2) + 1 - g.$$

On montre que B est principalement polarisée avec le lemme 4.2.4 comme dans la démonstration précédente. □

On est finalement en mesure de démontrer le théorème principal.

Théorème 4.4.5. *Soient g un entier naturel non nul et K un corps de nombres non ramifié en 2. On note $p_1, \ldots, p_n$ les diviseurs premiers impairs de $M(2g)$. Alors il existe une extension finie L de K telle que pour chaque $i \in \{1, \ldots, n\}$ il existe une variété abélienne A_i de dimension g principalement polarisée sur L et une place v_i de L avec*

$$\operatorname{Card} \Phi_{A_i,v_i} = p_i^{r(2g,p_i)}$$

et il existe une variété abélienne principalement polarisée A de dimension g sur L et une place v de L telles que

$$\operatorname{Card} \Phi_{A,v} = 2^\alpha$$

et $\alpha \geq r(2g,2) + 1 - g$.

Démonstration. On rappelle (voir paragraphe 4.1.1) que les groupes de monodromie finie sont invariants par extension non ramifiée.

On construit maintenant le corps L de l'énoncé par compositum. Pour un corps de nombres L' on note $S_{L'}$ l'ensemble des places ultramétriques de L' divisant 2 ou l'un des p_i.

Par le théorème 4.4.4 il existe un corps L_2 avec une variété abélienne principalement polarisée A de dimension g sur L_2 et une place v au-dessus de 2 de L_2 telles que

$$\operatorname{Card} \Phi_{A,v} = 2^\alpha$$

où $\alpha \geq r(2g,2)+1-g$.

Par ailleurs la proposition 4.2.2 assure l'existence de corps K_{p_i} pour tous les p_i, ramifiés seulement en p_i et des places de caractéristiques résiduelles $p > \max p_i$, tels que toute extension K'/K_{p_i} vérifie les hypothèses de la proposition 4.4.3 pour $S_{K'}$. On considère alors l'extension K' obtenue par compositum de K, L_2 et les K_{p_i}. Par construction K'/L_2 est non ramifiée au-dessus de v. La proposition 4.4.3 alors appliquée avec K' et chacun des p_i donne des extensions L_{p_i}/K' non ramifiées au-dessus de $S_{K'}$ et avec une place v_i au-dessus de p_i ainsi qu'une variété abélienne A_i de dimension g principalement polarisée sur L_{p_i} vérifiant

$$\operatorname{Card} \Phi_{A_i,v_i} = p_i^{r(2g,p_i)}.$$

Le corps L/K' obtenu par compositum des L_p est non ramifié au-dessus de $S_{K'}$ par construction et donc convient. □

Remarque 4.4.6. On aurait pu énoncer le théorème sur un corps de nombres K seulement modérément ramifié au-dessus de 2.

Si on ne demande que l'existence de variétés abéliennes avec monodromie finie sauvage maximale pour les premiers impairs le théorème vaut sur tout corps de nombres K.

Théorème 4.4.7. *Soient g un entier naturel non nul et K un corps de nombres. On note $p_1,\dots,p_n$ les diviseurs premiers impairs de $M(2g)$. Alors il existe une extension finie L de K non ramifiée au-dessus des places de caractéristiques résiduelles 2 de K telle que pour chaque $i \in \{1,\dots,n\}$ il existe une variété abélienne A_i de dimension g principalement polarisée sur L et une place v_i de L avec*

$$\operatorname{Card} \Phi_{A_i,v_i} = p_i^{r(2g,p_i)}$$

4.5 Une majoration dans le cas CM

On considère dans cette partie un corps de nombres K, une variété abélienne A de dimension g sur K et une place finie v de K. On note comme précédemment K_A le corps de définition des endomorphismes de $A_{\overline{K}}$ et A' la variété abélienne A_{K_A}. Le but est l'obtention du théorème 4.1.2 que l'on déduit du cas isotypique.

On suppose donc dans un premier temps que $A_{\overline{K}}$ est isotypique et CM. En particulier, par le théorème 6.(a) de [ST], la variété abélienne A a bonne

réduction potentielle et, par le lemme 4.2.5, A' est isogène à une puissance d'une variété abélienne B simple et CM sur K_A. On note Z le corps $\mathrm{End}\, B \otimes \mathbf{Q}$ qui n'est autre que le centre de $\mathrm{End}\, A' \otimes \mathbf{Q}$. On introduit pour cette partie les notations suivantes :

$$2d = [Z : \mathbf{Q}],\ h = \frac{g}{d} \text{ et } n = v_2(2d).$$

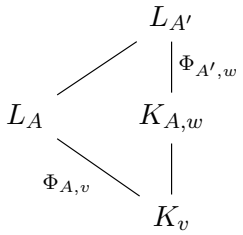
Avec ces notations A' est isogène à B^h et la dimension de $\mathrm{End}\, A' \otimes \mathbf{Q}$ sur son centre Z est h^2. On fixe de plus une place w de K_A au-dessus de v. Comme les groupes de monodromie finie sont invariants par isogénie et puissance on a $\Phi_{A',w} \simeq \Phi_{B,w}$.

Proposition 4.5.1. *On a la relation de divisibilité*

$$\mathrm{Card}\, \Phi_{A,v} \mid [K_A : K]\, \mathrm{Card}\, \mu_Z$$

où μ_Z est le groupe des racines de l'unité de Z.

Démonstration. On note $L_{A'}$ et L_A les extensions de $K_{A,w}$ et K_v respectivement telles que $\mathrm{Gal}(L_{A'}/K_{A,w}) = \Phi_{A',w}$ et $\mathrm{Gal}(L_A/K_v) = \Phi_{A,v}$. On a le diagramme d'extensions locales suivant



Il suit la relation de divisibilité

$$\mathrm{Card}\, \Phi_{A,v} \mid [K_{A,w} : K_v]\, \mathrm{Card}\, \Phi_{A',w}.$$

Or par le théorème 6.(b) de [ST] $\mathrm{Card}\, \Phi_{A',w} = \mathrm{Card}\, \Phi_{B,w}$ divise $\mathrm{Card}\, \mu_Z$ et par ailleurs $[K_{A,w} : K_v]$ divise $[K_A : K]$ du fait que K_A/K est une extension galoisienne. □

On est alors amené à majorer la 2-partie de $[K_A : K]$ en fonction de Z et g. Le théorème 1.2 de [GK] donne une borne de divisibilité pour $[K_A : K]$ optimale mais indépendante de Z ce qui n'est pas suffisant ici.

On rappelle que la borne de Schur est donnée pour un entier naturel non nul s et un corps de nombres F, par

$$S(s,F) = 2^{s-\lfloor s/t(F,2)\rfloor} \prod_{p \text{ premier}} p^{m(F,p)\lfloor s/t(F,p)\rfloor} \Big(\Big\lfloor \frac{s}{t(F,p)} \Big\rfloor ! \Big)_p,$$

où $\lfloor x \rfloor$ est la partie entière de x et $m_p = p^{v_p(m)}$. On a en particulier

$$v_2(S(s,\mathbf{Q}(\mathrm{i}))) = r(2s,2) - s.$$

D'après la preuve de la proposition 3.6 de [Ré2] on a la divisibilité

$$[K_A : K] \mid [Z : \mathbf{Q}]\Gamma_Z(h)$$

en notant

$$\Gamma_Z(h) = \mathrm{ppcm}\{\mathrm{Card}\, G \mid G \subset \mathfrak{A}^\times/Z^\times, [\mathfrak{A} : Z] = h^2\}$$

où $\mathfrak{A}$ parcourt les algèbres centrales simples sur Z de dimension h^2 et G les sous-groupes finis de $\mathfrak{A}^\times/Z^\times$. Les théorèmes 4.1 et 4.2 du même article relient $\Gamma_Z(d)$ à la borne de Schur et donnent ici

$$[K_A : K]\,\mathrm{Card}\,\mu_Z \mid [Z : \mathbf{Q}]S(h,Z). \tag{4.1}$$

On va majorer la valuation 2-adique du produit $[Z : \mathbf{Q}]S(h,Z)$. Avec les notations simplifiées $m(Z,2) = m$, $t(Z,2) = t$ on a, pour tout entier naturel non nul s,

$$v_2(S(s,Z)) = s + (m-1)\Big\lfloor \frac{s}{t} \Big\rfloor + \sum_{i=1}^{\infty} \Big\lfloor \frac{s}{2^i t} \Big\rfloor.$$

On remarque que $v_2(S(s,Z))$ ne dépend que de m et t, c'est-à-dire que $v_2(S(s,Z)) = v_2(S(s,Z^{(2)}))$.

De cette formule exacte on peut déduire le lemme suivant qui nous ramène à étudier le cas d'une valuation maximale lorsque le degré de l'extension $Z/\mathbf{Q}$ est fixé.

Lemme 4.5.2. *Soient s, d des entiers naturels non nuls et $n = v_2(2d)$. Le maximum des $v_2(S(s,Z))$ lorsque Z parcourt les corps de nombres de degré $2d$ est obtenu pour une extension de degré $\frac{2d}{2^n}$ de $Z^{(2)} = \mathbf{Q}(\mu_{2^{n+1}})$. De plus, ce maximum est atteint seulement si $Z^{(2)} = \mathbf{Q}(\mu_{2^{n+1}})$.*

Démonstration. On sait par le lemme 4.4 de [Ré2] que $t = 1$ ou 2. Comme la formule est croissante avec m pour t fixé il suffit de comparer les valeurs pour m maximal dans les deux cas. Pour $t = 1$ la valeur maximale possible de m est $n + 1$ et elle est $n + 2$ pour $t = 2$. Il suffit donc de vérifier

$$s + ns + \sum_{i=1}^{\infty} \Big\lfloor \frac{s}{2^i} \Big\rfloor - s - (n+1)\Big\lfloor \frac{s}{2} \Big\rfloor - \sum_{i=1}^{\infty} \Big\lfloor \frac{s}{2^{i+1}} \Big\rfloor > 0.$$

Or on a

$$\Big\lfloor \frac{s}{2} \Big\rfloor + ns > (n+1)\Big\lfloor \frac{s}{2} \Big\rfloor$$

pour $n \geq 1$. □

Appliqué à notre situation ce lemme donne l'inégalité suivante

$$v_2([Z : \mathbf{Q}]S(h, Z)) \leq v_2\big(2^n S(h, \mathbf{Q}(\mu_{2^{n+1}}))\big).$$

Par ailleurs le calcul suivant permet de se ramener à $\mathbf{Q}(\mathrm{i})$:

$$v_2(S(h, \mathbf{Q}(\mu_{2^{n+1}}))) = v_2(S(2^{n-1}h, \mathbf{Q}(\mathrm{i}))) - 3 \cdot 2^{n-1}h + (n+2)h.$$

En effet, on a

$$\begin{aligned} v_2(S(h, \mathbf{Q}(\mu_{2^{n+1}}))) - v_2(S(2^{n-1}h, \mathbf{Q}(\mathrm{i}))) &= h + nh + \sum_{i \geq 1} \Big\lfloor \frac{h}{2^i} \Big\rfloor \\ &\quad - 2^{n-1}h - 2^{n-1}h - \sum_{i \geq 1} \Big\lfloor \frac{2^{n-1}h}{2^i} \Big\rfloor \\ &= (n+1)h - 2 \cdot 2^{n-1}h - h \sum_{i=0}^{n-2} 2^i \\ &= (n+2)h - 3 \cdot 2^{n-1}h. \end{aligned}$$

On peut maintenant conclure dans le cas isotypique.

Théorème 4.5.3. *Soit A une variété abélienne de dimension g sur un corps de nombres K telle que $A_{\overline{K}}$ est isotypique et CM. Alors on a la majoration*

$$v_2(\mathrm{Card}\, \Phi_{A,v}) \leq r(2g, 2) - g + 1$$

pour toute place ultramétrique v de K. De plus l'égalité ne peut intervenir que lorsque $A_{\overline{K}}$ est isogène à une puissance de la courbe elliptique $y^2 = x^3 - x$.

Démonstration. Par la proposition 4.5.1 et la relation de divisibilité (4.1) on a

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2([Z:\mathbf{Q}]S(h,Z)).$$

Le calcul qui suit le lemme 4.5.2 permet alors de majorer $v_2(\mathrm{Card}\,\Phi_{A,v})$ par

$$v_2(S(2^{n-1}h,\mathbf{Q}(\mathrm{i}))) - 3\cdot 2^{n-1}h + (n+2)h + n.$$

Finalement avec $h \geq 1$ et la croissance stricte en s de $v_2(S(s,\mathbf{Q}(\mathrm{i})))$ on obtient

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(S(g,\mathbf{Q}(\mathrm{i}))) - 3\cdot 2^{n-1} + 2n + 2.$$

On raisonne maintenant suivant la valeur de n. Si $n \geq 2$ on a $-3\cdot 2^{n-1} + 2n + 2 \leq 0$ et il vient

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(S(g,\mathbf{Q}(\mathrm{i}))) = r(2g,2) - g.$$

Dans le cas $n = 1$, on distingue alors deux situations. Tout d'abord si $Z^{(2)} \neq \mathbf{Q}(\mathrm{i})$ l'inégalité du lemme 4.5.2 est stricte donc on obtient

$$v_2(\mathrm{Card}\,\Phi_{A,v}) < v_2(S(h,\mathbf{Q}(\mathrm{i}))) + 1$$

ce qui donne

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq r(2g,2) - g.$$

Il reste la situation où $n = 1$ et $Z^{(2)} = \mathbf{Q}(\mathrm{i})$. La majoration est alors

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(S(h,\mathbf{Q}(\mathrm{i}))) + 1.$$

Si $Z \neq Z^{(2)}$ la croissance stricte en s de $v_2(S(s,\mathbf{Q}(\mathrm{i})))$ donne

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(S(g,\mathbf{Q}(\mathrm{i}))) = r(2g,2) - g$$

et si $Z = Z^{(2)}$ alors $h = g$ et l'inégalité est bien

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(S(g,\mathbf{Q}(\mathrm{i}))) + 1 = r(2g,2) - g + 1.$$

Dans ce cas $Z = \mathbf{Q}(\mathrm{i})$ impose que B est une courbe elliptique avec multiplication complexe par $\mathbf{Q}(\mathrm{i})$. La théorie de la multiplication complexe donne alors que $B_{\overline{K}}$ est isogène à la courbe d'équation $y^2 = x^3 - x$. □

On termine cette partie par le passage du cas isotypique au cas général qui nécessite un dernier lemme technique de majoration inspiré du lemme 4.6 de [GK].

Lemme 4.5.4. *Soit p un nombre premier. Pour des entiers naturels non nuls s et g tels que s divise g, on a l'inégalité*

$$sr(\frac{2g}{s}, p) + v_p(s!) \leq r(2g, p).$$

Démonstration. Soit k le plus petit entier naturel tel que $\left\lfloor \frac{2g}{sp^k(p-1)} \right\rfloor = 0$. On a

$$r(2g,p) = \sum_{i=0}^{\infty} \left\lfloor \frac{2g}{p^i(p-1)} \right\rfloor = \sum_{i=0}^{k-1} \left\lfloor \frac{2g}{p^i(p-1)} \right\rfloor + \sum_{i=k}^{\infty} \left\lfloor \frac{2g}{p^i(p-1)} \right\rfloor.$$

Alors pour $i < k$, c'est-à-dire $\left\lfloor \frac{2g}{sp^i(p-1)} \right\rfloor \neq 0$, on a

$$s \cdot \left\lfloor \frac{2g}{sp^i(p-1)} \right\rfloor \leq \left\lfloor \frac{2g}{p^i(p-1)} \right\rfloor$$

d'où

$$sr(\frac{2g}{s}, p) + \sum_{i=1}^{\infty} \left\lfloor \frac{2g}{p^{k-1}p^i(p-1)} \right\rfloor \leq r(2g,p).$$

Par ailleurs, par choix de k, $\left\lfloor \frac{2g}{sp^{k-1}(p-1)} \right\rfloor \geq 1$ et il suit que, pour $i \geq 1$,

$$\left\lfloor \frac{2g}{p^{k-1}p^i(p-1)} \right\rfloor = \left\lfloor \frac{2g}{sp^{k-1}(p-1)} \cdot \frac{s}{p^i} \right\rfloor \geq \left\lfloor \frac{2g}{sp^{k-1}(p-1)} \right\rfloor \cdot \left\lfloor \frac{s}{p^i} \right\rfloor \geq \left\lfloor \frac{s}{p^i} \right\rfloor$$

ce qui donne

$$\sum_{i=1}^{\infty} \left\lfloor \frac{2g}{p^{k-1}p^i(p-1)} \right\rfloor \geq v_p(s!).$$

□

Une disjonction de cas permet finalement d'obtenir la majoration.

Théorème 4.5.5. *Soit A une variété de dimension g sur un corps de nombres K telle que $A_{\overline{K}}$ est CM. Alors on a*

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq r(2g,2) + 1 - g$$

pour toute place ultramétrique v de K. De plus, l'égalité ne peut intervenir que lorsque une composante isotypique de $A_{\overline{K}}$ est isogène à une puissance de la courbe elliptique $y^2 = x^3 - x$.

Démonstration. On raisonne par récurrence sur la dimension g de A.

Le cas où $A_{\overline{K}}$ est isotypique est traité dans le théorème 4.5.3. On suppose donc que $A_{\overline{K}}$ n'est pas isotypique.

Soient $C_1, \ldots, C_n$ les composantes isotypiques de $A_{\overline{K}}$, avec $n \geq 2$ par hypothèse, qui sont permutées par l'action de $\mathrm{Gal}(\overline{K}/K)$.

S'il existe deux parties $(C_i)_{i\in I}, (C_j)_{j\in J} \subset \{C_1, \ldots, C_n\}$ non vides et stables par cette action telles que $I \cup J = \{1, \ldots, n\}$, alors il existe des sous-variétés abéliennes non nulles C et D de A telles que $C_{\overline{K}} = \sum_{i\in I} C_i$, $D_{\overline{K}} = \sum_{j\in J} C_j$ et $A = C + D$. En particulier on a $\mathrm{Hom}_{\overline{K}}(C_{\overline{K}}, D_{\overline{K}}) = 0$ ce qui assure que seule l'une des variétés $C_{\overline{K}}$ et $D_{\overline{K}}$ peut avoir une composante isotypique isogène à une puissance de la courbe $E\colon y^2 = x^3 - x$. Soient L_A, L_C et L_D les plus petites extensions galoisiennes de K_v^{nr} sur lesquelles A, C et D atteignent réduction semi-stable. Alors on a l'inclusion $L_A \subset L_C L_D$ et comme le groupe de Galois de $L_C L_D$ sur K_v^{nr} est un sous-groupe du produit $\Phi_{C,v} \times \Phi_{D,v}$ on a l'inégalité

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(\mathrm{Card}\,\Phi_{C,v}) + v_2(\mathrm{Card}\,\Phi_{D,v}).$$

On note $g_1 = \dim C$ et $g_2 = \dim D$. Par l'hypothèse de récurrence on obtient

$$\begin{aligned} v_2(\mathrm{Card}\,\Phi_{C,v}) + v_2(\mathrm{Card}\,\Phi_{D,v}) &\leq r(2g_1, 2) - g_1 + r(2g_2, 2) - g_2 + 1 \\ &\leq r(2g, 2) - g + 1 \end{aligned}$$

ce qui conclut dans ce cas. De plus, l'une des variétés $C_{\overline{K}}$ ou $D_{\overline{K}}$ a une composante isotypique isogène à une puissance de la courbe $E\colon y^2 = x^3 - x$ si et seulement si c'est le cas pour $A_{\overline{K}}$. Il suit que si $A_{\overline{K}}$ n'a pas de telle composante isotypique l'inégalité est stricte.

Sinon l'action est transitive. Les variétés abéliennes C_i sont conjuguées sous l'action du groupe de Galois et ont donc même dimension g/n. Dans ce cas les algèbres $\mathrm{End}\, C_i \otimes \mathbf{Q}$ sont toutes isomorphes. La théorie de la multiplication complexe assure alors que si l'une des C_i est isogène à une puissance de la courbe $E\colon y^2 = x^3 - x$ les autres le sont aussi, ce qui est absurde.

Soit L/K donné par le noyau de l'action de $\mathrm{Gal}(\overline{K}/K)$ sur les C_i. On a $[L : K] | n!$ et il existe des sous-variétés D_i de A_L telles que $(D_i)_{\overline{K}} = C_i$ et A_L est isogène au produit des D_i. Par ailleurs pour une place $w|v$ de L on a l'inégalité

$$v_2(\mathrm{Card}\,\Phi_{A,v}) \leq v_2(\mathrm{Card}\,\Phi_{A_L,w}) + v_2([L : K]).$$

Or, par le théorème 4.5.3 on a

$$v_2(\mathrm{Card}\,\Phi_{D_i,w}) \leq r(\frac{2g}{n}, 2) - \frac{g}{n}$$

pour tout $i \geq 1$. Il suit par le lemme 4.5.4 et l'hypothèse de récurrence

$$\begin{aligned} v_2(\mathrm{Card}\,\Phi_{A_L,w}) &\leq \sum_{i=1}^{n} v_2(\mathrm{Card}\,\Phi_{D_i,w}) \\ &\leq \sum_{i=1}^{n} (r(\frac{2g}{n}, 2) - \frac{g}{n}) \\ &\leq r(2g, 2) - g - v_2(n!). \end{aligned}$$

Finalement on a obtenu

$$\begin{aligned} v_2(\mathrm{Card}\,\Phi_{A,v}) &\leq r(2g, 2) - g - v_2(n!) + v_2([L : K]) \\ &\leq r(2g, 2) - g. \end{aligned}$$

□

Bibliographie

[AT] E. Artin et J. Tate. *Class Field Theory.* Benjamin. New York. 1968.

[BL] C. Birkenhake et H. Lange. *Complex abelian varieties.* Grundlehren der mathematischen Wissenschaften. Springer Verlag. Berlin. 1992.

[BLR] S. Bosch, W. Lütkebohmert et M. Raynaud. *Néron Models.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer Verlag. Berlin. 1990.

[BK] A. Brumer et K. Kramer. Non-existence of certain semistable abelian varieties. *Manuscr. Math.* 106, p.291–304, 2001.

[Bo] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 4 à 7.* Springer. Berlin. 2007.

[CCO] C.-L. Chai, B. Conrad et F. Oort. *Complex multiplication and lifting problems.* Mathematical Surveys and Monographs. American Mathematical Society, Providence. 2014.

[Ch] S. Checcoli. A note on Galois groups and local degrees. *Manuscripta Mathematica.* 159. 2019. p. 1–12.

[CM] P. Chrétien et M. Matignon. Maximal wild monodromy in unequal characteristic. *Journal of Number Theory.* 133. 2013. p. 1389–1408.

[CTS] J.-L. Colliot-Thélène et J.-J. Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). *Algebraic groups and homogeneous spaces. Proceedings of the international colloquium, Mumbai, India, January 6–14, 2004* Narosa Publishing House. New Delhi. 2007. p. 113–186.

[Ek] T. Ekedahl. An effective version of Hilbert's irreducibility theorem. *Séminaire de théorie des nombres, Paris 1988-1989.* Progress in Mathematics. 91. Birkhäuser. Berlin. 1990. p. 241–248.

[GIT] D. Mumford, J. Fogarty et F. Kirwan. *Geometric invariant theory. 3rd enl. ed.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 34. Springer Verlag. Berlin. 1993.

[FO] J.-M. Fontaine et Y. Ouyang. *Theory of p-adic Galois representations.* https://www.imo.universite-paris-saclay.fr/∼fontaine/galoisrep.pdf, à paraître.

[GK] R. Guralnick et K. Kedlaya. Endomorphism fields of abelian varieties. *Research in Number Theory* 3. 2017. p. 1–10.

[GL] R. Guralnick et M. Lorenz. Orders of finite groups of matrices. *Groups, rings and algebras,* Contemp. Math. 420. Amer. Math. Soc. Providence. 2006. p. 141–161.

[Ka] Y. Katznelson. On the orders of finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$. *Expositiones Mathematicae*. 12. 1994. p. 453–457.

[Ko] H. Koch. *Galois theory of p-extensions.* Springer Monographs in Mathematics. Springer. Berlin. 2002.

[Kr] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Mathematica.* 69. 1990. p. 353–385.

[Mo] L. Moret-Bailly. Problèmes de Skolem sur les champs algébriques. *Compositio Mathematica.* 125. 2001. p. 1–30.

[Mu] D. Mumford. *Abelian Varieties.* Tata Institute of Fundamental Research Studies in Mathematics, London. 1970.

[MGE] B. Moonen, G. der Geer et B. Edixhoven. *Abelian varieties.* https://www.math.ru.nl/ bmoonen/research.html.

[N] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer Monographs in Mathematics. 2004.

[NSW] J. Neukirch, A. Schmidt et K. Wingberg. *Cohomology of Number Fields.* A Series of Comprenhsive Studies in Mathematics. Springer. Berlin. 2013.

[No] B. Noohi. Fundamental groups of algebraic stacks. *Journal of the Institute of Mathematics of Jussieu.* 3. 2004. p. 69–103.

[Ph] S. Philip. Variétés abéliennes CM et grosse monodromie finie sauvage. arXiv:2103.04197 (33 p.)

[Po] B. Poonen. *Rational points on varieties.* Graduate Studies in Mathematics. AMS. Providence. 2017.

[Ré1] G. Rémond. Variétés abéliennes et ordres maximaux. *Revista Matemática Iberoamericana* 33. 2017. p. 1173–1195.

[Ré2] G. Rémond. Degré de définition des endomorphismes d'une variété abélienne. *Journal of European Mathematical Society.* 22. 2020. p. 3059–3099.

[Ri] P. Ribenboim. *The theory of classical valuations.* Springer Monographs in Mathematics. Springer. New York. 1999.

[Sa] D. Saltman. Generic Galois extensions and problems in field theory. *Advances in Mathematics.* 43. 1982. p. 250–283.

[Se1] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae.* 15. 1972. p. 259–331.

[Se2] J.-P. Serre. *Cohomologie galoisienne.* Lecture Notes in Mathematics. Springer. Berlin. 1965.

[Se3] J.-P. Serre. *Bounds for the orders of finite subgroups of* $G(k)$. Group Representation Theory. EPFL Press. Lausanne. 2006.

[SGA1] A. Grothendieck. Séminaire de géométrie algébrique du Bois Marie 1960-61. Revêtements étales et groupe fondamental (SGA 1). Un séminaire dirigé par Alexander Grothendieck. Augmenté de deux exposés de M. Raynaud. *Documents Mathématiques.* Société Mathématique de France. Paris. 2003.

[SGA7] Groupes de monodromie en géométrie algébrique. I. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 1). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, 288. Springer-Verlag, Berlin-New York, 1972.

[ST] J.-P. Serre et J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88, p. 492–517, 1968.

[SZ1] A. Silverberg et Y. Zarhin. Semistable reduction and torsion subgroups of abelian varieties. *Annales de l'institut Fourier.* 45. 1995. p. 403–420.

[SZ2] A. Silverberg et Y. Zarhin. Subgroups of inertia groups arising from abelian varieties. *Journal of Algebra.* 209. 1998. p. 403–420.

[SZ3] A. Silverberg et Y. Zarhin. Étale cohomology and reduction of abelian varieties. *Bulletin de la Société Mathématique de France.* 129. 2001. p. 141–157.

[SZ4] A. Silverberg et Y. Zarhin. Inertia groups and abelian surfaces. *Journal of Number Theory.* 110. 2005. p. 178–198.

[Si] J. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics. 106. Springer. Dordrecht. 2009.

[ShTo] G. Shephard et J. Todd. Finite unitary reflection groups. *Canadian Journal of Mathematics.* 6. 1954. p. 274–304.

[Sh] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton Mathematical Series. 46. Princeton University Press. Princeton. 1960.

[Sp] T.A. Springer. *Linear Algebraic groups.* Modern Birkhäuser Classics. 1998.

[St] J. Stix *Rational Points and Arithmetic of Fundamental Groups. Evidence for the section conjecture.* Lecture Notes in Mathematics. 2054. Springer. Berlin. 2013.

[W] J. S. Wilson. *Profinite Groups.* London Mathematical Society Monographs New Series, 19. Oxford University Press. Oxford. 1998.