View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by OpenGrey Repository

UNIVERSITÉ DE LA MÉDITERRANÉE
AIX-MARSEILLE II
Faculté des Sciences de Luminy
ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE E.D. 184

THÈSE

pour obtenir le grade de

Docteur de l'Université de la Méditerranée

Discipline : Mathématiques

par

Safia HALOUI

sous la direction de Yves AUBRY

Titre :

SUR LE NOMBRE DE POINTS RATIONNELS DES VARIÉTÉS ABÉLIENNES SUR LES CORPS FINIS

soutenue publiquement le 14 juin 2011

JURY

Yves Aubry	MdC (HDR) Univ. Sud Toulon-Var	
Jean-Marc Couveignes	Prof. Univ. Toulouse II	
Sylvain Duquesne	Prof. Univ. Rennes I	
Gilles Lachaud	DR CNRS IML	
Kristin Lauter	Microsoft Research	Rapporteur
Marc Perret	Prof. Univ. Toulouse II	Rapporteur
Christophe Ritzenthaler	MdC (HDR) Univ. de la Méditerranée	

Remerciements

Je voudrais commencer par remercier mon directeur de thèse Yves Aubry pour son aide et sa patience, pour ses commentaires avisés qui m'ont permis de mettre de l'ordre dans mes idées, et aussi pour m'avoir toujours encouragée à aller jusqu'au bout de cette thèse bien que les choses n'aient pas toujours été faciles.

Mon travail sur les polynômes caractéristiques de variétés abéliennes de petite dimension fait suite à une suggestion de Christophe Ritzenthaler que je remercie vivement. Merci aussi d'avoir patiemment répondu à mes questions, particulièrement celles relatives à la rédaction de cette thèse, d'avoir accepté d'être membre de mon jury et bien sûr d'avoir activement participé à l'animation de la vie du laboratoire.

Je tiens également à remercier Gilles Lachaud pour l'intérêt qu'il a bien voulu porter à mon travail, pour avoir accepté ma contribution à son article avec Yves et pour sa présence en tant que membre du jury .

Je remercie Kristin Lauter et Marc Perret d'avoir accepté de rapporter cette thèse, qui plus est dans de si brefs délais. Merci encore à Marc Perret pour ses nombreuses remarques et corrections qui ont aidé à l'amélioration du présent document. Je remercie également Jean-Marc Couveignes et Sylvain Duquesne d'avoir accepté de faire partie de mon jury.

J'ai réellement apprécié l'ambiance régnant au sein de l'IML et je tiens donc à exprimer ma reconnaissance à tous ses membres. Je voudrais souligner l'importance qu'a eue pour moi le groupe de travail de l'équipe ATI : j'y ai énormément appris. J'aimerais spécialement remercier François Rodier, Stéphane Ballet et David Kohel pour les raisons évoquées ci-dessus. Il y a bien sûr aussi les thésards de l'équipe ATI sans qui mon séjour à l'IML aurait été quelque peu morose. Merci donc à Tammam, Christophe, Florian, Stéphanie, Virgile, Hamish, Marc, Julia, Yih-Dar et Alexey pour les discussions mathématiques, les blagues douteuses, avoir supporté ma "pénibilité", les soirées toujours très animées (les nausées du lendemain), et encore bien d'autres choses. J'en profite pour remercier Vijay, membre temporaire du groupe des thésards.

Je remercie chaleureusement ma mère Isabelle et Jean-Louis pour leur important soutien moral et pour les petits services rendus qui m'ont grandement simplifié la vie. J'ai plus généralement bénéficié de l'appui de ma famille, bien trop nombreuse pour citer tout le monde ; cela ne diminue en rien la gratitude que je leur porte.

Je remercie Mickaël pour avoir relu cette thèse et surtout pour avoir été à mes côtés depuis tant d'années. Je tiens également à exprimer ma reconnaissance à toutes les personnes qui m'ont offert une escapade hors de l'Univers des Mathématiques ; j'ai une pensée particulière pour Cécile, Laura, Laurène, Camille et ma soeur Leila.

J'aimerais dédier cette thèse à ma grand-mère Josette, bien qu'il soit un peu trop tard.

Table des matières

Préliminaires

0.1 Introduction

Etant donnée une variété abélienne A de dimension g sur un corps fini $\mathbb{F}_q$, $q = p^n$, nous pouvons considérer son polynôme caractéristique ; c'est par définition le polynôme caractéristique de l'endomorphisme de Frobenius de A agissant sur son module de Tate $T_\ell(A)$ où $\ell \neq p$ est un nombre premier, nous le noterons $p_A(t)$. Le polynôme $p_A(t)$ ne dépend que de la classe d'isogénie de A et de plus, par le Théorème de Honda-Tate, il caractérise cette dernière. C'est en outre un objet très intéressant lorsque l'on cherche à obtenir des informations sur le nombre de points rationnels des variétés abéliennes sur les corps finis puisque sa valeur en 1 est égale au nombre de points rationnels de A.

Le polynôme $p_A(t)$ est unitaire, à coefficients entiers, de degré $2g$ et l'ensemble de ses racines comptées avec multiplicité est constitué de couples de nombres complexes conjugués de module $\sqrt{q}$; un polynôme possédant ces propriétés sera appelé polynôme de Weil. On vérifie immédiatement que tout polynôme de Weil est de la forme

$$t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

pour certains entiers relatifs $a_1, \ldots, a_g$.

Ainsi, la description de l'ensemble des polynômes caractéristiques possibles pour une variété abélienne de dimension g définie sur $\mathbb{F}_q$ peut se faire en deux étapes : on commence par donner une caractérisation des $(a_1, \ldots, a_g)$ correspondant à des polynômes de Weil, puis on utilise des résultats de la théorie de Honda-Tate pour déterminer quels polynômes de Weil sont des polynômes caractéristiques de variétés abéliennes (on trouvera quelques rappels à ce sujet dans la Section 0.3.2).

Le problème évoqué ci-dessus a été résolu par Deuring [4] et Waterhouse [38] lorsque A est une courbe elliptique. En 1990, Rück a donné une description des polynômes caractéristiques irréductibles de surfaces abéliennes ; ses travaux ont été complétés par Maisner, Nart [16] et Xing [41, 42] qui ont traité le cas réductible et listé les polynômes caractéristiques supersinguliers. Xing a par ailleurs travaillé sur les polynômes caractéristiques des variétés abéliennes de dimension 3 et 4 dans [40].

Dans le premier chapitre, nous expliquons comment décrire l'ensemble des polynômes caractéristiques de variétés abéliennes de dimension donnée puis, après avoir rappelé les résultats cités ci-dessus, nous résolvons le problème en dimension 3 et 4 (ces travaux ont donné lieu à [6, 7]).

Dans le deuxième chapitre, nous nous intéressons au nombre de points rationnels des variétés abéliennes sur les corps finis ; plus précisément, nous cherchons à majorer et minorer celui-ci.

Il résulte des propriétés de $p_A(t)$ énoncées dans le premier paragraphe que le nombre de points rationnels de A est compris entre $(q + 1 - 2\sqrt{q})^g$ et $(q + 1 + 2\sqrt{q})^g$. Nous verrons qu'il

est en fait possible, comme dans le cas des courbes, de remplacer dans ces dernières quantités le $2\sqrt{q}$ par sa partie entière ; les bornes ainsi obtenues sont généralement optimales.

En 1990, Lachaud et Martin-Deschamps [12] ont donné des bornes sur le nombre de points de A dans le cas où celle-ci est la jacobienne d'une courbe lisse, projective, absolument irréductible (toutes les courbes considérées dans cette thèse seront supposées avoir ces propriétés). Leurs résultats peuvent être vus comme l'analogue pour les corps de fonctions à une variable sur un corps fini de formules d'estimation du nombre de classes des corps de nombres.

Lorsque nous travaillons en caractéristique impaire, la variété de Prym associée à un revêtement de courbes $\pi : \widetilde{C} \longrightarrow C$ double et non ramifié peut être définie comme étant l'image de $(\sigma - id)$, où σ est l'involution induite par π sur la jacobienne de $\widetilde{C}$. Des bornes sur le nombre de points de ces variétés de Prym ont été établies par Perret [23] en 2006. Dans son article, il remarque aussi que ses bornes peuvent être adaptées aux jacobiennes.

Les bornes dont il est question dans les deux paragraphes précédents dépendent de $\#C(\mathbb{F}_q)$ pour les jacobiennes et de $\#\widetilde{C}(\mathbb{F}_q) - \#C(\mathbb{F}_q)$ pour les variétés de Prym. Dans les deux cas, ce paramètre est au signe et éventuellement à translation par $(q+1)$ près la trace du polynôme caractéristique de la variété abélienne en question. Ainsi, on vérifie que les bornes de Perret se généralisent à une variété abélienne quelconque (mais pas celles de Lachaud et Martin-Deschamps).

Nous donnerons de nouvelles bornes sur le nombre de points des variétés abéliennes sur les corps finis en fonction de leur trace, spécifiques ou non aux jacobiennes (ces résultats proviennent de [1] qui est un travail en collaboration avec Yves Aubry et Gilles Lachaud).

0.2 Notations et conventions

Par corps, on entend corps commutatif ; un corps gauche désigne un corps non nécessairement commutatif. Dans toute la thèse, $\mathbb{F}_q$ désigne un corps à $q = p^n$ éléments, où p est un nombre premier. On note aussi $\mathbb{Q}_p$ le corps des nombres p-adiques et v_p la valuation p-adique.

Toutes les variétés algébriques considérées sont définies sur un corps parfait ; les morphismes entre variétés algébriques sont toujours supposés définis sur le corps de base. Pour plus de renseignements sur les notions de géométrie algébrique abordées, voir [8].

On note $[r]$ la partie entière (inférieure) d'un réel r et pour $k \in \mathbb{N}$, $\binom{r}{k} = \frac{r(r-1)\ldots(r-k+1)}{k!}$ le coefficient binomial (généralisé).

Enfin, lorsque rien n'est précisé, les polynômes irréductibles sont supposés l'être sur $\mathbb{Q}$.

0.3 Généralités sur les variétés abéliennes

Nous donnons ici les définitions et résultats relatifs aux variétés abéliennes dont nous aurons besoin par la suite. On trouvera des précisions ainsi que les preuves des résultats donnés sans justification dans [19, 17, 18]. Le livre de Mumford [21] est une référence classique concernant les variétés abéliennes (toutefois, il ne traite pas des jacobiennes). Aussi, [9] contient un résumé détaillé sur la théorie des variétés abéliennes et jacobiennes.

Dans toute cette section, $\mathbf{k}$ désigne un corps parfait.

0.3.1 Définitions et propriétés

Une *variété en groupe* sur $\mathbf{k}$ est une variété algébrique V sur $\mathbf{k}$ munie de morphismes

$$\begin{aligned} m : V \times_{\mathbf{k}} V &\to V \quad \text{(multiplication)} \\ inv : V &\to V \quad \text{(inverse)} \end{aligned}$$

et d'un élément $e \in V(\mathbf{k})$ tels que la structure sur $V(\overline{\mathbf{k}})$ définie par m et inv soit celle d'un groupe d'élément neutre e. Une variété en groupe est automatiquement non singulière.

Une *variété abélienne* est une variété en groupe complète. Toute application régulière entre variétés abéliennes est la composée d'un homomorphisme et d'une translation. En particulier la loi de groupe sur une variété abélienne est commutative (puisque inv est un homomorphisme) et par conséquent nous noterons la loi de groupe comme une loi additive. Dans les années 1950, Barsotti, Matsusaka et Weil ont prouvé que toute variété abélienne est projective ; nous aurions donc pu définir une variété abélienne comme étant une variété en groupe projective.

Un homomorphisme de variétés abéliennes $\alpha : A \to B$ est appelé *isogénie* s'il possède l'une des propriétés équivalentes suivantes :

1. α est surjective et $\ker(\alpha)$ est un schéma en groupe fini ;
2. $\dim A = \dim B$ et $\ker(\alpha)$ est un schéma en groupe fini ;
3. $\dim A = \dim B$ et α est surjective ;
4. α est finie, plate et surjective

où $\ker(\alpha)$ désigne la fibre au-dessus de l'élément neutre de B (vu comme point fermé de B). Nous dirons alors que A et B sont *isogènes* et nous écrirons $A \sim B$. Le *degré* d'une isogénie α est son degré en tant que morphisme fini, c'est-à-dire $\deg(\alpha) = [\mathbf{k}(A) : \alpha^*\mathbf{k}(B)]$, c'est aussi l'ordre du schéma en groupe fini $\ker(\alpha)$. Si α est séparable, alors elle est étale (si un point était ramifié, par translation, tous le seraient) et ses fibres sont donc réduites. Dans ce cas, le noyau de α aura $\deg(\alpha)$ points sur $\overline{\mathbf{k}}$.

Un exemple important d'isogénie est la multiplication par n où $n \in \mathbb{Z} \setminus \{0\}$; on la note $[n]_A$ et on pose $A[n] = \ker([n]_A)$.

Théorème 0.3.1. *Soient A une variété abélienne de dimension g et $n \in \mathbb{Z} \setminus \{0\}$. Alors $[n]_A : A \to A$ est une isogénie de degré n^{2g} qui est étale si et seulement si la caractéristique de $\mathbf{k}$ ne divise pas n.*

Soient A et B deux variétés abéliennes. La multiplication par n définit une structure de $\mathbb{Z}$-module sur $\mathrm{End}(A)$ et $\mathrm{Hom}(A, B)$; on pose $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ et $\mathrm{Hom}^0(A, B) = \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Si $\alpha : A \to B$ est une isogénie de degré n, alors $\ker(\alpha) \subset A[n]$ et en factorisant $[n]_A$ on obtient une isogénie $\beta : B \to A$ telle que $\beta \circ \alpha = [n]_A$.

Une variété abélienne est dite *simple* si elle ne possède pas de sous-variété abélienne non-triviale. On suppose que A est simple. Alors tout élément non nul $\alpha \in \mathrm{End}(A)$ est une isogénie. L'existence de $\beta : A \to A$ telle que $\beta \circ \alpha = [n]_A$, où $n = \deg(\alpha)$ implique que $\mathrm{End}^0(A)$ est un corps gauche. On montre par un raisonnement analogue que si A et B sont isogènes on a

$$\mathrm{End}^0(A) \simeq \mathrm{Hom}^0(A, B) \simeq \mathrm{End}^0(B)$$

et sinon on a $\mathrm{Hom}^0(A, B) = 0$.

Pour le cas où A n'est pas simple, nous avons la proposition suivante :

Proposition 0.3.2. *Toute variété abélienne A possède des sous-variétés abéliennes simples $A_1, \ldots, A_n$ telles que*

$$A \sim A_1 \times \cdots \times A_n.$$

Ainsi, si $A_1, \ldots, A_r$ sont des variétés abéliennes simples deux à deux non isogènes et $A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}$, on a

$$\mathrm{End}^0(A) \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i}\left(\mathrm{End}^0(A_i)\right)$$

où $\mathcal{M}_{n_i}\left(\mathrm{End}^0(A_i)\right)$ est l'anneau des matrices $n_i \times n_i$ à coefficients dans $\mathrm{End}^0(A_i)$.

Soit ℓ un nombre premier différent de la caractéristique de $\mathbf{k}$. Si A est une variété abélienne de dimension g, le Théorème 0.3.1 nous montre que pour $n \in \mathbb{N}\setminus\{0\}$, $A[\ell^n](\overline{\mathbf{k}})$ est un $\mathbb{Z}/\ell^n\mathbb{Z}$-module libre de rang $2g$.

L'isogénie $[\ell]_A$ induit des homomorphismes $A[\ell^{n+1}](\overline{\mathbf{k}}) \to A[\ell^n](\overline{\mathbf{k}})$, qui nous permettent de définir le *module de Tate* de A comme étant la limite projective

$$T_\ell(A) = \lim_{\leftarrow} A[\ell^n](\overline{\mathbf{k}}).$$

C'est un $\mathbb{Z}_\ell$-module libre de rang $2g$.

Tout élément $\alpha \in \mathrm{Hom}(A,B)$ induit un homomorphisme $T_\ell(\alpha) : T_\ell(A) \to T_\ell(B)$. On vérifie alors que l'application

$$\mathrm{Hom}(A,B) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

ainsi définie est injective. Il en résulte que $\mathrm{Hom}(A,B)$ est sans torsion. Un résultat du même acabit mais plus profond nous permet d'obtenir des informations supplémentaires sur $\mathrm{Hom}(A,B)$:

Théorème 0.3.3. *L'application naturelle*

$$\mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(A), T\ell(B))$$

est injective et de conoyau sans torsion. En particulier, $\mathrm{Hom}(A,B)$ *est un $\mathbb{Z}$-module libre de rang inférieur ou égal à* $4\dim(A)\dim(B)$.

Le *polynôme caractéristique* d'un élément $\alpha \in \mathrm{End}(A)$ est le polynôme caractéristique de $T_\ell(\alpha)$ regardé comme endomorphisme du $\mathbb{Q}_\ell$-espace vectoriel

$$V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell;$$

on le notera $p_\alpha(t)$. Le théorème suivant résume quelques propriétés du polynôme caractéristique d'une isogénie :

Théorème 0.3.4. *Soit A une variété abélienne de dimension g et $\alpha \in End(A)$ une isogénie. Alors*

1. *$p_\alpha(t)$ est indépendant du choix de ℓ,*
2. *$p_\alpha(t)$ est unitaire, à coefficients entiers et de degré $2g$,*
3. *pour tout entier n, on a $p_\alpha(n) = \deg(\alpha - [n]_A)$,*
4. *si $\mathbb{Q}[\alpha] \subseteq \mathrm{End}^0(A)$ est un corps, alors l'ensemble des racines sur $\mathbb{C}$ de $p_\alpha(t)$ coïncide avec celui des racines sur $\mathbb{C}$ du polynôme minimal de α.*

Remarque. Il n'est pas évident de démontrer directement que $p_\alpha(t)$ est indépendant du choix de ℓ. Dans [17], Milne montre d'abord l'existence d'un polynôme vérifiant les propriétés 2 et 3 du Théorème 0.3.4 (pour ce faire, il montre que l'application $\mathrm{End}^0(A) \to \mathbb{Q}$ induite par le degré est une fonction polynomiale homogène de degré $2g$), puis il prouve que ce polynôme est bien le polynôme caractéristique de $T_\ell(\alpha)$ sur $V_\ell(A)$. Cette approche est due à Weil.

0.3.2 Variétés abéliennes sur les corps finis

Dans toute cette section, A désigne une variété abélienne de dimension g définie sur un corps fini $\mathbb{F}_q$, $q = p^n$. Le morphisme $\pi_A : A \to A$ qui est l'identité sur l'espace topologique sous-jacent et $f \mapsto f^q$ sur les sections est appelé *endomorphisme de Frobenius* de A. On voit facilement que π_A est une isogénie ; nous noterons $p_A(t)$ son polynôme caractéristique et nous dirons (par abus de langage) que c'est le *polynôme caractéristique* de A.

Le polynôme $p_A(t)$ détermine le nombre de points rationnels sur $\mathbb{F}_q$ de A . Plus précisément, on a $A(\mathbb{F}_q) = \ker(\pi_A - [1]_A)(\overline{\mathbb{F}_q})$ et comme $\pi_A - [1]_A$ est séparable (on vérifie que sa différentielle est moins l'identité sur l'espace tangent à 0_A), elle est étale. D'où

$$\#A(\mathbb{F}_q) = \deg(\pi_A - [1]_A) = p_A(1).$$

Nous avons aussi le théorème classique suivant :

Théorème 0.3.5 (Weil)**.** *Les racines sur $\mathbb{C}$ de $p_A(t)$ sont toutes de module $\sqrt{q}$.*

Il résulte de ceci que l'ensemble des racines de $p_A(t)$ comptées avec multiplicité est de la forme

$$\{\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}\}$$

où $|\omega_k| = \sqrt{q}$, $k = 1, \ldots, g$. En effet, vu que $p_A(t)$ est à coefficients réels, c'est clair en ce qui concerne les racines non réelles et pour que le coefficient constant de $p_A(t)$ (qui est le degré de π_A) soit un entier positif, il faut que les racines réelles $(\pm\sqrt{q})$ soient de multiplicité paire.

On voit alors facilement que

$$p_A(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

pour certains entiers relatifs $a_1, \ldots, a_g$.

Le *p-rang* de A est la dimension du $\mathbb{F}_p$-espace vectoriel $A[p](\overline{\mathbb{F}_q})$. La proposition suivante nous permet de déduire le p-rang d'une variété abélienne de son polynôme caractéristique ; on trouvera sa démonstration dans [2].

Proposition 0.3.6. *Le p-rang de A est la somme des multiplicités des racines non-nulles de la réduction modulo p de $p_A(t)$.*

On en déduit que le p-rang de A est compris entre 0 et g et que c'est le plus grand entier tel que p ne divise pas a_k (en posant $a_0 = 1$). Une variété abélienne est dite *ordinaire* si elle est de p-rang maximal.

Une variété abélienne est dite *supersingulière* si elle est isogène sur $\overline{\mathbb{F}_q}$ à un produit de courbes elliptiques supersingulières (c'est-à-dire de p-rang nul). Comme il est expliqué dans [5], une variété abélienne est supersingulière si et seulement si tous les ω_i sont de la forme $\zeta\sqrt{q}$ où ζ est une racine de l'unité ; en particulier, une variété abélienne supersingulière est de p-rang nul. La réciproque est fausse pour $g > 2$: nous verrons dans le Chapitre 1 des exemples de variétés abéliennes de dimension 3 et 4 de p-rang nul et non-supersinguliéres (pour la dimension 3, celles dont le polygone de Newton est représenté par la Figure 1.10 et pour la dimension 4, celles dont le polygone de Newton est représenté par l'une des Figures 1.18 ou 1.17).

Les propriétés décrites ci-dessus peuvent facilement être lues sur le polygone de Newton de la variété abélienne étudiée (voir Section 1.1.3).

Le Théorème 0.3.3 implique que $\mathrm{End}^0(A)$ est un $\mathbb{Q}$-espace vectoriel de dimension finie (inférieure ou égale à $4g^2$). Si de plus A est simple, alors π_A est dans le centre du corps gauche $\mathrm{End}^0(A)$ et donc $\mathbb{Q}[\pi_A]$ est un corps.

Un q-nombre de Weil est un entier algébrique tel que pour tout plongement $\sigma : \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$, $|\sigma(\pi)| = \sqrt{q}$. Le Théorème 0.3.5 nous montre que si A est simple, alors π_A est un q-nombre de Weil.

Enfin, avant d'énoncer le Théorème de Honda-Tate, rappelons qu'une isogénie $A \to B$ définit un isomorphisme $\mathrm{End}^0(A) \to \mathrm{End}^0(B)$ (voir Section 0.3.1). Il est facile de vérifier que celui-ci envoie π_A sur π_B.

Théorème 0.3.7 (Honda-Tate)**.** *L'application qui à A associe π_A donne une bijection de l'ensemble des classes d'isogénie de variétés abéliennes simples sur $\mathbb{F}_q$ vers celui des classes de conjugaison des q-nombres de Weil.*

Compte tenu du fait que $p_{A\times B}(t) = p_A(t)p_B(t)$, le Théorème de Honda-Tate implique que la classe d'isogénie d'une variété abélienne sur un corps fini est entièrement déterminée par son polynôme caractéristique.

L'injectivité de l'application du Théorème 0.3.7 provient du Théorème de Tate :

$$\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \mathrm{Hom}(V_\ell(A), V_\ell(B))^{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}$$

et sa surjectivité se montre en utilisant la théorie de la multiplication complexe. Nous ne donnerons pas les détails de la preuve de ce théorème (celle-ci se trouve dans [10, 34, 35]) mais nous allons tout de même énoncer certains résultats établis au cours de celle-ci. Nous avons d'abord besoin de quelques définitions.

Une *algèbre simple centrale* sur un corps $\mathbf{k}$ est une $\mathbf{k}$-algèbre R telle que

1. R soit de dimension finie sur $\mathbf{k}$,
2. $\mathbf{k}$ soit le centre de R,
3. R soit un anneau simple (sans idéal bilatère non-trivial).

Par exemple, un corps gauche de centre $\mathbf{k}$ et de dimension finie sur $\mathbf{k}$ est une algèbre simple centrale sur $\mathbf{k}$.

Le Théorème de Wedderburn nous dit que toute algèbre simple centrale R sur $\mathbf{k}$ est $\mathbf{k}$-isomorphe à une algèbre de matrices sur un corps gauche de centre $\mathbf{k}$ et de dimension finie sur $\mathbf{k}$, ce dernier étant uniquement déterminé par R. Deux algèbres simples centrales sont dites *semblables* si les corps gauches qui leur sont associés par le Théorème de Wedderburn sont isomorphes. L'ensemble des classes d'équivalence définies par cette relation est noté $\mathrm{Br}(\mathbf{k})$. Le produit tensoriel (sur $\mathbf{k}$) induit une loi de groupe commutative sur $\mathrm{Br}(\mathbf{k})$: l'élément neutre est la classe d'équivalence de $\mathbf{k}$ et l'inverse de $[R]$ est $[R^{\mathrm{opp}}]$ où R^{opp} est R en tant que groupe et ab dans R^{opp} est égal à ba dans R. Le groupe abélien $\mathrm{Br}(\mathbf{k})$ est appelé *groupe de Brauer* de $\mathbf{k}$.

Théorème 0.3.8. *1. Si $\mathbf{k}$ est un corps local, on a un homomorphisme injectif canonique*

$$\mathrm{inv}_{\mathbf{k}} : \mathrm{Br}(\mathbf{k}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

qui est un isomorphisme si $\mathbf{k}$ est non-archimédien , d'image $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ si $\mathbf{k} = \mathbb{R}$ et nul si $\mathbf{k} = \mathbb{C}$.

2. Si $\mathbf{k}$ est un corps de nombres, on a une suite exacte

$$0 \to \mathrm{Br}(\mathbf{k}) \to \bigoplus_v \mathrm{Br}(\mathbf{k}_v) \to \mathbb{Q}/\mathbb{Z} \to 0$$

où v parcourt l'ensemble des places de $\mathbf{k}$ et $\mathbf{k}_v$ est le complété de $\mathbf{k}$ en v.

3. *Si* $\mathbf{k}$ *est un corps de nombres et* D *un corps gauche de centre* $\mathbf{k}$ *et de dimension finie sur* $\mathbf{k}$*, alors l'ordre de* $[D]$ *dans* $\mathrm{Br}(\mathbf{k})$ *est* $[D:\mathbf{k}]^{1/2}$.

L'*invariant* d'une algèbre simple centrale R sur un corps de nombres $\mathbf{k}$ en une place v de $\mathbf{k}$ est $\mathrm{inv}_v(R) = \mathrm{inv}_{\mathbf{k}_v}([R \otimes \mathbf{k}_v])$. Le théorème ci-dessus implique que tout corps gauche de centre $\mathbf{k}$ et de dimension finie sur $\mathbf{k}$ est entièrement déterminé par ses invariants.

Revenons aux variétés abéliennes. La preuve du Théorème de Honda-Tate utilise le résultat suivant (voir [35] et [20] pour le calcul des invariants) :

Théorème 0.3.9 (Tate)**.** *Soient* $A/\mathbb{F}_q$ *une variété abélienne simple et* $D = \mathrm{End}^0(A)$*. Alors* D *est un corps gauche de centre* $\mathbb{Q}[\pi_A]$ *et de dimension finie sur* $\mathbb{Q}[\pi_A]$*. L'invariant de* D *en une place* v *de* $\mathbb{Q}[\pi_A]$ *est égal à :*

- $\frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)}[\mathbb{Q}[\pi_A]_v : \mathbb{Q}_p]$ *si* v *est au-dessus de* p*,*
- $1/2$ *si* v *est réelle,*
- 0 *sinon.*

où ord_v *est la valuation discrète associée à* v*. De plus, on a :*

$$2\dim(A) = [D : \mathbb{Q}[\pi_A]]^{1/2}[\mathbb{Q}[\pi_A] : \mathbb{Q}].$$

Le Théorème 0.3.4 nous dit que $p_A(t) = h(t)^e$, où $h(t)$ est le polynôme minimal de π_A. On a donc $e = [D : \mathbb{Q}[\pi_A]]^{1/2}$. Par le Théorème 0.3.8, on en déduit que e est l'ordre de $[D]$ dans $\mathrm{Br}(\mathbb{Q}[\pi_A])$ et donc le plus petit dénominateur commun des invariants de D.

Dans [35], Tate traite séparément le cas où $p_A(t)$ admet une racine réelle (il revient au même de dire que $\pi_A^2 = [q]_A$) : si q est un carré, alors $\mathbb{Q}[\pi_A] = \mathbb{Q}$, donc $e = 2$ et $\dim(A) = 1$; si q n'est pas un carré, alors $\mathbb{Q}[\pi_A] = \mathbb{Q}(\sqrt{p})$, donc $e = 2$ et $\dim(A) = 2$.

Soit maintenant v une place de $\mathbb{Q}[\pi_A]$ au-dessus de p. Le complété de $\mathbb{Q}[\pi_A]$ en v est une extension de $\mathbb{Q}_p$ contenant π_A et minimale pour cette propriété ; il est donc de la forme $\mathbb{Q}_p[t]/(g(t))$, où $g(t)$ est un facteur irréductible de $h(t)$ sur $\mathbb{Q}_p$. Réciproquement, si $g(t)$ est un facteur irréductible de $h(t)$ sur $\mathbb{Q}_p$, la valuation v_p de $\mathbb{Q}_p$ se prolonge de manière unique à $\mathbb{Q}_p[t]/(g(t))$, et la restriction de celle-ci à $\mathbb{Q}[\pi_A]$ donne lieu à une place de $\mathbb{Q}[\pi_A]$ au-dessus de p. Notons $h_v(t)$ le polynôme ainsi associé à v.

Soient $d_v = [\mathbb{Q}[\pi_A]_v : \mathbb{Q}_p]$ le degré de $h_v(t)$ et $\pi_1, \ldots, \pi_{d_v}$ ses racines dans $\overline{\mathbb{Q}_p}$. Pour $i = 1, \ldots, d_v$, la valuation discrète ord_v se prolonge à $\mathbb{Q}_p[\pi_i]$ (qui est isomorphe à $\mathbb{Q}_p[t]/(h_v(t))$) et on a $\mathrm{ord}_v(\pi_i) = \mathrm{ord}_v(\pi_A)$. D'où

$$d_v \mathrm{ord}_v(\pi_A) = \sum_{i=1}^{d_v} \mathrm{ord}_v(\pi_i) = \mathrm{ord}_v\left(\prod_{i=1}^{d_v} \pi_i\right) = \mathrm{ord}_v(h_v(0)) = v_p(h_v(0)).$$

En résumé, on a la proposition suivante :

Proposition 0.3.10. *Soit* $A/\mathbb{F}_q$ *une variété abélienne simple. On suppose que* $p_A(t)$ *est sans racine réelle. Alors*

$$p_A(t) = h(t)^e$$

où $h(t) \in \mathbb{Z}[t]$ *est un polynôme irréductible et* e *est le plus petit dénominateur commun des rationnels* $v_p(h_i(0))/v_p(q)$*, où* $h(t) = \prod_i h_i(t)$ *est la décomposition de* $h(t)$ *en facteurs irréductibles sur* $\mathbb{Q}_p$*.*

0.3.3 Jacobiennes et courbes sur les corps finis

Soit $C/\mathbf{k}$ une courbe lisse, projective, absolument irréductible de genre g. Si $\mathbf{k} \subseteq \mathbf{k}'$ est une extension de corps, on pose $C_{\mathbf{k}'} = C \times_{\mathbf{k}} \mathbf{k}'$. Le *groupe des diviseurs* de C, noté $\mathrm{Div}(C)$, est le groupe abélien libre engendré par les points fermés de C (dans notre cas, la notion de diviseur de Weil coïncide avec celle de diviseur de Cartier) ; il peut être identifié au sous-groupe de $\mathrm{Div}(C_{\overline{\mathbf{k}}})$ fixé par l'action de $\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})$. On note $\mathrm{Pic}^0(C)$ le quotient du groupe des diviseurs de degré 0 de C par celui des diviseurs principaux.

Nous pouvons associer à C une variété abélienne J_C appelée *jacobienne* de C telle que pour tout corps $\mathbf{k} \subseteq \mathbf{k}' \subseteq \overline{\mathbf{k}}$ avec $C(\mathbf{k}') \neq \emptyset$ on ait $J_C(\mathbf{k}') = \mathrm{Pic}^0(C_{\mathbf{k}'})$. En donner une définition rigoureuse et une construction nous mènerait bien trop loin (on trouvera tout ceci dans [18]) ; nous nous contenterons d'énoncer quelques unes des ses propriétés :

1. pour tout corps $\mathbf{k} \subseteq \mathbf{k}' \subseteq \overline{\mathbf{k}}$, on a $J_{C_{\mathbf{k}'}} = J_C \times_{\mathbf{k}} \mathbf{k}'$ (la jacobienne commute avec les extensions de corps),
2. on a $J_C(\mathbf{k}) = \mathrm{Pic}^0(C_{\overline{\mathbf{k}}})^{\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})}$,
3. si C possède un diviseur D de degré 1, alors l'application $C(\overline{\mathbf{k}}) \to J_C(\overline{\mathbf{k}})$ qui à P associe la classe de $P - D$ induit une immersion fermée $C \to J_C$.

Si un diviseur de C est principal dans $\mathrm{Div}(C_{\overline{\mathbf{k}}})$, alors il l'est aussi dans $\mathrm{Div}(C)$ (voir [9, Proposition A.2.2.10]). On a donc un homomorphisme injectif naturel

$$\mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C_{\overline{\mathbf{k}}})^{\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})},$$

c'est un isomorphisme si $C(\mathbf{k}) \neq \emptyset$.

Dans le cas général (voir [18, Remark 1.6]), on a toujours une suite exacte

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C_{\overline{\mathbf{k}}})^{\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})} \to \mathrm{Br}(\mathbf{k}).$$

Si $\mathbf{k}$ est un corps fini, alors $\mathrm{Br}(\mathbf{k})$ est nul (tout corps gauche fini est commutatif) et donc $\mathrm{Pic}^0(C) \simeq \mathrm{Pic}^0(C_{\overline{\mathbf{k}}})^{\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})}$; on trouvera des explications plus concrètes de ce fait dans [3]. Remarquons aussi qu'une courbe sur un corps fini possède toujours un diviseur de degré 1 (voir [33, Corollary 5.1.11]) et on peut donc toujours la plonger dans sa jacobienne.

On suppose maintenant que C est définie sur un corps fini $\mathbb{F}_q$ et pour $k \in \mathbb{N} \setminus \{0\}$, on pose $N_k = \#C(\mathbb{F}_{q^k})$.

La *fonction zêta* de C est

$$Z_C(t) = \exp\Big(\sum_{k=1}^{+\infty} N_k \frac{t^k}{k}\Big).$$

Weil a montré que c'est une fraction rationnelle de la forme

$$Z_C(t) = \frac{\prod_{i=1}^{2g}(1 - \pi_i t)}{(1-t)(1-qt)} \tag{1}$$

où $|\pi_i| = \sqrt{q}$ (analogue de l'Hypothèse de Riemann pour les corps de fonctions). Le numérateur de $Z_C(t)$ est donc un polynôme que nous noterons $\chi_C(t)$.

En appliquant la fonction logarithme à (1) et en développant le deuxième membre en série, on voit que

$$N_k = q^k + 1 - \sum_{i=1}^{2g} \pi_i^k. \tag{2}$$

Soient $p_C(t)$ le polynôme caractéristique de J_C et $\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}$ ses racines. L'identité suivante est basée sur un analogue de la Formule des traces de Lefschetz (voir [19, Theorem 11.1.]) :

$$N_k = q^k + 1 - \sum_{i=1}^{g} (\omega_i^k + \overline{\omega_i}^k). \tag{3}$$

Compte tenu du fait que la $\mathbb{C}$-algèbre des fonctions symétriques à $2g$ variables est engendrée par les sommes des puissances k-ièmes de ces variables, $k = 1, \ldots, 2g$, les identités (2) et (3) impliquent que les ensembles (avec multiplicité) $\{\pi_1, \ldots, \pi_{2g}\}$ et $\{\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}\}$ coïncident. On a donc

$$\chi_C(t) = t^{2g} p_C(\frac{1}{t}).$$

En d'autres termes, les polynômes $\chi_C(t)$ et $p_C(t)$ sont réciproques.

Chapitre 1

Polynômes caractéristiques des variétés abéliennes de petite dimension

Dans ce chapitre nous donnons une description de l'ensemble des polynômes caractéristiques de variétés abéliennes de dimension inférieure ou égale à 4. Les polynômes caractéristiques de courbes elliptiques ont été étudiés par Deuring [4] et Waterhouse [38]. La détermination des polynômes caractéristiques de surfaces abéliennes est due à Rück [26], ses résultats ont été complétés par Maisner, Nart [16] et Xing [41, 42] qui ont examiné le cas supersingulier. Nous expliquerons aussi comment calculer la dimension des variétés abéliennes associées aux q-nombres de Weil de degré 4. Xing a également travaillé sur les polynômes caractéristiques des variétés abéliennes de dimension 3 et 4 dans [40], nous rappellerons ses résultats. La description complète de ces derniers polynômes est faite dans [6, 7].

1.1 Méthode générale

Nous avons vu que le polynôme caractéristique d'une variété abélienne de dimension g définie sur $\mathbb{F}_q$, $q = p^n$ est un polynôme unitaire, à coefficients entiers, de degré $2g$ et dont l'ensemble des racines comptées avec multiplicité est constitué de paires de nombres complexes conjugués, tous de module $\sqrt{q}$. Un polynôme possédant ces dernières propriétés est appelé *polynôme de Weil*.

En faisant jouer les liens existant entre les racines d'un polynôme et ses coefficients, il est facile de voir qu'un polynôme de Weil de degré $2g$ s'écrit sous la forme

$$p(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

avec $a_1, \ldots, a_g \in \mathbb{Z}$. La réciproque est clairement fausse : un tel polynôme n'est pas nécessairement un polynôme de Weil ; en effet, le fait que le module des racines de $p(t)$ soit fixé force ses coefficients à vivre dans des intervalles bornés.

Notre problème qui consiste à décrire l'ensemble des polynômes caractéristiques des variétés abéliennes de dimension g se décompose alors en deux sous-problèmes :

1. Donner une caractérisation des $(a_1, \ldots, a_g)$ correspondant à des polynômes de Weil.
2. Etant donné un polynôme de Weil, déterminer si c'est le polynôme caractéristique d'une variété abélienne.

Le premier problème se traite par des manipulations de fonctions symétriques et l'utilisation de résultats basiques sur les polynômes (Section 1.1.1).

Pour résoudre le second problème, nous avons recours à la théorie de Honda-Tate : la dimension de la classe d'isogénie associée à un polynôme de Weil irréductible est liée à la valuation

p-adique de ses racines dans le corps $\mathbb{Q}_p$ des nombres p-adiques (Section 1.1.2). Un moyen simple d'avoir des informations sur la valuation p-adique des racines d'un polynôme est d'étudier son polygone de Newton. Nous en rappellerons la définition et quelques propriétés dans la Section 1.1.3. Nous expliquerons aussi comment utiliser les polygones de Newton pour résoudre notre problème.

1.1.1 Les coefficients des polynômes de Weil

Dans cette section, nous expliquons comment trouver une condition nécessaire et suffisante pour qu'un polynôme

$$p(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g,$$

$a_1, \ldots, a_g \in \mathbb{Z}$ soit un polynôme de Weil.

D'abord, les racines de $p(t)$ sont non nulles. On vérifie aussi facilement que l'on a

$$p(t) = \frac{t^{2g}}{q^g} p\left(\frac{q}{t}\right).$$

En particulier, si α est une racine de $p(t)$, alors q/α en est aussi une. De plus, comme le coefficient constant de $p(t)$ est un entier positif, $-\sqrt{q}$ et $\sqrt{q}$ ne peuvent être des racines de $p(t)$ que si elles sont de multiplicité paire. On en déduit que l'ensemble des racines de $p(t)$ comptées avec multiplicité est de la forme

$$\{\alpha_1, q/\alpha_1, \ldots, \alpha_g, q/\alpha_g\}.$$

Pour $i = 1, \ldots, g$, on pose $x_i = -(\alpha_i + q/\alpha_i)$, de telle sorte que

$$p(t) = \prod_{i=1}^{g} (t^2 + x_i t + q).$$

Si $p(t)$ est un polynôme de Weil, alors les α_i sont de module $\sqrt{q}$ et sont donc de conjugué complexe q/α_i ; il en résulte que les x_i sont des réels de module inférieur ou égal à $2\sqrt{q}$. Réciproquement, si x_i est réel et $|x_i| \leq 2\sqrt{q}$, alors le polynôme $t^2 + x_i t + q$ est à coefficients réels et de discriminant négatif ou nul ; ses racines sont donc des nombres complexes conjugués de module $\sqrt{q}$, et si ceci est vrai pour tout i, alors $p(t)$ est bien un polynôme de Weil.

En résumé, nous venons de montrer le lemme suivant :

Lemme 1.1.1. *Le polynôme $p(t)$ est un polynôme de Weil si et seulement si les racines des polynômes*

$$f^+(t) = \prod_{i=1}^{g} (t - (2\sqrt{q} + x_i)) \quad \text{et} \quad f^-(t) = \prod_{i=1}^{g} (t - (2\sqrt{q} - x_i))$$

sont toutes réelles et positives.

Nous nous sommes donc ramenés au problème de décider si un polynôme à coefficients réels de degré g ne possède que des racines réelles et positives. Ceci nous donnera des conditions sur les coefficients de $f^+(t)$ et de $f^-(t)$ et ces derniers sont en fait des polynômes en les a_i.

L'étude du discriminant de nos polynômes nous permettra de déterminer leur nombre de racines réelles. Par exemple, si $f(t)$ est un polynôme unitaire à coefficients réels et de degré g, d'une part il est clair que son discriminant Δ_f est nul si et seulement si $f(t)$ a une racine

multiple et d'autre part, si $\Delta_f \neq 0$, en notant respectivement $x_1, \ldots, x_k$ et $y_1, \overline{y_1}, \ldots, y_\ell, \overline{y_\ell}$ les racines réelles (rangées par ordre croissant) et non réelles de $f(t)$ (avec $k + 2\ell = g$), on déduit de la formule

$$\Delta_f = (-1)^{g(g-1)/2} \prod_{i=1}^{k} f'(x_i) \prod_{i=1}^{\ell} f'(y_i) f'(\overline{y_i}) = (-1)^{g(g-1)/2} \prod_{i=1}^{k} f'(x_i) \prod_{i=1}^{\ell} |f'(y_i)|^2$$

que le signe de Δ_f est celui de $(-1)^\ell$. En effet, $f(t)$ est alternativement croissante et décroissante au voisinage de $x_k, \ldots, x_1$, ce qui nous donne le signe des $f'(x_i)$. On en déduit que $\prod_{i=1}^{k} f'(x_i)$ est positif si $k \equiv 0$ ou $1 \mod 4$ et négatif sinon ; en d'autres termes, son signe est celui de $(-1)^{k(k-1)/2}$. Le signe de Δ_f est donc celui de $(-1)^{k(k-1)/2+g(g-1)/2}$. De plus, $k(k-1) = (g - 2\ell)(g-1-2\ell) = g(g-1) + 4\ell^2 - 4g\ell + 2\ell$ donc $k(k-1)/2 + g(g-1)/2 = g(g-1) + 2\ell^2 - 2g\ell + \ell$ est de même parité que ℓ.

Pour simplifier les calculs, on utilisera le fait que les racines de $f^+(t)$ et $f^-(t)$ sont toutes réelles si et seulement si celles de

$$f^0(t) \quad = \quad \prod_{i=1}^{g} (t + x_i - \frac{a_1}{g}) \tag{1.1}$$

le sont. Le polynôme $f^0(t)$ a l'avantage d'être de trace nulle, ce qui simplifie considérablement l'expression de son discriminant.

Soit $f(t) = t^g + r_1 t^{g-1} + \cdots + r_g$ un polynôme n'ayant que des racines réelles. Si toutes ses racines sont positives, alors il en est de même pour leurs fonctions symétriques et en particulier on a

$$(-1)^i r_i \quad \geq \quad 0 \tag{1.2}$$

pour $i = 1, \ldots, g$. La réciproque est vraie, cela peut se voir par récurrence. En effet, le résultat est trivial pour $g = 1$ et si $(-1)^i r_i \geq 0$ pour $i = 1, \ldots, g$ et que l'hypothèse est vérifiée pour $(g-1)$ alors $f'(t)$ n'a que des racines positives. Comme $f'(t)$ possède toujours une racine entre deux racines consécutives de $f(t)$, le polynôme $f(t)$ ne peut avoir qu'une seule racine négative. L'existence d'une unique racine négative implique $(-1)^g r_g \leq 0$, et donc $r_g = 0$ par notre supposition de départ. On obtient alors une contradiction en appliquant l'hypothèse de récurrence à $f(t)/t$.

Remarque. Il est aussi possible d'utiliser la méthode de Robinson décrite par Smyth dans [31, §2, Lemma] pour décider si les racines de $f^+(t)$ et de $f^-(t)$ sont toutes réelles et positives. Cela implique toutefois des calculs bien plus longs, particulièrement en dimension 4.

Remarque. L'utilisation de la méthode décrite dans cette section (ainsi que de celle de Robinson) nécessite le calcul des racines d'un polynôme de degré $(g-1)$; par conséquent, nous pourrons obtenir des formules générales et explicites si et seulement si $g \leq 5$. Vu les formules pour $g = 4$ (Théorème 1.4.1), nous pouvons nous attendre à ce que celles pour $g = 5$ soient compliquées et difficiles (sur le plan calculatoire) à établir.

1.1.2 Polynômes caractéristiques des variétés abéliennes

Nous expliquons ici comment décider si un polynôme de Weil donné est le polynôme caractéristique d'une variété abélienne de dimension g. Soient donc A une variété abélienne de dimension g définie sur $\mathbb{F}_q$, $q = p^n$ et $p_A(t)$ son polynôme caractéristique.

Si A n'est pas simple, disons $A \sim A_1 \times A_2$, alors $p_A(t) = p_{A_1}(t)p_{A_2}(t)$ et nous sommes ramenés à l'étude des polynômes caractéristiques des variétés abéliennes de dimension au plus $(g-1)$. Nous supposerons donc par la suite que A est simple.

Le Théorème de Honda-Tate nous assure que l'ensemble des classes de conjugaison de q-nombres de Weil est en bijection avec celui des classes d'isogénie de variétés abéliennes simples sur $\mathbb{F}_q$. Plus précisément, le polynôme caractéristique d'une variété abélienne simple $A/\mathbb{F}_q$ est de la forme $h(t)^e$ où $h(t)$ est le polynôme minimal du q-nombre de Weil associé à A.

Si $p_A(t)$ a une racine réelle, nous avons vu que celui-ci est alors égal à

$$(t \pm \sqrt{q})^2 \quad \text{ou} \quad (t^2 - q)^2$$

selon si n est pair ou impair (en particulier, $p_A(t)$ n'a jamais de racine réelle si $g \geq 3$).

Si $p_A(t)$ est sans racine réelle, alors $h(t)$ est un polynôme de Weil irréductible sur $\mathbb{Q}$. De plus, l'entier e est entièrement déterminé par $h(t)$: si $h(t) = \prod_i h_i(t)$ est la décomposition de $h(t)$ en facteurs irréductibles sur $\mathbb{Q}_p$ alors e est le plus petit dénominateur commun des rationnels $v_p(h_i(0))/n$ (voir Proposition 0.3.10).

Pour vérifier si un polynôme de Weil donné est irréductible, nous avons le critère suivant :

Proposition 1.1.2. *Soit $p(t) = \prod_{i=1}^{g}(t^2 + x_i t + q)$ un polynôme de Weil. On pose $f(t) = \prod_{i=1}^{g}(t + x_i)$. On suppose que $g \geq 2$ et $p(t) \neq (t - \sqrt{q})^2(t + \sqrt{q})^2$. Alors $p(t)$ est irréductible sur $\mathbb{Q}$ si et seulement si $f(t)$ l'est.*

Démonstration. Supposons que $p(t)$ est réductible. Il suffit de montrer que $p(t)$ se factorise alors comme produit de deux polynômes de Weil (ainsi, $f(t)$ sera le produit de leurs polynômes associés). On peut écrire $p(t)$ sous la forme $p(t) = (t-\sqrt{q})^{2k}(t+\sqrt{q})^{2\ell}h(t)$ où $h(t)$ est sans racine réelle. Si $k \neq \ell$, alors $\sqrt{q} \in \mathbb{Q}$ et la factorisation est évidente. Elle l'est aussi lorsque $k = \ell \neq 0$ et $h(t) \neq 1$. Si $k = \ell > 1$ et $h(t) = 1$, on a la factorisation $p(t) = [(t - \sqrt{q})^2(t + \sqrt{q})^2][(t - \sqrt{q})^{2k-2}(t + \sqrt{q})^{2\ell-2}]$. Enfin, si $k = \ell = 0$, $h(t)$ est par hypothèse le produit de deux polynômes non constants et ceux-ci sont des polynômes de Weil pour peu qu'ils soient choisis unitaires.

Réciproquement, si $f(t)$ est réductible, quitte à renuméroter les x_i, on peut supposer qu'il existe k compris entre 1 et $(g-1)$ tel que les polynômes $\prod_{i=1}^{k}(t + x_i)$ et $\prod_{i=k+1}^{g}(t + x_i)$ soient à coefficients entiers. Par suite, les polynômes $\prod_{i=1}^{k}(t^2 + x_i t + q)$ et $\prod_{i=k+1}^{g}(t^2 + x_i t + q)$ le sont aussi et leur produit est $p(t)$. □

1.1.3 Polygones de Newton

On se donne un polynôme $g(t) = \sum_{k=0}^{d} b_k t^k$ à coefficients dans $\mathbb{Q}_p$ avec $b_0 b_d \neq 0$. On définit le *polygone de Newton* de $g(t)$ comme étant l'enveloppe inférieure convexe des points $(k, v_p(b_k))$ pour $k = 0, \ldots, d$ (si $b_k = 0$, le point $(k, v_p(b_k))$ est "à l'infini" et peut donc être omis). On trouvera une démonstration du théorème suivant dans le Chapitre III.1 de [39]. La Figure 1.1 illustre notre situation (on notera que plus les abscisses sont grands, plus les pentes augmentent).

Théorème 1.1.3. *Si le segment $[(r, v_p(b_r)); (s, v_p(b_s))]$ est un côté du polygone Newton de $g(t)$ de pente $-\lambda$ alors $g(t)$ a exactement $|r - s|$ racines $\alpha_1, \ldots, \alpha_{|r-s|}$ de valuation λ. De plus, le polynôme*

$$f_\lambda(t) = \prod_{i=1}^{|r-s|}(t - \alpha_i)$$

est dans $\mathbb{Q}_p[t]$.

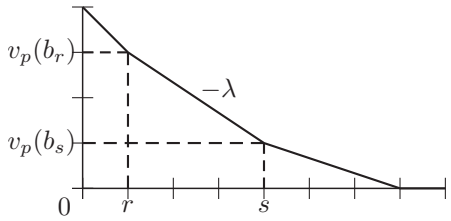

FIGURE 1.1 –

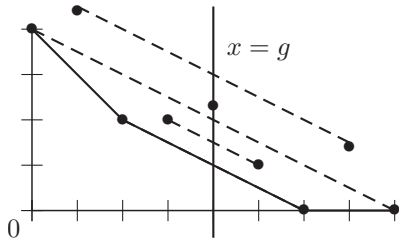

FIGURE 1.2 –

Revenons-en à nos polynômes de Weil. Pour simplifier les notations, on pose $a_0 = 1$. Le polygone de Newton de $p(t)$ est l'enveloppe inférieure convexe des points

$$(k, v_p(a_k) + n(g-k)),\ (2g-k, v_p(a_k)),\ k = 0, \ldots, g.$$

Comme $(2g-k, v_p(a_k))$ est l'image de $(k, v_p(a_k) + n(g-k))$ par la symétrie oblique

$$(x, y) \mapsto (2g - x, y + n(x-g))$$

d'axe $x = g$ et de direction $y = -nx/2$, le point $(k, v_p(a_k)+n(g-k))$ est extrémal si et seulement si $(2g-k, v_p(a_k))$ l'est (voir Figure 1.2).

De plus, tous les côtés sont de pente négative (les ordonnées de nos points sont toutes positives et le dernier point est $(0, 2g)$).

Aussi, les côtés qui ont pour extrémité l'un des $(2g-k, v_p(a_k))$ ont une pente supérieure ou égale à $-n/2$ puisque les segments $[(k, v_p(a_k)+n(g-k)); (2g-k, v_p(a_k))]$ se situent au dessus du polygone de Newton et sont de pente $-n/2$. De plus, un côté est de pente $-n/2$ si et seulement si il traverse l'axe de symétrie.

Soit $p(t) = \prod_\lambda f_\lambda(t)$ la décomposition de $p(t)$ associée à son polygone de Newton. On note d_λ le degré de $f_\lambda(t)$; c'est aussi la longueur du projeté sur l'axe des abscisses du côté de pente $-\lambda$ (le $|r-s|$ du Théorème 1.1.3). En particulier, si $\lambda \neq n/2$ on a toujours $d_\lambda \leq g$ (un côté avec $d_\lambda > g$ traverse obligatoirement l'axe de symétrie $x = g$).

On suppose que $p(t)$ est un polynôme de Weil de degré $2g$ irréductible sur $\mathbb{Q}$ et on note $p(t) = \prod_i p_i(t)$ sa décomposition en facteurs irréductibles sur $\mathbb{Q}_p$. Nous avons vu dans la section précédente que la dimension d'une variété abélienne simple associée à $p(t)$ est ge où e est le plus petit dénominateur commun des rationnels $v_p(p_i(0))/n$.

Si $\widetilde{e}$ le plus petit dénominateur commun des rationnels $v_p(f_\lambda(0))/n$ alors e est un dénominateur commun des $v_p(f_\lambda(0))/n$ donc un multiple de $\widetilde{e}$. L'intérêt de $\widetilde{e}$ est qu'il se déduit facilement

du polygone de Newton de $p(t)$. En effet, comme $f_\lambda(0)$ est le produit des racines de $f_\lambda(t)$ (qui sont toutes de valuation λ), on a $v_p(f_\lambda(0)) = \lambda d_\lambda$.

Dans la suite, nous allons chercher à décrire l'ensemble des polynômes de Weil irréductibles de degré donné (inférieur ou égal à 8) qui sont polynômes caractéristiques d'une certaine variété abélienne ; en d'autres termes, ceux avec $e = 1$. Les entiers $\widetilde{e}$ associés à ces polynômes sont nécessairement égaux à 1 puisqu'ils divisent $e = 1$. Une manière d'attaquer notre problème est donc de lister les polygones de Newton avec $\widetilde{e} = 1$, c'est-à-dire ceux tels que tous les $\lambda d_\lambda / n$ soient des entiers.

Soit P un tel polygone de Newton. Pour chacune de ses pentes $-\lambda$, on pose $\lambda/n = k_\lambda/\ell_\lambda$, avec $(k_\lambda, \ell_\lambda) = 1$. Comme $\lambda d_\lambda / n$ est un entier, l'entier ℓ_λ divise d_λ ; en particulier, si $\lambda \neq n/2$, on a $\ell_\lambda \leq g$. Nous avons vu que, si le côté considéré a pour extrémité l'un des $(2g - k, v_p(a_k))$, $k = 0, \ldots, g$ (les autres côtés se déduisent par symétrie), on a $0 \leq \lambda \leq n/2$.

Les pentes possibles pour les côtés de P dont une extrémité a une abscisse strictement supérieure à g sont donc $-n/2$ ou $-nk/\ell$ avec $(k, \ell) = 1$ et

$$1 \leq \ell \leq g \quad \text{et} \quad 0 \leq k \leq \frac{\ell}{2}.$$

1.2 Dimensions 1 et 2

1.2.1 Courbes elliptiques

Le cas le plus connu est celui des courbes elliptiques, c'est-à-dire $g = 1$. Les polynômes de Weil de degré 2 sont de la forme

$$p(t) = t^2 + a_1 t + q$$

et on a clairement $|a_1| \leq 2\sqrt{q}$.

Si $p(t)$ est le polynôme caractéristique d'une courbe elliptique, les pentes des côtés de son polygone de Newton ne peuvent être égales qu'à 0, $n/2$ ou n. Cela ne nous laisse que deux possibilités : le polygone de Newton avec deux côtés de pente n et 0 et celui avec un seul côté de pente $n/2$.

Le premier polygone de Newton est celui de $p(t)$ si et seulement si $v_p(a_1) = 0$ et si c'est le cas, on a clairement $e = 1$; les courbes elliptiques correspondantes sont ordinaires. Le deuxième polygone de Newton est celui de $p(t)$ si et seulement si $v_p(a_1) \geq n/2$ et si c'est le cas, $e = 1$ ou 2 selon si $p(t)$ est irréductible ou non sur $\mathbb{Q}_p$; si $e = 1$, les courbes elliptiques correspondantes sont supersingulières.

La condition $v_p(a_1) \geq n/2$ est très restrictive sachant que l'on a $|a_1| \leq 2\sqrt{q}$. Il est donc possible de vérifier "à la main" si les quelques a_1 satisfaisant ceci donnent des polynômes irréductibles sur $\mathbb{Q}_p$. Nous obtenons finalement le théorème suivant :

Théorème 1.2.1 (Deuring, Waterhouse)**.** *Le polynôme de Weil $p(t) = t^2 + a_1 t + q$, $|a_1| \leq 2\sqrt{q}$ est le polynôme caractéristique d'une courbe elliptique si et seulement si a_1 est premier avec q ou fait partie de la liste suivante :*

1. $\pm 2\sqrt{q}$, *n pair,*
2. $\pm\sqrt{q}$, *n pair, $p \not\equiv 1 \mod 3$,*
3. $\pm\sqrt{pq}$, *n impair, $p = 2$ ou 3,*
4. 0, *n impair ou n pair et $p \not\equiv 1 \mod 4$.*

Par des manipulations simples des polygones de Newton, il est aussi possible de montrer la proposition suivante dont nous aurons besoin dans la suite :

Proposition 1.2.2 (Maisner, Nart). *Soit $p(t) = t^2 + a_1 t + q$ un polynôme de Weil irréductible.*

1. *Si $v_p(a_1) \geq n/2$ alors e est égal à*
   - *1 si $(a_1^2 - 4q)$ n'est pas un carré dans $\mathbb{Q}_p$,*
   - *2 sinon.*
2. *Si $v_p(a_1) < n/2$ alors e est égal à $n/(n, v_p(a_1))$.*

1.2.2 Surfaces abéliennes

Les polynômes de Weil de degré 4 sont de la forme

$$p(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$$

avec $a_1, a_2 \in \mathbb{Z}$. En reprenant les notations de la Section 1.1.1, on a $f^{\pm}(t) = t^2 - (4\sqrt{q} \pm a_1)t + (2q \pm 2a_1\sqrt{q} + a_2)$ et $f^0(t) = t^2 + (-2q - \frac{a_1^2}{4} + a_2)$ et on déduit du Lemme 1.1.1 que $p(t)$ est un polynôme de Weil si et seulement si

$$|a_1| \leq 4\sqrt{q} \quad \text{et} \quad 2|a_1|\sqrt{q} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q.$$

Ces inégalités sont dues à Rück.

On suppose maintenant que $p(t)$ est le polynôme caractéristique d'une surface abélienne simple. Pour le cas où $p(t)$ est réductible, nous avons la proposition suivante :

Proposition 1.2.3 (Maisner, Nart, Xing). *Le polynôme $p(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$ est le polynôme caractéristique réductible d'une surface abélienne simple si et seulement si le couple (a_1, a_2) fait partie de la liste suivante :*

1. *$(0, -2q)$, n impair,*
2. *$(0, 2q)$, n pair, $p \equiv 1 \mod 4$,*
3. *$(\pm 2\sqrt{q}, 3q)$, n pair, $p \equiv 1 \mod 3$.*

En effet, si $p(t)$ a une racine réelle, n est impair et on a $p(t) = (t^2 - q)^2$; on obtient le premier couple de la liste. Si $p(t)$ n'a pas de racine réelle, par les résultats de la Section 1.1.1, on a $p(t) = h(t)^2$ où $h(t)$ est un polynôme de Weil irréductible, on applique la Proposition 1.2.2 et on a le reste de la liste. Les variétés abéliennes correspondantes sont toutes supersingulières.

Par la Proposition 1.1.2, le polynôme $p(t)$ est irréductible si et seulement si $f(t) = t^2 + a_1 t + a_2 - 2q$ l'est, ce qui revient à dire que $a_1^2 - 4a_2 + 8q$ n'est pas un carré dans $\mathbb{Z}$. On suppose dans la suite que cette condition est vérifiée.

On a trois possibilités pour le polygone de Newton de $p(t)$: celui avec deux côtés de pente n et 0, celui avec trois côtés de pente n, $n/2$ et 0 et celui avec un seul côté de pente $n/2$.

Le premier polygone de Newton est celui de $p(t)$ si et seulement si $v_p(a_2) = 0$ et si c'est le cas, on a $e = 1$; les surfaces abéliennes correspondantes sont ordinaires. Le deuxième polygone de Newton est celui de $p(t)$ si et seulement si $v_p(a_2) \geq n/2$ et $v_p(a_1) = 0$, si c'est le cas $e = 1$ ou 2 selon si $p(t)$ a un facteur irréductible de degré 2 ou non, mais d'autre part on vérifie facilement que la factorisation $p(t) = (t^2 + x_1 t + q)(t^2 + x_2 t + q)$ où x_1, x_2 sont les racines de $f(t)$ dans $\overline{\mathbb{Q}_p}$ est $p(t) = [f_0(t) f_n(t)] f_{n/2}(t)$ donc $e = 1$ si et seulement si le produit de

discriminants $(x_1^2 - 4q)(x_2^2 - 4q) = (a_2 + 2q)^2 - 4qa_1^2$ n'est pas un carré dans $\mathbb{Q}_p$; les surfaces abéliennes correspondantes sont de p-rang 1. Le troisième polygone de Newton est celui de $p(t)$ si et seulement si $v_p(a_2) \geq n$ et $v_p(a_1) \geq n/2$, si c'est le cas, $e = 1$ ou 2 selon si $p(t)$ est sans racine ou non dans $\mathbb{Q}_p$; les surfaces abéliennes correspondantes sont supersingulières. On obtient donc le théorème suivant :

Théorème 1.2.4 (Rück)**.** *Le polynôme de Weil $p(t)$ est le polynôme caractéristique irréductible d'une surface abélienne si et seulement si l'une des conditions suivantes est vérifiée :*

1. $v_p(a_2) = 0$,
2. $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$ *et* $((a_2 + 2q)^2 - 4qa_1^2)$ *n'est pas un carré dans* $\mathbb{Q}_p$,
3. $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$ *et* $p(t)$ *n'a pas de racine dans* $\mathbb{Q}_p$.

En utilisant les mêmes idées que pour les courbes elliptiques, il est possible de rendre plus explicite le cas supersingulier du Théorème 1.2.4. On obtient la proposition suivante :

Proposition 1.2.5 (Maisner, Nart, Xing)**.** *Le polynôme $p(t)$ est le polynôme caractéristique irréductible d'une surface abélienne supersingulière si et seulement si l'une des conditions suivantes est vérifiée :*

- *n est pair et le couple (a_1, a_2) fait partie de la liste suivante :*
  1. $(0, 0)$, $p \not\equiv 1 \mod 8$,
  2. $(0, -q)$, $p \not\equiv 1 \mod 12$,
  3. $(\pm\sqrt{q}, q)$, $p \not\equiv 1 \mod 5$,
- *n est impair et le couple (a_1, a_2) fait partie de la liste suivante :*
  1. $(0, 0)$, $p \neq 2$,
  2. $(0, q)$,
  3. $(0, -q)$, $p \neq 3$,
  4. $(\pm\sqrt{pq}, 3q)$, $p = 5$,
  5. $(\pm\sqrt{pq}, q)$, $p = 2$.

La proposition suivante est l'analogue de la Proposition 1.2.2 pour $g = 2$:

Proposition 1.2.6. *Soit $p(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$ un polynôme de Weil irréductible.*

1. *Si $v_p(a_1) < v_p(a_2)/2$ et $v_p(a_2) < v_p(a_1) + n/2$ alors e est égal à $n/(n, v_p(a_1), v_p(a_2))$.*
2. *Si $v_p(a_1) < n/2$ et $v_p(a_2) \geq v_p(a_1) + n/2$ alors e est égal à*
   - *$n/(n, v_p(a_1))$ si $((a_2 + 2q)^2 - 4qa_1^2)$ n'est pas un carré dans $\mathbb{Q}_p$,*
   - *$2n/(n, 2v_p(a_1))$ sinon.*
3. *Si $v_p(a_1) \geq v_p(a_2)/2$ et $v_p(a_2) < n$ alors e est égal à*
   - *$n/(n, v_p(a_2))$ si $(a_1^2 - 4a_2 + 8q)$ n'est pas un carré dans $\mathbb{Q}_p$,*
   - *$2n/(2n, v_p(a_2))$ sinon.*
4. *Si $v_p(a_1) \geq n/2$ et $v_p(a_2) \geq n$ alors e est égal à*
   - *1 si (a_1, a_2) est dans la liste de la Proposition 1.2.5,*
   - *2 sinon.*

Démonstration. Le polygone de Newton de $p(t)$ est l'enveloppe inférieure convexe des points $(0, 2n)$, $(1, v_p(a_1) + n)$, $(2, v_p(a_2))$, $(3, v_p(a_1))$ et $(4, 0)$. Par symétrie, le point $(1, v_p(a_1) + n)$ est un sommet si et seulement si $(3, v_p(a_1))$ l'est (voir Section 1.1.3). Les polygones de Newton possibles pour $p(t)$ sont donc représentés par les Figures 1.3, 1.4, 1.5 et 1.6.

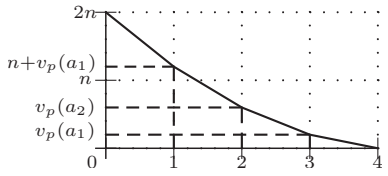

FIGURE 1.3 –

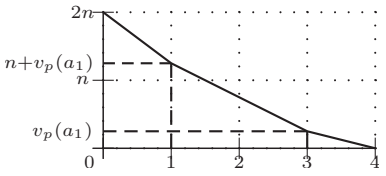

FIGURE 1.4 –

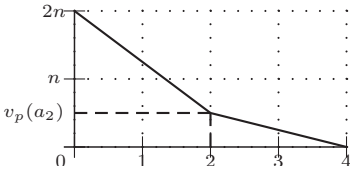

FIGURE 1.5 –

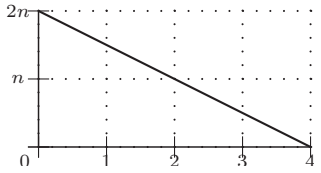

FIGURE 1.6 –

Les points faisant partie de la liste ci-dessus et qui ne sont pas des sommets se situent au-dessus du polygone de Newton ; on déduit de cette observation des conditions nécessaires et suffisantes sur les valuations de a_1 et a_2 pour qu'un polygone de Newton donné soit celui de $p(t)$.

Figure 1.3 : $\mathbf{v_p(a_1) < v_p(a_2)/2}$ et $\mathbf{v_p(a_2) < v_p(a_1) + n/2}$. Nous avons une factorisation $p(t) = f_{n-v_p(a_1)}(t) f_{n+v_p(a_1)-v_p(a_2)}(t) f_{v_p(a_2)-v_p(a_1)}(t) f_{v_p(a_1)}(t)$. Donc e est le plus petit dénominateur commun de $(v_p(a_2) - v_p(a_1))/n$ et $v_p(a_1)/n$ qui est $n/(v_p(a_2) - v_p(a_1), v_p(a_1), n) = n/(v_p(a_1), v_p(a_2), n)$.

Figure 1.4 : $\mathbf{v_p(a_1) < n/2}$ et $\mathbf{v_p(a_2) \geq v_p(a_1) + n/2}$. Nous avons une factorisation $p(t) = f_{n-v_p(a_1)}(t) f_{n/2}(t) f_{v_p(a_1)}(t)$. Pour les mêmes raisons que dans le cas (2) du Théorème 1.2.4, le polynôme $f_{n/2}(t)$ est irréductible sur $\mathbb{Q}_p$ si et seulement si $((a_2 + 2q)^2 - 4qa_1^2)$ n'est pas un carré dans $\mathbb{Q}_p$. Si cette condition est satisfaite, on a $e = n/(n, v_p(a_1))$. Sinon e est le plus petit dénominateur commun de $2v_p(a_1)/2n$ et $n/2n$ qui est $2n/(2n, 2v_p(a_1), n) = 2n/(n, 2v_p(a_1))$.

Figure 1.5 : $\mathbf{v_p(a_1) \geq v_p(a_2)/2}$ et $\mathbf{v_p(a_2) < n}$. Nous avons une factorisation $p(t) = f_{n-v_p(a_2)/2}(t)$ $f_{v_p(a_2)/2}(t)$. D'autre part, si x_1, x_2 sont les racines de $f(t) = t^2 + a_1 t + a_2 - 2q$ dans $\overline{\mathbb{Q}_p}$, nous avons aussi la factorisation $p(t) = (t^2 + x_1 t + q)(t^2 + x_2 t + q)$ qui est différente de la dernière (regarder les valuations des coefficients constants). On en déduit que $f_{n-v_p(a_2)/2}(t)$ est irréductible si et seulement si $f_{v_p(a_2)/2}(t)$ l'est si et seulement si $(a_1^2 - 4a_2 + 8q)$ n'est pas un carré dans $\mathbb{Q}_p$. Si cette dernière condition est satisfaite, on a $e = n/(n, v_p(a_2))$. Sinon $e = 2n/(2n, v_p(a_2))$.

Figure 1.6 : $\mathbf{v_p(a_1) \geq n/2}$ et $\mathbf{v_p(a_2) \geq n}$. On est dans le cas (3) du Théorème 1.2.4.

□

1.3 Dimension 3

1.3.1 Les coefficients

Les polynômes de Weil de degré 6 sont de la forme

$$p(t) = t^6 + a_1 t^5 + a_2 t^4 + a_3 t^3 + q a_2 t^2 + q^2 a_1 t + q^3$$

avec $a_1, a_2, a_3 \in \mathbb{Z}$. Nous allons montrer le théorème suivant :

Théorème 1.3.1. *Le polynôme $p(t)$ est un polynôme de Weil si et seulement si les inégalités ci-dessous sont satisfaites*

1. $|a_1| \leq 6\sqrt{q}$,
2. $4\sqrt{q}|a_1| - 9q \leq a_2 \leq \frac{a_1^2}{3} + 3q$,
3. $-\frac{2a_1^3}{27} + \frac{a_1 a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leq a_3 \leq -\frac{2a_1^3}{27} + \frac{a_1 a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}$,
4. $-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} \leq a_3 \leq -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}$.

La preuve de ce théorème est basée sur le Lemme 1.1.1. Pour $k = 1, 2, 3$, on note s_k les fonctions symétriques des $x_i = -(\alpha_i + q/\alpha_i)$, où $\alpha_1, q/\alpha_1, \ldots, \alpha_3, q/\alpha_3$ sont les racines de $p(t)$. En développant l'expression $p(t) = \prod_{i=1}^{3}(t^2 + x_i t + q)$, on trouve :

$$\begin{aligned} s_1 &= a_1, \\ s_2 &= a_2 - 3q, \\ s_3 &= a_3 - 2qa_1. \end{aligned}$$

On a $f^0(t) = \prod_{i=1}^{3}(t + x_i - \frac{a_1}{3}) = t^3 + r_2 t + r_3$ où :

$$\begin{aligned} r_2 &= -\frac{s_1^2}{3} + s_2, \\ r_3 &= \frac{2s_1^3}{27} - \frac{s_1 s_2}{3} + s_3. \end{aligned}$$

En remplaçant s_1, s_2, s_3 par leur expression en a_1, a_2, a_3 on obtient :

$$\begin{aligned} r_2 &= -\frac{a_1^2}{3} + a_2 - 3q, \\ r_3 &= \frac{2a_1^3}{27} - qa_1 - \frac{a_1 a_2}{3} + a_3. \end{aligned}$$

Le polynôme $f^0(t)$ n'a que des racines réelles si et seulement si son discriminant Δ_{f^0} est positif (voir Section 1.1.1). On a :

$$\Delta_{f^0} = -4r_2^3 - 27r_3^2.$$

On en déduit que $\Delta_{f^0} \geq 0$ équivaut à :

$$r_2 \leq 0 \quad \text{et} \quad -\frac{2}{27}(-3r_2)^{3/2} \leq r_3 \leq \frac{2}{27}(-3r_2)^{3/2}.$$

Ceci nous donne la deuxième inégalité de la condition (2) et la condition (3) du Théorème 1.3.1.

Pour $k = 1, 2, 3$, on note r_k^+ et r_k^- les coefficients respectifs de $f^+(t) = \prod_{i=1}^{3}(t - (2\sqrt{q} + x_i))$ et $f^-(t) = \prod_{i=1}^{3}(t - (2\sqrt{q} - x_i))$. On a :

$$\begin{array}{lcl} r_1^+ = -6\sqrt{q} - s_1, & & r_1^- = -6\sqrt{q} + s_1, \\ r_2^+ = 12q + 4\sqrt{q}s_1 + s_2, & \text{et} & r_2^- = 12q - 4\sqrt{q}s_1 + s_2, \\ r_3^+ = -8q\sqrt{q} - 4qs_1 - 2\sqrt{q}s_2 - s_3 & & r_3^- = -8q\sqrt{q} + 4qs_1 - 2\sqrt{q}s_2 + s_3. \end{array}$$

En remplaçant s_1, s_2, s_3 par leur expression en a_1, a_2, a_3 on obtient :

$$\begin{array}{lcl} r_1^+ = -6\sqrt{q} - a_1, & & r_1^- = -6\sqrt{q} + a_1, \\ r_2^+ = 9q + 4\sqrt{q}a_1 + a_2, & \text{et} & r_3^- = 9q - 4\sqrt{q}a_1 + a_2, \\ r_3^+ = -2q\sqrt{q} - 2qa_1 - 2\sqrt{q}a_2 - a_3 & & r_3^- = -2q\sqrt{q} + 2qa_1 - 2\sqrt{q}a_2 + a_3. \end{array}$$

Si les racines de $f^+(t)$ et $f^-(t)$ sont toutes réelles (ce qui revient à dire que celles de $f^0(t)$ le sont), elles sont toutes positives si et seulement si $(-1)^k r_k^+ \geq 0$ et $(-1)^k r_k^- \geq 0$ pour $k = 1, 2, 3$. Ceci nous donne les conditions manquantes du Théorème 1.3.1 et conclut la preuve.

1.3.2 Polynômes caractéristiques réductibles

Soit $p(t)$ le polynôme caractéristique d'une variété abélienne simple de dimension 3. Dans la Section 1.1.2 nous avons vu que $p(t) = h(t)^e$ où $h(t)$ est un polynôme de Weil irréductible. Il est clair que l'entier e doit diviser 6. Il ne peut pas être égal à 2 ou 6 car sinon $p(t)$ aurait alors une racine réelle et les q-nombres de Weil réels correspondent à des variétés abéliennes de dimension 1 ou 2. On en conclut que $e = 1$ ou 3. On étudiera le cas $e = 1$ dans la Section 1.3.3. Lorsque $e = 3$, l'ensemble des $h(t)$ possibles se déduit directement de la Proposition 1.2.2 :

Proposition 1.3.2 (Xing)**.** *Le polynôme $p(t)$ est le polynôme caractéristique réductible d'une variété abélienne simple de dimension* 3 *si et seulement si n est divisible par* 3 *et*

$$p(t) = (t^2 + b_1 t + q)^3$$

avec $|b_1| < 2\sqrt{q}$ et $b_1 = kq^{1/3}$ où k est un entier premier avec p.

En particulier toute variété abélienne simple de dimension 3 ayant un polynôme caractéristique réductible est de p-rang 0 (et non supersingulière). Le polygone de Newton des polynômes provenant de la Proposition 1.3.2 est celui représenté par la Figure 1.10 de la Section 1.3.3 (type 1/3).

En combinant la Proposition 1.1.2 avec la méthode de Cardan, il est possible de donner un critère d'irréductibilité pour les polynômes de Weil de degré 6 explicite et pas trop difficile à utiliser. Commençons par rappeler ce qu'est la méthode de Cardan ; nous en aurons aussi besoin dans la Section 1.4.1.

Lemme 1.3.3 (Méthode de Cardan)**.** *Etant donné un polynôme de la forme $\ell(t) = t^3 + u_2 t + u_3$, on pose $\delta = -u_3^2 - \frac{4}{27}u_2^3$. Alors $\ell(t)$ a toutes ses racines réelles si et seulement si $\delta \geq 0$. Si c'est le cas, les racines de $\ell(t)$ sont $\gamma_1 = \omega + \overline{\omega}$, $\gamma_2 = j\omega + j^2\overline{\omega}$ et $\gamma_3 = j^2\omega + j\overline{\omega}$ où $j = e^{\frac{2i\pi}{3}}$ et $\omega = (\frac{-u_3 + i\sqrt{\delta}}{2})^{1/3}$.*

Proposition 1.3.4. *Soient*

$$r_2 = -\frac{a_1^2}{3} + a_2 - 3q \quad \text{et} \quad r_3 = \frac{2a_1^3}{27} - qa_1 - \frac{a_1 a_2}{3} + a_3.$$

On définit

$$\delta = -r_3^2 - \frac{4}{27}r_2^3 \quad \text{et} \quad u = \frac{-r_3 + i\sqrt{\delta}}{2}.$$

Alors $p(t)$ est irréductible sur $\mathbb{Q}$ si et seulement si $\delta \neq 0$ et u n'est pas un cube dans $\mathbb{Q}(i\sqrt{\delta})$.

Démonstration. Par la Proposition 1.1.2, $p(t)$ est irréductible si et seulement si $f^0(t) = \prod_{i=1}^3 (t + x_i - \frac{a_1}{3}) = t^3 + r_2 t + r_3$ l'est. De plus, $f^0(t)$ est réductible si et seulement si il a une racine dans $\mathbb{Q}$.

Le polynôme $f^0(t)$ n'a que des racines réelles donc $\delta \geq 0$. Si $\delta = 0$, $f^0(t)$ est réductible puisqu'il a une racine multiple. Supposons maintenant $\delta > 0$. Si u est le cube d'un certain $v \in \mathbb{Q}(i\sqrt{\delta})$, alors $(v + \overline{v})$ est dans $\mathbb{Q}$ et est une racine de $f^0(t)$ (par la méthode de Cardan). Réciproquement, si $f^0(t)$ a une racine dans $\mathbb{Q}$ alors u a une racine cubique $v = a + ib$ avec $a \in \mathbb{Q}$ (car $2a = v + \overline{v} \in \mathbb{Q}$) et on a

$$u = v^3 = (a^3 - 3ab^2) + ib(3a^2 - b^2).$$

Si $a \neq 0$, en identifiant les parties réelles dans l'identité ci-dessus, on voit que $b^2 \in \mathbb{Q}$, puis, en identifiant les parties imaginaires, $b \in \mathbb{Q}(\sqrt{\delta})$. Donc $v \in \mathbb{Q}(i\sqrt{\delta})$. Si $a = 0$, on a $r_3 = 0$ et $\delta = \frac{4}{27}r_2^3 = (\frac{2}{3}r_2)^2\frac{r_2}{3}$. Donc $u = \frac{1}{2}\sqrt{\frac{4}{27}r_2^3} = (\sqrt{\frac{r_2}{3}})^3$ est un cube dans $\mathbb{Q}(i\sqrt{\delta}) = \mathbb{Q}(\sqrt{\frac{r_2}{3}})$.

□

1.3.3 Polynômes caractéristiques irréductibles

Dans cette section nous allons prouver le théorème suivant :

Théorème 1.3.5. *Le polynôme de Weil $p(t)$ est le polynôme caractéristique irréductible d'une variété abélienne de dimension 3 si et seulement si l'une des conditions suivantes est vérifiée :*

1. $v_p(a_3) = 0$,
2. $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$ *et* $p(t)$ *n'a pas de racine de valuation* $n/2$ *dans* $\mathbb{Q}_p$,
3. $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$ *et* $p(t)$ *n'a pas de racine de valuation* $n/2$ *dans* $\mathbb{Q}_p$,
4. $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$ *et* $p(t)$ *n'a pas de racine dans* $\mathbb{Q}_p$,
5. $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) \geq 3n/2$ *et* $p(t)$ *n'a dans* $\mathbb{Q}_p$ *ni de racine ni de facteur de degré* 3.

De plus, les cas (1), (2), (3), (4) et (5) correspondent respectivement à des variétés abéliennes de p-rang 3, 2, 1, 0 *et* 0. *Les variétés abéliennes du cas (5) sont supersingulières.*

Les polygones de Newton possibles pour $p(t)$ sont représentés par les Figures 1.7, 1.8, 1.9, 1.10 et 1.11 (voir Section 1.1.3).

Figure 1.7 : $\mathbf{v_p(a_3) = 0}$. On a toujours $e = 1$.

Figure 1.8 : $\mathbf{v_p(a_3) \geq n/2}$ et $\mathbf{v_p(a_2) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ un facteur de degré 2 dont les racines sont de valuation $n/2$ et $e = 1$ si et seulement si celui-ci est irréductible, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine de valuation $n/2$ dans $\mathbb{Q}_p$ (on notera que cette dernière condition est toujours vérifiée lorsque n est impair).

Figure 1.9 : $\mathbf{v_p(a_3) \geq n}$, $\mathbf{v_p(a_2) \geq n/2}$ et $\mathbf{v_p(a_1) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ un facteur de degré 4 dont les racines sont de valuation $n/2$ et $e = 1$ si et seulement si celui-ci n'a pas de racine, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine de valuation $n/2$ dans $\mathbb{Q}_p$.

Figure 1.10 : $\mathbf{v_p(a_3) = n}$, $\mathbf{v_p(a_2) \geq 2n/3}$ et $\mathbf{v_p(a_1) \geq n/3}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ deux facteurs de degré 3, l'un dont les racines sont de valuation $2n/3$ et l'autre dont les racines sont de valuation $n/3$; $e = 1$ si et seulement si ceux-ci sont irréductibles, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine dans $\mathbb{Q}_p$.

Figure 1.11 : $\mathbf{v_p(a_3) \geq 3n/2}$, $\mathbf{v_p(a_2) \geq n}$ et $\mathbf{v_p(a_1) \geq n/2}$. On a $e = 1$ si et seulement si $p(t)$ n'a dans $\mathbb{Q}_p$ ni de racine ni de facteur de degré 3.

1.3.4 Polynômes caractéristiques supersinguliers

La condition (5) du Théorème 1.3.5 peut être rendue plus explicite :

Proposition 1.3.6. *Le polynôme $p(t)$ est le polynôme caractéristique d'une variété abélienne supersingulière simple de dimension 3 si et seulement si l'une des conditions suivantes est vérifiée :*

- *n est pair et le triplet (a_1, a_2, a_3) fait partie de la liste suivante :*
  1. $(\varepsilon\sqrt{q}, q, \varepsilon q\sqrt{q})$, $\varepsilon \in \{-1, 1\}$, $p^3 \not\equiv 1 \mod 7$,
  2. $(0, 0, \varepsilon q\sqrt{q})$, $\varepsilon \in \{-1, 1\}$, $p \not\equiv 1 \mod 3$,
- *n est impair et le triplet (a_1, a_2, a_3) fait partie de la liste suivante :*
  1. $(\varepsilon\sqrt{pq}, 3q, \varepsilon q\sqrt{pq})$, $\varepsilon \in \{-1, 1\}$, $p = 7$,
  2. $(0, 0, \varepsilon q\sqrt{pq})$, $\varepsilon \in \{-1, 1\}$, $p = 3$.

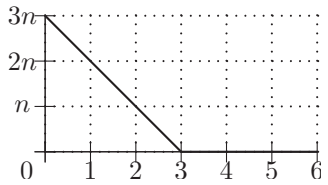

FIGURE 1.7 – Ordinaire

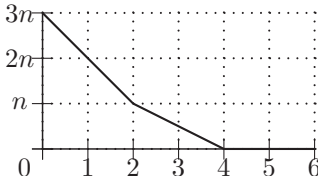

FIGURE 1.8 – p-rang 2

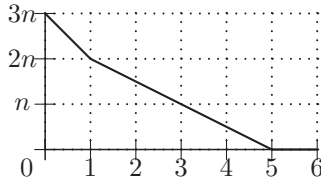

FIGURE 1.9 – p-rang 1

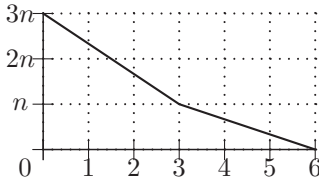

FIGURE 1.10 – Type 1/3

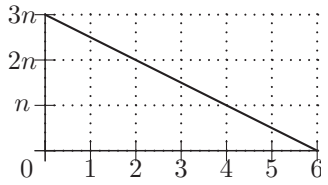

FIGURE 1.11 – Supersingulier

En effet, dans [22], Nart et Ritzenthaler ont montré que les seuls q-nombres de Weil supersinguliers de degré 6 sont :

$$\begin{array}{ll} \pm\sqrt{q}\zeta_7, \quad \pm\sqrt{q}\zeta_9, & \text{si } q \text{ est un carré,} \\ \sqrt{q}\zeta_{28}\ (p=7), \quad \sqrt{q}\zeta_{36}\ (p=3), & \text{si } q \text{ n'est pas un carré,} \end{array}$$

où ζ_m désigne une racine primitive m-ième de l'unité.

On note $\Phi_m(t)$ le m-ième polynôme cyclotomique. Pour calculer la dimension des variétés abéliennes associées à nos polynômes, nous utiliserons les résultats du Chapitre IV.4 de [27] : le degré de ζ_m sur $\mathbb{Q}_p$ est égal à l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^*$ si $(m,p)=1$ et à $(p-1)p^{k-1}$ si $m=p^k$ (et donc $\Phi_m(t)$ est irréductible sur $\mathbb{Q}_p$).

• Supposons que q est un carré. Les polynômes minimaux de $\pm\sqrt{q}\zeta_7$ et $\pm\sqrt{q}\zeta_9$ sont $p(t) = q^3\Phi_7(\pm\frac{t}{\sqrt{q}})$ et $p(t) = q^3\Phi_9(\pm\frac{t}{\sqrt{q}})$ où

$$\begin{aligned} \Phi_7(t) &= t^6+t^5+t^4+t^3+t^2+t+1, \\ \Phi_9(t) &= t^6+t^3+1. \end{aligned}$$

Dans le premier cas, $p(t)$ est sans facteur de degré 1 et 3 sur $\mathbb{Q}_p$ si et seulement si les racines primitives 7-ièmes de l'unité ne sont pas de degré divisant 3 sur $\mathbb{Q}_p$, si $p \neq 7$, ceci est équivalent à :

$$p^3 \not\equiv 1 \mod 7.$$

De même, dans le deuxième cas, $p(t)$ est sans facteur de degré 1 et 3 sur $\mathbb{Q}_p$ si et seulement si 9 ne divise pas $p^3-1=(p-1)(p^2+p+1)$. Comme 3 divise $p-1$ si et seulement si il divise

p^2+p+1, notre condition est équivalente à :

$$p \not\equiv 1 \mod 3.$$

Si $p=7$ dans le premier cas ou $p=3$ dans le deuxième cas, $p(t)$ est irréductible sur $\mathbb{Q}_p$.

• Supposons que q n'est pas un carré. Pour $p=7$, comme $\Phi_{28}(t) = t^{12}-t^{10}+t^8-t^6+t^4-t^2+1$, le polynôme unitaire ayant pour racines les $\sqrt{q}\zeta_{28}$ est $t^{12}-qt^{10}+q^2t^8-q^3t^6+q^4t^4-q^5t^2+q^6$ qui est le produit des polynômes irréductibles :

$$t^6+\sqrt{pq}t^5+3qt^4+q\sqrt{pq}t^3+3q^2t^2+q^2\sqrt{pq}t+q^3,$$
$$t^6-\sqrt{pq}t^5+3qt^4-q\sqrt{pq}t^3+3q^2t^2-q^2\sqrt{pq}t+q^3.$$

Pour $p=3$, comme $\Phi_{36}(t) = t^{12}-t^6+1$, le polynôme unitaire ayant pour racines les $\sqrt{q}\zeta_{36}$ est $t^{12}-q^3t^6+q^6$ qui est le produit des polynômes irréductibles :

$$t^6+q\sqrt{pq}t^3+q^3,$$
$$t^6-q\sqrt{pq}t^3+q^3.$$

Les polynômes obtenus sont tous des polynômes caractéristiques de variétés abéliennes de dimension 3. En effet, si $f(t)$ est un facteur sur $\mathbb{Q}_p$ d'un tel polynôme, comme $f(0)$ est dans $\mathbb{Q}_p$, sa valuation est entière ; elle est de plus égale à $dn/2$, où d est le degré de $f(t)$. Donc d est pair, compte tenu du fait que n est impair. On en conclut que $e=1$.

Remarque. Le même raisonnement est valable pour g quelconque. Ainsi, l'entier e associé à un polynôme de Weil irréductible supersingulier est toujours égal à 1 lorsque n est impair.

1.4 Dimension 4

1.4.1 Les coefficients

Les polynômes de Weil de degré 8 sont de la forme

$$p(t) = t^8+a_1t^7+a_2t^6+a_3t^5+a_4t^4+qa_3t^3+q^2a_2t^2+q^3a_1t+q^4$$

avec $a_1,a_2,a_3,a_4 \in \mathbb{Z}$. Nous allons montrer le théorème suivant :

Théorème 1.4.1. *Le polynôme $p(t)$ est un polynôme de Weil si et seulement si les inégalités ci-dessous sont satisfaites*

1. $|a_1| \leq 8\sqrt{q}$,
2. $6\sqrt{q}|a_1| - 20q \leq a_2 \leq \frac{3a_1^2}{8} + 4q$,
3. $-9qa_1 - 4\sqrt{q}a_2 - 16q\sqrt{q} \leq a_3 \leq -9qa_1 + 4\sqrt{q}a_2 + 16q\sqrt{q}$,
4. $-\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 - (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2} \leq a_3 \leq -\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 + (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2}$,
5. $2\sqrt{q}|qa_1+a_3| - 2qa_2 - 2q^2 \leq a_4$,
6. $\frac{9a_1^4}{256} - \frac{3a_1^2a_2}{16} + \frac{a_1a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + \omega + \overline{\omega} \leq a_4 \leq \frac{9a_1^4}{256} - \frac{3a_1^2a_2}{16} + \frac{a_1a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + j\omega + j^2\overline{\omega}$

où

$\omega = \frac{1}{24}\Big(8(-\frac{3a_1^2}{8}+a_2-4q)^6 + 540(-\frac{3a_1^2}{8}+a_2-4q)^3(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^2$

$-729(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^4$

$+i9|\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3|(-(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^2 - \frac{8}{27}(-\frac{3a_1^2}{8}+a_2-4q)^3)^{3/2}\Big)^{1/3}$,

$\omega^{1/3} = |\omega|^{1/3}e^{\frac{arg(\omega)i}{3}}$ *et* $j = e^{\frac{2i\pi}{3}}$.

Commençons par déterminer un critère pour qu'un polynôme à coefficients réels de degré 4 n'ait que des racines réelles.

Soit $f(t) = t^4 + r_1t^3 + r_2t^2 + r_3t + r_4$ un polynôme à coefficients réels. Une simple étude du tableau de variations de $f(t)$ nous permet de voir qu'il existe un r_4 pour lequel $f(t)$ n'a que des racines réelles si et seulement si $f'(t)$ n'a que des racines réelles. Cette dernière condition équivaut à :

$$\Delta_{f'} \geq 0 \tag{1.3}$$

où $\Delta_{f'}$ est le discriminant de $f'(t)$.

Le discriminant de $f(t)$ est un polynôme de degré 3 en r_4 que nous noterons $\Delta_f(t)$ (c'est-à-dire $\Delta_f(r_4)$ est le discriminant de $f(t)$). Si $f(t)$ n'a que des racines réelles, $\Delta_f(r_4)$ est positif. De plus, comme $\Delta_f(r_4) = 0$ quand $f(t)$ a une racine multiple, la fonction qui à r_4 associe le nombre de racines de $f(t)$ est constante sur les intervalles délimités par les racines de $\Delta_f(t)$.

Lorsque r_4 est grand, le graphe de $f(t)$ ne touche pas l'axe des abscisses et par conséquent $f(t)$ n'a pas de racine réelle. Par suite, si γ_3 est la plus grande racine de $\Delta_f(t)$, $f(t)$ n'a pas de racine réelle pour $r_4 \in]\gamma_3; +\infty[$.

En conclusion, si l'inégalité (1.3) est vérifiée alors $\Delta_f(t)$ possède 3 racines réelles $\gamma_1 \leq \gamma_2 \leq \gamma_3$ et $f(t)$ n'a que des racines réelles si et seulement si :

$$\gamma_1 \leq r_4 \leq \gamma_2. \tag{1.4}$$

Pour $k = 1, 2, 3, 4$, on note s_k les fonctions symétriques des $x_i = -(\alpha_i + q/\alpha_i)$, où $\alpha_1, q/\alpha_1, \ldots, \alpha_4, q/\alpha_4$ sont les racines de $p(t)$. En développant l'expression $p(t) = \prod_{i=1}^{4}(t^2 + x_it + q)$, on trouve :

$$\begin{aligned} s_1 &= a_1, \\ s_2 &= a_2 - 4q, \\ s_3 &= a_3 - 3qa_1, \\ s_4 &= a_4 - 2qa_2 + 2q^2. \end{aligned}$$

Nous allons appliquer notre critère à $f^0(t) = \prod_{i=1}^{4}(t + x_i - \frac{a_1}{4}) = t^4 + r_2t^2 + r_3t + r_4$ où :

$$\begin{aligned} r_2 &= -\frac{3s_1^2}{8} + s_2, \\ r_3 &= \frac{s_1^3}{8} - \frac{s_1s_2}{2} + s_3, \\ r_4 &= -\frac{3s_1^4}{256} + \frac{s_1^2s_2}{16} - \frac{s_1s_3}{4} + s_4. \end{aligned}$$

En remplaçant s_1, s_2, s_3, s_4 par leur expression en a_1, a_2, a_3, a_4, on obtient :

$$\begin{aligned} r_2 &= -\frac{3a_1^2}{8} + a_2 - 4q, \\ r_3 &= \frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3, \\ r_4 &= -\frac{3a_1^4}{256} + \frac{qa_1^2}{2} + \frac{a_1^2a_2}{16} - \frac{a_1a_3}{4} - 2qa_2 + 2q^2 + a_4. \end{aligned}$$

On a :

$$\Delta_{f^0}(t) = 256t^3 - 128r_2^2t^2 + 16r_2(r_2^3 + 9r_3^2)t - r_3^2(4r_2^3 + 27r_3^2).$$

Pour calculer les racines de $\Delta_{f^0}(t)$, on utilise la méthode de Cardan décrite dans la Lemme 1.3.3. Soient :

$$\begin{aligned} u_2 &= -\frac{r_2^4}{48} + \frac{9r_2r_3^2}{16}, \\ u_3 &= \frac{r_2^6}{864} + \frac{5r_2^3r_3^2}{64} - \frac{27r_3^4}{256}, \\ \delta &= -u_3^2 - \frac{4}{27}u_2^3 = \frac{r_3^2(-8r_2^3 - 27r_3^2)^3}{1769472}. \end{aligned}$$

On suppose que l'inégalité (1.3) est vérifiée. Alors $\delta \geq 0$ et les racines de $\Delta_{f^0}(t)$ sont :

$$\begin{aligned} \gamma_1 &= \omega + \overline{\omega} + \frac{r_2^2}{6}, \\ \gamma_2 &= j\omega + j^2\overline{\omega} + \frac{r_2^2}{6}, \\ \gamma_3 &= j^2\omega + j\overline{\omega} + \frac{r_2^2}{6}. \end{aligned}$$

où

$$\omega = \frac{1}{24}\left(8r_2^6 + 540r_2^3r_3^2 - 729r_3^4 + i9|r_3|(-r_3^2 - \frac{8}{27}r_2^3)^{3/2}\right)^{1/3}.$$

De plus, en adoptant la convention $\omega^{1/3} = |\omega|^{1/3}e^{\frac{arg(\omega)i}{3}}$, on a $\gamma_1 \leq \gamma_2 \leq \gamma_3$. En remplaçant r_2, r_3, r_4 par leur expression en a_1, a_2, a_3, a_4 dans (1.4) on trouve la condition (6) du Théorème 1.4.1.

Il nous faut maintenant déterminer quand est-ce que (1.3) est vérifiée. On a :

$$\Delta_{f'} = -16(8r_2^3 + 27r_3^2).$$

On en déduit que (1.3) équivaut à :

$$r_2 \leq 0 \ \text{ et } \ -(\frac{-2r_2}{3})^{3/2} \leq r_3 \leq (\frac{-2r_2}{3})^{3/2}.$$

Ceci nous donne la deuxième inégalité de la condition (2) et la condition (4) du Théorème 1.4.1.

Enfin, pour $k = 1, 2, 3, 4$, on note r_k^+ et r_k^- les coefficients respectifs de $f^+(t) = \prod_{i=1}^4(t - (2\sqrt{q} + x_i))$ et $f^-(t) = \prod_{i=1}^4(t - (2\sqrt{q} - x_i))$. On a :

$$\begin{aligned} r_1^+ &= -8\sqrt{q} - s_1, \\ r_2^+ &= 24q + 6\sqrt{q}s_1 + s_2, \\ r_3^+ &= -32q\sqrt{q} - 12qs_1 - 4\sqrt{q}s_2 - s_3, \\ r_4^+ &= 16q^2 + 8q\sqrt{q}s_1 + 4qs_2 + 2\sqrt{q}s_3 + s_4 \end{aligned}$$

et

$$\begin{aligned} r_1^- &= -8\sqrt{q} + s_1, \\ r_2^- &= 24q - 6\sqrt{q}s_1 + s_2, \\ r_3^- &= -32q\sqrt{q} + 12qs_1 - 4\sqrt{q}s_2 + s_3, \\ r_4^- &= 16q^2 - 8q\sqrt{q}s_1 + 4qs_2 - 2\sqrt{q}s_3 + s_4. \end{aligned}$$

En remplaçant s_1, s_2, s_3 par leur expression en a_1, a_2, a_3, on obtient :

$$\begin{aligned} r_1^+ &= -8\sqrt{q} - a_1, \\ r_2^+ &= 20q + 6\sqrt{q}a_1 + a_2, \\ r_3^+ &= -16q\sqrt{q} - 9qa_1 - 4\sqrt{q}a_2 - a_3, \\ r_4^+ &= 2q^2 + 2q\sqrt{q}a_1 + 2qa_2 + 2\sqrt{q}a_3 + a_4 \end{aligned}$$

et

$$\begin{aligned} r_1^- &= -8\sqrt{q} + a_1, \\ r_2^- &= 20q - 6\sqrt{q}a_1 + a_2, \\ r_3^- &= -16q\sqrt{q} + 9qa_1 - 4\sqrt{q}a_2 + a_3, \\ r_4^- &= 2q^2 - 2q\sqrt{q}a_1 + 2qa_2 - 2\sqrt{q}a_3 + a_4. \end{aligned}$$

Si les racines de $f^+(t)$ et $f^-(t)$ sont toutes réelles (ce qui revient à dire que celles de $f^0(t)$ le sont), elles sont toutes positives si et seulement si $(-1)^k r_k^+ \geq 0$ et $(-1)^k r_k^- \geq 0$ pour $k = 1, 2, 3, 4$. Ceci nous donne les conditions manquantes du Théorème 1.4.1 et conclut la preuve.

1.4.2 Polynômes caractéristiques réductibles

Soit $p(t)$ le polynôme caractéristique d'une variété abélienne de dimension 4. Alors $p(t) = h(t)^e$ où $h(t)$ est un polynôme de Weil irréductible et e un entier divisant 8. Comme $p(t)$ n'a pas de racine réelle on a $e \neq 8$. On étudiera le cas $e = 1$ dans la Section 1.3.3. Lorsque $e = 2$ ou $e = 4$, l'ensemble des $h(t)$ possibles se déduit directement des Propositions 1.2.2 et 1.2.6. Une version un peu moins explicite de la proposition suivante a été prouvée par Xing.

Proposition 1.4.2 (Xing)**.** *Le polynôme $p(t)$ est le polynôme caractéristique réductible d'une variété abélienne simple de dimension 4 si et seulement si soit n est divisible par 4 et*

$$p(t) = (t^2 + b_1 t + q)^4$$

avec $|b_1| < 2\sqrt{q}$ et $b_1 = kq^{1/4}$ où k est un entier premier avec p, soit

$$p(t) = (t^4 + b_1 t^3 + b_2 t^2 + q b_1 t + q^2)^2$$

et l'une des conditions suivantes est vérifiée :

- *$v_p(b_1) = 0$, $v_p(b_2) \geq n/2$ et $((b_2 + 2q)^2 - 4qb_1^2)$ est un carré dans $\mathbb{Q}_p$,*
- *$v_p(b_1) \geq n/4$, $v_p(b_2) = n/2$, n est pair et $(b_1^2 - 4b_2 + 8q)$ n'est pas un carré dans $\mathbb{Q}_p$,*
- *n est pair et le couple (b_1, b_2) fait partie de la liste suivante :*
  1. *$(0, 0)$, $p \equiv 1 \mod 8$,*
  2. *$(0, -q)$, $p \equiv 1 \mod 12$,*
  3. *$(\pm\sqrt{q}, q)$, $p \equiv 1 \mod 5$.*

Pour $e = 4$, le seul polygone de Newton possible est celui représenté par la Figure 1.18 de la Section 1.4.3 ; le p-rang des variétés abéliennes associées est 0. Dans le cas où $e = 2$, les polygones de Newton correspondant aux différents points de la Proposition 1.4.2 sont respectivement ceux représentés par les Figures 1.14, 1.18 et 1.19 (le dernier point est le cas supersingulier) et les p-rangs sont 2, 0 et 0.

1.4.3 Polynômes caractéristiques irréductibles

Dans cette section nous allons prouver le théorème suivant :

Théorème 1.4.3. *Le polynôme de Weil $p(t)$ est le polynôme caractéristique irréductible d'une variété abélienne de dimension 4 si et seulement si l'une des conditions suivantes est vérifiée :*

1. $v_p(a_4) = 0$,
2. $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$ *et* $p(t)$ *n'a pas de racine de valuation* $n/2$ *dans* $\mathbb{Q}_p$,
3. $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq n$ *et* $p(t)$ *n'a pas de racine de valuation* $n/2$ *dans* $\mathbb{Q}_p$,
4. $v_p(a_1) = 0$, $v_p(a_2) \geq n/3$, $v_p(a_3) \geq 2n/3$, $v_p(a_4) = n$ *et* $p(t)$ *n'a pas de racine de valuation* $n/3$ *et* $2n/3$ *dans* $\mathbb{Q}_p$,
5. $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 3n/2$ *et* $p(t)$ *n'a pas de racine de valuation* $n/2$ *ni de facteur de degré* 3 *dans* $\mathbb{Q}_p$,
6. $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$, $v_p(a_4) \geq 3n/2$ *et* $p(t)$ *n'a pas de racine dans* $\mathbb{Q}_p$,
7. $v_p(a_1) \geq n/4$, $v_p(a_2) \geq n/2$, $v_p(a_3) = 3n/4$, $v_p(a_4) = n$ *et* $p(t)$ *n'a pas de racine ni de facteur de degré* 2 *dans* $\mathbb{Q}_p$,
8. $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) = 3n/2$, $v_p(a_4) \geq 2n$ *et* $p(t)$ *n'a pas de racine ni de facteur de degré* 3 *dans* $\mathbb{Q}_p$.

De plus, les cas (1), (2), (3), (4), (5), (6), (7) et (8) correspondent respectivement à des variétés abéliennes de p-rang 4, 3, 2, 1, 1, 0, 0 *et* 0. *Les variétés abéliennes du cas (8) sont supersingulières.*

Les polygones de Newton possibles pour $p(t)$ sont représentés par les Figures 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18 et 1.19 (voir Section 1.1.3).

Figure 1.12 : $\mathbf{v_p(a_4) = 0}$. On a toujours $e = 1$.

Figure 1.13 : $\mathbf{v_p(a_4) \geq n/2}$ et $\mathbf{v_p(a_3) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ un facteur de degré 2 dont les racines sont de valuation $n/2$ et $e = 1$ si et seulement si celui-ci est irréductible, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine de valuation $n/2$ dans $\mathbb{Q}_p$.

Figure 1.14 : $\mathbf{v_p(a_4) \geq n}$, $\mathbf{v_p(a_3) \geq n/2}$ et $\mathbf{v_p(a_2) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ un facteur de degré 4 dont les racines sont de valuation $n/2$ et $e = 1$ si et seulement si celui-ci n'a pas de racine, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine de valuation $n/2$ dans $\mathbb{Q}_p$.

Figure 1.15 : $\mathbf{v_p(a_4) = n}$, $\mathbf{v_p(a_3) \geq 2n/3}$, $\mathbf{v_p(a_2) \geq n/3}$ et $\mathbf{v_p(a_1) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ deux facteurs de degré 3, un dont les racines sont de valuation $2n/3$ et l'autre dont les racines sont de valuation $n/3$; $e = 1$ si et seulement si ceux-ci sont irréductibles, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine de valuation $2n/3$ et $n/3$ dans $\mathbb{Q}_p$.

Figure 1.16 : $\mathbf{v_p(a_4) \geq 3n/2}$, $\mathbf{v_p(a_3) \geq n}$, $\mathbf{v_p(a_2) \geq n/2}$ et $\mathbf{v_p(a_1) = 0}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ un facteur de degré 6 dont les racines sont de valuation $n/2$ et donc $e = 1$ si et seulement si $p(t)$ n'a dans $\mathbb{Q}_p$ ni de racine ni de facteur de degré 3.

Figure 1.17 : $\mathbf{v_p(a_4) \geq 3n/2}$, $\mathbf{v_p(a_3) = n}$, $\mathbf{v_p(a_2) \geq 2n/3}$ et $\mathbf{v_p(a_) \geq n/3}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ deux facteurs de degré 2 et un de degré 3 ; $e = 1$ si et seulement si ceux-ci sont irréductibles, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine dans $\mathbb{Q}_p$.

Figure 1.18 : $\mathbf{v_p(a_4) = n}$, $\mathbf{v_p(a_3) \geq 3n/4}$, $\mathbf{v_p(a_2) \geq n/2}$ et $\mathbf{v_p(a_1) \geq n/4}$. Le polynôme $p(t)$ a dans $\mathbb{Q}_p$ deux facteurs de degré 4 ; $e = 1$ si et seulement si ceux-ci sont irréductibles, c'est-à-dire si et seulement si $p(t)$ n'a pas de racine ni de facteur de degré 2 dans $\mathbb{Q}_p$.

Figure 1.19 : $\mathbf{v_p(a_4) \geq 2n}$, $\mathbf{v_p(a_3) \geq 3n/2}$, $\mathbf{v_p(a_2) \geq n}$ et $\mathbf{v_p(a_1) \geq n/2}$. On a $e = 1$ si et seulement si $p(t)$ n'a dans $\mathbb{Q}_p$ ni de racine ni de facteur de degré 3.

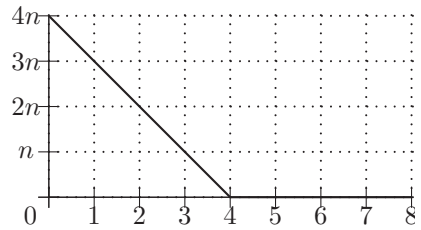

FIGURE 1.12 – Ordinaire

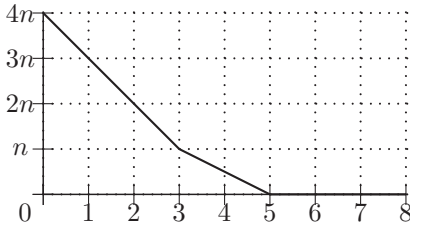

FIGURE 1.13 – p-rang 3

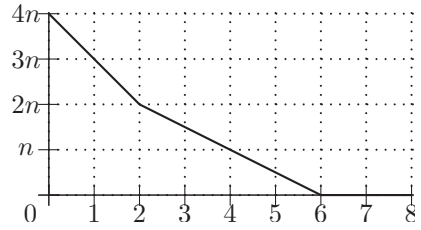

FIGURE 1.14 – p-rang 2

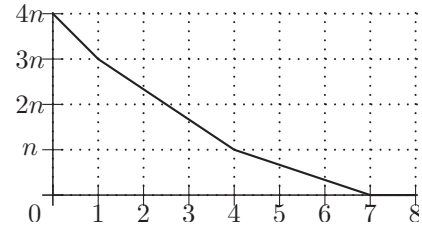

FIGURE 1.15 – p-rang 1 : 1er cas

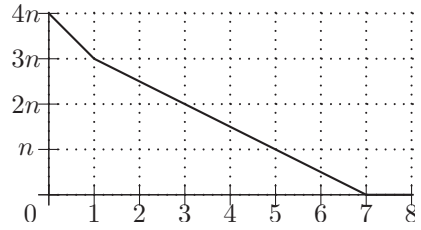

FIGURE 1.16 – p-rang 1 : 2ième cas

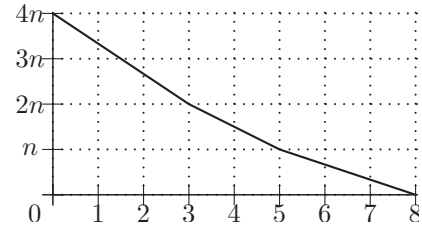

FIGURE 1.17 – p-rang 0 : 1er cas

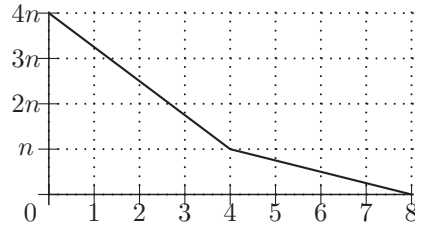

FIGURE 1.18 – p-rang 0 : 2ième cas

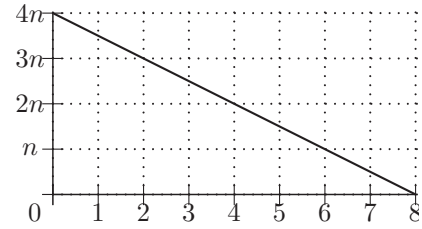

FIGURE 1.19 – Supersingulier

1.4.4 Polynômes caractéristiques supersinguliers

La condition (8) du Théorème 1.4.3 peut être rendue plus explicite :

Proposition 1.4.4. *Le polynôme $p(t)$ est le polynôme caractéristique irréductible d'une variété abélienne supersingulière de dimension 4 si et seulement si l'une des conditions suivantes est vérifiée :*

- *n est pair et le quadruplet (a_1, a_2, a_3, a_4) fait partie de la liste suivante :*
  1. $(\varepsilon\sqrt{q}, 0, -\varepsilon q\sqrt{q}, -q^2)$, $\varepsilon \in \{-1, 1\}$, $p \not\equiv 1 \mod 15$,
  2. $(0, 0, 0, 0)$, $p \not\equiv 1 \mod 16$,

3. $(0, -q, 0, q^2)$, $p \not\equiv 1 \mod 20$,
4. $(0, 0, 0, -q^2)$, $p \not\equiv 1 \mod 24$,

- *n est impair et le quadruplet (a_1, a_2, a_3, a_4) fait partie de la liste suivante :*
  1. $(\varepsilon\sqrt{pq}, q, 0, -q^2)$, $\varepsilon \in \{-1, 1\}$, $p = 2$,
  2. $(\varepsilon\sqrt{pq}, 2q, \varepsilon q\sqrt{pq}, q^2)$, $\varepsilon \in \{-1, 1\}$, $p = 3$,
  3. $(0, 0, 0, 0)$,
  4. $(0, -q, 0, q^2)$,
  5. $(0, q, 0, q^2)$, $p \neq 5$,
  6. $(0, 0, 0, -q^2)$, $p \neq 2$,
  7. $(\varepsilon\sqrt{pq}, 2q, \varepsilon q\sqrt{pq}, 3q^2)$, $\varepsilon \in \{-1, 1\}$, $p = 5$.

Démonstration. La liste des polynômes caractéristiques irréductibles de variétés abéliennes supersingulières de dimension 4 quand q n'est pas un carré se trouve dans l'article de McGuire, Singh et Zaytsev [15]. Supposons donc que q est un carré.

Les q-nombres de Weil supersinguliers sont de la forme $\sqrt{q}\zeta_m$. On en déduit que les polynômes caractéristiques irréductibles de variétés abéliennes supersingulières de dimension 4 sont de la forme :

$$p(t) = q^g \Phi_m(\frac{t}{\sqrt{q}})$$

avec $\varphi(m) = 2g = 8$ (où φ est la fonction indicatrice d'Euler) ce qui revient à dire que $\Phi_m(t)$ fait partie de la liste suivante :

$$\begin{aligned}
\Phi_{15}(t) &= t^8 - t^7 + t^5 - t^4 + t^3 - t + 1, \\
\Phi_{16}(t) &= t^8 + 1, \\
\Phi_{20}(t) &= t^8 - t^6 + t^4 - t^2 + 1, \\
\Phi_{24}(t) &= t^8 - t^4 + 1, \\
\Phi_{30}(t) &= t^8 + t^7 - t^5 - t^4 - t^3 + t + 1.
\end{aligned}$$

Il reste à regarder quand $p(t)$ est sans facteurs de degré 1 et 3 sur $\mathbb{Q}_p$, c'est-à-dire quand les racines primitives m-ièmes de l'unité ne sont pas de degré divisant 3 sur $\mathbb{Q}_p$. Si $(m, p) = 1$, le degré de ζ_m sur $\mathbb{Q}_p$ est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^*$ qui est soit égal à 1 soit pair puisque $\varphi(m) = 2^3$. Notre condition est donc équivalente à :

$$p \not\equiv 1 \mod m.$$

Si $(m, p) \neq 1$, nous allons montrer que le corps $\mathbb{Q}_p(\zeta_m)$ contient un élément de degré pair sur $\mathbb{Q}_p$ et notre condition sera donc vérifiée. Si $p \neq 2$ ou $v_2(m) \neq 1$, le degré d'une racine primitive $p^{v_p(m)}$-ième de l'unité est $(p-1)p^{v_p(m)-1}$ qui est bien un nombre pair. Si $m = 30$ et $p = 2$, on peut par exemple prendre ζ_3 qui est de degré 2 sur $\mathbb{Q}_p$. □

Chapitre 2

Bornes sur le nombre de points rationnels des variétés abéliennes et jacobiennes sur les corps finis

Nous donnons ici des majorations et minorations du nombre de points des variétés abéliennes et jacobiennes sur les corps finis.

En ce qui concerne les variétés abéliennes, nous disposons d'estimations classiques du nombre de points : les bornes de Weil. Nous montrerons comment utiliser l'inégalité arithmético-géométrique pour améliorer celles-ci ; les bornes obtenues ainsi seront généralement optimales. Nous verrons ensuite des bornes sur le nombre de points des variétés abéliennes qui dépendent de leur trace ; l'intérêt de faire cela est que si nos variétés abéliennes sont des jacobiennes ou des variétés de Prym, la trace de celles-ci s'exprime facilement en fonction du nombre de points des courbes correspondantes.

Il est aussi possible d'obtenir des bornes qui sont spécifiques aux jacobiennes ; c'est ce qu'ont fait par exemple Lachaud et Martin-Deschamps dans [12]. Ceci se fait en établissant des identités combinatoires reliant les nombres de points d'une courbe sur les extensions finies du corps de base et les nombres de ses points et diviseurs effectifs de degré donné.

Ce chapitre est un résumé d'un travail commun [1] avec Yves Aubry et Gilles Lachaud.

2.1 Variétés abéliennes

On se donne une variété abélienne $A/\mathbb{F}_q$ de dimension g, $q = p^n$, on note $p_A(t)$ son polynôme caractéristique et $\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}$ les racines de $p_A(t)$ comptées avec multiplicité (les ω_i sont des nombres complexes de module $\sqrt{q}$). On pose $x_i = -(\omega_i + \overline{\omega_i})$; par le Théorème de Honda-Tate, la donnée des x_i est équivalente à celle de la classe d'isogénie de A ; nous dirons que A est de *type* $[x_1, \ldots, x_g]$. La *trace* de A est celle de son polynôme caractéristique, c'est-à-dire la somme $\sum_{i=1}^{g}(\omega_i + \overline{\omega_i}) = -\sum_{i=1}^{g} x_i$. Rappelons que dans les chapitres précédents nous avions noté

$$a_1 = \sum_{i=1}^{g} x_i.$$

Le nombre de points rationnels de A est donné par

$$\#A(\mathbb{F}_q) = p_A(1),$$

et comme

$$p_A(t) = \prod_{i=1}^{g}(t-\omega_i)(t-\overline{\omega_i}) = \prod_{i=1}^{g}(t^2 + x_i t + q),$$

on a

$$\#A(\mathbb{F}_q) = \prod_{i=1}^{g}(q+1+x_i). \tag{2.1}$$

Comme les x_i sont de valeur absolue inférieure ou égale à $2\sqrt{q}$, on a les bornes de Weil :

$$(q+1-2\sqrt{q})^g \leq \#A(\mathbb{F}_q) \leq (q+1+2\sqrt{q})^g.$$

L'utilisation de l'inégalité arithmético-géométrique va nous permettre d'obtenir des estimations plus précises du nombre de points de A. Celle-ci se prouve de manière élémentaire : on applique la fonction logarithme népérien aux termes à comparer et on remarque que cette fonction est strictement concave.

Lemme 2.1.1 (Inégalité arithmético-géométrique)**.** *Si $c_1, \ldots, c_n$ sont des réels strictement positifs, on a*

$$\sqrt[n]{c_1 \ldots c_n} \leq \frac{1}{n}(c_1 + \cdots + c_n)$$

(la moyenne géométrique est inférieure ou égale à la moyenne arithmétique) avec égalité si et seulement si tous les c_i sont égaux.

En appliquant ce lemme à (2.1), nous obtenons la proposition suivante, prouvée par Quebbemann [24] dans le cas des jacobiennes et Perret [23] dans le cas des variétés de Prym :

Proposition 2.1.2. *On a*

$$\#A(\mathbb{F}_q) \leq \left(q+1+\frac{a_1}{g}\right)^g$$

avec égalité si et seulement si tous les x_i sont égaux.

Remarque. Soient $a_1 = g\left[\frac{a_1}{g}\right] + r$ et $y_i = x_i - \left[\frac{a_1}{g}\right]$, $i = 1, \ldots, g$. Supposons que les $(y_{i_1} + \cdots + y_{i_r})$ soient tous strictement positifs, un raisonnement analogue à celui de le preuve du Théorème 2.1.3 ci-dessous nous donne :

$$\begin{aligned}
1 &\leq \left(\prod_{\{i_1,\ldots,i_{g-r}\}\subseteq\{1,\ldots,g\}} (y_{i_1} + \cdots + y_{i_{g-r}})\right)^{1/\binom{g}{g-r}} \\
&\leq \frac{1}{\binom{g}{g-r}} \sum_{\{i_1,\ldots,i_{g-r}\}\subseteq\{1,\ldots,g\}} (y_{i_1} + \cdots + y_{i_{g-r}}) \\
&= \frac{1}{\binom{g}{g-r}} \binom{g-1}{g-r-1} \sum_{i=1}^{g} y_i \\
&= \frac{r(g-r)}{g}.
\end{aligned}$$

Il en résulte que si $r = 1$, $r = g-1$ ou encore si tous les x_i sont de degré inférieur ou égal à 4 (par exemple si $g \leq 4$), notre hypothèse de départ est fausse et donc que, quitte à renuméroter les x_i,

nous avons $\sum_{i=1}^{g-r} y_i \leq 0$, c'est-à-dire $\sum_{i=1}^{g-r} x_i \leq (g-r)\left[\frac{a_1}{g}\right]$ (et donc $\sum_{i=g-r+1}^{g} x_i \geq r(\left[\frac{a_1}{g}\right]+1)$). Par suite,

$$\begin{aligned}\#A(\mathbb{F}_q) = \prod_{i=1}^{g}(q+1+x_i) &\leq \left(q+1+\frac{\sum_{i=1}^{g-r} x_i}{g-r}\right)^{g-r}\left(q+1+\frac{\sum_{i=g-r+1}^{g} x_i}{r}\right)^{r} \\ &\leq \left(q+1+\left[\frac{a_1}{g}\right]\right)^{g-r}\left(q+2+\left[\frac{a_1}{g}\right]\right)^{r}\end{aligned}$$

où pour la dernière inégalité, nous avons utilisé le fait que si $(g-r)a+rb = (g-r)c+rd$ et $0 \leq a \leq c \leq d \leq b$ alors $a^{g-r}b^r \leq c^{g-r}d^r$ (en effet, le barycentre de $(a;\ln a)$ et $(b;\ln b)$ munis des poids $g-r$ et r est $(((g-r)a+rb)/g);((g-r)\ln a + r\ln b)/g)$ et celui de $(c;\ln c)$ et $(d;\ln d)$ avec les mêmes poids est $(((g-r)c+rd)/g);((g-r)\ln c+r\ln d)/g) = (((g-r)a+rb)/g);((g-r)\ln c+r\ln d)/g)$; on conclut en utilisant la concavité de la fonction logarithme).

Notons qu'il existe des minorations plus fines du rapport entre la trace et le degré d'un entier algébrique totalement positif (par exemple dans [31]) mais celles-ci n'améliorent que très peu nos restrictions. Il serait intéressant da savoir ce qu'il se passe dans le cas général.

On pose $m = [2\sqrt{q}]$. Dans [28], Serre a montré que

$$|a_1| \leq gm \tag{2.2}$$

avec égalité si et seulement si les x_i sont tous égaux à $-m$ ou tous égaux à m. En combinant (2.2) et la Proposition 2.1.2 on trouve

$$\#A(\mathbb{F}_q) \leq (q+1+m)^g.$$

Il est naturel de se demander si $\#A(\mathbb{F}_q)$ admet une borne inférieure de la même forme, et la réponse à cette question s'avère être positive.

Théorème 2.1.3. *Soit $A/\mathbb{F}_q$ une variété abélienne de dimension g. Alors*

$$(q+1-m)^g \leq \#A(\mathbb{F}_q) \leq (q+1+m)^g$$

avec égalité à gauche si et seulement si tous les x_i sont égaux à $-m$ et égalité à droite si et seulement si tous les x_i sont égaux à m.

Démonstration. Il suffit de prouver la première inégalité. Pour $k = 0,\ldots,g$, on note t_k les fonctions symétriques des $(m+1+x_i)$, $i = 1,\ldots,g$. Si $k \geq 1$, on définit la quantité

$$p_k = \prod_{\{i_1,\ldots,i_k\}\subseteq\{1,\ldots,g\}}\prod_{j=1}^{k}(m+1+x_{i_j}).$$

On voit que p_k est un entier algébrique rationnel (car fixé par tout $\overline{\mathbb{Q}}$-automorphisme), c'est donc un entier strictement positif (car les $(m+1+x_{i_j})$ le sont), et par conséquent

$$p_k \geq 1.$$

De plus, l'inégalité arithmético-géométrique nous donne

$$p_k^{1/\binom{g}{k}} \leq \frac{1}{\binom{g}{k}}\sum_{\{i_1,\ldots,i_k\}\subseteq\{1,\ldots,g\}}\prod_{j=1}^{k}(m+1+x_{i_j}) = \frac{1}{\binom{g}{k}}t_k.$$

En combinant ces deux dernières inégalités, on trouve

$$\binom{g}{k} \leq t_k. \tag{2.3}$$

Si on multiplie chaque membre de (2.3) par $(q-m)^{g-k}$ puis on additionne les inégalités obtenues pour $k = 0, \ldots, g$, il vient

$$\sum_{k=0}^{g} \binom{g}{k} (q-m)^{g-k} \leq \sum_{k=0}^{g} t_k (q-m)^{g-k}$$

ce qui est exactement le résultat à prouver. Enfin, remarquons que toutes les inégalités de la preuve sont des égalités si et seulement si les x_i sont égaux à $-m$. □

Aussi, l'inégalité (2.3) nous donne une borne inférieure du nombre de points de A en fonction de sa trace.

Proposition 2.1.4. *Soit $A/\mathbb{F}_q$ une variété abélienne de type $[x_1, \ldots, x_g]$. On a*

$$\#A(\mathbb{F}_q) \geq (q+1-m)^g + (gm + a_1)(q-m)^{g-1}.$$

Démonstration. Avec les notations de la preuve du Théorème 2.1.3, on a

$$\begin{aligned} \#A(\mathbb{F}_q) &= \sum_{k=0}^{g} \binom{g}{k} (q-m)^{g-k} + \sum_{k=0}^{g} (t_k - \binom{g}{k})(q-m)^{g-k} \\ &= (q+1-m)^g + \sum_{k=0}^{g} (t_k - \binom{g}{k})(q-m)^{g-k} \\ &\geq (q+1-m)^g + (t_1 - g)(q-m)^{g-1}. \end{aligned}$$

où la dernière inégalité provient de (2.3). □

Remarque. Par (2.2), on a $gm + a_1 \geq 0$ et donc

$$(q+1-m)^g + (gm + a_1)(q-m)^{g-1} \geq (q+1-m)^g.$$

De plus, pour $g = 1$ (si $q \leq 4$ on a $q - m = 0$ et on adopte la convention $0^0 = 1$) la borne inférieure de la Proposition 2.1.4 est une égalité.

Il est aussi possible de minorer $\#A(\mathbb{F}_q)$ en utilisant des méthodes d'analyse réelle ; c'est ce qu'a fait Perret dans [23]. Son idée est de chercher à minimiser la fonction $(x_1, \ldots, x_g) \mapsto \prod_{i=1}^{g}(q+1+x_i)$ sur l'ensemble $\{(x_1, \ldots, x_g) \in [-2\sqrt{q}; 2\sqrt{q}]^g, \sum_{i=1}^{g} x_i = a_1\}$. En faisant le changement de variables $y_i = \frac{x_i}{2\sqrt{q}}$, on voit que cela revient à minimiser la fonction

$$F : (y_1, \ldots, y_g) \longmapsto \sum_{i=1}^{g} \ln(c + y_i),$$

$c = \frac{q+1}{2\sqrt{q}}$ sur $P = \{(y_1, \ldots, y_g) \in [-1; 1]^g, \sum_{i=1}^{g} y_i = \omega\}$ où $\omega = \frac{a_1}{2\sqrt{q}}$. La fonction F est strictement concave. Ses minimums sur le convexe compact P sont donc atteints en les points extrémaux de P. On vérifie qu'à permutation des coordonnées près les points extrémaux de P sont de la

forme $\gamma = (1, \dots, 1, -1, \dots, -1, \beta)$ où $\beta \in [-1; 1]$. On note u et v le nombre de 1 et de -1 de γ et on pose $\delta = 1$ si $\beta \in]-1; 1[$ et 0 sinon. On a

$$\begin{aligned} u + v + \delta &= g \\ u - v + \delta\beta &= \omega \end{aligned}$$

et en additionnant ces équations, on voit que si $\delta = 0$ alors $g+\omega$ est un entier pair ; la réciproque est vraie : si $\delta = 1$ alors $\beta \in]-1; 1[$ donc soit $\beta \neq 0$ et $g + \omega$ n'est pas un entier, soit $\beta = 0$ et $g + \omega = 2u + 1$.

Par suite, on a

$$\begin{aligned} \min_{(y_1,\dots,y_g)\in P} \exp F(y_1, \dots, y_g) &= (c+\beta)^\delta (c+1)^u (c-1)^v \\ &= (c+\beta)^\delta (c^2-1)^{\frac{u+v}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{u-v}{2}} \\ &= (c+\beta)^\delta (c^2-1)^{\frac{g-\delta}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{\omega-\delta\beta}{2}} \end{aligned}$$

et aussi $c + \beta \geq c - 1$ et $\omega - \delta\beta \geq \omega - \delta$. On en déduit le théorème suivant qui est une version légèrement rectifiée du résultat figurant dans [23] :

Théorème 2.1.5 (Perret)**.** *On a*

$$\#A(\mathbb{F}_q) \geq (q-1)^g \Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\frac{a_1}{2\sqrt{q}} - 2\delta}$$

où $\delta = 0$ si $g + \frac{a_1}{2\sqrt{q}}$ est un entier pair et 1 sinon.

Il est possible d'améliorer un peu cette borne en calculant plus explicitement les coordonnées de $\gamma = (1, \dots, 1, -1, \dots, -1, \beta)$. Si $\gamma \neq (1, \dots, 1)$, on note r et s le nombre de 1 et de -1 de γ cette fois-ci sans compter β. On a $r - s = \omega - \beta$ donc β doit être égal à $\{\omega\} = \omega - [\omega]$ ou $\{\omega\} - 1$ (quitte à permuter β avec une des coordonnées égales à -1 dans le cas où $\beta = 1$). On a donc

$$\begin{aligned} r + s &= g - 1 \\ r - s &= [\omega] + \epsilon \\ \beta &= \{\omega\} - \epsilon \end{aligned}$$

où $\epsilon \in \{0, 1\}$. Si $\gamma = (1, \dots, 1)$, les identités ci-dessus sont toujours vraies en posant $r = g$ et $s = -1$. Les équations $2r = g - 1 + [\omega] + \epsilon$ et $2s = g - 1 - [\omega] - \epsilon$, nous montrent que $\epsilon = 1$ si et seulement si $g + [\omega]$ est pair et que

$$r = \Big[\frac{g + [\omega]}{2}\Big] \quad \text{et} \quad s = \Big[\frac{g - 1 - [\omega]}{2}\Big].$$

Aussi, par le même calcul que ci-dessus on voit que

$$\min_{(y_1,\dots,y_g)\in P} \exp F(y_1, \dots, y_g) = (c + \{\omega\} - \epsilon)(c^2-1)^{\frac{g-1}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{[\omega]+\epsilon}{2}}.$$

D'où la proposition suivante

Proposition 2.1.6. *On a*

$$\begin{aligned}\#A(\mathbb{F}_q) &\geq (q-1)^{g-1}\Big(q+1+2\sqrt{q}\Big(\Big\{\frac{a_1}{2\sqrt{q}}\Big\}-\epsilon\Big)\Big)\Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\frac{\left[\frac{a_1}{2\sqrt{q}}\right]+\epsilon}{2}} \\ &= (q+1+a_1-2(r-s)\sqrt{q})(q+1+2\sqrt{q})^r(q+1-2\sqrt{q})^s\end{aligned}$$

où $\epsilon = 1$ *si* $g+\left[\frac{a_1}{2\sqrt{q}}\right]$ *est pair et* 0 *sinon,* $r = \left[\frac{g+\left[\frac{a_1}{2\sqrt{q}}\right]}{2}\right]$ *et* $s = \left[\frac{g-1-\left[\frac{a_1}{2\sqrt{q}}\right]}{2}\right]$.

Remarque. Si q n'est pas un carré, la borne de la Proposition 2.1.6 n'est pas atteinte sauf si $r = s$ (ceci implique $|a_1| < 2\sqrt{q}$) et a_1 est la trace d'une certaine courbe elliptique. Si q est un carré, cette borne est atteinte sauf si $a_1 - 2(r-s)\sqrt{q}$ n'est pas la trace d'une courbe elliptique (en particulier, elle est atteinte si a_1 est premier avec p).

2.2 Jacobiennes

Dans cette section, nous nous intéressons au cas où $A/\mathbb{F}_q$ est la jacobienne d'une courbe algébrique, projective, lisse, absolument irréductible, définie sur $\mathbb{F}_q$ et de genre g. Nous étudierons aussi les quantités

$$J_q(g) = \max_C \#J_C(\mathbb{F}_q) \quad \text{et} \quad j_q(g) = \min_C \#J_C(\mathbb{F}_q)$$

où C parcourt l'ensemble de telles courbes.

Nous commençons par rappeler quelques résultats et notations concernant les courbes sur les corps finis et leur fonction zêta. Pour plus de renseignements à ce sujet, on pourra par exemple consulter [33, 36] pour les résultats relatifs aux courbes et [25, 32] pour ceux relatifs à la formule exponentielle.

2.2.1 Courbes sur les corps finis

Soit C une courbe algébrique, projective, lisse, absolument irréductible de genre g définie sur $\mathbb{F}_q$. Pour $k \in \mathbb{N}\setminus\{0\}$, on pose $N_k = \#C(\mathbb{F}_{q^k})$; on utilisera souvent la notation $N_1 = N$. On note aussi A_k le nombre de diviseurs effectifs de C de degré k, $k \in \mathbb{N}$ et B_k le nombre de ses points de degré k, $k \in \mathbb{N}\setminus\{0\}$. Remarquons que $A_0 = 1$ et que l'on a la relation

$$N_k = \sum_{d|k} dB_d.$$

La *fonction zêta* de C est

$$Z_C(t) = \exp\Big(\sum_{k=1}^{+\infty} N_k \frac{t^k}{k}\Big) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)}$$

(voir Section 0.3.3). On a les identités

$$Z_C(t) = \prod_{k=1}^{+\infty}(1-t^k)^{-B_k} = \sum_{k=0}^{+\infty} A_k t^k. \tag{2.4}$$

La première égalité se prouve en appliquant la fonction logarithme et en développant les termes du second membre en série ; pour montrer la seconde égalité, on développe en série les $(1-t^k)$. On trouvera les détails de cette démonstration dans [36, Proposition 3.1.2.].

On définit le *type d'une courbe* (algébrique, projective, lisse, absolument irréductible) sur $\mathbb{F}_q$ comme étant celui de sa jacobienne. Les données suivantes sont équivalentes :

- le type de C,
- $Z_C(t)$,
- les N_k pour $k \in \mathbb{N} \setminus \{0\}$,
- les N_k pour $1 \leq k \leq g$.

En effet, en notant $\chi_C(t)$ le numérateur de la fonction zêta de C, on vérifie que $\chi'_C(t)/\chi_C(t) = \sum_{k=1}^{+\infty}(N_k - q^k - 1)t^{k-1}$ et, en posant $\chi_C(t) = \sum_{k=0}^{2g} c_k t^k$, on a donc les relations

$$kc_k = (N_k - q^k - 1)c_0 + (N_{k-1} - q^{k-1} - 1)c_1 + \cdots + (N_1 - q - 1)c_{k-1}$$

pour $1 \leq k \leq g$, $c_0 = 1$ et $c_{2g-k} = q^{g-k}c_i$ pour $0 \leq k \leq g$. Donc les N_k, $1 \leq k \leq g$ déterminent $Z_C(t)$. Le reste se vérifie facilement vu ce qui précède.

Soit $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ une suite d'indéterminées. A un élément $b = (b_1, \ldots, b_n) \in \mathbb{N}^n$ on associe le monôme $\mathbf{y}^b = y_1^{b_1} \ldots y_n^{b_n}$ de l'anneau des séries formelles $\mathbb{Q}[[\mathbf{y}]]$. On vérifie que

$$\begin{aligned}\exp\Big(\sum_{n=1}^{+\infty} y_n \frac{t^n}{n}\Big) &= \prod_{n=1}^{+\infty} \exp\Big(y_n \frac{t^n}{n}\Big) = \prod_{n=1}^{+\infty}\sum_{b_n=0}^{+\infty} \frac{1}{b_n!}\Big(y_n \frac{t^n}{n}\Big)^{b_n} \\ &= \sum_{b_1,\ldots b_k \in \mathbb{N}} \frac{\mathbf{y}^b}{b_1! \ldots b_k!} \frac{t^{b_1+2b_2+\cdots+kb_k}}{2^{b_2} \ldots k^{b_k}}.\end{aligned}$$

On pose $c(b) = \frac{n!}{b_1!\ldots b_n!}\frac{1}{2^{b_2}\ldots n^{b_n}}$, $b \in \mathbb{N}^n$, $C_0(\mathbf{y}) = 1$ et

$$C_n(\mathbf{y}) = \sum_{b\in\mathcal{P}_n} c(b)\mathbf{y}^b$$

pour $n \in \mathbb{N} \setminus \{0\}$ et

$$\mathcal{P}_n = \{b = (b_1, \ldots, b_n) \in \mathbb{N}^n | b_1 + 2b_2 + \cdots + nb_n = n\}.$$

On pose aussi

$$\mathcal{C}_n(\mathbf{y}) = \frac{C_n(\mathbf{y})}{n!}.$$

Le calcul effectué ci-dessus nous donne :

Proposition 2.2.1 (Formule exponentielle)**.** *Dans l'anneau $\mathbb{Q}[[\mathbf{y}]][[t]]$, on a*

$$\exp\Big(\sum_{n=1}^{+\infty} y_n \frac{t^n}{n}\Big) = \sum_{n=0}^{+\infty} \mathcal{C}_n(\mathbf{y})t^n.$$

Le polynôme $C_n(\mathbf{y})$ est à coefficients entiers et positifs. Plus précisément, on vérifie que $C_n(\mathbf{y}) = \sum_{\sigma\in\mathfrak{S}_n} \mathbf{y}^{\beta(\sigma)}$ où $\beta(\sigma) = (b_1(\sigma), \ldots, b_n(\sigma))$ et $b_k(\sigma)$ est le nombre de cycles de longueur k dans la décomposition en produit de cycles à supports disjoints de σ. Le polynôme $C_n(\mathbf{y})$ est appelé *indicateur de cycle* de $\mathfrak{S}_n$. Pour plus de renseignements à ce sujet et les détails de la preuve de la formule exponentielle, voir [25, 32].

Les coefficients de la série entière définie par le premier membre de (2.4) sont ceux intervenant dans la formule exponentielle, on développe facilement le deuxième membre en utilisant la formule du binôme négatif

$$(1-t)^{-M} = \sum_{n=0}^{+\infty} \binom{M+n-1}{n} t^n.$$

On trouve alors

$$\mathcal{C}_n(N_1,\dots,N_n)=\sum_{b\in\mathcal{P}_n}\prod_{i=1}^{n}\binom{B_i+b_i-1}{b_i}=A_n. \tag{2.5}$$

Nous aurons aussi besoin de la proposition suivante :

Proposition 2.2.2. *Soient* $\mathbf{y}=(y_n)_{n\in\mathbb{N}}$ *et* $\mathbf{z}=(z_n)_{n\in\mathbb{N}}$ *des suites d'indéterminées et* $M\in\mathbb{N}$. *Pour* $n\in\mathbb{N}$, *on a :*

$$\mathcal{C}_n(\mathbf{y}+\mathbf{z})=\sum_{k=0}^{n}\mathcal{C}_k(\mathbf{y})\mathcal{C}_{n-k}(\mathbf{z})$$

et

$$\mathcal{C}_n(M,\dots,M)=\binom{M+n-1}{n}.$$

Démonstration. Pour prouver première identité, il suffit d'appliquer la formule exponentielle à tous les termes de

$$\exp\Big(\sum_{n=1}^{+\infty}(y_n+z_n)\frac{t^n}{n}\Big)=\exp\Big(\sum_{n=1}^{+\infty}y_n\frac{t^n}{n}\Big)\exp\Big(\sum_{n=1}^{+\infty}z_n\frac{t^n}{n}\Big)$$

et de développer le second membre. En ce qui concerne la deuxième identité, on a

$$\exp\Big(\sum_{n=1}^{+\infty}M\frac{t^n}{n}\Big)=\exp\Big(\sum_{n=1}^{+\infty}\frac{t^n}{n}\Big)^M=(1-t)^{-M}$$

et on conclut en appliquant la formule du binôme négatif. □

En utilisant le Théorème de Riemann-Roch, Lachaud et Martin-Deschamps [12] ont montré le résultat suivant :

Proposition 2.2.3 (Lachaud, Martin-Deschamps)**.** *Si* $g\geq 2$, *on a*

$$\begin{aligned}A_{n+g} &= q^{n+1}A_{g-n-2}+\#J_C(\mathbb{F}_q)\frac{q^{n+1}-1}{q-1} \quad \textit{pour } 0\leq n\leq g-2,\\ A_{n+g} &= \#J_C(\mathbb{F}_q)\frac{q^{n+1}-1}{q-1} \quad \textit{pour } n\geq g-1.\end{aligned}$$

Si on multiplie les deux côtés de l'identité $\frac{1}{(1-t)(1-qt)}=1+\sum_{n=0}^{+\infty}\frac{q^{n+1}-1}{q-1}t^n$ par $\chi_C(t)=\sum_{k=0}^{2g}c_kt^k$ et que l'on identifie les coefficients des séries entières obtenues, on trouve pour $1\leq n\leq 2g$

$$A_n=\sum_{k=0}^{n}c_k\frac{q^{n-k+1}-1}{q-1}.$$

La Proposition 2.2.3 se déduit facilement de ces dernières identités (compte tenu du fait que $\#J_C(\mathbb{F}_q)=\chi_C(1)=\sum_{k=0}^{2g}c_k$). En particulier, elle est vraie pour toute variété abélienne.

Il résulte de la Proposition 2.2.3 que

$$\sum_{n=0}^{g-2}A_nt^n+\sum_{n=0}^{g-1}q^{g-1-n}A_nt^{2g-2-n}=\frac{\chi_C(t)}{(1-t)(1-qt)}+\#J_C(\mathbb{F}_q)\frac{t^{g-1}}{q-1}\Big(\frac{1}{1-t}-\frac{1}{1-qt}\Big).$$

En faisant "tendre t vers 1", on trouve

Proposition 2.2.4 (Lachaud, Martin-Deschamps)**.**

$$\sum_{n=0}^{g-2} A_n + \sum_{n=0}^{g-1} q^{g-1-n} A_n = \#J_C(\mathbb{F}_q) \sum_{i=1}^{g} \frac{1}{|1-\omega_i|^2}.$$

Dans le même article, Lachaud et Martin-Deschamps ont donné deux majorations de $\sum_{i=1}^{g} \frac{1}{|1-\omega_i|^2}$:

$$\sum_{i=1}^{g} \frac{1}{|1-\omega_i|^2} \leq \frac{g}{(\sqrt{q}-1)^2}, \tag{2.6}$$

$$\sum_{i=1}^{g} \frac{1}{|1-\omega_i|^2} \leq \frac{1}{(q-1)^2}((g+1)(q+1)-N), \tag{2.7}$$

la seconde étant toujours meilleure que la première (mais dépendante de N).

2.2.2 Application des résultats de la Section 2.1

Comme les jacobiennes sont des variétés abéliennes particulières, les résultats de la section précédente s'appliquent. Tout d'abord, le Théorème 2.1.3 nous donne

$$(q+1-m)^g \leq j_q(g) \leq J_q(g) \leq (q+1+m)^g.$$

Soit $C/\mathbb{F}_q$ une courbe algébrique, projective, lisse, absolument irréductible, de genre g, de type $[x_1, \ldots, x_g]$ et N son nombre de points rationnels. Rappelons que l'on a $N = q+1+a_1$. La Proposition 2.1.2 nous donne donc

$$\#J_C(\mathbb{F}_q) \leq \Big(q+1+\frac{N-(q+1)}{g}\Big)^g.$$

En particulier, on a

$$J_q(g) \leq \Big(q+1+\frac{N_q(g)-(q+1)}{g}\Big)^g$$

où $N_q(g)$ est le nombre maximal de points rationnels sur une courbe algébrique, projective, lisse, absolument irréductible de genre g sur $\mathbb{F}_q$.

En utilisant la borne de Drinfeld-Vlăduţ $\limsup_{g\to\infty} N_q(g)/g \leq \sqrt{q}-1$, il vient

$$\limsup_{g\to\infty} (J_q(g))^{1/g} \leq q+\sqrt{q}$$

(la borne de Weil nous aurait seulement donné $q+1+2\sqrt{q}$). Notons que Vlăduţ [37] a prouvé que si q est un carré, alors

$$q(\frac{q}{q-1})^{\sqrt{q}-1} \leq \limsup_{g\to\infty} (J_q(g))^{1/g}.$$

Et lorsque $q \gg 0$, on a

$$q(\frac{q}{q-1})^{\sqrt{q}-1} = q+\sqrt{q}-\frac{1}{2}+o(1).$$

Remarque (sur les liens entre $N_q(g)$ et $J_q(g)$). Il se peut que le nombre de points de la jacobienne d'une courbe maximale (avec $N_q(g)$ points) n'atteigne pas $J_q(g)$. Par exemple, Serre [30, p. Se47] a montré qu'il existe deux courbes de genre 2 sur $\mathbb{F}_3$ possédant chacune $N_3(2) = 8$ points dont les jacobiennes ont 35 points pour l'une et 36 points pour l'autre.

Nous allons voir dans la Section 2.3 qu'une surface jacobienne maximale (avec $J_q(2)$ points) est toujours celle d'une courbe maximale (mais il n'y a aucune raison que cela reste vrai lorsque $g > 2$).

Une courbe atteignant la borne de Serre-Weil (avec $q+1+m$ points) est de type $[m, \dots, m]$ (voir (2.2)) donc dans le cas où la borne de Serre-Weil est atteinte, une courbe est maximale si et seulement si sa jacobienne l'est.

En ce qui concerne les bornes inférieures, la Proposition 2.1.4 nous donne

$$\#J_C(\mathbb{F}_q) \geq (q+1-m)^g + (gm + N - (q+1))(q-m)^{g-1}$$

et la Proposition 2.1.6 nous donne

$$\#J_C(\mathbb{F}_q) \geq (N - 2(r-s)\sqrt{q})(q+1+2\sqrt{q})^r(q+1-2\sqrt{q})^s$$

où $r = \left[\frac{g+\left[\frac{N-(q+1)}{2\sqrt{q}}\right]}{2}\right]$ et $s = \left[\frac{g-1-\left[\frac{N-(q+1)}{2\sqrt{q}}\right]}{2}\right]$.

2.2.3 Bornes spécifiques aux jacobiennes

Nous allons maintenant donner des bornes inférieures de $\#J_C(\mathbb{F}_q)$ ne provenant pas de bornes sur le nombre de points de variétés abéliennes. La méthode utilisée est d'exprimer au moyen d'identités combinatoires $\#J_C(\mathbb{F}_q)$ en fonction des N_k puis de minorer ces derniers par N ou de minorer les B_k par 0.

Soit $C/\mathbb{F}_q$ une courbe algébrique, projective, lisse, absolument irréductible de genre g. On lui attache les entiers N_n, A_n et B_n comme dans la Section 2.2.1. Le lemme suivant nous donne une minoration des A_n :

Lemme 2.2.5. *Pour $n \geq 2$, on a*

$$A_n \geq \binom{N+n-1}{n} + \sum_{i=2}^{n} B_i \binom{N+n-i-1}{n-i}.$$

Démonstration. Nous avons vu que pour $n \geq 1$, on a

$$A_n = \sum_{b \in \mathcal{P}_n} \prod_{i=1}^{n} \binom{B_i + b_i - 1}{b_i}$$

avec

$$\mathcal{P}_n = \{b = (b_1, \dots, b_n) \in \mathbb{N}^n \mid b_1 + 2b_2 + \cdots + nb_n = n\}.$$

Tous les termes de cette somme sont positifs, on peut donc la minorer par la somme des termes où b est l'un des

$$(n, 0, \dots, 0), (n-2, 1, 0, \dots, 0), (n-3, 0, 1, 0, \dots, 0), (n-4, 0, 0, 1, 0, \dots, 0), \dots,$$

$$\dots, (1, 0, \dots, 0, 1, 0), (0, \dots, 0, 1).$$

□

Par la Proposition 2.2.3, on a

$$A_{2g-1} = \#J_C(\mathbb{F}_q)\frac{q^g-1}{q-1},$$

et donc le Lemme 2.2.5 nous donne

Proposition 2.2.6. *On a*

$$\#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\Big(\binom{N+2g-2}{2g-1} + \sum_{i=2}^{2g-1} B_i\binom{N+2g-2-i}{2g-1-i}\Big).$$

En particulier,

$$\#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\binom{N+2g-2}{2g-1}.$$

La deuxième inégalité de la Proposition 2.2.6 a été obtenue en minorant les B_i par 0 pour $2 \leq i \leq 2g-1$. Il est en fait possible de n'effectuer cette minoration seulement pour $2 \leq i \leq g$:

Théorème 2.2.7. *On a*

$$\#J_C(\mathbb{F}_q) \geq \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}.$$

Démonstration. Tout d'abord, si $N = 0$, notre borne inférieure est négative ou nulle et il n'y a rien à montrer. Supposons donc que $N > 0$. On a

$$\begin{aligned}\binom{N+g-1}{g} - q\binom{N+g-3}{g-2} &= \binom{N+g-3}{g-2}\left(\frac{(N+g-1)(N+g-2)}{g(g-1)} - q\right)\\ &= \binom{N+g-3}{g-2}\left(\left(\frac{N-1}{g}+1\right)\left(\frac{N-1}{g-1}+1\right) - q\right).\end{aligned}$$

Nous pouvons donc aussi supposer que

$$\left(\frac{N-1}{g}+1\right)\left(\frac{N-1}{g-1}+1\right) - q \geq 0. \tag{2.8}$$

Soient $\mathbf{y}$ et $\mathbf{z}$ des suites d'indéterminées. Par la Proposition 2.2.2 on a

$$\begin{aligned}\mathcal{C}_g(\mathbf{y}+\mathbf{z}) - q\mathcal{C}_{g-2}(\mathbf{y}+\mathbf{z}) &= \sum_{k=0}^{g}\mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z}) - q\sum_{k=0}^{g-2}\mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-2-k}(\mathbf{z})\\ &= \sum_{k=0}^{g}\mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z}) - q\sum_{k=2}^{g}\mathcal{C}_{k-2}(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z})\\ &= \mathcal{C}_0(\mathbf{y})\mathcal{C}_g(\mathbf{z}) + \mathcal{C}_1(\mathbf{y})\mathcal{C}_{g-1}(\mathbf{z}) + \sum_{k=2}^{g}(\mathcal{C}_k(\mathbf{y}) - q\mathcal{C}_{k-2}(\mathbf{y}))\mathcal{C}_{g-k}(\mathbf{z}).\end{aligned}$$

On pose $\mathbf{n} = (N, N, N, \dots)$ et $\mathbf{d} = (N-N, N_2-N, N_3-N, \dots)$ de telle sorte que

$$\mathcal{C}_g(\mathbf{n}+\mathbf{d}) - q\mathcal{C}_{g-2}(\mathbf{n}+\mathbf{d}) = A_g - qA_{g-2} = \#J_C(\mathbb{F}_q)$$

(par (2.5) et la Proposition 2.2.3). Les termes de $\mathbf{n}$ et de $\mathbf{d}$ sont tous positifs, il en est donc de même pour les $\mathcal{C}_k(\mathbf{n})$ et les $\mathcal{C}_k(\mathbf{d})$. De plus, par la Proposition 2.2.2, on a

$$\mathcal{C}_k(\mathbf{n}) = \binom{N+k-1}{k}.$$

Donc pour $k = 2, \ldots, g$, on a

$$\begin{aligned}
\mathcal{C}_k(\mathbf{n}) - q\mathcal{C}_{k-2}(\mathbf{n}) &= \binom{N+k-1}{k} - q\binom{N+k-3}{k-2} \\
&= \binom{N+k-3}{k-2}\left(\frac{(N+k-1)(N+k-2)}{k(k-1)} - q\right) \\
&= \binom{N+k-3}{k-2}\left(\left(\frac{N-1}{k}+1\right)\left(\frac{N-1}{k-1}+1\right) - q\right) \\
&\geq \binom{N+k-3}{k-2}\left(\left(\frac{N-1}{g}+1\right)\left(\frac{N-1}{g-1}+1\right) - q\right) \\
&\geq 0
\end{aligned}$$

où la dernière inégalité provient de (2.8). On déduit de tout cela que

$$\begin{aligned}
\#J_C(\mathbb{F}_q) &= \mathcal{C}_0(\mathbf{n})\mathcal{C}_g(\mathbf{d}) + \mathcal{C}_1(\mathbf{n})\mathcal{C}_{g-1}(\mathbf{d}) + \sum_{k=2}^{g}(\mathcal{C}_k(\mathbf{n}) - q\mathcal{C}_{k-2}(\mathbf{n}))\mathcal{C}_{g-k}(\mathbf{d}) \\
&\geq (\mathcal{C}_g(\mathbf{n}) - q\mathcal{C}_{g-2}(\mathbf{n}))\mathcal{C}_0(\mathbf{d}) \\
&= \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}.
\end{aligned}$$

□

Remarque. On peut minorer $C_n(\mathbf{d}) = \sum_{b\in\mathcal{P}_n} c(b)\mathbf{d}^b$ par $(N_n - N)/n$ qui est le terme de la somme correspondant à $b = (0, \ldots, 0, 1)$, d'où

$$\mathcal{C}_0(\mathbf{n})\mathcal{C}_g(\mathbf{d}) \geq \frac{N_g - N}{g} \quad \text{et} \quad \mathcal{C}_1(\mathbf{n})\mathcal{C}_{g-1}(\mathbf{d}) \geq N\frac{N_{g-1} - N}{g-1}.$$

On en déduit que si la condition (2.8) est satisfaite, on a aussi

$$\#J_C(\mathbb{F}_q) \geq \frac{N_g - N}{g} + N\frac{N_{g-1} - N}{g-1} + \binom{N+g-1}{g} - q\binom{N+g-3}{g-2},$$

en particulier

$$\#J_C(\mathbb{F}_q) \geq \frac{q^g + 1 - 2gq^{g/2} - N}{g} + N\frac{q^{g-1} + 1 - 2gq^{(g-1)/2} - N}{g-1} + \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}.$$

La Proposition 2.2.4, les majorations (2.6) et (2.7) et le fait que $A_n \geq N$, $n \geq 1$ nous donnent le théorème suivant énoncé dans [12] :

Théorème 2.2.8 (Lachaud, Martin-Deschamps)**.** *On a*

$$\#J_C(\mathbb{F}_q) \geq (\sqrt{q} - 1)^2\frac{q^{g-1} - 1}{g}\frac{N+q-1}{q-1}$$

et

$$\#J_C(\mathbb{F}_q) \geq q^{g-1}\frac{(q-1)^2}{(q+1)(g+1)}.$$

Si de plus, on utilise le Lemme 2.2.5 au lieu de minorer les A_n par N, on trouve :

Théorème 2.2.9. *Si $g \geq 2$, on a*

$$\#J_C(\mathbb{F}_q) \geq \left[\sum_{n=0}^{g-2}\binom{N+n-1}{n} + \sum_{n=2}^{g-2}\sum_{i=2}^{n} B_i\binom{N+n-i-1}{n-i} + \right.$$

$$\left.\sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n} + \sum_{n=2}^{g-1} q^{g-1-n}\sum_{i=2}^{n} B_i\binom{N+n-i-1}{n-i}\right]\frac{(q-1)^2}{(g+1)(q+1)-N}.$$

En particulier,

$$\#J_C(\mathbb{F}_q) \geq \left[\sum_{n=0}^{g-2}\binom{N+n-1}{n} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}\right]\frac{(q-1)^2}{(g+1)(q+1)-N}.$$

Pour $n \in \mathbb{N}$ et $x > 0$ on pose $e_n(x) = \sum_{j=0}^{n} \frac{x^j}{j!}$. Soit $\Gamma(n,x)$ la fonction Gamma incomplète

$$\Gamma(n,x) = \int_x^\infty t^{n-1}e^{-t}dt.$$

On a

$$e_n(x) = e^x\frac{\Gamma(n+1,x)}{n!}$$

(ceci se montre en effectuant plusieurs intégrations par partie successives).

Corollaire 2.2.10. *Si $g \geq 2$, on a*

$$\#J_C(\mathbb{F}_q) \geq (e_{g-2}(N) + q^{g-1}e_{g-1}(q^{-1}N))\frac{(q-1)^2}{(g+1)(q+1)-N}.$$

Démonstration. Vu que

$$\binom{N+n-1}{n} \geq \frac{N^n}{n!},$$

le résultat provient directement du Théorème 2.2.9. □

2.3 Courbes elliptiques, surfaces jacobiennes

Les possibilités pour le nombre de points d'une courbe elliptique sont connues grâce au Théorème de Deuring et Waterhouse. La description de l'ensemble des polynômes caractéristiques de surfaces jacobiennes a récemment été achevée (voir [11]). Nous rappelons ici ces résultats et voyons comment les utiliser pour calculer $J_q(2)$ et $j_q(2)$.

Les nombres de points possibles pour une courbe elliptique sont donnés dans le Théorème 1.2.1 ; on en déduit la proposition suivante qui nous donne les valeurs de $J_q(1)$ et $j_q(1)$ (rappelons que $q = p^n$) :

Proposition 2.3.1 (Deuring, Waterhouse)**.**

1. *$J_q(1)$ vaut*
   - *$(q+1+m)$ si $n = 1$, n pair ou $p \nmid m$*
   - *$(q+m)$ sinon.*
2. *$j_q(1)$ vaut*
   - *$(q+1-m)$ si $n = 1$, n pair ou $p \nmid m$*

- $(q+2-m)$ *sinon.*

Les polynômes caractéristiques de surfaces abéliennes sont décrits dans la Section 1.2.2. On notera que contrairement au cas des courbes elliptiques, il n'est pas tout à fait évident de retrouver les polynômes caractéristiques correspondant à un nombre de points donné.

Weil a montré qu'une surface abélienne principalement polarisée sur $\mathbb{F}_q$ est soit la jacobienne polarisée d'une courbe de genre 2 sur $\mathbb{F}_q$, soit le produit de deux courbes elliptiques polarisées sur $\mathbb{F}_q$, soit la restriction des scalaires d'une courbe elliptique polarisée sur $\mathbb{F}_{q^2}$. Depuis, de nombreuses personnes ont mené des travaux visant à déterminer quelles classes d'isogénie de surfaces abéliennes contiennent une jacobienne, notamment Serre qui avait besoin de résultats à ce sujet pour calculer $N_q(2)$. Une réponse complète à cette question a finalement été donnée en 2009 dans [11] par Howe, Nart et Ritzenthaler : le polynôme caractéristique d'un produit de deux courbes elliptiques $p(t) = (t^2 - ut + q)(t^2 - vt + q)$, $u \leq v$ est celui d'une jacobienne si et seulement il ne figure pas dans le Tableau 2.1 et le polynôme caractéristique d'une surface abélienne simple $p(t) = t^4 + at^3 + bt^2 + qat + q^2$ est celui d'une jacobienne si et seulement il ne figure pas dans le Tableau 2.2.

p-rang	Conditions sur p et q	Conditions sur u et v
		$\lvert u - v\rvert = 1$
2		$u = v$ et $v^2 - 4q \in \{-3, -4, -7\}$
	$q = 2$	$\lvert u\rvert = \lvert v\rvert = 1$ et $u \neq v$
1	q carré	$u^2 = 4q$ et $u - v$ sans facteurs carrés
0	$p > 3$	$u^2 \neq v^2$
	$p = 3$ et q non carré	$u^2 = v^2 = 3q$
	$p = 3$ et q carré	$3\sqrt{q} \not\mid (u - v)$
	$p = 2$	$2q \not\mid (u^2 - v^2)$
	$q = 2$ ou 3	$u = v$
	$q = 4$ ou 9	$u^2 = v^2 = 4q$

TABLE 2.1 – Conditions pour qu'une surface abélienne non simple ne soit pas isogène à une jacobienne

p-rang	Conditions sur p et q	Conditions sur a et b
		$a^2 - b = q$, $b < 0$ et les diviseurs premiers de b sont $1 \mod 3$
2		$a = 0$ et $b = 1 - 2q$
	$p > 2$	$a = 0$ et $b = 2 - 2q$
0	$p \equiv 11 \mod 12$ et q carré	$a = 0$ et $b = -q$
	$p = 3$ et q carré	$a = 0$ et $b = -q$
	$p = 2$ et q non carré	$a = 0$ et $b = -q$
	$q = 2$ ou 3	$a = 0$ et $b = -2q$

TABLE 2.2 – Conditions pour qu'une surface abélienne simple ne soit pas isogène à une jacobienne

Soient maintenant A une surface abélienne sur $\mathbb{F}_q$ de type $[x_1, x_2]$ et

$$p_A(t) = (t^2 + x_1 t + q)(t^2 + x_2 t + q) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$$

son polynôme caractéristique. Remarquons que les coefficients de $p_A(t)$ sont liés au type de A par les formules

$$a_1 = x_1 + x_2 \quad \text{et} \quad a_2 = x_1x_2 + 2q.$$

On rappelle que

$$\#A(\mathbb{F}_q) = p_A(1) = q^2 + 1 + (q+1)a_1 + a_2.$$

Les inégalités

$$|a_1| \leq 2m \quad \text{et} \quad 2|a_1|\sqrt{q} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q \tag{2.9}$$

(voir Section 1.2.2) nous permettent de lister (Tableau 2.3) les couples (a_1, a_2) possibles avec $a_1 \geq 2m-2$. Les nombres de points sont classés par ordre décroissant et une variété abélienne

a_1	a_2	Type	Nb de pts
$2m$	m^2+2q	$[m,m]$	$(q+1+m)^2$
$2m-1$	m^2-m+2q	$[m,m-1]$	$(q+1+m)(q+m)$
	$m^2-m-1+2q$	$[m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}]$	$(q+1+m+\frac{-1+\sqrt{5}}{2})(q+1+m+\frac{-1-\sqrt{5}}{2})$
$2m-2$	$m^2-2m+1+2q$	$[m-1,m-1]$	$(q+m)^2$
	$m^2-2m+2q$	$[m,m-2]$	$(q+1+m)(q-1+m)$
	$m^2-2m-1+2q$	$[m-1+\sqrt{2}, m-1-\sqrt{2}]$	$(q+m+\sqrt{2})(q+m-\sqrt{2})$
	$m^2-2m-2+2q$	$[m-1+\sqrt{3}, m-1-\sqrt{3}]$	$(q+m+\sqrt{3})(q+m-\sqrt{3})$

TABLE 2.3 – Couples (a_1, a_2) maximisant le nombre de points de A

avec (a_1, a_2) ne figurant pas dans le tableau a un nombre de points strictement inférieur aux valeurs du tableau. En effet, si $-2m \leq a_1 < 2m-2$ on a :

$$\begin{aligned}
(q+1)a_1 + a_2 &\leq [(q+1)a_1 + \frac{{a_1}^2}{4} + 2q] \\
&\leq [(q+1)(2m-3) + \frac{(2m-3)^2}{4} + 2q] \\
&= (q+1)(2m-3) + m^2 - 3m + 2 + 2q \\
&= (q+1)(2m-2) + (m^2 - 2m - 2 + 2q) + (3 - (q+m)) \\
&< (q+1)(2m-2) + (m^2 - 2m - 2 + 2q).
\end{aligned}$$

Pour la deuxième inégalité, remarquer que la fonction $x \mapsto (q+1)x + \frac{x^2}{4}$ est croissante sur $[-2m; 2m-3]$.

De même, on dresse le Tableau 2.4 des couples (a_1, a_2) avec $a_1 \leq -2m+2$. Les nombres de points sont classés par ordre croissant et ici aussi une variété abélienne avec (a_1, a_2) ne figurant pas dans le tableau a un nombre de points strictement supérieur aux valeurs du tableau. En effet, si $-2m+2 < a_1 \leq 2m$ on a :

a_1	a_2	Type	Nb de pts
$-2m$	m^2+2q	$[-m,-m]$	$(q+1-m)^2$
$-2m+1$	$m^2-m-1+2q$	$[-m+\frac{1+\sqrt{5}}{2},-m+\frac{1-\sqrt{5}}{2}]$	$(q+1-m+\frac{1+\sqrt{5}}{2})(q+1-m+\frac{1-\sqrt{5}}{2})$
	m^2-m+2q	$[-m,-m+1]$	$(q+1-m)(q+2-m)$
$-2m+2$	$m^2-2m-2+2q$	$[-m+1+\sqrt{3},-m+1-\sqrt{3}]$	$(q+2-m+\sqrt{3})(q+2-m-\sqrt{3})$
	$m^2-2m-1+2q$	$[-m+1+\sqrt{2},-m+1-\sqrt{2}]$	$(q+2-m+\sqrt{2})(q+2-m-\sqrt{2})$
	$m^2-2m+2q$	$[-m,-m+2]$	$(q+1-m)(q+3-m)$
	$m^2-2m+1+2q$	$[-m+1,-m+1]$	$(q+2-m)^2$

TABLE 2.4 – Couples (a_1,a_2) minimisant le nombre de points de A

$$\begin{aligned}
(q+1)a_1+a_2 &\geq (q+1)a_1+2|a_1|\sqrt{q}-2q\\
&\geq (q+1)(-2m+3)+2(2m-3)\sqrt{q}-2q\\
&= (q+1)(-2m+2)+2(2m-3)\sqrt{q}-q+1\\
&= (q+1)(-2m+2)+(m^2-2m+1+2q)-(m^2-2m+1+2q)+2(2m-3)\sqrt{q}-q+1\\
&= (q+1)(-2m+2)+(m^2-2m+1+2q)-(m-1)^2+4(m-1)\sqrt{q}-4q+q+2\sqrt{q}+1\\
&= (q+1)(-2m+2)+(m^2-2m+1+2q)-(m-1-2\sqrt{q})^2+(\sqrt{q}+1)^2\\
&> (q+1)(-2m+2)+(m^2-2m+1+2q).
\end{aligned}$$

Pour la deuxième inégalité, remarquer que la fonction $x\mapsto(q+1)x+2|x|\sqrt{q}$ est croissante sur $[-2m+3;2m]$.

Pour connaître $J_q(2)$ et $j_q(2)$ il est souvent suffisant de déterminer dans les Tableaux 2.3 et 2.4 quelle est la ligne la plus haute correspondant au polynôme caractéristique d'une jacobienne.

Rappelons d'abord la définition suivante introduite par Serre : une puissance impaire q d'un nombre premier p est *spéciale* si l'une des conditions suivantes est vérifiée (on pose $m=[2\sqrt{q}]$) :

1. p divise m,
2. il existe $x\in\mathbb{Z}$ tel que $q=x^2+1$,
3. il existe $x\in\mathbb{Z}$ tel que $q=x^2+x+1$,
4. il existe $x\in\mathbb{Z}$ tel que $q=x^2+x+2$.

Dans [29], Serre affirme que si q est premier, seules les conditions (2) et (3) sont possibles ; lorsque q est non premier, la condition (2) est impossible, la condition (3) est possible seulement si $q=7^3$ et la condition (4) est possible seulement si $q=2^3$, 2^5 ou 2^{13}. De plus, on vérifie que les conditions (2), (3) et (4) sont respectivement équivalentes à $m^2-4q=-4$, -3 et -7 (pour plus de détails, voir [14]).

Proposition 2.3.2.

a) Si q est un carré, alors $J_q(2)$ vaut

- $(q+1+m)^2$ *si* $q\neq 4,9$
- 55 *si* $q=4$
- 225 *si* $q=9$.

b) Si q n'est pas un carré, alors $J_q(2)$ vaut

- $(q+1+m)^2$ *si q n'est pas spécial*

- $(q+1+m+\frac{-1+\sqrt{5}}{2})(q+1+m+\frac{-1-\sqrt{5}}{2})$ *si* q *est spécial et* $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$
- $(q+m)^2$ *if* q *est spécial,* $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$ *et* $p \neq 2$ *ou* $p|m$
- $(q+1+m)(q-1+m)$ *sinon.*

Démonstration. **a) Si q est un carré.**
• Si $q \neq 4, 9$, $N_q(2)$ atteint la borne de Serre-Weil (voir [29]) et par conséquent il existe une courbe de type $[m, m]$.

• Si $q = 4$, on a $m = 4$. Montrons d'abord que $J_4(2) \leq 55$. Toute courbe de genre 2 sur $\mathbb{F}_q$ est hyperelliptique et a donc un nombre de points qui est au plus égal à $2(q+1) = 10$. On doit donc avoir $a_1 \leq 10 - (q+1) = 5$.

Si $a_1 = 5$, par (2.9) on a $a_2 \leq 14$. On vérifie qu'une variété abélienne sur $\mathbb{F}_4$ avec $(a_1, a_2) = (5, 14)$ est de type $[3, 2]$ et ne peut pas être une jacobienne. On en déduit que $a_2 \leq 13$ et qu'une jacobienne sur $\mathbb{F}_4$ avec $a_1 = 5$ a au plus $q^2 + 1 + 5(q+1) + 13 = 55$ points.

Si $a_1 < 5$, on a

$$\begin{aligned} q^2 + 1 + (q+1)a_1 + a_2 &\leq q^2 + 1 + (q+1)a_1 + \frac{{a_1}^2}{4} + 2q \\ &= 25 + 5a_1 + \frac{{a_1}^2}{4} \\ &\leq 25 + 5 \times 4 + \frac{4^2}{4} \\ &= 49 \end{aligned}$$

(pour la troisième ligne, remarquer que la fonction $x \mapsto 5x + \frac{x^2}{4}$ est croissante sur $[-8; 4]$ et $a_1 \geq -8$). Donc toute surface abélienne sur $\mathbb{F}_4$ avec $a_1 < 5$ possède moins de 55 points, et $J_4(2) \leq 55$.

Reste à montrer que $J_4(2) \geq 55$. On vérifie qu'une variété abélienne sur $\mathbb{F}_4$ avec $(a_1, a_2) = (5, 13)$ est de type $\left[\frac{5+\sqrt{5}}{2}, \frac{5-\sqrt{5}}{2}\right]$. C'est bien le type d'une certaine jacobienne. Celle-ci aura $q^2 + 1 + 5(q+1) + 13 = 55$ points.

• Si $q = 9$, on a $m = 6$. Comme $2(q+1) = 20$, on doit avoir $a_1 \leq 20 - (q+1) = 10 = 2m - 2$. La ligne la plus haute avec $a_1 = 2m - 2$ du Tableau 2.3 correspond au type $[m-1, m-1]$; celui-ci est bien le type d'une certaine jacobienne. Cette jacobienne aura $(q+m)^2 = 225$ points.

b) Si q n'est pas un carré.

Cette partie de la preuve se déduit directement des résultats de Serre. En effet, il a prouvé dans [30] les faits suivants :

• Il existe une courbe de type $[m, m]$ si et seulement si q n'est pas spécial.

• Une surface abélienne de type $[m, m-1]$ n'est jamais une jacobienne.

• Si q est spécial, il existe une courbe de type $[m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}]$ si et seulement si $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$. On notera que $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$ est équivalent à $m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$, donc la nécessité de cette condition est claire.

• Si q est spécial, $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$ et $p \neq 2$ ou $p|m$, il existe une courbe de type $[m-1, m-1]$.

• Si q est spécial, $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$, $p = 2$ et $p \not| m$, c'est-à-dire $q = 2^5$ ou 2^{13} (pour $q = 2^3$, on a $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$), il existe une courbe de type $[m, m-2]$.

Pour conclure, on remarque que pour $q = 2^5$ et 2^{13}, il n'existe pas de surface abélienne de type $[m-1, m-1]$ (voir Section 1.2.2). □

Dans la preuve de la proposition suivante, nous utiliserons quelques fois le fait que pour toute courbe sur $\mathbb{F}_q$ de genre 2 et de polynôme caractéristique associé à (a_1, a_2) il existe une autre courbe (sa *twistée quadratique*) de polynôme caractéristique associé à $(-a_1, a_2)$ afin de nous ramener à la preuve de la Proposition 2.3.2.

Proposition 2.3.3.

a) Si q est un carré, alors $j_q(2)$ vaut

- $(q+1-m)^2$ *si* $q \neq 4, 9$
- 5 *si* $q = 4$
- 25 *si* $q = 9$.

b) Si q n'est pas un carré, alors $j_q(2)$ vaut

- $(q+1-m)^2$ *si q n'est pas spécial*
- $(q+1-m+\frac{1+\sqrt{5}}{2})(q+1-m+\frac{1-\sqrt{5}}{2})$ *si q est spécial et* $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$
- $(q+2-m-\sqrt{2})(q+2-m+\sqrt{2})$ *si q est spécial et* $\sqrt{2}-1 \leq \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$
- $(q+1-m)(q+3-m)$ *si q est spécial,* $\{2\sqrt{q}\} < \sqrt{2}-1$, $p \not| m$ *et* $q \neq 7^3$
- $(q+2-m)^2$ *sinon.*

Démonstration. **a) Si q est un carré.**

• Si $q \neq 4, 9$, on a vu qu'il existe une courbe de type $[m, m]$; sa twistée quadratique est de type $[-m, -m]$.

• Si $q = 4$, on a $m = 4$. Montrons d'abord que $j_4(2) \geq 5$. On a $a_1 \geq -5$ puisque la twistée quadratique d'une courbe avec $a_1 < -5$ aurait $a_1 > 5$ et nous avons vu que cela est impossible.

Si $a_1 = -5$, par (2.9) on a $a_2 \geq 12$. On vérifie qu'une variété abélienne sur $\mathbb{F}_4$ avec $(a_1, a_2) = (-5, 12)$ est de type $[-4, 1]$ et ne peut pas être une jacobienne. On en déduit que $a_2 \geq 13$ et qu'une jacobienne sur $\mathbb{F}_4$ avec $a_1 = -5$ a au plus $q^2 + 1 - 5(q+1) + 13 = 5$ points.

Si $a_1 > -5$, on a

$$\begin{aligned} q^2 + 1 + (q+1)a_1 + a_2 &\geq q^2 + 1(q+1)a_1 + 2|a_1|\sqrt{q} - 2q \\ &= 9 + 5a_1 + 4|a_1| \\ &\geq 9 + 5 \times (-4) + 4 \times 4 \\ &= 5 \end{aligned}$$

(pour la troisième ligne, remarquer que la fonction $x \mapsto 5x + 4|x|$ est croissante sur $[-4, 8]$). Donc toute surface abélienne sur $\mathbb{F}_4$ avec $a_1 > -5$ possède plus de 5 points, et $j_4(2) \geq 5$.

Reste à montrer que $j_4(2) \leq 5$. Il existe une courbe avec $(a_1, a_2) = (-5, 13)$: la twistée quadratique de la courbe avec $(a_1, a_2) = (5, 13)$ de la preuve de la Proposition 2.3.2. Sa jacobienne a $q^2 + 1 - 5(q+1) + 13 = 5$ points.

• Si $q = 9$, on a $m = 6$, et le même argument que dans l'étape précédente nous montre que $a_1 \geq -2m + 2$. On regarde les lignes du Tableau 2.4 avec $a_1 = -2m + 2$. Les deux premières peuvent être ignorées puisque $\{2\sqrt{q}\} = 0$ est inférieur à $\sqrt{3} - 1$ et $\sqrt{2} - 1$. On vérifie en fait que parmi ces lignes seul le type $[-m+1, -m+1]$ est celui d'une courbe.

b) Si q n'est pas un carré.

En utilisant l'existence des twistées quadratiques et la preuve de la Proposition 2.3.2, on obtient :

• Il existe une courbe de type $[-m, -m]$ si et seulement si q n'est pas spécial.

• Si q est spécial, il existe une courbe de type $[-m + \frac{1-\sqrt{5}}{2}, -m + \frac{1+\sqrt{5}}{2}]$ si et seulement si $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$.

• Une surface abélienne de type $[-m, -m+1]$ n'est jamais une jacobienne.

Dans le reste de la preuve, on suppose que q est spécial et que $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$.

• L'existence d'une surface abélienne de type $[-m+1+\sqrt{3}, -m+1-\sqrt{3}]$ nécessite $m-1+\sqrt{3} \leq 2\sqrt{q}$ c'est-à-dire $\{2\sqrt{q}\} \geq \sqrt{3}-1$. Ceci est impossible puisque $\frac{\sqrt{5}-1}{2} < \sqrt{3}-1$.

• L'existence d'une surface abélienne de type $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$ nécessite $\{2\sqrt{q}\} \geq \sqrt{2}-1$.

Supposons que cette condition est satisfaite. En utilisant le même genre d'arguments que ceux utilisés par Serre dans [30], nous allons montrer qu'il existe une surface abélienne de type $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$. Si $p|m$, le résultat est vrai puisque $p \not| a_2 = m^2-2m-1+2q$. Sinon, $(m-2\sqrt{q})(m+2\sqrt{q}) = m^2-4q \in \{-3,-4,-7\}$, donc $\{2\sqrt{q}\} = 2\sqrt{q}-m = \frac{4q-m^2}{m+2\sqrt{q}} \leq \frac{7}{2m}$ et si $m \geq 9$, $\frac{7}{2m} < \sqrt{2}-1$. Reste à regarder "à la main" les puissances de premiers x^2+1, x^2+x+1 et x^2+x+2 avec $m < 9$ (donc $q < 21$). Ces dernières sont : 2, 3, 4, 5, 7, 8, 13 et 17. Pour $q = 2, 8$, on a $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$. Pour $q = 3$, on a $p|m$. Pour $q = 4, 7, 13, 17$, on a $\{2\sqrt{q}\} < \sqrt{2}-1$. Pour $q = 5$, $m = 4$ et $p = 5$ ne divise pas $a_2 = m^2-2m-1+2q = 17$. Donc le résultat est prouvé.

Enfin, on vérifie que notre surface abélienne est bien isogène à une jacobienne.

• Si $\{2\sqrt{q}\} < \sqrt{2}-1$, $p \not| m$ et $q \neq 7^3$, alors $p \not| (m-2)$.

Pour le voir, on se donne $p \neq 2$ (si $p = 2$, le résultat est trivial) et on utilise la remarque après la définition de "spécial". Si p divise $(m-2)$, alors il divise aussi $m^2-4-4q = (m+2)(m-2)-4q$. Comme $p \neq 2$, nous devons avoir $m^2-4q \in \{-3,-4\}$. Si $m^2-4q = -3$, p divise $-3-4 = -7$ donc $p = 7$; q n'est pas premier (car pour $q = 7$, $p \not| (m-2) = 5$) et nous devons donc avoir $q = 7^3$ et ce cas est exclu. Si $m^2-4q = -4$, p divise $-4-4 = -8$ donc $p = 2$ ce qui contredit notre hypothèse. Donc le résultat est prouvé.

Ceci nous montre qu'il existe des courbes elliptiques de trace m et $(m-2)$ et on vérifie que leur produit est bien isogène à une jacobienne.

• Supposons que $\{2\sqrt{q}\} < \sqrt{2}-1$ et $p|m$, ou $q = 7^3$. Si $p|m$, il n'existe pas de courbe elliptique de trace m ($q = 2$ et 3 sont exclus puisque dans ces cas $\{2\sqrt{q}\} \geq \sqrt{2}-1$). Si $q = 7^3$ (donc $(m-2) = 35$) il n'existe pas de courbe elliptique de trace $(m-2)$. Dans tous les cas, une surface abélienne de type $[-m, -m+2]$ ne peut donc pas exister.

• Si $\{2\sqrt{q}\} < \sqrt{2}-1$ et $p|m$ ou $q = 7^3$, alors il existe une courbe de type $[-m+1, -m+1]$: la twistée quadratique de la courbe de type $[m-1, m-1]$ de la preuve de la Proposition 2.3.2. □

2.4 Comparaison entre les bornes

Soit $C/\mathbb{F}_q$ une courbe algébrique, projective, lisse, absolument irréductible de genre g ; on reprend les notations de la Section 2.2. Rappelons que nous avons établi (respectivement dans la Proposition 2.2.6, le Théorème 2.2.7, le Théorème 2.2.9 et la Proposition 2.1.6) les minorations

suivantes :

$$\#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\binom{N+2g-2}{2g-1} \tag{2.10}$$

$$\#J_C(\mathbb{F}_q) \geq \binom{N+g-1}{g} - q\binom{N+g-3}{g-2} \tag{2.11}$$

$$\#J_C(\mathbb{F}_q) \geq \left[\sum_{n=0}^{g-2}\binom{N+n-1}{n} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}\right]\frac{(q-1)^2}{(g+1)(q+1)-N} \tag{2.12}$$

$$\#J_C(\mathbb{F}_q) \geq (N-2(r-s)\sqrt{q})(q+1+2\sqrt{q})^r(q+1-2\sqrt{q})^s \tag{2.13}$$

où $r = \left[\frac{g+\left[\frac{N-(q+1)}{2\sqrt{q}}\right]}{2}\right]$ et $s = \left[\frac{g-1-\left[\frac{N-(q+1)}{2\sqrt{q}}\right]}{2}\right]$.

Les graphes en fin de section nous montrent le comportement des membres de droite des inégalités ci-dessus lorsque l'on fixe q et g et que N parcourt l'intervalle $[\max(0, q+1-gm); q+1+gm]$.

Remarquons que (2.12) est toujours meilleure que la borne de Lachaud et Martin-deschamps (Théorème 2.2.8) :

$$\#J_C(\mathbb{F}_q) \geq (\sqrt{q}-1)^2\frac{q^{g-1}-1}{g}\frac{N+q-1}{q-1}.$$

En effet, si $n \in \mathbb{N}\setminus\{0\}$. On a $\binom{0+n-1}{n} = 0$ et pour $N \geq 1$,

$$\begin{aligned}\binom{N+n-1}{n} &= \frac{(N+n-1)(N+n-2)\dots(N+1)N}{n!}\\ &\geq \frac{(1+n-1)(1+n-2)\dots(1+1)N}{n!}\\ &= N\end{aligned}$$

donc la minoration $A_n \geq \binom{N+n-1}{n}$ est meilleure que $A_n \geq N$.

Si g est petit par rapport à q les bornes citées ci-dessus sont vérifiées par toute variété abélienne. Plus précisément, on peut attacher des N_k à n'importe quelle variété abélienne en posant $N_k = q^k + 1 - \sum_{i=1}^{g}(\omega_i^k + \overline{\omega_i}^k)$ et ceux-ci vont clairement satisfaire les bornes de Weil $(q^k+1-2gq^{k/2} \leq N_k \leq q^k+1+2gq^{k/2})$; si $g \leq (q-\sqrt{q})/2$ (il revient au même de dire que $q+1+2g\sqrt{q} \leq q^2+1-2gq$) on aura $q+1+2g\sqrt{q} \leq q^k+1-2gq^{k/2}$ pour tout $k>1$ et tous les N_k seront donc automatiquement supérieurs ou égaux à N.

Vu que la minoration (2.13) est généralement atteinte pour les variétés abéliennes lorsque q est un carré, nous pouvons nous attendre à ce que celle-ci soit meilleure que toutes les autres dès que $g \leq (q-\sqrt{q})/2$; c'est effectivement ce que l'on constate, la Figure 2.1 nous montre un exemple où q n'est pas un carré. On observe aussi dans la Figure 2.2 que la condition $g \leq (q-\sqrt{q})/2$ pour que (2.13) soit meilleure que les autres est loin d'être optimale ; toutefois, (2.12) devient meilleure que (2.13) quand g est "très grand" (Figure 2.3).

Supposons que pour $2 \leq i \leq g$, les B_i attachés à notre courbe soient tous nuls. Alors $q+1+2gq^{1/2} \geq N = N_g \geq q^g+1-2gq^{g/2}$, et donc

$$\begin{aligned}2g &\geq \frac{q^g-q}{q^{g/2}+q^{1/2}}\\ &= q^{g/2}-q^{1/2}\\ &\geq 2^{g/2}-2^{1/2}.\end{aligned}$$

La fonction $x \mapsto 2^{x/2} - 2x - 2^{1/2}$ est croissante sur $[8, +\infty[$ et prend une valeur positive en 9 et donc l'inégalité $2g \geq 2^{g/2} - 2^{1/2}$ ne peut être vérifiée que si $g < 9$. On en déduit qu'il n'existe pas de courbe de genre supérieur à 9 avec $B_2 = \cdots = B_g = 0$; en particulier, les bornes (2.10) et (2.11) ne sont jamais optimales pour $g \geq 9$.

La borne (2.11) peut être bonne même si $g \geq 9$ (Figures 2.5 et 2.6) ; toutefois, lorsque g est grand, la minoration (2.12) semble meilleure que (2.10) et (2.11).

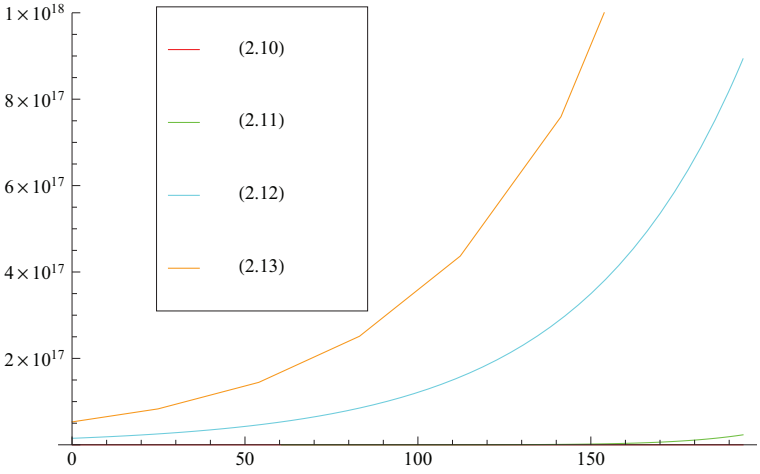

FIGURE 2.1 – $g = 10$, $q = 53$

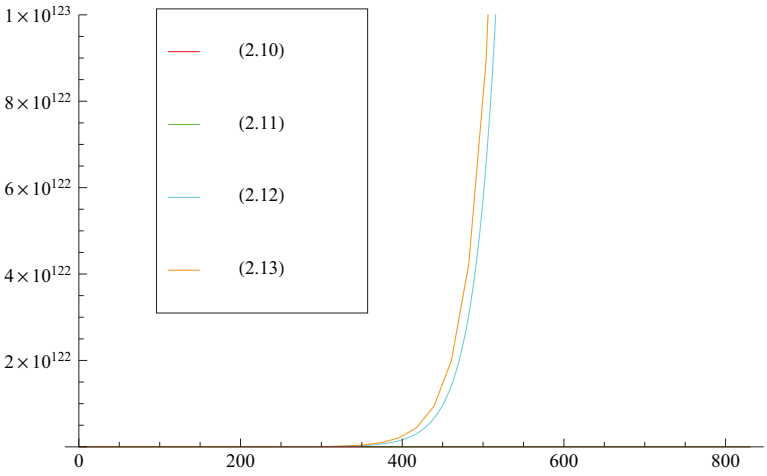

FIGURE 2.2 – $g = 80$, $q = 29$

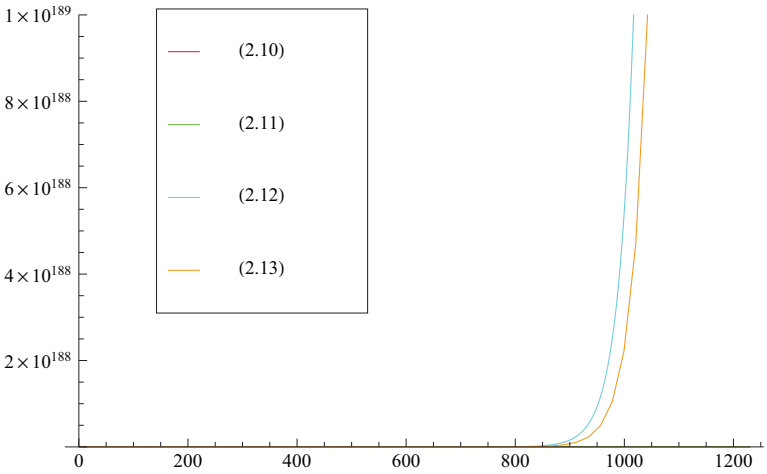

FIGURE 2.3 – $g = 120$, $q = 29$

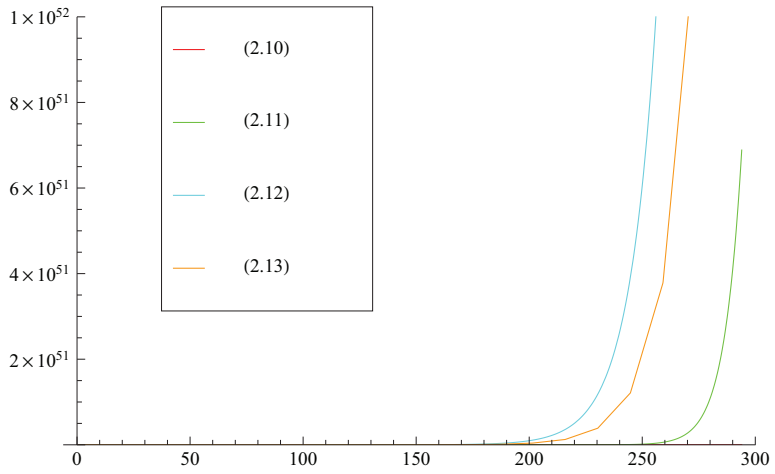

FIGURE 2.4 – $g = 40$, $q = 13$

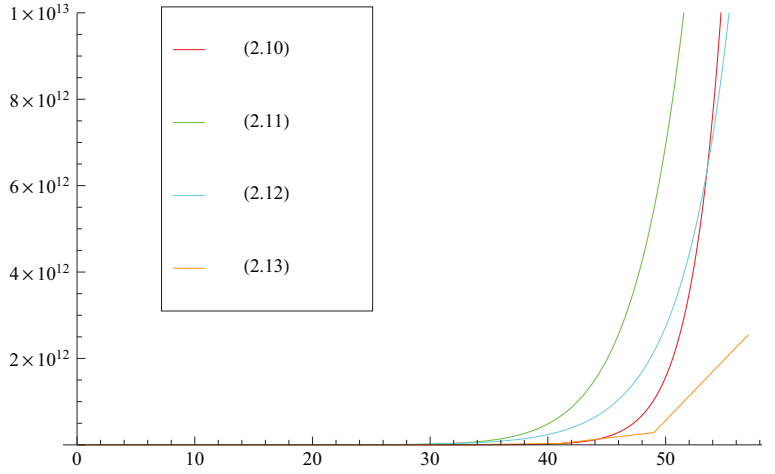

FIGURE 2.5 – $g = 13$, $q = 4$

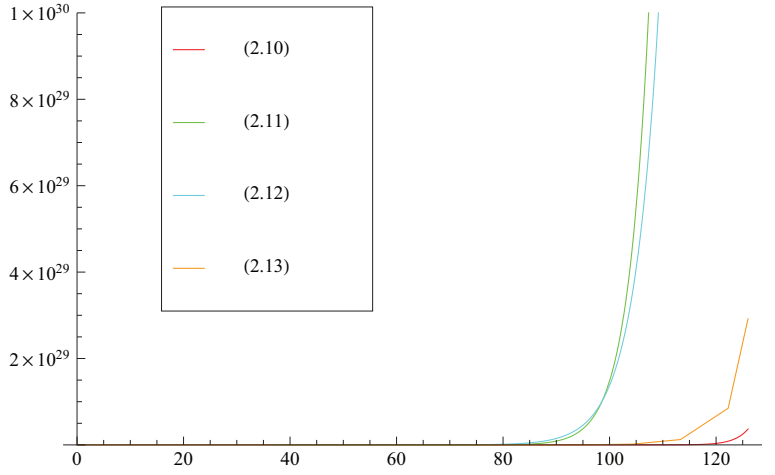

FIGURE 2.6 – $g = 30$, $q = 5$

Bibliographie

[1] Y. Aubry, S. Haloui, G. Lachaud. Number of points on abelian varieties and Jacobians over finite fields. En préparation, 2011.

[2] P. Bayer, J. González. On the Hasse-Witt invariants of modular curves. *Experimental Math.* **6** (1997), 57-76.

[3] N. Bruin, E. Flynn. Rational divisors in rational classes. *Lecture Notes in Computer Science*, Springer-Verlag **3076** (2004), 132-139.

[4] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.

[5] J. González. On the p-rank of an abelian variety and its endomorphism algebra. *Publications Math.* **42** (1998), 119-130.

[6] S. Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *J. Number Theory* **130** (2010), 2745-2752.

[7] S. Haloui, V. Singh. The characteristic polynomials of abelian varieties of dimensions 4 over finite fields. Preprint : `http://arxiv.org/abs/1101.5070`.

[8] R. Hartshorne. *Algebraic geometry*. GTM 52, Springer, 1977.

[9] M. Hindry, J. Silverman. *Diophantine geometry, an introduction*. GTM 201, Springer, 2000.

[10] T. Honda. Isogeny classes of abelian varieties over finite fields. *Journ. Math. Soc. Japan* **20** (1968), 83-95.

[11] E. Howe, E. Nart, C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourrier, Grenoble* **59** (2009), 239-289.

[12] G. Lachaud, M. Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.* **16** (1990), 329-340.

[13] K. Lauter, appendice de J.-P. Serre. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. of Algebraic Geometry* **10** (2001), no. 1, 19-36.

[14] K. Lauter, appendice de J.-P. Serre. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Math.* **134** (2002), 87-111.

[15] G. McGuire, V. Singh, A. Zaytsev. On the characteristic polynomial of Frobenius of supersingular abelian varieties of dimension up to 7 over finite fields. Preprint : `http://arxiv.org/abs/1005.3635`.

[16] D. Maisner, E. Nart, appendice de E. W. Howe. Abelian surfaces over finite fields as jacobians. *Experiment. Math.* **11** (2002), 321-337.

[17] J. S. Milne, Abelian varieties, dans *Arithmetic geometry*, G. Cornell et J. H. Silverman, Springer-Verlag, 1986.

[18] J. S. Milne, Jacobian varieties, dans *Arithmetic geometry*, G. Cornell et J. H. Silverman, Springer-Verlag, 1986.

[19] J. S. Milne. Abelian varieties. Notes de cours, v2.00. Sur `http ://www.jmilne.org/math/`.

[20] J. S. Milne, W. Waterhouse. Abelian varieties over finite fields. *Proc. Symp. Pure Math.* **20** (1971), 53-64.

[21] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Math., Oxford University Press, London, 1970.

[22] E. Nart, C. Ritzenthaler. Jacobians in isogeny classes of supersingular threefolds in characteristic 2. *Finite Fields and Their Applications* **14** (2008), 676-702.

[23] M. Perret. Number of points of Prym varieties over finite fields. *Glasgow Math. J.* **48** (2006), 275-280.

[24] H.-G. Quebbemann. Lattices from curves over finite fields. Preprint (Avril 1989).

[25] J. Riordan. *Introduction to combinatorial analysis*. Wiley, New York, 1958.

[26] H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.* **76** (1990), 351-366.

[27] J.-P. Serre, *Corps locaux*. Hermann, 1967.

[28] J.-P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris* **296** (1983), série I, 397-402.

[29] J.-P. Serre. Nombre de points des courbes algébriques sur $\mathbb{F}_q$. *Sém. de Théorie des nombres de Bordeaux* 1982/83, exp. no. 22. (Oeuvres III, no 132, 701-705).

[30] J.-P. Serre. Rational points on curves over finite fields. Notes de F. Gouvea des cours donnés à l'université de Harvard, 1985.

[31] C. Smyth. Totally positive algebraic integers of small trace. *Ann. Inst. Fourrier* **33** (1973), 285-302.

[32] R. Stanley. *Enumerative combinatorics*, Vol. 2. Cambridge University Press, Cambridge, 1999.

[33] H. Stichtenoth. *Algebraic function fields and codes*. GTM 254, Springer, 2009.

[34] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134-144.

[35] J. Tate. Classes d'isogénies de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki* **21** (1968/69), Exp. 352.

[36] M. Tsfasman, S. Vlăduţ, D. Nogin. *Algebraic geometric codes : basic notions*. Vol. 139, Math. Surveys and Monographs, A.M.S, 2007.

[37] S. Vlăduţ. An exhaustion bound for algebro-geometric "modular" codes. *Problemy Peredachi Informatsii* **23** (1987), no. 1, 28-41.

[38] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. Sc. E.N.S.* (4), **2** (1969), 521-560.

[39] E. Weiss. *Algebraic number theory*. McGraw, New-York, 1963.

[40] C.P. Xing. The characteristic polynomials of abelian varieties of dimension three and four over finite fields. *Science in China* **37** (1994), no. 3,147-150.

[41] C.P. Xing. The structure of the rational point groups of simple abelian varieties over finite fields. *Archiv der Mathematik* **63** (1994), 427-430.

[42] C.P. Xing. On supersingular abelian varieties of dimension two over finite fields. *Finite Fields and Their Applications* **2** (1996), 407-421.

Résumé : Le polynôme caractéristique d'une variété abélienne sur un corps fini est défini comme étant celui de son endomorphisme de Frobenius. La première partie de cette thèse est consacrée à l'étude des polynômes caractéristiques de variétés abéliennes de petite dimension. Nous décrivons l'ensemble des polynômes intervenant en dimension 3 et 4, le problème analogue pour les courbes elliptiques et surfaces abéliennes ayant été résolu par Deuring, Waterhouse et Rück.
Dans la deuxième partie, nous établissons des bornes supérieures et inférieures sur le nombre de points rationnels des variétés abéliennes sur les corps finis. Nous donnons ensuite des bornes inférieures spécifiques aux variétés jacobiennes. Nous déterminons aussi des formules exactes pour les nombres maximum et minimum de points rationnels sur les surfaces jacobiennes.

Mots-clés : Variétés abéliennes sur les corps finis, polynômes de Weil, jacobiennes, fonctions zêta.

Title : On the number of rational points on abelian varieties over finite fields

Abstract : The characteristic polynomial of an abelian variety over a finite field is defined to be the characteristic polynomial of its Frobenius endomorphism. The first part of this thesis is devoted to the study of the characteristic polynomials of abelian varieties of small dimension. We describe the set of polynomials which occur in dimension 3 and 4 ; the analogous problem for elliptic curves and abelian surfaces has been solved by Deuring, Waterhouse and Rück.
In the second part, we give upper and lower bounds on the number of points on abelian varieties over finite fields. Next, we give lower bounds specific to Jacobian varieties. We also determine exact formulas for the maximum and minimum number of points on Jacobian surfaces.

Keywords : Abelian varieties over finite fields, Weil polynomials, Jacobians, zeta functions.

Discipline : Mathématiques

Laboratoire : Institut de Mathématiques de Luminy (UMR 6206), Campus de Luminy, Case 907, 13288 Marseille Cedex 9, France

---