Université Paris Diderot – Paris VII
Sorbonne Paris Cité
École Doctorale de Sciences Mathématiques
de Paris Centre

THÈSE DE DOCTORAT
Discipline : Mathématiques

présentée par

Ivan BOYER

Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe

dirigée par Jean-François MESTRE

Soutenue le 24 janvier 2014 devant le jury composé de :

M. Régis de la BRETÈCHE	Université Paris 7
M. Jean-Marc COUVEIGNES	Université de Bordeaux 1
M. Pierrick GAUDRY	Loria
M. Loïc MEREL	Université Paris 7
M. Jean-François MESTRE	Université Paris 7
M. Benjamin SMITH	Inria Saclay

Rapportée par

M. Jean-Marc COUVEIGNES	Université de Bordeaux 1
M. Jaap TOP	Université de Groningen

Institut de Mathématiques de Jussieu
UP7D – Campus des Grands Moulins
Bâtiment Sophie Germain, Case 7012
75 205 Paris cedex 13

École doctorale de sciences mathématiques de Paris centre, Case 188
4 place Jussieu
75 252 Paris cedex 05

Remerciements

Le moment des remerciements est peut-être l'un des plus délicats de la rédaction de ce mémoire de thèse, d'une part car il est périlleux de n'oublier personne et d'autre part car il représente le point final de ce travail qu'il est si difficile d'interrompre. J'espère éviter les maladresses dans cet exercice peu aisé et beaucoup moins codifié que ne l'est la rédaction de mathématiques !

Tout d'abord, mes plus vifs remerciements vont tout naturellement à mon directeur de thèse, Jean-François Mestre, sans qui ce travail n'aurait pas existé. Il a été un excellent directeur de thèse, attentif à mon travail, m'aiguillant dans mes recherches, comme tout doctorant peut en rêver : j'ai passé de très longues heures en sa compagnie, apprenant de très belles mathématiques, des points de vues géométriques et des techniques algébriques et algorithmiques subtiles et efficaces. Il m'a permis, à de nombreuses reprises, de me relancer dans des calculs qui semblaient pourtant inextricables, et d'arriver aux résultats des chapitres 2 et 4. Enfin, grâce à ses conseils avisés de laisser un problème de côté « travailler tout seul », j'ai pu obtenir les nombreuses courbes du chapitre 2, deux ans après avoir arrêté la recherche dans une impasse !

Je remercie également chaleureusement Jean-Marc Couveignes et Jaap Top d'avoir rapporté ma thèse ainsi que Régis de la Bretèche, Pierrick Gaudry, Loïc Merel et Benjamin Smith pour avoir accepté de faire partie de mon jury.

Un grand merci aussi aux organisateurs des agct 13 et 14, Yves Aubry, Christophe Ritzenthaler, Alexey Zykin, et Stéphane Ballet, Marc Perret, et Alexey Zaytsev, qui m'ont si bien accueilli à Marseille et m'ont donné l'occasion et la chance d'exposer deux fois mes travaux.

Je n'oublie pas les professeurs de mathématiques qui m'ont formé, et je remercie notamment pour mon master Régis de la Bretèche et Marc Hindry qui m'a fait découvrir les courbes elliptiques et les variétés abéliennes. Je pense aussi beaucoup à mon professeur de mp*, Romain Krust qui m'a ouvert aux mathématiques et m'a conduit à l'excellence de la formation de l'Ens.

Ensuite, mes remerciements vont à mes camarades de bureau qui ont partagé ces années avec moi à travers des discussions mathématiques et autres, je pense notamment à mes voisins du bureau 7C1, Dimitri Ara qui m'a beaucoup aidé au début de ma thèse, Ngô Văn Định avec qui les discussions ont toujours été enrichissantes, Benjamin Wagener qui travaille sur les courbes elliptiques, Moheddinne Imsatfia pour m'avoir fait découvrir les coutumes tunisiennes et enfin Mounir Hajli que j'ai croisé de temps en temps avec joie. Un merci aussi à Régine Guittard pour m'avoir guidé dans le périple administratif.

Enfin, des remerciements plus personnels pour ma famille qui m'a encouragé tout au long de ces longues études aboutissant à ce travail de thèse, et m'a soutenu (et relu !) pendant la rédaction de ce mémoire lors de l'été 2013. Une pensée à mon grand-père qui n'aura malheureusement pas vu la fin de ce travail.

Résumé

Titre. Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe.

Résumé. On discute dans ce mémoire de quelques propriétés de variétés abéliennes à multiplication réelle ou complexe, et principalement de jacobiennes de courbes hyperelliptiques. On utilise, dans différentes situations, des outils communs comme les fonctions thêta ou la théorie des correspondances.

Après avoir donné, dans un premier chapitre, un rappel de ces notions que l'on utilise de façon transversale tout au long de ce mémoire, on s'intéresse à des familles de courbes à multiplication réelle par des sous-corps cyclotomiques dont l'existence a été montrée dans *Endomorphism Algebras of Jacobians* par Ellenberg. Nous donnons, à chaque fois, les constructions explicites de ces courbes, en les rapprochant de ce qui est déjà connu.

Dans le troisième chapitre, on utilise la multiplication complexe pour factoriser, sur les corps finis et en temps polynomial déterministe, des polynômes dont le groupe de Galois sur $\mathbb{Q}$ est abélien : c'est une généralisation de l'extraction de racines carrées donnée par Schoof. On construit à la fin une variété abélienne de dimension 3 dont on prouve qu'elle est à multiplication complexe, grâce à la théorie des correspondances.

Enfin, dans le dernier chapitre, on généralise un résultat de Richelot en genre 2. On donne ici toutes les courbes hyperelliptiques de genre 3 pour lesquelles il y a une $2-2-2$ isogénie entre leurs jacobiennes. On fait apparaître 4 familles parmi lesquelles 2 sont duales : on utilise la construction trigonale de Recillas pour trouver une première correspondance entre ces familles, puis on exhibe une seconde correspondance qui respecte les involutions hyperelliptiques. On fournit des caractérisations géométriques de ces deux familles.

Mots-clés. Variétés abéliennes, jacobiennes, courbes hyperelliptiques, multiplication complexe, multiplication réelle, fonction zêta, fonctions thêta, correspondances, types-CM, factorisation sur les corps finis, extensions abéliennes, polynômes cyclotomiques, sous-corps des cyclotomiques, $2-2-2$ isogénies, construction trigonale, noyaux « tractables », noyaux de « Fano ».

Abstract

Title. Abelian Varieties and Hyperelliptic Jacobians, especially with Real or Complex Multiplication.

Abstract. We discuss in this thesis some properties of abelian varieties with real or complex multiplication, especially of jacobians of hyperelliptic curves. We use, in different contexts, common tools, such as thêta functions or the theory of correspondences.

After giving, in a first chapter, a recall of some notions we use all along this thesis, we get interested in families of curves with real multiplication by cyclotomic subfields. The existence of such curves has been proven in *Endomorphism Algebras of Jacobians* by Ellenberg. For each family of curves, we give explicit constructions, recalling what is already known.

In the third chapter, we use complex multiplication in order to factorise, over finite fields and in deterministic polynomial time, polynomials whose Galois group over $\mathbb{Q}$ is abelian : this is a generalisation of the extraction of square roots by Schoof. We construct, at the end of the chapter, an abelian variety of dimension 3 for which we prove it has complex multiplication, thanks to the theory of correspondences.

Finally, in the last chapter, we generalise a result of Richelot in genus 2. We give here all the hyperelliptic curves, such as there is a $2-2-2$ isogeny between their jacobians. There are four families, and two of them are duals : we use Recillas trigonal construction to find a correspondence between the curves of these families and then, we give another correspondence, which respects hyperelliptic involutions. We also give geometrical characterisations of these two families.

Keywords. Abelian varieties, jacobian, hyperelliptic curves, complex multiplication, real multiplication, zêta function, thêta functions, correspondences, CM-types, factorisation over finite fields, abelian extensions, cyclotomic polynomials, cyclotomic subfields, $2-2-2$ isogeny, trigonal construction, « tractable » kernels, « Fano » kernels.

Table des matières

Introduction

Dans le premier chapitre de ce mémoire de thèse, on introduit un certain nombre de notions dont on se sert tout au long des chapitres suivants. Outre les définitions et notions classiques sur les variétés abéliennes et les jacobiennes sur $\mathbb{C}$ ou sur les corps finis, on introduit les fonctions thêta, l'utilisation des correspondances et la théorie de la multiplication complexe.

$$\begin{array}{ccc} & \star & \\ \star & & \star \end{array}$$

Dans le deuxième chapitre, on s'intéresse aux familles de courbes à multiplication réelle dont J. Ellenberg montre l'existence dans *Endomorphism Algebras of Jacobians* [Ell 01]. Pour chaque famille, nous montrons comment construire explicitement de telles courbes sur des extensions convenables de $\mathbb{Q}$ ou lorsque le calcul est trop lourd, sur des corps finis. Plus précisément, nous obtenons

- une famille à trois paramètres de courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$,
- une famille à un paramètre de courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$
- une famille à un paramètre de courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^{(6)})$,
- deux courbes à multiplication réelle respectivement par $\mathbb{Q}(\zeta_l^{(8)})$ et $\mathbb{Q}(\zeta_l^{(10)})$.

On peut aussi se reporter au tableau final de la section 5 de ce chapitre II, un peu plus détaillé. Parmi ces familles, on s'attache à donner des exemples définis sur $\mathbb{Q}$.

Théorème. *Il existe une famille explicite et définie sur $\mathbb{Q}$, à deux paramètres, de courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$.*

Par exemple, on obtient à nouveau (*cf.* p. 26) une famille à deux paramètres de courbes hyperelliptiques de genre 2 à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$. Dans le cas $l = 7$, nous obtenons la famille à deux paramètres suivante.

Théorème. *Les courbes de genre 3, d'équations quartiques suivantes, en U et V et à deux paramètres r et t, sont à multiplication réelle par $\mathbb{Q}(\zeta_7^+)$.*

$$\begin{aligned}&-(2tr-r-t^3)(-r^3-40t^2r^3+10tr^3-80r^3t^4+80t^3r^3+32r^3t^5+16r^2t^7-56r^2t^6+64r^2t^5-30r^2t^4+\\&5r^2t^3+12rt^8-16rt^7+5rt^6+t^9)+2r(2t-1)^2(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)U+\\&r^2(2t-1)^4U^2-r(2t-1)^2U^3+r(2t-1)^2(-2r^3-6r^2t^2+12tr^3+24r^2t^3-24t^2r^3-12rt^5-24r^2t^4+\\&16t^3r^3+28rt^6-5t^8-8rt^7)V-2t^2(t^3+2r-6tr+4t^2r)^2UV-t(t^3+2r-6tr+4t^2r)(r^2-4tr^2+\\&4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)V^2-2rt(2t-1)^2(t^3+2r-6tr+4t^2r)UV^2+t(t^3+2r-6tr+\\&4t^2r)U^2V^2+2r(2t-1)^2(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)V^3+(r^2-4tr^2+4t^3r+\\&4r^2t^2-10rt^4+2t^6+4rt^5)UV^3+t^2(t^3+2r-6tr+4t^2r)^2V^4=0.\end{aligned}$$

Parmi cette famille, on exhibe l'exemple :

$$v^3(2u-1)-u(u^3+2u^2-u-1)=0,$$

qui est à multiplication complexe par $\mathbb{Q}(\zeta_7^+, i\sqrt{3})$. En utilisant une autre construction, on donne aussi deux autres familles à un et deux paramètres de telles courbes.

Théorème. *Les courbes de genre 3, données par les équations quartiques à un paramètre s,*

$$2v + u^3 + (u+1)^2 + s\Big((u^2+v)^2 - v(u+v)(2u^2 - uv + 2v)\Big) = 0,$$

et deux paramètres s et t,

$$-(s+t)^2 + 2(s+t)sv + (-s^2+3t^2-t)v^2 + (6t^2-2t-2s^2)v^3 + 2(s+t)^2u + (6t^2-2t-2s^2)uv^2 + (-s^2+3t^2-t)uv^3 - (s+t)(s-t)u^2 + (2t+2s^2-6t^2)u^2v + (t-3t^2+s^2)u^2v^2 + (s+t)(s-t)u^3 + (2t+2s^2-6t^2)u^3v + (-s^2+3t^2-t)u^4 = 0,$$

sont à multiplication réelle par $\mathbb{Q}(\zeta_7^+)$.

On donne enfin, pour les exemples définis sur $\mathbb{Q}$, la courbe quartique

$$u^3 + 2u^2v + 2u^2 - uv^3 - 2uv^2 - 2uv - 2u + v^4 + v^2 - v + 2 = 0$$

qui est à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$; c'est un exemple du résultat plus général suivant.

Théorème. *Soit $l \equiv 1 \mod 4$ un nombre premier. Il existe une courbe, définie sur $\mathbb{Q}(i)$, à multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$.*

⋆
⋆ ⋆

Dans la troisième chapitre, on généralise un résultat de J. Pila [Pil 90], en utilisant des variétés abéliennes à multiplication complexe. Pila a donné un algorithme *déterministe* permettant, pour l fixé, de calculer une racine l-ième de l'unité dans $\mathbb{F}_p$, pour $p \equiv 1 \mod l$, le tout en *temps polynomial* en $\log(p)$.

On propose ici plusieurs généralisations de ce résultat, en utilisant d'autres variétés abéliennes, notamment la courbe hyperelliptique $y^2 = x^l - 1$, qui contrairement à la courbe de Fermat $x^l + y^l = z^l$ utilisée par Pila, est simple, et à multiplication complexe par $\mathbb{Q}(\zeta_l)$. En utilisant de plus, les courbes $y^2 = x^{l^n} - 1$, pour $l = 2$ aussi, on obtient le résultat suivant.

Théorème. *Soit n un entier fixé et $p \equiv 1 \mod n$ un nombre premier. Il existe un algorithme déterministe polynomial en $\log(p)$ qui permet de calculer les racines n-ième de l'unité dans $\mathbb{F}_p$.*

En fait, en utilisant toujours la même jacobienne, on a un résultat un peu plus fort.

Théorème. *Soit n un entier fixé et p un nombre premier d'ordre impair dans $(\mathbb{Z}/l^{k_l}\mathbb{Z})^*$, pour tous les entiers premiers l divisant n, de valuation k_l. Alors, il existe un algorithme déterministe polynomial en $\log(p)$ qui factorise le polynôme cyclotomique Φ_n.*

Notons que la condition sur p est équivalente à p d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$ pour les nombres premiers l impairs divisant n et p d'ordre 1 dans $\mathbb{Z}/2^{k_2}\mathbb{Z}$.

Grâce à d'autres variétés abéliennes, on arrive à étendre le théorème précédent.

Proposition. *Soit l un entier premier fixé, $p \equiv -1 \mod l$ et $p \equiv 1 \mod 4$. Il existe un algorithme déterministe, polynomial en $\log(p)$, donnant la factorisation de Φ_l.*

De plus, par une conjecture technique que l'on peut vérifier sur l indépendamment de p, l'algorithme donné s'affranchit de la condition $p \equiv -1 \mod l$. On a vérifié cette conjecture pour $l \leqslant 1000$. De manière analogue, on a une autre conjecture pour remplacer la condition $p \equiv 1 \mod 4$ par $p \not\equiv 1 \mod 8$, que l'on a vérifiée pour $l \leqslant 100$.

Finalement, on donne un exemple de construction de variété abélienne *ad hoc* pour notre problème de factorisation.

Théorème. *Soit $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$. La courbe hyperelliptique définie par*

$$y^2 = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right)$$

est à multiplication complexe par $\mathbb{Q}(\zeta_{13}^{(4)}, i)$.

$$\begin{array}{ccc} & \star & \\ \star & & \star \end{array}$$

Dans le quatrième et dernier chapitre, on s'intéresse à une généralisation d'un résultat de Richelot en genre 2. On cherche toutes les courbes hyperelliptiques de genre 3 telles qu'il existe une $2-2-2$ isogénie entre leurs jacobiennes. On construit des correspondances entres elles, notamment en utilisant la construction trigonale de S. Recillas [Rec 74].

Plus précisément, on appelle, suivant B. Smith [Smi 08], *tractables* les noyaux engendrés par des différences de deux points et *en situation de Fano* les seuls autres noyaux possibles, que l'on introduit en 2.5. On définit les ensembles suivants.

$$\begin{aligned}
N(3) &= \Big\{X \text{ hyperelliptique de genre 3 telle qu'il existe } Y \text{ hyperelliptique de} \\
&\qquad \text{genre 3 et une } 2-2-2 \text{ isogénie} f : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)\Big\} \\
T(3) &= \Big\{X \in N(3),\ \ker f \text{ est } \textit{tractable}\Big\} \\
T'(3) &= \Big\{X \in T(3) \text{ décrite par J.-F. Mestre, dans [Mes 13]}\} \\
F(3) &= \Big\{X \in N(3),\ \ker f \text{ est } \textit{en situation de Fano}\Big\} \\
F'(3) &= \Big\{X \in F(3),\ \text{il existe une partition 4-4 des points de Weierstrass de} X \\
&\qquad \text{ayant un birapport commun.}\Big\}
\end{aligned}$$

Avec les mêmes définitions de N, T et T' en genre 2, la construction de Richelot donne $N(2) = T(2) = T'(2)$.

Notons que si X est dans l'un de ces ensembles, la courbe « duale » Y appartient elle aussi à un de ces ensembles. On parlera d'ensembles « auto-duaux » si X et Y sont dans le même ensemble.

Théorème. *En genre 3, on obtient ici les résultats suivants.*

- *L'ensemble $T'(3)$ correspond aux courbes hyperelliptiques de genre 3 telles qu'il n'existe aucune application trigonale.*
- *L'ensemble $T(3)$ correspond aux courbes hyperelliptiques de genre 3 telles qu'il existe exactement une application trigonale.*

- *$T'(3)$ et $F(3) \setminus F'(3)$ sont « auto-duaux »*
- *La construction trigonale de S. Recillas fournit une correspondance entre les ensembles $T(3) \setminus T'(3)$ et $F(3)$.*
- *Il existe une autre correspondance, respectant les involutions hyperelliptiques.*
- *Il existe des formules explicites pour passer d'une courbe de $T(3) \setminus T'(3)$ à sa duale dans $F(3)$ et réciproquement.*

Courbes et jacobiennes, variétés abéliennes, isogénies

Nous présentons dans ce chapitre un certain nombre de notions et résultats classiques. Le but recherché n'est pas l'exhaustivité, mais simplement d'exposer un ensemble, le plus cohérent possible, de notions et résultats principaux que nous utilisons dans les chapitres suivants. Il s'agit en quelque sorte d'un socle commun et transversal des outils que nous utilisons par la suite.

Sommaire

Pour une introduction aux variétés abéliennes, nous renvoyons par exemple à *Diophantine Geometry : An Introduction* de M. Hindry et J.H. Silverman [HS 00] ou encore à *Abelian Varieties* de J.S. Milne [Mil 08].

Pour un exposé détaillé des fonctions thêta, nous renvoyons aux « incontournables » *Tata lectures on theta* (I et II principalement) de D. Mumford [Mum 83, Mum 84].

Enfin, la référence que nous utilisons pour la multiplication complexe est le livre de G. Shimura et Y. Taniyama, *Abelian Varieties With Complex Multiplication and Modular Functions*, [Shi 98], dont on conserve la plupart des notations.

— 1 —
Variétés abéliennes et isogénies

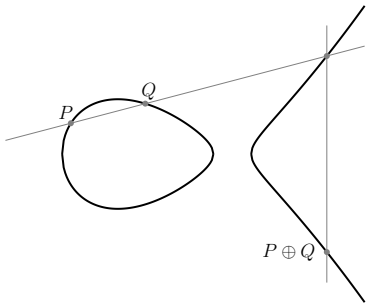
Les variétés abéliennes que l'on considère sont soit définies sur $\mathbb{C}$, soit sur un corps fini. Dans ce dernier cas, il s'agit toujours de réduction de jacobiennes, ce qui fait l'objet du chapitre II.

1.1 Variétés abéliennes

Définition 1.1. *On appelle variété abélienne une variété projective lisse qui est aussi un groupe algébrique.*

On peut ainsi représenter une variété abélienne par un ensemble d'équations définissant la variété ainsi que des équations représentant la loi de groupe. C'est cette représentation générale que Pila [Pil 90] considère pour son algorithme de comptage de points rationnels (sur les corps finis) que l'on rappelle dans le théorème 0.3 du chapitre III. L'exemple le plus classique consiste en les courbes elliptiques, courbes de genre 1 avec un point fixé, dont la loi de groupe est représentée dans la figure I.1.

Figure I.1 Exemple de loi de groupe sur une courbe elliptique



Réseaux dans $\mathbb{C}^g$, formes de Riemann. Les variétés abéliennes sur $\mathbb{C}$ sont les tores $\mathbb{C}^g/\Lambda$ tels qu'il existe une forme de Riemann sur Λ.

Proposition–Définition 1.2. *Soit H une forme hermitienne sur $\mathbb{C}^g$ et $\Lambda \subset \mathbb{C}^g$ un réseau. On dit que H est forme de Riemann par rapport à Λ si elle est définie positive et prend des valeurs entières sur Λ. Les tores complexes $\mathbb{C}^g/\Lambda$ pour lesquels il existe une forme de Riemann sont les variétés abéliennes complexes.*

Le fait que l'on ait une variété projective peut se voir par les fonctions thêta, dont on donne quelques rappels dans la section suivante.

Exemple 1.3. Pour $g = 1$, si l'on note $\mathbb{Z} + \omega\mathbb{Z}$ un réseau de $\mathbb{C}$ alors,

$$H(z, w) = \frac{z\overline{w}}{\Im\omega}$$

est une forme de Riemann sur ce réseau. Ainsi, tous les tores de $\mathbb{C}$ peuvent être munis d'une structure de variété abélienne : ce sont les courbes elliptiques. En dimension supérieure, si l'on note $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ un réseau avec la partie imaginaire de Ω définie positive, alors,

$$H(z, w) = {}^t z(\Im\Omega)^{-1}\overline{w}$$

est une forme de Riemann. Ces exemples sont fondamentaux et paramétrisent les variétés abéliennes sur $\mathbb{C}$.

Définition 1.4. *On appelle demi-espace de Siegel de dimension g, que l'on note $\mathscr{H}_g$, l'ensemble des matrices complexes, symétriques, de taille $g \times g$ dont la partie imaginaire est définie positive.*

Il s'agit de la généralisation multidimensionnelle du demi-plan de Poincaré, dont la définition coïncide pour $g = 1$. On note généralement Ω un élément de $\mathscr{H}_g$ que l'on appelle matrice des périodes, en référence aux jacobiennes sur $\mathbb{C}$ que l'on introduit désormais.

Jacobiennes. Voici un exemple essentiel de variétés abéliennes.

Définition 1.5 (Diviseurs). *On appelle diviseur sur une courbe algébrique C toute somme formelle $\sum n_i P_i$, à support fini, de points de C et on définit son degré par* $\deg(D) = \sum n_i$. *On note* $\mathrm{Div}(C)$ *l'ensemble des diviseurs de C et* $\mathrm{Div}^0(C)$ *l'ensemble des diviseurs de degré 0.*

Si f est une fonction sur C on note $\mathrm{div}(f)$ *la somme formelle de ses zéros et pôles, comptés avec multiplicité. On appelle* diviseur principal *un tel diviseur et on note* $\mathrm{Pr}(C)$ *leur ensemble et* $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Pr}(C)$, *le* groupe de Picard. *Enfin, on note* $\mathrm{Pic}^0(C)$ *l'ensemble des diviseurs de degré 0 de* $\mathrm{Pic}(C)$.

Notons qu'un diviseur principal est de degré 0, et la réciproque n'est vraie qu'en genre 0. En fait, plus généralement, on a le théorème de Riemann-Roch suivant.

Définition 1.6. *On note $\mathscr{L}(D)$ l'espace vectoriel des fonctions f sur C telles que le support de* $\mathrm{div}(f) + D$ *n'ait que des coefficients positifs — on parle de diviseur effectif. On note aussi $\ell(D)$ sa dimension.*

Théorème 1.7 (Riemann-Roch). *Soit C une courbe lisse de genre g et $K_c = \mathrm{div}(\omega)$ le diviseur d'une forme différentielle ω non nulle. Alors,*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1$$

et $\deg(K_C) = 2g - 2$ *et* $\ell(K_C) = g$.

Si C est de genre 0 et $\deg(D) = 0$, $\ell(D) = 1$, ce qui montre que tous les diviseurs de degré 0 sont principaux. On en vient désormais à la notion de jacobienne.

Théorème 1.8 (Jacobienne). *Soit C une courbe algébrique lisse de genre g. Il existe une variété abélienne de dimension g, que l'on note* $\mathrm{Jac}(C)$, *et un plongement $j : C \hookrightarrow \mathrm{Jac}(C)$ tel que j, étendu linéairement à* $\mathrm{Div}(C)$, *induise un isomorphisme entre* $\mathrm{Jac}(C)$ *et* $\mathrm{Pic}^0(C)$.

Grâce au théorème de Riemann-Roch, on peut voir $\mathrm{Jac}(C)$ comme la donnée de g copies de C et d'un diviseur effectif D de degré g.

Proposition 1.9. *Soit C une courbe lisse de genre g et D_0 un diviseur effectif de degré g. Alors, pour tout diviseur D principal, il existe un diviseur D' effectif de degré g tel que $D = D' - D_0$ dans* $\mathrm{Pic}^0(C)$.

En particulier, une jacobienne d'une courbe de genre 1 est la donnée de cette courbe et d'un point de celle-ci. C'est la définition classique d'une courbe elliptique.

La proposition ci-dessus permet notamment de représenter efficacement les points de la jacobienne d'une courbe hyperelliptique. En caractéristique différente de 2, on peut la donner par une équation $y^2 = f(x)$ avec f de degré $2g + 1$ où $2g + 2$ et de discriminant non nul. Par homographie, on peut supposer que f est de degré $2g + 1$, avec donc un seul point à l'infini que l'on note O_∞.

Définition 1.10 (Représentation de Mumford). *Soit $u(x)$ et $v(x)$ des polynômes avec $\deg(v) < \deg(u) \leqslant g$ et $u(x) \mid v^2(x) - f(x)$; on représente le point de $\mathrm{Jac}(C)$*

$$\sum_{u(x_0)=0} (x_0, v(x_0)) - \deg(u(x))(O_\infty)$$

par le couple $(u(x), v(x))$. Réciproquement, pour un point

$$\sum_{i=1}^{k} (P_i) - k(O_\infty),$$

on associe $u(x) = \prod_{i=1}^{k} (x - x_{P_i})$ et $v(x)$ le polynôme interpolateur des y_{P_i} en x_{P_i}.

Sur $\mathbb{C}$, on peut faire le lien avec la notion 1.8 de jacobiennes et celle de variétés abéliennes sur $\mathbb{C}$ introduite au paragraphe précédent.

Définition 1.11. *Soit C une courbe de genre g, $\{\omega_1, \ldots, \omega_g\}$ une base de différentielles et $\{\gamma_1, \ldots, \gamma_{2g}\}$ une base de l'homologie $H_1(C, \mathbb{Z})$. On appelle matrice des périodes de C relativement à ces deux bases, la matrice*

$$\Omega = \left(\int_{\gamma_i} \omega_j \right)_{\substack{1 \leqslant i \leqslant 2g \\ 1 \leqslant j \leqslant g}}.$$

Le lien avec les variétés abéliennes sur $\mathbb{C}$ provient des relations de Riemann.

Théorème 1.12 (Relation de Riemann). *Soit $\{\gamma_1, \ldots, \gamma_{2g}\}$ une base de l'homologie $H_1(C, \mathbb{Z})$ vérifiant de plus*

$$\gamma_k \cdot \gamma_{k'} = \begin{cases} 1 & \text{si } k' = k + g \\ 0 & \text{sinon.} \end{cases}$$

Alors, pour des différentielles régulières ω et ω' on a

$$\sum_{k=1}^{g} \left(\int_{\gamma_k} \omega \int_{\gamma_{g+k}} \omega' - \int_{\gamma_k} \omega' \int_{\gamma_{g+k}} \omega \right) = 0,$$

$$i \sum_{k=1}^{g} \left(\int_{\gamma_k} \omega \overline{\int_{\gamma_{g+k}} \omega} - \overline{\int_{\gamma_k} \omega} \int_{\gamma_{g+k}} \omega \right) > 0.$$

1.2 Isogénies

Parmi les applications entre variétés abéliennes, les isogénies jouent un rôle central.

Définition 1.13 (Isogénie). *Soient A, B deux variétés abéliennes et soit $f : A \to B$ un morphisme de groupes algébriques. On dit que f est une isogénie si f est surjective et possède un noyau fini.*

Remarque 1.14. En particulier, on a nécessairement $\dim A = \dim B$. En fait, dans cette situation $f : A \to B$ est une isogénie si et seulement si f est surjective ou si et seulement si f a un noyau fini. D'autre part, en dimension 1, cela équivaut à simplement demander que le morphisme algébrique, non constant, respecte les origines.

Voyons maintenant les principaux exemples d'isogénies, dont nous nous servons par la suite.

Multiplication par n. Comme en dimension 1, les isogénies qui apparaissent naturellement sont les multiplications par un entier. En effet, la structure de groupe des variétés abéliennes permet d'itérer l'addition.

Notation 1.15 (Multiplication par n.). *On note par* $[n] : A \to A$ *l'application*

$$P \mapsto P + \cdots + P$$

où le membre de droite comporte n *termes. C'est une isogénie.*

Isogénie duale. Pour une isogénie $f : A \to B$, on peut définir naturellement une isogénie duale $\check{f} : \check{B} \to \check{A}$, et donc une isogénie de B vers A via une polarisation. On a le résultat général suivant.

Proposition 1.16. *Soient* A, B *deux variétés abéliennes et* $f : A \to B$ *une isogénie. Alors, il existe un entier* n *et une isogénie* $g = B \to A$ *telle que* $g \circ f = [n]$.

Cela permet, entre autres, de définir une relation d'équivalence sur les variétés abéliennes, en assurant la propriété de réflexivité, puis d'en déduire un théorème de décomposition.

Définition 1.17. *Soient* A, B *deux variétés abéliennes. On dit que* A *est équivalente à* B*, et on note* $A \simeq B$ *s'il existe une isogénie* $f : A \to B$.

Définition 1.18 (Simplicité). *On dit qu'une variété abélienne est* simple *si elle n'admet pas d'autres sous-variétés abéliennes qu'elle-même et* $\{0\}$.

Théorème 1.19 (Irréductibilité de Poincaré). *Soit* A *une variété abélienne et* B *une sous-variété abélienne de* A*. Alors, il existe une sous-variété abélienne* C *de* A *telle que*

$$\begin{array}{rcl} B \times C & \to & A \\ (b\,,\,c) & \mapsto & b + c \end{array}$$

est une isogénie.

Corollaire 1.20 (Décomposition en variétés abéliennes simples). *Soit* A *une variété abélienne. Il existe des variétés abéliennes simples* $A_1, \ldots, A_s$*, deux à deux non isogènes, et des entiers* $h_1, \ldots, h_s$ *tels que* A *soit isogène au produit*

$$A \simeq A_1^{h_1} \times \cdots \times A_s^{h_s}.$$

Isogénies et variétés abéliennes sur $\mathbb{C}$. Afin d'expliciter la notion d'isogénie sur les variétés abéliennes de $\mathbb{C}$, on considère deux tores complexes, munis de leur forme de Riemann, dont on note (Ω_1, Ω_2) et (Ω_1', Ω_2') leurs réseaux représentés par des matrices de $\mathscr{M}_{g,2g}(\mathbb{C})$. On désigne ces variétés abéliennes par A, respectivement A'.

Définition 1.21 (Matrices symplectiques). *On appelle matrice symplectique une matrice à coefficients entiers* $M \in \mathscr{M}_{2g}(\mathbb{Z})$ *telle que*

$${}^tMJM = J$$

où $J = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$*. On note* $\mathrm{Sp}_{2g}(\mathbb{Z})$ *l'ensemble des matrices symplectiques.*

Proposition 1.22. *Une isogénie $f : A \to B$ peut être représentée par une matrice inversible $\alpha \in \mathscr{M}_g(\mathbb{C})$ et une matrice symplectique $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ telles que*

$$\alpha(\Omega_1, \Omega_2) = (\Omega'_1, \Omega'_2)\gamma.$$

L'isogénie f est donnée simplement sur les tores par $z \mapsto \alpha z$.

Caractéristique finie et Frobenius. On considère des variétés abéliennes définies sur un corps fini $\mathbb{F}_q = \mathbb{F}_{p^n}$, sur lequel on a l'automorphisme de Frobenius, $x \mapsto x^q$.

Proposition–Définition 1.23. *Soit A une variété abélienne définie sur $\mathbb{F}_q$. Alors, l'action du Frobenius de $\mathbb{F}_q$ sur les coordonnées induit une isogénie, que l'on appelle encore Frobenius de A, noté π_A. Le noyau de $\pi_A - \mathrm{id}$ est constitué des points de A qui sont $\mathbb{F}_q$–rationnels.*

C'est l'un des objets centraux de l'étude des variétés abéliennes sur les corps finis. Il est relié à la fonction zêta définie pour une variété V de dimension g

$$Z(V,t) = \exp\Big(\sum_{n\geqslant 1} N_n \frac{t^n}{n!}\Big)$$

où N_n est le nombre de points $\mathbb{F}_{q^n}$–rationnels de A. Pour les jacobiennes, cas qui nous intéresse, on considère la fonction zêta de la courbe, plutôt que celle de sa jacobienne. On a alors

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

Théorème 1.24 (Weil). *Dans l'écriture ci-dessus, $L(t)$ est un polynôme de degré $2g$, à coefficients entiers vérifiant $q^g t^{2g} L(\frac{1}{qt}) = L(t)$ et dont les racines sont de module $\sqrt{q}$.*

Il y a une généralisation aux variétés V de genre supérieur, appelée *conjectures de Weil*, démontrées grâce aux travaux de Dwork, Grothendieck et Deligne. Le polynôme $L(t)$ est le polynôme réciproque du polynôme caractéristique du Frobenius de $\mathrm{Jac}\, C$, que l'on note encore π_C. En particulier $t^{2g} L(\frac{1}{t})$ est un polynôme annulateur de π_C.

Définition 1.25 (q–entiers de Weil). *On appelle q–entiers de Weil tout entier algébrique π tel que pour tout plongement de $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, on a $|\sigma(\pi)| = q$. On dit que deux q–entiers de Weil π et π' sont conjugués s'ils ont le même polynôme minimal sur $\mathbb{Q}$.*

Théorème 1.26 (Honda-Tate). *L'application $A \mapsto \pi_A$ induit une bijection entre les variétés abéliennes simples définies sur $\mathbb{F}_q$, à isogénie près et les q–entiers de Weil à conjugaison près.*

En particulier, la factorisation du polynôme caractéristique du Frobenius sur $\mathbb{Q}$ donne la décomposition en variétés abéliennes, suivant le théorème 1.20.

1.3 Correspondances

Le dernier exemple d'isogénie que nous donnons provient des correspondances, que nous utilisons dans les chapitres III et IV.

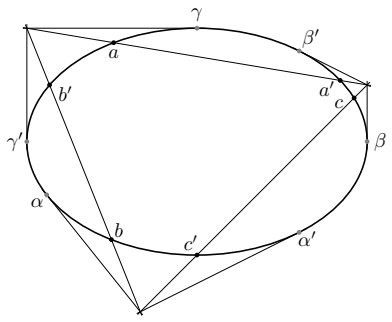
Définition 1.27 (Correspondance). *Soient C et C' deux courbes algébriques lisses. On appelle correspondance entre C et C' une courbe algébrique $\mathscr{C}$ tracée sur $C \times C'$. On définit les projections π_C et $\pi_{C'}$ de $\mathscr{C}$ sur C et C' et on dit qu'une correspondance est de type (k,l) où k et l sont les degrés de π_C et $\pi_{C'}$.*

Proposition 1.28. *Soit $\mathscr{C} \subset C \times C'$ une correspondance. Alors, on définit les isogénies* induites *par $\mathscr{C}$ par $\varphi = (\pi_{C'})_* \circ (\pi_C)^*$ isogénie de $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$, et l'isogénie duale en échangeant les rôles de C et C'.*

Exemple 1.29. Voici quelques exemples de correspondances classiques.

- Une fonction polynomiale de degré d, est une correspondance $(1,d)$ sur $\mathbb{P}^1 \times \mathbb{P}^1$.
- Les courbes hyperelliptiques donnent un exemple important de correspondances, utilisé par la suite : considérons des équations de Weierstrass $y^2 = f(x)$ et $y'^2 = g(x')$ telles qu'il existe des polynômes $C(x,x')$ et $V(x,x')$ vérifiant la relation $C(x,x') \mid V(x,x')^2 - f(x)g(x')$. Alors, l'équation $C(x,x')$, *aux abscisses*, et celle, *aux ordonnées*(⋆), $yy' = V(x,x')$ définissent une correspondance $(\deg_{x'}(C), \deg_x(C))$, respectant les involutions hyperelliptiques. On ignore si, étant donné une correspondance entre deux courbes hyperelliptiques, on peut toujours en trouver une autre de cette forme, induisant la même isogénie. Dans le chapitre IV, en 3.4.5, on a l'existence d'une telle correspondance par un calcul explicite.
- Dans la même veine, on peut citer la correspondance de Richelot–Humbert en genre 2 dont le chapitre IV en est un pendant en genre 3. On trouve la formulation moderne, esquissée ci-dessous, dans [BM 88]. On considère donc une courbe hyperelliptique H de genre 2 que l'on écrit sous la forme $y^2 = P(x)Q(x)R(x)$. On note δ le déterminant de (P,Q,R) dans la base $(1,x,x^2)$, puis on définit $U = [Q,R]$, $V = [R,P]$ et $W = [P,Q]$ où l'on note $[f,g] = f'g - fg'$. Depuis Humbert, on sait relier les polynômes P,Q,R et U,V,W : en notant a,a',b,b',c,c' les racines des premiers et $\alpha,\alpha',\beta,\beta',\gamma,\gamma'$ les racines des seconds, ils sont reliés par la conique I.2.

Figure I.2 Conique de Humbert



En considérant la courbe hyperelliptique H' d'équation $\delta y'^2 = -U(x')V(x')W(x')$, on définit la correspondance $(2,2)$ sur $H \times H'$ par

$$\begin{cases} 0 = P(x)U(x') + Q(x)V(x') \\ yy' = P(x)U(x')(x - x') \end{cases}$$

(⋆). Sans l'équation aux ordonnées, l'isogénie engendrée sur $\mathrm{Jac}(C)$ est nulle.

où l'équation sur les ordonnées se justifie par la relation

$$P(x)U(x') + Q(x)V(x') + R(x)W(x') = \delta(x - x')^2.$$

- La notion de correspondance généralise en quelque sorte celle de fonction : c'est une fonction *multivaluée*, c'est-à-dire qu'à un point on associe une somme de points et donc un diviseur, ce qui permet de construire des isogénies sur des jacobiennes qui ne proviennent pas de morphismes de courbes. Ainsi, les correspondances jouent un rôle important dans la théorie de la multiplication complexe que l'on introduit ci-dessous à la section 2.2. Elles sont par exemple utilisées dans [Mes 91], [TTV 91] ou encore dans la dernière section du chapitre III où il s'agit de l'argument central permettant de démontrer qu'une courbe est à multiplication complexe.

1.4 Variétés abéliennes duales

Sans entrer dans les détails, on mentionne la notion de variété abélienne duale et celle de polarisation qui vient avec.

Définition 1.30 (Variété abélienne duale). *Soit A et $\check{A}$ deux variétés abéliennes. Pour $\check{a} \in \check{A}$, on note $i_{\check{a}} : A \mapsto A \times \check{A}$, $a \mapsto (a, \check{a})$ et i_a de façon similaire. On dit que $\check{A}$ est une variété abélienne duale de A s'il existe un diviseur, nommé diviseur de Poincaré, $\mathscr{P} \in \mathrm{Pic}(A \times \check{A})$ tel que les applications suivantes soient des bijections.*

$$\begin{array}{ccc} \check{A} \to \mathrm{Pic}^0(A) \\ \check{a} \mapsto \quad i_{\check{a}}^*(\mathscr{P}) \end{array} \qquad \textit{et} \qquad \begin{array}{ccc} A \to \mathrm{Pic}^0(\check{A}) \\ a \mapsto \quad i_a^*(\mathscr{P}) \end{array}$$

Théorème 1.31. *Pour toute variété abélienne A il existe un unique couple $(\check{A}, \mathscr{P})$, à isomorphisme près, tel que $\check{A}$ soit la duale de A.*

La notion de polarisation peut être définie dans un cadre formel général.

Proposition–Définition 1.32 (Polarisation). *Pour $a \in A$ soit t_a la translation par a. Soit $c \in \mathrm{Pic}(A)$ tel que $K(c) := \{a \in A,\ t_a^* c = c\}$ soit fini. Alors, $\Phi_c : A \to \mathrm{Pic}(A)$ définie par $a \mapsto t_a^* c - c$ induit une isogénie de $A \to \check{A}$, que l'on appelle* polarisation. *On dit qu'elle est* principale *si c'est un isomorphisme, c'est-à-dire $K(c) = \{0\}$.*

Un exemple fondamental et éclairant de dualité et polarisation est celui des variétés abéliennes sur $\mathbb{C}$, en suivant Mumford [Mum 74]. Soit donc $A = \mathbb{C}^g/\Lambda$ une variété abélienne. On considère l'espace vectoriel $\check{V} = \mathrm{Hom}_{\overline{\mathbb{C}}}(\mathbb{C}^g, \mathbb{C})$ des formes $\mathbb{C}$–antilinéaires de $\mathbb{C}^g$. C'est un $\mathbb{C}$–espace vectoriel isomorphe à $\mathbb{C}^g$. On définit alors

$$\check{\Lambda} = \{l \in \check{V},\ \forall z \in \Lambda, \Im(l(z)) \in \mathbb{Z}\}$$

qui est un réseau de $\check{V}$. La forme $H : (\mathbb{C}^g \times \check{V})^2 \to \mathbb{C}$ définie par

$$H\Big((z_1, l_1), (z_2, l_2)\Big) = \overline{l_2(z_1)} + l_1(z_2)$$

est une forme de Riemann pour le réseau $\Lambda \times \check{\Lambda}$ qui, associée au semi-caractère $\chi(l, z) = \exp(i\pi\Im(l(z)))$ en fait un diviseur de Poincaré, assurant que $\check{V}/\check{\Lambda}$ est la variété duale de $\mathbb{C}^g/\Lambda$.

Un autre exemple fondamental de polarisation provient des jacobiennes.

Théorème 1.33. *Soit C une courbe de genre g, P_0 un point de C et $j : C \to \mathrm{Jac}(C)$, définie par $P \mapsto \mathscr{C}\ell((P)-(P_0))$. Alors, le diviseur $\theta = j(C) + \cdots + j(C)$, formé de $g-1$ facteurs, définit une polarisation principale, appelée polarisation canonique.*

Remarque 1.34 (Problème de Schottky). En dimension g, l'espace des variétés abéliennes principalement polarisées est de dimension $\frac{g(g+1)}{2}$ tandis que celui des jacobiennes est de dimension $3g-3$, ce qui diffère pour $g \geqslant 4$. Le théorème de Torelli assure que la jacobienne d'une courbe et sa polarisation canonique déterminent complètement la courbe. Le *problème de Schottky* consiste en la « réciproque », c'est-à-dire déterminer parmi les variétés abéliennes principalement polarisées, lesquelles sont des jacobiennes de courbes. Le théorème 3.7 de ce chapitre en est une réponse partielle, pour les courbes hyperelliptiques.

— 2 —
Endomorphismes et multiplication complexe

2.1 Algèbre des endomorphismes.

Définition 2.1 (Algèbre des endomorphismes). *Soit A une variété abélienne. On note* $\mathrm{End}(A)$ *le $\mathbb{Z}$-module libre de type fini des morphismes de A vers A. On note aussi* $\mathrm{End}_{\mathbb{Q}}(A)$ *le produit tensoriel*

$$\mathrm{End}_{\mathbb{Q}}(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

qui a une structure d'algèbre sur $\mathbb{Q}$.

Cette définition rend les multiplications par $[n]$ inversibles et donc toutes les isogénies aussi, grâce à la proposition 1.16. En particulier, pour une variété abélienne A simple, $\mathrm{End}_{\mathbb{Q}}(A)$ est une algèbre à division. Plus généralement, le théorème 1.20 permet d'exprimer $\mathrm{End}_{\mathbb{Q}}(A)$ en termes des algèbres à divisions des facteurs simples $\mathrm{End}_{\mathbb{Q}}(A_i)$:

$$\mathrm{End}_{\mathbb{Q}}(A) \simeq \mathscr{M}_{h_1}\Big(\mathrm{End}_{\mathbb{Q}}(A_1)\Big) \times \cdots \times \mathscr{M}_{h_s}\Big(\mathrm{End}_{\mathbb{Q}}(A_s)\Big),$$

où l'on note $\mathscr{M}_n(R)$ la $\mathbb{Q}$-algèbre des matrices de dimension n à coefficients dans R.

Soit $A = \mathbb{C}^g/\Omega$ une variété abélienne sur $\mathbb{C}$. Comme on l'a vu dans la proposition 1.22, on peut voir $\mathrm{End}(A)$ comme l'ensemble des applications linéaires de $\mathbb{C}^g$ qui stabilisent le réseau Ω.

Définition 2.2 (Représentation rationnelle et analytique). *Cette description des endomorphismes permet de donner naturellement une représentation dite* analytique *de* $\mathrm{End}_{\mathbb{Q}}(A)$ *de dimension g,*

$$\rho_{\mathbb{C}} : \mathrm{End}_{\mathbb{Q}}(A) \hookrightarrow \mathscr{M}_g(\mathbb{C}).$$

On peut aussi regarder l'action des endomorphismes sur le réseau $\Omega \in \mathscr{M}_{g,2g}(\mathbb{C})$ ce qui donne une représentation dite rationnelle *de* $\mathrm{End}_{\mathbb{Q}}(A)$ *de dimension $2g$,*

$$\rho_{\mathbb{Q}} : \mathrm{End}_{\mathbb{Q}}(A) \hookrightarrow \mathscr{M}_{2g}(\mathbb{Q}).$$

2.2 Multiplication complexe

Ainsi, à partir de la dimension 2, $\mathrm{End}_{\mathbb{Q}}(A)$ peut contenir des algèbres de matrices, ce qui n'est pas vraiment la situation qui nous intéresse le plus. La proposition suivante montre que la situation de la multiplication complexe est un peu plus délicate qu'en dimension 1.

Proposition 2.3. *Soit A une variété abélienne de dimension g.*

(i) Si $R \subset \mathrm{End}_{\mathbb{Q}}(A)$ est une sous-algèbre semi-simple commutative, alors on a $[R : \mathbb{Q}] \leqslant 2g$ et s'il y a égalité, le commutant de R est R.

(ii) On suppose que $\mathrm{End}_{\mathbb{Q}}(A)$ contient un corps de degré $2g$. Alors, A est isogène à un produit d'une même variété abélienne B simple :

$$A \simeq B^h.$$

Notons qu'il est tout à fait possible que $h \neq 1$, c'est-à-dire que A ne soit pas simple. On voit en 2.4 quelles sont les conditions pour que A soit simple. C'est cette situation qui est la situation la « plus intéressante » comme le montre la remarque suivante.

Remarque 2.4 (Matrices compagnons)**.** Soit A une variété abélienne isogène à une puissance d'une même variété abélienne B, $A \simeq B^h$. Comme on l'a vu ci-dessus, $\mathrm{End}_{\mathbb{Q}}(A) \simeq \mathscr{M}_g(\mathrm{End}_{\mathbb{Q}}(B))$. Soit $P = x^h + \sum_{i=0}^{h-1} c_i x^i$ un polynôme irréductible de degré h, à coefficients dans un corps K contenu dans $\mathrm{End}_{\mathbb{Q}}(B)$. Alors, la matrice compagnon de P,

$$M_P := \begin{pmatrix} 0 & 0 & \cdot & 0 & -c_0 \\ 1 & 0 & \cdot & 0 & -c_1 \\ 0 & 1 & \cdot & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{h-1} \end{pmatrix}$$

correspond à un élément de $\mathrm{End}_{\mathbb{Q}}(A)$ qui, par le théorème de Cayley-Hamilton, possède comme polynôme minimal P. Ainsi, $\mathrm{End}_{\mathbb{Q}}(A)$ contient le corps de rupture de P, de degré h au-dessus de K. Par exemple, si A est la puissance n-ième d'une courbe elliptique, $\mathrm{End}_{\mathbb{Q}}(A)$ contient tous les corps de nombres de degré divisant g.

Définition 2.5. *Soit A une variété abélienne de dimension g. On dit que A est à multiplication complexe par une $\mathbb{Q}$-algèbre F de dimension $2g$, si $F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A)$.*

Cela revient en fait à demander l'existence d'une sous-$\mathbb{Q}$-algèbre de $\mathrm{End}_{\mathbb{Q}}(A)$ de dimension maximale. On retrouve l'idée de la dimension 1 où l'on demande que $\mathrm{End}_{\mathbb{Q}}(A)$ soit plus grand qu'à l'ordinaire.

Dans la suite, on ne considère en fait que le cas où F est un corps. En particulier, $\mathrm{End}(A)$ est un *ordre* de F. On retrouve, en dimension 1, le fait que l'anneau des endomorphismes de la courbe elliptique soit un ordre d'un corps quadratique.

Exemple 2.6 (Dimension 1)**.** Soit $E/\mathbb{F}_p$ une courbe elliptique définie sur $\mathbb{F}_p$. En caractéristique finie, on a toujours un anneau d'endomorphismes plus important que $\mathbb{Z}$ du fait de l'existence du Frobenius, π_E. Son polynôme minimal est donné par

$$t^2 - \mathrm{tr}\,\pi_E t + p,$$

et donne l'inclusion d'un corps quadratique de discriminant $\delta = (\operatorname{tr}\pi_E)^2 - 4p$ dans $\mathrm{End}_{\mathbb{Q}}(E)$. La courbe elliptique E est donc à multiplication complexe par $\mathbb{Q}(\sqrt{\delta})$ qui est de dimension 2. De plus, le théorème 1.24 de Weil affirme précisément que $|\operatorname{tr}\pi_E| \leqslant 2\sqrt{p}$, ce qui est équivalent à dire que E est un corps quadratique totalement imaginaire.

De même que dans cet exemple, en dimension 1, les corps quadratiques possibles sont totalement imaginaires, de même les corps pouvant intervenir en dimensions supérieures doivent respecter certaines conditions.

Définition 2.7. *On dit qu'un élément d'un corps de nombres F est* totalement réel*, respectivement* positif*, respectivement* imaginaire*, si ses images par tous les plongements de F dans $\mathbb{C}$ sont* réelles*, respectivement* réelles positives*, respectivement* non réelles*.*

De même, on dit que le corps est totalement réel, respectivement imaginaire, si tous ses éléments le sont.

Proposition 2.8. *Soit A une variété abélienne simple et F le centre de $\mathrm{End}_{\mathbb{Q}}(A)$. Alors, F est un corps totalement réel ou une extension quadratique totalement imaginaire d'un corps totalement réel.*

C'est le deuxième cas de la proposition qui va nous intéresser par la suite. Dans cette situation, on reprend la terminologie utilisée dans la définition 2.5, ce qui est justifié par le théorème 2.14, théorème principal de cette section.

Définition 2.9. *On dit qu'un corps F est à multiplication complexe, ou simplement un corps-CM, si F est une extension quadratique totalement imaginaire d'un corps totalement réel.*

En particulier, si une variété abélienne de dimension g est à multiplication complexe par un corps de degré $2g$ (*i.e.* la $\mathbb{Q}$-algèbre de dimension $2g$ de la définition 2.5 est un corps) alors, ce corps est à multiplication complexe. Si l'on note F_0 le sous-corps d'indice 2 de F totalement réel, alors, il existe $\zeta \in F$ tels que $-\zeta^2$ est totalement positif et $F = F_0(\zeta)$. On retrouve facilement cette situation pour tous les corps quadratiques imaginaires. Finissons ce paragraphe par une des caractérisations principales des corps-CM.

Proposition 2.10 (Caractérisation des corps-CM)**.** *Soit F un corps de nombres et ρ un automorphisme de F d'ordre 2. Soit F_0 le sous-corps de F fixé par ρ. On suppose*

$$\forall \xi \in K^*, \operatorname{Tr}_{F/\mathbb{Q}}(\xi\rho(\xi)) > 0.$$

Alors, F est un corps-CM, F_0 étant totalement réel. De plus, pour tout plongement $\tau : F \hookrightarrow \mathbb{C}$, on a $\tau\rho(\xi) = \overline{\tau(\xi)}$.

2.3 Types-CM

Soit A une variété abélienne en caractéristique 0, à multiplication complexe par un corps-CM F de degré $2g = 2\dim A$. La représentation rationnelle de A vérifie

$\rho_{\mathbb{Q}}(A) \simeq \rho_{\mathbb{C}}(A) \oplus \overline{\rho_{\mathbb{C}}(A)}$, où $\rho_{\mathbb{C}}$ est sa représentation analytique. Cette dernière, de dimension g, est la somme de g représentations irréductibles de degré 1, données par des plongements de F dans $\mathbb{C}$: Si l'on note $\varphi_1, \dots \varphi_{2g}$ les $2g$ plongements de corps de F vers $\mathbb{C}$, alors, $\rho_{\mathbb{Q}}$ est la somme directe de g de ces plongements, disons $\varphi_1, \dots, \varphi_g$, et $\overline{\rho_{\mathbb{C}}}$ la somme directe des g autres, conjugués des premiers, disons $\varphi_{g+i} = \overline{\varphi_i}$. Ceci motive la définition suivante.

Définition 2.11. *Une telle partition en deux sous-ensembles de cardinaux g des $2g$ plongements d'un* corps-CM *F dans $\mathbb{C}$ est appelée* type-CM *; le couple $(F, \{\varphi_1, \dots, \varphi_g\})$ est nommé* paire-CM*.*

On remarque que dans de telles partitions, il n'y a jamais, dans le même ensemble, deux plongements qui sont conjugués l'un de l'autre. Ceci contredirait en effet que F est un corps-CM.

On sait par ailleurs que S est équivalente à la représentation de $\mathrm{End}_{\mathbb{Q}}(A)$ par les formes différentielles invariantes. Cela peut s'avérer pratique pour calculer facilement le type-CM d'une variété abélienne, du fait de la proposition suivante.

Proposition 2.12. *On garde les même notations. Soient $\omega_1, \dots, \omega_g$ les formes différentielles de degré 1 de A. Alors, on a l'équivalence*

1. *Pour tout $\alpha \in F$ et pour tout $i \in [\![1, g]\!]$,*
$$\alpha^* \omega_i = \varphi_i(\alpha)\omega_i.$$
2. *Le type-CM de A est $\{\varphi_1, \dots, \varphi_g\}$.*

En particulier, lorsque A est la jacobienne d'une courbe hyperelliptique de genre g, on connaît des bases de différentielles, par exemple
$$\frac{\mathrm{d}x}{y}, x\frac{\mathrm{d}x}{y}, \dots, x^{g-1}\frac{\mathrm{d}x}{y},$$
ce qui permet de calculer le type-CM de A.

Exemple 2.13.

- La courbe elliptique $y^2 = x^3 + x$ est à multiplication complexe par i, engendré par l'automorphisme de degré 4, $\alpha : (x, y) \mapsto (-x, iy)$. On a les deux plongements définis par $\varphi_1 : \alpha \mapsto i$ et $\varphi_2 : \alpha \mapsto -i$ On calcule $[\alpha]^*(\frac{\mathrm{d}x}{y}) = i\frac{\mathrm{d}x}{y} = \varphi_1(\alpha)$, ce qui donne pour type-CM $(\{\varphi_1\}, \{\varphi_2\})$, seul type possible.
- La courbe hyperelliptique H d'équation $y^2 = x^5 + 1$ possède un automorphisme $\alpha : (x, y) \mapsto (\zeta_5 x, y)$ d'ordre 5, engendrant, dans $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(H)$, un corps F isomorphe à $\mathbb{Q}(\zeta_5)$. Les 4 plongements sont $\varphi_k : \alpha \mapsto \zeta_5^k$, pour $1 \leqslant k \leqslant 4$, et l'action de α sur la base de différentielles est
$$[\alpha]^*\frac{\mathrm{d}x}{y} = \zeta_5\frac{\mathrm{d}x}{y} = \varphi_1(\alpha)\frac{\mathrm{d}x}{y}$$
$$[\alpha]^*\Big(x\frac{\mathrm{d}x}{y}\Big) = \zeta_5^2 x\frac{\mathrm{d}x}{y} = \varphi_2(\alpha)x\frac{\mathrm{d}x}{y},$$
ce qui donne comme type-CM $(\{\varphi_1, \varphi_2\}, \{\varphi_3, \varphi_4\})$ et l'on vérifie que $\varphi_4 = \overline{\varphi_1}$ et $\varphi_3 = \overline{\varphi_2}$.

On développe ce dernier exemple dans la section 1 du chapitre II. Ici, les calculs sont facilités par le fait que les endomorphismes de la jacobienne proviennent directement de la courbe hyperelliptique. Cela n'est bien évidemment pas toujours le cas. Néanmoins, on travaille souvent sur des courbes quotients où il est facile d'adapter ce genre de calculs. C'est notamment le cas dans le chapitre II, où la construction principale repose sur le quotient d'une courbe possédant beaucoup d'automorphismes. On voit lors de la section 3.2 du chapitre III comment déterminer le type-CM d'un endomorphisme engendré par une correspondance.

Nous avons vu des conditions nécessaires pour qu'un corps F et la moitié des plongements de F dans $\mathbb{C}$, soit le type-CM d'une variété abélienne à multiplication complexe par F. En fait, elles sont suffisantes comme le montre la construction faite par G. Shimura et Y. Taniyama dans [Shi 98]. On énonce ici simplement ce théorème. On reprend la construction explicite, dans le chapitre III, quand on construit , dans la section 3, une variété abélienne dont on a imposé la multiplication complexe et le type-CM.

Théorème 2.14. *Soit un couple $\mathscr{T} := (F, \{\varphi_1, \ldots, \varphi_g\})$ où F est un corps de degré $2g$ et les φ_i sont g plongements de F dans $\mathbb{C}$. Alors, il existe une variété abélienne de type-CM, $\mathscr{T}$, si et seulement si (1) F est une extension quadratique totalement imaginaire d'un corps totalement réel et (2) les φ_i sont deux à deux non conjugués.*

Enfin, le type-CM d'une variété abélienne à multiplication complexe détermine la variété abélienne à isogénie près.

Proposition 2.15. *Deux variétés abéliennes à multiplication complexe sont isogènes si et seulement si elles ont le même type-CM.*

2.4 Types-CM primitifs et réflex

Comme on l'a vu dans la proposition 2.3, une variété abélienne à multiplication complexe n'est pas nécessairement simple ; elle peut être le produit d'une même sous-variété abélienne simple.

Définition 2.16. *On dit qu'un type-CM est primitif si la variété abélienne à multiplication complexe par ce type-CM est simple.*

Dans [Shi 98], on trouve deux caractérisations de types-CM primitifs.

Proposition 2.17. *Soit $(F, \{\varphi_i\})$ un type-CM, F_0 le sous-corps de F d'indice 2 totalement réel, et soient $\eta \in F$ totalement positif et $\zeta \in F$ tels que $-\zeta^2 = \eta$ et $\Im(\varphi_i(\zeta)) > 0$. Alors, ce type-CM est primitif si et seulement si*

(i) $F = F_0(\zeta) = \mathbb{Q}(\zeta)$ et

(ii) tout conjugué ζ' de ζ, distinct de ζ vérifie $\frac{\zeta'}{\zeta}$ n'est pas totalement positif.

Si on applique cette proposition en dimension 1, on a un seul conjugué ζ' de ζ et le quotient vaut -1, ce qui veut bien dire que le type-CM est primitif : c'est heureux, puisque les variétés abéliennes de dimension 1 sont simples.

La deuxième caractérisation est plus facile à vérifier et utilise la théorie de Galois. Pour cela, commençons par noter L une extension galoisienne de $\mathbb{Q}$ de groupe de

Galois G contenant le corps F du type-CM. On note $\rho \in G$ l'élément qui agit par la conjugaison complexe et on désigne par $S \subset G$ l'ensemble des éléments de G qui induisent un des plongements φ_i, de F dans $\mathbb{C}$, constituant le type-CM.

Proposition 2.18. *Le type-CM $(F, \{\varphi_i\})$, L, G, ρ et S étant définis ci-dessus, on a l'équivalence entre les propriétés suivantes.*

(i) Le type-CM $(F, \{\varphi_i\})$ est primitif.

(ii) Le groupe

$$\Big\{\gamma \in G, \quad \gamma S = S\Big\}$$

est précisément le sous-groupe de G correspondant à F.

Avec ces mêmes notations, cela permet de définir le réflex d'un type-CM.

Proposition–Définition 2.19 (Réflex). *Les notations de la proposition précédente 2.18 sont conservées. On note aussi*

$$S^* = \Big\{\sigma^{-1}, \quad \sigma \in S\Big\}$$
$$H^* = \Big\{\gamma \quad \gamma \in G, \gamma S^* = S^*\Big\}.$$

Alors, le sous-corps F^* de L correspondant à H^* et tous les plongements ψ_i de F^* dans $\mathbb{C}$ forment un type-CM primitif, indépendant de L que l'on appelle le réflex de $(F, \{\varphi_i\})$.

Ainsi, le réflex est toujours primitif et donc le réflex du réflex n'est pas forcément le type-CM du départ. En fait, cela est vérifié si et seulement si on part d'un type-CM primitif.

Remarque 2.20 (Extensions abéliennes). Dans le chapitre III, on ne considère que des extensions abéliennes de corps. Dans ce cas, le réflex d'un type-CM primitif $(F, \{\varphi_i\})$ est simplement $(F, \{\varphi_i^{-1}\})$ et la proposition 2.18 est simplifiée puisqu'il suffit de vérifier qu'aucun élément du groupe de Galois de F, hormis l'identité, ne stabilise les g plongements de F vers $\mathbb{C}$ du type-CM.

— 3 —
Fonctions thêta

3.1 Définitions—notations

On rappelle ici brièvement des notions de base sur les fonctions thêta, principalement pour fixer les notations. Pour de plus amples détails, nous renvoyons aux *Tata lectures* de Mumford [Mum 83, Mum 84], dont nous conservons les notations. De plus, afin d'alléger celles-ci, on sous-entend le produit scalaire entre deux vecteurs ainsi que le produit matrice-vecteur. Enfin, sauf ambiguïté, on note sans distinction particulière les scalaires et les vecteurs de $\mathbb{C}^g, \mathbb{Z}^g$.

Proposition–Définition 3.1. *On appelle fonction thêta de $z \in \mathbb{C}^g$ et $\Omega \in \mathscr{H}_g$, demi-espace de Siegel, la fonction holomorphe sur $\mathbb{C}^g \times \mathscr{H}_g$ suivante.*

$$\boldsymbol{\vartheta}(z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp(i\pi {}^t n\Omega n + 2i\pi {}^t nz).$$

En effet, cette série converge absolument et uniformément sur $\mathbb{C}^g$ et $\mathscr{H}_g$.

Comme en dimension 1, les fonctions thêta possèdent des propriétés de périodicité et de quasi-périodicité qui sont rappelées dans la proposition suivante.

Proposition 3.2. *Pour tout vecteur $m \in \mathbb{Z}^g$,*

$$\begin{aligned}\boldsymbol{\vartheta}(z+m,\Omega) &= \boldsymbol{\vartheta}(z,\Omega)\\ \boldsymbol{\vartheta}(z+\Omega m,\Omega) &= \exp(-i\pi {}^t m\Omega m - 2i\pi {}^t mz)\boldsymbol{\vartheta}(z,\Omega).\end{aligned}$$

On introduit ensuite un outil essentiel dans l'étude des variétés abéliennes, les *fonctions thêta avec caractéristiques* $\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right] \in \mathscr{M}_{2,g}(\mathbb{Q})$.

$$\begin{aligned}\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](z,\Omega) &= \exp\Big(i\pi {}^t\eta'\Omega\eta' + 2i\pi {}^t\eta'(z+\eta'')\Big)\boldsymbol{\vartheta}(\Omega\eta'+\eta''+z,\Omega)\\ &= \sum_{n\in\mathbb{Z}^g}\exp\Big(i\pi {}^t(\eta'+n)\Omega(\eta'+n) + 2i\pi {}^t(n+\eta')(z+\eta'')\Big).\end{aligned}$$

La fonction thêta de départ est $\boldsymbol{\vartheta} = \boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right]$. Le dénominateur des caractéristiques correspond à un poids si bien que les ensembles de fonctions de *poids* l,

$$\begin{aligned}&\left\{\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'_i\\ \frac{l}{0}\end{smallmatrix}\right](l\cdot, l\Omega),\quad 0\leqslant \eta'_i < l, 1\leqslant i\leqslant g\right\} \text{ et}\\ &\left\{\boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \eta''_i\\ \frac{}{l}\end{smallmatrix}\right](\cdot, \frac{1}{l}\Omega),\quad 0\leqslant \eta''_i < l, 1\leqslant i\leqslant g\right\},\end{aligned}$$

forment des bases des fonctions holomorphes vérifiant les conditions de périodicité :

$$\forall m\in\mathbb{Z}^g,\ \begin{cases} f(z+m) = f(z)\\ f(z+\Omega m) = \exp(-i\pi l\,{}^t m\Omega m - 2i\pi l\,{}^t zm)f(z).\end{cases}$$

Ce sont ces fonctions qui permettent d'injecter les tores complexes issus du demi-espace de Siegel dans le plan projectif et donc de décrire les variétés abéliennes.

3.2 Thêta constantes et courbes hyperelliptiques

En dimension 1 les variétés abéliennes sont les courbes elliptiques et en dimension 2, ce sont soit le produit de deux courbes elliptiques, soit la jacobienne d'une courbe hyperelliptique. À partir de la dimension 3, on trouve d'autres types de variétés abéliennes ; pour $g \geqslant 4$, l'espace des variétés abéliennes est de dimension $\frac{g(g+1)}{2}$ alors que celui des jacobiennes n'est que de dimension $3g-3$ et celui des jacobiennes de courbes hyperelliptiques est seulement de dimension $2g-1$.

Comme on l'a rappelé plus haut, le problème de Schottky consiste précisément à caractériser les jacobiennes parmi les variétés abéliennes. Mumford détaille, dans [Mum 84], une caractérisation simple et élégante des jacobiennes de courbes hyperelliptiques (⋆). Celle-ci repose sur les *thêta constantes* qui sont des évaluations en 0 des thêta avec caractéristiques. On choisit le plus petit poids possible, 2, et on parle alors de demi-caractéristiques.

(⋆). *cf.* théorème 3.7 de ce chapitre.

Définition 3.3 (Demi-caractéristiques et thêta constantes). *On considère les* demi-caractéristiques $\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right] \in \mathscr{M}_{2,g}(\frac{1}{2}\mathbb{Z}/\mathbb{Z})$ *où* η' *et* η'' *sont des vecteurs lignes. On appelle* thêta constantes *les évaluations de ces demi-caractéristiques en* 0 *:*

$$\begin{aligned}\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](0,\Omega) &= \exp(i\pi\,{}^t\eta'\Omega\eta' + 2i\pi\,{}^t\eta'\eta'')\boldsymbol{\vartheta}(\Omega\eta'+\eta'',\Omega)\\ &= \sum_{n\in\mathbb{Z}^g}\exp\Big(i\pi\,{}^t(n+\eta')\Omega(n+\eta') + 2i\pi\,{}^t(n+\eta')\eta''\Big).\end{aligned}$$

En partant de la relation

$$\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](-z,\Omega) = (-1)^{4\,{}^t\eta'\eta''}\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](z,\Omega),$$

on dit qu'une demi-caractéristique est paire [(◇)] *si* $4\,{}^t\eta'\eta''$ *est pair,* impaire *sinon.*

En particulier, en prenant $z = 0$ et une demi-caractéristique impaire, on en déduit que les thêta constantes impaires sont nulles.

Remarque 3.4. On peut dénombrer les demi-caractéristiques paires et impaires. Il y a 2^{2g} demi-caractéristiques. Celles paires s'obtiennent comme réunion de noyaux de formes linéaires, de cardinaux 2^{g-1} pour $\eta' \neq 0$ et 2^g sinon. On a donc $(2^g-1)2^{g-1}+2^g$ soit $2^{g-1}(2^g+1)$ demi-caractéristiques paires et $2^{g-1}(2^g-1)$ impaires.

La condition nécessaire et suffisante énoncée dans Mumford [Mum 84], porte sur la nullité d'un certain nombre de thêta constantes paires. Par exemple, en genre 3, cela se réduit à une unique thêta constante paire nulle. Cela fait l'objet du théorème 3.7 ci-après.

Formule de Thomae. La formule de Thomae permet de faire le lien entre la définition analytique des fonctions thêta et son utilisation algébrique dans notre situation, en ce sens qu'elle permet d'exprimer les thêta constantes de la jacobienne d'une courbe hyperelliptique en fonction de ses points de Weierstrass.

Il y a beaucoup de choix non canoniques pour faire ce lien. On fait les mêmes que dans Mumford [Mum 83, Mum 84] dans un souci de cohérence et afin de simplifier le calcul des signes notamment. Commençons par considérer une courbe hyperelliptique de genre g que l'on choisit d'écrire sans point à l'infini,

$$y^2 = \prod_{i=1}^{2g+2}(x-x_i)$$

où les x_i sont des réels 2 à 2 distincts. On peut donc, sans perte de généralité, supposer que $x_1 > x_2 > \cdots > x_{2g+2}$. Quitte à réaliser une translation, on suppose de plus $x_{2g+2} > 0$. On note $\mathscr{B}_g$ l'ouvert de $\mathbb{R}^{2g+2}$ défini par ces inégalités et $B \in \mathscr{B}_g$ l'ensemble des racines $\{x_1, x_2, \ldots, x_{2g+2}\}$. Ce choix n'entre pas directement en compte dans la formule de Thomae à proprement parler, mais permet de faciliter la détermination du signe des thêta constantes.

(◇). On attire l'attention sur le fait que l'on utilise les mêmes notations que Mumford dans [Mum 83, Mum 84], où les caractéristiques utilisées sont *fractionnaires*, d'où par exemple le facteur 4 pour la définition de leur parité.

On choisit un sous-ensemble $U = \{x_1, x_3, \ldots, x_{2g+1}\} \subset B$ composé de $g+1$ racines et on reprend l'équivalence, décrite dans [Mum 84], entre un sous-ensemble de cardinal pair de B modulo son complémentaire et une demi-caractéristique $\eta_S = \begin{bmatrix} \eta'_S \\ \eta''_S \end{bmatrix}$, qui vérifie, entre autres (‡), les propriétés suivantes :

a) $\eta_{S_1 \Delta S_2} = \eta_{S_1} + \eta_{S_2}$

b) $(-1)^{4^t \eta'_S \eta''_S} = (-1)^{\frac{|S\Delta U|-g-1}{2}}$.

On pose pour $1 \leqslant i \leqslant g+1$, le $\frac{1}{2}$ de la première ligne étant à la i-ième colonne,

$$\eta_{2i-1} = \eta_{\{2i-1,2g+2\}} = \begin{pmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \ldots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

pour $1 \leqslant i \leqslant g$

$$\eta_{2i} = \eta_{\{2i,2g+2\}} = \begin{pmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \ldots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} & 0 & \cdots & 0 \end{pmatrix},$$

et pour un ensemble S, $\eta_S = \sum_{i \in S} \eta_i$. Mumford, dans [Mum 84], établit finalement l'équivalence :

$$\begin{array}{ccccc} \{S \subset B, |S| \equiv 0 \mod 2\}/(S \sim \overline{S}) & \leftrightarrow & \mathscr{M}_{2,g}\left(\frac{1}{2}\mathbb{Z}/\mathbb{Z}\right) & \leftrightarrow & \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) \\ S & \leftrightarrow & \eta_S & \leftrightarrow & \Omega\eta'_S + \eta''_S. \end{array} \tag{I.1}$$

La propriété *b)* ci-dessus permet de déterminer si une thêta constante est paire ou impaire : les demi-caractéristiques paires correspondent aux ensembles S tels que

$$|S\Delta U| \equiv g+1 [4].$$

On peut par ailleurs utiliser la bijection $S \leftrightarrow S\Delta U$ pour dénombrer les thêta constantes paires et impaires.

Remarque 3.5. Dans le cas $g = 3$, les demi-caractéristiques paires correspondent à un ensemble S tel que $S\Delta U$ est soit de cardinal 0, au nombre de 1 ($S = U$), ou soit de cardinal 4, au nombre, modulo passage au complémentaire, de $\binom{7}{3} = 35$. On retrouve bien les 36 demi-caractéristiques paires.

On peut désormais énoncer la formule de Thomae qui relie les thêta constantes aux points de Weierstrass de la courbe hyperelliptique, c'est-à-dire les x_i.

Théorème 3.6 (Formule de Thomae). *Il existe une constante c telle que pour tout sous-ensemble S de B, de cardinal pair, on ait*

$$\vartheta[\eta_S](0,\Omega)^4 = \begin{cases} c \prod\limits_{\substack{i,j \in S\Delta U \\ i<j}} (x_i - x_j) \prod\limits_{\substack{i,j \notin S\Delta U \\ i<j}} (x_i - x_j) & si\ |S\Delta U| = g+1, \\ 0 & si\ |S\Delta U| \neq g+1. \end{cases}$$

(‡). On renvoie encore à Mumford [Mum 84] pour des détails supplémentaires.

La constante c n'a ici que peu d'importance, puisque le système des thêta constantes est homogène.

On remarque, par ailleurs, que cette formule fait apparaître des thêta constantes qui s'annulent, du fait que la courbe est hyperelliptique. Pour faciliter la distinction de cas, on considère les thêta constantes $\boldsymbol{\vartheta}[\eta_{S\Delta U}]$ et la condition de nullité devient $|S| \neq g+1$ à laquelle il faut bien sûr rajouter les pré-requis $|S| \equiv 0 \mod 2$ et l'équivalence $S \sim \overline{S}$.

On voit donc apparaître $\binom{2g+1}{g}$ demi-caractéristiques paires issues d'un ensemble de cardinal $g+1$ tandis qu'il y en a $2^{g-1}(2^g+1)$ au total. C'est cette différence qui constitue le critère que nous utilisons par la suite pour distinguer, parmi les variétés abéliennes, celles qui sont des jacobiennes de courbes hyperelliptiques.

Théorème 3.7 (*cf.* Mumford, [Mum 84, §9]). *Une variété abélienne est la jacobienne d'une courbe hyperelliptique si et seulement si parmi ses thêta constantes paires,*

$$2^{g-1}(2^g+1) - \binom{2g+1}{g}$$

sont nulles.

Remarque 3.8. Pour $g = 1$ ou 2 la formule ci-dessus donne 0 : ainsi si toutes les thêta constantes paires sont non nulles, on a bien des jacobiennes de courbes (hyper)elliptiques. Pour $g = 2$, on peut toutefois avoir une thêta constante paire nulle, auquel cas on est dans la situation du produit de deux courbes elliptiques.

Pour $g = 3$, la condition se résume à une thêta constante nulle : l'espace des jacobiennes en genre 3 est de dimension 6 alors que celui des jacobiennes de courbes hyperelliptiques est de dimension 5. On rencontre par la suite des courbes de genre 3 qui ne sont pas hyperelliptiques : ce sont nécessairement des courbes planes lisses données par une équation quartique, c'est-à-dire homogène de degré 4. Pour trouver une telle équation à partir d'un autre modèle, on peut par exemple calculer une base de différentielles puis chercher une équation quartique annulée en cette base, ce qui permet de se ramener à un système d'équations linéaires.

Courbes à multiplication réelle

Ce chapitre est consacré à la construction explicite de familles de courbes à multiplication réelle par des sous-corps de corps cyclotomiques.

Sommaire

Dans son article, *Endomorphism Algebras of Jacobians*, [Ell 01], J. Ellenberg donne un certain nombre d'outils théoriques pour construire des variétés abéliennes, plus précisément des jacobiennes de courbes, à multiplication réelle. Il en déduit l'existence d'un certain nombre de courbes ou de familles de courbes, à un ou plusieurs paramètres, dont certaines sont déjà connues explicitement, par exemple celle de J.-F. Mestre [Mes 91], ou celles de W. Tautz, J. Top et A. Verberkmoes [TTV 91]. Nous proposons ici d'utiliser les outils fournis par J. Ellenberg pour donner des familles explicites de courbes dont les jacobiennes sont à multiplication réelle.

— 1 —
Recouvrements, monodromie et multiplication réelle

Multiplication réelle. Avant de décrire ces familles, commençons par fixer les notions et les notations principales pour la suite. On a déjà vu en 2.2 ce qu'était une variété abélienne à multiplication complexe ; il nous faut préciser ce que l'on entend par multiplication réelle.

Définition 1.1 (Multiplication réelle). *On dit qu'une variété abélienne A de dimension g est à* multiplication réelle *s'il existe un corps de nombres totalement réel F de dimension g tel que*

$$F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A).$$

De plus, on dit plus simplement qu'une courbe de genre g est à multiplication réelle *par F si sa jacobienne l'est.*

En particulier, une variété abélienne à multiplication complexe est toujours à multiplication réelle. En effet, comme on l'a vu en 2.2, un corps à multiplication complexe est nécessairement une extension quadratique d'un corps totalement réel.

D'un autre côté, deux variétés abéliennes à même multiplication réelle peuvent avoir des multiplications complexes différentes. Par exemple, toutes les courbes elliptiques à multiplication complexe ont la même multiplication réelle. De manière moins triviale, on peut prendre l'exemple de $\mathbb{Q}(\zeta_l)$, corps cyclotomique de degré $l-1$ qui est à multiplication complexe : c'est une extension totalement imaginaire de corps totalement réel $\mathbb{Q}(\cos(\frac{2\pi}{l}))$, que l'on note plus simplement, par la suite, $\mathbb{Q}(\zeta_l^+)$. Or, comme pour tout corps totalement réel, on peut considérer l'extension par $i^2=-1$, qui est totalement imaginaire. Ainsi, les corps $\mathbb{Q}(\zeta_l)$ et $\mathbb{Q}(\zeta_l^+, i)$ ont tous les deux la même multiplication réelle $\mathbb{Q}(\zeta_l^+)$.

Sur les corps finis de caractéristique p, on peut vérifier la multiplication complexe grâce au polynôme caractéristique du Frobenius, $\pi(t)$. Ici, comme on s'intéresse à la multiplication réelle, il est avantageux de regarder le polynôme caractéristique de la trace du Frobenius, donné par $\mathrm{Res}_t(\pi(t), rt - t^2 - p)$.

Recouvrements. Le point de départ de J. Ellenberg consiste à considérer une courbe algébrique projective, non singulière, Y, définie sur un corps algébriquement clos, k, telle que son groupe d'automorphismes soit « important ». En notant $G \subset \mathrm{Aut}(Y)$ un sous-groupe, on a une action naturelle

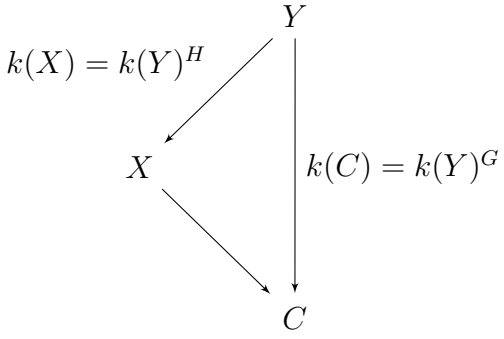
$$\mathbb{Q}[G] \to \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(Y)).$$

On note C la courbe quotient non singulière Y/G, associée aux éléments G–invariants de $k(Y)$; on considère alors un sous-groupe H de G et on définit l'élément $\pi_H \in \mathbb{Q}[G]$,

$$\pi_H := \frac{1}{|H|} \sum_{h \in H} h,$$

et l'algèbre $\mathbb{Q}[H\backslash G/H]$ engendrée par $\{\pi_H g \pi_H,\ g \in G\}$, sous-algèbre de $\mathbb{Q}[G]$ dite de Hecke. On note enfin $X = Y/H$, la courbe quotient non singulière, associée aux éléments H–invariants de $k(Y)$.

L'action naturelle de $\mathbb{Q}[G]$ se restreint en une action de $\mathbb{Q}[H\backslash G/H]$ sur $\mathrm{Jac}(X)$. On note, suivant J. Ellenberg, $\mathscr{H}_{X/C}$ l'image de cette algèbre dans $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X))$. On a le diagramme suivant qui résume la situation.



(II.1)

Branchements et monodromie. En considérant l'injection

$$\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X)) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(H_1(X, \mathbb{Q}_l))$$

pour un entier premier $l \neq \mathrm{car}(k)$, on peut calculer $\mathscr{H}_{X/C}$ grâce à la représentation de $\mathbb{Q}[H\backslash G/H]$ sur $H_1(X, \mathbb{Q}_l)$. Cela permet à J. Ellenberg de relier $\mathscr{H}_{X/C}$ au branchement de $Y \to C$. Grâce à une utilisation fine de la formule de Riemann-Hurwitz, J. Ellenberg exhibe des cas de monodromie de ce recouvrement, que nous détaillons ci-dessous, permettant d'obtenir des courbes X à multiplication réelle.

Afin d'énoncer ce résultat, nous avons encore besoin de quelques définitions et notations.

Définition 1.2 (Groupes métacycliques). *On dit qu'un groupe est* métacyclique *s'il possède un sous-groupe normal cyclique dont le quotient est lui aussi cyclique.*

Par la suite, on considère un type plus restreint de groupes métacycliques. Soit l un entier premier impair, n un entier divisant $l-1$ et $k \in (\mathbb{Z}/l\mathbb{Z})^*$ d'ordre n.

Définition 1.3 (Groupes métacycliques $G_{l,n}$). *On définit le groupe* métacyclique $G_{l,n}$ *par deux générateurs α, σ d'ordres respectifs l et n avec la relation de conjugaison $\alpha\sigma\alpha^{-1} = \sigma^k$:*

$$G_{l,n} := \langle \alpha, \sigma,\ \sigma^l = \alpha^n = 1, \alpha\sigma\alpha^{-1} = \sigma^k \rangle.$$

On reconnaît bien évidemment dans cette définition les groupes diédraux, pour $n = 2$. Du fait que l'on a choisi $n \mid l-1$, on peut considérer des sous-corps d'indice n des corps cyclotomiques.

Notation 1.4 (Sous-corps des cyclotomiques). *Soit l un entier premier impair. On note ζ_l une racine l-ième de l'unité et $\mathbb{Q}(\zeta_l)$ le corps cyclotomique de degré $l-1$. Pour n divisant $l-1$, on note $\mathbb{Q}(\zeta_l^{(n)})$ le sous-corps d'indice n de $\mathbb{Q}(\zeta_l)$. Il est engendré par*

$$\zeta_l^{(n)} := \sum_{i=0}^{n-1} \zeta_l^{k^i}$$

où $k \in (\mathbb{Z}/l\mathbb{Z})^*$ est d'ordre n. On rappelle que l'on note de manière abrégée dans la suite $\mathbb{Q}(\zeta_l^+) := \mathbb{Q}(\zeta_l^{(2)})$, le sous-corps totalement réel maximal de $\mathbb{Q}(\zeta_l)$.

En particulier, pour tout n pair divisant $l-1$, le corps $\mathbb{Q}(\zeta_l^{(n)})$ est totalement réel, de dimension $\frac{l-1}{n}$.

Enfin, afin de décrire les branchements et la monodromie, on conserve la notation de J. Ellenberg suivante.

Notation 1.5. *Soit $Y \to \mathbb{P}^1$ un recouvrement de groupe de Galois $G_{l,n}$, possédant r points de branchement. On note $g_1, \ldots, g_r \in G_{l,n}$ la monodromie de ce recouvrement en chacun des points de branchement. On note alors $d_i = 0$ si l'ordre de g_i est l, $d_i = \frac{n}{\mathrm{ord}\, g_i}$ sinon.*
On dit enfin qu'un tel recouvrement est de type $(d_1, \ldots, d_r)$.

On est maintenant en mesure d'énoncer un des principaux résultats que J. Ellenberg expose dans son article, [Ell 01], reliant les données de branchement de $Y \to C$ à $\mathscr{H}_{X/C}$, dans le cas où G est un groupe métacyclique et $C = \mathbb{P}^1$.

Théorème 1.6 (Ellenberg). *Soient l un entier premier impair, n un entier pair, divisant $l-1$. Soit $Y \to \mathbb{P}^1$ un recouvrement de groupe de Galois métacyclique, $G_{l,n}$. On note H le sous-groupe de $G_{l,n}$ engendré par α, d'ordre n et $X = Y/H$.*

Alors, $\mathrm{Jac}(X)$ *est à multiplication réelle par $\mathbb{Q}(\zeta_l^{(n)})$ si et seulement si le recouvrement $Y \to \mathbb{P}^1$ est parmi les types listés dans la table II.1 ci-dessous.*

Table II.1 Types de recouvrement de groupe $G_{l,n}$

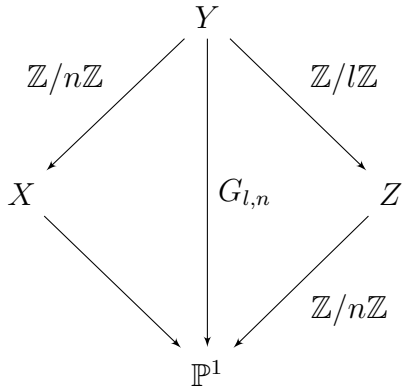
n	*types*
2	$(0,0,1,1)$, $(0,1,1,1,1)$,$(1,1,1,1,1,1)$
4	$(0,1,1)$,$(1,1,2,2)$
6	$(1,1,2)$,$(2,2,3,3)$
8	$(1,1,4)$
10	$(1,2,5)$

La suite de ce chapitre consiste à donner des exemples explicites de recouvrements correspondant à ces types. L'idée consiste à construire Y en deux temps, en passant par une courbe Z, dont les recouvrements $Y \to Z \to \mathbb{P}^1$ sont de degrés respectifs l et n et de groupes de Galois cycliques $\mathbb{Z}/l\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

Si le type considéré de la table II.1 possède des zéros, on cherche des revêtements $Y \to Z$ ramifiés, et non-ramifiés dans le cas contraire.

On commence dans tous les cas par chercher un recouvrement $Z \to \mathbb{P}^1$ de groupe de Galois cyclique d'ordre n. On conserve la même notion de type de ramification, en adaptant la notation 1.5 sans difficulté. On cherche donc des revêtements de degré n dont les types figurent dans la table II.1, hormis les 0. On construit ensuite un deuxième recouvrement $Y \to Z$, de groupe de Galois $\mathbb{Z}/l\mathbb{Z}$, de façon à obtenir le bon type et, par composition, le groupe de Galois $G_{l,n}$, ce qui est en fait le plus contraignant. Cette stratégie se résume sur le diagramme suivant.

Figure II.1 Revêtements métacycliques galoisiens



— 2 —
Multiplication réelle par $\mathbb{Q}(\zeta_l^+)$

Sauf mention contraire, on se place dans cette section sur le corps de base $k = \mathbb{Q}$. Le cas $n = 2$ a déjà beaucoup été étudié, et l'on renvoie par exemple à W. Tautz, J. Top et A. Verberkmoes [TTV 91] et J.-F. Mestre [Mes 91] pour des familles à un, respectivement deux, paramètres de courbes hyperelliptiques à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$. On retrouve ici les familles de [TTV 91] et on donne d'autres familles différentes. Le type 2.3 correspond par ailleurs aux résultats de A. Brumer.

2.1 Type (0,0,1,1)

Comme on l'a expliqué à la fin de le section précédente, on commence par chercher un recouvrement de la droite projective $Z \to \mathbb{P}^1$, branché en deux points, de « type » (1,1), c'est-à-dire simplement un recouvrement de degré 2 ramifié en deux points. Par la formule d'Hurwitz, cela impose

$$g(Z) = \tfrac{1}{2}\Big(2 + 2(2g(\mathbb{P}^1) - 2) + (2-1) + (2-1)\Big) = 0$$

Si $f(x) \in k(x)$ est une fraction rationnelle quelconque, non constante, $y = f(x)$ est une courbe de genre 0 et le revêtement de degré 2 $(x, y) \mapsto x^2$ est ramifié en 0 et ∞.

On cherche ensuite un revêtement de Z de degré l, non ramifié en $0, \infty$ mais en deux autres points, dont la ramification est nécessairement d'ordre l. On vérifie qu'en choisissant $P(x) \in k[x]$ un polynôme de degré 2, la courbe Y définie par

$$t^l = y \quad \text{et} \quad y = \frac{P(x)}{P(-x)},$$

possède les propriétés souhaitées : en effet, le recouvrement $Y \to Z$ donné par $(x, y, t) \mapsto (x, y)$ est ramifié d'ordre l en les 4 racines des polynômes $P(x)$ et $P(-x)$, qui sont ensuite identifiées deux par deux par $(x, y) \mapsto x^2$.

Il est clair que l'on peut choisir P unitaire, et que par un changement de variable homographique $x \mapsto \lambda x$, on peut choisir $P(x) = x^2 + x + a$, P ne pouvant pas être un polynôme pair.

Proposition 2.1. *Soit Y la courbe définie par l'équation*

$$t^l = \frac{x^2 + x + a}{x^2 - x + a}.$$

Alors, le revêtement $Y \to \mathbb{P}^1$, $(x, y) \mapsto x^2$ est de degré $2l$, de type $(0, 0, 1, 1)$ et de groupe de Galois le groupe diédral $G_{l,2}$.

Démonstration. Il ne reste qu'à vérifier que le groupe de Galois du revêtement est bien $G_{l,2}$. En effet, on trouve les automorphismes $\sigma : (x, t) \mapsto (x, \zeta_l t)$ et $\alpha : (x, t) \mapsto \left(-x, \frac{1}{t}\right)$ d'ordres respectifs l et 2, tels que

$$\alpha\sigma\alpha^{-1} : (x, t) \mapsto (x, \zeta_l^{-1} t) = \sigma^{-1}(x, t). \qquad \square$$

Grâce à la construction de J. Ellenberg présentée dans la section précédente, ceci fournit donc une famille à un paramètre, a, de courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$, dont on peut mener tous les calculs explicitement.

En effet, la courbe quotient $Y/\langle\alpha\rangle$ est obtenue en calculant le polynôme minimal $\Pi(z,x)$ de $z_t := t+\frac{1}{t}$, qui doit nécessairement être un polynôme invariant par $x \mapsto -x$: une équation de X est donnée par le polynôme $Q(z,w)$ tel que $\Pi(z,x) = Q(z,x^2)$. On peut voir Q comme le reste de la division euclidienne en x de Π par $w^2 - x$.

On retrouve en fait la même famille que dans [TTV 91]. En effet, la courbe Y possède un autre modèle qui rejoint celui des courbes de cet article.

Proposition 2.2. *La courbe Y est une courbe hyperelliptique de genre $l-1$. Elle peut être donnée, à torsion près, par une équation de type*

$$y^2 = z^{2l} + bz^l + 1.$$

La courbe X est elle aussi hyperelliptique, donnée par l'équation

$$\mu^2 = (w+2)(wg_l(w^2-2)+b)$$

où g_l est le polynôme minimal de $-\zeta_l - \zeta_l^{-1}$.

Démonstration. Il s'agit simplement d'un changement de variables,

$$\begin{cases} z = t \\ y' = 2(t^l-1)x - (t^l+1), \end{cases}$$

qui aboutit au modèle hyperelliptique $y'^2 = (1-4a)(z^{2l} + 2\frac{1+4a}{1-4a}z^l + 1)$ et, quitte à prendre une racine carrée de $1-4a$ et à poser $b = \frac{1+4a}{1-4a}$ comme nouveau paramètre, on obtient la courbe hyperelliptique de genre $l-1$

$$y^2 = z^{2l} + bz^l + 1.$$

Le groupe de Galois sur ce modèle est réalisé par les éléments notés comme avant

$$\sigma : (z,y) \mapsto (\zeta_l z, y)$$
$$\alpha : (z,y) \mapsto \left(\tfrac{1}{z}, \tfrac{y}{z^l}\right).$$

Le reste de la démonstration est identique à [TTV 91] : on pose $\omega = z + \frac{1}{z}$ et on a

$$z^{2l} + 1 = z^l\Big(z + \frac{1}{z}\Big)g_l\Big(z^2 + \frac{1}{z^2}\Big)$$
$$\omega + 2 = \frac{(z+1)^2}{z}$$

qui permet d'écrire $y^2 = z^l(b + \omega g_l(\omega^2-2))$ puis

$$z^l = \left(\frac{z^{\frac{p+1}{2}}}{z+1}\right)^2(\omega+2)$$

pour en tirer finalement, après avoir posé $\mu = \frac{y(z+1)}{z^{\frac{l+1}{2}}}$ que

$$\mu^2 = (\omega+2)\Big(b + \omega g_l(\omega^2-2)\Big)$$

et que les fonctions $\mu(z,y)$ et $\omega(z)$ sont invariantes par α, ce qui assure que l'on a trouvé un modèle de la courbe quotient $X = Y/\langle\alpha\rangle$. □

On peut vérifier simplement, comme dans [TTV 91], que la courbe quotient $X = Y/\langle\alpha\rangle$ est bien à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$, en vérifiant (⋆) que $[\sigma] + [\sigma^{-1}]$ est bien un endomorphisme de la jacobienne du quotient : cela suffit puisque l'on est alors assuré d'avoir le corps totalement réel $\mathbb{Q}(\zeta_l^+)$ dans $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X))$ d'une part et que d'autre part, l'expression explicite de la courbe hyperelliptique X assure qu'elle est de genre $\frac{l-1}{2}$, étant définie par un polynôme de degré $l+1$.

(⋆). On note toujours $[\sigma]$ l'endomorphisme de la jacobienne, issu d'un automorphisme σ de la courbe.

2.2 Type (0,1,1,1,1)

On cherche, comme précédemment, un revêtement de $\mathbb{P}^1$ ramifié en 4 points d'ordre 2. On trouve ici les courbes de genre 1 données par une équation de Weierstrass, famille à un paramètre, avec le revêtement qui « oublie » les ordonnées du modèle de Weierstrass. En munissant E de son point à l'infini, on en fait une courbe elliptique sur laquelle on veut un revêtement ramifié en seulement un point, de groupe $\mathbb{Z}/l\mathbb{Z}$. Il faut, de plus, que le groupe de Galois du revêtement total soit le groupe diédral. On cherche alors une fonction sur E qui, de façon similaire au cas précédent, soit changée en son opposée par l'involution hyperelliptique.

Proposition 2.3. *Il existe une famille rationnelle sur* $\mathbb{Q}$*, à deux paramètres, de courbes à multiplication réelle par* $\mathbb{Q}(\zeta_l^+)$*, issue du type* $(0,1,1,1,1)$*.*

Démonstration. Commençons par considérer un point générique $P \in E$ et posons $Q = lP$. Le diviseur sur E, de degré 0,

$$D = (Q) - (-Q) + l((P) - (-P))$$

est principal car $Q - (-Q) + lP - l(-P) = O_E$. C'est le diviseur d'une fonction dont on souhaite, comme avant, qu'elle soit changée en son opposée par l'involution elliptique $\imath$. Pour cela, en concentrant les pôles à l'infini, on écrit $D = D' + \imath(D')$ avec

$$D' = (-Q) + l(P) - (l+1)O_E.$$

Pour les mêmes raisons que D, le diviseur D' est principal, et soit

$$\varphi(x,y) = a(x) + yb(x)$$

une fonction de diviseur D'. Alors, le diviseur de $\frac{\varphi(x,y)}{\varphi(x,-y)}$ est D. On considère ensuite le revêtement de E par la courbe Y définie par l'équation de E ainsi que

$$t^l = \frac{\varphi(x,y)}{\varphi(x,-y)}.$$

Le revêtement est donné par l'application $(x,y,t) \mapsto (x,y)$ qui n'est ramifié qu'en Q et $-Q$ car la ramification en P et $-P$ est tuée par le facteur l dans le diviseur de la fonction φ. Ainsi, le revêtement cherché de Y sur $\mathbb{P}^1$ est donné par $(x,y,t) \mapsto x$.

Il reste à déterminer le groupe de Galois. On a déjà l'involution hyperelliptique, qui « monte », par construction, sur Y ainsi que les racines l-ièmes agissant t :

$$\alpha : (x,y,t) \mapsto (x,-y,\tfrac{1}{t})$$
$$\sigma : (x,y,t) \mapsto (x,y,\zeta_l y)$$

Comme précédemment, on vérifie sans difficulté que $\alpha\sigma\alpha^{-1} = \sigma^{-1}$ si bien que le groupe diédral est bien le groupe de Galois de ce revêtement.

Le choix de E et de $P \in E$ point générique constitue les deux paramètres de la famille recherchée. Sa rationalité est donnée dans l'algorithme II.2 ci-après. □

On peut, comme dans le cas précédent, mener les calculs pour obtenir des familles à 2 paramètres. Du moins, on a un algorithme facile permettant, une fois donné l, d'écrire une équation de $X = Y/\langle\alpha\rangle$. Pour cela, on part d'une équation générale de courbe elliptique E de la forme $y^2 = x^3 + ux^2 + vx + w^2$, possédant de plus le point rationnel « générique » $P = (0, w)$. On obtient les deux paramètres de la famille par homogénéité de l'équation E ; le changement de paramètres rationnels

$$u = \tau s, \quad v = \tau^2 r, \quad w^2 = \tau^3 r \quad \text{et} \quad x = \tau x'$$

élimine la variable τ et donne une famille de courbes en x', z à 2 paramètres, r, s.

Algorithme II.1 Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ (I)

Entrée : l

1: $E(x, y) \leftarrow y^2 = x^3 + ux^2 + vx + w^2$
2: $P \leftarrow (0, w)$ et $Q \leftarrow lP$
3: **Calculer**, à l'aide de Riemann-Roch, une fonction $\varphi(x, y)$ telle que

$$\operatorname{div}(\varphi) = (-Q) + l(P) - (l + 1)O_E.$$

4: $\Pi(x, y, z) \leftarrow \operatorname{Res}_t(\varphi(x, -y)t^l - \varphi(x, y), t^2 + 1 - tz)$
5: $X(x, z) \leftarrow \Pi(x, y, z) \mod_y E(x, y)$

Sortie X.

Avant de donner des exemples, il faut faire quelques remarques sur cet algorithme. Comme précédemment, la ligne 4 permet de calculer le polynôme minimal de $z_t := t + \frac{1}{t}$ à l'aide d'un calcul classique d'élimination par résultant. Enfin, il est à préciser que dans la ligne 5, ce résultant, modulo l'équation de E, ne dépend plus de y, puisque $y \mapsto -y$ change t en $\frac{1}{t}$, et laisse donc z_t invariant.

Exemple 2.4 (Courbes à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$ et $\mathbb{Q}(\zeta_7^+)$). Voici deux exemples de familles à deux paramètres fournies par l'algorithme II.1.

***l* = 5** On a $\mathbb{Q}(\zeta_5^+) = \mathbb{Q}(\sqrt{5})$ et X est une courbe de genre 2, hyperelliptique. L'algorithme ci-dessus et le changement de variables $x \mapsto \frac{1}{x}$ fournissent l'équation

$$z(z^4 - 5z^2 + 5) = \frac{1}{(d_1 x + d_0)} \sum_{i=0}^{6} c_i x^i,$$

où on a l'identité polynomiale $z^4 - 5z^2 + 5 = g_5(z^2 - 2)$, avec g_5 défini en 2.2. L'équation ci-dessus est à variables séparées de la forme $g(z) = h(x)$, avec la relation sur les différentielles

$$g'(z)\,\mathrm{d}z = h'(x)\,\mathrm{d}x.$$

On peut alors calculer une base de différentielles holomorphes $(\omega_1\,\mathrm{d}x, \omega_2\,\mathrm{d}x)$ puis poser un nouveau paramètre $X = \frac{\omega_2}{\omega_1}$, qui nous permet de calculer $\mathrm{d}X = \left(\frac{\partial X}{\partial x} + \frac{\partial X}{\partial z}\frac{h'(x)}{g'(z)}\right)\mathrm{d}x$, et de poser $Y = \frac{\mathrm{d}X}{\omega_1\,\mathrm{d}x}$. On écrit alors

$$Y^2 = \sum_{i=0}^{6} a_i X^i,$$

on réduit modulo l'équation de départ, puis on résout les équations linéaires en les a_i. Il est pratique de poser $s = r + t$ et on obtient une famille à deux paramètres

sous forme hyperelliptique donnée par les coefficients a_i, dont les coefficients sont donnés par

$$a_0 = \frac{100t^2r^3 + 5r^3 - 36tr^3 - 8t^3r^2 - 40t^5r^2 + 36r^2t^4 - 128t^3r^3 - 20t^6r - 12t^8r + 64r^3t^4 + 48t^7r - 8t^9}{r},$$
$$a_1 = 20(-5t^8 - 8t^7r + 28t^6r - 12rt^5 - 24r^2t^4 + 16t^3r^3 + 24t^3r^2 - 24t^2r^3 - 6t^2r^2 + 12tr^3 - 2r^3),$$
$$a_2 = a_4 = 0,$$
$$a_3 = 10(r^2 - 4tr^2 + 4t^3r + 4t^2r^2 - 10rt^4 + 2t^6 + 4rt^5)r^2,$$
$$a_5 = 4(6r^5t^2 - t^4r^4 - 4r^5t^3 - 2tr^5),$$
$$a_6 = r^6 - 4r^6t + 4r^6t^2$$

Enfin, comme on a deux paramètres en genre 2, cette famille contient donc, à rationalité près, toutes les courbes de genre 2 à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$, qui sont, par exemple, données dans [Mes 91] sous une forme hyperelliptique plus simple.

***l* = 7** Cette fois, le corps $\mathbb{Q}(\zeta_7^+) = \mathbb{Q}(\cos(\frac{2\pi}{7}))$ est de degré 3 et l'on obtient une famille à deux paramètres de courbes de genre 3 à multiplication réelle par ce corps. Elle est donnée, de façon similaire, par une équation de la forme

$$z(z^6 - 7z^4 + 14z^2 - 7) = \frac{1}{(d_1x + d_0)} \sum_{i=0}^{8} c_i x^i.$$

Cette famille est différente des familles exposées dans [Mes 91] car, comme expliqué dans la remarque 3.8, on peut déterminer une équation quartique à deux paramètres. Comme ci-dessus, le changement de variable $s = r + t$ diminue fortement la taille de l'équation et permet de calculer une base de différentielles, par exemple avec la commande `differentials` du paquet `algcurves` de Maple [Map 13]. On obtient l'équation générale en U et V avec deux paramètres r et t.

$-(2tr - r - t^3)(-r^3 - 40t^2r^3 + 10tr^3 - 80r^3t^4 + 80t^3r^3 + 32r^3t^5 + 16r^2t^7 - 56r^2t^6 + 64r^2t^5 - 30r^2t^4 + 5r^2t^3 + 12rt^8 - 16rt^7 + 5rt^6 + t^9) + 2r(2t - 1)^2(r^2 - 4tr^2 + 4t^3r + 4r^2t^2 - 10rt^4 + 2t^6 + 4rt^5)U + r^2(2t - 1)^4U^2 - r(2t - 1)^2U^3 + r(2t - 1)^2(-2r^3 - 6r^2t^2 + 12tr^3 + 24r^2t^3 - 24t^2r^3 - 12rt^5 - 24r^2t^4 + 16t^3r^3 + 28rt^6 - 5t^8 - 8rt^7)V - 2t^2(t^3 + 2r - 6tr + 4t^2r)^2UV - t(t^3 + 2r - 6tr + 4t^2r)(r^2 - 4tr^2 + 4t^3r + 4r^2t^2 - 10rt^4 + 2t^6 + 4rt^5)V^2 - 2rt(2t - 1)^2(t^3 + 2r - 6tr + 4t^2r)UV^2 + t(t^3 + 2r - 6tr + 4t^2r)U^2V^2 + 2r(2t - 1)^2(r^2 - 4tr^2 + 4t^3r + 4r^2t^2 - 10rt^4 + 2t^6 + 4rt^5)V^3 + (r^2 - 4tr^2 + 4t^3r + 4r^2t^2 - 10rt^4 + 2t^6 + 4rt^5)UV^3 + t^2(t^3 + 2r - 6tr + 4t^2r)^2V^4 = 0.$

Finissons cet exemple par une courbe spéciale dans cette famille, obtenue en fixant au début $u = v = 0$; on obtient dans un premier temps la courbe

$$x^6z(z^6 - 7z^4 + 14z^2 - 7) = 2x^6 + 4x^3 + 1$$

qui a un modèle quartique donné par l'équation

$$v^3(2u - 1) - uf(u) = 0,$$

où $f(u) = u^3 + 2u^2 - u - 1$ est le polynôme minimal de $(\zeta_7 + \zeta_7^{-1})^{-1}$. Notons que sur les deux modèles, il est facile de voir que l'anneau des endomorphismes de cette courbe contient $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$, par $(x, z) \mapsto (\zeta_3 x, z)$, ou $(u, v) \mapsto (u, \zeta_3 v)$ sur le modèle quartique. Ceux-ci proviennent de la courbe elliptique $y^2 = x^3 + 1$. Comme cet automorphisme sur Y commute avec σ et α, on en déduit, par la proposition 2.3 du chapitre I, que X est à multiplication complexe par $\mathbb{Q}(\zeta_7^+, i\sqrt{3})$.

2.3 Type (1,1,1,1,1,1)

Un tel revêtement est donné par une courbe de genre 2, disons

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

que l'on note H. Le revêtement de degré 2 ramifié en les 6 points de Weierstrass est bien entendu $(x,y) \mapsto x$.

Proposition 2.5. *Il existe une famille de courbes à trois paramètres, « explicite », à multiplication réelle par* $\mathbb{Q}(\zeta_l^+)$.

Démonstration. On cherche un revêtement non ramifié de la courbe hyperelliptique H, sur lequel agit le groupe diédral $G_{l,2}$.

Pour cela, on considère $P \in \mathrm{Jac}(H)$ de l–torsion, défini dans la clôture algébrique k de $\mathbb{Q}(\lambda_1,\lambda_2,\lambda_3)$. Ainsi, par définition le diviseur de lP, en représentation de Mumford, est un diviseur principal : c'est le diviseur d'une fonction $\varphi(x,y)$. Comme dans le cas précédent, il nous suffit ensuite de considérer la courbe Y donnée par les équations

$$(Y)\ \begin{cases} y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3) \\ t^l\ = \dfrac{\varphi(x,y)}{\varphi(x,-y)} \end{cases}$$

dont le recouvrement de H par $(x,y,t) \mapsto (x,y)$ est non ramifié, de degré l.

On a de manière analogue aux deux cas précédents, les morphismes

$$\alpha : (x,y,t) \mapsto (x,-y,\tfrac{1}{t})$$
$$\sigma : (x,y,t) \mapsto (x,y,\zeta_l t)$$

qui engendrent le groupe diédral $G_{l,2}$. Encore une fois, pour donner une équation de la courbe quotient $X = Y/\langle\alpha\rangle$, on commence par calculer le polynôme minimal en z de $z_t := t + \frac{1}{t}$ dans $k(x,y)$. Le résultat est invariant par $y \mapsto -y$ et ainsi, modulo l'équation de H, on obtient un polynôme en x et z qui est une équation plane de la courbe X. □

Cette démonstration donne, comme dans le cas précédent, un algorithme de calcul d'une équation plane de X, en tout point similaire à l'algorithme II.1, à la différence que l'on doit trouver un élément $P \in \mathrm{Jac}(H)$ de l–torsion.

Pour cela, on peut faire comme dans le cas des courbes elliptiques, où, partant d'un point « générique » (x,y), on applique successivement la loi d'addition. On aboutit en fait aux polynômes de division (que l'on peut calculer plus efficacement) dont les racines sont les points de l–torsion. En genre 2, on peut faire la même chose, en utilisant la représentation de Mumford des points de la jacobienne, vue dans le chapitre I, en 1.10. Ainsi, on choisit de représenter un point P de la jacobienne de la courbe hyperelliptique H, par deux points P_1, P_2 de la courbe H, et de l'identifier au diviseur

$$\mathrm{Div}(P) := (P_1) + (P_2) - D_\infty, \tag{II.2}$$

où $D_\infty = 2(P_\infty)$, s'il n'y a qu'un point à l'infini, ou $D_\infty = (P_{\infty,1}) + (P_{\infty,2})$ sinon. Ensuite, on applique les lois d'addition sur la jacobienne, de façon similaire au genre 1. Néanmoins, même si tous les calculs sont effectifs, cet algorithme reste théorique au sens où la puissance de calcul nécessaire reste, à l'heure actuelle, insuffisante.

Familles de courbes hyperelliptiques à deux paramètres. Dans le cas où la jacobienne de la courbe de genre 2 n'est pas simple et que l'on a un morphisme vers une courbe elliptique, J.-F. Mestre, dans [Mes 91], donne une famille à deux paramètres de courbes hyperelliptiques à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$. Celle-ci repose aussi sur un point de la courbe elliptique. Ainsi, quand $X_1(l)$ est de genre 0, cela fournit des familles rationnelles, explicitées dans [Mes 91], pour $l = 5, 7$ par exemple.

Courbes modulaires $X_0(n)$. Dans le cas où la jacobienne de H est simple, on trouve d'autres courbes que celles fournies plus haut. On peut donner des exemples (◇) issus des courbes modulaires $X_0(n)$ qui sont des courbes (hyperelliptiques) de genre 2. On sait — voir par exemple [Ogg 74] — qu'il n'existe qu'un nombre fini de courbes modulaires qui sont hyperelliptiques, qui plus est de genre 2. Elles sont données pour les entiers $n \in \{22, 23, 26, 29, 31, 37\}$. On considère leur modèle de Weierstrass, avec deux points à l'infini. Parmi ces entiers n, il y a soit des nombres premiers, soit des composés de deux nombres premiers. Toujours dans [Ogg 74], on a des points rationnels sur les jacobiennes de $X_0(n)$ dont on connaît l'ordre. Ainsi, pour n premier, le point (‡) $(P_{\infty,1}) - (P_{\infty,2})$ est d'ordre le numérateur de $\frac{n-1}{12}$, et dans le cas où $n = pq$, on a des points d'ordre les numérateurs des $\frac{(p-1)(q-1)}{24}$, $\frac{(p+1)(q-1)}{24}$ et $\frac{(p-1)(q+1)}{24}$. On peut résumer cela dans la table II.2 suivante, où les équations ont été obtenues par Fricke [Fri 24]

Table II.2 Points rationnels de courbes modulaires hyperelliptiques de genre 2

n	Équation de $X_0(n)$	Points rationnels	Ordre l
22	$y^2 = (x^3+8x^2+16x+16)(x^3+4x^2+8x+4)$	$(P_{\infty,1}) - (P_{\infty,2})$	5
		$(0,8) - (P_{\infty,2})$	5
		$(0,-8) - (P_{\infty,2})$	5
23	$y^2 = x^6 - 14x^5 + 57x^4 - 106x^3 + 90x^2 - 16x - 19$	$(P_{\infty,1}) - (P_{\infty,2})$	11
26	$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$	$(P_{\infty,1}) - (P_{\infty,2})$	21
29	$y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$	$(P_{\infty,1}) - (P_{\infty,2})$	7
31	$y^2 = x^6 - 14x^5 + 61x^4 - 106x^3 + 66x^2 - 8x - 3$	$(P_{\infty,1}) - (P_{\infty,2})$	5
37	$y^2 = x^6 - 9x^4 - 11x^2 + 37$	$(P_{\infty,1}) - (P_{\infty,2})$	3

Dans toutes les situations, on voit que le point $(P_{\infty,1}) - (P_{\infty,2})$ des jacobiennes permet de construire des courbes à multiplication réelle par l'un des $\mathbb{Q}(\zeta_5^+)$, $\mathbb{Q}(\zeta_7^+)$ ou $\mathbb{Q}(\zeta_{11}^+)$, les points d'ordre 3 ne donnant rien ici car $\mathbb{Q}(\zeta_3^+) = \mathbb{Q}$.

La forme de ce diviseur, très particulière, permet de construire très facilement les courbes Y et X en donnant des formes isomorphes, mais plus faciles à calculer. En effet, le diviseur principal $l((P_{\infty,1}) - (P_{\infty,2}))$ est le diviseur d'une fonction de la forme $P(x) + yQ(x)$ telle que sa norme $P^2(x) - H(x)Q^2(x)$ soit une constante, où l'on a noté $y^2 = H(x)$ la fonction définissant la courbe modulaire hyperelliptique.

(◇). On peut aussi consulter, pour des exemples de points de torsion de jacobiennes de courbes modulaires, la thèse de Matt Baker, à l'adresse people.math.gatech.edu/~mbaker/papers.html.

(‡). Si l'on se tient à la formule II.2 que l'on a choisie pour représenter un point de la jacobienne, il s'agit de $2(P_{\infty,1}) - (P_{\infty,1}) - (P_{\infty,2})$, qui est bien le même.

Cela a deux avantages. D'une part, on peut calculer assez facilement une telle fonction, sans utiliser les méthodes liées au théorème de Riemann-Roch. Supposons $H(x)$ unitaire et écrivons

$$x^6 H(\tfrac{1}{x}) = \frac{\left(x^l P(\frac{1}{x})\right)^2 - cx^{2l}}{\left(x^{l-3}Q(\frac{1}{x})\right)^2},$$

où c est la constante telle que $P^2(x) - H(x)Q^2(x) = c$. Par développements limités, on a alors

$$\sqrt{x^6 H(\tfrac{1}{x})} = \frac{x^l P(\frac{1}{x})}{x^{l-3}Q(\frac{1}{x})} - \frac{c}{2}x^{2l} + o(x^{2l}),$$

si bien que les approximants de Padé de $\sqrt{x^6 H(\frac{1}{x})}$ d'ordre $(l, l-3)$ sont $x^l P(\frac{1}{x})$ et $x^{l-3}Q(\frac{1}{x})$, ce qui s'obtient aisément, par exemple par la résolution d'un système linéaire.

D'autre part, par le théorème 90 de Hilbert, à la constante $k = P(x)^2 - H(x)Q(x)^2$ près, la fonction obtenue s'écrit déjà sous la forme $\frac{\varphi(x,y)}{\varphi(x,-y)}$. Ainsi, quitte à multiplier φ par une constante telle que sa norme soit une puissance l-ième, que l'on note κ^l, on a pour Y les équations $\{y^2 = H(x)$ et $t^l = \varphi(x,y)\}$, avec comme automorphismes

$$\alpha : (x, y, t) \mapsto (x, -y, \tfrac{\kappa}{t})$$
$$\sigma : (x, y, t) \mapsto (x, y, \zeta_l t)$$

et $z_t := t + \frac{\kappa}{t}$, l'élément invariant permettant de calculer une équation de X.

Exemple 2.6 (Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ issues des courbes modulaires $X_0(n)$). On finit ce paragraphe en donnant des exemples pour $l = 5$ et 7, les calculs pour les différents l étant d'une difficulté quasi-égale pour la machine.

***l* = 5** On utilise la courbe modulaire $X_0(31)$ et les approximants de Padé donnent

$$\varphi(x, y) = x^5 - 19x^4 + 125x^3 - 328x^2 + 280x - 13 + y(x^2 - 12x + 35)$$

de diviseur $5((P_{\infty,1}) - (P_{\infty,2}))$ et de norme 62^2 permettant de prendre $\kappa = 1$ avec $\frac{\varphi}{62}$. On obtient une équation de X,

$$z g_5(z^2 - 2) = \tfrac{1}{31}(x^5 - 19x^4 + 125x^3 - 328x^2 + 280x - 13)$$

et sous forme hyperelliptique

$$y^2 - \frac{1}{31}y = x^6 + x^5 - \frac{5}{31}x^3 + \frac{4}{31^2}x$$

qui a mauvaise réduction en 5 et en 31.

***l* = 7** Ici, on choisit la courbe modulaire $X_0(29)$. La fonction $\varphi(x, y)$ déterminée par les approximants de Padé

$$x^7 - 13x^6 + 45x^5 + 25x^4 - 269x^3 + 29x^2 + 300x + 166 + (x^4 - 11x^3 + 31x^2 + 14x - 100)y$$

a pour norme $29 \cdot 58^2$, ce qui impose de prendre $\kappa = 29 \neq 1$ et $\tilde{\varphi} = \frac{29^2}{2}\varphi$. Comme X est de genre 3 non-hyperelliptique, on peut la mettre sous forme quartique,

$$\begin{aligned} 841u^4 - 1682u^3v + 116uv^3 + 29v^4 + 841u^3 - 232u^2v \\ + 58uv^2 + 58v^3 - 87u^2 + 58uv - 13v^2 - 58u - 17v + 4 = 0 \end{aligned}$$

qui a mauvaise réduction en 7 et en 29.

D'autres courbes rationnelles ayant des diviseurs rationnels d'ordre l. Outre les courbes modulaires, il existe beaucoup de courbes qui permettent des constructions similaires, aboutissant à des multiplications réelles par $\mathbb{Q}(\zeta_l^+)$, n'appartenant pas, *a priori*, aux familles déjà vues ou mentionnées. On peut citer, entre autres (⊛), les familles à 1 paramètre de courbes de genre 2 possédant des points d'ordre 15 ou 21 exposées par F. Leprévost dans [Lep 91] ou celles présentées dans [Lep 95] du même auteur. On peut alors, comme pour les courbes modulaires, chercher des courbes hyperelliptiques de genre 2 dont le point de la jacobienne $P_{\infty,1}$–$P_{\infty,2}$ est d'ordre fini l. Les outils algorithmiques déjà rencontrés permettent de démontrer les propositions suivantes.

Proposition 2.7. *Les courbes hyperelliptiques de genre* 2*, de la famille à deux paramètres* s *et* t*, d'équation*

$$y^2 = s(16t - 27 + 4s)x^6 + 2s(-16t + 27 + s)x^5 + 10stx^3 + 2t^2x + t^2,$$

sont à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$.

Démonstration. Il s'agit une fois encore de la totalité, à rationalité près, des courbes à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$. Soit $y^2 = x^6 + ax^4 + bx^3 + cx^2 + dx + e$ une courbe hyperelliptique de genre 2 générale. On calcule, sous représentation de Mumford, les diviseurs $2(P_{\infty,1} - P_{\infty,2})$ et $3(P_{\infty,1} - P_{\infty,2})$ dont on égale la première coordonnée (unitaire). Cela nous donne deux équations, le coefficient en x et le coefficient constant, dont on prend le résultant en e. Un des facteurs est de genre 0 que l'on paramètre. On obtient une famille de courbes de genre 2 dont le point $(P_{\infty,1} - P_{\infty,2})$ est d'ordre 5.
$y^2 = 82944x^6+(13824t+3456s-31104)x^4+(1728s-3456t+5184)x^3+(864ts-648s+36s^2+576t^2-2592t+2916)x^2+(-972+216ts-288t^2+1080t-216s+36s^2)x+81+54s-108t+36t^2-108ts+9s^2+48t^2s.$

Il ne reste plus qu'à appliquer la méthode décrite ci-dessus des approximants de Padé pour trouver une fonction φ. Ensuite, on mène les mêmes calculs que ceux expliqués dans l'exemple 2.4 pour trouver le modèle hyperelliptique donné. □

Proposition 2.8. *Les courbes suivantes, de genre* 3 *et d'équations quartiques, sont à multiplication réelle par* $\mathbb{Q}(\zeta_7^+)$*. Elles appartiennent à* 2 *familles, la première à* 1 *paramètre* s*,*

$$2v + u^3 + (u+1)^2 + s\Big((u^2+v)^2 - v(u+v)(2u^2 - uv + 2v)\Big) = 0$$

et la seconde à 2 *paramètres* s *et* t*,*

$-(s+t)^2 + 2(s+t)sv + (-s^2+3t^2-t)v^2 + (6t^2-2t-2s^2)v^3 + 2(s+t)^2u + (6t^2-2t-2s^2)uv^2 + (-s^2+3t^2-t)uv^3 - (s+t)(s-t)u^2 + (2t+2s^2-6t^2)u^2v + (t-3t^2+s^2)u^2v^2 + (s+t)(s-t)u^3 + (2t+2s^2-6t^2)u^3v + (-s^2+3t^2-t)u^4 = 0.$

Démonstration. La situation est un peu plus délicate ici. Pour pouvoir obtenir une condition de genre 0, on commence par considérer une courbe hyperelliptique d'équation $y^2 = f(x) = x^6 + ax^4 + bx^3 + cx^2 + dx$, puis on calcule les approximants de Padé de $\sqrt{\frac{1}{x^6}f(\frac{1}{x})}$ d'ordre $(7,4)$. On les note $\frac{1}{x^7}P(\frac{1}{x})$ et $\frac{1}{x^4}Q(\frac{1}{x})$ si bien que $P(x)^2 - f(x)Q(x)^2$ est un polynôme de degré 2. Le résultant des coefficients en x et x^2 relativement à a possède un facteur de genre 0 que l'on paramètre : on obtient la courbe hyperelliptique à un paramètre t,

$$y^2 = x^6 + \tfrac{2t-1}{2}x^4 + tx^3 + \tfrac{4t^2-12t+1}{16}x^2 + \tfrac{t^2}{2}x$$

dont on peut vérifier directement, par un calcul d'approximation de Padé similaire, que le point $(P_{\infty,1} - P_{\infty,2})$ est bien d'ordre 7.

(⊛). On peut consulter la thèse d'Andreas Schoepp, à l'adresse http://page.math.tu-berlin.de/~kant/publications/diss/Diss_Schoepp.pdf, qui propose une synthèse des familles connues.

Il ne reste plus qu'à calculer l'équation de X comme dans le paragraphe précédent, puis à déterminer une équation quartique, comme expliqué dans la remarque 3.8 du chapitre I et utilisé plusieurs fois depuis le début de ce chapitre. On aboutit à la première famille.

Pour la seconde famille, on part cette fois d'une équation hyperelliptique générale de degré 6, que l'on peut toujours ramener à la forme $y^2 = x^6+ax^5+ax^4+bx^3+cx^2+dx$. En effectuant des calculs similaires d'approximation de Padé, on trouve la famille de courbes à deux paramètres s et t,

$$\begin{aligned} y^2 = x^6 &+ (2t+s)x^5 + (2t+s)x^4 + \left(\tfrac{1}{2}s^2 - ts^2 + 3ts + 4t^2 - 3t^2s - \tfrac{1}{8}s^3 - \tfrac{5}{2}t^3\right)x^3 \\ &+ \left(\tfrac{1}{4}s^2 + \tfrac{1}{64}s^4 - \tfrac{1}{8}s^3 + ts + t^2 - \tfrac{1}{4}ts^2 - \tfrac{1}{2}t^2s^2 - \tfrac{1}{2}t^4 - t^3s\right)x^2 \\ &+ \tfrac{1}{32}t(-4s + s^2 - 8t + 6ts + 6t^2)^2 x, \end{aligned}$$

dont le point $(P_{\infty,1} - P_{\infty,2})$ est d'ordre 7. On finit les calculs comme dans le cas de la première famille, pour aboutir à une équation quartique plane, à deux paramètres. □

Corps finis. Une autre approche consiste à se placer sur les corps finis, ce qui permet d'obtenir des courbes dont la jacobienne possède des points d'ordre l. Voici un algorithme probabiliste, qui fournit, sur $\mathbb{F}_p$, des courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$.

Algorithme II.2 Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ (II)

Entrée : (l, p)

Répéter
  Choisir $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p$
  $H \leftarrow y^2 - x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$
  $n \leftarrow \#\operatorname{Jac}(H) =: J$
Jusqu'à $n \equiv 0 \mod l$
$m \leftarrow \frac{n}{l}$
Répéter
  Choisir $Q \in \operatorname{Jac}(H) \setminus \{O_J\}$.
Jusqu'à $mQ \neq O_H$
$P \leftarrow mQ$ ▷ P est d'ordre l
Calculer $\varphi(x, y)$ telle que $\operatorname{div}(\varphi) = l \operatorname{Div}(P)$
$\Pi \leftarrow \operatorname{Res}_t(\varphi(x,-y)t^l - \varphi(x,y), t^2 + 1 - zt)$
$X \leftarrow \Pi \mod_y H$ ▷ X est un polynôme en x, z.

Sortie : X

Exemple 2.9. Finissons par donner, comme dans le cas précédent, deux exemples.

***l* = 5.** L'algorithme ci-dessus fournit, dans $\mathbb{F}_{31}$, la courbe hyperelliptique H d'équation $y^2 = x(x-1)(x-2)(x+4)(x-5)$ dont la jacobienne possède 1120 éléments. $P = [x(x-7), 20x]$, en représentation de Mumford, est d'ordre 5 et la fonction $x^2(4y + 3x^3 + 7x^2 + 3x$ a comme diviseur $5((0,0,1) + (7,16,1) - 2(0,1,0))$: elle conduit à la courbe X dont on donne une équation hyperelliptique

$$y^2 = (x+18)(x^5 + 7x^4 + x^3 + 25x^2 + 7x + 12).$$

Le polynôme caractéristique de la trace du Frobenius, est $r^2+19r+89$, de discriminant 5 et définissant bien le corps de nombre $\mathbb{Q}(\zeta_5^+) = \mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{Q}(\pi_H)$.

***l* = 7.** Pour $p = 41$, l'algorithme II.2 propose $y^2 = x(x-1)(x-3)(x+7)(x-7)$ pour l'équation de H, dont la jacobienne possède $7 \cdot 240$ points. Parmi eux, en représentation de Mumford, $[(x+5)^2, -2x+16]$, est d'ordre 7. La fonction

$$(x^4 + 22x^3 + 22x^2 + 17x + 24)y + 10x^7 + 20x^6 + 35x^4 + 14x^3 + 40x^2 + 6x + 36$$

a pour diviseur $14((36, 26, 1) - (0, 1, 0))$. On calcule alors une équation de X sur $\mathbb{F}_{41}$, sous forme quartique,

$$u^3v + u^2v^2 + 26uv^3 + 2v^4 + 24u^3 + 11u^2v + 21uv^2 + 2v^3 + 24u^2 + 37uv + 3v^2 + 20u + 11v + 3 = 0.$$

On vérifie à nouveau, par un calcul de fonction zêta, que le polynôme caractéristique de la trace du Frobenius est $r^3 + 21r^2 + 126r + 203$ qui définit le corps de nombres $\mathbb{Q}(\zeta_7^+)$.

— 3 —
Multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$.

Dans toute cette section, nous considérons naturellement des entiers premiers l congrus à 1 modulo 4. De plus, on se place ici plus volontiers sur le corps $k = \mathbb{Q}(i)$ ou éventuellement sur des corps de caractéristique p avec $p \equiv 1 \mod 4$ de façon à encore disposer d'une racine carrée de -1.

3.1 Type (0,1,1)

On a, à nouveau, un zéro dans le type du revêtement : on cherche donc un revêtement $Z \to \mathbb{P}^1$, de degré 4, ramifié en deux points, d'ordre 4 aussi. La formule d'Hurwitz donne

$$g(Z) = \frac{1}{2}\Big(2 + 4(2g(\mathbb{P}^1) - 2) + (4-1) + (4-1)\Big) = 0.$$

Une équation de Z, de genre 0, peut être $y^4 = x$ avec le revêtement de $\mathbb{P}^1$, $(x, y) \mapsto x$, ramifié en 0 et ∞, dont le groupe de Galois est $\mathbb{Z}/4\mathbb{Z}$, engendré par $(x, y) \mapsto (x, iy)$.

On cherche alors un revêtement $Y \to Z$ de groupe $\mathbb{Z}/l\mathbb{Z}$ tel que le revêtement $Y \to \mathbb{P}^1$ soit de type (0,1,1). Comme d'habitude on le cherche sous la forme d'une extension de Kummer $t^l = \varphi(x, y) = \psi(y)$. Comme on travaille au-dessus de $\mathbb{P}^1$, on ne peut pas espérer de ramification annulée par un diviseur dont l'ordre en chacun des points de son support est multiple de l, car sur $\mathbb{P}^1$, seules les puissances l-ièmes ont de tels diviseurs « multiples » de l.

Ainsi, la ramification est donnée exactement par les pôles et les zéros de $\psi(y)$. Comme on ne veut qu'un seul point de ramification au-dessus de $\mathbb{P}^1$, les pôles et les zéros de ψ doivent avoir les mêmes puissances 4^{e}. À homographie près, on a donc essentiellement un seul revêtement convenable, fourni par la proposition suivante.

Proposition 3.1. *Soit* $\psi(y)=\frac{(y-1)(y-i)}{(y+1)(y+i)}$ *et* $a\in\mathbb{Z}$*, d'ordre* 4 *dans* $(\mathbb{Z}/l\mathbb{Z})^*$*. On définit la courbe*

$$(Y)\ \begin{cases} y^4 = x \\ t^l\ = \psi(y)\psi(iy)^a. \end{cases}$$

Alors, le revêtement $Y\to\mathbb{P}^1$ *donné par l'application* $(x,y,t)\mapsto x$ *est de type (0,1,1). De plus, en considérant* k *tel que* $kl-a^2=1$*, les automorphismes*

$$\alpha : (x,y,t)\mapsto (x, iy, t^{-a}\psi(iy)^k)$$
$$\sigma : (x,y,t)\mapsto (x, y, \zeta_l y)$$

engendrent le groupe métacyclique $G_{l,4}$*, groupe de Galois de ce revêtement.*

Démonstration. Commençons par vérifier que le revêtement est bien celui attendu. Le revêtement intermédiaire $(x,y,t)\mapsto(x,y)$ est ramifié en les zéros et pôles de ψ, à chaque fois d'ordre l. On a 4 points de ramification $(1,1)$, $(1,-1)$, $(1,i)$ et $(1,-i)$. Ces quatre points ont même image, 1, par $(x,y)\mapsto x$. Enfin, on a bien une ramification d'ordre 4 au-dessus des points $x=0$ et $x=\infty$. On calcule ensuite

$$\begin{aligned}\psi(iy)\psi(i\cdot iy)^\alpha = \psi(-y)^\alpha\psi(iy) &= \psi(y)^{-\alpha}\psi(iy)^{kl-a^2}\\ &= \big(\psi(y)\psi(iy)\big)^{-a}\psi(iy)^{kl} = \Big(t^{-a}\psi(iy)^k\Big)^l,\end{aligned}$$

ce qui montre l'existence du morphisme α, d'ordre 4 (on vérifie aisément que $\alpha^2:(x,y,t)\mapsto(x,-y,\frac{1}{t})$). Quant à σ, il découle comme d'habitude de la forme des extensions de type Kummer. Il reste à montrer que ces deux morphismes engendrent bien $G_{l,4}$. Pour cela, on effectue le calcul suivant.

$$\begin{aligned}\alpha\sigma\alpha^{-1}(x,y,t) = \alpha\sigma(x,-iy,t^a\psi(iy)^{-k}) &= \alpha(x,-iy,\zeta_l^a t^a\psi(iy)^{-k})\\ &= (x,y,\zeta_l^a t) = \sigma^a(x,y,t).\end{aligned}$$ □

Il reste à déterminer une équation de $X=Y/\langle\alpha\rangle$ de façon analogue à ce que l'on a vu pour le type $(0,1,1,1,1)$, quoiqu'un peu plus délicat. En effet, il s'agit de calculer le polynôme minimal d'un élément stabilisé par α, par exemple

$$z_t := t+\alpha(t)+\alpha^2(t)+\alpha^3(t) = t+t^{-a}\psi(iy)^k+t^{-1}+t^a\psi(iy)^{-k}.$$

On en déduit un algorithme partageant des techniques avec l'algorithme II.1, en se plaçant sur $\mathbb{Q}(i)$, c'est-à-dire en introduisant un élément i et la relation $i^2=-1$.

Algorithme II.3 Courbe à multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$ (I)

Entrée : l

1: **Factoriser** $u^2+1 \mod l$ et choisir a, une racine.
2: $\psi(y)\leftarrow(y-1)(y-i)/(y+1)/(y+i)$
3: $\Pi(y,z)\leftarrow \mathrm{Res}_t\left(t^l-\psi(y)\psi(iy)^a, t+t^{-a}\psi(iy)^k+t^{-1}+t^a\psi(iy)^{-k}-z\right)$
4: $X(x,z)\leftarrow \Pi(y,z) \mod_y y^4-x$

Sortie X.

Notons l'abus de notation de la ligne 3 : on prend le résultant des numérateurs des quantités décrites, et comme pour chaque calcul de résultant, il est possible qu'il faille éliminer les facteurs non pertinents. Enfin, pour la ligne 4, Π est par construction un polynôme invariant par α et donc n'a nécessairement que des puissances 4^{e} de y, ce qui justifie le fait que X soit un polynôme en x et z uniquement.

Exemple 3.2. On choisit $l = 13$ et $a = 5$ d'ordre 4 dans $(\mathbb{Z}/13\mathbb{Z})^*$ et on travaille sur $\mathbb{Q}(i)$. On trouve comme équation de Y

$$(Y)\begin{cases} y^4 = x \\ t^{13} = \dfrac{(y+i)^4(y-1)^6}{(y-i)^4(y+1)^6} \end{cases}$$

puis une équation de X, de genre 3,

$(x-1)^6z^{13}-26(x-1)^6z^{11}+221(x-1)^6z^9-104(x^2+14x+1)(x-1)^4z^8-26(31x^2-126x+31)(x-1)^4z^7+884(x^2+14x+1)(x-1)^4z^6+26(31x^2+66x+31)(x-1)^4z^5+52(-37x^4-380x^3+256ix^3+1858x^2-380x-256ix-37)(x-1)^2z^4+52(25x^4+252x^3+4566x^2+252x+25)(x-1)^2z^3-416(x^4-44x^3+32ix^3-810x^2-44x-32ix+1)(x-1)^2z^2+13(5x^4-1684x^3+15646x^2-1684x+5)(x-1)^2z-4+4824x-141312ix^4+5120ix^5-5120ix+141312ix^2+4824x^5+42180x^4-4x^6-356144x^3+42180x^2=0.$

Cette dernière, non hyperelliptique possède une équation quartique plus simple,

$$u^3 + 2u^2v + 2u^2 - uv^3 - 2uv^2 - 2uv - 2u + v^4 + v^2 - v + 2 = 0.$$

En réduisant par exemple cette équation dans $\mathbb{F}_{53}$, on trouve une jacobienne d'une courbe non supersingulière, dont le polynôme caractéristique de la trace du Frobenius,

$$r^3 - 6r^2 - 40r - 8$$

définit le corps de nombres $\mathbb{Q}(\zeta_{13}^{(4)})$. On a choisi expressément $p = 53$ de façon à ce que $\mathbb{F}_p$ possède les racines 13^{e} de l'unité. La table II.3, rassemble quelques exemples de polynômes caractéristiques de la trace du Frobenius pour des réductions de X dans divers $\mathbb{F}_p$.

Table II.3 Polynômes caractéristiques pour des réductions de courbes X à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$ sur des corps finis (I).

$\mathbb{F}_p$	Ordre de $l \in (\mathbb{Z}/13\mathbb{Z})^*$	Polynôme caractéristique de la trace du Frobenius
53	1	$r^3 - 6r^2 - 40r - 8$
181	2	$r^3 + 39r^2 + 416r + 689$
73	4	$r^3 - 12r^2 - 43r + 3269$
29	3	$r^3 - 87r - 80$, $(t^6 - 80t^3 + 29^3)$
17	6	$r^3 - 51r - 52$, $(t^6 - 52t^3 + 17^3)$
37	12	$r^3 - 111r - 306$, $(t^6 - 306t^3 + 37^3)$

Pour les trois premières lignes, on a en fait $\zeta_{13}^{(4)} \in \mathbb{F}_p$ et les trois polynômes caractéristiques définissent le corps de nombres $\mathbb{Q}(\zeta_{13}^{(4)})$. Par contre, on voit pour les trois dernières lignes que la courbe devient supersingulière. On vérifie, en calculant le résultant en x des polynômes caractéristiques $P(x)$ et $z - x^k$, que sur une extension de degré $k = 3$, on obtient en fait des jacobiennes isogènes à un produit de 3 courbes elliptiques identiques. On peut aussi le vérifier sur le polynôme caractéristique de la trace du Frobenius. Par exemple

$$\mathrm{Res}_x(x^6 - 80x^3 + 29^3, z - x^3) = (z^2 - 80z + 29^3)^3,$$
$$\mathrm{Res}_t(t^3 - 87t - 80, \mathrm{Res}_x(z - x^3, tx - x^2 - 29) = -(z^2 - 80z + 29^3)^3.$$

Dès lors, $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X))$ contient au moins l'algèbre $\mathscr{M}_3(\mathbb{Q})$ qui, comme on l'a vu en 2.4 grâce aux matrices compagnons, contient tous les corps de nombres de degré 3, et en particulier $\mathbb{Q}(\zeta_{13}^{(4)})$. On remarque enfin que dans ces trois cas, $\zeta_{13}^{(4)} \in \mathbb{F}_{l^3}$, extension minimale, de degré 3.

3.2 Type (1,1,2,2)

On cherche ici un recouvrement $H \to \mathbb{P}^1$ de degré 4, ramifié en 4 points, deux d'ordre 2 et deux d'ordre 4. On peut calculer le genre de H par la formule d'Hurwitz, même s'il y a plusieurs possibilités. En effet, pour la ramification d'ordre 2, on peut avoir 2 points d'ordre 2 dans la fibre ou 1 point d'ordre 2 et deux autres points. Pour des raisons de parité, cela laisse deux possibilités

$$g(H) = \tfrac{1}{2}(2 + 4(2g(\mathbb{P}^1) - 2) + 2(4-1) + 4(2-1)) = 2$$

ou

$$g(H) = \tfrac{1}{2}(2 + 4(2g(\mathbb{P}^1) - 2) + 2(4-1) + 2(2-1)) = 1.$$

La deuxième possibilité ne nous intéresse pas ici car on veut ensuite un revêtement non ramifié d'ordre l, qui serait alors encore une courbe elliptique, ce qui n'est pas possible pour Y.

Proposition 3.3. *Soit $\tau \in \mathbb{Q}$ un paramètre, différent de 2 et -2. et soit H la courbe hyperelliptique de genre 2, d'équation $y^2 = x(x^4 + \tau x^2 + 1)$. Alors, l'application $(x, y) \mapsto x^2$ est un revêtement de $\mathbb{P}^1$, de degré 4 et de type $(1, 1, 2, 2)$. Son groupe de Galois est $\mathbb{Z}/4\mathbb{Z}$, engendré par l'automorphisme $(x, y) \mapsto (-x, iy)$.*

Démonstration. Ce revêtement est ramifié en 0 et ∞, de degré 4. De plus, notons ω une racine de $x^4 + \tau x^2 + 1$. Alors, les quatre racines distinctes ($\tau \neq \pm 2$) sont $\pm\omega$ et $\pm\frac{1}{\omega}$. On a une ramification d'ordre 2 en ces points de Weierstrass, et l'application $(x, y) \mapsto x^2$ identifie ces points par paires : le revêtement est ramifié en deux points supplémentaires, ω^2 et $\frac{1}{\omega^2}$, d'ordre 2, en plus des points 0 et ∞ d'ordre 4. □

Ici, le groupe d'automorphismes de H est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, avec $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^3})$ en plus. Néanmoins, l'automorphisme $(x, y) \mapsto (-\frac{1}{x}, i\frac{y}{x^3})$ est d'ordre 4, mais ne convient pas ici car il ne stabilise pas les fibres.

La suite peut se traiter de manière similaire au type $(1, 1, 1, 1, 1, 1)$, en construisant un revêtement non ramifié d'ordre l grâce à un point de $\mathrm{Jac}(H)$ d'ordre l. En fait, la situation est ici bien simplifiée par l'existence d'un morphisme non constant de H vers une courbe elliptique E, quotient de H par le groupe d'ordre 2 engendré par $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^3})$. La jacobienne de H est isogène à un produit de deux courbes elliptiques isomorphes à E. C'est en fait un cas particulier, pour $l = 2$ des courbes qui apparaissent dans [TTV 91] et que l'on a croisées en 2.1. On vérifie de manière immédiate la proposition suivante.

Proposition 3.4. *Il existe un morphisme entre la courbe H et la courbe elliptique E d'équation $Y^2 = (X + 2)(X^2 + \tau - 2)$. Il est donné par les équations (affines)*

$$\begin{aligned} X &= x + \frac{1}{x} \\ Y &= \frac{y(x+1)}{x^2}. \end{aligned} \tag{II.3}$$

Ce morphisme repose essentiellement sur l'identité $x(X + 2) = (x + 1)^2$, qui relie x et X à un carré près. En changeant les signes, on a aussi $x(X - 2) = (x - 1)^2$, ce qui donne la deuxième courbe isomorphe E' d'équation $Y'^2 = (X - 2)(X^2 + \tau - 2)$, avec $Y' = \frac{y(x-1)}{x^2}$ et l'isomorphisme $(X, Y) \mapsto (-X, iY)$. On se sert de la courbe elliptique E pour construire un revêtement non ramifié de H de degré l.

Proposition 3.5. *Soit P un point de E d'ordre l et soit $a \in \mathbb{Z}$ d'ordre 4 dans $(\mathbb{Z}/l\mathbb{Z})^*$. On considère une fonction $\varphi(X,Y)$ de diviseur $l((P)-(O_E))$ et $\psi(x,y)$ la fonction correspondante sur H. On définit alors la courbe*

$$(Y)\ \begin{cases} y^2 = x(x^4+\tau x^2+1) \\ t^l\ = \psi(x,y)\psi(-x,iy)^a. \end{cases}$$

Alors, le revêtement $Y \to \mathbb{P}^1$, $(x,y,t) \mapsto x^2$ est de type $(1,1,2,2)$, de groupe de Galois $G_{l,4}$, engendré par les automorphismes

$$\alpha : (x,y,t) \mapsto (-x, iy, t^{-a}\psi(-x,iy)^k \Phi(x)^a)$$
$$\sigma : (x,y,t) \mapsto (x,y,\zeta_l t)$$

où k est tel que $kl - a^2 = 1$, et $\Phi(x)$ est une fonction que l'on précisera.

Démonstration. Comme $lP = O_E = lO_E$ le diviseur $l((P)-(O_E))$ est principal, ce qui justifie l'existence de φ puis ψ par composition avec le morphisme (II.3). Comme $\psi(x,y)\psi(x,-y)$ est stable par l'involution hyperelliptique, c'est une fonction de x seulement, dont le diviseur, vu sur $\mathbb{P}^1$, ne possède que des points d'ordre l. C'est donc nécessairement le diviseur d'une puissance l-ième, que l'on note $\Phi(x)^l$.

Le revêtement $Y \to H$ est non ramifié, car le diviseur de $\psi(x,y)\psi(-x,iy)^a$ a par construction un support « multiple » de l. C'est un revêtement habituel de type Kummer, de degré l et de groupe de Galois $\mathbb{Z}/l\mathbb{Z}$. Ainsi, la composition par le revêtement $H \to \mathbb{P}^1$ est bien du type annoncé $(1,1,2,2)$. Pour justifier que ce revêtement composé est galoisien de groupe de Galois $G_{l,4}$ on montre que l'automorphisme de H de degré 4 se « remonte » sur Y,

$$\begin{aligned} \psi(-x,iy)\psi(x,-y)^a &= \psi(-x,iy)\psi(x,y)^{-a}\Phi(x)^{al} \\ &= \Big(\psi(x,y)\psi(-x,iy)^a\Big)^{-a}\psi(-x,iy)^{kl}\Phi(x)^{al} \\ &= \Big(t^{-a}\psi(-x,iy)^k\Phi(x)^a\Big)^l \end{aligned}$$

ce qui justifie l'existence de l'automorphisme α. On calcule enfin

$$\begin{aligned} \alpha\sigma\alpha^{-1}(x,y,t) &= \alpha\sigma(-x,-iy,t^a\psi(-x,iy)^{-k}\Phi(-x)) \\ &= \alpha(-x,-iy,\zeta_l^a t^a\psi(-x,iy)^{-k}\Phi(-x)) = (x,y,\zeta_l^a t) = \sigma^a(x,y,t). \ \square \end{aligned}$$

Le calcul d'une équation de la courbe $X/\langle\alpha\rangle$ se fait comme précédemment en calculant le polynôme minimal d'un élément invariant par $\langle\alpha\rangle$, par exemple

$$z_t := \sum_{i=0}^{3} \alpha^i(t) = t + t^{-a}\psi(-x,iy)^k\Phi(x)^a + \frac{\Phi(x)\Phi(-x)^a}{t} + t^a\psi(-x,iy)^{-k}\Phi(-x).$$

Pour calculer une équation de X, on prend $\mathrm{Res}_t(z - z_t, t^l - \psi(x,y)\psi(-x,iy)^a)$, qui est invariant par $(x,y) \mapsto (-x,iy)$ et donc par $y \mapsto -y$; on élimine y en prenant le reste modulo $y^2 - x(x^4+\tau x^2+1)$. Le résultat est invariant par $x \mapsto -x$ et une équation de X s'obtient en prenant le reste par $w - x^2$. Le tout aboutit à la proposition suivante.

Proposition 3.6. *Les courbes construites ci-dessus sont une famille à un paramètre, τ, dont la jacobienne est à multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$.*

Démonstration. Il suffit de trouver une fonction ψ qui provient d'un point de l-–torsion de E, donné par une racine du polynôme de l–division. On peut aussi utiliser $X_1(l)$ qui paramétrise les courbes elliptiques possédant un point de l–torsion. $\square$

Si comme dans le cas 2.3 tous les calculs exposés ci-dessus sont explicites, ils semblent exiger une puissance trop importante à l'heure actuelle. On peut toutefois en tirer un algorithme qui fournit des courbes à multiplications réelles par $\mathbb{Q}(\zeta_l^{(4)})$ sur un corps fini $\mathbb{F}_p$, aléatoirement parmi cette famille à 1 paramètre. Pour s'assurer que les courbes sont définies sur $\mathbb{F}_p$ on choisit $p \equiv 1 \mod 4$ afin de disposer d'une racine carrée de -1 dans $\mathbb{F}_p$. Enfin, une difficulté peut venir de Φ : définie à partir d'un diviseur, on peut avoir $\varphi(x,y)\varphi(x,-y) = k\Phi(x)^l$. Mais alors, il suffit de remplacer φ par $\tilde{\varphi} = k^{\frac{l-1}{2}}\varphi$. Ce détail réglé, on en déduit l'algorithme suivant.

Algorithme II.4 Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^{(4)})$ (II)

Entrée : l, p

1: **Factoriser** $u^2 + 1 \mod l$ et choisir a, une racine.
2: **Répéter**
3: **Choisir** $\tau \in \mathbb{F}_p$
4: $E \leftarrow Y^2 - (X+2)(X^2 + \tau - 2)$
5: **Jusqu'à** $\#E \equiv 0 \mod l$
6: **Choisir** $P \in E[l] \setminus \{O_E\}$
7: **Calculer** $\varphi(x,y)$ vérifiant $\mathrm{div}(\varphi) = l((P)-(O_E))$ de coefficient dominant adéquat
8: $\psi(x,y) \leftarrow \varphi(x + \frac{1}{x}, \frac{y(x+1)}{x^2})$ et $\Phi(x) \leftarrow (x + 1/x - x_P)$
9: $\Pi \leftarrow \mathrm{Res}_t(z - z_t, t^l - \psi(x,y)\psi(-x,iy)^a)$
10: $X(w,z) \leftarrow \left(\Pi \mod_y y^2 - x(x^4 + \tau x^2 + 1)\right) \mod_x w - x^2$

Sortie X.

Exemple 3.7. On donne, dans la table II.4, des équations quartiques à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$ pour différentes valeurs de p. On fournit dans la table II.5 les polynômes caractéristiques du Frobenius, permettant de vérifier que les courbes obtenues sont à multiplication complexe par une extension quadratique de $\mathbb{Q}(\zeta_{13}^{(4)})$.

Table II.4 Quartiques à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$ sur des corps finis.

$\mathbb{F}_p$	τ	Équation quartique
53	7	$u^4 + 42u^3v + 38u^2v^2 + 5uv^3 + 7v^4 + 37u^3 + 26u^2v + 37uv^2 + 24v^3 + 13u^2 + 41uv + 37v^2 + 21u + 40v + 26 = 0$
181	24	$u^4 + 28u^3v + 5u^2v^2 + 152uv^3 + 99v^4 + 151u^3 + 126u^2v + 22uv^2 + 34v^3 + 92u^2 + 158uv + 157v^2 + 74u + 140v + 61 = 0$
73	32	$u^4 + 71u^3v + 3u^2v^2 + 5uv^3 + 70v^4 + 70u^3 + 13u^2v + 49uv^2 + 56v^3 + 20u^2 + 32uv + 18v^2 + 39u + 59v + 68 = 0$
29	19	$u^4 + 4u^3v + 26u^2v^2 + 3uv^3 + 7v^4 + 12u^3 + 24u^2v + 28uv^2 + 26v^3 + 5u^2 + 6uv + 3v^2 + 24u + 22v + 17 = 0$
101	15	$u^4 + 37u^3v + 85u^2v^2 + 77uv^3 + 97v^4 + 65u^3 + 10u^2v + 57uv^2 + 13v^3 + 100u^2 + 67uv + 86v^2 + 75u + 12v + 54 = 0$
41	3	$u^4 + 19u^3v + 4u^2v^2 + 2uv^3 + 5v^4 + 28u^3 + 11u^2v + 33v^3 + 17u^2 + 30uv + 29v^2 + 32v + 29 = 0$

Dans les trois premières lignes de la table II.5, $\zeta_{13}^{(4)}$ est dans le corps de base $\mathbb{F}_p$: le corps de rupture du polynôme caractéristique du Frobenius est bien une extension quadratique de $\mathbb{Q}(\zeta_{13}^{(4)})$. Dans les trois dernières lignes, on obtient une courbe supersingulière dont la jacobienne, sur une extension de degré 3, est isogène au cube d'une courbe elliptique.

Table II.5 Polynômes caractéristiques pour des réductions de courbes X à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$ sur des corps finis (II).

$\mathbb{F}_p$	Ordre de $l \in (\mathbb{Z}/13\mathbb{Z})^*$	τ	Polynôme caractéristique de la trace du Frobenius
53	1	7	$r^3 + 20r^2 + 77r - 46$
181	2	24	$r^3 + 26r^2 + 13r - 1625$
73	4	32	$r^3 + 40r^2 + 529r + 2315$
29	3	19	$r^3 - 87r + 63$, $(t^6 + 63t^3 + 29^3)$
101	6	17	$r^3 - 303r + 286$, $(t^6 + 286t^3 + 101^3)$
41	12	12	$r^3 - 123r - 30$, $(t^6 - 30t^3 + 41^3)$

— 4 —
Multiplication réelle par $\mathbb{Q}(\zeta_l^{(k)})$ pour $k = 6, 8$ et 10.

On peut donner un traitement similaire à la section 3.2, notamment dans la manière de construire la courbe Y comme une extension de Kummer d'un produit de fonctions, où l'on fait agir l'automorphisme de la première courbe, afin d'obtenir une extension *globalement* galoisienne. Ainsi, dans le cas 3.2 on a dû considérer la fonction $\psi(x, y)\psi(-x, iy)^a$ et non pas $\psi(x, y)$. Ici, on peut faire de même, avec respectivement 3, 6, 4 et 5 facteurs pour les types $(2, 2, 3, 3)$, $(1, 1, 2)$, $(1, 1, 4)$ et $(1, 2, 5)$.

On propose à la place d'utiliser dans la mesure du possible, les propriétés, notamment liées à la multiplication complexe, de la courbe sur laquelle on considère l'extension de Kummer.

Pour les deux sections suivantes, l'indice est 6 et on considère des entiers premiers l congrus à 1 modulo 6. On se place sur $\mathbb{Q}(j)$ avec $j^3 = 1$, ou sur des corps finis de caractéristique $p \equiv 1 \mod 3$ de manière à disposer d'une racine 3^{e} de l'unité.

4.1 Type (2,2,3,3)

On commence encore une fois par la formule d'Hurwitz pour trouver un revêtement $H \to \mathbb{P}^1$ de degré 6, ramifié en 4 points, de type (2,2,3,3),

$$2g(H) - 2 = 6(2g(\mathbb{P}^1) - 2 + r(3 - 1) + s,$$

où $r \in \{1, 2, 3, 4\}$ est le nombre de points ramifiés dans les fibres d'ordre 3 et $s \in \{2, 4, 6\}$ est le nombre de points ramifiés dans les fibres d'ordre 2, nécessairement

pair, d'après cette même formule d'Hurwitz. Cela impose donc $g(H) \in \{0,1,2\}$ et comme on veut ensuite un revêtement non ramifié d'ordre l, on a nécessairement $r = 4$ et $s = 6$ de façon à obtenir $g(H) = 2$.

Proposition 4.1. *Soit $\tau \notin \{-2,2\}$ un paramètre et soit H la courbe hyperelliptique de genre 2, définie par l'équation*

$$y^2 = x^6 + \tau x^3 + 1.$$

Alors, l'application $H \to \mathbb{P}^1$, $(x,y) \mapsto x^3$ est un revêtement de type $(2,2,3,3)$, de degré 6, tout comme l'automorphisme

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

qui engendre le groupe de Galois, $\mathbb{Z}/6\mathbb{Z}$, de ce revêtement.

Démonstration. Soient ω et ω' les racines non nulles et distinctes de $z^2 + \tau z + 1$. Le revêtement $(x,y) \mapsto x^3$ est ramifié en $0, \infty, \omega$ et ω'. La fibre au-dessus de 0 est constituée des deux points $(0, \pm 1)$ tout comme celle au-dessus de ∞ constituée des deux points à l'infini. Les fibres au-dessus de ω et ω' sont quant à elles constituées de 3 points de Weierstrass chacune. □

De façon similaire à la construction associée au type $(1,1,2,2)$ on peut utiliser le fait que $\mathrm{Jac}(H)$ est le produit de deux courbes elliptiques $Y^2 = (X \pm 2)(X^3 - 3X + \tau)$ pour construire le revêtement de degré l, non ramifié.

Proposition 4.2. *Soit P un point de E d'ordre l et soit $a \in \mathbb{Z}$, d'ordre 3 dans $(\mathbb{Z}/l\mathbb{Z})^*$. On considère une fonction $\varphi(X,Y)$ de diviseur $l((P) - (O_E))$ et $\psi(x,y)$ la fonction correspondante sur H. On définit alors la courbe*

$$(Y) \begin{cases} y^2 = (x^6 + \tau x^3 + 1) \\ t^l = \psi(x,y)\psi(jx,y)^a \psi(j^2 x, y)^{a^2}. \end{cases}$$

Alors, le revêtement $Y \to \mathbb{P}^1$, $(x,y,t) \mapsto x^3$ est de type $(2,2,3,3)$, de groupe de Galois $G_{l,6}$, engendré par les automorphismes

$$\alpha : (x,y,t) \mapsto \left(jx, -y, t^{-a^2}\psi(jx,y)^k \psi(j^2x,y)^{ak} \Phi(jx)\Phi(j^2x)^a \Phi(x)^{a^2}\right)$$
$$\sigma : (x,y,t) \mapsto (x,y,\zeta_l t)$$

où k est tel que $a^3 = 1 + kl$, et $\Phi(x)$ est une fonction que l'on précisera.

Pour calculer l'équation de $Y = X/\langle\alpha\rangle$, on procède de façon usuelle :

$$\Pi(x,y,z) := \mathrm{Res}_t\left(z - \sum_{r=0}^{5} \alpha^r(t), z^l - \prod_{r=0}^{2} \psi(j^r x, y)^{a^r}\right)$$

qui est un polynôme invariant par $(x,y) \mapsto (jx,-y)$: c'est donc un polynôme en y^2 et x^3 et l'équation de X est donnée par

$$X(w,z) = \Pi(x,y,z) \mod_{x,y} [y^2 - (x^6 + \tau x^3 + 1), x^3 - w].$$

Ceci montre, comme dans le cas 3.2, la proposition suivante.

Proposition 4.3. *Les courbes construites ci-dessus sont une famille à un paramètre, τ, dont la jacobienne est à multiplication réelle par $\mathbb{Q}(\zeta_l^{(6)})$.*

Utilisation des sous-groupes stables. Toutefois, comme on l'a évoqué dans l'introduction de cette section, on peut « simplifier » la courbe Y en cherchant un point sur la jacobienne de $y^2 = x^6 + \tau x^3 + 1$ dont le groupe engendré est stable par $\alpha : (x, y) \mapsto (jx, -y)$. Sur les corps finis, on l'utilise dans l'algorithme suivant.

Algorithme II.5 Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^{(6)})$

Entrée : l, p

Répéter
  Choisir $\tau \in \mathbb{F}_p$
  $J \leftarrow \mathrm{Jac}(x^6 + \tau x^3 + 1)$
Jusqu'à $\exists P \in J$ tel que $\langle P \rangle$ soit stable par α
Calculer a tel que $\alpha(P) = aP$
Calculer $\varphi(x, y)$ vérifiant $\mathrm{div}(\varphi) = l\,\mathrm{Div}(P)$
Calculer $\Phi(x, y)$ tel que $\mathrm{div}(\Phi) = \alpha(P) - aP$
Définir $\alpha' : (x, y, t) \mapsto (jx, -y, \Phi(x, y)t^a)$
$\Pi \leftarrow \mathrm{Res}_t \left(z - \sum_{r=0}^{5} \alpha'^r(t), z^l - \varphi(x, y) \right)$
$X(w, z) \leftarrow \Pi \mod_{x,y} [x^2 - w, y^2 - (x^6 + \tau x^3 + 1)]$

Sortie X.

Exemple 4.4. On finit cette section en regardant deux exemples. Dans le premier, on considère le cas $l = 13$. On applique l'algorithme précédent pour différentes caractéristiques p et on regroupe les résultats dans la table II.6 donnant les équations courbes hyperelliptiques et les polynômes caractéristiques.

Table II.6 Polynômes caractéristiques pour des réductions de courbes X à multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(6)})$ sur des corps finis.

$\mathbb{F}_p$	Ordre de $l \in (\mathbb{Z}/13\mathbb{Z})^*$	τ	Équation hyperelliptique de X Polynôme caractéristique de la trace du Frobenius
79	1	15	$y^2 = x^6 + 34x^5 + 30x^4 + 65x^3 + 46x^2 + 30x + 9$ $r^2 - 4r - 9$
103	2	17	$y^2 = 3x^6 + 94x^5 + 67x^4 + 83x^3 + 63x^2 + 93x + 23$ $r^2 - 13r + 39$
139	3	17	$y^2 = 2x^6 + 77x^5 + 61x^4 + 104x^3 + 118x^2 + 91x + 137$ $r^2 + 27r + 101$
127	6	12	$y^2 = 3x^6 + 20x^5 + 106x^4 + 125x^3 + 34x^2 + 73x + 63$ $r^2 + 26r + 156$
31	4	7	$y^2 = 3x^6 + 24x^5 + 7x^4 + 17x^3 + 14x^2 + 21x + 15$ $r^2 - 75$, $(t^4 - 13t^2 + 31^2)$
37	12	14	$y^2 = x^6 + 26x^5 + 31x^4 + 2x^3 + 9x^2 + 34x + 9$ $r^2 - 100$, $(t^4 - 26t^2 + 37^2)$

Pour les ordres de $p \in (\mathbb{Z}/13\mathbb{Z})^*$ divisant 6, le polynôme caractéristique du Frobenius définit un corps de nombres qui est une extension quadratique de $\mathbb{Q}(\zeta_{13}^{(6)})$. Dans les

deux autres cas, ce sont des jacobiennes de courbes supersingulières, qui se scindent en un produit de deux courbes elliptiques sur une extension de degré 2.

Dans un second temps, on spécifie $\tau = 0$, mais pour $l \equiv 1 \mod 3$ général. Dans ce cas (⋆), H, d'équation $y^2 = x^6 + 1$, possède une jacobienne non simple dont on peut prendre comme facteur elliptique $Y^2 = X^3 + 1$, avec $Y = y$ et $X = x^2$.

Cette courbe elliptique est à multiplication complexe par $\mathbb{Q}(j)$. Comme on a $l \equiv 1 \mod 3$, l'idéal (l) est décomposé dans $\mathbb{Q}(j)$. On écrit $a + bj$ un de ces facteurs et on voit E comme $\mathbb{C}/(\mathbb{Z} + j\mathbb{Z})$. Parmi les points de l–torsion de E, le sous-groupe engendré par $\frac{a+jb}{l}$ est stable par multiplication par j. Cela veut dire que le polynôme de l–division de E se scinde sur $\mathbb{Q}(j)$, possédant deux facteurs de degré $\frac{l-1}{2}$, dont le produit est un polynôme à coefficients dans $\mathbb{Q}$ de degré $l-1$. On note $P_l = (x_0, y_0)$ un point de l–torsion, dont x_0 est racine de ce polynôme. Les coordonnées de P_l sont donc dans un corps de nombres degré $2l - 2$. On considère ensuite, comme précédemment une fonction $\varphi(X, Y)$ de diviseur $l((P_l) - (O_E))$, puis la fonction $\psi(x, y) = \varphi(x^2, y)$ sur H. Cette fonction nous permet, comme expliqué précédemment de considérer la courbe Y d'équation

$$(Y) \begin{cases} y^2 = (x^6 + 1) \\ t^l \ = \psi(x, y). \end{cases}$$

Pour $l = 13$, les calculs aboutissent et donnent les deux propositions suivantes. Notons que la courbe hyperelliptique de genre 2 que l'on obtient possède des invariants absolus définis sur $\mathbb{Q}(j)$.

Proposition 4.5. *Soit x_0 une racine du polynôme $x^6 + (12j + 8)x^3 + \frac{1}{13}(48j + 64)$ et y_0 tel que $y_0^2 = x_0^3 + 1$. Alors, le point (x_0, y_0) de la courbe elliptique $y^2 = x^3 + 1$ est d'ordre 13, et le sous-groupe qu'il engendre contient (jx_0, y_0).*

Proposition 4.6. *La courbe hyperelliptique d'équation*
$Y^2 = \big(X + (\frac{1}{468}(-110j - 115)x_0^5 + \frac{1}{234}(-451j + 289)x_0^2)y_0\alpha + (\frac{1}{156}(67j + 47)x_0^5 + \frac{1}{39}(73j - 85)x_0^2)y_0\big)\big(X + (\frac{1}{936}(653j + 337)x_0^5 + \frac{1}{234}(314j - 1331)x_0^2)y_0\alpha + (\frac{1}{24}(47j + 19)x_0^5 + \frac{1}{6}(5j - 110)x_0^2)y_0\big)\big(X^2 + ((\frac{1}{312}(-128j - 57)x_0^5 + \frac{1}{78}(-29j + 300)x_0^2)y_0\alpha + (\frac{1}{72}(-58j - 11)x_0^5 + \frac{1}{18}(35j + 166)x_0^2)y_0)X + (\frac{1}{13}(22j + 23)x_0^4 + (10j - 1)x_0)\alpha + \frac{1}{52}(283j + 196)x_0^4 + \frac{1}{13}(124j - 245)x_0\big)\big(X^2 + ((\frac{1}{936}(227j + 76)x_0^5 + \frac{1}{117}(-11j - 265)x_0^2)y_0\alpha + (\frac{1}{72}(11j - 8)x_0{}^5 + \frac{1}{9}(-20j - 28)x_0^2)y_0)X + (\frac{1}{52}(j - 22)x0^4 + 1/13(-53j - 4)x_0)\alpha + \frac{1}{26}(-21j - 45)x_0^4 + \frac{1}{13}(-201j - 24)x_0\big)$
est à multiplication réelle par $\mathbb{Q}(\sqrt{13})$.

Dans les trois dernières sections qui suivent, on a simplement l'existence d'une courbe et non plus une famille de courbes. Une fois les revêtements $H \to \mathbb{P}^1$ déterminés, on peut obtenir sans peine la courbe Y puis le quotient X de manière analogue aux types $(1, 1, 2, 2)$ et $(2, 2, 3, 3)$. Les fonctions dont on prend les racines l-ième dans l'extension de Kummer sont de degré trop important, pour pouvoir être utilisées, même sur les corps finis. On propose ici d'utiliser, comme exposé ci-dessus, des points de l–torsion stables par certains automorphismes de la courbe H.

(⋆). On ne pouvait pas utiliser cela dans la section précédente du fait que l'on obtient nécessairement une fonction $\varphi(x, y)$ en x^2 faisant tomber l'ordre de $(x, y) \mapsto (-jx, y)$ à 3.

4.2 Type (1,1,2)

On commence comme précédemment avec la formule d'Hurwitz : si $H \mapsto \mathbb{P}^1$ est un revêtement de degré 6 de type $(1,1,2)$, alors on a aussi deux possibilités ;

$$g(H) = \tfrac{1}{2}(2 + 4(2g(\mathbb{P}^1) - 2) + 2(6-1) + 2(3-1)) = 2$$

ou

$$g(H) = \tfrac{1}{2}(2 + 4(2g(\mathbb{P}^1) - 2) + 2(6-1) + (3-1)) = 1.$$

On écarte la deuxième solution pour les mêmes raisons que dans le type $(1,1,2,2)$.

Proposition 4.7. *Soit H la courbe hyperelliptique d'équation $y^2 = x^6 - 1$, de genre 2. On définit un revêtement de $\mathbb{P}^1$ par $(x,y) \mapsto y$. Il est de type $(1,1,2)$, de degré 6, comme l'automorphisme $(x,y) \mapsto (-jx, y)$ qui engendre son groupe de Galois.*

Démonstration. Le revêtement est ramifié en les y tels que $y^2 - 1$ vaut 0 ou ∞, c'est-à-dire pour $y = \pm 1$, qui sont ramifiés d'ordre 6, et pour $y = \infty$ dont la fibre se compose des deux points à l'infini de H, d'ordre 3. On a donc bien un revêtement de type $(1,1,2)$. □

La courbe hyperelliptique H n'est pas simple et on peut adapter le résultat de la section précédente 3.2 pour trouver un revêtement de degré l non ramifié ainsi que le quotient explicite X.

On se propose, à la place, de chercher un point de la jacobienne de H qui soit d'ordre l tel que son sous-groupe soit stable par l'action du groupe de Galois $\alpha : (x,y) \mapsto (-jx, y)$. En effet, si l'on dispose d'un tel point P alors, on a une fonction $\varphi(x,y)$ dont le support est l fois celui du « diviseur » de ce point, au sens où on l'a défini par la formule (II.2). Le fait que le groupe engendré par ce point P est stable par l'automorphisme α assure que l'on peut trouver $a \in \mathbb{Z}$ d'ordre 6 dans $(\mathbb{Z}/l\mathbb{Z})^*$ tel que $\alpha(P) = aP$, ce qui montre l'existence d'une fonction $\Phi(x,y)$ telle que

$$\varphi(-jx, y) = \varphi(x,y)^a \Phi(x,y)^l.$$

Cela nous permet de considérer simplement la courbe

$$(Y) \begin{cases} y^2 = x^6 + 1 \\ t^l = \varphi(x,y). \end{cases}$$

ainsi que le revêtement $Y \to \mathbb{P}^1$, $(x,y,t) \mapsto y$, qui est de type $(1,1,2)$, de groupe de Galois $G_{l,6}$ et qui engendré par les automorphismes

$$\alpha : (x,y,t) \mapsto \big(-jx, y, t^a \Phi(x,y)\big)$$
$$\sigma : (x,y,t) \mapsto (x, y, \zeta_l t).$$

Pour déterminer une équation plane du quotient X, on prend le résultant

$$\mathrm{Res}_t\Big(t^l - \varphi(x,y), z - \sum_{i=0}^{5} \alpha^i(t)\Big).$$

C'est un polynôme en y, z et x^6, dont il suffit de considérer le reste en x par $x^6 = y^2 + 1$, pour obtenir une équation plane de X en les variables y et z.

Exemple 4.8. Dans le cas $l = 13$, on vérifie sans mal, à l'aide d'un logiciel tel Magma [Mag 13], la proposition suivante.

Proposition 4.9. *Soit x_0 une racine du polynôme $x^{24} - 4x^{18} + 6x^{12} - \frac{13}{64}x^6 + \frac{13}{256}$ et y_0 vérifiant $y_0^2 = x_0^6 - 1$. Alors, le point de la jacobienne*

$$P := (x_0, y_0) + (-x_0, -y_0) - P_{\infty,1} - P_{\infty,2}$$

est d'ordre 13 et vérifie de plus, en notant $\alpha(P) = (jx_0, -y_0) + (-jx_0, y_0) - P_{\infty,1} - P_{\infty,2}$, $\alpha(P) = 4P$, où l'on a choisi $j = \frac{1}{81}(-128x_0^{18} + 528x_0^{12} - 780x_0^6 - 25)$.

Remarque 4.10. Pour aboutir à ce résultat, on utilise le logiciel Magma, qui, via la commande `EndomorphismRing`, donne l'anneau des endomorphismes de la jacobienne « analytique » de la courbe H d'équation $y^2 = x^6 - 1$. Dès lors, il suffit de chercher un point du réseau dont l'action par l'endomorphisme de degré 6 soit la multiplication par $a = 4$ par exemple. Cela se fait en résolvant des équations linéaires en des entiers. Ensuite, on repasse à la jacobienne algébrique par la fonction `FromAnalyticJacobian`, puis on détermine, à l'aide de Pari [GP 13] et `algdep` par exemple, une extension dans laquelle pourraient être définies les cordonnées des points ainsi trouvés. Cela permet d'écrire le genre d'énoncé de la proposition ci-dessus, que l'on peut ensuite vérifier de façon algébrique, directement. Si les calculs pour déterminer X semblent demander trop de puissance, on peut néanmoins utiliser cette proposition sur les corps finis. En effet, pour $p = 139$, tout est défini sur $\mathbb{F}_p$ et on trouve finalement pour équation de X la courbe hyperelliptique

$$y^2 = 2x^6 + 106x^5 + 21x^4 + 13x^3 + 77x^2 + 92x.$$

Le polynôme caractéristique de la trace du Frobenius est $r^2 + 12r - 16$, de discriminant réduit $4 \cdot 13$, d'où la multiplication réelle par $\mathbb{Q}(\sqrt{13})$.

4.3 Type (1,1,4)

Ici, on considère $l \equiv 1 \mod 8$. On travaille sur des corps possédant une racine carrée de i, que l'on note ζ_8, c'est-à-dire sur $\mathbb{Q}(\zeta_8)$ ou, par exemple, sur des corps finis de caractéristique p congru à 1 modulo 8. On veut un recouvrement de degré 8, ramifié en trois points, deux d'ordre 8 et un d'ordre 2. La formule d'Hurwitz donne

$$g(H) = \frac{1}{2}\Big(2 + 8(2g(\mathbb{P}^1 - 2) + 2(8 - 1) + k(2 - 1)\Big)$$

avec $k \in \{2, 4\}$ le nombre de points dans la fibre au-dessus du troisième point de ramification, nécessairement pair. La seule possibilité, pour avoir ensuite un revêtement non ramifié d'ordre l avec $g(H) \neq 1$, est $k = 4$ et $g(H) = 2$.

Proposition 4.11. *Soit H la courbe hyperelliptique de genre 2, définie par l'équation $y^2 = x^5 + x$. Alors le revêtement $H \to \mathbb{P}^1$, $(x, y) \mapsto x^4$ est de type $(1, 1, 4)$, de degré 8 tout comme l'automorphisme $(x, y) \mapsto (ix, \zeta_8 y)$, qui engendre son groupe de Galois.*

Démonstration. En effet, ce revêtement est ramifié en $0, \infty$ et 1. Pour les deux premiers, la fibre ne comporte qu'un seul point, respectivement $(0, 0)$ et le point à l'infini. En -1, la fibre comporte les quatre points de Weierstrass restants, identifiés par $(x, y) \mapsto x^4$. □

Comme précédemment, H n'est pas simple et on peut encore utiliser les mêmes techniques pour construire un revêtement non ramifié Y, puis le quotient X.

On peut aussi adapter l'algorithme II.5 afin d'utiliser un revêtement Y « plus simple », du type exposé à la section précédente. Notons d'une part que la jacobienne de $y^2 = x^5+x$ peut posséder un point d'ordre l sur $\mathbb{F}_p$, sans que ses facteurs elliptiques n'en possèdent. D'autre part, si le nombre de points sur $\mathbb{F}_p$ de la jacobienne est de la forme kl avec l ne divisant pas k, alors, on est sûr que le sous-groupe d'ordre l est stable par $\alpha : (x, y) \mapsto (ix, \zeta_8 y)$. Enfin, pour trouver un point d'ordre l, on peut utiliser des « tordues » de H, d'équations $y^2 = x^5 + ax$.

Exemple 4.12. Pour $l = 17$, à l'aide de Magma et de façon similaire à la section précédente, on aboutit à la proposition suivante.

Proposition 4.13. *Soit H la courbe hyperelliptique $y^2 = x^5 + x$. Il existe un point P de la jacobienne de H, défini en représentation de Mumford sur une extension de degré 64, d'ordre 17 tel que $\alpha(P) = -2P$. Il est défini en langage Magma, à l'adresse* www.normalesup.org/~iboyer/files/pt17stable.m.

Exemple 4.14. Pour $p = 137$, la jacobienne de la courbe hyperelliptique $y^2 = x^5 + 3x$ possède $2 \cdot 17^2 \cdot 41$ points sur $\mathbb{F}_p$. On vérifie que le point, en représentation de Mumford, $P = (x^2 + 41x + 11, 98x + 84)$, est d'ordre 17, et satisfait $\alpha(P) = -2P$. On trouve finalement pour X la courbe hyperelliptique de genre 2

$$y^2 = x^6 + 10x^5 + 3x^4 + 103x^3 + 20x^2 + 10x + 120$$

et le polynôme caractéristique de la trace du Frobenius, $r^2 - 9 \cdot 17$, définit, malgré des apparences « supersingulières », le corps de nombres $\mathbb{Q}(\sqrt{17})$.

Comme on l'a déjà remarqué, le sous-groupe des points d'ordre 41 est nécessairement stable par α, et on vérifie par exemple que pour $P = (x^2 + 70x + 60, 84x + 18)$, on a $\alpha(P) = 3P$. Cela nous permet de calculer une équation de X de genre 5, à multiplication réelle par $\mathbb{Q}(\zeta_{41}^{(8)})$. Le calcul est très rapide, alors qu'il serait certainement impossible en utilisant les techniques exposées dans les sections 3.2 et 4.1. On obtient une courbe de genre 5 que l'on peut exprimer comme l'intersection de 3 quadriques sur $\mathbb{P}^4$. Il suffit, comme on l'a déjà fait plusieurs fois avec les courbes de genre 3, de résoudre des équations linéaires en les coefficients d'une quadrique homogène générale en 5 variables, que l'on évalue sur une base de différentielles holomorphes. Parmi les quadriques que l'on trouve, on en choisit 3 « indépendantes », ce que l'on peut vérifier en calculant, par exemple, la dimension de leur intersection dans $\mathbb{P}^4$. On trouve les équations quadriques suivantes en a, b, c et d, de degré total 2.

$$\begin{aligned}
q_1(a,b,c,d) &= ac + 105ad + 118b^2 + 107bc + 136bd + 126c^2 + 113cd + 98d^2 \\
&\quad + 132a + 40b + 47c + 69d + 1 \\
q_2(a,b,c,d) &= ab + 77ad + 101b^2 + 17bc + 45bd + 131c^2 + 36cd + 69d^2 \\
&\quad + 121a + 113c + 33d + 14 \\
q_3(a,b,c,d) &= a^2 + 122ad + 107b^2 + 132bc + 65bd + 90c^2 + 111cd + 47d^2 \\
&\quad + 91a + 131b + 73c + 128d + 59
\end{aligned}$$

4.4 Type (1,2,5)

Pour ce dernier cas, on a nécessairement $l \equiv 1 \mod 10$. On travaille sur des corps possédant une racine cinquième de l'unité, que l'on note ζ_5, c'est-à-dire sur $\mathbb{Q}(\zeta_5)$ ou, par exemple, sur des corps finis de caractéristique p congrue à 1 modulo 5.

On veut ici un recouvrement de degré 10, ramifié en trois points, d'ordre 10, 5 et 2. La formule d'Hurwitz nous donne

$$g(H) = \frac{1}{2}\Big(2 + 10(2g(\mathbb{P}^1 - 2) + (10 - 1) + r(5 - 1) + s(2 - 1)\Big)$$

avec $r \in \{1, 2\}$ le nombre de points dans la fibre au-dessus du point de ramification d'ordre 5 et $s \in \{1, 3, 5\}$ pour la fibre d'ordre 2, nécessairement impair. La seule possibilité, pour avoir ensuite un revêtement non ramifié d'ordre l qui ne soit pas une courbe elliptique, est $r = 2$, $s = 5$ pour $g(H) = 2$.

Proposition 4.15. *Soit H la courbe hyperelliptique de genre 2, définie par l'équation $y^2 = x^5 + 1$. Alors le revêtement $H \to \mathbb{P}^1$, $(x, y) \mapsto y^2$ est de type $(1, 2, 5)$, de degré 10 tout comme l'automorphisme $(x, y) \mapsto (\zeta_5 x, -y)$, qui engendre son groupe de Galois.*

Démonstration. En effet, ce revêtement est ramifié en 0, ∞ et 1. En 0, la fibre comporte les 5 points de Weierstrass $((-\zeta_5)^k, 0)$, en 1, la fibre est composée des deux points $(-1, 0)$ et $(1, 0)$ tandis qu'en l'infini, la fibre ne comporte que le dernier point de Weierstrass, le point à l'infini. □

À partir d'un point d'ordre l sur la jacobienne de H, on trouve une fonction $\psi(x, y)$ sur H dont chacun des points du diviseur est d'ordre multiple de l. Comme précédemment, on cherche des points qui sont stables par $\alpha : (x, y) \mapsto (\zeta_5 x, -y)$, le signe moins sur l'ordonnée s'obtenant par $[-1]$ sur la jacobienne.

La jacobienne de la courbe H est simple, à multiplication complexe par $\mathbb{Q}(\zeta_5)$, ce qui facilite beaucoup la recherche d'un tel point. Comme expliqué dans G. Shimura et Y. Taniyama [Shi 98], ainsi que dans la section 3 du chapitre III, la jacobienne de H peut être vue comme $\mathbb{C}^2/\Phi(\mathscr{O})$ où $\mathscr{O}$ est l'anneau des entiers de $\mathbb{Q}(\zeta_5)$ et Φ est donné par le type-CM. On vérifie que le réseau

$$\begin{pmatrix} \zeta_5 & \zeta_5^3 & 1 & \zeta_5^2 + 1 \\ \zeta_5^2 & \zeta_5^6 & 1 & \zeta_5^4 + 1 \end{pmatrix}$$

convient. Soit maintenant l un nombre premier vérifiant de plus $l \equiv 1 \mod 10$. Alors, l'idéal (l) est décomposé dans $\mathbb{Q}(\zeta_5)$. Soit a d'ordre 5 dans $(\mathbb{Z}/l\mathbb{Z})^*$, si bien que l'idéal $(\zeta_5 - a)$ possède un facteur premier, et principal, (π) qui divise (l). Ainsi,

$$\frac{\zeta_5}{\pi} = \frac{a}{\pi} \mod \mathscr{O}$$

si bien que le point de la jacobienne $\frac{1}{\pi}$ est d'ordre l, et le sous-groupe qu'il engendre est stable par la multiplication complexe par ζ_5. Grâce à ce point de la jacobienne, on construit une fonction $\varphi(x, y)$ dont le diviseur est l fois le diviseur de ce point, au sens (II.2). On peut alors prendre simplement comme extension $t^l = \varphi(x, y)$ puisque par construction, on a l'existence d'une fonction $f(x, y)$ vérifiant

$$\varphi(\zeta_5 x, y) = \varphi(x, y)^a f(x, y)^l$$

et on en déduit, de façon classique sur les ordonnées, une fonction $\Phi(x, y)$ telle que

$$\varphi(\zeta_5 x, -y) = \varphi(x, y)^a \Phi(x, y)^l.$$

Le revêtement de H par la courbe Y, définie par l'extension de Kummer $t^l = \varphi(x, y)$, donne un revêtement total sur $\mathbb{P}^1$ galoisien dont le groupe de Galois $G_{l,10}$ est engendré par les automorphismes

$$\alpha : (x, y, t) \mapsto \left(\zeta_5 x, -y, t^a \Phi(x, y)\right)$$
$$\sigma : (x, y, t) \mapsto (x, y, \zeta_l t).$$

On obtient ensuite, comme depuis le début, la courbe X en prenant le résultant

$$\mathrm{Res}_t \left(t^l - \varphi(x, y), z - \sum_{i=0}^{5} \alpha^i(t)\right).$$

Ce résultant s'exprime en y^2 et x^5, ce qui fournit l'équation de X en prenant le reste par $y^2 - (x^5 + 1)$ d'une part, puis par $x^5 - w$ d'autre part.

Exemple 4.16. Dans un premier temps, on cherche des points de la jacobienne de $y^2 = x^5 + 1$ d'ordre l et dont le sous-groupe engendré est stable par la multiplication complexe. On donne la proposition suivante pour $l = 11$ et $l = 31$, qui se vérifie facilement avec Magma par exemple.

Proposition 4.17. *Les points suivants engendrent des groupes d'ordre l, stables par $(x, y) \mapsto (\zeta_5 x, y)$.*

1. *On considère $l = 11$ et soit γ une racine de $t^5 + \frac{1}{121}(80\zeta_5^3 + 320\zeta_5^2 + 1040\zeta_5 + 1264)$ et δ une racine de $t^2 + \frac{1}{11}(-36\zeta_5^3 - 12\zeta_5^2 - 28\zeta_5 + 1)$. Alors, le point*

$$P = \left(t^2 + \tfrac{1}{4}(\zeta_5^3 + 2\zeta_5)\gamma^3 t + \gamma, \tfrac{1}{22}(-\zeta_5^3 + \zeta_5^2 + 8\zeta_5 - 6)\gamma^2 \delta t + \delta\right)$$

   est d'ordre 11 et vérifie $\alpha(P) = 2P$.

2. *On considère $l = 31$. Il existe un point P de la jacobienne de $y^2 = x^5 + 1$, donné en représentation de Mumford sur une extension de degré 120, tel que $31P = 0$ et $\alpha(P) = -2P$. Sa définition est donnée à l'adresse* www.normalesup.org/~iboyer/files/pt31stable.m*, dans le langage Magma.*

Toutefois, le degré des extensions considérées semble trop important pour calculer un modèle plan de la courbe X. Néanmoins, on peut utiliser ces résultats pour réduire les calculs sur $\mathbb{F}_p$. Notons que l'on peut aussi utiliser les jacobiennes des courbes $y^2 = x^5 + a$ dont le nombre de points sur $\mathbb{F}_p$ est divisible par l mais pas par l^2.

Exemple 4.18. Pour $l = 31$, on se place pour $\mathbb{F}_{61}$. La jacobienne de $y^2 = x^5 + 8$ possède $11^2 \cdot 31$ points, ce qui assure la stabilité du sous-groupe d'ordre 31. On trouve pour X l'équation quartique

$$u^4+30u^3v+2u^2v^2+26uv^3+41v^4+46u^3+50u^2v+37uv^2+17v^3+14u^2+21uv+16v^2+35u+8v+32 = 0$$

dont le polynôme caractéristique de la trace du Frobenius est

$$r^3 + 34r^2 + 375r + 1334,$$

définit le corps de nombres $\mathbb{Q}(\zeta_{31}^{(10)})$.

— 5 —
Résumé des résultats

Pour terminer ce chapitre résumons dans la table II.7 les principaux résultats obtenus ci-dessus, concernant des courbes explicites à multiplication réelle dont J. Ellenberg montre l'existence dans [Ell 01].

Table II.7 Courbes explicites à multiplication réelle par des sous-corps de cyclotomiques

n, l	Courbes exposées	Corps de définition	Existence théorique
$\mathbb{Q}(\zeta_l^+)$	famille à 1 paramètre [TTV 91] famille à 2 paramètres famille à 3 paramètres	$\mathbb{Q}$ $\mathbb{Q}$ extension	famille à 3 paramètres
$\mathbb{Q}(\zeta_l^{(4)})$	1 courbe famille à 1 paramètre	$\mathbb{Q}(i)$ extension	famille à 1 paramètre
$\mathbb{Q}(\zeta_l^{(6)})$	famille à 1 paramètre 1 courbe	extension extension	famille à 1 paramètre
$\mathbb{Q}(\zeta_l^{(8)})$	1 courbe	extension	1 courbe
$\mathbb{Q}(\zeta_l^{(10)})$	1 courbe	extension	1 courbe

Factorisation dans $\mathbb{F}_p[t]$ et multiplication complexe

Nous présentons ici un algorithme de factorisation des polynômes cyclotomiques sur les corps finis, en temps polynomial, déterministe en la caractéristique du corps.

Sommaire

On connaît des algorithmes efficaces qui permettent de factoriser dans $\mathbb{F}_p[t]$. Sans s'étendre sur les notions de complexité, on dit qu'un algorithme de factorisation d'un polynôme $P \in \mathbb{F}_p[t]$ s'exécute *en temps polynomial*, si son exécution nécessite un nombre d'opérations élémentaires sur $\mathbb{F}_p$ borné par un polynôme en $\deg(P)$ et $\log(p)$. Ici, c'est bien entendu le caractère polynomial en $\log(p)$ qui est crucial. On sous-entend toujours par algorithme, un *algorithme déterministe*, sauf quand on mentionne explicitement *algorithme probabiliste*.

Sur $\mathbb{F}_p$, pour p « petit », on peut citer par exemple l'algorithme de Berlekamp, assez efficace. Néanmoins, il ne s'exécute pas en temps polynomial car il fait appel à une boucle sur les éléments de $\mathbb{F}_p$, qui le rend ainsi impraticable pour p grand. On connaît des algorithmes probabilistes en temps polynomial, et en acceptant l'hypothèse de Riemann généralisée, certains deviennent déterministes.

Néanmoins, la question reste ouverte quant à l'existence d'algorithmes de factorisation sur $\mathbb{F}_p$ déterministes, en temps polynomial. On propose ici un point de vue un peu différent, semblable à celui que R. Schoof expose à la fin de [Sch 85] : on *fixe* un polynôme sur $\mathbb{Q}[t]$ et on cherche la factorisation de sa réduction sur $\mathbb{F}_p[t]$. On rappelle le théorème suivant, qui justifie que l'on ne s'occupe dans la suite que des polynômes cyclotomiques.

Théorème 0.1 (Kronecker–Weber). *Toute extension galoisienne de $\mathbb{Q}$ est contenue dans un corps cyclotomique.*

Voici aussi un résultat élémentaire dont on se sert tout au long de ce chapitre.

Proposition 0.2. *Soit p et l deux nombres premiers distincts, $m \geqslant 1$ un entier et f l'ordre de p dans $\mathbb{Z}/l^m\mathbb{Z}$. Alors, le polynôme cyclotomique $\Phi_{l^m}(t)$ se factorise sur $\mathbb{F}_p[t]$ en $\frac{l^{m-1}(l-1)}{f}$ polynômes irréductibles de degré f.*

Enfin, mentionnons que l'on ne considère que la complexité en $\log p$: même si cette complexité paraît efficace, la plupart des algorithmes que l'on présente ne sont que théoriques, d'un temps d'exécution impraticable pour des degrés de polynômes à factoriser élevés. Dans le même esprit, on s'autorise des pré-calculs — ne dépendant pas de p — aussi longs que l'on veut : tant qu'ils sont en temps fini, ils sont négligeables devant $\log(p)$.

Algorithme de Schoof pour les racines carrées. Pour les polynômes de degré 2, soit l'extraction de racines carrées, on n'a pas d'algorithme polynomial, déterministe. Le plus proche que l'on ait est une conséquence de l'algorithme de R. Schoof [Sch 85] qui permet, étant donné une courbe elliptique, de compter le nombre de ses points rationnels, en temps polynomial en $\log(p)$. À la fin de son article, R. Schoof a ajouté une application pour l'extraction de racines carrées dans $\mathbb{F}_p$, en temps polynomial en $\log(p)$. Malheureusement, cela nécessite de construire une courbe elliptique dépendant du nombre dont on doit extraire la racine. On ne peut donc pas espérer en déduire des énoncés meilleurs que, par exemple, « *il existe un algorithme polynomial en* $\log(p)$ *qui extrait la racine carrée de* -1 *dans* $\mathbb{F}_p$ ».

Racines l-ièmes de l'unité. On cherche donc ici à généraliser l'algorithme de R. Schoof, c'est-à-dire, *étant fixé un polynôme*, le factoriser dans $\mathbb{F}_p[t]$, en temps polynomial en $\log(p)$. J. Pila, dans [Pil 90], propose dans cette veine, une généralisation de l'algorithme de Schoof aux variétés abéliennes et comme Schoof, il donne une application à l'extraction de racines l-ièmes de l'unité. Les deux principaux résultats que J. Pila obtient dans son article [Pil 90], en 1989, sont les théorèmes suivants.

Théorème 0.3 (Pila, 1989). *On se donne une variété abélienne A définie par des équations sur $\mathbb{F}_q$ et des équations donnant sa loi de groupe. Alors, il existe un algorithme déterministe qui fournit le nombre des points $\mathbb{F}_q$-rationnels de A, en temps polynomial en* $\log(q)$.

De ce théorème, J. Pila en tire la possibilité de calculer la fonction zêta d'une variété abélienne en temps polynomial, et donc le corollaire suivant.

Corollaire 0.4. *On se donne un nombre premier impair l fixé et soit p un autre nombre premier tel que $p \equiv 1 \mod l$. Alors, il existe un algorithme déterministe et polynomial en* $\log(p)$ *qui scinde le polynôme $t^l - 1 \in \mathbb{F}_p[t]$.*

Pour démontrer ce corollaire, J. Pila utilise la courbe de Fermat $X^l + Y^l + Z^l$. La jacobienne de cette dernière n'est pas simple et sa dimension est assez élevée. De plus, cette courbe ne se prête pas beaucoup à la généralisation.

On se propose, afin de généraliser ce résultat, d'utiliser, comme T. Honda [Hon 66], la courbe hyperelliptique

$$y^2 = x^l - 1, \qquad (\mathscr{H}_l)$$

ce qui fait l'objet de la section suivante. On voit ensuite comment généraliser ce résultat, en utilisant d'autres courbes hyperelliptiques similaires. Enfin, dans une dernière section, on propose quelques pistes de généralisation, avec notamment l'étude d'une courbe de genre 3 à multiplication complexe par $\mathbb{Q}(\zeta_{13}^{(4)}, i)$, que l'on construit et dont on démontre qu'elle est bien à multiplication complexe par ce corps, à l'aide d'une correspondance.

— 1 —
Multiplication complexe de $\mathscr{H}_l$

La courbe hyperelliptique $\mathscr{H}_l$, définie ci-dessus, est souvent étudiée pour les nombreuses propriétés de sa jacobienne, notamment en théorie de la multiplication complexe qui lui est conférée par l'automorphisme

$$[\zeta_l] : (x, y) \mapsto (\zeta_l x, y)$$

où on note ζ_l une racine l-ième primitive de l'unité et Φ_l le polynôme cyclotomique de degré $l-1$, polynôme minimal de ζ_l. Dans la suite, on utilise toujours le plongement $\mathbb{Q}(\zeta_l) \hookrightarrow \mathbb{C}$, $\zeta_l \mapsto \exp(\frac{2i\pi}{l})$, et on note encore $\zeta_l = \exp(\frac{2i\pi}{l})$. On trouve, tout au long d'*Abelian Varieties with Complex Multiplication* [Shi 98], des exemples liés à cette courbe.

1.1 Type-CM et simplicité de Jac($\mathscr{H}_l$)

La proposition suivante généralise l'exemple 2.13 du chapitre I, où $l = 5$.

Proposition 1.1. *On note $\mathbb{Q}(\zeta_l)$ le corps cyclotomique de degré $l-1$. La jacobienne de la courbe hyperelliptique $\mathscr{H}_l$ définie par l'équation $y^2 = x^l - 1$ est simple et possède une multiplication complexe par $\mathbb{Q}(\zeta_l)$, de type-CM*

$$\left\{\varphi_i,\ 1 \leqslant i \leqslant \tfrac{l-1}{2}\right\}, \tag{III.1}$$

où l'automorphisme $\varphi_i : \mathbb{Q}(\zeta_l) \to \mathbb{C}$ est défini par $\varphi_i(\zeta_l) = \zeta_l^i$.

Démonstration. En effet, l'automorphisme $[\zeta_l] : (x, y) \mapsto (\zeta_l x, y)$ sur la courbe $\mathscr{H}_l$ induit un élément de $\mathrm{End}_{\mathbb{Q}}(A)$ de polynôme minimal Φ_l, ce qui assure que $\mathrm{End}_{\mathbb{Q}}(A)$ contient le corps $\mathbb{Q}(\zeta_l)$ de degré $l-1$ et Jac($\mathscr{H}_l$) est de dimension $n = \frac{l-1}{2}$. De plus, le sous-corps $\mathbb{Q}(\zeta_l^+) \subset \mathbb{Q}(\zeta_l)$ engendré par $\zeta_l + \zeta_l^{-1}$ est totalement réel et $\mathbb{Q}(\zeta_l)$ en est une extension quadratique totalement imaginaire. Le type-CM se calcule en utilisant la base de différentielles

$$\left\{x^i \frac{\mathrm{d}x}{y}, \quad i = 0, \cdots, \frac{l-3}{2}\right\},$$

par la formule

$$[\zeta_l]^* x^i \frac{\mathrm{d}x}{y} = \zeta_l^{i+1} x^i \frac{\mathrm{d}x}{y} = \varphi_{i+1}(\zeta_l) x^i \frac{\mathrm{d}x}{y}.$$

Il reste à démontrer que la jacobienne de $\mathscr{H}_l$ est simple, autrement dit que son type-CM est primitif. Le groupe de Galois de $\mathbb{Q}(\zeta_l)$ est le groupe cyclique $\mathbb{Z}/(l-1)\mathbb{Z}$ dont les éléments sont donnés par les restrictions des φ_i à $\mathbb{Q}(\zeta_l)$. On est donc dans le cas abélien de la remarque 2.20 du chapitre I : supposons donc que φ_k stabilise le type-CM calculé précédemment c'est-à-dire

$$\left\{\varphi_k \circ \varphi_1, \ldots, \varphi_k \circ \varphi_{\frac{l-1}{2}}\right\} = \left\{\varphi_1, \ldots, \varphi_{\frac{l-1}{2}}\right\}$$

ce qui donne, en sommant les exposants, modulo l

$$k\sum_{i=1}^{\frac{l-1}{2}} i \equiv \sum_{i=1}^{\frac{l-1}{2}} i \mod l.$$

Ainsi, puisque $\frac{l^2-1}{8}$ est premier à l, on a $k \equiv 1$ modulo l, c'est-à-dire $\varphi_k = \mathrm{id}$, qui est donc le seul élément stabilisant le type-CM, ce qui montre que ce dernier est primitif et termine la démonstration en vertu de la proposition 2.18 et de la remarque 2.20 sur les extensions abéliennes. □

1.2 Réduction de $\mathrm{Jac}(\mathscr{H}_l)$ modulo p

L'idée principale de R. Schoof, et développée par J. Pila en dimension supérieure, est de considérer une variété abélienne à multiplication complexe par un corps adéquat, de réduire cette variété abélienne modulo p et de calculer sa fonction zêta. Le Frobenius ainsi déterminé, il est possible de trouver les racines souhaitées. C'est ce que l'on explique dans la fin de cette section.

Dans la suite, on ne considère que des jacobiennes de courbes hyperelliptiques. Ainsi, par un théorème d'Igusa [Igu 56] (voir aussi T. Honda [Hon 66]), si la réduction C' d'une courbe C modulo p est non singulière, alors (⋆), la réduction de la jacobienne de C modulo p est la jacobienne de C'.

Ici, $\mathscr{H}_l$, comme toute courbe hyperelliptique de genre au moins 2, possède un point singulier à l'infini. Néanmoins, on peut facilement désingulariser ce point, en recollant $\mathscr{H}_l$ et la courbe isomorphe $y^2 = x - x^{l+1}$, grâce à $(x, y) \mapsto (\frac{1}{x}, y/(x^{\frac{l+1}{2}}))$. De plus, le discriminant de $x^l + 1$ est $(-1)^{\frac{l-1}{2}} l^l$, non nul pour p premier distinct de l. Sur le modèle non-singulier, on peut ainsi appliquer le théorème cité ci-dessus, pour montrer que sa réduction est la désingularisation de la réduction du modèle non singulier.

Ainsi, pour tout p premier impair distinct de l, on considère naturellement les réductions modulo p de $\mathscr{H}_l$, en notant que l'anneau des endomorphismes s'injecte dans celui de la jacobienne réduite. Ces courbes sont de genre $n = \frac{l-1}{2}$.

Soit maintenant un nombre premier p impair tel que $p \equiv 1$ modulo l. Ainsi, p est totalement décomposé dans $\mathbb{Q}(\zeta_l)$ et si l'on note $\mathfrak{P}$ un idéal premier au-dessus de p alors,

$$(p) = \prod_{i=1}^{2n} \varphi_i(\mathfrak{P}).$$

On note π le morphisme de Frobenius de la jacobienne, notée $\mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_l)$, réduction modulo p de la jacobienne de $\mathscr{H}_l$. On note enfin $[\zeta_{l,p}]$ le morphisme $(x, y) \mapsto (\zeta_{l,p}x, y)$ où $\zeta_{l,p}$ est une racine primitive l-ième de l'unité dans $\mathbb{F}_p$.

Proposition 1.2 (Honda [Hon 66]). *On note $\mathbb{Q}[\pi]$ la $\mathbb{Q}$-algèbre engendrée par le Frobenius. Alors, c'est un corps et*

$$\mathbb{Q}[\pi] \simeq \mathbb{Q}(\zeta_l).$$

(⋆). Le résultat est en fait un peu plus fort mais c'est cette situation simple qui nous intéresse. Notons par ailleurs que la réduction de $\mathrm{Jac}(C)$ peut exister tandis que C dégénère mais ce n'est pas non plus la situation ici.

Démonstration. Tout d'abord, on remarque que la $\mathbb{Q}$-algèbre $\mathbb{Q}([\zeta_{l,p}])$ est de dimension $2n = l-1$ dans $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_l))$ et donc, d'après la proposition 2.3, son commutant est elle-même. Or,

$$\begin{aligned}[\zeta_{l,p}] \circ \pi(x,y) = \left(\zeta_{l,p}x^p, y^p\right) &= \left((\zeta_{l,p}x)^p, y^p\right) \\ &= \pi \circ [\zeta_{l,p}](x,y)\end{aligned}$$

car comme $p \equiv 1$ modulo l, on a $\zeta_{l,p}^p = \zeta_{l,p}$. Ainsi, le Frobenius commute avec $[\zeta_{l,p}]$ et donc $\pi \in \mathbb{Q}([\zeta_{l,p}])$. Comme le polynôme minimal de $\zeta_{l,p}$ est le polynôme cyclotomique Φ_l, cette $\mathbb{Q}$-algèbre est un corps isomorphe à $\mathbb{Q}(\zeta_l)$.

Il reste à voir pourquoi π engendre le corps $\mathbb{Q}(\zeta_l)$ tout entier en montrant que (π) n'est pas un idéal d'un sous-corps propre de $\mathbb{Q}(\zeta_l)$. Pour cela, en rappelant (*cf.* proposition 1.1) que l'on a noté $\{\varphi_1, \ldots, \varphi_n\}$ le type-CM de $\mathrm{Jac}(\mathscr{H}_l)$ et donc celui de $\mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_l)$ aussi, on utilise un des théorèmes principaux de G. Shimura et Y. Taniyama [Shi 98, th. 1, chap III] qui décrit l'idéal (π) :

$$(\pi) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}), \tag{III.2}$$

pour un certain idéal $\mathfrak{P}$ de $\mathbb{Q}(\zeta_l)$ au-dessus de (p). Supposons dès lors que (π) soit invariant par un certain φ_k. Comme (p) est totalement décomposé, l'action de φ_k sur les idéaux premiers au-dessus de (p) est transitive. Alors, on aura, d'après la décomposition (III.2), et par unicité de celle-ci,

$$\left\{\varphi_1^{-1}, \ldots, \varphi_n^{-1}\right\} = \left\{\varphi_k \circ \varphi_1^{-1}, \ldots, \varphi_k \circ \varphi_n^{-1}\right\}$$

soit encore, en composant par φ_k^{-1} et en prenant l'inverse,

$$\{\varphi_i \circ \varphi_k\} = \{\varphi_i\}.$$

Comme le type-CM est primitif, cela permet de conclure, comme dans la démonstration de la proposition 1.1, que φ_k est l'identité et que (π) n'est pas un idéal d'un sous-corps propre de $\mathbb{Q}(\zeta_l)$. □

1.3 Propriété de séparation et algorithme de factorisation

Il reste à voir comment utiliser ces résultats pour trouver les racines primitives l-ième de l'unité modulo p, pour $p \equiv 1 \mod l$.

Afin de ne pas donner toutes les définitions en double, on ne suppose plus cette congruence vérifiée et on note f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$. On note alors $K_0 \subset \mathbb{Q}(\zeta_l)$ le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$, d'indice f et de degré $g = \frac{l-1}{f}$. On note enfin $\{\psi_1, \ldots, \psi_g\}$ les éléments du groupe de Galois $\mathrm{Gal}(K_0/\mathbb{Q})$.

Avant d'introduire une propriété de « séparation » des idéaux premiers par le Frobenius, il nous faut modifier la formule (III.2), qui n'est valable que pour $f = 1$. C'est en fait la décomposition de l'idéal (π^f) qui nous est aussi donnée par G. Shimura et Y. Taniyama, dans [Shi 98]. Pour l'utiliser, il faut tout d'abord remarquer que cette fois, c'est π^f qui est bien un élément de $\mathbb{Q}([\zeta_{l,p}]) \simeq \mathbb{Q}(\zeta_l)$:

$$\begin{aligned}[\zeta_{l,p}] \circ \pi^f(x,y) = \left(\zeta_{l,p}x^{p^f}, y^{p^f}\right) &= \left((\zeta_{l,p}x)^{p^f}, y^{p^f}\right) \\ &= \pi^f \circ [\zeta_{l,p}](x,y)\end{aligned}$$

car cette fois, c'est p^f qui est congru à 1 modulo l et donc $\zeta_{l,p}^{p^f} = \zeta_{l,p}$. Notons, au passage, que l'endomorphisme $[\zeta_{l,p}]$ n'est plus défini sur $\mathbb{F}_p$ mais sur $\mathbb{F}_{p^f}$, ce qui n'est pas gênant.

On peut alors énoncer le théorème suivant, qui donne la décomposition de l'idéal (π^f) de $\mathbb{Q}(\zeta_l)$, et constitue une généralisation de la formule (III.2).

Théorème 1.3 (G. Shimura et Y. Taniyama, [Shi 98]). *Pour un idéal premier $\mathfrak{P}$ de $\mathbb{Q}(\zeta_l)$ au-dessus de (p), on a*

$$\left(\pi^f\right) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}). \tag{III.3}$$

On retrouve sur cette formule que $\pi^f \in K_0$. En fait, on peut la réécrire entièrement dans ce sous-corps K_0, en regroupant les idéaux, et en utilisant les automorphismes de $\mathrm{Gal}(K_0/\mathbb{Q})$ plutôt que ceux de $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$,

$$\left(\pi^f\right) = \prod_{i=1}^{g} \psi_i(\mathfrak{P})^{h_i},$$

où l'on a encore noté $\mathfrak{P}$ un idéal de K_0 au-dessus de (p). On a $\sum h_i = n = \frac{fg}{2}$. Enfin, pour $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$ on note $\nu_\psi(i)$ la puissance de $\psi_i(\mathfrak{P})$ dans la décomposition en idéaux premiers de $\psi\left((\pi^f)\right)$.

Définition 1.4 (Séparation). *En gardant les notations introduites ci-dessus, on dit que les idéaux $\mathfrak{P}_i$ et $\mathfrak{P}_j$, pour $i \neq j$, sont* séparés *s'il existe $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$ tel que*

$$\nu_\psi(i) \neq \nu_\psi(j).$$

Si tous les idéaux sont séparés, on dit que l'on a la propriété de séparation.

En d'autres termes, on demande à deux idéaux distincts de ne pas apparaître systématiquement à la même puissance dans les décompositions de tous les conjugués de l'idéal (π^f).

Remarque 1.5 (Séparation et type-CM primitif). Notons qu'une variété abélienne en caractéristique 0 peut être simple sans que sa réduction modulo p le soit. C'est la raison de l'introduction de cette notion de séparation, qui n'est donc pas impliquée par le caractère primitif des types-CM. Bien entendu, si le type-CM n'est pas primitif, on ne peut pas espérer la propriété de séparation. Néanmoins, on peut ne pas avoir la propriété de séparation sur la réduction modulo p de la variété abélienne, même si le type-CM est primitif, comme le montre la proposition 1.6 ci-après.

Proposition 1.6 (Honda [Hon 66]). *Soit p un entier premier impair d'ordre f pair dans $(\mathbb{Z}/l\mathbb{Z})^*$ et soit π le Frobenius de la réduction modulo p de $\mathscr{H}_l$. Alors,*

$$\pi^f = -p^{\frac{f}{2}}.$$

En particulier, si $f \neq l-1$ alors, $\mathbb{Q} = \mathbb{Q}(\pi^f) \subsetneq K_0$.

Le théorème suivant donne un critère permettant de vérifier la propriété de séparation.

Théorème 1.7. *On a la propriété de séparation si et seulement si $\mathbb{Q}(\pi^f)$ est le corps K_0 de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$.*

Démonstration. Supposons que $\mathbb{Q}(\pi^f)$ soit un sous-corps strict de K_0 : on peut décomposer l'idéal (π^f) en idéaux premiers de ce sous-corps. Mais alors, pour chaque idéal de cette décomposition, les idéaux dans K_0, au-dessus, seront en nombre supérieur à 1 puisque K_0 est le corps de décomposition de (p). Ainsi, aucun de ces idéaux au-dessus n'est séparé, car ils apparaissent tous avec la même puissance, celle de l'idéal au-dessus duquel ils se trouvent.

Réciproquement, supposons qu'il existe deux indices $i \neq j$ tels que $\nu_\psi(i) = \nu_\psi(j)$ pour tout élément $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$. L'action du groupe de Galois est transitive sur les idéaux au-dessus de (p) : $\psi := \psi_{ji^{-1}}$ envoie $\psi_i(\mathfrak{P})$ sur $\psi_j(\mathfrak{P})$. Montrons que $\psi^{-1} \neq \mathrm{id}$ stabilise l'idéal (π^f). Pour cela, considérons l'idéal $\psi_k(\mathfrak{P})$, pour un certain indice k et notons $\psi' := \psi_{ki^{-1}}$ et $l := jki^{-1}$ si bien que l'on a le diagramme commutatif

$$\begin{array}{ccc} \psi_i(\mathfrak{P}) & \xrightarrow{\psi} & \psi_j(\mathfrak{P}) \\ {\scriptstyle\psi'}\downarrow & & \downarrow{\scriptstyle\psi'} \\ \psi_k(\mathfrak{P}) & \xrightarrow{\psi} & \psi_l(\mathfrak{P}) \end{array} \tag{III.4}$$

On lit alors directement $\nu_{\mathrm{id}}(k) = \nu_{\psi'^{-1}}(i)$ et $\nu_{\mathrm{id}}(l) = \nu_{\psi^{-1}}(k) = \nu_{\psi'^{-1}}(j)$. Or, par l'hypothèse de départ, $\nu_{\psi'^{-1}}(i) = \nu_{\psi'^{-1}}(j)$ et on en déduit que

$$\nu_{\mathrm{id}}(k) = \nu_{\psi^{-1}}(k)$$

et ce pour un k quelconque. Par la définition même de ν, cela implique que

$$\left(\pi^f\right) = \left(\psi^{-1}(\pi^f)\right)$$

et donc que $\mathbb{Q}(\pi^f)$ est un sous-corps strict de K_0. □

Corollaire 1.8. *Si (p) est complètement décomposé dans $\mathbb{Q}(\pi)$, alors on a la propriété de séparation si et seulement si le type-CM est primitif.*

L'intérêt — et la dénomination — de la propriété de séparation que l'on a introduite, est qu'elle permet une factorisation du polynôme cyclotomique $\Phi_l(t) \in \mathbb{F}_p[t]$.

Théorème 1.9. *Soit l un entier premier impair fixé. Soit A une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$ et soit p un entier premier tel que A ait bonne réduction en p. On note f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ et π le Frobenius de A modulo p.*

On suppose que $\mathbb{Q}(\pi^f)$ coïncide avec le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$. Alors, il existe un algorithme déterministe en temps polynomial en $\log(p)$ qui donne la factorisation de $\Phi_l \in \mathbb{F}_p[t]$.

Démonstration. On conserve les notations que l'on a introduites depuis le début de cette section, notamment celles de la définition 1.4. Les hypothèses sont formulées pour que la propriété de séparation découle du théorème 1.7.

Supposons dans un premier temps que $\psi_i(\mathfrak{P})$ divise (π^f) pour tout i. Alors, (p), qui est le produit de ces idéaux, divise (π^f), et on considère plutôt $\frac{\pi^f}{p^k}$ où k est le plus

grand entier tel que p^k divise π^f. Si jamais $k = \frac{f}{2}$ alors, $(\pi^f) = (p^{\frac{f}{2}})$; mais comme on a supposé que π^f engendre le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$, cela implique que ce dernier est $\mathbb{Q}$ et que Φ_l est irréductible dans $\mathbb{F}_p[t]$: il n'y a rien à faire pour le factoriser. Cette situation est facilement détectable, puisqu'elle ne survient que lorsque p engendre $(\mathbb{Z}/l\mathbb{Z})^*$, ce qui ne dépend que de la classe de p modulo l, fixé.

Ainsi, quitte à remplacer π^f par $\frac{\pi^f}{p^k}$, on a l'existence d'un idéal $\psi_i(\mathfrak{P})$ qui ne divise pas (π^f). Comme on a la propriété de séparation par le théorème 1.7, on en déduit que pour tout indice j, on peut trouver $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$ tel que

$$\nu_\psi(i) = 0 < \nu_\psi(j).$$

Notons par ailleurs, par transitivité de l'action du groupe de Galois sur les idéaux premiers, que cette propriété reste vraie pour tout indice i :

$$\forall i \neq j, \exists \psi \in \mathrm{Gal}(K_0/\mathbb{Q}), \quad \psi_i(\mathfrak{P}) \nmid \big(\psi(\pi^f)\big) \text{ et } \psi_j(\mathfrak{P}) \mid \big(\psi(\pi^f)\big). \tag{III.5}$$

Dès lors, grâce à l'algorithme de Pila [Pil 90], on calcule la fonction zêta de la réduction de la variété abélienne A, modulo p, ce qui fournit le polynôme caractéristique du Frobenius π puis celui de π^f, que l'on note $\Pi(t)$. Or, comme on a supposé que $\mathbb{Q}(\pi^f) \subset \mathbb{Q}(\zeta_l)$, on peut écrire

$$\pi^f = P(\zeta_l)$$

avec $P \in \mathbb{Z}[t]$. En effet, d'une part, π^f est un entier algébrique dans $\mathbb{Q}(\zeta_l)$ dont l'anneau des entiers est précisément $\mathbb{Z}(\zeta_l)$, ce qui assure l'existence du polynôme P. D'autre part, son calcul peut se réaliser en factorisant $\Pi(t)$ dans l'anneau des polynômes $\mathbb{Q}(\zeta_l)[t]$. Cela s'obtient, par exemple, avec l'algorithme LLL [LLL 82], en temps polynomial en le degré de Π et en les logarithmes des coefficients de Π. Le degré de Π est borné par l qui est une constante. Ses coefficients sont, d'après les conjectures de Weil 1.24, bornés par $p^{2\dim A}$.

La première partie de l'algorithme terminée, on introduit alors les polynômes

$$P_i(\zeta_l) = \psi_i(P(\zeta)) = \psi_i\big(\pi^f\big).$$

On sait que la décomposition de la réduction de ces polynômes P_i dans $\mathbb{F}_p[t]$ fait apparaître des facteurs irréductibles correspondant soit à des unités de $\mathbb{Q}(\zeta_l)$, soit aux idéaux premiers apparaissant dans la décomposition de $\psi_i(\pi^f)$.

Il ne nous reste plus qu'à dérouler la procédure suivante : on considère P_1 puis on calcule son pgcd avec P_2. Soit il vaut 1 et on calcule le pgcd avec P_3 plutôt qu'avec P_2, soit on garde ce résultat et on calcule son pgcd avec P_3. On recommence ainsi de suite. La propriété (III.5) montre précisément que cet algorithme « sépare » les facteurs irréductibles des P_i et termine en découvrant un facteur de degré f qui est forcément irréductible. Il suffit ensuite de recommencer, après avoir éliminé ce facteur des P_i, pour trouver la factorisation complète

Cette dernière partie de l'algorithme s'exécute encore en temps polynomial puisqu'il s'agit de calculer un nombre borné de pgcd de polynômes de degré borné par l, à coefficients dans $\mathbb{F}_p[t]$, ce qui est encore polynomial en $\log(p)$. Ceci termine la démonstration. □

Notons que dès que l'on a trouvé un facteur, on peut utiliser l'action de $\mathrm{Gal}(K_0/\mathbb{Q})$ pour trouver tous les autres, comme on l'explique à la fin de l'algorithme III.1, ci-après.

Première généralisation. Ceci permet de généraliser le résultat de J. Pila [Pil 90] tout en le redémontrant de manière plus simple. La première généralisation consiste à pouvoir factoriser $\Phi_l(t) \in \mathbb{F}_p[t]$, pour p d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$.

Corollaire 1.10. *On fixe toujours un entier premier l impair. Soit p un entier premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. Alors, il existe un algorithme que factorise $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial en $\log(p)$. Il est fourni ci-dessous par l'algorithme III.1.*

Démonstration. Afin d'appliquer le théorème 1.9, il nous faut trouver une variété abélienne A dont la réduction modulo p possède la propriété de séparation 1.4.

Pour cela, on commence par choisir $A = \mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_l)$, et on cherche à déterminer le corps $\mathbb{Q}(\pi^f) \subset \mathbb{Q}(\zeta_l)$ où π est le Frobenius de la réduction modulo p de $\mathrm{Jac}(\mathscr{H}_l)$. Supposons que pour un certain $\varphi \in \mathrm{Gal}(\mathbb{Q}(\zeta_l/\mathbb{Q}))$, on ait

$$\varphi\Big((\pi^f)\Big) = (\pi^f).$$

En utilisant la formule (III.2), on a alors

$$\prod_{i=1}^{n} \varphi \circ \varphi_i^{-1}(\mathfrak{P}) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}),$$

en notant encore K_0 le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$, on en déduit que

$$\{\varphi \circ \varphi_1^{-1}, \ldots, \varphi \circ \varphi_n^{-1}\} = \{\varphi_1^{-1}, \ldots, \varphi_n^{-1}\} \mod \mathrm{Gal}(K_0/\mathbb{Q}).$$

En notant $k \in [\![1, 2n]\!]$ tel que $\varphi^{-1} = \varphi_k$, en composant par φ^{-1} et en prenant l'inverse, on doit donc résoudre

$$\{\varphi_k \circ \varphi_i\} = \{\varphi_i\} \mod \mathrm{Gal}(K_0/\mathbb{Q}). \tag{III.6}$$

Cette équation est similaire à celle qui apparaît dans la démonstration de la proposition 1.1 pour montrer la simplicité du type-CM, mais la présence de $\mathrm{Gal}(K_0/\mathbb{Q})$ nous oblige à adapter cette démonstration. Pour cela, on considère l'isomorphisme de groupes entre $\mathbb{F}_l^*$ et $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ donné par $i \mapsto \varphi_i$, puis un caractère χ d'ordre g tel que via cet isomorphisme, $\mathrm{Gal}(K_0/\mathbb{Q})$ se retrouve dans le noyau de χ. Alors, l'équation III.6 à résoudre se traduit en

$$\{\chi(k)\chi(i)\} = \{\chi(i)\}$$

et donc, en sommant

$$\sum_{i=1}^{n} \chi(k)\chi(i) = \sum_{i=1}^{n} \chi(i)$$

soit encore

$$(\chi(k) - 1) \sum_{i=1}^{n} \chi(i) = 0.$$

On conclut, en utilisant le lemme 1.11 ci-dessous, que $\chi(k) = 1$, soit encore que φ_k et donc $\varphi = \varphi_k^{-1}$ est un élément de $\mathrm{Gal}(K_0/\mathbb{Q})$. Ceci termine la démonstration, car alors, $K_0 \subset \mathbb{Q}(\pi^f)$. En effet, l'autre inclusion est acquise dans tous les cas, et on peut utiliser le théorème 1.7 pour montrer la propriété de séparation 1.4, puis conclure grâce au théorème 1.9. □

La démonstration complète repose sur le corollaire suivant qui utilise une conséquence de la formule du nombre de classes relatif

$$h_1(l) = \frac{h(\mathbb{Q}(\zeta_l))}{h(Q(\zeta_l^+))} = \frac{1}{(2l)^{\frac{l-3}{2}}} \prod_{\chi \text{ impair}} \left| \sum_{i=1}^{l-1} i\chi(i) \right|$$

que l'on trouve par exemple dans [Was 97].

Lemme 1.11. *Soit $\chi : (\mathbb{Z}/l\mathbb{Z})^* \to \mathbb{C}^*$ un caractère d'ordre g tel que $\frac{l-1}{g}$ soit impair. Alors,*

$$\sum_{i=1}^{n} \chi(i) \neq 0$$

où on a noté, comme depuis le début, $n = \frac{l-1}{2}$.

Démonstration. Montrons tout d'abord que χ est impair. Soit pour cela $\alpha \in \mathbb{F}_l^*$ un générateur. Alors, comme χ est d'ordre g, on a nécessairement $\chi(\alpha^{\frac{g}{2}}) = -1$, soit, en élevant à la puissance $f = \frac{l-1}{g}$, $\chi(-1) = -1$.

Ainsi, χ est impair et par la formule du nombre de classes relatif que l'on a rappelée ci-dessus,

$$\sum_{i=0}^{l-1} i\chi(i) \neq 0.$$

Or, on a d'une part

$$\begin{aligned} \sum_{i=0}^{l-1} i\chi(i) &= \sum_{i=1}^{n} \Big(i\chi(i) + (l-i)\chi(l-i) \Big) \\ &= 2\sum_{i=1}^{n} i\chi(i) - l\sum_{i=1}^{n} \chi(i) \end{aligned}$$

et d'autre part, en partitionnant les entiers de $[\![1, l-1]\!]$ en $\{2, 4, \ldots, l-1\}$ et $\{l-2, l-4, \ldots, 1\}$,

$$\begin{aligned} \sum_{i=0}^{l-1} i\chi(i) &= \sum_{i=1}^{n} \Big(2i\chi(2i) + (l-2i)\chi(l-2i) \Big) \\ &= 4\chi(2)\sum_{i=1}^{n} i\chi(i) - l\chi(2)\sum_{i=1}^{n} \chi(i) \end{aligned}$$

ce qui montre finalement que

$$-l\chi(2)\sum_{i=1}^{n} \chi(i) = (2\chi(2) - 1)\sum_{i=1}^{l-1} i\chi(i) \neq 0 \qquad \square.$$

On a ainsi complètement démontré la validité de l'algorithme suivant, qui permet la factorisation des polynômes cyclotomiques $\Phi_l(t)$ dans $\mathbb{F}_p[t]$, sous réserve que l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ soit impair.

On est désormais en mesure d'écrire l'algorithme III.1 ci-après qui résume ce que l'on a dit dans cette section et dont la validité repose sur le théorème 1.9 et son corollaire 1.10.

Algorithme III.1 Factorisation de $\Phi_l(t) \in \mathbb{F}_p[t]$ (I)

Entrée : (p, l) avec p d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$; $g = \frac{l-1}{f}$.

1: $\Pi(t^f) \leftarrow$Fonction-Zêta(Jac$_{\mathbb{F}_p}(\mathscr{H}_l)$)
2: Factoriser $\Pi(t)$ dans $\mathbb{Q}(\zeta_l)[t]$ grâce à LLL par exemple
3: Soient $P_1, \ldots, P_g$ tels que $\Pi(t) = \prod_{j=1}^{g} \left(t - P_j(\zeta_l)\right)$ dans la factorisation ci-dessus
4: $Q_j \leftarrow \mathrm{pgcd}_{\mathbb{F}_p}\left(\frac{P_j}{p^k}, \Phi_l\right)$ avec k défini dans la démonstration du théorème 1.9
5: $F \leftarrow Q_1$, $j \leftarrow 2$
6: **Répéter**
7: $\quad F' \leftarrow$pgcd$(F, Q_j) \mod p$
8: $\quad$ **Si** $F' \neq 1$ **Alors**
9: $\quad\quad F \leftarrow F'$
10: $\quad$ **Fin Si**
11: $\quad j \leftarrow j + 1$
12: **Jusqu'à** $\deg F = f$
13: **Recommencer** en 5 avec les numérateurs de $Q_1/F, \ldots, Q_g/F$ modulo p.
14: **Jusqu'à** ce que les g facteurs de Φ_l soient déterminés.

Voici enfin deux remarques pour conclure sur cet algorithme. Tout d'abord, la ligne 4 nécessite quelques explications. En effet, on ne connaît pas k à l'avance, mais de simples calculs de pgcd permettent de déterminer le contenu des polynômes P_j. Ces calculs, portant sur des entiers plus petits que p^l s'effectuent en temps polynomial en $\log(p)$. Ensuite, le pgcd avec Φ_l sur $\mathbb{F}_p$ permet d'éliminer des facteurs « parasites » des P_j, correspondant à des unités dans $\mathbb{Q}(\zeta_l)$.

La deuxième remarque porte sur les deux dernières lignes : celles-ci peuvent être remplacées par l'action de $\mathrm{Gal}(K_0/\mathbb{Q})$ sur le facteur trouvé, par exemple par un calcul de résultant, associé à un calcul de pgcd,

$$\mathrm{pgcd}(\mathrm{Res}_t(F(t), t^j - s), \Phi_l(s)) \mod p,$$

pour les j tels que $\{\varphi_j,\ j\}$ engendre $\mathrm{Gal}(K_0/\mathbb{Q})$.

Exemple 1.12 (Factorisation de $\Phi_l(t) \in \mathbb{F}_p[t]$, p d'ordre impair). On déroule cet algorithme dans deux situations, la première pour $l = 5$ et $p = 11$, d'ordre $f = 1$ et la seconde pour $l = 13$ et $p = 29$ d'ordre $f = 3$.

***l* =5 et *p* =11** Voici le polynôme caractéristique du Frobenius de la jacobienne de $y^2 = x^5 - 1$ sur $\mathbb{F}_{11}$.

$$\Pi(t) = t^4 + 4t^3 + 6t^2 + 4 \cdot 11t + 11^2$$

dont la factorisation sur $\mathbb{Q}(\zeta_5)$ est donnée par

$$\Pi(t) = (t - 2\zeta_5^2 + 2\zeta_5 + 1)(t - 4\zeta_5^3 - 2\zeta_5^2 - 2\zeta_5 - 1)(t + 2\zeta_5^3 - 2\zeta_5 + 1)(t + 2\zeta_5^3 + 4\zeta_5^2 + 2\zeta_5 + 3)$$

ce qui fournit finalement la factorisation

$$\Phi_5(t) = (t + 8)(t + 2)(t + 6)(t + 7) \mod 11$$

où les facteurs ont été ordonnés suivant l'ordre de découverte par l'algorithme III.1. Afin d'illustrer la propriété de séparation, voici la factorisation des $\gcd(P_i(t), \Phi_5(t))$ modulo 11,

$$(t+2)(t+8),\ (t+6)(t+8),\ (t+2)(t+7) \text{ et } (t+6)(t+7)$$

$l = 13$ et $p = 29$ Ici, $p = 29$ est d'ordre 3 impair. Le polynôme caractéristique du Frobenius au cube de la jacobienne de $y^2 = x^{13} - 1$ modulo 29 est

$$t^4 - 576t^3 + 131254t^2 - 576 \cdot 29^3 t + 29^6$$

qui se factorise sur $\mathbb{Q}(\zeta_{13})$ en

$$\begin{aligned}\Pi(t) =&(t - 26\zeta_{13}^{11} - 40\zeta_{13}^{9} - 26\zeta_{13}^{8} - 26\zeta_{13}^{7} - 2\zeta_{13}^{6} - 2\zeta_{13}^{5} - 40\zeta_{13}^{3} - 2\zeta_{13}^{2} - 40\zeta_{13} - 161)\\ &(t - 14\zeta_{13}^{11} + 24\zeta_{13}^{9} - 14\zeta_{13}^{8} - 14\zeta_{13}^{7} + 26\zeta_{13}^{6} + 26\zeta_{13}^{5} + 24\zeta_{13}^{3} + 26\zeta_{13}^{2} + 24\zeta_{13} - 135)\\ &(t + 2\zeta_{13}^{11} - 24\zeta_{13}^{9} + 2\zeta_{13}^{8} + 2\zeta_{13}^{7} - 38\zeta_{13}^{6} - 38\zeta_{13}^{5} - 24\zeta_{13}^{3} - 38\zeta_{13}^{2} - 24\zeta_{13} - 159)\\ &(t + 38\zeta_{13}^{11} + 40\zeta_{13}^{9} + 38\zeta_{13}^{8} + 38\zeta_{13}^{7} + 14\zeta_{13}^{6} + 14\zeta_{13}^{5} + 40\zeta_{13}^{3} + 14\zeta_{13}^{2} + 40\zeta_{13} - 121)\end{aligned}$$

et fournit la factorisation irréductible

$$\begin{aligned}\Phi_{13}(t) =&(t^3 + 17t^2 + 26t + 28)(t^3 + 24t^2 + 14t + 28)\\ &(t^3 + 15t^2 + 5t + 28)(t^3 + 3t^2 + 12t + 28).\end{aligned}$$

Pour visualiser le déroulement de l'algorithme, on mentionne les $\gcd(P_i(t), \Phi_{13}(t))$ modulo 29,

$$\begin{aligned}&(t^3 + 24t^2 + 14t + 28)(t^3 + 15t^2 + 5t + 28)(t^3 + 17t^2 + 26t + 28)\\ &(t^3 + 24t^2 + 14t + 28)(t^3 + 3t^2 + 12t + 28)(t^3 + 17t^2 + 26t + 28)\\ &(t^3 + 3t^2 + 12t + 28)(t^3 + 15t^2 + 5t + 28)(t^3 + 17t^2 + 26t + 28)\\ &(t^3 + 24t^2 + 14t + 28)(t^3 + 3t^2 + 12t + 28)(t^3 + 15t^2 + 5t + 28).\end{aligned}$$

Deuxième généralisation. L'autre généralisation que l'on obtient du résultat de J. Pila [Pil 90], grâce au théorème 1.9, consiste en la factorisation de $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$, pour l impair.

Corollaire 1.13. *Soit p un nombre premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. Alors, il existe un algorithme, s'exécutant en temps polynomial, qui donne la factorisation du polynôme cyclotomique Φ_{l^m} dans $\mathbb{F}_p[x]$.*

Notons que le théorème 1.9 s'adapte sans modification, en changeant partout l par l^m. De même, la plupart des arguments de la démonstration du corollaire 1.10 et de ses lemmes s'adaptent sans difficulté, en modifiant simplement l en l^m comme on l'explique ci-après. La difficulté principale est d'exhiber une variété abélienne A simple, à multiplication complexe par $\mathbb{Q}(\zeta_{l^m})$ et qui vérifie la propriété de séparation 1.4. C'est l'objet du lemme suivant.

Lemme 1.14. *Soit J_m la jacobienne de la courbe hyperelliptique $\mathscr{H}_{l^m}$ d'équation $y^2 = x^{l^m} - 1$. Alors, J se décompose en un produit de m variétés abéliennes simples à multiplication complexe par $\mathbb{Q}(\zeta_{l^k})$, pour $k \in [\![1, m]\!]$.*

Démonstration. On démontre le résultat par récurrence sur m. Ce dernier est acquis pour $m = 1$, puisqu'il s'agit de $\mathrm{Jac}(\mathscr{H}_l)$ que l'on a étudiée jusqu'à présent. On suppose le résultat au rang $m-1$. Le morphisme

$$\begin{array}{ccc} \mathscr{H}_{l^m} & \mapsto & \mathscr{H}_{l^{m-1}} \\ (x,y) & \to & (x^l, y) \end{array} \tag{III.7}$$

assure que $\mathrm{Jac}(\mathscr{H}_{l^{m-1}})$ est une sous-variété de $\mathrm{Jac}(\mathscr{H}_{l^m})$, ce qui, grâce au théorème 1.19, assure l'existence d'une variété abélienne A_m telle que

$$\begin{aligned} \mathrm{Jac}(\mathscr{H}_{l^m}) &\simeq \mathrm{Jac}(\mathscr{H}_{l^{m-1}}) \times A_m \\ &\simeq A_1 \times \cdots \times A_{m-1} \times A_m \end{aligned}$$

où, par hypothèse de récurrence, les A_i pour $1 \leqslant i \leqslant m-1$ sont simples, à multiplication complexe par $\mathbb{Q}(\zeta_{l^i})$.

Ajoutons à l'hypothèse de récurrence que pour la sous-variété A_i de $\mathrm{Jac}(\mathscr{H}_{l^i})$ une base de différentielles est fournie par

$$\left\{ x^j \frac{\mathrm{d}x}{y}, \quad 0 \leqslant j \leqslant \frac{l^i - 3}{2}, j \neq 0 \mod l \right\}.$$

Ceci est bien entendu vérifié à l'ordre 1. Maintenant, grâce aux morphismes du type (III.7), on calcule facilement les bases de différentielles des A_i, vues comme sous-variétés de $\mathrm{Jac}(\mathscr{H}_{l^m})$, pour $i \leqslant m-1$. On s'aperçoit que les seules restantes, pour A_m sont

$$\left\{ x^i \frac{\mathrm{d}x}{y}, \quad 0 \leqslant i \leqslant \frac{l^m - 3}{2}, i \neq 0 \mod l \right\}.$$

Or, l'automorphisme de $\mathscr{H}_{l^m}$ noté $[\zeta_{l^n}]$ et donné par $(x,y) \mapsto (\zeta_{l^n} x, y)$, induit l'inclusion $\mathbb{Q}(\zeta_{l^m}) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(\mathscr{H}_{l^m}))$ et agit sur cette base de différentielles,

$$[\zeta_{l^m}]^* \left(x^i \frac{\mathrm{d}x}{y} \right) = \varphi_{i+1}(\zeta_{l^m}) x^i \frac{\mathrm{d}x}{y},$$

fournissant le type-CM

$$\left\{ x^i \frac{\mathrm{d}x}{y}, \quad 1 \leqslant i \leqslant \frac{l^m - 1}{2}, i \neq 0 \mod l \right\},$$

où l'on a noté, de manière similaire à la proposition 1.1, $\varphi_i : \mathbb{Q}(\zeta_{l^m}) \to \mathbb{C}$ définie par $\varphi_i(\zeta_{l^m}) = \zeta_{l^m}^i$, avec comme condition supplémentaire $i \neq 0 \mod l$.

Un calcul élémentaire, ou bien l'application du lemme 1.15 suivant pour $g = l^m - 1$, assure que ce type-CM est primitif et donc que A_m est simple. Enfin, comme on a $\dim A_m = l^m - l^{m-1} = \deg \Phi_{l^m}$, la variété abélienne A_m est à multiplication complexe par $\mathbb{Q}(\zeta_{l^m})$. Ceci termine la récurrence et la démonstration de ce lemme. □

Maintenant que l'on a trouvé une variété abélienne simple à multiplication complexe par $\mathbb{Q}(\zeta_{l^m})$, il nous faut encore montrer la propriété de séparation 1.4. Comme dans le cas $m = 1$, cela repose sur le lemme suivant.

Lemme 1.15. *Soit $\chi : (\mathbb{Z}/l^m\mathbb{Z})^* \to \mathbb{C}^*$ un caractère d'ordre g tel que $\frac{l-1}{g}$ soit impair. Alors, la quantité*

$$\sum_{i=1}^{n} \chi(i)$$

est non-nulle, où l'on a noté cette fois $n = l^{m-1}\frac{l-1}{2}$.

Démonstration. Notons que le cardinal de $(\mathbb{Z}/l\mathbb{Z}^m)^*$ est $l^{m-1}(l-1)$, ce qui permet de montrer, comme dans le lemme 1.11, que χ est impair. Dès lors, on peut reprendre point par point la démonstration, en modifiant l par l^m et en adoptant la convention classique $\chi(i) = 0$ pour $l \mid i$. □

Démonstration du corollaire 1.13. Ces lemmes, mis bout à bout comme précédemment, démontrent ce second corollaire de la même façon que le premier. Il faut simplement noter que l'on a simplement demandé que p soit d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$ mais ceci est équivalent à demander que p soit d'ordre impair dans $(\mathbb{Z}/l^m\mathbb{Z})^*$ puisque ce dernier est de cardinal $l^{m-1}(l-1)$. Le lemme 1.15 s'utilise alors de la même façon que le lemme 1.11. □

Pour finir ce paragraphe, mentionnons que l'algorithme III.1 se modifie sans peine, en calculant cette fois le polynôme caractéristique du Frobenius sur $\mathrm{Jac}(\mathscr{H}_{l^m})$. On le factorise ensuite une première fois sur $\mathbb{Q}$: il se décompose nécessairement en m facteurs irréductibles correspondant aux facteurs simples de $\mathrm{Jac}(\mathscr{H}_{l^m})$ et on retient le facteur de plus haut degré, qui est nécessairement un polynôme en une puissance f-ième de l'indéterminé, où f est l'ordre de p dans $(\mathbb{Z}/l^m\mathbb{Z})^*$. Le reste de l'algorithme est identique. Voici un exemple de fonctionnement.

Exemple 1.16 (Factorisations de $\Phi_{\zeta_{5^2}}$ sur $\mathbb{F}_{11}$ et de $\Phi_{\zeta_{7^2}}$ sur $\mathbb{F}_{67}$)**.** Notons que sur $\mathbb{Q}$, on sait déjà que $\Phi_{l^m}(X) = \Phi_l(X^{l^{m-1}})$. Comme on va le voir sur ces deux exemples, la factorisation de $\Phi_l(X)$ ne suffit pas forcément : cela dépend de l'ordre de p non plus dans $(\mathbb{Z}/l\mathbb{Z})^*$ mais dans $(\mathbb{Z}/l^m\mathbb{Z})^*$.

$l^m = 25$ et $p = 11$ Tout d'abord, 11 n'est plus d'ordre 1 dans $(\mathbb{Z}/25\mathbb{Z})^*$, mais d'ordre 5. La factorisation du Frobenius sur $\mathbb{Q}$ fait apparaître le facteur de degré 5 de l'exemple 1.12 et un autre facteur

$$\Pi(t^5) = t^{20} + 484t^{15} + 87846t^{10} + 484 \cdot 11^5 t^5 + 11^{10}$$

où Π est donc le polynôme caractéristique de la puissance 5^{e} du Frobenius sur la sous-variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_{5^2})$. Le polynôme Π se décompose sur ce corps et on obtient la factorisation

$$\Phi_{25}(t) = (t^5+8)(t^5+2)(t^5+6)(t^5+7) = \Phi_5(t^5) \mod 11$$

où les Q_i, de la ligne 4 de l'algorithme III.1 se factorisent, eux, en

$$Q_1 = (t^5+2)(t^5+8), Q_2 = (t^5+6)(t^5+8), Q_3 = (t^5+2)(t^5+7) \text{ et } Q_4 = (t^5+6)(t^5+7).$$

Notons au passage que cet exemple illustre le début de la démonstration du théorème 1.9, puisque π^5 est divisible par 11^2.

***l*^{m} = 49 et *p* = 67** Cette fois, $p = 67$ est non seulement d'ordre 3 dans $(\mathbb{Z}/7\mathbb{Z})^*$, mais aussi dans $(\mathbb{Z}/49\mathbb{Z})^*$.
La sous-variété abélienne de $\mathrm{Jac}(\mathscr{H}_{49})$ à multiplication complexe par $\mathbb{Q}(\zeta_{49})$ a pour polynôme caractéristique de son Frobenius au cube

$$\begin{aligned}
&t^{14} - 2100t^{13} + 1206317t^{12} + 184234456t^{11} - 199919567715t^{10} - 1213283343703 48t^9\\
&\quad + 114827360300456 09t^8 + 5775276301315905 5952t^7 + 11482736030045609 \cdot 67^3t^6\\
&\quad - 121328334370348 \cdot 67^6t^5 - 199919567715 \cdot 67^9t^4 + 184234456 \cdot 67^{12}t^3\\
&\quad + 1206317 \cdot 67^{15}t^2 - 2100 \cdot 67^{18}t + 67^{21},
\end{aligned}$$

qui se scinde complètement sur $\mathbb{Q}(\zeta_{49})$ et permet d'obtenir la factorisation

$$\Phi_{49}(t) = \prod_{i=1}^{14} f_i(t) \mod 67,$$

où les f_i sont données par les polynômes suivants, découverts dans cet ordre par l'algorithme III.1,

$$\begin{aligned}
f_1(t) &= t^3 + 37t^2 + 60t + 66, & f_2(t) &= t^3 + 40t^2 + 33t + 66, & f_3(t) &= t^3 + 34t^2 + 27t + 66,\\
f_4(t) &= t^3 + 38t^2 + 22t + 66, & f_5(t) &= t^3 + 13t^2 + t + 66, & f_6(t) &= t^3 + 32t^2 + 62t + 66,\\
f_7(t) &= t^3 + 24t^2 + 56t + 66, & f_8(t) &= t^3 + 7t^2 + 24t + 66, & f_9(t) &= t^3 + 66t^2 + 54t + 66,\\
f_{10}(t) &= t^3 + 5t^2 + 35t + 66, & f_{11}(t) &= t^3 + 7t^2 + 30t + 66, & f_{12}(t) &= t^3 + 45t^2 + 29t + 66,\\
f_{13}(t) &= t^3 + 11t^2 + 43t + 66, & f_{14}(t) &= t^3 + 43t^2 + 60t + 66
\end{aligned}$$

On rappelle enfin les factorisations des polynômes P_i, racines de Π dans $\mathbb{Q}(\zeta_{49})$, qui font apparaître la propriété de séparation ainsi que l'ordre des facteurs f_i découverts par l'algorithme III.1.

$$\begin{aligned}
&f_1f_2f_3f_4f_5f_6f_7f_8f_9f_{10}f_{11}f_{12}, && f_1f_2f_3f_4f_5f_6f_7f_8f_9f_{10}f_{13}f_{14},\\
&f_1f_2f_3f_4f_5f_6f_7f_8f_{11}f_{12}f_{13}f_{14}, && f_1f_2f_3f_4f_5f_6f_9f_{10}f_{11}f_{12}f_{13}f_{14},\\
&f_1f_2f_3f_4f_7f_8f_9f_{10}f_{11}f_{12}f_{13}f_{14}, && f_1f_2f_5f_6f_7f_8f_9f_{10}f_{11}f_{12}f_{13}f_{14},\\
&f_1f_3f_4f_5f_6f_7f_8f_9f_{10}f_{11}f_{13}f_{14}, && f_1f_3f_4f_5f_6f_7f_8f_9f_{11}f_{12}f_{13}f_{14},\\
&f_2f_3f_5f_6f_7f_8f_9f_{10}f_{11}f_{12}f_{13}f_{14}, && f_1f_2f_3f_4f_5f_6f_7f_8f_9f_{10}f_{12}f_{13},\\
&f_1f_2f_4f_5f_7f_8f_9f_{10}f_{11}f_{12}f_{13}f_{14}, && f_1f_2f_3f_4f_6f_7f_8f_9f_{10}f_{11}f_{12}f_{14},\\
&f_2f_3f_4f_5f_6f_7f_9f_{10}f_{11}f_{12}f_{13}f_{14}, && f_1f_2f_3f_4f_5f_6f_8f_{10}f_{11}f_{12}f_{13}f_{14}.
\end{aligned}$$

Finissons cette section en mentionnant qu'il existe en fait une variété abélienne simple, définie sur $\mathbb{Q}$, qui est à multiplication complexe par $\mathbb{Q}(\zeta_{l^m})$.

Proposition 1.17. *La jacobienne de la courbe donnée par l'équation superelliptique*

$$y^l = x(x^{l^{m-1}} - 1)$$

est de dimension $l^{m-1}(l-1)$ et possède l'automorphisme

$$(x, y) \mapsto (\zeta_{l^{m-1}}x, \zeta_{l^m}y),$$

qui engendre une multiplication complexe par $\mathbb{Q}(\zeta_{l^m})$. De plus, le type-CM est donné par

$$\Big\{\varphi_{l(i+1)-j},\ 1 \leqslant j \leqslant l-1,\ 0 \leqslant i \leqslant l^{n-2}j - 1\Big\}.$$

qui est primitif, si bien que cette jacobienne est simple.

Néanmoins, la forme particulière de ce type-CM rend plus compliquée la vérification de la propriété de séparation, dès que l'ordre de p est d'ordre différent de 1.

D'autre part, le genre de cette courbe est plus petit que celui de $\mathscr{H}_{l^m}$, ce qui en théorie est un avantage pour la rapidité d'exécution de l'algorithme. En pratique, l'algorithme de Pila en l'état, bien que polynomial, est limité aux petits genres et aux petits corps finis. D'un autre côté, il existe des méthodes spécifiques aux courbes hyperelliptiques qui sont bien plus efficaces, de telle sorte qu'à l'heure actuelle, Magma [Mag 13], par exemple, refuse d'effectuer les calculs de l'exemple 1.16 sur ce modèle, alors qu'avec les courbes hyperelliptiques, le résultat est presque instantané.

Troisième généralisation. Pour $m > 1$ on peut désormais considérer le polynôme cyclotomique non trivial $\Phi_{2^m}(t) = t^{2^{m-1}} + 1$. Le seul ordre impair dans $(\mathbb{Z}/2^m\mathbb{Z})^*$ est 1 et on considère donc des nombres premiers $p \equiv 1 \mod 2^m$.

Proposition 1.18. *Il existe un algorithme polynomial en* $\log(p)$ *qui donne la factorisation de* $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ *pour* $m > 1$ *et* $p \equiv 1 \mod 2^m$.

Démonstration. La démonstration du lemme 1.14 donnant la décomposition de la jacobienne de $\mathscr{H}_{l^m}$ s'adapte ici, à la différence que le type-CM n'est plus primitif. En effet, l'ensemble

$$\{\varphi_i,\ 1 \leqslant i \leqslant 2^{m-1} - 1, i \not\equiv 0 \mod 2\},$$

est stabilisé par $\{\mathrm{id}, \varphi_{2^{m-1}-1}\} \neq \{\mathrm{id}\}$ pour $m > 2$. Ainsi, les variétés abéliennes ne sont plus simples, mais le carré de variétés abéliennes simples, sauf pour la première :

$$\mathrm{Jac}(\mathscr{H}_{2^m}) \simeq B_1 \times B_2^2 \times \cdots \times B_{m-1}^2.$$

Le type-CM n'étant plus primitif, on ne peut pas espérer la propriété de séparation 1.4, mais les idéaux « inséparables » viennent par paires invariantes par l'automorphisme $\varphi_{2^{m-1}-1}$. Néanmoins, on dispose de la variété $B_1 \simeq \mathrm{Jac}(\mathscr{H}_4)$, qui n'est autre que la courbe elliptique $y^2 = x^4 + 1$: son Frobenius π vérifie $(\pi)(\overline{\pi}) = (p)$. Cette identité, vue dans $\mathbb{Q}(\zeta_{2^m})$ montre que (π) n'est pas stabilisé par $\varphi_{2^{m-1}-1}$: il permet donc de séparer les paires ci-dessus, ce qui termine la démonstration. □

Exemple 1.19 (Factorisation de $\Phi_{16}(t) \in \mathbb{F}_{17}[t]$). La factorisation du polynôme caractéristique de $\mathrm{Jac}(\mathscr{H}_{16})$ sur $\mathbb{Q}$ fait apparaître 3 facteurs, dont 2 sont des carrés, comme démontré ; ceux qui nous intéressent,

$$\pi_1 = t^2 - 2t + 17 \text{ et } \pi_3 = t^4 + 4t^3 + 6t^2 + 68t + 289,$$

correspondent respectivement aux variétés B_1 et B_3. On a alors

$$\pi_3(t) = \prod_{k=1}^{4} \left(t - P_k(\zeta_{16}\right)$$

puis en prenant les $\mathrm{pgcd}(P_k(t), t^8 + 1) \mod 17$, on obtient la factorisation

$$t^8 + 1 = (t^2 + 15t - 1)(t^2 + 14t - 1)(t^2 + 3t - 1)(t^2 + 2t - 1) \mod 17.$$

Ensuite, on factorise $\pi_1(t) = (t - 4\zeta_{16}^4 - 1)(t + 4\zeta_{16}^4 - 1)$ et il ne reste plus qu'à calculer 4 pgcd. Par exemple,

$$\mathrm{pgcd}(t^2 + 15t - 1, 4t^4 + 1) = t + 10 \mod 17,$$

ce qui fournit finalement la factorisation complète de $\Phi_{16}(t) \in \mathbb{F}_{17}[t]$.

— 2 —
Situation où p d'ordre pair dans $(\mathbb{Z}/l\mathbb{Z})^*$.

Jusqu'à présent, on est en mesure de factoriser tous les polynômes cyclotomiques $\Phi_n(t)$ sur $\mathbb{F}_p[t]$ du moment que p est d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$, pour tous les diviseurs premiers impairs l de n, et que p est d'ordre 1 dans $(\mathbb{Z}/2^k\mathbb{Z})^*$ où k est la valuation en 2 de n. En particulier, pour $p \equiv 1 \mod n$, on sait factoriser $\Phi_n(t)$ en temps polynomial en $\log(p)$. Néanmoins, comme on l'a vu dans la proposition 1.6, on ne peut pas espérer mieux avec l'utilisation des jacobiennes des courbes de type $\mathscr{H}_n$.

2.1 Ordre 2 et courbes à multiplication réelle

On cherche, dans ce paragraphe, à factoriser $\Phi_l(t)$ sur $\mathbb{F}_p[t]$ pour p d'ordre dans $(\mathbb{Z}/l\mathbb{Z})^*$ *quelconque*, mais on demande, par la forme des courbes que l'on utilise, d'avoir une racine carrée de -1 dans $\mathbb{F}_p$, soit encore $p \equiv 1 \mod 4$.

Courbes à multiplication complexe par $\mathbb{Q}(\zeta_l^+, i)$. On utilise certaines courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ que l'on a rencontrées à la section 2.1 du chapitre II et qui sont étudiées dans [TTV 91]. On montre que la propriété de séparation, fondamentale pour le type d'algorithme présenté en III.1, est vérifiée lorsque p est d'ordre 2 dans $(\mathbb{Z}/l\mathbb{Z})^*$, c'est-à-dire $p \equiv -1 \mod l$. On émet de plus la conjecture que ce résultat est vrai tout le temps, sous réserve que $p \equiv 1 \mod 4$, n'est pas d'ordre $\frac{l-1}{2}$, auquel cas on sait résoudre le problème d'une autre façon.

Proposition 2.1. *Soit $l > 5$ un nombre premier(⋆). La courbe $y^2 = x^{2l+1} + x$ possède un quotient donné par l'équation*

$$y^2 = x g_l(x^2 - 2), \qquad (\mathscr{H}_{l^+,i})$$

où g_l est le polynôme minimal de $-\zeta_l - \zeta_l^{-1}$. La jacobienne de cette courbe hyperelliptique est à multiplication complexe par $\mathbb{Q}(\zeta_l^+, i)$.

Démonstration. La multiplication par i est donnée par l'automorphisme de degré 4

$$[i] : (x, y) \mapsto (-x, iy),$$

et on sait déjà que cette courbe est à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$. Il faut alors vérifier que $[i]$ commute avec le reste, et donc préciser les endomorphismes de $\mathbb{Q}(\zeta_l^+)$. Pour cela, on note, comme d'habitude $[\zeta_l]$ l'automorphisme de la courbe de départ

$$(x, y) \mapsto \left(\zeta_l x, \zeta_l^{\frac{l-1}{2}} y\right).$$

Ensuite, on rappelle que le quotient est donné par l'involution sur la courbe de départ $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^{l+1}})$, comme on l'a expliqué dans la section 2.1 du chapitre II. Dès lors, on peut calculer une base de différentielles de $\mathscr{H}_{l^+,i}$, invariante sous cette involution

$$\omega_j := \left(x^j - x^{l-1-j}\right)\frac{\mathrm{d}x}{y}, \quad 0 \leqslant j \leqslant \frac{l-3}{2}$$

(⋆). C'est faux pour $l = 5$ mais la conjecture 2.7 et la remarque 2.8 sont vérifiées.

et vérifier que $[\zeta_l^+] := [\zeta_l] + [\zeta_l^{-1}]$ stabilise cette base de différentielles. L'avantage est que l'on en tire de plus le type-CM de $\mathscr{H}_{l^+,i}$:

$$[\zeta_l^+]^*\omega_j = \varphi_{\frac{l-1}{2}-j}(\zeta_l^+)\omega_j$$

avec de plus

$$[i]^*\omega_j = (-1)^j i\omega_j. \qquad \square$$

On choisit d'écrire $\mathrm{Gal}(\mathbb{Q}(\zeta_l^+, i)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})/\{\pm 1\}$ et de représenter ses éléments par des couples de $\Big((\{\pm 1\}, \times), \mathbb{F}_p^*/\pm 1\Big)$. Ainsi, le type-CM trouvé ci-dessus peut être écrit comme la partition

$$\Big\{\Big((-1)^i, \pm i\Big)\Big\} \cup \Big\{\Big((-1)^{i+1}, \pm i\Big)\Big\}.$$

Proposition 2.2 (Tautz, Top, Verberkmoes [TTV 91])**.** *Le type-CM ci-dessus est primitif, si bien que la jacobienne de $y^2 = xg(x^2 - 2)$ est simple sur $\mathbb{Q}$.*

Décomposition de (p) dans $\mathbb{Q}(\zeta_l^+, i)$ et propriété de séparation. On rappelle que l'on a fait l'hypothèse sur p qu'il vérifie la congruence $p \equiv 1 \mod 4$ de telle façon que l'on dispose de $i \in \mathbb{F}_p$, tel que $i^2 = -1$. Cela est nécessaire pour avoir le Frobenius, ou une de ses puissances dans $\mathbb{Q}(\zeta_l^+, i)$. Ici, ce n'est plus tout à fait l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ qui détermine cette puissance, mais c'est ce qui est introduit ci-dessous.

Notation 2.3. *Soit f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$. On introduit l'entier f' défini par*

$$f' = \begin{cases} f & \text{si } f \text{ est impair,} \\ \dfrac{f}{2} & \text{si } f \text{ est pair.} \end{cases}$$

Proposition 2.4. *Soit $p \equiv 1 \mod 4$ d'ordre f dans $(\mathbb{Z}/l\mathbb{Z})^*$ et f' comme ci-dessus. Alors, $\mathbb{Q}(\pi^{f'}) \subset \mathbb{Q}(\zeta_l^+, i)$.*

Démonstration. D'après la proposition 2.3 du chapitre I, il suffit de montrer que $\pi^{f'}$ commute avec tous les éléments de $\mathbb{Q}(\zeta_l^+, i)$. On effectue alors le calcul

$$[i] \circ \pi(x, y) = [i](x^p, y^p) = (-x^p, iy^p) = ((-x)^p, (iy)^p) = \pi \circ [i](x, y),$$

où l'on a utilisé le fait que $p \equiv 1 \mod 4$ pour écrire $i^p = i$. Ainsi π, et *a fortiori* $\pi^{f'}$, commutent avec $[i]$. Pour $[\zeta_{l,p}^+] = [\zeta_{l,p}] + [\zeta_{l,p}^{-1}]$, c'est un peu plus délicat. On commence par calculer

$$[\zeta_{l,p}] \circ \pi^{f'}(x, y) = \Big(\zeta_{l,p}^+ x^{p^{f'}}, y^{p^{f'}}\Big)$$

et on remarque que $p^{f'} \equiv \pm 1 \mod l$. Ainsi, on a

$$[\zeta_{l,p}] \circ \pi^{f'} = \pi^{f'} \circ [\zeta_{l,p}] \quad \text{ou} \quad [\zeta_{l,p}] \circ \pi^{f'} = \pi^{f'} \circ [\zeta_{l,p}^{-1}],$$

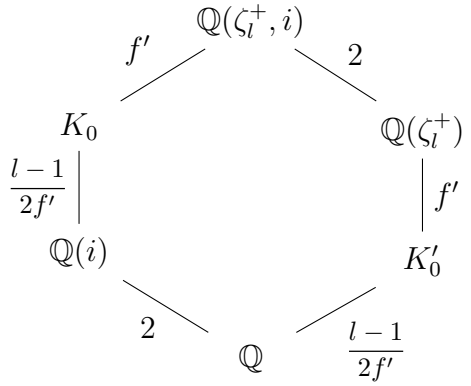
ce qui montre bien, dans les deux cas, que $\pi^{f'}$ commute avec $[\zeta_l^+]$. $\square$

Venons-en maintenant à la décomposition de l'idéal (p) dans $\mathbb{Q}(\zeta_l^+, i)$.

Proposition 2.5. *On note f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ et soit f' l'entier défini ci-dessus. Alors l'idéal (p) se décompose dans $\mathbb{Q}(\zeta_l^+)$ en $\frac{l-1}{2f'}$ idéaux premiers.*

De plus, la condition $p \equiv 1 \mod 4$ assure que ces idéaux se décomposent totalement dans l'extension $\mathbb{Q}(\zeta_l^+, i)/\mathbb{Q}(\zeta_l^+)$.

En particulier, que p soit d'ordre impair f ou d'ordre $2f$ dans $(\mathbb{Z}/l\mathbb{Z})^*$, la décomposition de (p) est de la « même forme », c'est-à-dire possède le même nombre d'idéaux premiers, de même indice de ramification. Plus généralement, on peut résumer la situation décrite dans la proposition précédente à l'aide du diagramme suivant, où l'on a posé comme d'habitude K_0 le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l^+, i)$ et K_0' celui de (p) dans $\mathbb{Q}(\zeta_l^+)$.



(III.8)

Proposition 2.6. *Soit p un nombre premier vérifiant les congruences $p \equiv 1 \mod 4$ et $p \equiv -1 \mod l$, pour $l > 5$. Alors, la jacobienne de la réduction sur $\mathbb{F}_p$ de la courbe $y^2 = xg(x^2 - 2)$, vérifie la propriété de séparation (1.4).*

Démonstration. Cela découle directement de la simplicité du type-CM, qui dans le cas où l'idéal (p) est totalement décomposé, implique la propriété de séparation (*cf.* corollaire 1.8). C'est ici le cas, car p est d'ordre 2 et donc $f' = 1$. □

Pour obtenir un résultat plus général, il faut résoudre l'équation en $k \in \mathbb{F}_p$,

$$((-1)^k, \pm k)\mathscr{T} = \mathscr{T} \mod \mathrm{Gal}(K_0/\mathbb{Q}). \tag{III.9}$$

Comme on l'a vu avec le diagramme (III.8), la conjugaison complexe ne peut stabiliser les idéaux premiers au-dessus de (p). Ainsi, on peut réécrire l'équation (III.9) en utilisant un caractère

$$\chi = \chi_1 \times \chi_2 : \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_l^+)/\mathbb{Q}) \to \mathbb{C}^* \times \mathbb{C}^*$$

dont les deux composantes sont telles que χ_1 est non triviale et χ_2 est d'ordre $\frac{l-1}{2f'}$. On cherche alors à résoudre l'équation

$$\Big\{\big((-1)^{i+k}, \chi(\pm ik)\big)\Big\} = \Big\{\big((-1)^i, \chi(\pm i)\big)\Big\}.$$

Les techniques utilisées plus haut ne fonctionnent pas car la somme

$$\sum_{i=1}^{\frac{l-1}{2}} (-1)^i \chi(i)$$

peut [(◇)] valoir 0. Un calcul exhaustif, vérifié pour tous les entiers premiers $l \leqslant 1000$ conduit à la conjecture suivante.

Conjecture 2.7. *Soit $p \equiv 1 \mod 4$ et l deux nombres premiers. On définit comme précédemment l'entier f' suivant l'ordre de p sans $(\mathbb{Z}/l\mathbb{Z})^*$ Alors, on a*

1. *Si $l \equiv 3 \mod 4$, le corps $\mathbb{Q}(\pi^{f'})$est précisément K_0 si bien que la propriété de séparation est vérifiée.*
2. *Si $l \equiv 1 \mod 4$, le corps $\mathbb{Q}(\pi^{f'})$est précisément K_0 sauf si $f' = \frac{l-1}{4}$ auquel cas, il contient K_0'.*

Remarque 2.8. Dans ce dernier cas on a en fait $f = \frac{l-1}{2}$ et même si l'algorithme III.2 suivant fonctionne encore, la factorisation de Φ_l peut se réaliser avec l'algorithme de Schoof [Sch 85]. On l'utilise en effet pour trouver une racine carrée de l dans $\mathbb{F}_p$ et on écrit $a^2 = l + kp$. Alors, le polynôme $t^2 + 2at + kp$ se scinde sur $\mathbb{Q}(\zeta_l)$, ayant pour discriminant $4l$. Si l'on note $t_1 = P_1(\zeta_l)$ et $t_2 = P_2(\zeta_l)$ les deux racines, alors, les deux facteurs irréductibles de Φ_l ne sont autres que les $\mathrm{pgcd}_{\mathbb{F}_p[t]}(P_1(t), \Phi_l(t))$ et $\mathrm{pgcd}_{\mathbb{F}_p[t]}(P_2(t), \Phi_l(t))$.

Ainsi, si l'on fait l'hypothèse que la conjecture 2.7 est vérifiée, on obtient l'existence, pour $p \equiv 1 \mod 4$ d'un algorithme s'exécutant en temps polynomial en $\log(p)$ permettant de factoriser $\Phi_l(t) \in \mathbb{F}_p[t]$. Il est facile de vérifier la conjecture sur l (indépendamment de p bien entendu) comme on l'a fait pour $l \leqslant 1000$. On peut trouver un exemple de programme, non optimisé, à l'adresse `www.normalesup.org/~iboyer/files/conj1.mw`.

Algorithme III.2 Factorisation de $\Phi_l(x) \in \mathbb{F}_p[x]$ (II)

Entrée : (p, l) avec $p \equiv 1 \mod 4$ d'ordre f dans $(\mathbb{Z}/l\mathbb{Z})^*$; $g = \frac{l-1}{f}$.

1: $\Pi(t^{f'}) \leftarrow$Fonction-Zêta$(\mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_{l^+,i}))$
2: Factoriser $\Pi(t)$ dans $\mathbb{Q}(i\zeta_l^+)[t]$ grâce à LLL par exemple
3: Soient $P_1, \ldots, P_g$ tels que $\Pi(t) = \prod_{j=1}^{g} \left(t - P_j(i\zeta_l^+)\right)$ dans la factorisation ci-dessus
4: Soit $i \in \mathbb{F}_p$ une racine de $t^2 + 1$, avec l'algorithme de Schoof par exemple
5: $Q_j \leftarrow \mathrm{pgcd}_{\mathbb{F}_p}\left(\frac{1}{p^k}\text{Numérateur}\left(P_j(i(t + \frac{1}{t}))\right), \Phi_l\right)$
6: $F \leftarrow Q_1$, $j \leftarrow 2$
7: **Répéter**
8: $\quad F' \leftarrow \mathrm{pgcd}(F, Q_j) \mod p$
9: $\quad$ **Si** $F' \neq 1$ **Alors**
10: $\quad\quad F \leftarrow F'$
11: $\quad$ **Fin Si**
12: $\quad j \leftarrow j + 1$
13: **Jusqu'à** $\deg F = f$
14: **Recommencer** en 6 avec les numérateurs de $Q_1/F, \ldots, Q_g/F$ modulo p.
15: **Jusqu'à** ce que les g facteurs de Φ_l soient déterminés.

(◇). Il n'y a pas d'exemple de nombre premier $l \leqslant 1000$ tel que cette somme est différente de 0.

Les principaux changements vis-à-vis de l'algorithme III.1 se situent ligne 2 où l'on n'utilise plus $\mathbb{Q}(\zeta_l)$ mais $\mathbb{Q}(\zeta_l^+, i)$ dont on utilise d'ailleurs la propriété que $i\zeta_l^+$ en est un générateur. Le second changement est que l'on doit donc utiliser $i(t+\frac{1}{t})$ et non plus simplement t dans l'argument de P_i — modification de la ligne 4 de l'algorithme III.1 par la ligne 5. Cela implique de connaître une racine de t^2+1 dans $\mathbb{F}_p$, ce que l'on sait faire avec l'algorithme de Schoof [Sch 85], en temps polynomial en $\log(p)$.

Exemple 2.9 (Factorisation de Φ_5 dans $\mathbb{F}_{109}$, de Φ_{13} dans $\mathbb{F}_{79}$ et $\mathbb{F}_{181}$ et de Φ_{17} dans $\mathbb{F}_{13}$)**.** Finissons par des exemples illustrant les différentes situations rencontrées ici.

$\boldsymbol{\Phi_5(t) \in \mathbb{F}_{109}[t]}$**.** Ici, 109 est d'ordre 2 dans $(\mathbb{Z}/5\mathbb{Z})^*$, cas particulier de la proposition 2.2. Néanmoins, $l=5$ vérifie la conjecture 2.7. En effet, la jacobienne de $\mathscr{H}_{5^+,i}$ se scinde en deux courbes elliptiques sur $\mathbb{F}_{109}$ dont le polynôme caractéristique du Frobenius est $t^2-16t+109$ engendrant le corps $\mathbb{Q}(i\sqrt{5}) \subset \mathbb{Q}(\zeta_5^+, i)$, corps de décomposition de (p) dans $\mathbb{Q}(\zeta_5^+)$. Cela suffit à faire fonctionner l'algorithme III.2. En effet, on obtient

$$t^2-16t+109 = \big(t-3(i\zeta_5^+)^3-12(i\zeta_5^+)-8\big)\big(t+3(i\zeta_5^+)^3+12(i\zeta_5^+)-8\big)$$

puis, en trouvant $i=33 \in \mathbb{F}_{109}$, on obtient les polynômes Q_i,

$$t^2+99t+1 \text{ et } t^2+11t+1,$$

ce qui fournit directement la factorisation de $\Phi_5(t)$ sur $\mathbb{F}_{109}[t]$.

$\boldsymbol{\Phi_{13}(t) \in \mathbb{F}_{79}[t]}$**.** Ici, (79) est complètement décomposé dans $\mathbb{Q}(\zeta_{13})$ et on sait faire avec le premier algorithme III.1. Néanmoins, le polynôme caractéristique du Frobenius de $\mathrm{Jac}_{\mathbb{F}_p}(\mathscr{H}_{13^+,i})$ est $(t^2-79)^6$. Cela illustre la nécessité d'avoir une racine carrée de -1 dans $\mathbb{F}_p$ ce qui n'est pas le cas, car $79 \equiv 3 \mod 4$.

$\boldsymbol{\Phi_{13}(t) \in \mathbb{F}_{181}[t]}$**.** Cette fois, $181 \equiv 1 \mod 4$ et il est d'ordre 2 dans $(\mathbb{Z}/13\mathbb{Z})^*$. On est dans la situation où l'on a démontré la validité de l'algorithme III.2 pour tout l. Le polynôme caractéristique du Frobenius est

$$\begin{aligned} &t^{12}+56t^{11}+1422t^{10}+23800t^9+353495t^8+5643696t^7+84134884t^6 \\ &\quad +5643696\cdot 181t^5+353495\cdot 181^2t^4+23800\cdot 181^3t^3+1422\cdot 181^4t^2+56\cdot 181^5t+181^6. \end{aligned}$$

En prenant $i=19 \in \mathbb{F}_{181}$, on obtient la factorisation

$$\Phi_{13}(t) = \prod_{j=1}^{6} f_j(t),$$

où les f_i sont donnés dans cet ordre par l'algorithme III.2, grâce aux polynômes Q_i,

$$\begin{aligned} f_1(t) &= t^2+128t+1, \quad f_2(t) = t^2+89t+1, \quad f_3(t) = t^2+64t+1, \\ f_4(t) &= t^2+45t+1, \quad f_5(t) = t^2+149t+1, \quad f_6(t) = t^2+69t+1. \end{aligned}$$

Voici les trois premiers polynômes Q_i, sous forme factorisée, qui suffisent déjà à fournir la factorisation des $\Phi_{13}(t) \in \mathbb{F}_p[t]$.

$$Q_1 = f_1f_2f_3, \qquad Q_2 = f_1f_4f_5, \qquad Q_3 = f_2f_4f_6.$$

$\Phi_{17}(t) \in \mathbb{F}_{13}[t]$. Ici, 13 est d'ordre 4 et c'est cette fois le polynôme caractéristique du carré du Frobenius qui est en jeu. La propriété de séparation fait l'objet de la conjecture 2.7, qui est vérifiée ici, comme pour tous les $l < 1000$.

$$t^8 + 40t^7 + 596t^6 + 1976t^5 - 28730t^4 + 1976\cdot 13^2 t^3 + 596\cdot 13^4 t^2 + 40\cdot 13^4 t + 13^6.$$

On prend alors $i = 5 \in \mathbb{F}_{13}$ et on trouve la factorisation

$$\Phi_{17}(t) = \prod_{j=1}^{4} f_j(t),$$

où, comme précédemment, les f_i sont fournis dans l'ordre

$$f_1(t) = t^4 + 10t^3 + 9t^2 + 10t + 1, \quad f_2(t) = t^4 + 2t^3 + 5t^2 + 2t + 1,$$
$$f_3(t) = t^4 + 9t^3 + 9t + 1, \quad f_4(t) = t^4 + 6t^3 + 6t^2 + 6t + 1,$$

et les trois premiers facteurs Q_i suffisent à factoriser $\Phi_{17}[t]$,

$$Q_1 = f_1 f_2 f_3, \qquad Q_2 = f_1 f_2 f_4, \qquad Q_3 = f_1 f_3 f_4.$$

2.2 Conjecture pour $p \not\equiv -1 \mod 8$

Les courbes précédentes, sous réserve de la conjecture 2.7, ont l'inconvénient d'imposer $p \equiv 1 \mod 4$ afin d'avoir une racine carrée de -1. Comme on l'a vu dans l'exemple 2.9, ces courbes ne permettent pas d'obtenir plus.

Courbes à multiplication complexe par $\mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$. On modifie légèrement les courbes utilisées dans la section précédente, en utilisant toujours un quotient d'une courbe qui n'est pas totalement à multiplication complexe, mais possède un endomorphisme d'ordre $8l$ que l'on note, comme d'habitude $[\zeta_{8l}]$.

Proposition 2.10. *Soit H_l la courbe d'équation $y^2 = x^{4l+1} + x$. L'automorphisme*

$$[\zeta_{8l}] : (x, y) \mapsto (\zeta_{8l}^2 x, \zeta_{8l} y),$$

d'ordre $8l$, assure l'injection $\mathbb{Q}(\zeta_{8l}) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(H_l))$. De plus, la jacobienne de la courbe hyperelliptique H_l se décompose en le carré d'une courbe elliptique et le carré d'une variété abélienne simple à multiplication complexe par $\mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$.

Démonstration. La première assertion est une vérification aisée. Pour la seconde, on commence, comme précédemment, par exhiber l'involution

$$\sigma : (x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{2l+1}}\right)$$

sur la courbe $y^2 = x^{4l+1} + x$, qui assure que sa jacobienne se décompose en un carré de variétés abéliennes. D'autre part, on a le morphisme

$$\begin{cases} X = x^l \\ Y = y x^{\frac{l-1}{2}} \end{cases}$$

vers la courbe hyperelliptique H_1 de genre 2 définie par $Y^2 = X^5 + X$, telle que l'involution σ sur cette courbe de genre 2 devienne $(X, Y) \mapsto (\frac{1}{X}, \frac{Y}{X^3})$ et décompose $\mathrm{Jac}(H_1) \simeq E^2$ où E est, comme on l'a vu dans la proposition 3.4 du chapitre II, la courbe elliptique d'équation $u^2 = (v-2)(v^2+2)$. Cela démontre la décomposition

$$\mathrm{Jac}(H_l) \simeq A^2 \times E^2,$$

où A est une variété abélienne de dimension $2l-2$. Une base de différentielles de A est donnée par celles de $\mathrm{Jac}(H_l)$, invariante par σ et ne provenant pas de E. On commence par calculer

$$\sigma^* x^i \frac{\mathrm{d}x}{y} = -x^{2l-i-1}\frac{\mathrm{d}x}{y} \quad \text{et} \quad \frac{\mathrm{d}X}{Y} = l x^{\frac{l-1}{2}}\frac{\mathrm{d}x}{y}$$

ce qui donne pour base de différentielles de A,

$$\omega_i := \left(x^i - x^{2l-i-1}\right)\frac{\mathrm{d}x}{y}, \quad 0 \leqslant i \leqslant l-1, i \neq \tfrac{l-1}{2}$$

dont on vérifie qu'elle est laissée invariante par $[\zeta_{8l}] - [\zeta_{8l}^{-1}]$. Non seulement cela montre que A est à multiplication complexe par $\mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$, car de dimension $2l-2$, mais ce calcul a l'avantage, comme précédemment, de fournir le type-CM. En effet, un calcul élémentaire donne

$$([\zeta_{8l}] - [\zeta_{8l}^{-1}])^* \omega_i = (\zeta_{8l}^{2i+1} - \zeta_{8l}^{-(2i+1)})\omega_i = \varphi_{2i+1}(\zeta_{8l} - \zeta_{8l}^{-1})\omega_i,$$

où on a noté $\varphi_k(\zeta_{8l}) = \zeta_{8l}^k$, qui est un automorphisme pour k premier à $2l$. Ceci nous donne comme type-CM

$$\left\{\varphi_{2i+1},\ 0 \leqslant i \leqslant l-1, i \neq \tfrac{l-1}{2}\right\}.$$

Pour assurer la simplicité de A, il reste à montrer que ce type-CM est primitif. Pour cela, commençons par remarquer que dans $\mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$, les automorphismes φ_k et φ_{4l-k} sont identifiés. Supposons par l'absurde que pour $a \geqslant 3$, l'automorphisme φ_a stabilise l'ensemble

$$\left\{\varphi_{2i+1},\ 0 \leqslant i \leqslant 2l-1, i \notin \{\tfrac{l-1}{2}, \tfrac{3(l-1)}{2}\}\right\},$$

et soit k le plus petit entier impair supérieur à la partie entière de $\frac{4l-1}{a}$. Alors,

$$4l - 1 \leqslant ka < 8l - 1,$$

ce qui n'est possible que si $k \in \{\frac{l-1}{2}, \frac{3l-1}{2}\}$ ou $ka = 4l-1$. Dans le premier cas, comme $a \geqslant 3$, on a nécessairement $k = \frac{l-1}{2}$ mais alors, $4l \leqslant (k+2)a < 8l-1$ ce qui est impossible. C'est le même argument dans le second cas si $k \geqslant 3$. Il ne reste donc que $k = 1$ mais alors $a^2 \equiv 8l - 1 \mod 8l$, ce qui est aussi impossible. Ceci démontre finalement que le type-CM est primitif. □

Conjecture sur la propriété de séparation. Tout d'abord, on remarque que pour p premier, $p^2 \equiv 1 \mod 8$. Ainsi, pour p d'ordre f pair dans $(\mathbb{Z}/l\mathbb{Z})^*$, on a

$$\pi^f \circ [\zeta_{8l}](x, y) = \left(\zeta_{8l}^{2p^f} x^{p^f}, \zeta_{8l}^{p^f} y^{p^f}\right) = [\zeta_{8l}] \circ \pi^f$$

si bien que π^f commute avec $[\zeta_{8l}] - [\zeta_{8l}^{-1}]$ sur A et donc $\mathbb{Q}(\pi^f) \subset \mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$. La décomposition des idéaux premiers (p) dans $\mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$ rend plus délicate l'étude de la propriété de séparation. Grâce à un programme informatique (‡), écrit dans le

(‡). On peut le trouver à l'adresse www.normalesup.org/~iboyer/files/conj2.m.

langage Magma [Mag 13], on peut tester cette propriété de séparation à un l fixé pour un certain nombre d'entiers p choisis pour leurs ordres dans $(\mathbb{Z}/8l\mathbb{Z})^*$, c'est-à-dire pour les classes modulo p d'ordre pair dans $(\mathbb{Z}/l\mathbb{Z})^*$ et pour les classes dans $(\mathbb{Z}/8\mathbb{Z})^*$.

Conjecture 2.11. *Soit $p \not\equiv -1 \mod 8$ d'ordre pair dans $(\mathbb{Z}/l\mathbb{Z})^*$ différent de $\frac{l-1}{2}$. Alors, la propriété de séparation est vérifiée.*

Remarque 2.12. Notons tout d'abord que la propriété de séparation dans $\mathbb{Q}(\zeta_{8l}-\zeta_{8l}^{-1})$ n'implique pas une propriété similaire dans $\mathbb{Q}(\zeta_{8l})$. Ainsi, il ne faut pas espérer trouver la factorisation de $\Phi_{\zeta_{8l}}$ Néanmoins, on a tout de même $\mathbb{Q}(\zeta_l^+) \subset \mathbb{Q}(\zeta_{8l}-\zeta_{8l}^{-1})$ et comme on travaille avec des p d'ordre pair dans $(\mathbb{Z}/l\mathbb{Z})^*$ la propriété de séparation est encore vérifiée sur le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l^+)$.

Cela complique un peu la situation et on doit modifier en conséquence l'algorithme III.1. Pour cela, on commence par factoriser le polynôme caractéristique de π^f dans $\mathbb{Q}(\zeta_{8l})$. On déroule ensuite l'algorithme III.1, même si à la fin, on n'obtient pas forcément des facteurs irréductibles de Φ_{8l}. Si l'on note $R(z)$ l'un des facteurs obtenus, on a nécessairement, par la propriété de séparation,

$$\mathrm{Res}_z(R(z), z^8 - t) \equiv Q(t)^2 \mod p \tag{III.10}$$

où Q est un facteur irréductible de $\Phi_l(t) \in \mathbb{F}_p[t]$. L'extraction d'une racine carrée est très facile. On peut même ici se contenter d'un pgcd avec la dérivée.

Comme on l'a vu dans la remarque 2.8, si p est d'ordre $\frac{l-1}{2}$, on sait factoriser Φ_l grâce à l'algorithme de Schoof. Ainsi, grâce à cette conjecture, vérifiée pour $l \leqslant 150$, on serait capable de factoriser les polynômes $\Phi_l(t)$ dans $\mathbb{F}_p[t]$ sauf pour $p \equiv -1 \mod 8$ d'ordre pair différent de $\frac{l-1}{2}$. Voici un exemple pour conclure cette section.

Exemple 2.13 (Factorisation de $\Phi_{13}(t)$ dans $\mathbb{F}_{83}[t]$ et $\mathbb{F}_{103}[t]$).

$\Phi_{13}(t) \in \mathbb{F}_{83}[t]$. On est dans le cadre de la conjecture, avec $83 \not\equiv -1 \mod 8$, d'ordre 4 dans $(\mathbb{Z}/83\mathbb{Z})^*$. Le polynôme caractéristique du Frobenius à la puissance 4,

$$t^6 - 9794t^5 + 34879007t^4 + 47268487716t^3 + 34879007 \cdot 83^4 t^2 - 9794 \cdot 83^8 t + 83^{12}$$

se factorise sur $\mathbb{Q}(\zeta_{8l})[t]$ et l'algorithme III.1 donne les facteurs non irréductibles

$$\Phi_{104}(t) = \prod_{i=1}^{4} R_i(t)$$

avec

$$\begin{aligned}
R_1(t) &= t^8 + 72t^7 + 19t^6 + 13t^5 + 35t^4 + 70t^3 + 19t^2 + 11t + 1,\\
R_2(t) &= t^8 + t^7 + 42t^6 + 7t^5 + 34t^4 + 76t^3 + 42t^2 + 82t + 1,\\
R_3(t) &= t^8 + 62t^7 + 13t^6 + 51t^5 + 25t^4 + 32t^3 + 13t^2 + 21t + 1,\\
R_4(t) &= t^8 + 21t^7 + 13t^6 + 32t^5 + 25t^4 + 51t^3 + 13t^2 + 62t + 1,
\end{aligned}$$

fournissant chacun un facteur irréductible de $\Phi_{13}(t) \in \mathbb{F}_{83}[t]$ par la formule (III.10),

$$\begin{aligned}
Q_1(t) &= t^4 + 8t^3 + 55t^2 + 8t + 1, & Q_2(t) &= t^4 + 46t^3 + 77t^2 + 46t + 1,\\
Q_3(t) &= t^4 + 30t^3 + 39t^2 + 30t + 1, & Q_4(t) &= t^4 + 30t^3 + 39t^2 + 30t + 1,
\end{aligned}$$

$\Phi_{13}(t) \in \mathbb{F}_{103}[t]$. Cette fois, on tombe dans le cas où $p = 103 \equiv -1 \mod 8$ et effectivement, la courbe $y^2 = x^{53} + x$ ne nous est d'aucun secours puisque le polynôme minimal du Frobenius est $(t^2 + 103)^{26}$.

— 3 —
Variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

On cherche ici à contourner les conjectures 2.7 et 2.11, en construisant directement une variété abélienne possédant un type-CM et une multiplication complexe que l'on a choisis. On sait — voir par exemple [Shi 98] — que cela est toujours possible. On montre ici une telle construction en genre 3.

3.1 Construction ad-hoc

L'intérêt de ce type de construction est de contourner la difficulté de la propriété de séparation en prenant un corps-CM où (p) est totalement décomposé ; ainsi un type-CM primitif assure la propriété de séparation, par le corollaire 1.8.

On choisit ici le corps-CM $\mathbb{Q}(\zeta_{13}^{(4)}, i)$, où l'on a gardé les mêmes notations que dans le chapitre II, de telle façon que la variété abélienne que l'on va construire peut être utilisée pour $p \equiv 1 \mod 4$ d'ordre 1,2 ou 4 dans $(\mathbb{Z}/13\mathbb{Z})^*$.

Ainsi, pour vérifier la propriété de séparation, il suffit que le type-CM soit primitif, et on choisit par exemple

$$\Big\{(\mathrm{id}, \mathrm{id}), (\varphi_4, \tau), (\varphi_3, \mathrm{id})\Big\} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{13}^+)) \times \mathrm{Gal}(\mathbb{Q}(i)), \tag{III.11}$$

où on a encore noté φ_i les restrictions des $\varphi_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_{13}))$, et $\tau \in \mathrm{Gal}(\mathbb{Q}(i))$ la conjugaison complexe. On notera, pour alléger les notations, $F_0 = \mathbb{Q}(\zeta_{13}^{(4)})$ le sous-corps totalement réel et $F = \mathbb{Q}(\zeta_{13}^{(4)}, i)$ le corps-CM. Par ailleurs, on considère le plongement $\sigma : F \hookrightarrow \mathbb{C}$, de façon « naturelle », avec $F \ni i \mapsto i \in \mathbb{C}$ et $\zeta_{13} \mapsto \exp(\frac{2i\pi}{13})$ et au type-CM, on associe les plongements $\{\sigma_1, \sigma_2, \sigma_3\}$. En particulier, $\sigma(\tau(x)) = \overline{\sigma(x)}$.

La construction de variétés abéliennes à multiplication complexe en genre 2 ou 3 est un problème très étudié. La principale différence ici, est que l'on montre, dans la section 3.2, que la variété abélienne obtenue possède bien la multiplication complexe désirée. Les deux références utilisées dans cette section sont P. Van Wamelen, [VW 99], dont la première partie traite d'un genre g quelconque, et A. Weng [Wen 01].

Variétés abéliennes à multiplication complexe sur $\mathbb{C}$. On reprend la construction présentée par G. Shimura et Y. Taniyama dans [Shi 98]. Celle-ci est générale et on peut remplacer tous les 3 par des g. On note O_F l'anneau des entiers de F et Ψ l'injection, associée au type-CM

$$\Psi : F \to \mathbb{C}^3, \qquad z \mapsto (\sigma_1(z), \sigma_2(z), \sigma_3(z)),$$

si bien que $\Psi(\mathscr{O}_F)$ est un réseau de $\mathbb{C}^g$. Pour faire de $\mathbb{C}^g/\Psi(\mathscr{O}_F)$ une variété abélienne, il faut la munir d'une forme de Riemann non dégénérée. Pour cela, on considère un élément $\xi \in \mathscr{O}_f$ tel que $\xi^2 \in \mathbb{F}_0$ soit totalement réel et $\Im(\sigma_j(\xi)) > 0$. Alors,

$$H(z, w) = 2\sum_{j=1}^{3} \Im(\sigma_j(\xi))\overline{z}_j w_j$$

est une forme de Riemann. En effet, c'est une forme hermitienne définie positive dont la partie imaginaire

$$\Im H(z,w) = \sum_{j=1}^{3} \sigma_j(\xi)(\overline{z}_j w_j - z_j \overline{w}_j)$$

vérifie $\Im H(\Psi(x),\Psi(y)) = \mathrm{Tr}_{F/\mathbb{Q}}(\xi\tau(x)y)$, si bien qu'elle est à valeurs entières sur le réseau $\mathscr{O}_F$. On vérifie que la variété abélienne ainsi obtenue est à multiplication complexe par F grâce aux endomorphismes, pour $\alpha \in \mathscr{O}_F$,

$$[\alpha] : \mathbb{C}^3/\Psi(\mathscr{O}_F) \mapsto \mathbb{C}^3/\Psi(\mathscr{O}_F), \quad z \mapsto (\sigma_1(\alpha)z_1, \sigma_2(\alpha)z_2, \sigma_3(\alpha)z_3),$$

qui respectent bien le réseau $\Psi(\mathscr{O}_F)$.

Polarisation principale. Les variétés abéliennes construites ci-dessus ne sont pas uniques car elles dépendent du choix de ξ. Van Wamelen, dans [VW 99], explique comment le choisir pour obtenir une variété abélienne principalement polarisée. Ici, la situation est assez simplifiée car la différente de $\mathscr{O}_F$ est un idéal principal, engendré par (ξ_d^{-1}) avec

$$\xi_d = \frac{1}{130}(7z^5 + 60z^3 + 78z)$$

où on a noté $z = i\zeta_{13}^{(4)}$, générateur de F sur $\mathbb{Q}$. Comme $\tau(z) = -z$, on a déjà ξ totalement imaginaire. Il reste à trouver une unité $u \in \mathscr{O}_{F_0}$ telle que $\Im(\sigma_j(u\xi_d)) > 0$ pour tout $j = 1, 2, 3$. Par exemple,

$$u = \frac{1}{5}(3z^4 + 20z^2 + 2)$$

convient et on pose alors

$$\xi = u\xi_d = \frac{1}{26}(-z^5 - 7z^3 + z).$$

Il reste à trouver une base $\mathscr{B} = \{b_1, \ldots, b_6\}$ de $\mathscr{O}_F$ telle que la matrice de terme général $(\mathrm{tr}_{\mathbb{Q}/F}(\xi\tau(b_i)b_j)_{i,j}$ soit sous forme de Frobenius

$$\begin{pmatrix} 0 & \mathrm{I}_3 \\ -\mathrm{I}_3 & 0 \end{pmatrix}$$

où les facteurs invariants sont tous 1 du fait du choix de ξ et de la polarisation principale. On trouve par exemple

$$\mathscr{B} = \left\{z, \tfrac{1}{5}(3z^4 + 20z^2 + 2), -z^4 - 7z^2 - 1, 1, z^3 + z, \tfrac{1}{5}(z^5 + 10z^3 + 4z)\right\}.$$

On note ensuite (ω_1, ω_2) la matrice $(g \times 2g)$ de $\Psi(\mathscr{O}_F)$ dans cette base et on considère le réseau $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ où $\Omega = \omega_2^{-1}\omega_1$ est une matrice symétrique dont la partie imaginaire est définie positive

$$\Omega = \frac{1}{65}\begin{pmatrix} 286z^5+2480z^3+3644z & -z^5-10z^3+31z & 84z^5+730z^3+836z \\ -z^5-10z^3+31z & 71z^5+620z^3+779z & -324z^5-2830z^3-3546z \\ 84z^5+730z^3+836z & -324z^5-2830z^3-3546z & 1501z^5+13110z^3+16409z \end{pmatrix}$$

telle que la variété abélienne $V_F = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, munie de la forme de Riemann $(z,w) \mapsto {}^t z(\Im\Omega)^{-1}\overline{w}$, est à multiplication complexe par $F = \mathbb{Q}(\zeta_{13}^{(4)}, i)$.

Fonctions thêta, modèle de Rosenhain. À partir de ce paragraphe et jusqu'à la section 3.2, on effectue des calculs approchés, de façon à chercher des équations de la variété abélienne V_F. La section 3.2 s'attache à montrer que le résultat obtenu ici est valide. On commence par calculer les thêta constantes paires, en vue d'appliquer le théorème 3.7, du chapitre I. Un calcul approché permet de conjecturer

$$\boldsymbol{\vartheta}\begin{bmatrix} \frac{1}{2} 0 \frac{1}{2} \\ \frac{1}{2}\frac{1}{2}\frac{1}{2} \end{bmatrix}(\Omega) = 0$$

et donc que V_F est la jacobienne d'une courbe hyperelliptique, que l'on note $\mathscr{H}$.

Notons au passage, comme dans [Wen 01], que la multiplication par i implique que si V_F est la jacobienne d'une courbe C, alors, C est nécessairement hyperelliptique. En effet, l'automorphisme $[i]$ d'ordre 4 sur la jacobienne de C montre l'existence d'un automorphisme α de degré 2 sur C : comme $\mathrm{Jac}(C/\langle\alpha\rangle)$ est une sous-variété de V_F, qui est simple puisque son type-CM est primitif, $C/\langle\alpha\rangle$ est nécessairement de genre 0 et C est hyperelliptique.

De manière analogue au genre 2, classique, on peut « inverser » la formule de Thomae 3.6 afin de déterminer les points de Weierstrass en fonction des thêta constantes. Pour cela, on utilise le modèle de Rosenhain d'une courbe hyperelliptique de genre 3 où l'on a fixé trois points de Weierstrass par homographie, 0, 1 et ∞,

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)(x-\lambda_4)(x-\lambda_5).$$

On a alors

$$2\lambda_1 = 1 + \frac{(\alpha_1\alpha_{12})^4 - (\alpha_2\alpha_{14})^4}{(\alpha_3\alpha_{15})^4}, \quad 2\lambda_2 = 1 + \frac{(\alpha_6\alpha_{11})^4 - (\alpha_8\alpha_{13})^4}{(\alpha_4\alpha_9)^4}, \quad 2\lambda_3 = 1 + \frac{(\alpha_5\alpha_6)^4 - (\alpha_7\alpha_8)^4}{(\alpha_9\alpha_{10})^4},$$
$$2\lambda_4 = 1 + \frac{(\alpha_5\alpha_{12})^4 - (\alpha_7\alpha_{14})^4}{(\alpha_3\alpha_{10})^4}, \quad 2\lambda_5 = 1 + \frac{(\alpha_1\alpha_{11})^4 - (\alpha_2\alpha_{13})^4}{(\alpha_4\alpha_{15})^4},$$

où les α_i sont donnés par les thêta constantes et où on a noté de façon abrégée $\boldsymbol{\vartheta}_{ij}$, pour $\boldsymbol{\vartheta}\begin{bmatrix} \frac{-2}{i} \\ \frac{-2}{j} \end{bmatrix}$, avec les développements binaires de i et j,

$$\begin{aligned} &\alpha_1 = \boldsymbol{\vartheta}_{00}, \quad \alpha_2 = \boldsymbol{\vartheta}_{75}, \quad \alpha_3 = \boldsymbol{\vartheta}_{10}, \quad \alpha_4 = \boldsymbol{\vartheta}_{01}, \quad \alpha_5 = \boldsymbol{\vartheta}_{03}, \\ &\alpha_6 = \boldsymbol{\vartheta}_{70}, \quad \alpha_7 = \boldsymbol{\vartheta}_{76}, \quad \alpha_8 = \boldsymbol{\vartheta}_{05}, \quad \alpha_9 = \boldsymbol{\vartheta}_{30}, \quad \alpha_{10} = \boldsymbol{\vartheta}_{43}, \\ &\alpha_{11} = \boldsymbol{\vartheta}_{41}, \quad \alpha_{12} = \boldsymbol{\vartheta}_{50}, \quad \alpha_{13} = \boldsymbol{\vartheta}_{34}, \quad \alpha_{14} = \boldsymbol{\vartheta}_{25}, \quad \alpha_{15} = \boldsymbol{\vartheta}_{40}, \end{aligned}$$

relations dépendant de la thêta constante nulle, comme expliqué dans la table 1 de [Wen 01]. En calculant les thêta constantes avec une bonne précision — ici 10^{-30} suffit — on peut utiliser les algorithmes classiques de dépendance linéaire basés sur l'algorithme LLL pour calculer un corps de définition des λ_i. Pari [GP 13] permet de trouver sans effort comme corps de définition des λ_k, le corps de nombres $\mathbb{Q}(\alpha)$ où α vérifie

$$\alpha^9 - \alpha^8 - 2\alpha^7 - t^6 + 5\alpha^5 + t^4 - 5\alpha^3 + 2\alpha^2 + 2\alpha - 1 = 0.$$

Cela donne une première équation de la courbe hyperelliptique $\mathscr{H}$, avec

$$\begin{aligned} \lambda_1 &= 2\alpha^8 - \alpha^7 - 4\alpha^6 - 4\alpha^5 + 8\alpha^4 + 5\alpha^3 - 7\alpha^2 - \alpha + 3 \\ \lambda_2 &= \frac{1}{2}(2\alpha^8 - \alpha^7 - 4\alpha^6 - 4\alpha^5 + 8\alpha^4 + 5\alpha^3 - 7\alpha^2 - \alpha + 3) \\ \lambda_3 &= 5\alpha^8 - 2\alpha^7 - 11\alpha^6 - 12\alpha^5 + 18\alpha^4 + 16\alpha^3 - 14\alpha^2 + 9 \\ \lambda_4 &= -10\alpha^8 - 10\alpha^7 + 8\alpha^6 + 32\alpha^5 + 8\alpha^4 - 18\alpha^3 + 12\alpha^2 + 14\alpha - 1 \\ \lambda_5 &= 3\alpha^8 - 5\alpha^6 - 8\alpha^5 + 6\alpha^4 + 6\alpha^3 - 8\alpha^2 - 2\alpha + 3. \end{aligned}$$

Invariants d'Igusa et équation de la courbe. La technique précédente fixe trois points de Weierstrass, ce qui a tendance à faire monter le corps sur lequel l'équation est définie. Pour déterminer le corps de définition de $\mathscr{H}$, une technique consiste à calculer les invariants absolus d'Igusa de la courbe $\mathscr{H}$, de genre 3. En effet, le corps de définition contient nécessairement le corps des invariants absolus car deux courbes sont isomorphes si et seulement si elles ont les mêmes invariants absolus : ce résultat est obtenu par Shioda, dans [Shi 67], et on le rappelle ici, dans le théorème 3.1.

Commençons par rappeler les invariants que l'on utilise ici. On considère deux polynômes homogènes f, g en deux variables (x, y) de degré m et n et on note

$$(fg)_k = \frac{(m-k)!(n-k)!}{m!n!}\left(\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x}\right)^k$$

où la puissance k-ième désigne un calcul symbolique par le binôme de Newton, avec les notations de la forme

$$\left(\frac{\partial f}{\partial x}\right)^k := \frac{\partial^k f}{\partial x^k}.$$

Pour un polynôme f de degré 8 homogène, on définit alors

$$\begin{aligned} p &= (ff)_4, \quad q = (ff)_6, \quad r = (qq)_2, \quad s = (fq)_4, \\ t &= (fr)_4, \quad u = (pq)_4, \quad v = (qr)_4, \quad w = (ff)_2. \end{aligned}$$

On définit ensuite les invariants relatifs I_k où k est le poids de l'invariant, ainsi que $\Delta = \Delta(f)$ le discriminant, de poids 14,

$$\begin{aligned} &I_2 = (ff)_8, \quad I_3 = (fp)_8, \quad I_4 = (qq)_4, \quad I_5 = (qs)_4, \quad I_6 = (qr)_4, \\ &I_7 = (rs)_4, \quad I_8 = (ru)_4, \quad I_9 = (rt)_4, \quad I_{10} = (rv)_4. \end{aligned}$$

On termine ce résumé sur les invariants d'Igusa d'une courbe hyperelliptique de genre 3 en introduisant des invariants absolus du polynôme homogène de degré 8 $f(x, y)$ et par extension de la courbe hyperelliptique sous forme homogène $z^2y^6 = f(x, y)$,

$$\begin{aligned} &j_1 = \frac{I_2^7}{\Delta}, \quad j_3 = \frac{I_2^5 I_4}{\Delta}, \quad j_5 = \frac{I_2^4 I_6}{\Delta}, \quad j_7 = \frac{I_2^3 I_8}{\Delta}, \quad j_9 = \frac{I_2^2 I_{10}}{\Delta}, \\ &j_2 = \frac{I_2^3 I_3^2}{\Delta}, \quad j_4 = \frac{I_2^2 I_5^2}{\Delta}, \quad j_6 = \frac{I_2 I_7^2}{\Delta}, \quad j_8 = \frac{I_9^2}{I_2^2 \Delta}. \end{aligned}$$

Théorème 3.1 (Shioda, [Shi 67]). *Deux courbes hyperelliptiques de genre 3 sont isomorphes si et seulement si elles possèdent les mêmes invariants j_i.*

Notons que Shioda démontre un résultat un peu plus fort sur l'anneau gradué des invariants de f, en montrant qu'il est engendré par les 9 invariants $I_2, \ldots, I_{10}$ ainsi que 5 relations.

En revenant à notre situation, on commence par remarquer que la forme des courbes en $y^2 = xP(x^2)$ avec $\deg P = 3$ possédant un automorphisme de degré 4, $(x, y) \mapsto (-x, iy)$, vérifient la proposition suivante, qui découle d'un calcul direct.

Proposition 3.2. *Soit H une courbe hyperelliptique d'équation*

$$y^2 = f(x) = x(x^6 + ax^4 + bx^2 + c).$$

Alors, $I_3 = I_5 = I_7 = I_9 = 0$, tout comme les invariants absolus j_i d'indice pair.

On revient désormais à notre courbe $\mathscr{H}$ dont la jacobienne est *supposée* être V_F à multiplication complexe par F, à la précision des calculs près. Soit $\mathbb{Q}(\beta)$ le corps de nombres défini par

$$\beta^3 - \beta^2 + 9\beta - 1.$$

Avec $\mathbb{Q}(\zeta_{13}^{(4)})$, ce sont les deux sous-corps de degré 3 de $\mathbb{Q}(\alpha)$. Les invariants d'Igusa absolus de $\mathscr{H}$ sont dans $\mathbb{Q}(\beta)$. Le résultat qui suit est en fait un peu plus fort.

Proposition 3.3. *La courbe $\mathscr{H}$ est isomorphe à la courbe hyperelliptique*

$$\begin{aligned} y^2 &= x\Big(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\Big) \\ &= x\Big(x^3 - \gamma x^2 + (\beta - \gamma)x + \beta\Big)\Big(x^3 + \gamma x^2 + (\beta - \gamma)x - \beta\Big), \end{aligned}$$

où on a posé $\gamma = \frac{1}{2}(\beta - 1)^2$. On la note encore $\mathscr{H}$. Enfin, le corps de définition de $\mathscr{H}$ est précisément $\mathbb{Q}(\beta)$.

Démonstration. Il s'agit simplement de calculer les invariants absolus j_i et de vérifier l'égalité, après avoir choisi le plongement $\mathbb{Q}(\beta) \hookrightarrow \mathbb{Q}(\alpha)$ défini par

$$\beta = -2\alpha^8 + 3\alpha^7 + \alpha^6 + 3\alpha^5 - 9\alpha^4 + 5\alpha^3 + \alpha^2 - 7\alpha + 3.$$

De plus, on vérifie que les invariants absolus sont dans $\mathbb{Q}(\beta) \setminus \mathbb{Q}$, ce qui montre que le corps de définition est $\mathbb{Q}(\beta)$ en ayant, de plus, une équation sur ce même corps. □

Remarque 3.4 (Détermination du modèle sur $\mathbb{Q}(\beta)$)**.** Finissons ce paragraphe en mentionnant l'algorithme que l'on a utilisé pour déterminer l'équation de C sur son corps de définition $\mathbb{Q}(\beta)$. Il s'agit simplement de calculer les invariants d'Igusa absolus pour une courbe à multiplication par $[i]$, à trois indéterminées

$$y^2 = f(x) = x(x^6 + ax^4 + bx^2 + c),$$

comme dans la proposition 3.2. On les égale ensuite aux invariants absolus de $\mathscr{H}$ sur $\mathbb{Q}(\alpha)$ et on résout le système obtenu — redondant — par un algorithme de bases de Gröbner, assez efficace dans cette situation.

3.2 Correspondance

Si la multiplication par $[i]$ dans $\mathrm{Jac}(\mathscr{H})$ est assurée par l'automorphisme sur $\mathscr{H}$ donné par $(x, y) \mapsto (-x, iy)$, rien n'assure la multiplication réelle par $\mathbb{Q}(\zeta_{13}^{(4)})$. Il y a bien sûr beaucoup d'indices en sa faveur, par exemple, le fait que le corps de définition de $\mathscr{H}$ ait comme corps de classe de Hilbert le corps $\mathbb{Q}(\alpha)$, extension de $\mathbb{Q}(\beta)$ par le sous-corps cyclotomique $\mathbb{Q}(\zeta_{13}^{(4)})$.

Détermination d'une correspondance. Pour montrer la validité des calculs menés jusqu'à présent, l'idée est de trouver une correspondance sur $\mathscr{H}$ qui engendre la multiplication réelle.

Proposition 3.5. *Il existe une correspondance 8-3 sur $\mathscr{H}$ définie sur le corps $\mathbb{Q}(\alpha)$ donnée par un polynôme $C(x,x')$ de degré 3 en x et 8 en x', ainsi qu'une fraction rationnelle $V(x,x')$ tels que*

$$\begin{cases} y^2 = f(x) \\ y'^2 = f(x') \\ 0 = C(x,x') \\ yy' = V(x,x') \mod C(x,x') \end{cases}$$

Démonstration. Il suffit d'exhiber C et V puis de vérifier la relation sur les ordonnées $V(x,x')^2 = f(x)f(x') \mod C(x,x')$. Dans un souci de complétude, les voici !
$C(x,x') = \big((-10\alpha^8+10\alpha^7+24\alpha^6+16\alpha^5-54\alpha^4-26\alpha^3+40\alpha^2-10\alpha-26)x^7+(-2\alpha^8+4\alpha^7-6\alpha^6+4\alpha^5-2\alpha^4+20\alpha^3-18\alpha^2-16\alpha+30)x^5+(8\alpha^8-10\alpha^7+6\alpha^6-24\alpha^5+10\alpha^4-38\alpha^3+52\alpha^2+50\alpha-36)x^3+(14\alpha^8-12\alpha^7-36\alpha^6-20\alpha^5+82\alpha^4+52\alpha^3-76\alpha^2-20\alpha+18)x\big)x'^3+\big(2x^8+(-6\alpha^7+10\alpha^6+2\alpha^5+4\alpha^4-30\alpha^3+26\alpha^2+16\alpha-30)x^6+(19\alpha^8-16\alpha^7-44\alpha^6-26\alpha^5+99\alpha^4+53\alpha^3-100\alpha^2+30)x^4+(-28\alpha^8+15\alpha^7+70\alpha^6+63\alpha^5-129\alpha^4-120\alpha^3+97\alpha^2+36\alpha-27)x^2-21\alpha^8+8\alpha^7+57\alpha^6+54\alpha^5-95\alpha^4-111\alpha^3+67\alpha^2+47\alpha-22\big)x'^2+\big((-2\alpha^7-4\alpha^6+6\alpha^5+14\alpha^4+4\alpha^3-24\alpha^2-8\alpha+16)x^7+(2\alpha^8+11\alpha^7+17\alpha^6-47\alpha^5-79\alpha^4-12\alpha^3+146\alpha^2+65\alpha-63)x^5+(31\alpha^8-18\alpha^7-144\alpha^6-18\alpha^5+271\alpha^4+283\alpha^3-388\alpha^2-204\alpha+142)x^3+(-43\alpha^8+41\alpha^7+56\alpha^6+91\alpha^5-164\alpha^4-23\alpha^3+27\alpha^2-76\alpha+37)x\big)x'+\big((23\alpha^8-20\alpha^7-46\alpha^6-42\alpha^5+113\alpha^4+53\alpha^3-72\alpha^2-6\alpha+14)x^6+(-94\alpha^8+25\alpha^7+217\alpha^6+291\alpha^5-309\alpha^4-430\alpha^3+88\alpha^2+97\alpha-19)x^4+(-5\alpha^8+145\alpha^7-42\alpha^6-293\alpha^5-442\alpha^4+461\alpha^3+575\alpha^2-118\alpha-89)x^2+61\alpha^8-11\alpha^7-191\alpha^6-167\alpha^5+278\alpha^4+411\alpha^3-236\alpha^2-195\alpha+93\big)$;
$V(x,x') = \big((x-\alpha+1)(x+\alpha-1)(x-2\alpha^8+2\alpha^7+3\alpha^6+3\alpha^5-9\alpha^4-\alpha^3+6\alpha^2-3\alpha)(x+2\alpha^8-2\alpha^7-3\alpha^6-3\alpha^5+9\alpha^4+\alpha^3-6\alpha^2+3\alpha)\big(x^{10}x'^2+1/2(-\alpha^8-3\alpha^7+4\alpha^6+8\alpha^5+6\alpha^4-14\alpha^3-6\alpha^2+\alpha-1)x^9x'+1/2(31\alpha^8-18\alpha^7-68\alpha^6-64\alpha^5+128\alpha^4+86\alpha^3-104\alpha^2+9\alpha+50)x^8x'^2+1/2(-\alpha^8-2\alpha^7+8\alpha^6-3\alpha^4-16\alpha^3+25\alpha^2-2\alpha-15)x^8+1/2(28\alpha^8-34\alpha^7-6\alpha^6-61\alpha^5+75\alpha^4-78\alpha^3+63\alpha^2+134\alpha-66)x^7x'+1/2(-76\alpha^8+46\alpha^7+167\alpha^6+159\alpha^5-320\alpha^4-225\alpha^3+240\alpha^2-4\alpha-94)x^6x'^2+1/4(63\alpha^8-64\alpha^7-57\alpha^6-121\alpha^5+189\alpha^4-61\alpha^3-17\alpha^2+274\alpha-83)x^6+1/4(51\alpha^8-44\alpha^7-224\alpha^6+8\alpha^5+452\alpha^4+400\alpha^3-694\alpha^2-221\alpha+190)x^5x'+1/4(149\alpha^8-48\alpha^7-285\alpha^6-465\alpha^5+403\alpha^4+489\alpha^3-5\alpha^2+46\alpha+13)x^4x'^2+1/4(315\alpha^8-252\alpha^7-1020\alpha^6-354\alpha^5+2188\alpha^4+1714\alpha^3-2452\alpha^2-1031\alpha+734)x^4+1/4(-137\alpha^8+134\alpha^7+219\alpha^6+255\alpha^5-615\alpha^4-163\alpha^3+277\alpha^2-134\alpha+41)x^3x'+1/4(-85\alpha^8-79\alpha^7+198\alpha^6+506\alpha^5+88\alpha^4-644\alpha^3-462\alpha^2+83\alpha+89)x^2x'^2+1/4(-1080\alpha^8+467\alpha^7+2625\alpha^6+2825\alpha^5-4453\alpha^4-4843\alpha^3+2561\alpha^2+1445\alpha-612)x^2+1/4(264\alpha^8+173\alpha^7-643\alpha^6-1385\alpha^5+39\alpha^4+1909\alpha^3+961\alpha^2-341\alpha-212)xx'+1/4(119\alpha^8-147\alpha^7-325\alpha^6-55\alpha^5+911\alpha^4+375\alpha^3-961\alpha^2-262\alpha+258)x'^2+1/4(-356\alpha^8+500\alpha^7+977\alpha^6+15\alpha^5-2953\alpha^4-983\alpha^3+3227\alpha^2+795\alpha-849)\big)\big)/\big(x(x-\alpha^8+\alpha^7+2\alpha^6+2\alpha^5-5\alpha^4-2\alpha^3+2\alpha^2-\alpha)(x+\alpha^8-\alpha^7-2\alpha^6-2\alpha^5+5\alpha^4+2\alpha^3-2\alpha^2+\alpha)(x^2+\alpha^8-2\alpha^7-\alpha^6-\alpha^5+6\alpha^4-2\alpha^3-\alpha^2+4\alpha-2)^3\big)$. □

Remarque 3.6 (Détermination algorithmique de cette correspondance). On fait le chemin inverse de la section précédente, en calculant une matrice des périodes approchée de $\mathrm{Jac}(\mathscr{H})$ et en calculant une matrice M préservant le réseau, de polynôme caractéristique t^3+t^2-4t+1. Cela est implémenté dans Magma, via la commande `EndomorphismRing`. Ensuite, on prend des points (k, y_k), pour k entier, on calcule leurs images dans $\mathbb{C}^3$ via la commande `ToAnalyticJacobian`, on leur applique la matrice M et on revient sur la courbe via la commande `FromAnalyticJacobian` : on

trouve trois abscisses $(x'_{k,1}, x'_{k,2}, x'_{k,3})$: on calcule ensuite un polynôme interpolateur en les $(k, x'_{k,j})$ en recommençant pour d'autres abscisses $x = k$, jusqu'à ce que les coefficients du polynôme interpolateur soient dans $\mathbb{Q}(\alpha)$.

Pour V, on le considère comme un polynôme de degré 2 en x' dans l'anneau $\mathbb{Q}(\alpha)(x)[x'] \simeq \mathbb{Q}(\alpha)[x, x']/C(x, x')$ et on résout, par bases de Gröbner, l'équation $f(x)f(x') - V(x, x')^2$ en les trois coefficients — fonctions rationnelles en x — de V vu comme polynôme en x'.

Avant de montrer que cette correspondance induit la multiplication réelle sur $\mathrm{Jac}(\mathscr{H})$, il faut aussi s'assurer de la commutation avec $[i]$ donné par $(x, y) \mapsto (-x, iy)$.

Proposition 3.7. *L'endomorphisme induit par la correspondance sur* $\mathrm{Jac}(\mathscr{H})$ *commute avec* $[i]$.

Démonstration. Tout d'abord, on vérifie les relations $C(-x, x') = C(x, -x')$ et $V(-x, x') = -V(x, -x')$ qui sont primordiales. Écrivons la correspondance sous la forme

$$(x_0, y_0) \mapsto \sum (x'_k, y'_k).$$

Alors, en notant

$$(-x_0, iy_0) \mapsto \sum (x''_k, y''_k),$$

on a $0 = C(-x_0, x''_k) = C(x_0, -x''_k) = C(x_0, x'_l)$, ce qui assure que $x''_k = -x'_{\sigma(k)}$ pour une permutation $\sigma \in \mathfrak{S}_3$. D'autre part

$$\begin{aligned} iy_0 y''_k = V(-x_0, x''_k) = -V(x_0, -x''_k) &= -V(x_0, x'_{\sigma(k)}) \\ &= -y_0 y'_{\sigma(k)}, \end{aligned}$$

ce qui montre que

$$\Big\{(x''_k, y''_k)\Big\} = \Big\{(-x'_k, iy'_k)\Big\}$$

puis la commutation avec l'endomorphisme issu de $(x, y) \mapsto (-x, iy)$. □

Action de la correspondance sur les différentielles. Afin de déterminer l'endomorphisme induit sur $\mathrm{Jac}(\mathscr{H})$ par cette correspondance, on calcule son action sur la base de différentielles

$$\mathscr{B} = \Big\{\frac{\mathrm{d}x}{y}, x\frac{\mathrm{d}x}{y}, x^2\frac{\mathrm{d}x}{y}\Big\},$$

ce qui est un peu plus délicat que lorsque l'endomorphisme provient d'un automorphisme de la courbe.

Théorème 3.8. *Soit* $\mathbb{Q}(\beta)$ *le corps de nombres défini par* $\beta^3 - \beta^2 + 9\beta - 1$. *La courbe hyperelliptique* $\mathscr{H}$ *définie par*

$$y^2 = x\Big(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\Big)$$

est à multiplication complexe par $\mathbb{Q}(\zeta_{13}^{(4)}, i)$, *avec un type-*CM *primitif.*

Démonstration. À un point (x, y) de $\mathscr{H}$, la correspondance associe trois points (x'_1, y'_1), (x'_2, y'_2) et (x'_3, y'_3) et il s'agit donc de décomposer les différentielles

$$\left\{ x_1'^k \frac{\mathrm{d}x'_1}{y'_1} + x_2'^k \frac{\mathrm{d}x'_2}{y'_2} + x_3'^k \frac{\mathrm{d}x'_3}{y'_3}, \quad k = 0, 1, 2 \right\}$$

sur la base $\mathscr{B}$. Pour cela, on commence par inverser $V(x, x')$ modulo $C(x, x')$ dans $\mathbb{Q}(\alpha)(x)[x']$

$$V(x, x')W(x, x') + U(x, x')C(x, x') = 1,$$

puis on écrit

$$\frac{\mathrm{d}x'_1}{y'_1} = \frac{f(x'_1)}{V(x, x'_1)} \frac{\mathrm{d}x'_1}{y} = W(x, x'_1) f(x'_1) \frac{\mathrm{d}x'_1}{y}.$$

Ensuite, on utilise les sommes de Newton pour exprimer les fonctions symétriques en x'_i en fonction de x, grâce au polynôme $C(x, x')$. Cela fournit la matrice de l'action de l'endomorphisme induit par la correspondance, sur la base de différentielles $\mathscr{B}$,

$$\begin{pmatrix} a_{11} & 0 & a_{13} \\ 0 & a_{22} & 0 \\ a_{31} & 0 & a_{33} \end{pmatrix}$$

avec

$$\begin{aligned}
a_{11} &= 2a^8 - 3a^6 - 5a^5 + 4a^4 + 3a^3 - 5a^2 + 2 \\
a_{13} &= -9a^8 + 2a^7 + 16a^6 + 21a^5 - 25a^4 - 19a^3 + 26a^2 - 12 \\
a_{22} &= a^8 - a^7 - 3a^6 - 2a^5 + 6a^4 + 5a^3 - 4a^2 - a + 2 \\
a_{31} &= 3a^8 - 5a^7 - 2a^6 - 2a^5 + 16a^4 - 9a^3 - 7a^2 + 9a - 2 \\
a_{33} &= -3a^8 + a^7 + 6a^6 + 7a^5 - 10a^4 - 8a^3 + 9a^2 + a - 5.
\end{aligned}$$

Notons que la forme de cette matrice était prévisible vu que c'est la forme générale des matrices qui commutent avec la matrice de l'action de l'endomorphisme $[i]$ sur la base $\mathscr{B}$,

$$\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & i \end{pmatrix}$$

Enfin, comme ces deux matrices commutent, il y a une base commune de diagonalisation $(\omega_1, \omega_2, \omega_3)$, avec $\omega_1, \omega_3 \in \mathrm{vect}\left\{\frac{\mathrm{d}x}{y}, x^2\frac{\mathrm{d}x}{y}\right\}$ et $\omega_2 = x\frac{\mathrm{d}x}{y}$. On vérifie sans mal que $[i]^*\omega_k = (-1)^{k+1} i\omega_k$ et on a donc comme type-CM

$$\{(\mathrm{id}, \mathrm{id}), (\varphi, \tau), (\varphi^2, \mathrm{id})\}$$

où φ engendre $\mathrm{Gal}(\mathbb{Q}(\zeta_{13}^{(4)}))$, cyclique d'ordre 3. Ce type-CM est primitif, et il est équivalent à celui dont on était parti (III.11). □

3.3 Exemples

Donnons désormais un exemple d'utilisation de cette variété pour la factorisation de $\Phi_{13}(t)$ sur $\mathbb{F}_{109}[t]$. En effet, l'idéal (109) est complètement décomposé

dans $F = \mathbb{Q}(\zeta_{13}^{(4)}, i)$ car d'ordre 4 dans $(\mathbb{Z}/13\mathbb{Z})^*$ et congru à 1 modulo 4. De plus, $t^3 - t^2 + 9t - 1$ est scindé sur $\mathbb{F}_{109}$, ce qui assure que la réduction de $\mathscr{H}$ est définie sur le corps de base $\mathbb{F}_{109}$. Le polynôme caractéristique du Frobenius est donné par

$$t^6 + 14t^5 - 93t^4 - 3148t^3 - 93 \cdot 109t^2 + 14 \cdot 109^2 t + 109^3,$$

qui se scinde sur $F = \mathbb{Q}(z)$ en $\prod_{k=1}^{6}(t - P_k(z))$, où l'on note comme précédemment $z = i\zeta_{13}^{(4)}$. En appliquant la boucle finale de l'algorithme III.1 aux polynômes

$$Q_k = \mathrm{pgcd}(P(i(t + t^5 + t^8 + t^{12}), \Phi_{13}(t))$$

avec $i = 33 \in \mathbb{F}_{109}$ on trouve la factorisation $\Phi_{13}(t) = \prod_{k=1}^{3} f_k(t)$ avec

$$f_1(t) = t^4 + 101t^3 + 71t^2 + 101t + 1, \quad f_2(t) = t^4 + 78t^3 + 10t^2 + 78t + 1$$
$$f_3(t) = t^4 + 40t^3 + 33t^2 + 40t + 1.$$

On donne enfin la factorisation des Q_i où on peut « voir » la propriété de séparation

$$Q_1 = f_1,\ Q_2 = f_2,\ Q_3 = f_1 f_2,\ Q_4 = f_1 f_3,\ Q_5 = f_3,\ Q_6 = f_2 f_3.$$

Pour être complet, il faut mentionner le cas où la courbe $\mathscr{H}$ n'est pas définie sur $\mathbb{F}_p$: cela n'est pas problématique, puisqu'il suffit de calculer le polynôme caractéristique du Frobenius sur $\mathbb{F}_{p^3}$. On trouve par exemple, pour $p = 73$, le polynôme

$$t^6 + 898t^5 - 159993t^4 - 524577380t^3 - 159993 \cdot 73^3 t^2 + 898 \cdot 17^6 t + 73^9,$$

dont on vérifie, comme dans le cas $p = 109$, qu'il convient.

3.4 Prolongements

Toujours dans la situation $p \equiv 1 \mod 4$, la généralisation de cette construction pour obtenir un algorithme polynômial en $\log(p)$ de factorisation de $\Phi_l(t)$ se heurte au problème majeur des calculs approchés. Ainsi, même si l'on arrive à construire une variété abélienne — c'est nettement plus difficile lorsqu'elle n'est plus la jacobienne d'une courbe hyperelliptique — dont on suppose fortement qu'elle est à multiplication complexe, on ne sait pas le vérifier, en calculant son anneau d'endomorphismes. La méthode utilisée ici ne peut se généraliser car rien n'indique que l'on peut toujours se ramener à la jacobienne d'une courbe. La conjecture 2.7 est peut-être plus facilement accessible...

2−2−2 isogénies et familles de courbes hyperelliptiques

Dans ce chapitre, nous décrivons les quatre familles de courbes hyperelliptiques de genre 3 pour lesquelles il existe une $2-2-2$ isogénie avec une autre courbe hyperelliptique.

Sommaire

Structure. Ce chapitre est formé de deux parties pouvant se lire indépendamment.

1°— Les sections 1 et 2 permettent de déterminer *toutes* les familles de courbes hyperelliptiques de genre 3 pour lesquelles il existe une autre courbe hyperelliptique dont les jacobiennes respectives sont $2-2-2$ isogènes. On utilise la théorie fonctions thêta, comme elle est exposée dans les *Tata lectures* de Mumford, notamment [Mum 83] et [Mum 84]. Le point clé est la caractérisation des jacobiennes de courbes hyperelliptiques parmi les variétés abéliennes (théorème 3.7 du chapitre I).

Grâce à la formule de Thomae (théorème 3.6 du chapitre I) et aux formules de duplications (proposition 1.2), on peut calculer les thêta constantes de la variété abélienne $2-2-2$ isogène. Grâce à elles, nous donnons un lieu d'annulation où les variétés abéliennes sont des jacobiennes de courbes hyperelliptiques. Ceci fournit quatre familles, qui se divisent en deux groupes de deux, suivant la nature du noyau de la $2-2-2$ isogénie, soit tractable (définition 2.2), soit en configuration du plan de Fano (proposition 2.5).

2°— La section 3 s'attache à décrire deux familles de courbes dont l'existence a été montrée dans les sections précédentes ; néanmoins, la lecture du résumé (section 2.4) suffit à l'introduire. On montre que deux des quatre familles sont « duales » (et les deux autres « auto-duales ») c'est-à-dire que la $2-2-2$ isogénie entre les jacobiennes des deux courbes fait passer d'une famille à l'autre (resp. les deux courbes sont dans la même famille).

La première famille repose sur la construction trigonale classique, exposée par S. Recillas [Rec 74], reprise et étudiée par R. Donagi et R. Livné [DL 99] et plus récemment rendue explicite par B. Smith [Smi 08]. On propose ici une paramétrisation efficace du problème (proposition 3.2) ainsi que la caractérisation (théorème 3.5) des courbes qui nous intéressent. On donne ensuite une équation (IV.18) de la courbe hyperelliptique associée (c'est-à-dire dont les jacobiennes sont $2-2-2$ isogènes), une caractérisation géométrique (théorème 3.11) ainsi que les équations pour passer de l'une à l'autre (IV.19 et IV.20). Enfin, on explicite deux correspondances, la première (IV.13) provenant de la construction trigonale, la deuxième (proposition 3.15) respectant les involutions hyperelliptiques.

Notations. Quand les arguments sont généraux, on les donne pour un genre noté g : c'est le genre des courbes considérées mais aussi tout naturellement la dimension des variétés abéliennes en jeu.

Par ailleurs, on désigne par une $\overbrace{2\cdots 2}^{g}$ isogénie, une isogénie de noyau isomorphe à $(\mathbb{Z}/2\mathbb{Z})^g$. Pour alléger les notations, on note aussi plus simplement une $2\cdots 2$ isogénie, le g étant sous-entendu.

— 1 —
$2\cdots 2$ isogénies et formule de duplication

1.1 Isogénies

La problématique est de chercher des paires de courbes hyperelliptiques dont les jacobiennes sont $2\cdots 2$ isogènes. Cette isogénie doit donc factoriser, avec sa duale, la multiplication par 2. D'un point de vue des variétés abéliennes de dimension g sur $\mathbb{C}$, on a le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g) & \xrightarrow{\ \varphi\ } & \mathbb{C}^g/(\mathbb{Z}^g+2\Omega\mathbb{Z}^g) \\ & \searrow^{[2]} & \downarrow{\scriptstyle z\mapsto z} \\ & & \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g) \end{array} \qquad \text{(IV.1)}$$

où $[2]$ désigne la multiplication par 2, et l'isogénie φ est donnée dans la proposition suivante, qui justifie que ce diagramme décrit la situation qui nous intéresse.

Proposition 1.1. *Il y a une $2\cdots 2$ isogénie entre les variétés abéliennes $\mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g)$ et $\mathbb{C}^g/(\mathbb{Z}^g+2\Omega\mathbb{Z}^g)$ qui est donnée par*

$$\begin{array}{rccc} \varphi: & \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g) & \longrightarrow & \mathbb{C}^g/(\mathbb{Z}^g+2\Omega\mathbb{Z}^g) \\ & z & \longmapsto & 2z \end{array}$$

et son noyau est

$$\left(\tfrac{1}{2}\mathbb{Z}^g + \Omega\mathbb{Z}^g\right)/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) \simeq (\mathbb{Z}/2\mathbb{Z})^g.$$

Démonstration. Pour justifier qu'il s'agit bien d'une $2\cdots 2$ isogénie il suffit de calculer son noyau : si l'on écrit $z = \Omega x + y$, on a

$$\begin{aligned} z \in \ker\varphi &\Leftrightarrow 2z = 2\Omega x + 2y \in 2\Omega\mathbb{Z}^g + \mathbb{Z}^g \\ &\Leftrightarrow x \in \mathbb{Z}^g \text{ et } 2y \in \mathbb{Z}^g \\ &\Leftrightarrow x \in \mathbb{Z}^g \text{ et } y \in \tfrac{1}{2}\mathbb{Z}^g, \end{aligned}$$

si bien que le noyau de cette isogénie est isomorphe à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g \simeq (\mathbb{Z}/2\mathbb{Z})^g$. □

Néanmoins, la situation n'est pas tout à fait générale puisque les matrices des périodes des deux variétés abéliennes sont fortement reliées, l'une étant le double de l'autre. Pour passer au cas général, en considérant toutes les variétés abéliennes isomorphes à $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, on doit utiliser l'action des matrices symplectiques $\mathrm{Sp}_{2g}(\mathbb{Z})$ sur $\mathbb{C}\times\mathscr{H}_g$ comme l'explique Mumford dans [Mum 83]. On modifie un peu le diagramme ci-dessus en considérant

$$\begin{array}{ccccc} & & \overset{\varphi}{\frown} & & \\ \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) & \xrightarrow[\sim]{\alpha_\Gamma} & \mathbb{C}^g/(\mathbb{Z}^g + \Omega'\mathbb{Z}^g) & \xrightarrow{\beta} & \mathbb{C}^g/(\mathbb{Z}^g + 2\Omega'\mathbb{Z}^g) \\ & & & & \Big\downarrow z\mapsto z \\ & & & \searrow^{[2]} & \mathbb{C}^g/(\mathbb{Z}^g + \Omega'\mathbb{Z}^g) \end{array} \qquad \text{(IV.2)}$$

où Ω' et les isogénies α_Γ et β sont définies par

$$\Omega' = (A\Omega + B)(C\Omega + D)^{-1},$$

$$\begin{array}{rccc} \beta \ : & \mathbb{C}^g/(\mathbb{Z}^g + \Omega'\mathbb{Z}^g) & \longrightarrow & \mathbb{C}^g/(\mathbb{Z}^g + \Omega'\mathbb{Z}^g) \\ & z & \longmapsto & 2z \end{array}$$

et

$$\begin{array}{rccc} \alpha_\Gamma : & \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) & \longrightarrow & \mathbb{C}^g/(\mathbb{Z}^g + \Omega'\mathbb{Z}^g) \\ & z & \longmapsto & {}^t(C\Omega + D)^{-1}z. \end{array}$$

Maintenant que l'on a déterminé les $2\cdots 2$ isogénies φ dans les diagrammes ci-dessus, il faut donner les conditions dans lesquelles les variétés abéliennes en jeu sont des jacobiennes de courbes hyperelliptiques. Pour cela, on commence par utiliser les fonctions thêta, plus particulièrement la formule de Thomae 3.6 du chapitre I, pour déterminer les thêta constantes de la variété abélienne de départ. Ensuite, il nous faut déterminer les thêta constantes des variétés abéliennes $\mathbb{C}^g/(\mathbb{Z}^g + 2\Omega\mathbb{Z}^g)$ ou $\mathbb{C}^g/(\mathbb{Z}^g + 2\Omega'\mathbb{Z}^g)$. Pour cela, on utilise une formule de duplication 1.3 ci-après puis éventuellement l'équation fonctionnelle 2.8 de $\boldsymbol{\vartheta}$ pour passer de Ω à Ω'. Il suffit ensuite d'appliquer le critère donné par le théorème 3.7 du chapitre I, pour avoir une condition sur les points de Weierstrass de la variété de départ pour que la variété abélienne d'arrivée soit la jacobienne d'une courbe hyperelliptique.

1.2 Formules d'addition et de duplication

On a vu dans les diagrammes commutatifs (IV.1) et (IV.2) que l'on devait passer des périodes Ω à 2Ω. Or, depuis Riemann, on connaît des relations, dites d'additions, entre les thêta constantes. En voici l'une d'elles.

Proposition 1.2 (Riemann). *La formule suivante exprime les fonctions thêta de la variété abélienne associée aux périodes 2Ω en fonction de celles liées aux périodes Ω :*

$$\boldsymbol{\vartheta}(x+y,2\Omega)\boldsymbol{\vartheta}(x-y,2\Omega) = 2^{-g}\sum_{\delta\in(\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g} \boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \delta\end{smallmatrix}\right](x,\Omega)\boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \delta\end{smallmatrix}\right](y,\Omega). \tag{IV.3}$$

On déduit de cette proposition la formule de duplication suivante :

Proposition 1.3. *On peut calculer les thêta constantes associées à 2Ω en fonction de celles associées à Ω.*

$$2^g\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](0,2\Omega)^2 = \sum_{\delta\in(\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g}(-1)^{4{}^t\eta'\delta}\boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \eta''+\delta\end{smallmatrix}\right](0,\Omega)\boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \delta\end{smallmatrix}\right](0,\Omega). \tag{IV.4}$$

Démonstration. En effet, dans la formule (IV.3) ci-dessus, on choisit $y = 0$ et $x = 2\Omega\eta' + \eta''$ et on écrit

$$\boldsymbol{\vartheta}(2\Omega\eta'+\eta'',2\Omega) = \boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta'\\ \eta''\end{smallmatrix}\right](0,\Omega)\exp(-2i\pi{}^t\eta'\Omega\eta' - 2i\pi{}^t\eta'\eta''),$$

dont la formule (IV.4) découle sans peine. □

Remarque 1.4 (Moyenne arithmético-géométrique). Cette formule peut être interprétée comme une généralisation multidimensionnelle de la moyenne arithmético-géométrique. Pour $g = 1$, si l'on note

$$a_n = \boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0,2^n\Omega)^2$$
$$b_n = \boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \frac{1}{2}\end{smallmatrix}\right](0,2^n\Omega)^2,$$

la relation (IV.4) avec $\eta' = 0$ et $\eta'' \in \{0, \frac{1}{2}\}$ donne précisément les relations de récurrence entre (a_n) et (b_n) de la moyenne arithmético-géométrique. Pour $g = 2$, cela était déjà connu par Borchardt en 1876, comme on peut le lire dans [Bor 76] et on peut par exemple voir [Dup 06] où il est proposé, en genre supérieur, de généraliser la moyenne arithmético-géométrique grâce à cette formule de Riemann (IV.4).

1.3 Détermination des signes

Afin de combiner la formule de Thomae 3.6 et la formule de duplication (IV.4), il reste à déterminer la racine quatrième des fonctions $\boldsymbol{\vartheta}$ dans les égalités fournies par la formule de Thomae.

C'est pour simplifier ce problème que l'on a introduit, au chapitre I, pour la formule de Thomae, l'ouvert

$$\mathscr{B}_g = \{(x_1,\dots x_{2g+2}) \in \mathbb{R}^{2g+2},\ x_1 > x_2 > \cdots x_{2g+2} > 0\}$$

et l'on donne une démonstration rapide dans le cas $g = 3$ qui nous intéresse (⋆).

(⋆). En fait, tout est dit par Mumford dans [Mum 84], mais la mise bout à bout de tous les arguments, notations, conventions, etc., est assez fastidieuse.

Proposition 1.5. *Les thêta constantes de la jacobienne d'une courbe hyperelliptique, dont les abscisses des points de Weierstrass sont dans le domaine $\mathscr{B}_3$, sont positivement liées, c'est-à-dire qu'à une même constante multiplicative près, les 35 thêta paires non-nulles sont réelles, strictement positives.*

Démonstration. On prend un point de $\mathscr{B}_3$ et on vérifie numériquement la proposition (on sait borner la précision des calculs). Ensuite, on remarque que sur $\mathscr{B}_3$, aucune différence $x_i - x_j$ ne peut s'annuler, ni les 35 thêta constantes paires non nulles. Or, le calcul intégral de la matrice des périodes de la jacobienne d'une courbe hyperelliptique assure que cette matrice est continue en les x_i sur le domaine $\mathscr{B}_3$. Il en est donc de même des thêta constantes puisque $\boldsymbol{\vartheta}$ est holomorphe en la matrice des périodes. Ainsi, la continuité des thêta constantes en les x_i, le résultat en un point et la non-annulation des thêta constantes assurent le résultat. □

Cela permet donc de mener plus facilement les calculs avec un logiciel de calcul formel tel Maple [Map 13], en demandant systématiquement de considérer les racines réelles positives. Maple dispose d'une telle possibilité, avec l'option `symbolic` de la commande `simplify`.

Par ailleurs le produit de toutes les thêta constantes non-nulles est un polynôme. Ainsi, par identité polynomiale, on peut se contenter d'effectuer les calculs avec les simplifications justifiables sur $\mathscr{B}_3$ mais le polynôme obtenu est le même, sans restrictions sur les points de Weierstrass, tout comme une éventuelle factorisation de ce polynôme.

— 2 —
Groupes totalement isotropes — familles à 4 paramètres

Désormais, on fixe $g = 3$. En suivant les choix de Mumford dans [Mum 84], on est parti ci-dessus d'une courbe hyperelliptique de genre 3 avec 8 points de Weierstrass auxquels on a associé un certain choix de demi-caractéristiques, une jacobienne et des thêta constantes. Ce choix n'est évidemment pas le seul et ne détermine une variété abélienne qu'à isomorphisme près.

Comme dans le diagramme (IV.2), pour une variété abélienne donnée par une matrice des périodes $\Omega \in \mathscr{M}_3(\mathbb{C})$, le groupe symplectique $\mathrm{Sp}_6(\mathbb{Z})$ détermine toutes les variétés abéliennes isomorphes, par l'action sur la matrice des périodes Ω :

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}.$$

Ce groupe agit par ailleurs sur le noyau comme on le détaille plus loin en (2.3.2) et donc sur les demi-caractéristiques. Comme ce sont ces dernières qui déterminent les thêta constantes, on peut se limiter aux matrices à coefficients dans $\mathbb{F}_2$.

Néanmoins, énumérer le groupe $\mathrm{S}_6(2) = \mathrm{Sp}_6(\mathbb{F}_2) \subset \mathscr{M}_6(\mathbb{F}_2)$, de cardinal 1451520, rend, à l'heure actuelle, un calcul systématique peu envisageable. On travaille donc

sur les noyaux possibles pour la 2−2−2 isogénie. Ce dernier doit être d'une part isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$ et d'autre part totalement isotrope pour le pairing de Weil modulo 2 :

$$4({}^t\eta_1'\eta_2'' + {}^t\eta_2'\eta_1'') \mod 2.$$

L'intérêt repose sur le fait qu'il n'existe pas beaucoup de tels groupes :

Proposition 2.1. *Il existe 135 groupes totalement isotropes, isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$. D'autre part, ils se répartissent en seulement 2 situations géométriques distinctes.*

Démonstration. Un tel groupe est clairement déterminé par trois points P_1, P_2 et P_3 indépendants et dont les pairing 2 à 2 sont nuls. En effet, le groupe s'énumère ensuite

$$\{0 = 2P_1, P_1, P_2, P_1 + P_2, P_3, P_1 + P_3, P_2 + P_3, P_1 + P_2 + P_3\}.$$

Il suffit dès lors d'imbriquer trois boucles et de tester les trois pairing, ce qui constitue donc, sans chercher de simplifications plus fines, $63 \cdot 62 \cdot 61 \cdot 3 = 714798$ tests de pairing (⋆). L'étude des 2 situations géométriques fait l'objet des deux sections suivantes. □

2.1 Groupes « tractables »

Une première situation géométrique bien connue et étudiée par exemple par R. Donagi, R. Livné [DL 99] et B. Smith [Smi 08] consiste en les groupes que l'on nomme tractables, en suivant la terminologie de B. Smith. Cette situation est généralisable sans difficulté en dimension g quelconque, mais on garde ici $g = 3$.

Définition 2.2. *Un groupe est dit tractable s'il est engendré par des différences de 2 points.*

Remarque 2.3. Comme l'on parle toujours de points de Weierstrass, il est sous-entendu que ces groupes sont isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$ puisque tous leurs éléments sont d'ordre 2.

Si l'on note P_i, $1 \leqslant i \leqslant 8$, les 8 points de Weierstrass, déterminer un tel groupe revient à énumérer ces 8 points dans un certain ordre, puis à les grouper 2 par 2.

En effet, $(\mathbb{Z}/2\mathbb{Z})^3$ peut être engendré par trois éléments qui, ici, par définition, doivent être des différences (◇) de 2 points : cela fait 6 points distincts et isole donc une 4e différence de deux points (qui est la somme des trois premières).

Il y a 8! façons d'énumérer les points de Weierstrass et une même partition apparaît $2^4 \cdot 4!$ fois, ce qui donne au final $7 \cdot 5 \cdot 3 = 105$ groupes distincts.

Pour relier les groupes tractables à notre situation, il suffit de montrer qu'ils sont totalement isotropes puisqu'ils sont, par construction, isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$.

Proposition 2.4. *Un groupe tractable correspond, via l'association (I.1) du chapitre I, à un groupe de demi-caractéristiques totalement isotrope pour le pairing de Weil modulo 2.*

(⋆). Le tout peut être effectué en 5s sur une machine personnelle.
(◇). Ou bien des sommes, le signe importe peu, c'est le support qui compte.

Démonstration. Cela découle de la propriété aisément vérifiable

$$4({}^t\eta'_i\eta''_j - {}^t\eta'_j\eta''_i) = 1 - \delta_{i,j}$$

où δ est le symbole de Kronecker. Dès lors, si l'on note $\langle\cdot,\cdot\rangle$ le pairing de Weil modulo 2, on a, pour des ensembles S et T de racines :

$$\begin{aligned}\langle \eta_S, \eta_S\rangle &= \sum_{i\in S}\Big(\langle \eta_{P_i}, \eta_{P_i}\rangle + \langle \eta_{P_i}\eta_{S\setminus\{P_i\}}\rangle\Big)\\ &= \sum_{i\in S}\Big(|S|-1\Big) = |S|(|S|-1) \equiv 0 \mod 2\end{aligned}$$

et

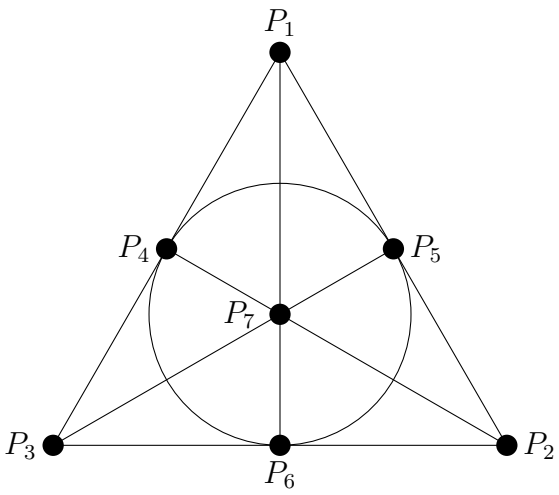
$$\begin{aligned}\langle \eta_S, \eta_T\rangle &= \langle \eta_{S\setminus T}, \eta_T\rangle + \langle \eta_{S\cap T}, \eta_T\rangle\\ &= \langle \eta_{S\setminus T}, \eta_T\rangle + \langle \eta_{S\cap T}, \eta_{S\cap T}\rangle + \langle \eta_{S\cap T}, \eta_{T\setminus S}\rangle\\ &\equiv |S\setminus T|\cdot|T| + 0 + |S\cap T|\cdot|T\setminus S| \mod 2\\ &\equiv |S\setminus T|\cdot|T\setminus S| + |S\cap T|\cdot|S\Delta T| \mod 2\\ &\equiv |S|\cdot|T| + |S\cap T| \mod 2. \qquad \text{(IV.5)}\end{aligned}$$

Pour conclure, il suffit de remarquer que si S et T sont deux paires de racines distinctes, alors la formule ci-dessus donne bien 0 modulo 2. Comme le groupe est engendré par de telles paires de racines, on conclut simplement grâce à la bilinéarité du pairing. □

2.2 Plan de Fano

La deuxième situation géométrique provient du plan de Fano dont on donne une représentation dans la figure IV.1.

Figure IV.1 Plan de Fano



On a représenté 7 points de Weierstrass $P_1, \ldots, P_7$ dans une configuration de Fano, ainsi que les 7 droites passant par trois points chacune.

On fait correspondre à chaque droite constituée de 3 points, l'ensemble des 4 autres points. On définit l'addition de deux tels ensembles distincts de 4 points par leur différence symétrique, qui correspond au final à la troisième droite concourante.

Par exemple, la situation ci-dessus correspond à l'ensemble suivant :

$$\{0, P_2+P_5+P_6+P_7, P_2+P_3+P_4+P_5,\\ P_3+P_4+P_6+P_7, P_1+P_2+P_4+P_6,\\ P_1+P_3+P_5+P_6, P_1+P_2+P_3+P_7, P_1+P_4+P_5+P_7.\}$$

Proposition 2.5. *L'addition décrite ci-dessus définit une structure de groupe. Il est isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^3$ *et totalement isotrope pour le pairing de Weil modulo 2.*

Démonstration. Les points de Weierstrass sont d'ordre 2 et la loi de groupe est simplement une différence symétrique sur l'ensemble des indices. De plus tous les éléments sont d'ordre 2 et donc le groupe ne peut être que $(\mathbb{Z}/2\mathbb{Z})^3$.

Deux droites se coupent en un point et donc leurs « complémentaires » ont deux points en commun. Comme par ailleurs leur support est composé de 4 points, la formule (IV.5) montre que leur pairing est nul modulo 2. □

Remarque 2.6. La loi de groupe décrite ici peut se concevoir de nombreuses façons.

- On peut remarquer que le groupe peut se « lire » directement sur la figure IV.1 du plan de Fano : l'addition de deux droites est soit l'élément neutre (non représenté) soit la troisième droite qui passe par le point d'intersection des deux premières.
- De même, l'addition de trois droites distinctes est la droite formée des points qui appartiennent à une exclusivement des trois droites : cela démontre au passage l'associativité de la loi d'addition.
- En fait, tout ceci peut aussi se lire directement sur la matrice d'incidence « droites/points », dressée dans la table IV.1, que l'on considère dans $\mathscr{M}_7(\mathbb{F}_2)$ et dont le complémentaire à 2 de l'addition des lignes correspond à la loi de groupe décrite.

Table IV.1 Matrice d'incidence du plan de Fano

	1	2	3	4	5	6	7
{1,3,4}	1	0	1	1	0	0	0
{1,6,7}	1	0	0	0	0	1	1
{1,2,5}	1	1	0	0	1	0	0
{3,5,7}	0	0	1	0	1	0	1
{2,4,7}	0	1	0	1	0	0	1
{4,5,6}	0	0	0	1	1	1	0
{2,3,6}	0	1	1	0	0	1	0

Il ne nous reste qu'à justifier le dénombrement : on peut permuter les 7 chiffres aux sommets de la figure IV.1 pour obtenir d'autres groupes. On obtient les mêmes si la permutation laisse stable une configuration de Fano. On sait que le groupe stabilisateur est $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ de cardinal $168 = 2\cdot 3\cdot 4\cdot 7$. Cela induit donc $\frac{7!}{168} = 5\cdot 6 = 30$ groupes de demi-caractéristiques.

2.3 Deux groupes pour les noyaux

On a donc montré qu'il y avait essentiellement deux groupes isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$ et totalement isotropes : un groupe tractable et un groupe issu d'une configuration de plan de Fano. Il suffit donc de faire les calculs dans ces deux cas seulement.

2.3.1 Groupes tractables

Dans cette situation, tous les outils ont été présentés dans les sections précédentes. Il ne reste plus qu'à mener effectivement ces calculs. C'est impossible à la main et on utilise un système de calcul formel tel Maple, avec notamment l'option `symbolic` de la commande `simplify`, comme on l'a expliqué dans la section 1.3 sur la détermination des signes des thêta constantes.

Ceci ne permet toutefois pas d'alléger suffisamment les calculs. Aussi, on fixe trois racines, par exemple $x_8 = 0$, $x_7 = 1$ et $x_6 = 2$. Cela détermine une homographie mais ne perd rien en généralité puisque le résultat est invariant par homographie. C'est d'ailleurs pour cela que l'on a des familles à $8 - 1 - 3 = 4$ paramètres, puisque ces familles sont définies par une relation, à homographie près. Il suffit alors d'appliquer l'homographie inverse (‡) pour retrouver le polynôme homogène en 8 variables.

On calcule, dans un premier temps, les thêta constantes de la variété abélienne 2–2–2 isogène, en appliquant la formule de la duplication (IV.4) et en se reportant au diagramme (IV.1) dont la 2–2–2 isogénie possède le noyau $(\frac{1}{2}\mathbb{Z}^g + \Omega\mathbb{Z}^g)/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$. Ce dernier s'écrit aussi, par l'équivalence (I.1),

$$G_1 = \left\{ \left[\begin{smallmatrix}000\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\\frac{1}{2}00\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\0\frac{1}{2}0\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\00\frac{1}{2}\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\\frac{1}{2}\frac{1}{2}0\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\\frac{1}{2}0\frac{1}{2}\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\0\frac{1}{2}\frac{1}{2}\end{smallmatrix}\right], \left[\begin{smallmatrix}000\\\frac{1}{2}\frac{1}{2}\frac{1}{2}\end{smallmatrix}\right] \right\}.$$

qui est précisément le groupe tractable, engendré par $P_1 - P_2$, $P_3 - P_4$ et $P_5 - P_6$.

Il s'agit ensuite de multiplier les thêta constantes entre elles, de simplifier et de factoriser afin de trouver les conditions d'annulation (⊛).

Là aussi, il n'est pas question d'effectuer le produit en une fois. On regroupe les 36 thêta constantes paires en 8 sous-ensembles.

- Le premier est constitué des 8 demi-caractéristiques du groupe G_1' « transposé » de G_1 :

$$G_1' = \left\{ \left[\begin{smallmatrix}000\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac{1}{2}00\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}0\frac{1}{2}0\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}00\frac{1}{2}\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac{1}{2}\frac{1}{2}0\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac{1}{2}0\frac{1}{2}\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}0\frac{1}{2}\frac{1}{2}\\000\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac{1}{2}\frac{1}{2}\frac{1}{2}\\000\end{smallmatrix}\right] \right\}.$$

  Les thêta constantes associées à 2Ω sont, d'après (IV.4), des sommes de carrés 8 thêta constantes associées à Ω.

(‡). Maple® a tendance à avoir du mal avec les dénominateurs. Le plus rapide pour appliquer cette homographie inverse consiste à refaire tout le calcul avec 6 variables et non pas 5 pour ne pas avoir de dénominateurs dans l'homographie !
On peut toutefois se passer de l'homographie car avec la construction trigonale de la section 3 on peut deviner le résultat : il suffit donc de le spécialiser en trois variables et de vérifier l'égalité, éventuellement à permutation des variables près.
Ainsi, sans le calcul de l'homographie, une machine personnelle vient à bout de ces calculs en 2 minutes environ.

(⊛). On passe bien entendu les conditions du type $x_i - x_j$ qui correspondent simplement à la dégénérescence de la courbe de départ.

Là encore, on ne peut effectuer le produit d'une traite : on multiplie les thêta constantes deux à deux en simplifiant au fur et à mesure. Le résultat est le carré d'un polynôme et on utilise un algorithme d'extraction de racines beaucoup plus efficace qu'une factorisation générale.
On aboutit à un polynôme en 8 variables, de degré total 16 et de degré 4 en chaque variable. Il est la somme de 19591 monômes. Ce polynôme définit donc une famille de courbes à 4 paramètres, qui fait l'objet d'une étude détaillée dans la section 3.

- Les sept autres correspondent au choix d'un vecteur $\eta'' \in \mathbb{Z}^3$ non nul. Pour un tel vecteur, on considère l'ensemble des vecteurs $\eta' \in \mathbb{Z}^3$ tels que $4{}^t\eta''\eta' \equiv 0[2]$. À $\eta'' \neq 0$ fixé, cette forme linéaire est surjective et donc son noyau est formé de 4 éléments. On obtient bien les $4 \cdot 7$ thêta constantes restantes.
L'intérêt de les regrouper comme ceci vient encore une fois de la formule (IV.4) : en effet, de cette façon, on obtient une somme de 4 (doubles) produits dont les termes sont les mêmes, seuls les signes changent : on obtient ainsi 7 polynômes qui donnent essentiellement (§) une autre famille de courbes, à 4 paramètres, qui est la spécification $g = 3$ de la famille présentée par J.-F. Mestre dans [Mes 13].

2.3.2 Configuration de Fano

Action sur le noyau. Le cas des groupes issus du plan de Fano est un peu plus délicat. En effet, le point central est l'utilisation de la formule de duplication (IV.4) qui relie les deux variétés abéliennes $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ et $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega\mathbb{Z}^3)$, selon l'isogénie φ décrite dans le diagramme (IV.1) mais dont le noyau, G_1, est tractable.

Il faut donc agir sur la variété abélienne de départ, (⋆⋆) comme on l'a dit sur le diagramme commutatif (IV.2). Il est assez facile de vérifier (⋄⋄) que $\mathrm{S}_6(2)$ agit de façon transitive sur les noyaux (isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$, totalement isotropes).

La difficulté revient donc à exprimer les thêta constantes d'une variété abélienne $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega'\mathbb{Z}^3)$ isomorphe à $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ via l'action de $\mathrm{S}_6(2)$. Ceci fait l'objet du prochain paragraphe.

Équation fonctionnelle et généralisation. Dans ce paragraphe et dans un souci de généralité, on considère à nouveau la situation où le genre g est quelconque et on travaille avec le groupe (‡‡) $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Commençons par poser quelques définitions sur les matrices symplectiques.

Définition 2.7. *On note dans toute la suite I la matrice identité de $\mathscr{M}_g(\mathbb{Z})$. On appelle matrice de* rotation *dans $\mathrm{Sp}_{2g}(\mathbb{Z})$ les matrices de la forme*

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{pmatrix}, \quad A \in \mathrm{GL}_g(\mathbb{Z}).$$

(§). À permutation des variables près.
(⋆⋆). On pourrait aussi agir sur celle d'arrivée, mais les calculs sont plus délicats.
(⋄⋄). Un petit programme systématique montre même qu'en combinant au plus trois matrices parmi les translations et l'involution J on peut engendrer tous les noyaux à partir de G_1'.
(‡‡). Il est facile de voir que tout élément de $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ se remonte en un élément de $\mathrm{Sp}_{2g}(\mathbb{Z})$.

On appelle matrice de translation *dans* $\mathrm{Sp}_{2g}(\mathbb{Z})$ *les matrices de la forme*

$$\begin{pmatrix} I & B \\ 0 & I \end{pmatrix},\ B \in \mathscr{M}_g(\mathbb{Z}),\ \textit{symétrique.}$$

On note enfin J *la matrice*

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}).$$

Mumford rappelle, dans [Mum 83], l'équation fonctionnelle de $\boldsymbol{\vartheta}$, pour un sous-ensemble de $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Théorème 2.8 (Équation fonctionnelle). *Soit* $\Gamma_{1,2} \subset \mathrm{Sp}_{2g}(\mathbb{Z})$ *l'ensemble*(⊛⊛) *de matrices symplectiques* $\Gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ *telles que les diagonales des matrices* ${}^tAC$ *et* ${}^tBD$ *soient paires.*

Alors, pour un tel Γ*, il existe une racine* 8^e *de l'unité* ζ_Γ *telle que*

$$\begin{aligned} &\boldsymbol{\vartheta}\Big({}^t(C\Omega+D)^{-1}z, (A\Omega+B)(C\Omega+D)^{-1}\Big) \\ &\quad = \zeta_\Gamma\Big(\det(C\Omega+D)\Big)^{\frac{1}{2}} \exp\Big(i\pi\, {}^tz(C\Omega+D)^{-1}Cz\Big)\boldsymbol{\vartheta}\Big(z,\Omega\Big). \end{aligned} \tag{IV.6}$$

Exemple 2.9. Voici deux exemples qui serviront par la suite. Avant de les exposer, l'équation fonctionnelle fait apparaître un certain nombre de « constantes » multiplicatives. Or, il nous suffit de déterminer un système homogène des thêta constantes. Ainsi, les racines 8^{e} de l'unité, ne dépendant que de Γ, seront les mêmes pour toutes les thêta constantes et n'influent donc pas. Il en est de même pour la racine du déterminant qui ne dépend que de Ω et Γ.

On écrit ainsi dans la suite un λ dans les égalités, afin de se rappeler que les équations sont vraies « à une constante multiplicative près », identique pour toutes les thêta constantes.

- Dans le cas où $B \in \mathscr{M}_g(\mathbb{Z})$ est symétrique, de diagonale paire, on a $\left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right) \in \Gamma_{1,2}$ et simplement
$$\boldsymbol{\vartheta}(z, \Omega+B) = \lambda\boldsymbol{\vartheta}(z,\Omega)$$
ce qui donne sur les thêta constantes
$$\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ \eta'' \end{smallmatrix}\right](0,\Omega+B) = \lambda\exp(-i\pi\, {}^t\eta' B\eta')\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ B\eta'+\eta'' \end{smallmatrix}\right](0,\Omega). \tag{IV.7}$$
- Pour J, on a la formule sur les thêta constantes :
$$\boldsymbol{\vartheta}\left[\begin{smallmatrix} 0 \\ \eta'' \end{smallmatrix}\right](0, J\cdot\Omega) = \lambda\boldsymbol{\vartheta}\left[\begin{smallmatrix} -\eta'' \\ 0 \end{smallmatrix}\right](0,\Omega) = \lambda\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta'' \\ 0 \end{smallmatrix}\right](0,\Omega), \tag{IV.8}$$
la dernière égalité découlant de la parité de $\boldsymbol{\vartheta}$.

On va expliquer dans la suite comment on peut, d'une part, étendre cette formule à tout $\mathrm{Sp}_{2g}(\mathbb{Z})$ et d'autre part, l'utiliser pour calculer les thêta constantes. Avant tout, mentionnons qu'un calcul sans difficulté montre que

$$\alpha_\Gamma \circ \alpha_\Delta = \alpha_{\Gamma\Delta},$$

ce qui justifie l'intérêt de la proposition suivante.

(⊛⊛). Ce sont aussi les matrices qui préservent le pairing de Weil modulo 2.

Proposition 2.10 (Générateurs de $\mathrm{Sp}_{2g}(\mathbb{Z})$ et $\Gamma_{1,2}$)**.**

1. *Les matrices de rotations, de translations et J engendrent $\mathrm{Sp}_{2g}(\mathbb{Z})$.*
2. *Les matrices de rotations, de translations dont la matrice symétrique B est de diagonale paire et J engendrent $\Gamma_{1,2}$.*

Ainsi, grâce à cette proposition, on voit que pour généraliser la formule issue de l'équation fonctionnelle de $\boldsymbol{\vartheta}$ à $\mathrm{Sp}_{2g}(\mathbb{Z})$ tout entier, il suffit de le faire sur les matrices de translation de diagonale quelconque.

Soit donc $\left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right)$ une telle matrice et $\Delta = \mathrm{Diag}(B) \in \mathscr{M}_g(\{0,1\})$ sa « diagonale » modulo 2.

On a de ce fait $\left(\begin{smallmatrix} I & B-\Delta \\ 0 & I \end{smallmatrix}\right) \in \Gamma_{1,2}$ et $\left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right) = \left(\begin{smallmatrix} I & B-\Delta \\ 0 & I \end{smallmatrix}\right)\left(\begin{smallmatrix} I & \Delta \\ 0 & I \end{smallmatrix}\right)$, ce qui ramène donc l'étude aux matrices de translation telles que la matrice $g \times g$ en haut à droite soit diagonale, à valeurs dans $\{0,1\}$.

Proposition 2.11. *On note $\mathbf{1} \in \mathbb{C}^g$ le vecteur $[1 \cdots 1]$ et si $\eta' \in \{0, \frac{1}{2}\}^g$ est une ligne d'une demi-caractéristique, on note $\overline{\eta}'$ le vecteur de $\{0, \frac{1}{2}\}^g$ tel que $\eta' + \overline{\eta}' = \frac{1}{2}\mathbf{1}$.*

Soit $\Delta \in \mathscr{M}_g(\{0,1\})$ une matrice diagonale. On a

$$\boldsymbol{\vartheta}(z, \Omega + \Delta) = \boldsymbol{\vartheta}\Big(z + \tfrac{1}{2}\Delta\mathbf{1}, \Omega\Big)$$

et

$$\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ \eta'' \end{smallmatrix}\right](0, \Omega + \Delta) = \exp(i\pi\, {}^t\eta'\Delta\eta')\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ \eta''+\Delta\overline{\eta}' \end{smallmatrix}\right](0, \Omega).$$

Démonstration. La preuve réside sur la même remarque qu'en genre 1, qui consiste tout simplement à utiliser que $n(n+1)$ est pair pour tout n :

$$\begin{aligned} {}^tn\Delta n = \sum_{i=1}^{g} \Delta_i n_i^2 &\equiv \sum_{i=1}^{g} \Delta_i n_i \mod 2 \\ &\equiv {}^tn\Delta\mathbf{1} \mod 2. \end{aligned}$$

Ainsi, de la définition de la série $\boldsymbol{\vartheta}$, on tire

$$\begin{aligned} \boldsymbol{\vartheta}(z, \Omega + \Delta) &= \sum_{n \in \mathbb{Z}^g} \exp(i\pi\, {}^tn(\Omega + \Delta)n + 2i\pi\, {}^tnz) \\ &= \sum_{n \in \mathbb{Z}^g} \exp(i\pi\, {}^tn\Omega n + i\pi\, {}^tn\Delta\mathbf{1} + 2i\pi\, {}^tnz) \\ &= \boldsymbol{\vartheta}\Big(z + \tfrac{1}{2}\Delta\mathbf{1}, \Omega\Big) \end{aligned}$$

puis, en l'appliquant au calcul des thêta constantes,

$$\begin{aligned} \boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ \eta'' \end{smallmatrix}\right](0, \Omega+\Delta) &= \exp(i\pi\, {}^t\eta'(\Omega + \Delta)\eta' + 2i\pi\, {}^t\eta'\eta'') \\ &\qquad \cdot \boldsymbol{\vartheta}\Big((\Omega + \Delta)\eta' + \eta'', \Omega + \Delta\Big) \\ &= \exp(i\pi\, {}^t\eta'\Delta\eta') \exp(i\pi\, {}^t\eta'\Omega\eta' + 2i\pi\, {}^t\eta'\eta'') \\ &\qquad \cdot \boldsymbol{\vartheta}\Big(\Omega\eta' + \eta'' + \Delta(\eta' + \tfrac{1}{2}\mathbf{1}), \Omega\Big) \\ &= \exp(i\pi\, {}^t\eta'\Delta\eta') \exp(i\pi\, {}^t\eta'\Omega\eta' + 2i\pi\, {}^t\eta'\eta'') \\ &\qquad \cdot \boldsymbol{\vartheta}\Big(\Omega\eta' + \eta'' + \Delta\overline{\eta}', \Omega\Big) \\ &= \exp(i\pi\, {}^t\eta'\Delta\eta')\boldsymbol{\vartheta}\left[\begin{smallmatrix} \eta' \\ \eta''+\Delta\overline{\eta}' \end{smallmatrix}\right](0, \Omega) \end{aligned}$$

la dernière égalité venant de ${}^t\eta'\Delta\overline{\eta}' = 0$. □

Cela nous permet donc de calculer toutes les thêta constantes par l'action de $\mathrm{Sp}_{2g}(\mathbb{Z})$. Il reste à voir comment ce dernier agit sur les noyaux et donc sur les demi-caractéristiques correspondantes. Pour cela, il faut préciser un peu l'application α_Γ décrite dans le diagramme (IV.2). Encore une fois, cela est expliqué en détails par Mumford dans [Mum 83]. La seule chose importante ici sont les égalités,

$$\begin{aligned}\alpha_\Gamma(\Omega x+y) &= {}^t(C\Omega+D)^{-1}(y+\Omega x)\\ &= \Omega'(Dx-Cy)+(Ay-Bx).\end{aligned}$$

La dernière égalité découle du fait que $\Gamma\in\mathrm{Sp}_{2g}(\mathbb{Z})$ et que Ω' est symétrique. On a dès lors

$${}^t(C\Omega+D)^{-1} = -\Omega' C + A,$$

ce qui permet d'expliciter l'action de $\mathrm{Sp}_{2g}(\mathbb{Z})$ sur les demi-caractéristiques :

$$\begin{array}{rccc}\alpha_\Gamma: & \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g) & \longrightarrow & \mathbb{C}^g/(\mathbb{Z}^g+\Omega'\mathbb{Z}^g)\\ & \Omega x+y & \longmapsto & \Omega'(Dx-Cy)+(Ay-Bx)\\ & \Omega(Ax+Cy)+(Bx+Dy) & \longmapsto & \Omega' x+y\end{array}$$

C'est le noyau de φ, suivant le diagramme (IV.2), qui nous intéresse. En termes de demi-caractéristiques, le noyau de β n'a pas changé, et on écrit, toujours sous forme de demi-caractéristiques,

$$\begin{aligned}\ker\varphi = \alpha_\Gamma^{-1}(\ker\beta) &= \alpha_\Gamma^{-1}(G_1)\\ &= \left\{\left[\begin{smallmatrix}Cy\\ Dy\end{smallmatrix}\right], y\in\tfrac{1}{2}\mathbb{Z}^g\right\}\end{aligned}\qquad\text{(IV.9)}$$

Application au noyau issu d'une configuration de Fano. En appliquant les résultats du paragraphe précédent à $g=3$, il reste à déterminer une matrice Γ qui transforme, via α_Γ, un groupe issu d'une configuration de Fano en G_1. Tout d'abord, dressons ce groupe, en respectant la construction issue de la figure IV.1 du plan de Fano :

$$G_2 = \left\{\left[\begin{smallmatrix}0&0&0\\0&0&0\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac12&0&0\\0&\frac12&0\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac12&0&\frac12\\0&0&0\end{smallmatrix}\right], \left[\begin{smallmatrix}0&0&\frac12\\0&\frac12&0\end{smallmatrix}\right], \left[\begin{smallmatrix}0&\frac12&\frac12\\\frac12&0&\frac12\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac12&\frac12&0\\\frac12&0&\frac12\end{smallmatrix}\right], \left[\begin{smallmatrix}0&\frac12&0\\\frac12&\frac12&\frac12\end{smallmatrix}\right], \left[\begin{smallmatrix}\frac12&\frac12&\frac12\\\frac12&\frac12&\frac12\end{smallmatrix}\right]\right\}.$$

On trouve facilement que la matrice symplectique

$$\Gamma = \begin{pmatrix}0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&1&0\\0&1&0&1&1&1\\0&0&1&0&1&0\end{pmatrix} \in \mathrm{S}_6(2) = \mathrm{Sp}_6(\mathbb{F}_2)$$

transforme G_2 en G_1 via l'application α_Γ, comme décrit en (IV.9). On note comme précédemment $\Omega' = \Gamma\cdot\Omega$ et on définit

$$B = \begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix} \text{ et } \Delta = \begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}.$$

Il suffit ensuite de décomposer, modulo 2, d'où l'absence de signes,

$$\Gamma = J\begin{pmatrix}I&B\\0&I\end{pmatrix}\begin{pmatrix}I&\Delta\\0&I\end{pmatrix} \in \mathrm{S}_2(6),$$

pour calculer les thêta constantes de $\mathbb{C}^3/(\mathbb{Z}^3+\Omega'\mathbb{Z}^3)$. On utilise pour cela l'équation fonctionnelle pour les deux premières matrices (formules IV.8 et IV.7) et sa généralisation (2.11) pour la dernière. On note $\Omega_1 = \left(\begin{smallmatrix} I & \Delta \\ 0 & I \end{smallmatrix}\right)\cdot\Omega$ et $\Omega_2 = \left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right)\cdot\Omega_1$ de sorte que $\Omega' = J\cdot\Omega_2$ et

$$\begin{aligned}\boldsymbol{\vartheta}\left[\begin{smallmatrix}0\\ \eta''\end{smallmatrix}\right](0,\Omega') &= \boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta''\\ 0\end{smallmatrix}\right](0,\Omega_2)\\ &= \exp(-i\pi\,{}^t\eta''B\eta'')\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta''\\ B\eta''\end{smallmatrix}\right](0,\Omega_1)\\ &= \exp(i\pi\,{}^t\eta''(\Delta-B)\eta'')\boldsymbol{\vartheta}\left[\begin{smallmatrix}\eta''\\ B\eta''+\Delta\overline{\eta}''\end{smallmatrix}\right](0,\Omega).\end{aligned}$$

Deux nouvelles familles de courbes. Il suffit désormais de programmer tout cela dans un logiciel tel Maple en procédant comme dans le cas des groupes tractables. On regroupe de même les 36 thêta constantes paires en 8 sous-ensembles.

- Le premier conduit comme précédemment aux calculs les plus lourds. En fixant 3 paramètres on obtient (§§) une autre famille à 4 paramètres. L'homographie inverse est assez délicate et coûteuse en temps et en mémoire.
  Néanmoins, on finit par obtenir un polynôme homogène en 8 variables, de degré total 24, de degré 6 en chaque variable et possédant cette fois 215601 monômes.
- Les sept autres conduisent, comme précédemment, à une même condition, à permutation des variables près, condition bien plus simple. En effet, il s'agit d'un polynôme homogène en 8 variables, de 24 monômes, de degré total 4, linéaire en chaque variable.

2.4 Résumé de la 1re partie : les 4 familles à 4 paramètres

Théorème 2.12. *L'ensemble des courbes hyperelliptiques de genre 3 pour lesquelles il existe une courbe hyperelliptique de genre 3 et une 2−2−2 isogénie entre leurs jacobiennes est composé de 4 familles irréductibles à 4 paramètres, décrites ci-dessous par des polynômes irréductibles en x_i, à permutation des variables près.*

Famille tractable (*f-1*). C'est la condition pour qu'étant données trois paires (x_1,x_2), (x_3,x_4) et (x_5,x_6), il existe une involution qui échange les éléments de ces paires :

$$\begin{aligned}x_1x_2x_3 + x_1x_2x_4 - x_1x_2x_5 - x_1x_2x_6 - x_1x_3x_4 + x_1x_5x_6 \\ - x_2x_3x_4 + x_2x_5x_6 + x_3x_4x_5 + x_3x_4x_6 - x_3x_5x_6 - x_4x_5x_6.\end{aligned} \qquad (f\text{-}1)$$

Le groupe qui laisse ce polynôme (anti-)invariant est engendré par les transpositions (12), (34) et (46) mais aussi par $\mathfrak{S}_3$ agissant sur ces paires : c'est un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathfrak{S}_3$ de cardinal 48. On peut enfin l'exprimer par une trace « tordue » par la signature :

$$\widetilde{\mathrm{Tr}}\,(x_1x_2x_3 + x_1x_2x_4) := \sum_{\sigma\in\mathfrak{S}_3}\varepsilon(\sigma)(x_1x_2x_3 + x_1x_2x_4)^{\varphi(\sigma)}$$

où $\varphi(\sigma)\in\mathfrak{S}_6$ est la permutation obtenue par l'action de σ sur les paires ordonnées (x_1,x_2), (x_3,x_4) et (x_5,x_6).

(§§). Il faut ici un peu plus de mémoire mais environ 2min30s pour effectuer ce calcul sur un ordinateur personnel.

Famille tractable (*f-2*). Elle est donnée par un polynôme en 8 variable de degré total 16, de degré 4 en chaque variable et possédant 19591 monômes. Comme on va le voir dans la section suivante, il provient de l'existence d'une unique application trigonale (*cf.* théorème 3.5). Le groupe qui le stabilise est par exemple engendré par les transpositions (12), (34), (56) et (78) puis par $\mathfrak{S}_4$ agissant sur ces paires. C'est un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathfrak{S}_4$ d'indice 105 dans $\mathfrak{S}_8$, qui correspond aux groupes tractables que l'on a déjà dénombrés en 2.1. Enfin, cette famille peut être donnée par la trace (classique) sous l'action de ce groupe stabilisateur d'un polynôme de 158 monômes ; *cf.* www.normalesup.org/~iboyer/files/trac.mw.

Famille Fano (*f-3*). Elle correspond (*cf.* théorème 3.11 suivant) à l'existence d'une homographie transformant (x_1, x_2, x_3, x_4) en (x_5, x_6, x_7, x_8) :

$$\begin{aligned} &x_1x_2x_5x_7 - x_1x_2x_5x_8 - x_1x_2x_6x_7 + x_1x_2x_6x_8 - x_1x_3x_5x_6 + x_1x_3x_5x_8 \\ &+ x_1x_3x_6x_7 - x_1x_3x_7x_8 + x_1x_4x_5x_6 - x_1x_4x_5x_7 - x_1x_4x_6x_8 + x_1x_4x_7x_8 \\ &+ x_2x_3x_5x_6 - x_2x_3x_5x_7 - x_2x_3x_6x_8 + x_2x_3x_7x_8 - x_2x_4x_5x_6 + x_2x_4x_5x_8 \\ &+ x_2x_4x_6x_7 - x_2x_4x_7x_8 + x_3x_4x_5x_7 - x_3x_4x_5x_8 - x_3x_4x_6x_7 + x_3x_4x_6x_8. \end{aligned} \tag{*f-3*}$$

Le groupe qui stabilise ce polynôme est engendré par le groupe symétrique $\mathfrak{S}_4$ agissant en parallèle sur les deux ensembles de 4 racines, par la permutation qui échange ces deux groupes, ainsi que par les permutations (56)(78), (57)(68) et (58)(67). Ce groupe est un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathfrak{S}_4$, d'ordre 192, d'indice 210 : chacun des 30 groupes vus en 2.2 correspondant à 7 polynômes. Enfin, on peut encore exprimer ce polynôme par une trace « tordue » :

$$\widetilde{\mathrm{Tr}}_{\mathfrak{S}_4}(x_1x_2x_5x_7) := \sum_{\sigma\in\mathfrak{S}_4} \varepsilon(\sigma)(x_1x_2x_5x_7)^{\varphi(\sigma)}$$

où $\varphi(\sigma) \in \mathfrak{S}_8$ est la permutation qui agit par σ sur $\{1,2,3,4\}$ *et* $\{5,6,7,8\}$.

Famille Fano (*f-4*). Elle est donnée à un polynôme de degré total 24, de degré 6 en chaque variable et possédant 215601 monômes. Le stabilisateur est assez important puisqu'il s'agit du sous-groupe de $\mathfrak{S}_8$ d'ordre 1344, isomorphe à un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathrm{PSL}_3(\mathbb{F}_2)$. On peut aussi l'exprimer par la trace d'un polynôme de 282 monômes ; *cf.* www.normalesup.org/~iboyer/files/fano.mw.

L'objet de la section suivante est l'étude des familles (*f-2*) et (*f-3*). Celles-ci sont duales en ce sens où si une courbe fait partie de l'une, alors la courbe, dont la jacobienne est $2-2-2$ isogène à celle de la première, fait partie de l'autre famille.

Pour les deux autres familles, les deux courbes appartiennent à la même famille puisque c'est le cas dans la famille (*f-1*). Il en est ainsi nécessairement de même pour la famille (*f-4*).

Pour finir, (*f-1*) est le cas particulier du genre 3, traité par J.-F. Mestre, dans [Mes 13]. Par ailleurs, B. Smith, dans [Smi 10], exhibe des exemples de courbes appartenant à la famille (*f-4*).

— 3 —
Courbes « tractables » et de « Fano », construction trigonale

3.1 Applications trigonales

Dans [Rec 74], S. Recillas expose une construction dite « trigonale » qui prolonge la construction bigonale connue depuis Humbert (en 1901) et explicitée par J.-B. Bost et J.-F. Mestre dans [BM 88]. Ces constructions *bi-* et *tri*-gonales permettent de déterminer des jacobiennes qui sont isogènes et dont le noyau est lagrangien *i.e.* isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$ où n est maximal, égal à la dimension des jacobiennes (ici 2 ou 3).

Dans [DL 99], R. Livné et R. Donagi partent d'un point de vue un peu plus général que celui de Humbert, S. Recillas ou celui qui va nous intéresser ici. Ils considèrent en effet trois courbes $\mathscr{C}, \widetilde{\mathscr{C}}$ et K et deux applications surjectives φ et π comme suit :

$$\widetilde{\mathscr{C}} \xrightarrow{\pi} \mathscr{C} \xrightarrow{\varphi} K \tag{IV.10}$$

telles que π est un recouvrement double et φ est de degré 2 ou 3 suivant que la construction est dite *bi-* ou *tri*-gonale.

Ici, nos courbes sont hyperelliptiques et le recouvrement de degré 2 naturel est le recouvrement hyperelliptique, ce qui transforme (IV.10) en

$$\mathscr{H} \xrightarrow{\pi} \mathbb{P}^1 \xrightarrow{\varphi} \mathbb{P}^1$$

où $\mathbb{P}^1$ est la droite projective sur un corps K, $\mathscr{H}$ est une courbe hyperelliptique de genre 3 et φ est de degré 3. De plus, on demande à φ d'identifier des paires de points de Weierstrass de $\mathscr{H}$, afin d'assurer que le noyau de l'isogénie que l'on va construire est tractable, *i.e.* engendré précisément par ces différences des points identifiés (voir la définition 2.2).

On sait qu'il y a génériquement deux telles applications trigonales φ pour une courbe hyperelliptique quelconque de genre 3. R. Donagi et R. Livné, dans [DL 99], donnent deux démonstrations naturelles de ce fait qui permettent une construction explicite, comme décrite par B. Smith, dans [Smi 08].

On propose de redémontrer ce fait afin d'introduire une nouvelle paramétrisation du problème, plus efficace pour la construction explicite.

Proposition 3.1. *Pour une courbe hyperelliptique $\mathscr{H}$, il y a 0, 1 ou 2 applications trigonales vérifiant les propriétés ci-dessus, à transformation homographique près.*

Démonstration. Grâce aux homographies de $\mathbb{P}^1$, on peut rigidifier une éventuelle application trigonale en imposant les valeurs prises sur les paires de points. On peut par exemple demander qu'elle vaille 0, 1 et ∞ sur trois des quatre paires. Dès lors, il nous faut montrer qu'il y a exactement 0, 1 ou 2 telles applications « rigidifiées ».

On note (x_i, x_{i+4}), pour $i = 1, \dots, 4$, les quatre paires de points de Weierstrass et on demande donc que x_1 et x_5 s'envoient sur 0, x_2 et x_6 sur l'infini et x_3 et x_7 sur 1. Cela impose que la fonction trigonale $\varphi(x)$ soit de la forme :

$$\varphi(x) = \mu \frac{(x-x_1)(x-x_5)}{(x-x_2)(x-x_6)} \frac{x-a}{x-b}$$

avec donc $\varphi(x_3) = \varphi(x_7) = 1$ et $\varphi(x_4) = \varphi(x_8)$. Les deux premières égalités sont linéaires en a et b.

Ce système linéaire ne présente aucune solution si la courbe hyperelliptique appartient à la famille étudiée par J.-F. Mestre dans [Mes 13]. Sinon, en réinjectant cette solution dans la dernière équation $\varphi(x_4) = \varphi(x_8)$, on aboutit à un polynôme de degré 2 en μ : on a donc bien génériquement deux fonctions trigonales qui se confondent en une seule lorsque ce discriminant est nul. On retrouve alors le polynôme de degré total 16 qui définit la famille (*f-2*). □

Afin de pouvoir travailler avec cette famille de courbes hyperelliptiques, il est nécessaire d'en donner une paramétrisation plus simple.

Proposition 3.2. *Soit $P(x) = x^2 + bx + c$ et $a, d, e \in K$. Alors, la famille des courbes hyperelliptiques possédant au moins une application trigonale peut se décrire par*

$$y^2 = f(x) = f_1(x) f_2(x) f_3(x) f_4(x),$$

avec

$$\begin{aligned} f_1(x) &= P(x) \\ f_2(x) &= P(x) + a(x-1)(x-d) \\ f_3(x) &= P(x) - a(x-d) \\ f_4(x) &= f_2(x) \frac{\varphi(x) - \varphi(e)}{x-e} \end{aligned}$$

où

$$\varphi(x) = \frac{x f_1(x)}{f_2(x)}$$

est une application trigonale. La seconde est

$$\widetilde{\varphi}\,(x) = \frac{f_1(x)}{f_2(x)} \frac{x(ae - ad - ed - c - be) + (d-e)(ad+c)}{\big((d-e)x + ed + bd + c\big)(ad+c)}.$$

Démonstration. Tout étant défini à homographie près, on peut, comme précédemment rigidifier φ. Cette fois, on impose trois conditions au départ, mais aussi à l'arrivée. On choisit ainsi d'avoir $0, 1$ et l'∞ comme points fixes de φ, qui correspondent à trois paires de points de Weierstrass.

La première paire de points de Weierstrass, racines de $f_1(x) := x^2 + bx + c$, s'envoie sur 0 et la deuxième paire, correspondant à f_2 sur l'infini. Comme on demande $\varphi(\infty) = \infty$, cela impose déjà la forme de $\varphi(x)$

$$\varphi(x) = \frac{x f_1(x)}{f_2(x)}.$$

On veut ensuite $\varphi(1) = 1$, ce qui impose $f_2(1) = f_1(1)$, soit encore que $(x-1)$ divise $f_2(x) - f_1(x)$ d'où deux nouveaux paramètres a et d tels que

$$f_2(x) := f_1(x) + a(x-1)(x-d).$$

D'autre part, en les zéros de f_3, la trigonale φ doit valoir 1, ce qui impose, par un calcul immédiat

$$f_3(x) := f_1(x) - a(x-d).$$

Il ne reste plus qu'à déterminer f_4 ce que l'on fait en imposant qu'en un certain point e, $\varphi(e)$ soit la valeur commune aux deux racines de f_4. Ceci définit entièrement f_4 par le polynôme de degré 2 :

$$f_4(x) := f_2(x)\frac{\varphi(x) - \varphi(e)}{x-e}.$$

Quant à la deuxième trigonale, elle se trouve simplement, en posant

$$\widetilde{\varphi}\,(x) = \frac{f_1(x)}{f_2(x)}\frac{\alpha x + \beta}{\gamma x + \delta}$$

et en cherchant $\alpha, \beta, \gamma, \delta$ homogènes, tels qu'il existe des paramètres $s, t \in K$ qui vérifient $f_3(x)$ proportionnel à $f_2(x)(\widetilde{\varphi}\,(x) - \widetilde{\varphi}\,(s))$ et $f_4(x)$ proportionnel à $f_2(x)(\widetilde{\varphi}\,(x) - \widetilde{\varphi}\,(t))$. On trouve les deux solutions de la proposition. □

Remarque 3.3. Pour la suite, on peut d'ores et déjà remarquer que la condition pour qu'il n'y ait qu'une seule trigonale correspond simplement à $e = d$. Dans ce cas, $f_4(x)$ se réduit à

$$f_4(x) := P(x) + ad(1-x)$$

et l'on remarque que les quatre points $0, 1, d, \infty$ jouent les mêmes rôles, à savoir d'une part identifier par φ les paires de points de Weierstrass, et d'autre part être des points fixes de φ.

Enfin, il est intéressant de remarquer que le birapport $[f_2, f_1; f_3, f_4]$ vaut alors précisément d.

3.2 Construction trigonale

Une fois données notre courbe hyperelliptique $\mathscr{H}$ de genre 3 et une application trigonale φ, il est assez aisé de construire une courbe de genre 3 dont la jacobienne est 2−2−2 isogène à celle de $\mathscr{H}$. B. Smith donne, dans [Smi 08], une construction explicite d'une telle courbe. Commençons par dresser le diagramme de la construction trigonale :

$$\begin{array}{ccc} & & \mathscr{H} \\ & & \downarrow \pi \\ \mathscr{C} & & \mathbb{P}^1 \\ & \searrow^{\psi} \quad \swarrow_{\varphi} & \\ & \mathbb{P}^1 & \end{array} \qquad \text{(IV.11)}$$

où ψ est une application de degré 4. On note $\imath : \mathscr{H} \to \mathscr{H}$, l'involution hyperelliptique.

À partir de ce diagramme, on peut construire une correspondance entre $\mathscr{H}$ et $\mathscr{C}$ qui nous permet de donner une équation de $\mathscr{C}$.

On commence par considérer un point Q de $\mathscr{C}$ et $T = \psi(Q)$. On a naturellement six points de $\mathscr{H}$, P_1, P_2 et P_3 et leurs conjugués par l'involution hyperelliptique $\imath$, tels que leurs images par $\varphi \circ \pi$ valent précisément $T = \psi(Q)$.

L'existence d'une correspondance entre les deux courbes permet de séparer ces 6 points en 2 groupes de 3, qui définiront, chacun, une correspondance.

Pour écrire cette correspondance ainsi que l'équation de la courbe $\mathscr{C}$, une interpolation de Lagrange suffit : il existe un polynôme de degré 2,

$$b(x) = b_0 x^2 + b_1 x + b_2,$$

tel que les coordonnées des points P_i sont

$$\Big(\pi(P_i), b(\pi(P_i))\Big).$$

Toutefois, dans la pratique, il s'avère bien plus efficace d'interpoler nos trois points par une homographie

$$h(x) = \Lambda \frac{x+V}{x+W}.$$

Bien évidemment, le polynôme $-b$ ou l'homographie $-h$ interpolent les cordonnées des points $\imath(P_i)$ et forment l'autre correspondance. Ainsi, on obtient deux copies de la courbe $\mathscr{C}$ en considérant l'ensemble des points Λ, V, W, T tels que

$$\Lambda^2 (x+V)^2 = (x+W)^2 f(x) \mod T f_2(x) - x f_1(x).$$

De même que l'homographie simplifie les calculs, de même, il s'avère plus efficace « d'égaliser » les degrés en x en considérant plutôt l'équation

$$f_1 f_2 \Lambda^2 (x+V)^2 - f_3 f_4 (x+W)^2 \mod T f_2(x) - x f_1(x) \tag{IV.12}$$

ce qui s'obtient en changeant essentiellement h par

$$\tilde{h}\,(x) = f_1 f_2 h(x).$$

En effectuant la division euclidienne par x et en annulant les coefficients de degrés 0, 1 et 2, on obtient trois équations en Λ, V et W. On remarque que ces équations sont linéaires en $U := \Lambda^2$: on peut donc facilement éliminer U, ce qui laisse deux équations. En prenant leur résultant [(⋆)] en W, on aboutit à une unique équation en T et V. C'est en fait la même pour les deux copies de $\mathscr{C}$, puisque l'on passe de l'une à l'autre en faisant $\Lambda \mapsto -\Lambda$, qui laisse U invariant : on note encore $\mathscr{C}(T, V)$ l'équation polynomiale de cette courbe plane. Notons au passage que W peut s'écrire comme une fraction rationnelle de degré 2 en T.

Un ordinateur personnel permet de calculer les 200 monômes en T, V, a, b, c, d et e de $\mathscr{C}(T, V)$ en moins d'une seconde. Ce polynôme est de degré total 6 en T, V et 4 respectivement en T et V. Par ailleurs, on peut recommencer le même travail pour la seconde trigonale de la proposition 3.2.

(⋆). Ou bien en V, c'est un choix arbitraire.

Remarque 3.4 (Corps de définition). On remarque que la courbe $\mathscr{C}$ est définie sur le même corps que $\mathscr{H}$ et φ. L'équation d'une des deux correspondances naturelles entre $\mathscr{H}$ et $\mathscr{C}$ n'est autre que

$$\begin{cases} y^2 = f_1 f_2 f_3 f_4 \\ T = \varphi(x) \\ y = \Lambda \dfrac{x+V}{x+W} f_1 f_2 \\ 0 = \mathscr{C}(T,V) \end{cases} \tag{IV.13}$$

l'autre correspondance s'obtenant en remplaçant y par $-y$.

D'autre part, le calcul explicite [(◇)] de cette correspondance montre qu'elle est « presque » définie sur le même corps de base que les courbes $\mathscr{H}$ et $\mathscr{C}$. En effet, on peut écrire

$$\Lambda = \sqrt{\alpha} R(T,V)$$

où R est une fraction rationnelle en T et V définie sur le corps de base. On retrouve là ce que B. Smith explique dans [Smi 08].

Aussi, en modifiant l'équation de départ de $\mathscr{H}$ en $y^2 = \alpha f_1 f_2 f_3 f_4$, c'est-à-dire en prenant une tordue quadratique de $\mathscr{H}$, on obtient une correspondance définie sur le corps de base. Grâce au calcul explicite de cette correspondance, on peut choisir

$$\alpha = (1+b+c)(c+ad)(e^2+ae^2+be+ad+c-ae+ade). \tag{IV.14}$$

Enfin notons qu'à un couple (T,V) donné, on a trois x, via la trigonale, chacun correspondant à un unique y. Réciproquement, à un x donné on associe un unique T, qui définit 4 abscisses V solutions de $\mathscr{C}(T,V)$. Parmi ces 4, seulement 2 vérifient $y = \Lambda \frac{x+V}{x+W} f_1 f_2$. Au final, on a une correspondance $(3,2)$ entre $\mathscr{H}$ et $\mathscr{C}$.

3.3 Une ou deux applications trigonales

Équation quartique. On vient de donner une équation de la courbe plane $\mathscr{C}$, qui est de genre 3. Il est donc tout à fait naturel de vouloir l'écrire sous forme quartique ou hyperelliptique, puisque ce sont les deux seules possibilités en genre 3.

Pour cela, il suffit de trouver une base de différentielles et de faire le changement de variables adéquat. Il se trouve que cette base est assez difficile à calculer, du moins avec un ordinateur personnel. L'idée est de fixer quelques paramètres et de « deviner », par une interpolation de faible degré, un changement de variables plausible, dont on vérifie, *a posteriori*, qu'il est convenable. On trouve sans trop de difficulté

$$D_1 = \frac{V}{T} - \frac{ad+c}{e} \quad \text{et}$$
$$D_2 = \frac{(c+ad)(ade+bad+ae-be+bc)T + e(c+ad-ae-e)V^2 + e(c-e)(c+ad)}{(ad+c)T+eV},$$

ce qui conduit à poser

$$S = \frac{V}{T} \quad \text{et} \quad R = D_2\left(\frac{V}{S}, V\right)$$

(◇). C'est-à-dire exprimer Λ et W en fonction de T et V.

et qui permet, en prenant le résultant de $\mathscr{C}\left(\frac{V}{S}, V\right)$ et $R - D_2\left(\frac{V}{S}, V\right)$, d'éliminer V. On obtient alors une équation polynomiale $Q(S, R)$ de degré total 4, mais aussi 4 en chacune des deux variables.

Il ne nous reste plus qu'à calculer les éventuels points singuliers de cette courbe plane. Cette vérification est assez aisée : par exemple le calcul de résultant

$$\mathrm{Res}_S\left(\mathrm{Res}_R\left(\frac{\mathrm{d}Q(S,R)}{\mathrm{d}S}, Q(S,R)\right), \mathrm{Res}_R\left(\frac{\mathrm{d}Q(S,R)}{\mathrm{d}R}, Q(S,R)\right)\right)$$

montre qu'il n'y a « génériquement » pas de points singuliers, c'est-à-dire que le résultant n'est pas identiquement nul, mais un polynôme en a, b, c, d et e. Là où il est non nul, on a effectivement une équation quartique de $\mathscr{C}$.

Équation hyperelliptique. Ce résultant comporte, néanmoins, des « facteurs parasites ». Pour savoir précisément le lieu où l'équation ci-dessus n'est pas quartique, on calcule son discriminant, par exemple en utilisant la méthode (‡) décrite dans [GKZ 08].

Hormis les facteurs du discriminant de $\mathscr{H}$ qui apparaissent tous à diverses puissances, on trouve un unique facteur susceptible d'annuler le discriminant de Q. Il s'agit simplement d'une puissance de $(d - e)$, ce qui démontre le théorème suivant.

Théorème 3.5. *On a les équivalences suivantes :*

(i) La courbe hyperelliptique $\mathscr{H}$ possède exactement une application trigonale.

(ii) $d = e$ (c'est-à-dire les quatre abscisses qui identifient les points de $\mathscr{H}$ peuvent être choisies comme points fixes de la trigonale).

(iii) La courbe $\mathscr{C}$, de genre 3, est hyperelliptique.

Démonstration. En effet, *(i)⇔(ii)* est l'objet de la remarque 3.3. D'autre part, comme le discriminant de $\mathscr{H}$ est non-nul par hypothèse (afin que son genre soit bien 3), l'unique facteur susceptible d'annuler le discriminant de Q est $(d - e)$, ce qui montre *(ii)⇔(iii)*. □

Remarque 3.6. En fait, on peut voir d'une autre manière que, dans le cas où $d = e$, la courbe $\mathscr{C}$ devient hyperelliptique. En effet, il existe une involution entre les deux courbes correspondant aux deux applications trigonales. Cette dernière, quand $d = e$, ne dégénère pas en l'identité sur $\mathscr{C}$, mais en une involution. Plus précisément, après le changement de variables $T = \frac{V}{S}$, l'application

$$V \mapsto \frac{ad + c}{V}. \tag{IV.15}$$

est involutive sur la courbe $\mathscr{C}\left(\frac{V}{S}, V\right)$.

Cette remarque permet de décrire, lorsque $d = e$, le modèle de Weierstrass de la courbe $\mathscr{C}$.

(‡). On se place en caractéristique différente de 2.

3.4 Étude de la courbe $\mathscr{C}$, de type « Fano »

On se place, jusqu'à la fin, dans le cas où l'on a une unique application trigonale, c'est-à-dire que l'on fixe $e = d$. L'équation initiale de $\mathscr{C}$, en T et V se réduit à 161 monômes en T, V, a, b, c, d. On considère à nouveau le changement de variables $T = \frac{V}{S}$.

Partant de l'involution (IV.15), on commence par poser $z = V + \frac{ad+c}{V}$ invariant par cette involution puis on élimine V entre $\mathscr{C}\left(\frac{V}{S}, V\right)$ et ce z.

On obtient une équation $\mathscr{P}(z, S)$ de degré 2 en z et 4 en S. Le calcul de son discriminant en z montre qu'il s'agit bien d'une courbe de genre 0. En effet, si l'on note $\Delta_z = \Delta_z(S)$ son discriminant « réduit », c'est-à-dire sans facteurs carrés, on aboutit à l'équation d'une conique en (δ, S),

$$\delta^2 := \Delta_z = (1+b+c)(d^2+bd+c)\Big(cS^2 + 2(ad+c)S + (a+1)(ad+c)\Big). \quad \text{(IV.16)}$$

Pour écrire la courbe sous forme de Weierstrass, il faut paramétriser cette conique, qui n'a visiblement pas de points rationnels sur le corps de base. Avant cela, on va s'intéresser au corps de définition des points de Weierstrass, qui fournissent de bons candidats pour donner une paramétrisation de la conique.

3.4.1 Corps de définition des points de Weierstrass

Les points de Weierstrass sont obtenus comme points fixes de l'involution (IV.15), c'est-à-dire pour $V^2 = ad+c$. Ainsi, dans un corps dans lequel on a tous les points de Weierstrass, on a aussi la racine carrée de $ad+c$. En fait, la réciproque est presque vraie et tient du fait que l'on a choisi arbitrairement (⊛) dans l'équation (IV.12) « d'égaliser » le degré en x en scindant $f = f_1f_2f_3f_4$ en (f_1f_2) et (f_3f_4). Afin d'expliquer le lien entre l'involution $V \mapsto \frac{ad+c}{V}$ et ce choix de partition de f, commençons par introduire une notation.

Notation 3.7. *Pour deux polynômes $f(x)$ et $g(x)$, on note $[f,g](x)$ le polynôme*

$$[f,g](x) := f(x)g'(x) - f'(x)g(x).$$

Si $\deg f = \deg g$, le degré de $[f,g](x)$ est, en situation générale, $2\deg f - 2$. Ainsi, si $f(x)$ et $g(x)$ sont des polynômes de degré 2, alors $[f,g](x)$ l'est aussi. On a une proposition facile, qui nous sert pour la suite.

Proposition 3.8. *Soient $f(x)$ et $g(x)$ des polynômes de degré 2. Alors, le discriminant réduit de $[f,g](x)$ n'est autre que le résultant de f et g.*

En particulier, $[f,g](x)$ est scindé si et seulement si $\mathrm{Res}_x(f,g)$ est un carré parfait. Un calcul explicite nous montre la proposition suivante.

Proposition 3.9. *On considère une équation du type (IV.12) où les rôles des f_i sont échangés :*

$$f_kf_l\Lambda^2(x+V)^2 - f_if_j(x+V)^2 \mod Tf_2(x) - xf_1(x).$$

(⊛). Dans la pratique, ce choix est celui qui permet d'avoir les expressions les plus simples pour l'équation de $\mathscr{C}$ et de ses points de Weierstrass.

Alors, si l'on note

$$[f_i, f_j](x) = \alpha(x^2 + \beta x + \gamma),$$

l'involution en V est donnée par

$$V \mapsto \frac{\frac{\beta}{2}V - \gamma}{V - \frac{\beta}{2}}.$$

Remarquons d'une part que cette involution échange les opposés des racines de f_i et de f_j. D'autre part, les *points fixes* de cette involution sont les opposés des racines de $[f_i, f_j](x)$. Mis bout à bout, tous ces résultats montrent la partie nécessaire de la proposition qui suit.

Proposition 3.10. *Le corps engendré par les points de Weierstrass de $\mathscr{C}$ est celui dans lequel tous les résultants* $\mathrm{Res}_x(f_i, f_j)$ *sont des carrés.*

En fait, cette extension de corps est galoisienne de groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^3$: si l'on ajoute la racine carrée d'un résultant, on scinde les points de Weierstrass en deux groupes de 4 et d'autre part, le produit de quatre résultants différents est toujours un carré.

Il est facile de vérifier que cette extension contient bien les points de Weierstrass de $\mathscr{C}$. Pour cela, on effectue un changement de variables de telle façon que les résultants soient des carrés. Ceci est assez facile et s'obtient par exemple avec les équations suivantes :

$$\begin{aligned} a &= \frac{A^2 - dB^2 + d + dC^2 - C^2 - d^2}{d(d-1)}, \\ b &= \frac{A^2 + 1 - B^2 - d^2}{d-1}, \\ c &= \frac{dB^2 + d^2 - d - A^2}{d-1}, \end{aligned}$$

avec comme nouvelles variables A, B, C, d et comme automorphismes, les applications $A \mapsto -A$, $B \mapsto -B$ et $C \mapsto -C$. En particulier, on a $ad + c = C^2$

3.4.2 Modèle de Weierstrass de la courbe $\mathscr{C}$ de type « Fano »

Si l'on se place sur l'extension de degré 8 dans laquelle tous les points de Weierstrass sont définis, on peut donner une paramétrisation de la conique (IV.16) grâce à un point de Weierstrass. Sur le modèle $\mathscr{C}\left(\frac{V}{S}, V\right)$, les points de Weierstrass sont donnés par $V = \pm C$ et l'on considère donc un point (C, S_1) tel que $\mathscr{C}\left(\frac{C}{S_1}, C\right) = 0$. En ce point, $z = 2C$ et Δ_z est nécessairement un carré : la conique (IV.16) possède donc un point rationnel, que l'on note (δ_1, S_1). On effectue ensuite la paramétrisation $\delta = \delta_1 + X(S - S_1)$ qui nous permet de donner une solution z_1 à l'équation $\mathscr{P}(z, S)$. L'équation de $\mathscr{C}$, en V et S, devient

$$V + \frac{C^2}{V} - z_1 = 0,$$

ou encore, en prenant le déterminant en V, que l'on note Y^2,

$$Y^2 = z_1^2 - 4C^2.$$

Cela nous permet de donner une équation explicite de $\mathscr{C}$ sous forme de Weierstrass au-dessus de $\mathbb{P}^1$ dont on peut s'assurer directement que ses 8 points de Weierstrass vérifient la relation, à permutation des variables près, définissant la famille Fano (*f-3*).

Caractérisation géométrique de la famille Fano (*f-3*). Il y a un argument géométrique plus efficace pour s'assurer que la courbe $\mathscr{C}$ est de type « Fano », qui, de plus, nous permet de simplifier l'expression des points de Weierstrass.

Théorème 3.11. *Une courbe hyperelliptique* $Y^2 = \prod_{i=1}^{8}(X - X_i)$ *appartient à la famille Fano (f-3) si et seulement si il existe une partition de ses points de Weierstrass en deux ensembles de 4 possédant un birapport commun.*

Autrement dit, les $j-$*invariants des partitions de 4 sont identiques ou encore, il existe une homographie qui envoie les points du premier ensemble sur ceux du second.*

Démonstration. C'est un calcul immédiat. □

Dans notre cas, il suffit de calculer les 70 $j-$invariants possibles à partir de quatre points de Weierstrass : on en trouve deux égaux, qui correspondent bien à une partition des 8 points. De plus, cette valeur commune est le $j-$invariant, de la courbe $y^2 - x(x-1)(x-d)$ dont les 4 points de Weierstrass sont les points fixes de l'application trigonale φ. Ainsi, après homographie, les points de ramification d'un modèle de Weierstrass de $\mathscr{C}$ sont :

$$\begin{array}{llll} \mathscr{W}_1{:=}\infty & \mathscr{W}_2{:=}0 & \mathscr{W}_3{:=}1 & \mathscr{W}_4{:=}d \\ \mathscr{W}_5{:=}\dfrac{A+C+d}{B+C+1} & \mathscr{W}_6{:=}\dfrac{(B-C-1)d}{A-C-d} & \mathscr{W}_7{:=}\dfrac{Bd-Cd+A+C}{A+B-d+1} & \mathscr{W}_8{:=}\dfrac{(A+B+d-1)d}{Bd+Cd+A-C}. \end{array} \tag{IV.17}$$

Enfin, pour écrire totalement la courbe $\mathscr{C}$ sous forme de Weierstrass il faut préciser le coefficient de « tordue quadratique » :

$$Y^2 = (B+C+1)(C+d-A)(A+B-d+1)(Bd+Cd+A-C)\prod_{i=2}^{8}(X-\mathscr{W}_i). \tag{IV.18}$$

Remarque 3.12. Ainsi, une courbe de la famille Fano (*f-3*) n'est autre que la donnée d'un paramètre d et d'une homographie, déterminée par 3 paramètres, ce qui forme bien une famille à 4 paramètres. Cette caractérisation géométrique permet de donner des équations simples pour passer des familles (*f-2*) aux familles (*f-3*).

Passage d'une courbe de type « tractable » à une courbe de type « Fano ». En partant de la description de la famille tractable (*f-2*) proposée dans la proposition 3.2, on peut calculer directement l'équation de la courbe de « type Fano » en utilisant le fait que $\infty, 0, 1, d$ sont quatre points de Weierstrass et qu'une homographie donnant les quatre autres points est

$$\mathscr{J} : w \mapsto \frac{(\overline{x}_{1,3} + x_{3,4})w - d(\overline{x}_{1,4} + x_{3,4})}{(x_{1,4} + x_{3,4})w - (x_{1,3} + x_{3,4})} \tag{IV.19}$$

où $x_{i,j}$ et $\overline{x}_{i,j}$ sont les racines de $[f_i, f_j](x)$. Notons que cela définit en fait 8 homographies, qui sont données par les 8 automorphismes de l'extension de corps de groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^3$, ce qui donne, au final, *8 courbes isomorphes*.

Passage d'une courbe de type « Fano » à une courbe de type « tractable ». La caractérisation du théorème 3.11 permet aussi « d'inverser » les calculs : au lieu de partir d'une courbe de la famille tractable (*f-2*), on veut désormais partir d'une courbe de la famille Fano (*f-3*). Pour cela, on rigidifie l'équation d'une courbe de cette famille, en imposant $0, 1, \infty$ comme points de Weierstrass, puis en demandant aux ensembles

$$\{\infty, 0, 1, x_4\} \text{ et } \{x_5, x_6, x_7, x_8\}$$

d'avoir le même $j-$invariant. On choisit donc x_8 pour qu'il existe une homographie transformant le premier ensemble en le second, par exemple,

$$x_8 = \frac{x_7x_6 - x_5x_7 - x_7x_6x_4 + x_5x_6x_4}{x_6 - x_5 - x_7x_4 + x_5x_4}.$$

En imposant la même homographie à la courbe (IV.18), cela impose un ordre des points de Weierstrass des deux courbes, qu'il suffit ensuite d'identifier. On obtient, par exemple :

$$\begin{aligned} A &= -\frac{(x_5x_6 - x_6x_7 - x_5 + x_6)(x_4 - 1)x_4}{x_4x_5x_6 - x_4x_6x_7 - x_4x_6 + x_4x_7 - x_5x_7 + x_6x_7} \\ B &= \frac{(x_4 - 1)(x_4x_5 - x_4x_7 - x_5x_7 + x_6x_7}{x_4x_5x_6 - x_4x_6x_7 - x_4x_6 + x_4x_7 - x_5x_7 + x_6x_7} \\ C &= \frac{(x_4x_5 - x_4x_7 - x_5x_6 + x_5x_7 - x_5 + x_6)x_4}{x_4x_5x_6 - x_4x_6x_7 - x_4x_6 + x_4x_7 - x_5x_7 + x_6x_7} \\ d &= x_4. \end{aligned} \tag{IV.20}$$

Notons enfin que la courbe tractable $\mathscr{H}$ définie par ces relations n'est pas tout à fait la bonne puisque sa jacobienne est isogène à celle d'une tordue quadratique de $Y^2 = \prod(X - x_i)$ comme le montre l'équation (IV.18). Néanmoins cela n'a pas beaucoup d'importance puisqu'il suffit (§) de multiplier l'équation de la courbe $\mathscr{H}$ par le même coefficient que dans (IV.18).

Noyau de la $2-2-2$ isogénie. Dans la section 2.3.2, on a caractérisé les familles Fano (*f-3*) et (*f-4*) par le noyau de la $2-2-2$ isogénie entre les jacobiennes. On peut vérifier cela, grâce à la $(3, 2)$ correspondance (IV.13). Le tout provient de la fonction sur $\mathscr{H}$ issue de la $(3, 2)$ correspondance

$$y(x + W) - \Lambda(x + V)f_1f_2.$$

En effet, si les coordonnées (V, W, Λ, T) correspondent à un point de Weierstrass, on peut déterminer complètement le diviseur de cette fonction, qui nous permet d'exhiber des éléments du noyau de la $2-2-2$ isogénie.

Pour cela, on remarque qu'il y a une involution en T sur les points de Weierstrass. Elle provient du fait que W est une fraction rationnelle de degré 2 en T. Ainsi,

$$W(T, V) - W(T', V),$$

se factorise par $T - T'$, puis se résout linéairement en T' sous la forme d'une homographie en T. C'est évidemment une involution, qui laisse W invariant. On vérifie

(§). C'est d'autant plus facile avec la correspondance de la section 3.4.5 qui respecte les involutions hyperelliptiques.

que U est laissé invariant, ce qui assure que Λ est invariant ou anti-invariant (⋆⋆). Même si l'on n'a pas $\mathscr{C}(T', V) = 0$, c'est toutefois vrai sur les points de Weierstrass, ce qui nous suffit ici.

Soit $\mathscr{W}_i$ un point de Weierstrass dans le modèle des coordonnées de $\mathscr{C}(T, V)$. On note D_i le diviseur sur $\mathscr{H}$, associé à $\mathscr{W}_i$ par la $(3, 2)$ correspondance. Le support de D_i a trois points. On note encore $\mathscr{W}_i^\sigma$, d'image D_i^σ, le point de Weierstrass image de $\mathscr{W}_i$ par l'involution en T. Enfin, pour un diviseur D de $\mathscr{H}$, on note $\overline{D}$ le diviseur dont les points du support sont les images par l'involution hyperelliptique $\imath_{\mathscr{H}}$ des points du support de celui de D.

Alors, comme l'involution en T fixe V, W et change Λ en $-\Lambda$, il existe un diviseur Γ, de degré 4, tel que

$$\mathrm{Div}\Big((x + W_i)y - \Lambda_i(x + V_i)f_1 f_2\Big) = D_i + \overline{D_i^\sigma} + \Gamma - 5D_\infty,$$

où Λ_i, T_i, V_i, W_i sont les coordonnées de $\mathscr{W}_i$ et D_∞ le diviseur à l'infini de $\mathscr{H}$ de degré 2. De plus, Γ ne dépend pas de $\mathscr{W}_i$ puisque son support correspond aux 4 points de Weierstrass de $\mathscr{H}$, racines de $f_1 f_2$. Comme par ailleurs, $\overline{D} + D - \deg(D)D_\infty$ est un diviseur principal, on en déduit qu'en faisant le quotient de deux telles fonctions pour des indices i, j, le diviseur

$$(\mathscr{W}_i) + (\mathscr{W}_i^\sigma) - (\mathscr{W}_j) - (\mathscr{W}_j^\sigma)$$

est associé par la correspondance à un diviseur principal.

On vérifie sans peine que dans (IV.17), on a $\mathscr{W}_2 = \mathscr{W}_1^\sigma$, $\mathscr{W}_4 = \mathscr{W}_3^\sigma$, et ainsi de suite. Cela donne 4 points du noyau de l'isogénie engendrée par la $(3, 2)$ correspondance

$$0,\ \mathscr{W}_1 + \mathscr{W}_2 - \mathscr{W}_3 - \mathscr{W}_4,\ \mathscr{W}_1 + \mathscr{W}_2 - \mathscr{W}_5 - \mathscr{W}_6,\ \mathscr{W}_3 + \mathscr{W}_4 - \mathscr{W}_5 - \mathscr{W}_6,$$

où on a gardé les signes en accord avec les fonctions des diviseurs principaux ci-dessus, même s'ils sont insignifiants puisque les points de Weierstrass sont d'ordre 2.

Cela suffit pour affirmer que l'on est dans la configuration du plan de Fano (figure IV.1). En effet, l'autre possibilité est que le groupe soit tractable. Or, on a

$$(D_i^\sigma) - (D_i) \sim \Gamma - 2D_\infty$$

qui n'est donc pas un diviseur principal, cela impose que $\mathscr{W}_i - \mathscr{W}_i^\sigma$ n'est pas dans le noyau. Ainsi, à symétrie des rôles (de $\mathscr{W}_3$ et $\mathscr{W}_4$ d'une part et $\mathscr{W}_5$ et $\mathscr{W}_6$ d'autre part) on aurait nécessairement

$$\mathscr{W}_1 - \mathscr{W}_3,\ \mathscr{W}_2 - \mathscr{W}_4,\ \mathscr{W}_1 - \mathscr{W}_5,\ \mathscr{W}_2 - \mathscr{W}_6$$

dans le noyau de la 2−2−2 isogénie. Mais ces points engendrent un groupe d'ordre 16, ce qui est impossible. Notons que l'on peut reconstruire tout le groupe en choisissant, dans l'équation (IV.12), une autre partition des f_i.

(⋆⋆). C'est en fait la deuxième possibilité qui arrive, même si cela n'a pas beaucoup d'importance.

3.4.3 Équation de $\mathscr{C}$ au-dessus de sa conique

Sur une extension de degré 8, on a donc donné les relations complètes entre les modèles de Weierstrass des courbes des familles (*f-2*) et (*f-3*). Néanmoins, on peut essayer de limiter le degré de l'extension en écrivant la courbe $\mathscr{C}$ sous forme de Weierstrass au-dessus d'une conique. Comme on l'a vu précédemment et comme expliqué par B. Smith dans [Smi 08], la correspondance (IV.13) entre $\mathscr{H}$ et $\mathscr{C}$ est définie sur une extension au plus de degré 2. Si l'on reprend la formule (IV.14) sans tordre $\mathscr{H}$, cette correspondance est définie sur le corps contenant la racine $\sqrt{\alpha}$ avec

$$\alpha = (1+b+c)(d^2+bd+c)(ad+c) = \gamma^2 \operatorname{Res}_x(f_1,f_2)\operatorname{Res}_x(f_3,f_4),$$

où γ est un polynôme en a,b,c,d. Cette expression fait apparaître, en particulier, que cette correspondance est bien définie sur le corps contenant les points de Weierstrass.

En fait, on peut écrire une équation de $\mathscr{C}$ au-dessus de sa conique (IV.16) sur l'extension contenant seulement $\sqrt{\alpha}$. Plus précisément, en notant S_i les abscisses des points de Weierstrass correspondant aux $\mathscr{W}_i$, alors, les polynômes[(◇◇)] $(S-S_1)(S-S_2)(S-S_3)(S-S_4)$ et $(S-S_5)(S-S_6)(S-S_7)(S-S_8)$ sont définis et irréductibles sur l'extension contenant $\sqrt{\alpha}$. De plus, on passe de l'un à l'autre par $\psi_\alpha = \sqrt{\alpha} \mapsto -\sqrt{\alpha}$.

Pour obtenir l'équation désirée, il suffit, sur l'extension de degré 8, d'interpoler les points de la conique (IV.16) (S_i,δ_i), pour $i = 1\ldots4$, par une fonction de degré adéquat :

$$P_c(S,\delta) := (\gamma_1 S+\gamma_2)\delta + \gamma_3 + \gamma_4 S + \gamma_5 S^2.$$

Cette fonction est définie sur l'extension de degré 2 et l'équation de $\mathscr{C}$ au-dessus de cette conique n'est autre que

$$\begin{cases} Y^2 = \dfrac{P_c(S,\delta)}{\psi_\alpha\big(P_c(S,\delta)\big)} \\ \delta^2 \;= (1+b+c)(d^2+bd+c)\Big(cS^2+2(ad+c)S+(a+1)(ad+c)\Big). \end{cases}$$

3.4.4 Fonctions T et V.

Maintenant que l'on a un modèle de Weierstrass de $\mathscr{C}$, il est intéressant d'expliciter les fonctions T et V, qui font apparaître un lien avec le noyau de la $2-2-2$ isogénie et qui, de plus, donnent une autre caractérisation des courbes de type « Fano ».

Il s'avère dans notre situation qu'il est aisé d'écrire T et V en fonction de X,Y notamment grâce au fait que $S = \frac{V}{T}$ est invariant par l'involution hyperelliptique sur $\mathscr{H}$. En reprenant les équations du début de la section 3.4.2, on a, par exemple,

$$V = \frac{Y+z_1}{2},$$

puis en notant $F_1(X) = z_1 + 2C$ et $F_2(X) = z_1 - 2C$ et en remarquant que $Y^2 = F_1(X)F_2(X)$, on a

$$V = -C\frac{Y+F_1(X)}{Y-F_1(X)},$$

(◇◇). Correspondant aux deux groupes des points de Weierstrass homothétiques, dans la caractérisation 3.11.

expression sur laquelle on voit que l'involution hyperelliptique $Y \mapsto -Y$ se transforme bien en $V \mapsto \frac{C^2}{V}$.

Pour S, le travail avait déjà été fait, puisque en réinjectant la paramétrisation $\delta = \delta_1 + X(S - S_1)$ dans l'équation de la conique (IV.16), on obtient facilement :

$$\frac{\Delta_z(S) - \Delta_z(S_1)}{S - S1} = -(2\delta_1 X + X^2(S - S_1)),$$

et, le membre de gauche étant un polynôme de degré 1 en S, il s'agit d'une équation linéaire qui se résout en S par le quotient de deux polynômes de degré 2 en X :

$$S = \frac{P(X)}{Q(X)} \quad \text{et} \quad T = -C\frac{Y + F_1(X)}{Y - F_1(X)}\frac{Q(X)}{P(X)}$$

En fait, z_1 a un dénominateur, ce qui n'influe pas car il se retrouve au carré dans $F_1(X)F_2(X)$. Néanmoins, le dénominateur de z_1 est de la forme

$$\zeta := \mu P(X)Q(X)$$

avec $\mu = -\frac{1}{(A+B+d-1)Cd}$ et les mêmes P et Q que ci-dessus. Ainsi, en écrivant $F_1'(X) = \zeta F_1(X)$, $F_2'(X) = \zeta F_2(X)$ et $Y' = \zeta Y$, on a $Y'^2 = F_1'(X)F_2'(X)$ et d'une part

$$F_1'(X) - F_2'(X) = (4\mu C)P(X)Q(X)$$

et d'autre part,

$$V = -C\frac{Y' + F_1'(X)}{Y' - F_1'(X)} \quad \text{et} \quad T = -C\frac{Y' + F_1'(X)}{Y' - F_1'(X)}\frac{Q(X)}{P(X)}.$$

Sous cette forme, il est facile de vérifier que T est une fonction de degré 4 ramifiée en $0, 1, d$ et ∞. Ceci rejoint ce qu'expliquent R. Donagi et R. Livné dans [DL 99] qui paramétrisent les fonctions de degré 4 au-dessus d'une courbe de genre 3 vers $\mathbb{P}^1$ ayant génériquement 2 points de branchement, sauf dans le cas hyperelliptique où il y en a 4. En fait, on peut se servir de ce résultat pour décrire d'une autre manière la courbe de la famille Fano (*f-3*). Commençons par un lemme d'algèbre linéaire.

Lemme 3.13. *Soient $g_1 = (x-x_1)(x-x_2)$, $g_2 = (x-x_3)(x-x_4)$, $g_3 = (x-x_5)(x-x_6)$ et $g_4 = (x-x_7)(x-x_8)$, des polynômes de degré 2.*

- *Il existe des coefficients homogènes k, l, m, n tels que $kg_1 + lg_2 + mg_3 + ng_4 = 0$.*
- *On a la factorisation $g_3g_4 - \frac{kl}{mn}g_1g_2 = (kg_1 + lg_2)(kg_1 + mg_3)$.*

Démonstration. Le premier point est de l'algèbre linéaire élémentaire. Le second en découle directement. □

Si l'on note $\omega = \sqrt{\frac{kl}{mn}}$, $h_1(x) = g_1(x)g_2(x)$ et $h_2(x) = g_3(x)g_4(x)$, on remarque que $\omega h_1(x) - \frac{1}{\omega}h_2(x)$ se factorise en deux facteurs de degré 2 et on a encore $y^2 = \omega h_1(x)\frac{1}{\omega}h_2(x)$. C'est en fait ce qu'il se passe avec la factorisation $F_1(X) - F_2(X)$ ci-dessus. On en vient maintenant à la caractérisation suivante.

Proposition 3.14. *On reprend les notations du lemme en considérant la courbe hyperelliptique $\mathscr{A}$ d'équation $y^2 = g_1(x)g_2(x)g_3(x)g_4(x)$. Alors,*

- *il est toujours possible d'écrire* $y^2 = g(x) = h_1(x)h_2(x)$*, chacun de degré 4 et de factoriser* $h_2(x) - \omega^2 h_1(x) = P(x)Q(x)$ *comme dans le lemme précédent, de façon à ce que la fonction de degré 4*
$$t := \frac{y - \omega h_1(x)}{y + \omega h_1(x)} \frac{P(x)}{Q(x)},$$
vérifie pour un certain l*,*
$$t - l = \frac{y - \omega' h_1'(x)}{y + \omega' h_1'(x)} \frac{P'(x)}{Q(x)}$$
avec $g(x) = h_1'(x)h_2'(x)$ *et* $h_2'(x) - \omega'^2 h_1'(x) = x_1 P'(x)Q(x)$*.*
- *la courbe* $\mathscr{A}$ *est dans les familles (f-1) ou (f-3) si, et seulement si, il existe un deuxième point* l' *tel que* $t - l'$ *s'écrive de manière similaire à* $t - l$*.*

Démonstration. Pour vérifier le premier point, on remarque que t s'écrit aussi
$$t = \omega \frac{\left(\frac{1}{\omega} h_2(x) + \omega h_1(x)\right) - 2y}{Q(x)^2}.$$
Comme on veut que ce soit le même Q dans la factorisation $h_2'(x) - \omega'^2 h_1'(x)$, on en déduit que
$$\frac{1}{\omega} h_2(x) + \omega h_1(x) - \frac{l}{\omega} Q(x)^2 = \frac{1}{\omega}' h_2'(x) + \omega' h_1'(x),$$
d'où l'on tire qu'il existe une constante ν telle que
$$h_1(x) - \nu h_1'(x) = 0 \mod Q(x).$$

Il suffit ensuite de choisir 4 points de Weierstrass parmi les 8 et de faire la division euclidienne de $h_1(x) - \nu h_1'(x)$ par $Q(x)$: lorsque le reste se factorise par un terme en ν, on trouve un $h_1'(x)$ dont on vérifie qu'il convient.

Génériquement, on trouve quatre solutions, correspondant à $h_1(x)$, $h_2(x)$, $h_1'(x)$ et $h_2'(x)$, ce qui démontre le premier point.

Par ailleurs, on peut forcer la factorisation dans le reste ci-dessus pour trouver une solution supplémentaire. Pour chaque choix de 4 points de Weierstrass, on trouve alors une condition sur les x_i qui est soit celle de la famille (*f-1*), soit celle de la famille (*f-3*). Ceci démontre la partie nécessaire du deuxième point, la partie suffisante ayant été vue plus haut. □

Lien avec le noyau de la $2-2-2$ isogénie. Il est intéressant de noter que ces partitions des points de Weierstrass en deux sous-ensembles de 4 points sont les mêmes que celles du noyau de la $2-2-2$ isogénie, que ce soit dans les fonctions T et V ou par l'homographie $\mathscr{J}$ entre les points de Weierstrass du théorème 3.11.

En effet, on l'a déjà vu pour $\mathscr{W}_1 + \mathscr{W}_2 + \mathscr{W}_3 + \mathscr{W}_4$, correspondant à l'homographie $\mathscr{J}$. Il est facile de voir que T et V correspondent à $\mathscr{W}_1 + \mathscr{W}_2 + \mathscr{W}_5 + \mathscr{W}_6$. On vérifie que $T - 1$ correspond à $\mathscr{W}_1 + \mathscr{W}_3 + \mathscr{W}_5 + \mathscr{W}_7$, invariant par l'homographie $\mathscr{J}$ et $T - d$ correspond à $\mathscr{W}_1 + \mathscr{W}_4 + \mathscr{W}_6 + \mathscr{W}_7$, invariant par la composition des deux.

Enfin, on peut faire le même travail pour W, qui correspond à $\mathscr{W}_3 + \mathscr{W}_4 + \mathscr{W}_5 + \mathscr{W}_6$, mais aussi pour les fonctions V et W qui seraient obtenues en prenant une autre partition des f_1, f_2, f_3 et f_4 dans l'équation (IV.12).

Au final, le noyau est formé, à complémentaire près, des sous-ensembles de quatre points de Weierstrass qui sont invariants soit par $\mathscr{W} \mapsto \mathscr{W}^\sigma$, soit par $\mathscr{J}$ soit par la composition des deux.

3.4.5 Correspondance respectant les involutions hyperelliptiques

La correspondance $(3,2)$ entre $\mathscr{H}$ et le modèle en T, V de $\mathscr{C}$ ne respecte pas les involutions hyperelliptiques, c'est-à-dire, qu'à un point $P \in \mathscr{H}$ cette correspondance associe des points $Q_1, Q_2 \in \mathscr{C}$, alors, qu'au point $\imath_{\mathscr{H}}(P)$ ne sont pas associés les points $\imath_{\mathscr{C}}(Q_1), \imath_{\mathscr{C}}(Q_2)$.

En s'autorisant à augmenter un peu les degrés de la correspondance, on arrive, par un calcul explicite au théorème suivant.

Théorème 3.15. *Il existe, sur l'extension de degré 8 contenant A, B et C, une correspondance $(4,3)$ entre les modèles de Weierstrass des courbes $\mathscr{H}(x,y)$ et $\mathscr{C}(X,Y)$, qui respecte les involutions hyperelliptiques, c'est-à-dire, il existe un polynôme $P(x,X)$ et une fraction $Q(x,X)$ tels que les équations des courbes et de la correspondance soient :*

$$\begin{cases} y^2 &= f(x) \\ 0 &= P(x,X) \\ yY &= Q(x,X) \\ Y^2 &= F(X), \end{cases}$$

où $\deg_x(P) = 4$ *et* $\deg_X(P) = 3$.

Démonstration. On part de la correspondance $(3,2)$ que l'on connaît : l'équation $\mathscr{C}(\varphi(x), V)$ se scinde, par construction, en 2 facteurs, modulo l'équation de $\mathscr{H}$,

$$\mathscr{C}(\varphi(x), V) = C_1(x,y,V)C_2(x,y,V) \mod y^2 - f(x),$$

chacun des deux facteurs étant de degré 2 en V et correspondant respectivement aux points (x,y) et $(x,-y)$.

À partir des fonctions T et V obtenues précédemment en 3.4.4, on peut, grâce, par exemple, à un calcul d'élimination par résultant, les inverser en écrivant $X = \Phi(T,V)$ et $Y = \Psi(T,V)$, pour se ramener au modèle de Weierstrass, en (X,Y) de la courbe $\mathscr{C}$ sur laquelle on veut la correspondance.

Si l'on note, toujours sur le modèle de Weierstrass de $\mathscr{C}$, M_1, M_2 les points correspondants à C_1 et N_1, N_2 ceux correspondants à C_2, alors, par l'involution hyperelliptique sur $\mathscr{H}$, $(M_1) + (M_2)$ est changé en $(N_1) + (N_2)$. On cherche donc à écrire, en termes de diviseurs,

$$(M_1) + (M_2) - (N_1) - (N_2) \sim L - \imath_{\mathscr{C}}(L),$$

dont le second membre est invariant par l'involution hyperelliptique sur $\mathscr{C}$. La correspondance recherchée consiste alors à associer au point (x,y) les points du support de L. On cherche donc L, effectif, de degré minimal et on commence donc par $\deg L = 3$. Pour simplifier, on concentre la partie polaire à l'infini, en notant D_∞ le diviseur à l'infini de degré 2,

$$M_1 + M_2 + \imath_{\mathscr{C}}(N_1) + \imath_{\mathscr{C}}(N_2) + 2\imath_{\mathscr{C}}(L) \sim 5D_\infty.$$

On est donc amené à trouver une fonction sans dénominateur de degré 10 passant par $M_1, M_2, \imath(N_1), \imath(N_2)$ et dont le reste est un carré parfait. Une telle fonction s'écrit génériquement avec 8 coefficients homogènes en x, y

$$(\gamma_1 X + \gamma_0)Y + \mu_5 X^5 + \mu_4 X^4 + \mu_3 X^3 + \mu_2 X^2 + \mu_1 X + \mu_0.$$

De plus, comme on veut une correspondance invariante par les deux involutions hyperelliptiques, on peut en fait demander que $\gamma_i = y\gamma_i'$ et que γ_i' et μ_i soient des fonctions de x seulement,

$$(\gamma_1' X + \gamma_0')yY + \mu_5 X^5 + \mu_4 X^4 + \mu_3 X^3 + \mu_2 X^2 + \mu_1 X + \mu_0 . x \tag{IV.21}$$

En multipliant cette équation par sa conjuguée en $Y \mapsto -Y$, on obtient une fonction en X et x seulement, de degré 10 en X avec un facteur de degré 4 en X correspondant aux points $M_1, M_2, \imath(N_1)$ et $\imath(N_2)$. Ce dernier est, par construction, le numérateur de

$$P_4 := \mathrm{Res}_V\Big(\mathscr{C}\big(\varphi(x), V\big), X - \Phi\big(\varphi(x), V\big)\Big). \tag{IV.22}$$

Il ne reste donc plus qu'une fonction de degré 6 dont on veut qu'elle soit un carré parfait, et l'on dispose encore de 4 paramètres homogènes.

Pour trouver une telle fonction, on vérifie qu'il existe un polynôme P satisfaisant (‡‡) aux équations

$$\begin{aligned} P(x,0) &= \lambda_1(x+\lambda_2)^2 f_4(x) & P(x,1) &= \lambda_3 f_2(x) \\ P(x,d) &= \lambda_4(x+\lambda_5)^2 f_1(x) & P(x,\infty) &= \lambda_6(x+\lambda_7)^2 f_3(x) \end{aligned}$$

et

$$\begin{aligned} P(x,\mathscr{W}_5) &= \lambda_8 f_1 f_4 & P(x,\mathscr{W}_6) &= \lambda_9 f_1 f_4 \\ P(x,\mathscr{W}_7) &= \lambda_{10}(x^2+\lambda_{11}x+\lambda_{12})^2 & P(x,\mathscr{W}_8) &= \lambda_{13} f_3 f_4. \end{aligned}$$

Une fois un tel polynôme trouvé, il suffit de vérifier l'équation (IV.21). Pour cela, on vérifie par exemple que

$$P_4 P^2 + f(x)F(x)(\gamma_0' + \gamma_1' X)^2$$

est un carré parfait, ce qui est facile à déterminer, l'extraction de racine polynomiale étant un problème linéaire. Ce calcul explicite montre donc l'existence de la correspondance de la proposition 3.15. On la donne à l'adresse `www.normalesup.org/~iboyer/files/corresp.txt` □

Nous pouvons donc donner explicitement une famille à 4 paramètres donnant les équations des courbes appartenant aux familles (*f-2*) et (*f-3*) et une correspondance entre elles respectant l'involution hyperelliptique.

3.4.6 Discriminants des courbes $\mathscr{H}$ et $\mathscr{C}$

Les discriminants de deux courbes, considérées sous la forme de Weierstrass décrite précédemment, dont les jacobiennes sont $2-2-2$ isogènes, sont semblables dans le sens où des facteurs similaires apparaissent avec diverses puissances.

Néanmoins, si les 15 facteurs du discriminant de la courbe de type « Fano » figurent dans celui de la courbe de type « tractable », la réciproque est fausse.

Par exemple, pour $A = 0$, on vérifie, à l'aide des invariants d'Igusa, que la courbe de type « tractable » dégénère, sans que l'autre courbe, ni les jacobiennes ne cessent d'exister.

(‡‡). Il y a bien entendu d'autres relations similaires donnant d'autres correspondances. D'autre part il est naturel de voir associés à des points de Weierstrass de $\mathscr{C}$ des points de Weierstrass de $\mathscr{H}$ ou des carrés parfaits.

3.5 Un exemple numérique

Voici donc pour finir un exemple numérique de ce qui a été traité dans cette section 3. On commence par choisir des valeurs de A, B, C et d de façon à ce que tous les points de Weierstrass soient rationnels :

$$A = 1, B = 1, C = 4, d = -2 \quad \text{soit} \quad a = -\frac{17}{2}, b = 1, c = -1 \text{ et } d = -2,$$

ce qui donne pour $\mathscr{H}$:

$$y^2 = -\frac{1}{4}(x^2 + x - 1)(15x^2 + 15x - 32)(x^2 - 16x + 16)(2x^2 + 19x + 32).$$

L'unique trigonale vaut

$$\varphi = -2\frac{(x^2 + x - 1)x}{15x^2 + 15x - 32}$$

et le modèle $\mathscr{C}(T, V)$ est donné par l'équation

$$\begin{aligned} &V^4T^2 + 4V^4T - 64V^3T^2 + 240V^2T^3 + 20V^4 - 896V^3T + 12672V^2T^2 \\ &\quad - 71168VT^3 + 137280T^4 + 64V^2T - 1024VT^2 + 3840T^3 + 256T^2 = 0. \end{aligned}$$

On peut écrire l'équation de la correspondance $(3, 2)$ qui est bien définie sur $\mathbb{Q}$. Celle-ci est essentiellement donnée (voir IV.13) par W et Λ, une racine de U modulo $\mathscr{C}(T, V)$,

$$W = \frac{1}{4}\frac{-TV^2 + 120T^2 - 32TV + 2V^2 + 16T}{(10T - V)(6T - V)}$$

$$\begin{aligned} \Lambda \;= &-\tfrac{1}{64}\tfrac{1}{(5T+2)(3T+2)(3T-2)(5T-2)(8T^2-T+2)T^2}\Big[120T^7V^2 + 47T^6V^3 + 14400T^8 + 1800T^7V \\ &-2768T^6V^2 + 154T^5V^3 - 1764736T^7 + 496016T^6V - 37440T^5V^2 + 944T^4V^3 + 650240T^6 \\ &-250432T^5 + 20992T^4V^2 - 112T^3V^3 - 2514944T^5 + 982656T^4V - 104832T^3V^2 + 2800T^2V^3 \\ &-222208T^4 + 64128T^3V - 4864T^2V^2 + 32TV^3 + 563200T^3 - 217856T^2V + 23552TV^2 - 640V^3 \\ &+16384T^2 - 2048TV.\Big] \end{aligned}$$

Le modèle de Weierstrass de la courbe $\mathscr{C}$ est plus simple,

$$Y^2 = -3X(X - 1)(X + 2)(13X + 2)(5X - 11)(X + 8)(2X - 1),$$

et on a les relations entre T, V, X et Y :

$$\begin{aligned} V &= 4\frac{Y - 9X(X + 8)(2X - 1)}{Y + 9X(X + 8)(2X - 1)} \\ T &= 2\frac{5X^2 + 2X + 2}{13X^2 - 8X + 22} \cdot \frac{Y - 9X(X + 8)(2X - 1)}{Y + 9X(X + 8)(2X - 1)}, \end{aligned}$$

d'une part et d'autre part

$$\begin{aligned} X = \tfrac{1}{32}\tfrac{1}{T(208T^3-26T^2-40T^2V+5TV+52T-10V)}\Big[&4928T^4 - 152T^3V - 51712T^3 + 24T^3V^2 - 96T^2V^2 \\ &- 256T^2 + 20320T^2V + 3T^2V^3 - 2208TV^2 + 160TV + 12TV^3 + 60V^3\Big], \end{aligned}$$

$$\begin{aligned} Y = \tfrac{27}{2}\tfrac{V+4}{(V-4)(26T-5V)^3(8T^2-T+2)}\Big[&472T^4V^2 - 1107T^3V^3 + 2671680T^5 - 1287784T^4V + 159706T^3V^2 \\ &- 3207T^2V^3 - 6177968T^4 + 2445352T^3V - 272832T^2V^2 + 7052TV^3 \\ &+ 503296T^3 - 296544T^2V + 42584TV^2 - 1188V^3 - 9024T^2 - 5792TV\Big]. \end{aligned}$$

Sur le modèle de Weierstrass de $\mathscr{C}$, on a l'homographie (IV.19) qui transforme les points $\{\infty, 0, 1, -2\}$ en $\{\frac{1}{2}, -8, \frac{11}{5}, -\frac{2}{13}\}$:

$$w \mapsto \frac{3w+8}{6w-1}.$$

Finissons par écrire la correspondance $(4,3)$ du théorème 3.15 :

$$\begin{aligned}
P(x,X) = {} & -26X^3x^4 - 143X^3x^3 + 42X^2x^4 + 468X^3x^2 - 465X^2x^3 - 60Xx^4 + 676X^3x \\
& + 78X^2x^2 + 1224Xx^3 + 44x^4 - 1664X^3 + 1134X^2x - 3936Xx^2 - 616x^3 \\
& - 576X^2 - 6564Xx - 660x^2 + 10176X + 704x + 704 \\
yY = Q(x,X) = {} & \frac{-9/2Y^2}{(X-1)^2(13X^2-8X+22)^3(3Xx^2+2Xx-8+6x^2-2x-16X)}\Big[1600599X^5x^3 - 3461796X^5x^2 \\
& + 8805693X^4x^3 - 7955844X^5x - 12625002X^4x^2 - 9147156X^3x^3 + 15856256X^5 \\
& - 29381118X^4x + 42218424X^3x^2 - 30472428X^2x^3 + 49205312X^4 + 64016436X^3x \\
& + 112897332X^2x^2 + 33038016Xx^3 - 126384064X^3 + 171293208X^2x - 80611344Xx^2 \\
& - 13666224\,x^3 - 271934912\,X^2 - 137531856\,Xx - 14130864\,x^2 + 200468224\,X \\
& + 14682624x + 17315584\Big]
\end{aligned}$$

où l'on a laissé Y^2 à la place du polynôme en X par souci de lisibilité.

Index

— R —

— T —

— V —

Index des notations

Liste des figures

Liste des tableaux

Liste des algorithmes

Bibliographie

[Bor 76] **C.-W. Borchardt**. Über das arithmetisch-geometrische Mittel aus vier Elementen. *Monatsbericht der Akademie der Wissenschaften zu Berlin*, pp. 611–621, 1876. (*cf.* p. 86)

[BM 88] **J.-B. Bost et J.-F. Mestre**. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.*, Vol. 38, pp. 36–64, 1988. (*cf.* pp. 7, 98)

[DL 99] **R. Donagi et R. Livné**. The Arithmetic-Geometric Mean and Isogenies for Curves of Higher Genus. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze*, Vol. 28, N° 2, pp. 323–339, 1999. http://archive.numdam.org/item?id=ASNSP_1999_4_28_2_323_0. (*cf.* pp. 84, 88, 98, 110)

[Dup 06] **R. Dupont**. *Moyenne artihmético-géométrique, suites de Borchardt et applications*. Thèse de doctorat, 2006. www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf. (*cf.* p. 86)

[Ell 01] **J. S. Ellenberg**. Endomorphism Algebras of Jacobians. *Advances in Mathematics*, Vol. 162, N° 2, pp. 243 – 271, 2001. www.math.wisc.edu/~ellenber/EndJacAjour.pdf. (*cf.* pp. ix, 19, 21, 48)

[Fri 24] **R. Fricke**. *Lehrbuch der Algebra*. Vieweg u. Sohn, 1924. (*cf.* p. 29)

[GKZ 08] **I. M. Gelfand, M. Kapranov et A. Zelevinsky**. *Discriminants, Resultants, and Multidimensional Determinants*. Birkhäuser, Avr. 2008. (*cf.* p. 103)

[GP 13] **User's Guide to PARI / GP**. 2013. pari.math.u-bordeaux.fr. (*cf.* pp. 44, 75)

[HS 00] **M. Hindry et J. H. Silverman**. *Diophantine Geometry : An Introduction*. Springer, 2000. (*cf.* p. 1)

[Hon 66] **T. Honda**. On the Jacobian variety of the algebraic curve $y^2 = 1 - x^l$ over a field of characteristic $p > 0$. *Osaka Journal of Mathematics*, Vol. 3, N° 2, pp. 189–194, 1966. hdl.handle.net/11094/3647. (*cf.* pp. 50, 52, 54)

[Igu 56] **J.-I. Igusa**. Fibre Systems of Jacobian Varieties. *American Journal of Mathematics*, Vol. 78, N° 1, pp. 171–199, 1956. www.jstor.org/stable/2372489. (*cf.* p. 52)

[LLL 82] **A. K. Lenstra, H. W. Lenstra et L. Lovász**. Factoring polynomials with rational coefficients. *Mathematische Annalen*, Vol. 261, N° 4, pp. 515–534, 1982. (*cf.* p. 56)

[Lep 91] **F. Leprévost**. Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21. *C. R. Acad. Sci. Paris*, Vol. 313, N° I, pp. 771–774, 1991. (*cf.* p. 31)

[Lep 95] **F. Leprévost**. Jacobiennes de certaines courbes de genre 2 : torsion et simplicité. *Journal de Théorie des Nombres de Bordeaux*, Vol. 7, pp. 283–306, 1995. www.numdam.org/item?id=JTNB_1995__7_1_283_0. (*cf.* p. 31)

[Mag 13] **Handbook of Magma functions**. 2013. Edition 2.19(2013), magma.maths.usyd.edu.au/magma/. (*cf.* pp. 43, 64, 72)

[Map 13] **Maple®**. 2013. www.maplesoft.com/products/Maple/. (*cf.* pp. 27, 87)

[Mes 91] **J.-F. Mestre**. Familles de courbes hyperelliptiques à multiplications réelles. In : *Arithmetic Algebraic Geometry,* Progr. Math., Birkhäuser, Boston, 1991. (*cf.* pp. 8, 19, 23, 27, 29)

[Mes 13] **J.-F. Mestre**. Une généralisation d'une construction de Richelot. *Journal of Algebraic Geometry*, Vol. 22, pp. 575–580, 2013. dx.doi.org/10.1090/S1056-3911-2012-00589-X. (*cf.* pp. xi, 92, 97, 99)

[Mil 08] **J. S. Milne**. Abelian Varieties (v2.00). 2008. www.jmilne.org/math/CourseNotes/AV.pdf. (*cf.* p. 1)

[Mum 74] **D. Mumford**. *Abelian Varieties*. Oxford University Press, 1974. (*cf.* p. 8)

[Mum 83] **D. Mumford**. *Tata Lectures on Theta I*. Birkhäuser, 1983. (*cf.* pp. 1, 14, 16, 83, 85, 93, 95)

[Mum 84] **D. Mumford**. *Tata Lectures on Theta II*. Birkhäuser, 1984. (*cf.* pp. 1, 14, 15, 16, 17, 18, 83, 86, 87)

[Ogg 74] **A. P. Ogg**. Hyperelliptic modular curves. *Bulletin de la Société Mathématique de France*, Vol. 102, pp. 449–462, 1974. www.numdam.org/item?id=BSMF_1974__102__449_0. (*cf.* p. 29)

[Pil 90] **J. Pila**. Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields. *Mathematics of Computation*, Vol. 55, N° 192, pp. 745–763, 1990. www.jstor.org/stable/2008445. (*cf.* pp. x, 2, 50, 56, 57, 60)

[Rec 74] **S. Recillas**. Jacobians of Curves with g^1_4's are the Prym's of Trigonal Curves. *Bol. Soc. Mat. Mexicana*, Vol. 19, N° 1, pp. 9–13, 1974. (*cf.* pp. xi, 84, 98)

[Sch 85] **R. Schoof**. Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. *Mathematics of Computation*, Vol. 44, N° 170, pp. 483–494, 1985. (*cf.* pp. 49, 50, 68, 69)

[Shi 98] **G. Shimura**. *Abelian Varieties With Complex Multiplication and Modular Functions*. Princeton University Press, 1998. (*cf.* pp. 1, 13, 46, 51, 53, 54, 73)

[Shi 67] **T. Shioda**. On the Graded Ring of Invariants of Binary Octavics. *American Journal of Mathematics*, Vol. 89, N° 4, pp. 1022–1046, 1967. www.jstor.org/stable/2373415. (*cf.* p. 76)

[Smi 08] **B. Smith**. Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves. In : N. Smart, Ed., *Advances in Cryptology – EUROCRYPT 2008*, pp. 163–180, Springer, 2008. http://dx.doi.org/10.1007/978-3-540-78967-3_10. (*cf.* pp. xi, 84, 88, 98, 100, 102, 109)

[Smi 10] **B. Smith**. Families of Explicit Isogenies of Hyperelliptic Jacobians. In : D. R. Kohel et R. Rolland, Eds., *Arithmetic, Geometry, Cryptography, and Coding Theory 2009*, pp. 121–144, Contempory Mathematics, 2010. (*cf.* p. 97)

[TTV 91] **W. Tautz, J. Top et A. Verberkmoes**. Explicit Hyperelliptic Curves with Real Multiplication and Permutation Polynomials. *Canad. J. Math*, Vol. 43, N° 5, pp. 1055–1064, 1991. (*cf.* pp. 8, 19, 23, 24, 36, 48, 65, 66)

[VW 99] **P. Van Wamelen**. Examples of Genus two CM Curves over the Rationals. *Mathematics of Computation*, Vol. 68, N° 225, pp. 307–320, 1999. (*cf.* pp. 73, 74)

[Was 97] **L. C. Washington**. *Introduction to Cyclotomic Fields*. Springer, 1997. (*cf.* p. 58)

[Wen 01] **A. Weng**. Hyperelliptic CM-Curves of Genus 3. *Journal of the Ramanujan Math. Soc.*, Vol. 16, pp. 339–372, 2001. (*cf.* pp. 73, 75)