Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques.

Romain Cosset

Département de formation doctorale en informatique **École doctorale IAEM Lorraine**
UFR STMIA **Laboratoire: LORIA**

Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques

THÈSE

présentée et soutenue publiquement le lundi 7 novembre

pour l'obtention du

Doctorat de l'université Henri Poincaré – Nancy 1

(spécialité informatique)

par

Romain Cosset

Composition du jury

Rapporteurs :	François Morain	Prof. École polytechnique
	Kamal Khuri-Makdisi	Prof. American University of Beirut
Examinateurs :	Sylvain Lazard	DR Inria (Loria)
	Dominique Méry	Prof. Université Nancy 1
	Jean-François Mestre	Prof. Université Paris 7
	Frederik Vercauteren	Katholieke Universiteit Leuven
Directeur :	Guillaume Hanrot	Prof. ENS Lyon
Co-directeur :	Emmanuel Thomé	CR Inria (Loria)

Résumé

Depuis le milieu des années 1980, les variétés abéliennes ont été abondamment utilisées en cryptographie à clé publique: le problème du logarithme discret et les protocoles qui s'appuient sur celles-ci permettent le chiffrement asymétrique, la signature, l'authentification. Dans cette perspective, les jacobiennes de courbes hyperelliptiques constituent l'un des exemples les plus intéressants de variétés abéliennes principalement polarisées.

L'utilisation des fonctions thêta permet d'avoir des algorithmes efficaces sur ces variétés. En particulier nous proposons dans cette thèse une variante de l'algorithme ECM utilisant les jacobiennes de courbes de genre 2 décomposables. Par ailleurs, nous étudions les correspondances entre les coordonnées de Mumford et les fonctions thêta. Ce travail a permis la construction de lois d'additions complètes en genre 2. Finalement nous présentons un algorithme de calcul d'isogénies entre variétés abéliennes.

La majorité des résultats de cette thèse sont valides pour des courbes hyperelliptiques de genre quelconque. Nous nous sommes cependant concentré sur le cas du genre 2, le plus intéressant en pratique. Ces résultats ont été implémentés dans un package Magma appelé AVIsogenies.

Mots-clés: Cryptographie, courbes hyperelliptiques, variétés abéliennes, fonctions thêta, factorisation, isogénies

Abstract

Since the mid 1980's, abelian varieties have been widely used in cryptography: the discrete logarithm problem and the protocols that rely on it allow asymmetric encryption, signatures, authentification... For cryptographic applications, one of the most interesting examples of principally polarized abelian varieties is given by the Jacobians of hyperelliptic curves.

The theory of theta functions provides efficient algorithms to compute with abelian varieties. In particular, using decomposable curves of genus 2, we present a generalization of the ECM algorithm. In this thesis, we also study the correspondences between Mumford coordinates and theta functions. This led to the construction of complete addition laws in genus 2. Finally we present an algorithm to compute isogenies between abelian varieties.

Most of the results of this thesis are valid for hyperelliptic curves of arbitrary genus. More specifically we emphasize on genus 2 hyperelliptic curves, which is the most relevant case in cryptography. These results have been implemented in a Magma package called AVIsogenies.

Keywords: Cryptography, hyperelliptic curves, abelian varieties, theta functions, factorization, isogenies

Remerciements

Tout d'abord je remercie mes deux encadrants de thèse Guillaume Hanrot et Emmanuel Thomé. Emmanuel s'est toujours montré très disponible aussi bien pour m'aider dans mes recherches que pour relire et corriger mes articles. La présentation du chapitre 5 de cette thèse lui doit beaucoup. Par ailleurs Emmanuel a passé beaucoup de temps à m'apprendre à programmer et plus généralement à m'apprendre l'informatique. Guillaume a toujours su se placer exactement au bon niveau pour m'expliquer les maths. Je lui dois également beaucoup du point de vue administratif, en commençant par toutes les démarches qu'il a faites pour ma bourse de thèse.

Merci à François Morain et Kamal Khuri-Makdisi d'avoir accepté la lourde tâche de relire ce manuscrit de thèse. Leurs remarques m'ont permis de corriger de nombreuses erreurs et m'ont permis (j'espère) d'améliorer la qualité et la clarté du document. Je remercie Jean-François Mestre et Frederik Vercauteren dont les travaux m'ont beaucoup inspiré. Je me rappelle encore du temps passé sur certains de leurs articles. Je remercie Sylvain Lazard qui a été mon référent pendant ces trois années de thèse. Merci à Dominique Méry qui en plus d'avoir accepté de s'intéresser à ma thèse a été un collègue au cours de mon monitorat à l'ESIAL.

Je tiens à remercier deux personnes qui m'ont beaucoup apporté au cours de cette thèse. Tout d'abord, Jérôme Gärtner avec qui j'ai fait mes études à Cachan et à Jussieu. Bien qu'il ne soit cité qu'une fois dans cette thèse (ici), j'ai beaucoup travaillé avec lui : il m'expliquait les maths, et moi je les codais. Je le remercie d'avoir pensé à moi pour tester cette conjecture de Darmon. Cela m'a permis de travailler sur différents algorithmes de théorie algébrique des nombres. Merci Jérôme d'avoir pris le temps de répondre à mes questions et surtout d'avoir su te mettre à mon niveau pour m'expliquer la théorie.
La contribution de Guillaume Batog est plus discrète mais néanmoins aussi importante. Il m'a débloqué à plusieurs reprises et ses questions théoriques m'ont aussi obligé à bien comprendre un certain nombre de points. Par ailleurs, et c'est sans doute le plus important, nos pauses quotidiennes m'ont sans aucun doute permis de garder ma santé mentale au cours de ces 3 ans de thèse.

Continuons les remerciements par l'équipe CACAO puis CARAMEL. Plus que des collègues de travail, ces personnes sont devenus des amis. C'est grâce à Pierrick Gaudry dont j'ai suivi le cours de DEA que je me suis lancé dans cette thèse : « viens à Nancy, c'est cool et on te trouvera un sujet sympa »... Il a toujours pris le temps de répondre à mes questions et de m'expliquer avec les mains les outils mathématiques.
Merci à Damien Robert de m'avoir expliqué la théorie algébrique des fonctions thêta ainsi que tout son travail sur le calcul d'isogénies. J'ai eu la chance de partager mon bureau avec Gaëtan Bisson. La bibliothèque AVIsogenies a été le fruit d'une collaboration avec eux, je les remercie de m'avoir poussé à coder mes résultats. C'est toujours agréable de voir que la théorie fonctionne en pratique.
Paul Zimmermann m'a beaucoup apporté dans la compréhension de l'algorithme ECM. En particulier, il m'a expliqué les subtilités de GMP-ECM et c'est en partie grâce à lui que j'ai pu écrire GMP-HECM. Merci également à Nicolas Estibals, Jérémie Detrey, Răzvan Bărbulescu, Alexander Kruppa, Lionel Muller pour toutes les discussions aux pauses café ou devant une bière.

Durant ma thèse j'ai eu la chance de pouvoir travailler avec David Lubicz à Rennes. Ce fut des moments très enrichissants, l'enthousiasme de David est très communicatif.
J'ai passé 3 mois à Oldenburg et je tiens à remercier toutes les personnes qui m'ont si bien accueilli là-bas et en particulier Florian Hess et Osmanbey Uzunkol. Quel dommage de ne pas avoir réussi à utiliser les thêta constantes pour trouver de meilleurs invariants.
Je tiens à remercier également diverses personnes que j'ai embêtées avec mes questions. Merci donc à Christophe Arène, Christophe Ritzenthaler, David Kohel, David Gruenwald, Ben Smith, Vanessa Vitse...

Évidement, il n'y a pas que la science dans la vie. Je remercie donc ma famille et mes amis d'avoir réussi à me supporter. J'ai une pensée particulière pour Tof, Coralie, Émeline, Poulpe, Elsa, Corentin, Ramla, Stéphane, Chicco, Hyperion, Augustin, Mra et toutes les autres personnes que j'aie pu oublier.

Finalement je remercie Amélie Thomé, sans doute une des rares personnes qui aura apprécié le chapitre 5. Je regrette de n'avoir pas scanné ses illustrations.

Table des matières

Introduction

Depuis le milieu des années 1980, les variétés abéliennes ont été abondamment utilisées en cryptographie à clé publique : le problème du logarithme discret et les protocoles qui reposent dessus permettent le chiffrement asymétrique, la signature, l'authentification... Nous commençons par présenter ces applications des variétés abéliennes dans le premier chapitre et nous les définissons mathématiquement dans le deuxième chapitre.

Les fonctions thêta fournissent des coordonnées intéressantes pour utiliser les variétés abéliennes. Nous les étudierons au chapitre 3. En particulier, différentes bases de fonctions thêta peuvent être utilisées suivant les applications. Dans ce chapitre, nous décrivons également comment utiliser ces fonctions pour avoir une arithmétique efficace.

Il est possible de généraliser l'algorithme de factorisation ECM en utilisant des variétés abéliennes au lieu des courbes elliptiques. Nous présentons dans le chapitre 4 un algorithme utilisant des courbes hyperelliptiques de genre 2. Notre implémentation en C de cet algorithme est également comparée aux implémentations de ECM existantes.

Nous avons deux systèmes de coordonnées sur les jacobiennes de courbes hyperelliptiques : les coordonnées de Mumford et les coordonnées thêta. Le chapitre 5 prouve des formules permettant de passer d'une représentation à l'autre. Des résultats partiels avaient été obtenus par Mumford [Mum84], Van Wamelen [vW98] et Gaudry [Gau07]. Nous avons généralisé et complété ces travaux. Finalement, nous appliquons ces morphismes à l'obtention de lois d'additions k-complètes en genre 2. Cette application a été réalisée en collaboration avec Christophe Arène.

Le chapitre suivant généralise les formules de Thomae [Tho70]. Le but de ce travail commun avec David Lubicz est de pouvoir relier l'équation de Weierstraß d'une courbe hyperelliptique et le plongement de la jacobienne de la courbe dans $\mathbb{P}^{n^g-1}$ donné par les fonctions thêta de niveau n.

Le dernier chapitre de cette thèse est consacré au calcul d'isogénies entre variétés abéliennes. Nous commençons par présenter les travaux de Lubicz et Robert [LR10a] permettant de calculer des ℓ^2-isogénies entre variétés abéliennes principalement polarisées. En collaboration avec Damien Robert, nous avons trouvé des formules permettant de « changer de niveaux sans isogénie ». Combinées aux résultats précédents, cela permet le calcul de ℓ-isogénies. Le cas particulier des courbes hyperelliptiques de genre 2 y est également étudié. Signalons qu'avec Gaetan Bisson et Damien Robert, nous avons programmé ces formules dans une librairie Magma appelée AVIsogenies.

Les principaux résultats de cette thèse sont :
- L'étude théorique et pratique de l'algorithme de factorisation HECM.
- Des formules permettant de passer des coordonnées de Mumford aux fonctions thêta et inversement.
- L'utilisation des morphismes pour obtenir des lois d'addition complètes dans les jacobiennes de courbes hyperelliptiques de genre 2.
- Une généralisation des formules de Thomae et l'extraction de racines dans ces formules.
- Une méthode pour calculer des ℓ-isogénies entre variétés abéliennes et en particulier entre courbes hyperelliptiques de genre 2.
- La librairie AVIsogenies permettant de manipuler les variétés abéliennes et en particulier de calculer des ℓ-isogénies entre jacobiennes de courbes hyperelliptiques.

Chapitre 1

Cryptographie à clé publique

Les protocoles de cryptographie à clé publique reposent sur la difficulté de résoudre des problèmes mathématiques. Deux des problèmes les plus utilisés sont
- la factorisation d'entiers,
- le logarithme discret.

Nous détaillons la cryptographie basée sur le problème du logarithme discret dans la première section. Dans la section 1.2, nous parlons des isogénies qui ont de nombreuses applications en cryptographie basée sur les variétés abéliennes.

Dans ce chapitre, nous ne détaillons pas les définitions et propriétés mathématiques des différents objets. En particulier, les variétés abéliennes et les isogénies seront définies au chapitre 2. Nous nous concentrons sur l'utilisation de ces objets, en particulier en cryptographie.

1.1 Cryptographie basée sur le logarithme discret

Rappelons la définition du logarithme discret sur les groupes génériques

Définition 1.1.1. *Soit $G = (\langle g \rangle, \times)$ un groupe cyclique (noté multiplicativement) engendré par un élément g d'ordre n. Un élément x de G est une puissance de g : il existe donc un entier k de $\mathbb{Z}/n\mathbb{Z}$ tel que $x = g^k$. L'entier k est appelé le logarithme discret de x en base g et est noté* $\mathrm{dlog}_g(x)$.

Nous commençons par présenter différents protocoles reposant sur le logarithme discret puis nous discutons de différents groupes sur lesquels les implémenter. Dans la section 1.1.3, nous présentons sommairement les couplages qui permettent de créer de nouveaux protocoles.

1.1.1 Exemples de protocoles

Diffie et Hellman [DH76] ont proposé le protocole suivant qui permet à deux personnes, Alice et Bob, de se mettre d'accord sur un secret commun. Nous supposons qu'ils disposent d'un canal de communication sans erreur mais non sécurisé. C'est-à-dire que les messages ne sont pas modifiés lors de la transmission mais qu'une autre personne peut intercepter leurs communications.

Algorithme 1 Protocole d'échange de clés Diffie-Hellman

1: Alice et Bob se mettent d'accord sur un groupe cyclique G engendré par un élément g.
2: Alice choisit un entier a et envoie g^a à Bob.
3: Bob choisit un entier b et envoie g^b à Alice.
4: Alice et Bob calculent g^{ab}

Alice peut calculer g^{ab} sans connaître b en calculant $(g^b)^a$. Réciproquement, Bob calcule $(g^a)^b$. Quelqu'un qui a intercepté les communications connaît les éléments g^a et g^b. Il ne peut pas retrouver g^{ab} si le problème de Diffie-Hellman est difficile.

Définition 1.1.2. *Le problème de Diffie-Hellman (calculatoire) est : étant donnés un groupe cyclique engendré par un élément g et deux éléments g^a et g^b du groupe, calculer l'élément g^{ab}.*
Le problème de Diffie-Hellman décisionnel est de distinguer la donnée (g, g^a, g^b, g^{ab}) d'une donnée aléatoire (g, g^a, g^b, g^c).

Le problème de Diffie-Hellman n'est pas plus difficile que celui du logarithme discret. En effet il suffit à un attaquant de calculer le logarithme discret de g^a et g^b en base g pour obtenir les entiers a et b et alors de calculer g^{ab} pour résoudre le problème de Diffie-Hellman. Les deux problèmes de Diffie-Hellman ne sont pas équivalents. Par exemple dans les groupes équipés de couplages (voir section 1.1.3), le problème de Diffie-Hellman décisionnel est facile tandis que le calculatoire est supposé difficile.

Le chiffrement ElGamal [ElG85] est un protocole de chiffrement à clé publique basé sur le logarithme discret. Alice choisit un groupe cyclique $G = \langle g, * \rangle$ où le logarithme discret est difficile. Elle choisit un entier x entre 1 et $\#G$ et calcule $h = g^x$. La clé publique d'Alice est alors, (G, h) et sa clé privée x.

Algorithme 2 Chiffrement ElGamal

Entrée: Bob veut envoyer le message $m \in G$ à Alice.
1: Bob choisit un élément y de G.
2: Bob calcule g^y et $m\,h^y$.
3: **return** Bob envoie $(g^y, m\,h^y)$ à Alice

Pour déchiffrer un message (c_1, c_2), il suffit à Alice de calculer c_2/c_1^x. La sécurité du protocole repose sur le problème de Diffie-Hellman calculatoire. En effet, si un attaquant peut calculer g^{xy} à partir des données publiques, il peut retrouver le message. Si le problème de Diffie-Hellman décisionnel est difficile alors le chiffrement ElGamal est sémantiquement sûr (il résiste à des attaques IND-CPA-1).

1.1.2 Groupes pour la cryptographie basée sur le logarithme discret

Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, le calcul du logarithme discret est trivial. En effet, si $g = 1$ alors $\mathrm{dlog}_1(x) = x$. Plus généralement, si g est un générateur de $\mathbb{Z}/n\mathbb{Z}$ alors il est premier à n et l'algorithme d'Euclide étendu fournit un inverse u de g modulo n. Nous avons alors $\mathrm{dlog}_g(x) = xu$. Asymptotiquement, ce calcul est quasi-linéaire en la taille du groupe.

Le groupe des éléments inversibles d'un corps fini $\mathbb{F}_q$ est un groupe cyclique d'ordre $q - 1$ [Ser70, théorème I.2]. D'après [Odl99], la complexité du calcul du logarithme discret dans ce groupe est asymptotiquement sous-exponentielle : elle est en $\mathrm{L}_q\left[\frac{1}{3}; c\right]$ où

$$\mathrm{L}_n\left[\alpha; c\right] = \exp\left(c \log(n)^\alpha \log(\log(n))^{1-\alpha}\right).$$

Cette complexité est approximativement la même que celle du meilleur algorithme connu de factorisation.

L'algorithme de Pohlig-Hellman [PH78] permet de transformer le calcul du logarithme discret dans un groupe de cardinal composé en des calculs de logarithmes discrets dans des sous-groupes plus petits. Soit G un groupe de cardinal

$$\#G = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

La première étape de l'algorithme est de se ramener à calculer k logarithmes discrets dans les sous-groupes de cardinaux $p_i^{\alpha_i}$:

$$\begin{array}{ccc} G & \longrightarrow & G\left[p_1^{\alpha_1}\right] \times \ldots \times G\left[p_k^{\alpha_k}\right] \\ h & \longmapsto & \left(h^{n/p_1^{\alpha_1}}, \ldots, h^{n/p_k^{\alpha_k}}\right) \end{array}$$

Nous devons résoudre le logarithme discret de $h^{n/p_i^{\alpha_i}}$ dans le groupe $G\left[p_i^{\alpha_i}\right]$ engendré par $g^{n/p_i^{\alpha_i}}$. Le logarithme discret de h s'obtient alors par le théorème des restes chinois.

Soit maintenant un groupe G de cardinal p^α une puissance d'un nombre premier. Nous déterminons la décomposition en base p de $\mathrm{dlog}_g(h)$ par l'algorithme 3. Nous avons α logarithmes discrets à calculer dans le groupe $\langle g^{p^{\alpha-1}}, * \rangle$ qui est d'ordre p premier.

Dans le cas général d'un groupe G générique de cardinal premier, la complexité du calcul du logarithme discret est exponentielle. L'algorithme rho de Pollard, de complexité $O(\#G)$, est le meilleur connu.

Algorithme 3 Logarithme discret dans un groupe d'ordre p^α

Entrée: Un groupe $G = \langle g, * \rangle$ de cardinal p^α et un élément h dans G.
Sortie: Le logarithme discret $\mathrm{dlog}_g(h)$ de h en base g.

1: Calculer $\hat{g} = g^{p^{\alpha-1}}$. {Le groupe engendré par $\hat{g}$ est d'ordre p}
2: Calculer a_0, le logarithme discret de $h^{p^{\alpha-1}}$ en base $\hat{g}$.
3: Poser $\hat{h} = hg^{-a_0}$.
4: **for** $i = 1$ to $\alpha - 1$ **do**
5: Calculer a_i, le logarithme discret de $\hat{h}^{p^{\alpha-i-1}}$ en base $\hat{g}$.
6: Poser $\hat{h} = \hat{h}g^{-a_i p^i}$.
7: **end for**
8: **return** $\mathrm{dlog}_g(h) := \sum_{i=0}^{\alpha-1} a_i p^i$

Les variétés abéliennes fournissent des groupes intéressants pour la cryptographie basée sur le logarithme discret. En particulier, les courbes elliptiques (genre 1) et les jacobiennes de courbes hyperelliptiques de genre 2 sont, en général, des groupes pour lesquels nous ne connaissons pas de meilleur algorithme que Pollard rho.

Les conditions supplémentaires que doivent vérifier ces groupes sont d'être de cardinal premier (ou de contenir un sous-groupe premier d'indice faible), d'être défini sur un corps premier $\mathbb{F}_p$ ou sur une extension première de $\mathbb{F}_2$ ou $\mathbb{F}_3$... Étant donnée une courbe, il est facile de tester ces diverses conditions qui ne sont donc pas très contraignantes.

Il existe des algorithmes plus efficaces que Pollard rho pour résoudre le logarithme discret dans les jacobiennes de courbes de genre supérieur (plus grand que 3). Ces algorithmes reposent sur des méthodes de crible. On pourra consulter [Eng08] pour plus de détails sur les différentes méthodes utilisées.

L'idée principale [ADH94] consiste à décrire une base « agréable » de friabilité. De nombreuses personnes ont travaillé pour adapter cet algorithme selon deux directions privilégiées : fixer le genre de la courbe et faire tendre le cardinal du corps vers l'infini ou faire tendre le genre vers l'infini. Résoudre le logarithme discret dans les jacobiennes de courbes de genre supérieur est intéressant pour utiliser la méthode de descente de Weil. Cette dernière permet de transformer la résolution du problème du logarithme discret dans une courbe elliptique sur une extension composée à la résolution de ce problème dans la jacobienne d'une courbe hyperelliptique sur un sous-corps.

Soit $\mathcal{C}$ une courbe hyperelliptique de genre g fixé sur un corps fini $\mathbb{F}_q$. Nous pouvons rajouter la condition que la jacobienne de la courbe est un groupe cyclique car sinon le logarithme discret y est plus facile. Les auteurs de [GTTD07] montrent que le logarithme discret dans $\mathrm{Jac}(\mathcal{C})$ peut être résolu par un algorithme probabiliste de complexité $O\left(q^{2-\frac{2}{g}}\right)$. L'algorithme générique étant en $O\left(q^{\frac{g}{2}}\right)$, dès le genre 3 cet algorithme est plus efficace que l'algorithme générique.

Le modèle de la courbe joue également un rôle important : Diem [Die06] a montré que si la courbe admet un modèle plan de degré d alors il existe un algorithme permettant de résoudre le logarithme discret dans sa jacobienne en temps $O\left(q^{2-\frac{2}{d-2}}\right)$. Ainsi, les courbes non-hyperelliptiques de genre 3 sont isomorphes à une quartique plane, et il existe donc un algorithme en $O(q)$. On pourra consulter [DT08] pour une analyse de ce cas particulier.

Considérons maintenant des modèles de courbes dont le genre tend vers l'infini. Prenons une famille de courbe affine plane $\mathcal{C}_i \in \mathbb{F}_q[X, Y]$ de genre g_i. Supposons que les degrés des courbes en X et Y soient inclus dans l'intervalle $[g_i^\alpha, g_i^{1-\alpha}]$ où $\alpha \in [\frac{1}{3}, \frac{2}{3}]$. D'après [EGT11], Il existe un algorithme de complexité $\mathrm{L}_{q^{g_i}}\left[\frac{1}{3}; c\right]$

pour résoudre le logarithme discret dans $\mathrm{Jac}(\mathcal{C}_i)$. Notons que nous n'avons pas besoin de supposer que le corps de base est fixé, il suffit de faire l'hypothèse que son cardinal ne grossit pas trop vite par rapport au genre : $g_i \geq \log(q_i)^2$.

Pour des variétés abéliennes générales, les algorithmes ont été moins étudiés. On pourra consulter [Gau09] qui décrit un tel algorithme et l'applique à la restriction de Weil de courbes elliptiques et hyperelliptiques sur des extensions de petit degré de corps finis.

1.1.3 Couplages

Les couplages ont d'abord été introduits en cryptographie comme une attaque contre le logarithme discret. Mathématiquement la définition d'un couplage est

Définition 1.1.3. *Soient G_1, G_2, G_3 trois groupes abéliens finis. Un couplage est une application bilinéaire non dégénérée de $G_1 \times G_2$ dans G_3.*
Quand $G_1 = G_2$, le couplage est dit symétrique.

Cryptographiquement, en plus de la définition mathématique, nous demandons qu'un couplage soit calculable efficacement (c'est-à-dire en temps polynomial).

Soit A une variété abélienne principalement polarisée sur un corps k et soit m un entier premier à la caractéristique du corps. Le couplage de Weil e_m est une application

$$e_m : \ A[m] \times A[m] \longrightarrow \mu_m(\overline{k})$$

où $\mu_m(\overline{k})$ désigne le groupe des racines m-ièmes de l'unité de $\overline{k}$. En dehors du couplage de Weil, de nombreux autres couplages existent, par exemple le couplage de Tate. Nous renvoyons à [CF05, chapitres 6 et 16] pour plus de détails sur les couplages et leurs calculs. Dans cette thèse nous utiliserons principalement le couplage de Weil. Au chapitre 6, nous aurons à utiliser une application ressemblant au couplage de Tate.

Soient trois groupes cycliques G_i engendrés par des éléments g_i. S'il existe un couplage

$$e : G_1 \times G_2 \to G_3$$

calculable en temps polynomial alors la résolution du logarithme discret dans G_1 et G_2 se réduit en temps polynomial au logarithme discret dans G_3. En effet,

$$e\left(g_1^k, g_2\right) = e\left(g_1, g_2\right)^k .$$

Après avoir calculé les couplages $e\left(g_1, g_2\right)$ et $e\left(g_1^k, g_2\right)$, nous sommes amenés à résoudre le logarithme discret dans G_3. Cette idée est à la base des attaques sur le logarithme discret sur les courbes elliptiques [MOV91, FR94, HSSI99]. Dans ce cas, le groupe G_3 est l'ensemble des éléments inversibles d'un corps fini et le logarithme discret y est sous-exponentiel. Le groupe G_2 qui apparaît naturellement n'est pas un groupe cyclique. Il faut alors trouver un algorithme polynomial qui fournit un élément de G_2 rendant le couplage non dégénéré.

Des protocoles basés sur les couplages ont été proposés. Citons par exemple un schéma de signature courte [BLS01] ou le chiffrement basé sur l'identité [BF01]. Supposons que Alice, Bob et Charlie veulent se mettre d'accord sur un secret commun. En utilisant le protocole classique de Diffie-Hellman, cela peut être réalisé en deux tours de communication (en supposant que le choix du groupe G a été fait préalablement) comme décrit dans l'algorithme 4. Joux [Jou00] a proposé le protocole 5 permettant de faire cet échange en n'utilisant qu'un seul tour de communication.

Algorithme 4 Échange de clé tripartite

1: Alice, Bob et Charlie se sont mis d'accord un groupe cyclique $G = \langle g, * \rangle$.

2: Alice choisit un entier a,
Bob choisit un entier b,
Charlie choisit un entier c.

3: Alice calcule g^a et l'envoie à Bob,
Bob calcule g^b et l'envoie à Charlie,
Charlie calcule g^c et l'envoie à Alice.

4: Alice calcule $(g^c)^a$ et l'envoie à Bob,
Bob calcule $(g^a)^b$ et l'envoie à Charlie,
Charlie calcule $(g^b)^c$ et l'envoie à Alice.

5: Alice calcule $(g^{bc})^a$,
Bob calcule $(g^{ac})^b$,
Charlie calcule $(g^{ab})^c$.

6: **return** Alice, Charlie et Bob sont en possession de la clé g^{abc}.

Algorithme 5 Échange de clé tripartite en un tour

1: Alice, Bob et Charlie ont choisi trois groupes $G_i = \langle g_i, * \rangle$ et un couplage $e : \ G_1 \times G_2 \to G_3$.

2: Alice choisit un entier a,
Bob choisit un entier b,
Charlie choisit un entier c.

3: Alice calcule et envoie g_1^a à Bob et g_2^a à Charlie,
Bob calcule et envoie g_1^b à Charlie et g_2^b à Alice,
Charlie calcule et envoie g_1^c à Alice et g_2^c à Bob.

4: Alice calcule $e\left(g_1^c, g_2^b\right)^a$,
Bob calcule $e\left(g_1^a, g_2^c\right)^b$,
Charlie calcule $e\left(g_1^b, g_2^a\right)^c$.

5: **return** Alice, Charlie et Bob sont en possession de la clé $e\left(g_1, g_2\right)^{abc}$.

1.2 Utilisation des isogénies

Les isogénies sont un outil important pour l'étude des variétés abéliennes. Elles sont la « bonne » notion de morphismes entre variétés abéliennes. Nous les définirons proprement dans la section 2.1.2 et nous donnerons des algorithmes pour les calculer dans le chapitre 7. Contentons nous de dire que ce sont des morphismes de groupes qui sont calculables.

Le principal intérêt des isogénies est le transfert du logarithme discret d'une variété A initiale où ce dernier est difficile dans une variété B où nous espérons qu'il soit plus facile. Supposons donc que nous avons une isogénie φ entre deux variétés abéliennes A et B :

$$\varphi : \ A \longrightarrow B.$$

Soit g un élément de A d'ordre n et soit x un autre élément de A dont nous voulons calculer le logarithme discret en base g. Nous calculons les images $\varphi(x)$ et $\varphi(g)$ par l'isogénie. L'ordre de $\varphi(g)$ dans la variété B divise l'ordre de g dans A. D'après la discussion de la partie 1.1.2, nous pouvons supposer que g est d'ordre un nombre premier. Si g n'appartient pas au noyau de l'isogénie, alors $\varphi(g)$ et g ont le même ordre. Le logarithme discret de x en base g dans A est donc le même que le logarithme discret de $\varphi(x)$ en base $\varphi(g)$ dans B. Il suffit donc de résoudre le logarithme discret dans la variété B.

Un exemple d'utilisation de cette méthode dans le cas de variétés abéliennes de dimension 3 est donné par Smith [Smi09]. Nous avons vu que le logarithme discret dans les jacobiennes de courbes hyperelliptiques de genre 3 sur un corps fini $\mathbb{F}_q$ peut être résolu en $\tilde{O}\left(q^{\frac{4}{3}}\right)$. Pour les courbes non-hyperelliptiques de genre 3, cette complexité est de $\tilde{O}(q)$. En utilisant des isogénies, Smith montre que pour une certaine proportion de courbes hyperelliptiques, le logarithme discret est attaquable en $\tilde{O}(q)$.

Deux autres applications importantes des isogénies permettent de garantir la sécurité des variétés abéliennes utilisées. Dans le cas des courbes elliptiques, les isogénies sont un des outils de base de l'amélioration par Atkin et Elkies de l'algorithme de comptage de points [Sch85, Sch95, Atk92, Elk91]. Rappelons que connaître le nombre de points sur une variété permet de garantir la sécurité de la variété. On pourra également consulter [Gau04] qui présente les différents algorithmes de comptage de points.
Par ailleurs les isogénies sont utilisées lors du calcul des polynômes de classes [Sut11, GHK+06, CKL08], eux-même nécessaires pour la méthode CM (multiplication complexe). Cette méthode permet de construire directement des variétés ayant un nombre de points donné.

Les isogénies de petit degré sont utilisées pour calculer les polynômes modulaires [BLS10]. Un intérêt de ces derniers est qu'ils permettent de calculer de nouvelles isogénies mais d'un degré supérieur. L'algorithme de Satoh [Sat00] pour calculer le relevé canonique d'une variété ordinaire repose sur la calcul d'une suite de Verschiebung (isogénie contragrédiante du Frobenius). Finalement on utilise de manière cruciale les isogénies pour le calcul d'anneaux d'endomorphismes [Koh96, FM02, BS11].

Chapitre 2

Variétés abéliennes

Nous avons vu dans le chapitre précédent que les variétés abéliennes sont des groupes intéressants en cryptographie. Nous les étudions maintenant du point de vue mathématique.

Dans les chapitres suivants, pour simplifier l'exposition de nos résultats, nous nous placerons principalement sur le corps des complexes. En particulier, dans le chapitre 3, nous ne définirons les fonctions thêta que dans ce cadre. Même si, dans la majorité de cette thèse, nous n'utilisons pas directement les notions théoriques, il est important de définir les objets proprement. Certaines notions théoriques sont par ailleurs utilisées de manière fondamentale dans la preuve de certains des théorèmes cités.

Nous commençons donc ce chapitre par présenter une partie de la théorie générale des variétés abéliennes. Nous introduisons ensuite les jacobiennes de courbes et en particulier celles de courbes hyperelliptiques. Finalement, nous traitons le cas particulier des variétés abéliennes complexes qui sont analytiquement isomorphes à des tores.

Il existe de nombreux ouvrages sur les variétés abéliennes. Concernant la théorie générale, citons [Lan59, Mum70, vdGM07, Mil08]. Pour les variétés abéliennes sur le corps des complexes rajoutons également le livre [BL04].

2.1 Définitions et premières propriétés

2.1.1 Groupes algébriques et variétés abéliennes

Définition 2.1.1. *Soit k un corps, un groupe algébrique sur k est une variété algébrique G munie d'un point particulier $O_G \in G(k)$ et de deux morphismes*

$$\mu : \ G \times G \longrightarrow G, \qquad \iota : \ G \longrightarrow G$$

vérifiant

- *pour tout $P \in G$, $\mu(O_G, P) = \mu(P, O_G) = P$,*
- *pour tout $P \in G$, $\mu(P, \iota(P)) = \mu(\iota(P), P) = O_G$,*
- *pour tout $P, Q, R \in G$, $\mu(\mu(P, Q), R) = \mu(P, \mu(Q, R))$.*

Nous demandons de plus que la variété sous-jacente ainsi que les morphismes μ et ι soient définis sur k.

En pratique cela signifie que G est localement l'ensemble des zéros d'un système polynomial à coefficients dans k et est muni d'une loi de groupe qui s'exprime localement par des fractions rationnelles à coefficients dans k.
Le groupe de Galois $\mathrm{Gal}\left(\overline{k}/k\right)$ agit naturellement sur les points de G. Soit K/k une extension de corps, l'ensemble $G(K)$ correspond à l'ensemble des points qui sont les zéros d'un des systèmes polynomials précédents et ayant des coordonnées dans K. L'ensemble $G(K)$ est naturellement muni d'une structure de groupe.

Un morphisme de groupe algébrique $\phi : G \to H$ est un morphisme de variétés algébriques (c'est-à-dire

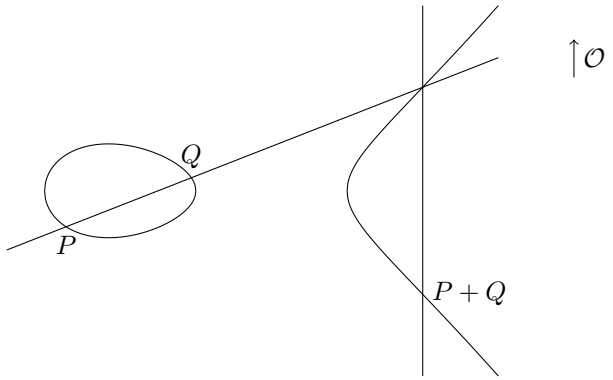


FIGURE 2.1 – Addition sur la courbe elliptique $y^2 = x^3 - x$

donné localement par des polynômes) qui commute avec la structure de groupe :

$$\phi(O_G) = O_H, \qquad \phi(\mu_G(P,Q)) = \mu_H(\phi(P), \phi(Q)), \qquad \phi(\iota_G(P)) = \iota_H(\phi(P)).$$

Soit K le corps de définition de ϕ. Un tel morphisme ϕ définit naturellement un morphisme de groupe de $G(L)$ dans $H(L)$ pour toute extention de corps L/K. De plus, il commute à l'action de $\mathrm{Gal}\left(\overline{K}/K\right)$.

Notons qu'un groupe algébrique est une variété lisse (voir par exemple [Sil86, proposition IV.1.5]).

Définition 2.1.2. *Une variété abélienne est un groupe algébrique complet connexe (pour la topologie de Zariski).*

Comme un groupe algébrique est lisse, un point ne peut être contenu que dans une seule composante irréductible de la variété. La connexité dans la définition de variété abélienne implique donc que ce sont des variétés algébriques irréductibles.
Un fibré $\mathcal{L}$ sur une variété A définit un morphisme rationnel de A dans $\mathbb{P}^{\deg \mathcal{L}}$. Ce morphisme est un plongement si $\mathcal{L}$ est très ample. Toute variété abélienne est alors projective [Mil08, I.6].
Par ailleurs, le groupe sous-jacent à une variété abélienne est obligatoirement commutatif [Mum70, p. 41] d'où le nom d'abélien. Une autre conséquence de la définition est qu'une variété abélienne sur $\mathbb{C}$ est un groupe de Lie compact [Mil08, I.2].

Exemple 2.1.3. *L'exemple le plus simple de variété abélienne est fourni par les courbes elliptiques. Une courbe elliptique sur un corps de caractéristique différente de 2 ou 3 a pour équation $y^2 = x^3 + ax + b$ avec $4a^3 + 27b^2$ non nul. Elle possède un unique point à l'infini noté $\mathcal{O}$. Les points sur la courbe forment un groupe avec les lois d'addition géométriques de la figure 2.1.*

Pour additionner deux points P_1 et P_2 nous avons les formules rationnelles qui suivent. Si P_1 (respectivement P_2) est le point $\mathcal{O}$ alors $P_1 + P_2$ est le point P_2 (respectivement P_1). Sinon, posons $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$. Si $x_2 = x_1$ et $y_2 = -y_1$ alors $P_1 + P_2$ est $\mathcal{O}$. L'opposé d'un point $P = (x, y) \neq \mathcal{O}$ est le point $-P = (x, -y)$.
Dans le cas général, posons

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{si } x_1 = x_2,\ y_1 = y_2, \end{cases}$$

$$\nu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & \text{si } x_1 \neq x_2 \\ \dfrac{-x_1^3 + a x_1 + 2b}{2y_1} & \text{si } x_1 = x_2,\ y_1 = y_2. \end{cases}$$

La droite $y = \lambda x + \nu$ passe par P_1 et P_2 (elle est tangente à la courbe en P_1 dans le cas où $P_1 = P_2$). Les coordonnées (x_3, y_3) du point $P_3 = P_1 + P_2$ sont alors données par

$$x_3 = \lambda^2 - (x_1 + x_2), \qquad y_3 = -\lambda x_3 - \nu.$$

La jacobienne d'une courbe de genre g sur un corps k est une variété abélienne de dimension g. Nous définirons la jacobienne d'une courbe dans la section 2.2.2. Dans le cas des courbes elliptiques (genre 1), la jacobienne est naturellement isomorphe à la courbe elle-même.

2.1.2 Isogénies, variété duale et polarisation

Définition 2.1.4. *Un morphisme de variétés abéliennes est un morphisme algébrique entre les deux variétés qui respecte les lois de groupes.*
Un isomorphisme ϕ entre deux variétés abéliennes A et B est un morphisme tel qu'il existe un morphisme ϕ^{-1} de B vers A vérifiant $\phi \circ \phi^{-1} = \mathrm{Id}_B$ et $\phi^{-1} \circ \phi = \mathrm{Id}_A$.

Avec les notation de la définition, nous avons alors $\ker(\phi) = O_A$ et $\mathrm{Im}(\phi) = B$.

Définition 2.1.5. *Soient A et B deux variétés abéliennes. L'ensemble des morphismes entre A et B est noté* $\mathrm{Hom}(A, B)$ *; c'est un groupe pour l'addition.*
Dans le cas où $B = A$, l'ensemble des morphismes de A dans A forme un anneau (avec la composition) et est noté $\mathrm{End}(A)$.

Pour qu'un morphisme algébrique respecte la loi de groupe, il suffit de supposer qu'il envoie le zéro de la première variété sur le zéro de la seconde [Mum70, corollaire 1 p. 43]. Cette propriété peut être utilisée pour donner une autre démonstration du caractère abélien des groupes sous-jacents à une variété abélienne [Mum70, corollaire 2 p. 44].

Si ϕ est un morphisme entre deux variétés abéliennes A et B alors $\mathrm{Im}(\phi)$ est une sous-variété abélienne de B et $\ker(\phi)$ contient une sous-variété maximale absolument irréductible notée $\ker(\phi)^0$. De plus

$$\dim\left(\ker(\phi)^0\right) + \dim\left(\mathrm{Im}(\phi)\right) = \dim(A)$$

Propriété 2.1.6. *Soit ϕ un morphisme entre deux variétés abéliennes A et B. Deux des propriétés suivantes impliquent la troisième :*
- *A et B ont même dimension,*
- *sur la clôture algébrique, ϕ est surjectif,*
- *sur la clôture algébrique, ϕ est de noyau fini.*

Si ϕ vérifie ces propriétés ont dit que ϕ est une isogénie. Dans le cas où $B = A$, les isogénies sont appelées endomorphismes.

Soient A et B deux variétés abéliennes sur un corps K et soit ϕ une isogénie de A dans B définie sur K. Le corps de fonctions $K(A)$ est une extension algébrique de $\phi^*(K(B))$. Nous disons que ϕ est une isogénie séparable si $K(A)/\phi^*(K(B))$ est séparable et que ϕ est inséparable si l'extension est purement inséparable. Le degré d'une isogénie est son degré en tant que morphisme de variétés algébriques c'est à dire

$$\deg(\phi) = [K(A) : \phi^* K(B)]\,.$$

Pour une isogénie séparable, c'est le cardinal de son noyau. Pour une isogénie inséparable, son noyau est réduit à $\{O_A\}$ mais ce n'est pas un isomorphisme.

Exemple 2.1.7. *La multiplication $[n]$ par un entier n est une isogénie de A dans A. Si g est la dimension de A, alors le degré de $[n]$ est n^{2g}. Si de plus n est premier à la caractéristique du corps alors c'est une isogénie séparable de degré n^{2g}.*
Pour une variété sur un corps fini $\mathbb{F}_q$, le Frobenius (mise à la puissance q) est une isogénie inséparable.

Nous définissons l'ensemble des points de n-torsion comme étant le noyau de la multiplication par n et nous le notons $A[n] = \ker([n])$. Ces points vivent dans une extension du corps de base de la variété de degré inférieur à $n^{2g} - 1$.

Propriété 2.1.8. *Soit A une variété abélienne de dimension g sur un corps algébriquement clos $\overline{k}$ de caractéristique p. Si n est premier à p alors*

$$A[n] \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^{2g}.$$

Si $n = p$ alors il existe un entier r appelé le p-rang de la variété tel que $0 \leq r \leq g$ et

$$A[p] \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{r}.$$

Une variété de p-rang maximal est dite ordinaire.

Soit A une variété abélienne et soit a un élément de $A(\overline{K})$, nous définissons $t_a(\cdot) = \mu(a, \cdot)$ la translation par a sur A. Nous avons alors les définitions

$$\mathrm{Pic}(A) = \{ \text{ faisceaux inversibles sur } A \text{ modulo isomorphisme } \},$$

$$\mathrm{Pic}^0(A) = \left\{\mathcal{L} \in \mathrm{Pic}(A),\ \forall a \in A(\overline{k}),\ t_a^*\mathcal{L} \simeq \mathcal{L}\right\}.$$

Il existe une variété abélienne $A^\vee$ appelée variété duale de A qui paramétrise les points de $\mathrm{Pic}^0(A)$. Une construction en est donnée par exemple dans [Mil08]. En particulier $A^\vee(\overline{k})$ est en bijection avec l'ensemble $\mathrm{Pic}^0(A)$. De plus $A^{\vee\vee}$ est isomorphe à la variété A initiale. Nous ne définissons pas plus en détail la variété duale et nous renvoyons aux diverses références citées au début du chapitre. Dans cette thèse, nous nous intéressons à des variétés abéliennes pour lesquelles la variété et sa duale sont isomorphes.
À toute isogénie $\phi :\ A \to B$, nous pouvons associer une isogénie $\phi^\vee : B^\vee \to A^\vee$ définie par $\phi^\vee(\mathcal{L}) = \phi^*\mathcal{L}$. Cette dernière s'appelle l'isogénie duale de ϕ et a pour noyau $\ker(\phi)^\vee$, le dual de Cartier de $\ker(\phi)$ [Mum70, theorem 1 p. 143]. Dans le cas où k est algébriquement clos et le cardinal de $\ker(\phi) \subset A[n]$ est premier à la caractéristique de k, nous avons

$$\ker\left(\phi^\vee\right) = \mathrm{Hom}\left(\ker(\phi), \mu_n(k)\right).$$

où $\mu_n(k)$ est l'ensemble des racines n-ièmes de l'unité de k [Mil08, p. 41]. À tout faisceau inversible $\mathcal{L}$ nous pouvons associer le morphisme

$$\phi_{\mathcal{L}} :\ \left\{ \begin{array}{ccc} A(\overline{K}) & \longrightarrow & \mathrm{Pic}^0(A) \\ a & \longmapsto & t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} \end{array} \right.$$

Définition 2.1.9. *Une polarisation est une isogénie entre A et $A^\vee$ qui est de la forme $\phi_{\mathcal{L}}$ sur $\overline{K}$ où $\mathcal{L}$ est un fibré ample. Une polarisation est dite principale si c'est un isomorphisme.*
Une variété abélienne est dite (principalement) polarisée si elle possède une polarisation (principale).

Les jacobiennes de courbes sont le principal exemple de variétés abéliennes principalement polarisées.

Définition 2.1.10. *Un morphisme ϕ entre deux variétés abéliennes polarisées A et B est un morphisme respectant les polarisations : si λ et λ' sont des polarisations respectivement sur A et sur B et correspondant respectivement aux faisceaux inversibles amples $\mathcal{L}$ et $\mathcal{M}$ alors nous devons avoir $\phi^*\mathcal{M} = \mathcal{L}$, c'est-à-dire que le diagramme suivant doit être commutatif :*

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^\vee \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle f^\vee} \\ B & \xrightarrow[\lambda']{} & B^\vee \end{array}$$

Pour tout entier m premier à la caractéristique du corps, il existe une application naturelle (généralisant le couplage de Weil dans le cas elliptique) allant de $A(\overline{k})[m] \times A^\vee(\overline{k})[m]$ dans les racines m-ièmes de l'unité $\mu_m(\overline{k})$. Combinée à une polarisation nous obtenons un morphisme

$$e_m^\lambda :\ A(\overline{k})[m] \times A(\overline{k})[m] \longrightarrow \mu_m(\overline{k}).$$

Nous abandonnons l'exposant λ car il n'y aura pas d'ambigüité. Mumford [Mum70, 20 p. 183] donne une expression « simple » de e_m : soit Θ le diviseur associé au fibré $\mathcal{L}$ définissant la polarisation et soit Q un point de m-torsion sur A, posons

$$D_Q = \mathrm{T}_Q\,\Theta - \Theta \in \mathrm{Pic}^0(A)[m]$$

où T_Q désigne la translation par Q. Il existe alors une fonction g_Q de diviseur $\mathrm{Div}(g_Q) = [m]^* D_Q$.

Définition 2.1.11. *Avec les notations précédentes,*

$$e_m : \left\{ \begin{array}{ccc} A(k)[m] \times A(k)[m] & \longrightarrow & \mu_m(k) \\ (P,Q) & \longmapsto & e_m(P,Q) := \frac{g_Q(X+P)}{g_Q(X)} \end{array} \right.$$

où X est un élément quelconque de A.

Mumford montre que cette définition a du sens et que de plus e_m est un couplage c'est-à-dire une application bilinéaire non dégénérée.

Soient P et Q deux éléments de $A[m]$, nous pouvons les considérer comme des éléments de $A^{\vee\vee}[m]$. Ces deux points sont donc des faisceaux inversibles sur $A^\vee$ correspondant à des diviseurs D_P et D_Q. Il existe deux fonctions f_P et f_Q sur A qui représentent les diviseurs mD_P et mD_Q. Lang [Lan58, théorème 6] montre que couplage de Weil est alors donné par la formule

$$e_m(P,Q) = \frac{f_Q(P) f_P(O)}{f_P(Q) f_Q(O)}.$$

Nous reviendrons sur ce couplage dans le cas particulier des jacobiennes de courbes, page 20, et dans celui des tores complexes, page 31.

Nous avons vu que le noyau d'une isogénie entre variétés abéliennes est un sous-groupe fini de la variété. Pour les variétés principalement polarisées, nous avons la condition supplémentaire

Propriété 2.1.12. *Soit ϕ une isogénie entre variété abélienne principalement polarisées. Si ϕ respecte les polarisations alors* $\ker(\phi)$ *est un sous-groupe isotrope pour le couplage de Weil sur A.*

Soit C un sous-groupe fermé d'une variété abélienne A, il existe une unique variété abélienne $B = A/C$ (à isomorphisme près) et une isogénie ϕ de A dans B tels que
- $\ker(\phi) = C$,
- $K(A)/\phi^*(K(B))$ soit séparable.

Soit λ une polarisation sur la variété A de degré premier à la caractéristique du corps et qui soit associée à un fibré ample $\mathcal{L}$. Il existe un fibré ample $\mathcal{M}$ sur B telle que $\mathcal{L} = \phi^*\mathcal{M}$ si et seulement si $\ker(\phi) \subset \ker(\lambda)$ et si le couplage de Weil est trivial sur $\ker(\phi) \times \ker(\phi)$. Ainsi, pour que l'isogénie soit une isogénie de variétés abéliennes polarisées, il faut supposer que le sous-groupe C est isotrope pour le couplage de Weil et inclus dans $\ker(\lambda)$.

Propriété 2.1.13. *Toute isogénie ϕ entre deux variétés abéliennes A et B se décompose en un produit $\pi \circ \psi$ avec*

$$\psi : \; A \longrightarrow A/\ker(\phi)$$

et où π est une isogénie inséparable.
Cette proposition reste valide si nous rajoutons la notion de polarisation.

Dans cette thèse nous nous intéressons uniquement aux d-isogénies séparables de degré premier à la caractéristique du corps (qui sera systématiquement différente de 2). Nous avons alors la décomposition

$$d = 2^{\beta_2} \ell_1^{\alpha_1} \dots \ell_k^{\alpha_k}$$

à laquelle correspond une décomposition

$$\phi = \phi_2^{\beta_2} \phi_{\ell_1}^{\alpha_1} \dots \phi_{\ell_k}^{\alpha_k}$$

où ϕ_ℓ est une isogénie séparable de degré ℓ. Nous avons séparé le degré 2 car comme nous le verrons dans le chapitre 7, les isogénies de degré pair se comportent différement de celles de degré impair.

Propriété 2.1.14. *Soient A et B deux variétés abéliennes. S'il existe une isogénie ϕ de degré n de A vers B alors il existe une isogénie $\hat{\phi}$ de degré n de B vers A appelée l'isogénie contragrédiante et qui vérifie*

$$\phi \circ \hat{\phi} = [n]_B \qquad et \qquad \hat{\phi} \circ \phi = [n]_A.$$

Deux variétés abéliennes sont dites isogènes s'il existe une isogénie entre elles. La relation « être isogène » est une relation d'équivalence sur les variétés abéliennes (la propriété précédente permettant de montrer que cette relation est bien symétrique). Cette relation est plus faible que « être isomorphe », mais il existe néanmoins une notion d' « irréductibilité » pour cette relation.

Définition 2.1.15. *Une variété abélienne sur un corps k est dite simple si ses seules sous-variétés abéliennes sur k sont $\{0\}$ et elle-même. Une variété abélienne est décomposable si elle n'est pas simple. Une variété abélienne est dite absolument simple si elle est simple sur la clôture algébrique du corps où elle est définie.*

Soit $B \subset A$ une sous-variété abélienne stricte. Alors il existe une variété abélienne C telle que A est isogène à $B \times C$. De ce fait,

Théorème 2.1.16. *Toute variété abélienne est isogène à un produit de variétés abéliennes simples. Ces dernières sont uniques à permutations et à isogénies près.*

2.1.3 Considérations arithmétiques

Du point de vue arithmétique, nous disposons d'une généralisation du théorème de Mordell-Weil :

Théorème 2.1.17. *Soit A une variété abélienne sur un corps de nombres K. Le groupe $A(K)$ est un groupe abélien de type fini.*

Ce théorème a été prouvé par Mordell pour les courbes elliptiques, par Weil dans sa thèse pour les jacobiennes et par Taniyama dans le cas général. Notons aussi une extension par Lang et Néron pour d'autres type de corps. Une preuve se trouve dans [Ser89].

Pour les corps finis, les conjuctures de Weil (prouvées par Weil dans le cas des variétés abéliennes et Deligne dans le cas des variétés algébriques générales) impliquent des bornes sur le nombre de points d'une variété. Soit A une variété algébrique sur un corps fini $\mathbb{F}_q$. La fonction zeta associée à A est définie par

$$\zeta_A(s) = \exp\left(\sum_{n=1}^{\infty} \frac{\#A\left(\mathbb{F}_{q^n}\right)}{n} \frac{1}{q^{ns}}\right).$$

La fonction $Z_A(t) \in \mathbb{Q}[[t]]$ définie par $\zeta_A(s) = Z_A(1/q^s)$ est plus pratique à manipuler. Par définition,

$$Z_A(t) = \exp\left(\sum_{n=1}^{\infty} \#A\left(\mathbb{F}_{q^n}\right) \frac{t^n}{n}\right).$$

Le Frobenius (mise à la puissance q) fixe uniquement les points de $A(\mathbb{F}_q)$ et donc

$$\#A(\mathbb{F}_q) = \deg(\pi - 1) = \chi_\pi(1)$$

où $\chi_\pi(t) \in \mathbb{Z}[t]$ est le polynôme caractéristique du Frobenius.

Théorème 2.1.18 (conjectures de Weil)**.** *Soit A une variété abélienne de dimension g. La fonction Z_A est rationnelle : il existe des polynômes P_i à coefficients dans $\mathbb{Q}$ tels que*

$$Z_A(t) = \frac{P_1(t)P_3(t)\dots P_{2g-1}(t)}{P_0(t)P_2(t)\dots P_{2g}(t)}.$$

La fonction Z_A vérifie l'équation fonctionnelle

$$Z_A\left(\frac{1}{q^g t}\right) = \pm q^{\frac{gE}{2}} t^E Z_A(t)$$

où E est la caractéristique d'Euler de A. Le polynôme caractéristique $\chi_\pi(t) \in \mathbb{Z}[t]$ du Frobenius s'écrit

$$\chi_\pi(t) = \prod_{i=1}^{2g}(t - a_i)$$

et l'analogue de l'hypothèse de Riemann précise que les $a_i \in \mathbb{C}$ sont de norme $\sqrt{q}$. Les polynômes P_i sont alors

$$P_0(t) = 1 - t, \qquad P_{2g}(t) = 1 - q^g t,$$

$$P_j(t) = \prod(1 - \alpha_{ij} t) \quad \forall 1 \leq j \leq 2g - 1$$

où α_{ij} parcourent les produits de j racines a_i distinctes de χ_π.

L'analogue de l'hypothèse de Riemann implique que

$$\mid \#A\left(\mathbb{F}_q\right) - q^g - 1 \mid \leq C q^{g-\frac{1}{2}}$$

où C est une constante. Ce théorème montre que le cardinal d'une variété abélienne sur un corps fini $\mathbb{F}_q$ est de l'ordre de q^g.

Dans le cas où la variété est une courbe ou sa jacobienne, les conjectures de Weil impliquent le théorème plus précis suivant :

Théorème 2.1.19. *Soit $\mathcal{C}$ une courbe de genre g sur un corps fini $\mathbb{F}_q$,*

$$\mid \#\mathcal{C}(\mathbb{F}_q) - (q+1) \mid \leq 2g\sqrt{q}$$

$$(\sqrt{q} - 1)^{2g} \leq \#\operatorname{Jac}_{\mathbb{F}_q}(\mathcal{C}) \leq (\sqrt{q} + 1)^{2g}$$

Tate [Tat66] a démontré que deux variétés isogènes ont le même polynôme caractéristique du Frobenius. De ce fait, les fonctions zeta et les cardinaux $\#A\left(\mathbb{F}_{q^m}\right)$ sont des invariants de la classe d'isogénie de A. Des polynômes unitaires à coefficients entiers ayant $2g$ racines complexes de normes $\sqrt{q}$ sont appelés des polynômes q de Weil. Honda [Hon68] a montré une réciproque au théorème de Tate : tout polynôme q de Weil est le polynôme caractéristique de l'action du Frobenius sur une certaine variété abélienne. Notons que cette variété abélienne n'est pas forcément principalement polarisée.

Les conjectures de Weil donnent des bornes sur le cardinal des variétés abéliennes sur les corps finis. Nous voulons savoir comment se comporte ce cardinal quand le corps et/ou la variété varie.

Considérons d'abord le cas de la dimension 1, c'est-à-dire celui des courbes elliptiques. Leur cardinal se trouve dans l'intervalle $\left[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}\right]$ et nous pouvons considérer la distribution de

$$\frac{\#\mathcal{E}(\mathbb{F}_q) - (q+1)}{2\sqrt{q}}.$$

Deux cas sont intéressants : le premier quand q est fixé mais que nous considérons toutes les courbes sur $\mathbb{F}_q$ et le deuxième cas quand nous prenons la réduction d'une courbe de $\mathbb{Q}$ et que nous faisons varier p.

Fixons une puissance q d'un nombre premier p. La distribution des cardinaux de classes d'isomorphismes de courbes elliptiques $\mathcal{E}(\mathbb{F}_q)$ tend vers celle de Sato-Tate quand q tend vers l'infini [Bir68, Yos73].

Le cardinal des courbes elliptiques sur $\mathbb{F}_p$ a de meilleures propriétés de divisibilité que les nombres aléatoires. Ainsi Lenstra [Len87, 1.14] et Howe [How93, th. 1] montrent que la probabilité qu'une courbe

sur $\mathbb{F}_p$ ait un cardinal divisible par un entier n est toujours strictement supérieure à celle d'un nombre « aléatoire » autour de p. Plus formellement, dans le cas où ℓ est premier,

$$\#\left\{\begin{array}{l}\text{courbes elliptiques } \mathcal{E} \text{ sur } \mathbb{F}_p \text{ modulo isomorphismes}\\ \text{telles que } \#\mathcal{E}(\mathbb{F}_p) \equiv 0 \mod \ell\end{array}\right\} = \left\{\begin{array}{ll}\frac{1}{\ell-1}p + O\left(\ell\sqrt{p}\right) & p \equiv 1 \mod \ell\\ \frac{\ell}{\ell^2-1}p + O\left(\ell\sqrt{p}\right) & p \not\equiv 1 \mod \ell\end{array}\right.$$

Pour un nombre aléatoire la probabilité qu'il soit divisible par ℓ est de $1/\ell$ et est donc strictement inférieure à celle pour les courbes elliptiques. On pourra également consulter [CH11]. Remarquons cependant que certaines paramétrisations (par exemple celle de Suyama page 76) ne permettent pas d'obtenir toutes les courbes sur $\mathbb{F}_p$. Il serait intéressant d'avoir de tels résultats pour des sous-familles de courbes sur $\mathbb{F}_p$.

Ces propriétés sont notamment utilisées pour estimer la probabilité de succès de l'algorithme ECM (chapitre 4).

Initialement, ces questions ont été étudiées pour avoir des heuristiques sur la conjecture de Sato-Tate. Soit une courbe elliptique $\mathcal{E}$ sur $\mathbb{Q}$, considérons les premiers p pour lesquels elle a bonne réduction. Supposons que la courbe n'est pas à multiplication complexe alors la conjecture de Sato-Tate donne la distribution de $(\#\mathcal{E}(\mathbb{F}_p) - (p+1))/(2\sqrt{p})$ dans $[-1,1]$ quand p varie. Cette distribution est semi-circulaire. La conjecture a été prouvée par Clozel, Harris, Taylor, Shepherd-Barron pour certaines familles de courbes.

Dans le cas de courbes de genre plus grand, citons les travaux de Kedlaya et Sutherland [KS10] qui ont généralisé ces conjectures aux courbes hyperelliptiques de genre 2.

2.2 Courbes hyperelliptiques

En dimension 1 et 2, toute variété abélienne simple principalement polarisée est la jacobienne d'une courbe hyperelliptique. Comme les cas intéressants cryptographiquement sont ceux de dimension petite, il est naturel de s'intéresser particulièrement à ces courbes.

En dehors des ouvrages généraux sur les variétés abéliennes déjà cités et qui comportent de nombreux résultats pour les courbes et leurs jacobiennes, on pourra consulter la thèse de Gaudry [Gau00] et les livres [CF05] et [Sti93]. Ce dernier est intéressant car il prend le point de vue des corps de fonctions.

2.2.1 Forme de Weierstraß

Définition 2.2.1. *Une courbe hyperelliptique $\mathcal{C}$ sur un corps k est un recouvrement séparable de degré 2 de la droite projective $\pi : \mathcal{C} \to \mathbb{P}^1(k)$.*
Il existe un morphisme non trivial appelé involution hyperelliptique qui échange les points dans les fibres de π.

On demande parfois, pour qu'une courbe soit hyperelliptique, que son genre soit supérieur ou égal à 2 car dans ce cas le corps $k(x)$ est unique. Nous ne faisons pas cette hypothèse ici car les propriétés qui en découlent (voir par exemple [Sti93, VI.2.4]) ne sont pas utilisées. Par conséquent, nos résultats sont aussi valides pour les courbes elliptiques (genre 1).

En tant que corps de fonctions, cette définition se traduit par le fait que $k(\mathcal{C})$ doit être une extension séparable de degré 2 de $k(x)$. Il existe donc un élément y dans $k(\mathcal{C})$ tel que $k(\mathcal{C}) = k(x,y)$. Nous pouvons supposer que y est un entier quitte à le multiplier par un élément de $k(x)$. Il existe donc des polynômes h et f de $k[x]$ tels que y soit une solution de $Y^2 + h(x)Y = f(x)$. La courbe a donc pour équation (affine)

$$\mathcal{C} : \; y^2 + h(x)y = f(x).$$

Le recouvrement $\pi : \mathcal{C} \to \mathbb{P}^1(k)$ est donné par $\pi(x,y) = x$ et l'involution hyperelliptique ι est définie par

$$\iota : \left\{\begin{array}{ccc}\mathcal{C} & \longrightarrow & \mathcal{C}\\ (x,y) & \longmapsto & (x, -y - h(x))\end{array}\right.$$

Remarque 2.2.2. *Dorénavant, nous nous plaçons dans le cas de corps de caractéristique différente de 2.*

Dans ce cadre, nous pouvons, par une translation sur y, supposer que le polynôme h est nul. De plus, quite à prendre une homothétie, f est supposé sans facteur carré. La courbe devient $\mathcal{C} : \ y^2 = f(x)$. Si de plus f est de degré impair $2g+1$, son coefficient dominant c est égal à 1 après le changement de variable $x = cX$ et $y = c^{g+1}Y$. Un modèle projectif de la courbe est donné par l'homogénéisation de cette équation :

$$\mathcal{C} : \ y^2 z^{d-2} = f(x, z)$$

où $d = \deg(f)$ et où nous avons encore noté f pour le polynôme homogénéisé de f.

Théorème 2.2.3. *La courbe hyperelliptique $\mathcal{C}$ d'équation $y^2 = f(x)$ où f est sans facteur carré est lisse en tout point affine de $\bar{k}$.*
Cette courbe possède un point à l'infini $P_\infty = (0 : 1 : 0)$ et pour $d = \deg(f) \geq 4$, la courbe est singulière en ce point. Après éclatement de la singularité, $\mathcal{C}$ possède à l'infini
- *un unique point rationnel si d est impair.*
- *Deux points rationnels si d est pair et si le coefficient dominant de f est un carré dans k.*
- *Deux points non rationnels conjugués sous l'action du groupe de Galois sinon.*

Quand le degré de f est impair on dit que la courbe a un modèle imaginaire, et dans l'autre cas, un modèle réel.

La preuve de ce théorème est donnée dans [Gal11, 11.1.1] en utilisant les coordonnées projectives avec poids : considérons l'espace projectif avec poids (X, Y, Z) où X et Z ont poids 1 et Y a poids $g+1$. La courbe $\mathcal{C}$ a pour équation

$$Y^2 = F_{g+1}(X, Z) \qquad F_{g+1}(X, Z) := Z^{g+1} f\left(\frac{X}{Z}\right)$$

cette courbe est lisse en tout point. Elle possède 1 ou 2 points à l'infini suivant le degré de f : ce sont les points $(1 : \alpha : 0)$ où α est une racine de $x^2 - a_{2g+2}$ et a_{2g+2} est le coefficient de degré $2g+2$ de f.
En spécialisant une variable, nous obtenons un recouvrement affine de la courbe. Commençons par poser $Z = 1$, dans ce cas nous retrouvons l'équation affine originelle de la courbe :

$$Y^2 = F_{g+1}(X, 1) = f(X)$$

Posons ensuite $X = 1$, nous obtenons l'équation

$$Y^2 = \sum_{i=0}^{2g+1} a_i Z^{2g+2-i}$$

Nous pouvons revérifier que sur ces deux ouverts ($X \neq 0$ et $Z \neq 0$), les équations respectives définissent des courbes lisses. De plus, sur l'intersection des ouverts nous pouvons définir l'application rationnelle

$$(X, Y) \longrightarrow (Z, Y) := \left(\frac{1}{X}, \frac{Y}{X^{g+1}}\right)$$

qui est un isomorphisme de la première courbe sur la deuxième (les courbes étant considérées sur l'intersection des ouverts).

Remarque 2.2.4. *Il faut faire attention aux abus de notations. Ainsi bien que nous définissions la courbe $\mathcal{C}$ par l'équation affine $y^2 = f(x)$, nous considérons bien souvent $\mathcal{C}$ comme étant la courbe projective associée. De même, nous utilisons aussi cette notation pour parler de la courbe désingularisée.*
Quand le degré du polynôme f est impair, il existe un unique point de la courbe désingularisée au dessus de $P_\infty = (0 : 1 : 0) \in \mathcal{C}$. Nous utilisons encore la notation P_∞ pour désigner le point sur la courbe désingularisée et informatiquement nous le « codons » par $(0 : 1 : 0)$.

Les points de ramification du morphisme $\pi : \ \mathcal{C} \to \mathbb{P}^1(k)$ sont appelés points de ramification ou points de Weierstraß. Ce sont les points $(a, 0)$ où a est une racine de f et si $\mathcal{C}$ a un modèle imaginaire il faut y rajouter le point P_∞.

Théorème 2.2.5. *Soit f un polynôme sans facteur carré de degré $2g+1$ ou $2g+2$, le genre de la courbe $y^2 = f(x)$ est g.*

Démonstration. Appliquons la formule de Hurwitz au morphisme $\pi : \mathcal{C} \to \mathbb{P}^1(k)$ de degré 2. Si f est de degré $2g+1$, ses points de ramification sont P_∞ et les $(a,0)$ où a est une racine de f. Si f a pour degré $2g+2$ alors les seuls points de ramification de π sont les $(a,0)$. Dans les deux cas, nous avons $2g+2$ points de ramification de degré 2. La formule de Hurwitz donne alors

$$2g(\mathcal{C}) - 2 = 2(2 \cdot 0 - 2) + (2g+2)(2-1)$$

où $g(\mathcal{C})$ est le genre de la courbe $\mathcal{C}$. Nous obtenons donc $g(\mathcal{C}) = g$. □

Un modèle très utile des courbes hyperelliptiques est celui de Rosenhain :

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

Toute courbe hyperelliptique peut se mettre sous cette forme mais il faut en général prendre une extension de corps. En effet, toute la 2-torsion est rationnelle. Même si la 2-torsion est rationnelle, il peut être nécessaire de prendre une extension de degré 2 pour obtenir une forme de Rosenhain de la courbe.

Nous considérons les courbes modulo isomorphisme. La classe d'isomorphisme d'une courbe n'est pas une notion géométrique.

Définition 2.2.6. *Soit $\mathcal{C}$ une courbe définie sur un corps k. Une tordue de $\mathcal{C}$ est une courbe isomorphe à $\mathcal{C}$ sur la clôture algébrique $\overline{k}$ de k mais pas sur k.*

Exemple 2.2.7. *Soit $\mathcal{C} :\ y^2 = f(x)$ une courbe hyperelliptique sur un corps k (non algébriquement clos) et soit κ un non résidu quadratique de k. La courbe*

$$\tilde{\mathcal{C}} :\ \kappa y^2 = f(x)$$

est une tordue quadratique de $\mathcal{C}$. S'il n'existe qu'une seule classe de non résidus quadratiques (comme c'est le cas sur les corps finis), nous parlerons de la tordue quadratique de $\mathcal{C}$.

2.2.2 Jacobiennes de courbes

Contrairement aux courbes elliptiques, les points sur une courbe de genre g ne forment pas un groupe. Il faut travailler sur la jacobienne de la courbe.

Dans cette section, nous ne considérons que des courbes projectives lisses définies sur un corps parfait. Ces conditions sont suffisantes pour avoir une équivalence entre les diviseurs de Weil (que nous allons présenter ici) et les faisceaux inversibles. Dans le cas particulier des courbes hyperelliptiques, ces conditions signifient que nous considérons les modèles désingularisés des courbes.

Définition 2.2.8. *Soit $\mathcal{C}$ une courbe lisse définie sur un corps k parfait. Le groupe des diviseurs $\mathrm{Div}_{\overline{k}}(\mathcal{C})$ sur $\overline{k}$ est le groupe libre engendré par les points de $\mathcal{C}(\overline{k})$.*
Un élément σ du groupe de Galois $G = \mathrm{Gal}(\overline{k}/k)$ agit sur $\mathrm{Div}_{\overline{k}}(\mathcal{C})$ de la façon suivante :

$$\sigma\left(\sum_{P\in\mathcal{C}(\overline{k})} n_P P\right) = \sum_{P\in} n_P \sigma(P)$$

Un diviseur sur k, est un élément de $\mathrm{Div}_{\overline{k}}(\mathcal{C})$ stable sous l'action de G. On note $\mathrm{Div}_k(\mathcal{C})$ l'ensemble des diviseurs sur k, c'est-à-dire

$$\mathrm{Div}_k(\mathcal{C}) = \mathrm{Div}_{\overline{k}}(\mathcal{C})^G$$

Un élément de $\mathrm{Div}_k(\mathcal{C})$ est donc une somme formelle finie de points $\mathcal{C}(\overline{k})$ globalement stable sous l'action de Galois. L'ensemble des points de cette somme forme le support du diviseur. Un diviseur D dont tous les coefficients sont positifs est dit effectif et est noté $D \geq 0$. Cette relation définit naturellement une relation d'ordre partiel compatible avec la structure de groupe sur $\mathrm{Div}_k(\mathcal{C})$.

Définition 2.2.9. *Il existe un morphisme de groupe appelé degré :*

$$\deg : \begin{cases} \mathrm{Div}_k(\mathcal{C}) & \longrightarrow & \mathbb{Z} \\ \sum_{P\in\mathcal{C}(\overline{k})} n_P P & \longmapsto & \sum_{P\in\mathcal{C}(\overline{k})} n_P \end{cases}$$

Le noyau de cette application est noté $\mathrm{Div}_k^0(\mathcal{C})$.

Parmi les diviseurs de degré 0 certains proviennent des fonctions rationnelles :

Théorème 2.2.10. *Soit f un élément de $k(\mathcal{C})$, les zéros et pôles de f sont des points de $\mathcal{C}(\overline{k})$ en nombre fini. Considérons*

$$\mathrm{div}(f) = \sum_{P\in\mathcal{C}(\overline{k})} \mathrm{ord}_P(f)P.$$

C'est un diviseur qui appartient à $\mathrm{Div}_k^0(\mathcal{C})$. *Les diviseurs de ce type sont appelés principaux.*

L'ensemble des diviseurs principaux $\mathrm{Pr}_k(\mathcal{C}) = \{\mathrm{div}(f),\ f \in k(\mathcal{C})^*\}$ forme un sous-groupe de $\mathrm{Div}_k^0(\mathcal{C})$. Il est donc naturel de considérer le groupe quotient.

Définition 2.2.11. *Le groupe de Picard zéro est le quotient du groupe des diviseurs de degré* 0 *par les diviseurs principaux :*

$$\mathrm{Pic}_k^0(\mathcal{C}) = \mathrm{Div}_k^0(\mathcal{C})/\mathrm{Pr}_k(\mathcal{C})$$

Le groupe $G = \mathrm{Gal}(\overline{k}/k)$ agit sur $\mathrm{Pic}_{\overline{k}}^0(\mathcal{C})$ de façon naturelle. En toute généralité, le groupe $\mathrm{Pic}_k^0(\mathcal{C})$ est différent du groupe $\mathrm{Pic}_{\overline{k}}^0(\mathcal{C})^G$. De ce fait, le groupe $\mathrm{Pic}_k^0(\mathcal{C})$ n'est pas pratique à utiliser. Il existe une variété abélienne de dimension g, le genre de la courbe, appelée jacobienne et notée $\mathrm{Jac}(\mathcal{C})$ telle que

$$\mathrm{Jac}_{\overline{k}}(\mathcal{C}) = \mathrm{Pic}_{\overline{k}}^0(\mathcal{C})$$

où nous notons $\mathrm{Jac}_k(\mathcal{C})$ l'ensemble des points k rationnels de la variété abélienne $\mathrm{Jac}(\mathcal{C})$. Pour un corps k quelconque, $\mathrm{Jac}_k(\mathcal{C})$ peut donc différer de $\mathrm{Pic}_k^0(\mathcal{C})$. Si la courbe $\mathcal{C}$ est de genre 0 alors $\mathrm{Jac}_k(\mathcal{C}) = 0$ et si elle est de de genre 1 et possède un point k-rationnel alors $\mathrm{Jac}_k(\mathcal{C}) = \mathcal{C}$.

Plus généralement, quand la courbe $\mathcal{C}$ a un point k-rationnel, nous avons les égalités

$$\mathrm{Pic}_{\overline{k}}^0(\mathcal{C})^G = \mathrm{Pic}_k^0(\mathcal{C}), \qquad \mathrm{Jac}_k(\mathcal{C}) = \mathrm{Pic}_k^0(\mathcal{C}).$$

Comme nous considérons principalement des courbes hyperelliptiques ayant un modèle (projectif désingularisé) imaginaire, les courbes ont toujours un point rationnel : le point à l'infini P_∞.

Soit D un diviseur, l'espace $\mathcal{L}(D)$ défini par

$$\mathcal{L}(D) = \{f \in k(\mathcal{C})^*,\ \mathrm{div}(f) \geq D\} \cup \{0\}$$

est un espace vectoriel de dimension finie. Le théorème suivant précise la dimension de cet espace

Théorème 2.2.12 (Riemann-Roch)**.** *Soit $\mathcal{C}$ une courbe de genre g. Il existe un diviseur W appelé diviseur canonique tel que pour tout diviseur $D \in \mathrm{Div}_k(\mathcal{C})$,*

$$\dim(\mathcal{L}(D)) = \deg(D) + 1 - g + \dim(\mathcal{L}(W - D)).$$

Une preuve du théorème de Riemann-Roch est par exemple donnée dans [Sti93, I.5.15]. Dans sa construction de la variété jacobienne, Weil a utilisé ce théorème pour obtenir une loi de groupe rationnelle sur $\mathcal{C}^{(g)}$, le produit symétrique de la courbe $\mathcal{C}$. Weil a ensuite construit un groupe algébrique à partir de $\mathcal{C}^{(g)}$ et de cette loi.
Le théorème de Riemann-Roch fournit une représentation compacte des diviseurs :

Théorème 2.2.13. *Soit $\mathcal{C}$ une courbe de genre g ayant un point k-rationnel P_0 fixé. Alors toute classe de diviseurs de* $\mathrm{Jac}(\mathcal{C})$ *contient un unique diviseur $D = E - rP_0$ vérifiant*
- *E est un diviseur effectif de degré $r \leq g$,*
- *P_0 n'appartient pas au support de E,*
- *r est minimal*

Un diviseur sous cette forme est dit réduit. L'entier r s'appelle le poids du diviseur.

Soit P_0 un point sur la courbe $\mathcal{C}(k)$ et soit r un entier. Nous avons une application naturelle

$$\begin{array}{ccc} \mathcal{C}^r & \longrightarrow & \mathrm{Jac}(\mathcal{C}) \\ (P_1, \ldots, P_r) & \longmapsto & P_1 + \ldots + P_r - rP_0 \end{array}$$

qui induit une application du produit symétrique $\mathcal{C}^{(r)}$ dans $\mathrm{Jac}(\mathcal{C})$. Nous notons W^r son image dans $\mathrm{Jac}(\mathcal{C})$. Pour $r \leq g$, cette application est birationnelle. En particulier, pour $r = g$, le produit symétrique $\mathcal{C}^{(g)}$ et la jacobienne $\mathrm{Jac}(\mathcal{C})$ sont birationnellement équivalents. Les W^r sont des sous-variétés fermées de $\mathrm{Jac}(\mathcal{C})$ qui peuvent être vues comme l'image des diviseurs effectifs de degré r.

Définition 2.2.14. *Comme W^{g-1} est une sous-variété fermée de* $\mathrm{Jac}(\mathcal{C})$ *de codimension* 1*, c'est un diviseur premier sur* $\mathrm{Jac}(\mathcal{C})$*. Elle est appelée diviseur thêta et est notée Θ.*

Le faisceau inversible $\mathcal{L}(\Theta)$ sur $\mathrm{Jac}(\mathcal{C})$ correspondant au diviseur Θ définit un isomorphisme de $\mathrm{Jac}(\mathcal{C})$ sur sa variété duale. De ce fait

Théorème 2.2.15. *La variété abélienne* $\mathrm{Jac}(\mathcal{C})$ *est principalement polarisée.*

La polarisation ainsi obtenue est appelée canonique. Le théorème de Torelli dit qu'une courbe est uniquement déterminée par sa jacobienne et la polarisation canonique sur cette variété abélienne.

Finalement, citons la propriété suivante qui justifie l'étude des jacobiennes de courbes hyperelliptiques

Propriété 2.2.16. *Toute variété abélienne de genre g, absolument simple et principalement polarisée est*
- *pour $g = 1$, une courbe elliptique,*
- *pour $g = 2$, la jacobienne d'une courbe hyperelliptique,*
- *pour $g = 3$, la jacobienne d'une courbe (non obligatoirement hyperelliptique).*

En genre plus grand, il existe des variétés abéliennes principalement polarisées qui ne sont pas des jacobiennes de courbe.

Dans le cas particulier des jacobiennes de courbes, le couplage de Weil a une forme plus agréable. Soient P et Q deux éléments de $\mathrm{Jac}_k(\mathcal{C})[m]$, c'est à dire que $[m]P = [m]Q = 0$ et supposons qu'ils soient de supports disjoints. Il existe donc deux fonctions f_P et f_Q sur $\mathcal{C}$ telles que

$$\mathrm{Div}(f_P) = [m]P, \qquad \mathrm{Div}(f_Q) = [m]Q.$$

Le couplage de Weil est alors donné par la formule

$$e_m(P, Q) = \frac{f_Q(P)}{f_P(Q)}.$$

Dans le cas elliptique, l'équivalence de cette formule et de celle de la définition 2.1.11 est classique : elle est par exemple mentionnée dans [Hus87, remarque 3.7] ou dans [Sil86, exercice 3.16] (avec une erreur de signe dans ce dernier cas). Une formule légèrement plus générale et permettant de s'affranchir de l'hypothèse des supports disjoints se trouve dans [How96].

2.2.3 Calcul dans les jacobiennes de courbes hyperelliptiques

Soit $\mathcal{C}$ une courbe hyperelliptique d'équation $y^2 = f(x)$ ayant un modèle imaginaire. Nous pouvons spécialiser le théorème 2.2.13 avec le point $P_\infty \in \mathcal{C}(k)$ au lieu du point P_0. Nous avons alors une caractérisation plus précise des diviseurs réduits.

Théorème 2.2.17. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre g, et d'équation*

$$y^2 = f(x) \qquad \text{avec } \deg(f) = 2g+1.$$

Toute classe de diviseurs de $\mathrm{Jac}(\mathcal{C})$ contient un unique diviseur $D = E - rP_\infty$ vérifiant
- *E est un diviseur effectif de degré $r \leq g$,*
- *P_∞ n'appartient pas au support de E,*
- *P et $\iota(P)$ (où ι est l'involution hyperelliptique) n'apparaissent pas simultanément dans le support.*

Un diviseur sous cette forme est dit réduit. L'entier r s'appelle le poids du diviseur.

Une conséquence du troisième point est qu'un point de Weierstraß (c'est-à-dire un point de coordonnées $(a, 0)$ où a est une racine de f) n'apparaît pas avec un coefficient plus grand que 1 dans le support de E. Une représentation agréable d'une classe de diviseur est donnée par

Définition 2.2.18. *Soit $\mathcal{C}$ une courbe hyperelliptique d'équation $y^2 + h(x)y = f(x)$ définie sur un corps k et soit*

$$D = \sum_{i=1}^{r} P_i - rP_\infty$$

avec $P_i = (x_i, y_i)$ un diviseur réduit sur cette courbe. Alors D peut être représenté (de manière unique) par deux polynômes u, v à coefficients dans k et vérifiant
- *$u(x) = \prod_{i=1}^{r}(x - x_i)$,*
- *$\deg v < \deg u = g$,*
- *$v(x_i) = y_i$ pour tout $1 \leq i \leq r$,*
- *u divise $v^2 - f$.*

On dit que (u, v) sont les coordonnées de Mumford du diviseur.

Le polynôme u code les abscisses des points du support de D tandis que v code leurs ordonnées. La dernière condition permet de prendre en compte les multiplicités des points.

Des variantes permettant de traiter les courbes de modèle réel ont été proposées par [EJS+07, GHMM08]. Dans le cas d'une courbe de modèle réel, nous avons deux points à l'infini P_∞^+ et P_∞^-. L'idée est de modifier la représentation 2.2.17 pour tenir compte de ces deux points. Par exemple si g est pair, nous pouvons remplacer gP_∞ par $\frac{g}{2}(P_\infty^+ + P_\infty^-)$.

Géométriquement, la loi de groupe est donnée par le dessin 2.2. Soit D_1 et D_2 deux diviseurs réduits génériques sur $\mathrm{Jac}(\mathcal{C})$. Nous construisons la courbe γ de degré $2g-1$ passant par les points des supports de ces diviseurs. Cette courbe coupe $\mathcal{C}$ en g autres points $R_1, \ldots, R_g$. De ce fait

$$D_1 + D_2 + \sum_{i=1}^{g} R_i - gP_\infty = \mathrm{Div}(\gamma) = 0.$$

Si R_i a pour coordonnées (x_i, y_i) alors la fonction $x - x_i$ a pour diviseur $R_i + \iota(R_i) - 2P_\infty$ et donc

$$D_1 + D_2 = \sum_{i=1}^{g} \iota(R_i) - gP_\infty.$$

Nous avons ainsi construit le diviseur réduit correspond à $D_1 + D_2$.

Soit $\mathcal{C}$ une courbe hyperelliptique de modèle imaginaire sur un corps de caractéristique différente de 2. L'algorithme de Cantor [Can87] permet de calculer la loi de groupe de $\mathrm{Jac}(\mathcal{C})$ avec des diviseurs

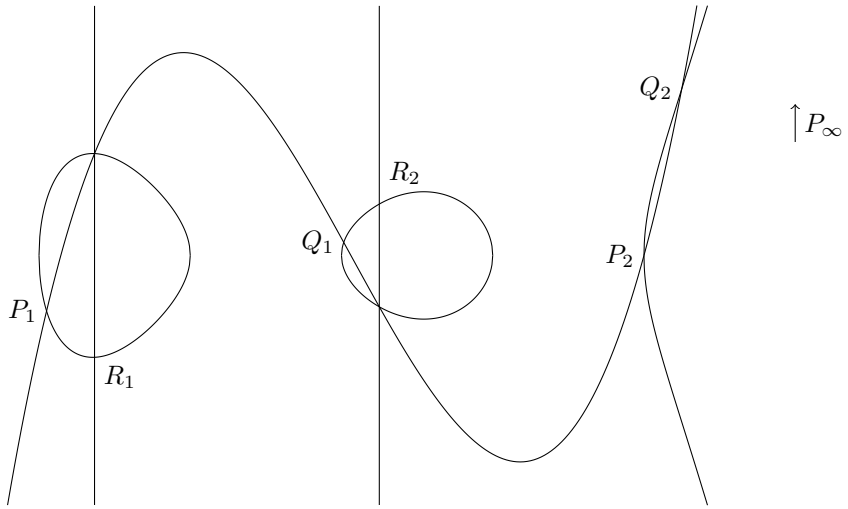


FIGURE 2.2 – Addition de deux diviseurs génériques dans la jacobienne d'un courbe hyperelliptique de genre 2 : $(P_1 + P_2 - 2P_\infty) + (Q_1 + Q_2 - 2P_\infty) = (R_1 + R_2 - 2P_\infty)$

représentés par leurs coordonnées de Mumford (algorithme 6). Il se décompose en deux étapes, la première (points 1 à 4) consiste à calculer les coordonnées du diviseur semi-réduit $D_1 + D_2$. La deuxième étape (points 5 à 8) consiste à le réduire jusqu'à obtenir un diviseur de poids inférieur ou égal à g.
Pour les courbes de modèle réel, des algorithmes du même type sont donnés dans [EJS+07, GHMM08].

Génériquement, la complexité de l'algorithme de Cantor est

$$O\left(M(g)\log(g) + gM(g)\right)$$

où $M(d)$ est le nombre d'opérations à effectuer pour faire une multiplication de polynômes de degré inférieur à d. Notons que pour les grands genres, Cantor [Can87] a proposé un autre algorithme de réduction asymptotiquement meilleur. En pratique, g est « petit » et $M(g)$ est égal à g^2 (avec la multiplication naïve) ou à $g^{\log_2(3)}$ (avec Karatsuba).
En genre fixé et notament pour le genre 2 et 3, il est possible de dérouler l'algorithme de Cantor. Ceci permet d'économiser certaines opérations. Par ailleurs, de nombreux paramètres rentrent en compte pour choisir le meilleur système de coordonnées (projectives, affines, variables supplémentaires,...) et les meilleurs formules. Parmis les divers papiers sur ce sujet, citons celui de Lange [Lan05] pour le genre 2 qui rassemble des formules et donne leur complexité pour trois systèmes différents de coordonnées.
Pour des applications cryptographiques, nous pouvons souvent choisir des courbes et des diviseurs particuliers. Ainsi si certains coefficients sont nuls ou s'ils sont petits alors les formules sont moins coûteuses. Par exemple l'utilisation de diviseurs du type $P - P_\infty$ permet d'avoir des polynômes u et v initiaux de degré 1 et 0 et de ce fait de n'avoir que deux coefficients à gérer.

2.3 Variétés analytiques

2.3.1 Liens avec les variétés algébriques

Comme les fractions rationnelles sont des fonctions méromorphes, les variétés algébriques sont des variétés analytiques. De même les morphismes algébriques entre deux telles variétés sont des morphismes analytiques. La réciproque est en générale fausse : le tore $\mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$ où Ω est une matrice de $\mathrm{Mat}_{g\times g}(\mathbb{C})$ ne peut être le lieu des zéros d'un système polynomial.

Le théorème de Chow [Cho49] montre que tout sous-ensemble analytique fermé de l'espace projectif est algébrique. Une application de ce théorème est que toute application holomorphe f entre une variété

Algorithme 6 Algorithme de Cantor

Entrée: les coordonnées de Mumford (u_1, v_1) et (u_2, v_2) de deux diviseurs D_1 et D_2 de $\mathrm{Jac}(\mathcal{C})$ où $\mathcal{C}$ est la courbe d'équation $y^2 = f(x)$.
Sortie: les coordonnées de Mumford (u, v) de $D_1 + D_2$.

Grâce au pgcd étendu, calculer $d = \mathrm{pgcd}(u_1, u_2, v_1 + v_2) = s_1u_1 + s_2u_2 + t(v_1 + v_2)$.
$u := u_1u_2/d^2$
$v := \left(s_1u_1v_2 + s_2u_2v_1 + t(v_1v_2 + f)\right)/d$
$v := v \bmod u$

while $\deg(g) > g$ **do**
  $u := \left(f - v^2\right)/u$
  $v := -v \bmod u$
end while

return Les polynômes (u, v).

algébrique compacte X dans une variété algébrique Y est régulière [Ser56, proposition 15]. En particulier, si X est une variété abélienne, alors X est compacte et il est possible d'appliquer la propriété précédente : tout morphisme analytique entre deux variétés abéliennes est un morphisme algébrique.

Par exemple, nous appliquerons ce résultat dans le cadre suivant : soit $\mathrm{Jac}(\mathcal{C})$ une jacobienne de courbe hyperelliptique sur $\mathbb{C}$ donnée avec les coordonnées de Mumford, d'après 2.2.2 et 2.1.1, $\mathrm{Jac}(\mathcal{C})$ est une variété abélienne donc compacte. Dans la section 2.3.3, nous donnerons un isomorphisme analytique entre $\mathrm{Jac}(\mathcal{C})$ et un tore $\mathbb{C}^g/\Lambda_\Omega$. Dans le chapitre suivant, nous utiliserons un résultat de Mumford donnant un plongement (analytique) de $\mathbb{C}^g/\Lambda_\Omega$ dans $\mathbb{P}^n(\mathbb{C})$ grâce aux fonctions thêta. Par composition de ces deux applications, nous obtenons un isomorphisme analytique entre $\mathrm{Jac}(\mathcal{C})$ et une sous-variété de l'espace projectif. Ce morphisme est donc algébrique d'après les résultats de Serre et il est donc naturel d'en trouver les équations. Cela sera fait dans le chapitre 5.

Dans toute cette thèse nous prouvons des propriétés algébriques sur $\mathbb{C}$ mais nous voulons les appliquer sur d'autres corps et en particulier sur les corps finis. Quand le corps est plongé dans $\mathbb{C}$, les équations sont valides par restriction.

Un corps algébriquement clos K de caractéristique 0 et de degré de transcendance sur $\mathbb{Q}$ dénombrable) peut être plongé dans $\mathbb{C}$ par le principe de Lefschetz. Le plongement n'est pas topologique mais nous avons le droit d'utiliser des résultats algébriques prouvés à l'aide de la topologie (et en particulier nous pouvons utiliser le tore complexe $\mathbb{C}^g/\Lambda_\Omega$). En résumé, tout résultat algébrique sur $\mathbb{C}$ se transporte sur K.
Étant donnée une variété abélienne sur un corps fini $\mathbb{F}_q$ avec $q = p^e$, nous pouvons relever la variété sur une extension algébrique K de $\mathbb{Q}_p$ puis la plonger dans $\mathbb{C}_p$ et utiliser le principe de Lefschetz. Nous obtenons alors des résultats sur le relevé de la variété dans K et par réduction modulo $\mathfrak{P}$ les résultats se transportent sur la variété originale sur $\mathbb{F}_q$. Ce principe de demonstration est applicable pour les variétés ordinaires. Il faut cependant faire attention à avoir de bonnes propriétés de réduction modulo p.

Par ailleurs, la majorité des résultats de cette thèse sont applicables sur des corps de fonctions. De ce fait nous pouvons considérer que les paramètres des courbes ou les coordonnées des points sont des paramètres formels. Il faut cependant faire attention au fait que les corps de fonctions ne sont pas obligatoirement parfaits.

2.3.2 Tores complexes

Cette section est basée sur le chapitre 4 de [CS86] écrit par Rosen.

Un tore complexe de dimension g est le quotient de $\mathbb{C}^g$ par un réseau Λ. Il est clair que $\mathbb{C}^g/\Lambda$ est une variété analytique compacte. Soit Λ_1 et Λ_2 deux réseaux de $\mathbb{C}^g$. Si $\alpha \in \mathrm{Mat}_{g\times g}(\mathbb{C})$ est telle que $\alpha\Lambda_1 \subset \Lambda_2$

alors la multiplication par α,

$$\phi_\alpha : \left\{ \begin{array}{ccc} \mathbb{C}^g/\Lambda_1 & \longrightarrow & \mathbb{C}^g/\Lambda_2 \\ z & \longmapsto & \alpha z \mod \Lambda_2, \end{array} \right.$$

est une application holomorphe entre les deux tores. Ce sont en fait les seules préservant 0.

Propriété 2.3.1. *L'application*

$$\begin{array}{ccc} \{\alpha \in \mathrm{Mat}_g(\mathbb{C}) \ \alpha\Lambda_1 \subset \Lambda_2\} & \longrightarrow & \{\phi : \ \mathbb{C}^g/\Lambda_1 \to \mathbb{C}^g/\Lambda_2 \text{ holomorphe et telle que } \phi(0) = 0\} \\ \alpha & \longmapsto & \phi_\alpha \end{array}$$

est une bijection.

L'équivalent de la polarisation pour les tores est fourni par l'existence d'une forme hermitienne particulière. Précisons la convention que nous utilisons pour les formes hermitiennes : ce sont des applications H de $\mathbb{C}^g \times \mathbb{C}^g$ dans $\mathbb{C}$ qui sont $\mathbb{C}$-linéaires par rapport à la première variable et telle que $H(x,y) = H(\bar{y}, x)$. De ce fait elles sont anti-linéaires par rapport à la deuxième variable.

Une forme hermitienne H se décompose en une partie réelle et une partie imaginaire : pour tout vecteurs x, y de $\mathbb{C}^g$, nous avons $H(x,y) = E(ix, v) + iE(x,y)$ où $E = \Im(H)$ est une forme bilinéaire alternée à valeurs réelles. Pour tout x, y, nous avons la relation $E(ix, iy) = E(x,y)$.

Définition 2.3.2. *Soit $T = \mathbb{C}^g/\Lambda$ un tore et soit H une forme hermitienne sur ce tore. On dit que H est une forme de Riemann si sa partie imaginaire $E = \Im(H)$ vérifie $E(\Lambda, \Lambda) \subset \mathbb{Z}$.*
Un tore est polarisé s'il existe une forme de Riemann H non dégénérée dessus. Il est principalement polarisé si de plus $\mathrm{Pf}(\Im(H)) = 1$ *(où* Pf *est le pfaffien).*

Demander que $\mathrm{Pf}(\Im(H)) = 1$ implique que $E = \Im(H)$ est non dégénérée. On parle alors de forme symplectique.

Matrice des périodes

Pour tout réseau $\Lambda \subset \mathbb{C}^g$, il existe une base de Λ sur $\mathbb{R}$ constituée de $2g$ vecteurs. Nous pouvons écrire le réseau Λ comme $\Lambda = P\mathbb{Z}^{2g}$ où P est une matrice de $\mathrm{Mat}_{g\times 2g}(\mathbb{C})$. Dans le cas où le tore est principalement polarisé, la matrice P peut être choisie comme étant la base dans laquelle la matrice de $E = \Im(H)$ est :

$$J := \begin{bmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{bmatrix}.$$

Streng [Str10, II.4.1] donne un algorithme permettant de transformer une base quelconque du réseau en une base symplectique. Par définition, $E(Px, Py) = {}^t x J y$. Lang [Lan72, chapitre 8] prouve que la matrice P vérifie des conditions supplémentaires suivantes appelées conditions de Riemann :

$$PJ^{-1}\,{}^tP = 0, \qquad 2i(\bar{P}J^{-1}\,{}^tP)^{-1} > 0$$

où > 0 signifie que la matrice hermitienne est définie positive. En fait la forme de Riemann est, sur la base canonique de $\mathbb{C}^g$,

$$H(u,v) = {}^t u \left(2i(\bar{P}J^{-1}\,{}^tP)^{-1}\right) \bar{v}.$$

Posons $P = (P_1, P_2)$ avec P_1 et P_2 dans $\mathrm{Mat}_{g\times g}(\mathbb{C})$, les matrices P_i sont inversibles car elles sont composées de g vecteurs linéairement indépendants. En considérant l'application

$$\begin{array}{ccc} \mathbb{C}^g & \longrightarrow & \mathbb{C}^g \\ z & \longmapsto & P_2^{-1} z \end{array}$$

Le tore C^g/Λ est isomorphe à $\mathbb{C}^g/\Lambda_\Omega$ où $\Lambda_\Omega = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ avec $\Omega = P_2^{-1}P_1 \in \mathrm{GL}(g, \mathbb{C})$. Les relations de Riemann imposent les conditions suivantes sur Ω :

$${}^t\Omega = \Omega, \qquad \Im(\Omega) > 0.$$

Définition 2.3.3. *L'ensemble des matrices de* $\mathrm{GL}(g, \mathbb{C})$ *symétriques et de partie imaginaire définie positive est appelé espace de Siegel et est noté $\mathcal{H}_g$.*

Action du groupe symplectique

Un autre choix de base symplectique produit, en général, une matrice Ω' de $\mathcal{H}_g$ différente de Ω. Explicitons ce qui se passe : soit $P' = (P'_1, P'_2)$ une autre base symplectique du réseau telle que E ait la même matrice J dans cette nouvelle base, il existe une matrice γ de $\mathrm{GL}_{2g}(\mathbb{Z})$ telle que $P' = P\,{}^t\gamma$ (la transposée permettant d'avoir une action à gauche). La matrice de E dans la nouvelle base est alors $\gamma J\,{}^t\gamma$. Or par hypothèse, celle-ci est égale à J donc γ appartient au groupe symplectique $\mathrm{Sp}(2g,\mathbb{Z})$ où

$$\mathrm{Sp}(2g,\mathbb{Z}) = \left\{\gamma \in \mathrm{GL}_{2g}(\mathbb{Z}),\ \gamma J\,{}^t\gamma = J\right\}$$

Posons

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \qquad A,B,C,D \in \mathrm{Mat}_{g\times g}(\mathbb{Z}).$$

L'équation $P' = P\,{}^t\gamma$ implique que

$$P'_1 = P_1\,{}^tA + P_2\,{}^tB, \qquad P'_2 = P_1\,{}^tC + P_2\,{}^tD.$$

Revenons sur le lien entre les matrices Ω et Ω'. Nous avons

$$\begin{aligned}
\Omega' &= {}^t\Omega' \\
&= {}^tP'_1\,{}^tP'^{-1}_2 \\
&= {}^t(P_1\,{}^tA + P_2\,{}^tB)\,{}^t(P_1\,{}^tC + P_2\,{}^tD)^{-1} \\
&= (A\,{}^tP_1 + B\,{}^tP_2)(C\,{}^tP_1 + D\,{}^tP_2)^{-1} \\
&= (A\,{}^tP_1\,{}^tP_2^{-1} + B)\,{}^tP_2\,{}^tP_2^{-1}(C\,{}^tP_1\,{}^tP_2^{-1} + D)^{-1} \\
&= (A\,{}^t\Omega + B)(C\,{}^t\Omega + D)^{-1} \\
\Omega' &= (A\Omega + B)(C\Omega + D)^{-1}
\end{aligned}$$

Avant d'étudier l'action de $\mathrm{Sp}(2g,\mathbb{Z})$ sur les éléments de $\mathcal{H}_g$, donnons quelques propriétés du groupe symplectique :

Lemme 2.3.4.

$$\gamma \in \mathrm{Sp}(2g,\mathbb{Z}) \Longleftrightarrow \gamma^{-1} \in \mathrm{Sp}(2g,\mathbb{Z}) \Longleftrightarrow {}^t\gamma \in \mathrm{Sp}(2g,\mathbb{Z})$$

Soit $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Mat}_{2g\times 2g}(\mathbb{Z})$*, nous avons les équivalences suivantes*

$$\begin{aligned}
\gamma \in \mathrm{Sp}(2g,\mathbb{Z}) &\iff \begin{cases} {}^tAC \text{ et } {}^tDB \text{ sont symétriques} \\ {}^tAD - {}^tCB = \mathrm{Id} \end{cases} \\
&\iff \begin{cases} A\,{}^tB \text{ et } D\,{}^tC \text{ sont symétriques} \\ A\,{}^tD - B\,{}^tC = \mathrm{Id} \end{cases}
\end{aligned}$$

Par ailleurs si $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *appartient à* $\mathrm{Sp}(2g,\mathbb{Z})$ *alors la matrice* γ^{-1} *est donnée par*

$$\gamma^{-1} = \begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix}.$$

Démonstration. La matrice γ appartient à $\mathrm{Sp}(2g,\mathbb{Z})$ si et seulement si $\gamma J\,{}^t\gamma = J$. En multipliant à gauche par γ^{-1} et à droite par ${}^t\gamma^{-1}$ nous obtenons l'équation $J = \gamma^{-1}J\,{}^t\gamma^{-1}$ qui montre que γ^{-1} appartient à $\mathrm{Sp}(2g,\mathbb{Z})$. Quand nous prennons l'inverse de cette dernière équation nous obtenons $-J = {}^t\gamma(-J)\,{}^t({}^t\gamma)$ ce qui montre que ${}^t\gamma$ appartient aussi à $\mathrm{Sp}(2g,\mathbb{Z})$.
Pour montrer la deuxième assertion du lemme, il suffit de calculer le produit de matrices

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} J \begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} = \begin{pmatrix} A\,{}^tB - B\,{}^tA & A\,{}^tD - B\,{}^tC \\ -D\,{}^tA + C\,{}^tB & C\,{}^tD - D\,{}^tC \end{pmatrix}$$

Cette matrice doit être égale à J et donc nous obtenons la première équivalence. Pour montrer la deuxième, nous appliquons cette équivalence à ${}^t\gamma$ au lieu de γ. Grâce à ces relations, nous vérifions que

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix} = \begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \mathrm{Id}_{2g}$$

d'où la forme de γ^{-1}. □

Définition 2.3.5. *Le groupe* $\mathrm{Sp}(2g,\mathbb{Z})$ *agit sur* $\mathcal{H}_g$ *par*

$$\begin{array}{ccc} \mathrm{Sp}(2g,\mathbb{Z})\times\mathcal{H}_g & \longrightarrow & \mathcal{H}_g \\ \begin{pmatrix} A & B \\ C & D \end{pmatrix},\ \Omega & \longmapsto & \gamma.\Omega = (A\Omega+B)(C\Omega+D)^{-1} \end{array}$$

On peut vérifier que cette action est bien définie. En particulier, il faut montrer que $\gamma.\Omega$ appartient bien à $\mathcal{H}_g$.

Quand nous considérons seulement l'action de $\mathrm{Sp}(2g,\mathbb{Z})$ sur le demi-espace de Siegel, nous voyons que $-\mathrm{Id}_{2g}$ agit trivialement (ceci n'est plus le cas si nous rajoutons l'action sur $\mathbb{C}^g$). Nous avons alors le théorème suivant

Théorème 2.3.6. *L'ensemble des classes de variétés abéliennes principalement polarisées de dimension g modulo isomorphismes est en bijection avec* $\mathrm{PSp}(2g,\mathbb{Z})\backslash\mathcal{H}_g$.

Soient Ω_1 et Ω_2 deux représentants de la même classe de $\mathrm{PSp}(2g,\mathbb{Z})\backslash\mathcal{H}_g$. Les tores $\mathbb{C}^g/\Lambda_{\Omega_1}$ et $\mathbb{C}^g/\Lambda_{\Omega_2}$ sont isomorphes. Il doit donc, d'après la propriété 2.3.1, exister une matrice $\alpha \in \mathrm{GL}_g(\mathbb{C})$ telle que l'isomorphisme soit donné par la multiplication par α. Un rapide calcul permet de trouver α et montre la propriété suivante.

Propriété 2.3.7. *Soient* Ω_1 *et* Ω_2 *deux matrices de* $\mathcal{H}_g$ *correspondant à des tores (principalement polarisés) isomorphes. Il existe alors une matrice* $\gamma = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ *de* $\mathrm{Sp}(2g,\mathbb{Z})$ *telle que*

$$\gamma.\Omega_1 := (A\Omega_1+B)(C\Omega_2+D)^{-1} = \Omega_2.$$

L'isomorphisme entre les deux tores étant donné par

$$\begin{array}{ccc} \mathbb{C}^g/\Omega_1\mathbb{Z}^g+\mathbb{Z}^g & \longrightarrow & \mathbb{C}^g/\Omega_2\mathbb{Z}^g+\mathbb{Z}^g \\ z & \longmapsto & \gamma._{\Omega_1}z := {}^t(C\Omega_1+D)^{-1}z = (-\Omega_2C+A)z \end{array}$$

Quand cela est clair par le contexte, nous écrivons $\gamma.z$ au lieu de $\gamma._{\Omega_1}z$.

Si nous décomposons $z \in \mathbb{C}^g/\Omega_1\mathbb{Z}^g+\mathbb{Z}^g$ en $z = \Omega_1 a + b$ où a et b appartiennent à $\mathbb{R}^g$, nous avons

$$\gamma.z = \gamma.\left(\Omega_1 a+b\right) = \left(\gamma.\Omega_1\right)\left(Da-Cb\right)+\left(-Ba+Ab\right) = \Omega_2\left(Da-Cb\right)+\left(-Ba+Ab\right)$$

Cette décomposition est utile pour étudier l'action sur les points de n-torsion du tore.

Sous-groupes du groupe symplectique

Nous allons souvent nous intéresser à des classes particulières d'isomorphismes. Commençons par définir les groupes de congruences suivants.

Définition 2.3.8. *Pour* $n \geq 1$, *posons*

$$\Gamma_0(n) = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}(2g,z),\ C \equiv 0 \bmod n \right\}$$

$$\Gamma_n = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}(2g,z),\ B \equiv C \equiv 0 \bmod n,\ A \equiv D \equiv \mathrm{Id}_g \bmod n \right\}$$

$$\Gamma_{n,2n} = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Gamma_n,\ \mathrm{diag}\left({}^tAC\right) \equiv \mathrm{diag}\left({}^tDB\right) \equiv 0 \bmod 2n \right\}$$

Avec les notations de la propriété 2.3.7, nous avons pour tout $a, b \in \mathbb{C}^g$

$$\gamma.(\Omega_1 a + b) = (Ab - Ba) + \Omega_2(-Cb + Da) \mod \Lambda_{\Omega_2}.$$

Toute matrice de $\Gamma_0(n)$ laisse globalement invariant le sous-groupe symplectique $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ des points de n-torsion du tore. Il y a en fait une bijection entre $\Gamma_0(n)\backslash\mathcal{H}_g$ et les classes d'équivalence de paires (A, K_1) où A est une variété abélienne principalement polarisée et où il existe K_2 tel que

$$A[n] = K_1 \oplus K_2$$

soit une décomposition symplectique de la n-torsion. Les classes d'équivalences (A, K_1) sont prises modulo la relation d'équivalence suivante : (A, K_1) est équivalent à (A', K_1') si et seulement s'il existe un isomorphisme de A vers A' envoyant K_1 sur K_1'.

Soit x et y deux points de n-torsion. Posons $x = \Omega a + b$ et $y = \Omega c + d$ avec a, b, c, d appartenant à $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$. Définissons alors

$$\tilde{e}_n(x, y) = \exp\big(-2i\pi n({}^t ad - {}^t bc)\big).$$

Le groupe $\Gamma(n)$ correspond à l'ensemble des isomorphismes qui fixent les points de n-torsion. De plus, le couplage $\tilde{e}_n$ de n'importe quelle paire d'éléments de n-torsion reste inchangé.

Dans la suite, il sera alors utile de considérer les sous-groupes suivants.

Définition 2.3.9. *Pour $n \geq 1$, posons*

$$\tilde{\Gamma}_n = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}(2g, z),\ B \equiv C \equiv 0 \bmod n,\ A \equiv D \equiv \pm \mathrm{Id}_g \bmod n \right\},$$

$$\tilde{\Gamma}_{n,2n} = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \tilde{\Gamma}_n,\ \mathrm{diag}\left({}^t AC\right) \equiv \mathrm{diag}\left({}^t DB\right) \equiv 0 \bmod 2n \right\}.$$

La différence par rapport aux groupes Γ_n et $\Gamma_{n,2n}$ est que nous autorisons les matrices à être congrues à $\pm\,\mathrm{Id}$ modulo n.

2.3.3 Application d'Abel-Jacobi

Définition

Une variété abélienne de dimension g sur $\mathbb{C}$ est un groupe de Lie complexe et compact. D'après les propriétés des groupes de Lie, elle est isomorphe analytiquement à un tore C^g/Λ où Λ est un réseau. Dans le cas d'une variété principalement polarisée, nous avons vu que ce tore est isomorphe au tore C^g/Λ_Ω avec $\Lambda_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ pour une certaine matrice Ω de $\mathcal{H}_g$.

En fait, nous pouvons construire explicitement cet isomorphisme pour les courbes hyperelliptiques. Le corps $\mathbb{C}$ étant algébriquement clos et de caractéristique 0, nous pouvons supposer qu'une courbe hyperelliptique $\mathcal{C}$ est de la forme

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

où les a_i sont des nombres complexes distincts. Posons $a_{2g+2} = \infty \in \mathbb{P}^1(\mathbb{C})$. Nous considérons la courbe $\mathcal{C}$ comme une surface de Riemann compacte.

Choisissons $g + 1$ chemins γ_n de $\mathbb{P}^1(\mathbb{C})$ d'origine a_{2n-1} et d'extrémité a_{2n} tels qu'aucun chemin ne se croise. Soit U l'ouvert de $\mathbb{P}^1(\mathbb{C})$ complémentaire de ces chemins. Les fonctions $\pm\sqrt{f(x)}$ sont holomorphes sur U (après un choix initial de racine en un point). En coupant deux copies de $\mathbb{P}^1(\mathbb{C})$ suivant les chemins γ_n et en les recollant, nous pouvons reconstruire $\mathcal{C}$: l'une des copies correspond à la fonction $y = \sqrt{f(x)}$ et l'autre à $y = -\sqrt{f(x)}$.

Considérons les chemins A_i et B_i du dessin 2.3. Dans le dessin 2.4, nous donnons leur projection sur la droite $x \in \mathbb{P}^1(\mathbb{C})$. Les chemins A_i et A_j ne se coupent pas si $i \neq j$, de même pour B_i et B_j. Le chemin A_i ne coupe B_j que si $i = j$ (dans ce cas, ils se coupent en un unique point). Ces chemins forment une base du premier groupe d'homologie $\mathrm{H}_1(\mathcal{C}, \mathbb{Z})$ de la surface de Riemann compacte $\mathcal{C}$.

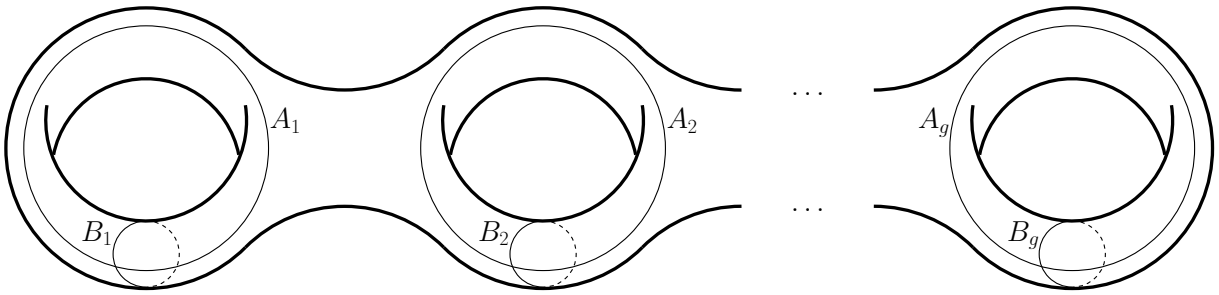


FIGURE 2.3 – Lacets sur la courbe $\mathcal{C}$ vue comme surface de Riemann

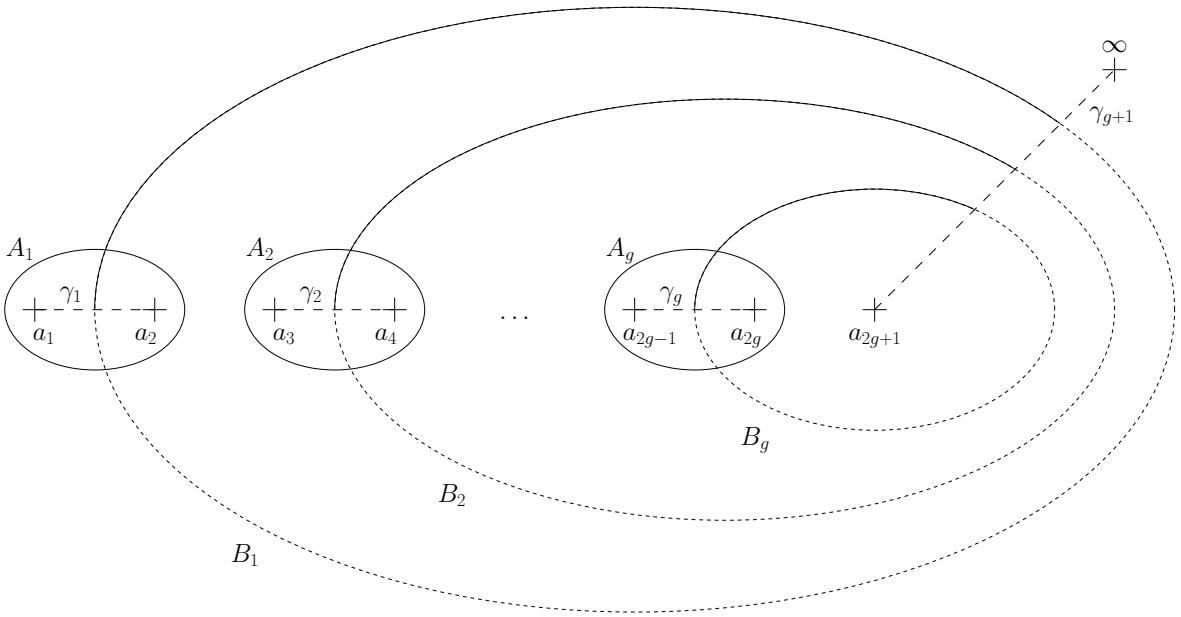


FIGURE 2.4 – Projection des lacets sur $\mathbb{P}^1(\mathbb{C})$

Propriété 2.3.10. *L'espace vectoriel des formes différentielles de première espèce $\Omega^1(\mathcal{C})$ est explicitement donné par*

$$\Omega^1(\mathcal{C}) = \left\{ \omega = \frac{P(x)\,\mathrm{d}\,x}{y} \qquad P \in \mathbb{C}[X],\ \deg(P) \leq g-1 \right\}$$

Définition 2.3.11. *La matrice des périodes Ω associée à une courbe hyperelliptique $\mathcal{C}$ est définie de la façon suivante : il existe une base normalisée $(\omega_i)_{1\leq i\leq g}$ de $\Omega^1(\mathcal{C})$ telle que*

$$\int_{A_i} \omega_j = \delta_{i,j}.$$

Le coefficient (i,j) de $\Omega \in \mathrm{Mat}_{g,g}(\mathbb{C})$ est alors donnée par

$$\Omega_{ij} = \int_{B_i} \omega_j.$$

La matrice Ω ainsi obtenue n'est pas quelconque, Mumford [Mum83, cor. 2.2] montre qu'elle appartient au demi-espace de Siegel $\mathcal{H}_g$. Nous notons ω le vecteur $(\omega_i)_{1\leq i\leq g}$.

Définition 2.3.12. *L'application d'Abel-Jacobi $\mathfrak{u}$ est définie par*

$$\mathfrak{u} : \left\{ \begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathbb{C}^g/\Lambda_\Omega \\ P & \longmapsto & \int_{P_\infty}^{P} \omega \mod \Lambda_\Omega \end{array} \right. \tag{2.1}$$

où n'importe quel chemin de P_∞ à P sur $\mathcal{C}$ peut être choisi.

Démonstration. Pour montrer que l'application d'Abel-Jacobi est bien définie, il suffit de vérifier que pour tous chemins γ et γ' de P_∞ à P nous avons

$$\int_\gamma \omega - \int_{\gamma'} \omega = \int_{\gamma-\gamma'} \omega \quad \in \Omega\mathbb{Z}^g + \mathbb{Z}^g$$

Le lacet $\gamma - \gamma'$ appartient à $\mathrm{H}_1(\mathcal{C},\mathbb{Z})$. Or par définition de la base normalisée $(\omega_i)_{1\leq i\leq g}$, le réseau Λ_Ω est exactement l'image de $\mathrm{H}_1(\mathcal{C},\mathbb{Z})$ par l'application envoyant un lacet σ sur $\int_\sigma \omega$. □

Nous prolongons par linéarité l'application d'Abel-Jacobi aux diviseurs :

$$\mathfrak{u} : \left\{ \begin{array}{ccc} \mathrm{Div}(\mathcal{C}) & \longrightarrow & \mathbb{C}^g/\Lambda_\Omega \\ \sum_{P\in\mathbb{C}} n_P P & \longmapsto & \left(\sum_{P\in\mathbb{C}} n_P \int_{P_\infty}^{P} \omega\right) \mod \Lambda_\Omega \end{array} \right.$$

Théorème 2.3.13 (Abel-Jacobi)**.** *L'application $\mathfrak{u}$ d'Abel-Jacobi est un isomorphisme entre la jacobienne algébrique $\mathrm{Jac}(\mathcal{C})$ et la jacobienne analytique $\mathbb{C}^g/\Lambda_\Omega$.*

Image de la 2-torsion

Les images des points de ramification par l'application d'Abel-Jacobi peuvent être déterminées en manipulant les intégrales 2.1.

Définition 2.3.14. *Soit i dans $\{1,\dots,2g+1\}\cup\{\infty\}$, définissons le vecteur*

$$\eta_i = \begin{pmatrix} \eta_i' \\ \eta_i'' \end{pmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}$$

par

$$\begin{array}{lrcccccc} & & & & i & & g \\ \textit{pour } i = 2n-1 & {}^t\eta'_{2n-1} & = & (0,\dots,0, & \tfrac{1}{2} & ,0,\dots, & 0) \\ \textit{avec } 1\leq n\leq g+1, & {}^t\eta''_{2n-1} & = & (\tfrac{1}{2},\dots,\tfrac{1}{2}, & 0 & ,0,\dots, & 0) \\ & & & & & & \\ \textit{pour } i = 2n & {}^t\eta'_{2n} & = & (0,\dots,0, & \tfrac{1}{2} & ,0,\dots, & 0) \\ \textit{avec } 1\leq n\leq g, & {}^t\eta''_{2n} & = & (\tfrac{1}{2},\dots,\tfrac{1}{2}, & \tfrac{1}{2} & ,0,\dots, & 0) \\ & & & & & & \\ \textit{pour } i = \infty, & {}^t\eta'_{\infty} & = & (0,\dots,0, & 0 & ,0,\dots, & 0) \\ & {}^t\eta''_{\infty} & = & (0,\dots,0, & 0 & ,0,\dots, & 0) \end{array}$$

Étendons cette définition à tout sous-ensemble S de $\{1,\dots,2g+1\}\cup\{\infty\}$ par

$$\eta'_S=\sum_{i\in S}\eta'_i,\qquad \eta''_S=\sum_{i\in S}\eta''_i,\qquad \eta_S=\sum_{i\in S}\eta_i.$$

Propriété 2.3.15. *Pour tout sous-ensemble S de $\{1,\dots,2g+1\}\cup\{\infty\}$,*

$$\mathfrak{u}\left(\sum_{i\in S}(a_i,0)-(\#S)P_\infty\right)=\Omega\eta'_S+\eta''_S$$

Considérons l'opération de différence symétrique $\circ$ sur les sous-ensembles de $\{1,\dots,2g+1\}$ et sur ceux de $\{1,\dots,2g+1\}\cup\{\infty\}$. Elle est définie par

$$A\circ B=(A\cup B)\setminus(A\cap B).$$

Cette opération correspond à l'addition dans le groupe de la 2-torsion $A[2]$. Remarquons qu'elle est commutative, involutive et que $\mathbb{1}_{A\circ B}\equiv\mathbb{1}_A+\mathbb{1}_B \mod 2$. La propriété 2.3.15 donne la valeur exacte de $\mathfrak{u}(D)$ en tant que vecteur de $\mathbb{C}^g$ et non en tant qu'élément du tore $\mathbb{C}^g/\Lambda_\Omega$. De la même façon que

$$\sum_{l\in S}(a_l,0)-\#SP_\infty\simeq\sum_{l\in S^c}(a_l,0)-\#S^cP_\infty,$$

nous avons la relation $\eta_S\equiv\eta_{S^c} \mod 1$. De façon plus précise,

$$\eta_{S^c}=\eta_S+(\eta_{\{1,\dots,2g+1\}\cup\{\infty\}}-2\eta_S).$$

Pour éviter les problèmes de notations dans le chapitre 5, posons $\zeta_g=\eta_{\{1,\dots,2g+1\}\cup\{\infty\}}$. Nous avons

$${}^t\zeta'_g=(1,1,\dots,1)\,,\qquad {}^t\zeta''_g=(g,g-1,\dots,1)\,.$$

Pour tout élément de 2-torsion $D=\sum_{l\in S}(a_l,0)-(\#S)P_\infty$ avec $S\subset\{1,\dots,2g+1\}$, il existe quatre sous-ensembles de $\{1,\dots,2g+1\}\cup\{\infty\}$ correspondant :

$$S,\qquad S\cup\{\infty\},\qquad \{1,\dots,2g+1\}\cup\{\infty\}\setminus S,\qquad \{1,\dots,2g+1\}\setminus S.$$

Mumford [Mum84] et Van Wamelen [vW98] ont choisi de représenter les points de 2-torsion par le système de représentants

$$\big\{S\subset\{1,\dots,2g+1\},\ \#S\equiv 0 \mod 2\big\}.$$

Dans cette thèse, nous en préférons un autre, plus naturel dans le cadre des morphismes (chapitre 5).

Définition 2.3.16. *Posons $\mathcal{U}=\{1,3,\dots,2g+1\}$ les indices impairs. L'image dans $\mathbb{C}^g$ du point de 2-torsion correspondant par l'application d'Abel-Jacobi s'appelle constante de Riemann et est notée $\mathcal{K}$:*

$$\mathcal{K}=\Omega\eta'_{\mathcal{U}}+\eta''_{\mathcal{U}}=\mathfrak{u}\left(\sum_{l\in\mathcal{U}}(a_l,0)-(g+1)P_\infty\right)$$

$${}^t\eta'_{\mathcal{U}}=\left(\frac12,\frac12,\dots,\frac12\right),\qquad {}^t\eta''_{\mathcal{U}}=\left(\frac g2,\frac{g-1}{2},\dots,\frac12\right)$$

Nous utilisons le système de représentants $\{\mathcal{U}\circ S,\ S\subset\{1,\dots,2g+1\},\ \#S\le g\}$ pour les points de 2-torsion.

Deux lemmes techniques

Mumford [Mum84, proposition IIIa.6.3] a prouvé la proposition

Lemme 2.3.17. *L'application e_2 définie par*

$$e_2 : \left\{ \begin{array}{ccc} \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \times \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} & \longrightarrow & \{\pm 1\} \\ (\eta, \zeta) & \longmapsto & (-1)^{4\left({}^t\zeta'\eta'' - {}^t\eta'\zeta''\right)} \end{array} \right.$$

est une forme bilinéaire. Pour tous sous-ensembles S_1, S_2 de $\{1, \ldots, 2g+1\} \cup \{\infty\}$ de cardinaux pairs, nous avons la formule

$$e_2\left(\eta_{S_1}, \eta_{S_2}\right) = (-1)^{\#(S_1 \cap S_2)}.$$

Lemme 2.3.18. *Pour tout sous-ensemble T de $\{1, \ldots, 2g+1\}$,*

$$(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ T}\eta''_{\mathcal{U}\circ T}} = (-1)^{\lfloor \frac{g+1-\#T}{2} \rfloor}.$$

Pour tout sous-ensemble T de $\{1, \ldots, 2g+1\} \cup \{\infty\}$ de cardinal congru à $g+1$ modulo 2,

$$(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ T}\eta''_{\mathcal{U}\circ T}} = (-1)^{\frac{g+1-\#T}{2}}.$$

La deuxième partie de cette proposition est la formule de Mumford. La première s'en déduit en considérant T ou $T \cup \{\infty\}$ suivant le cardinal de T.

Couplage de Weil

Soit A une variété abélienne principalement polarisée associée à une matrice des périodes $\Omega \in \mathcal{H}_g$. La forme de Riemann H, et plus exactement sa partie imaginaire $E = \Im(H)$, définit naturellement une application

$$\begin{array}{ccc} \mathbb{C}^g \times \mathbb{C}^g & \longrightarrow & \mathbb{C}^* \\ x, y & \longmapsto & e^{-2i\pi E(x,y)} \end{array}.$$

Rappellons que si nous écrivons $x = \Omega a + b$ et $y = \Omega c + d$ alors $E(x,y)$ est égal à ${}^t ad - {}^t bc$. L'application $e^{-2i\pi E(x,y)}$ ainsi définie coïncide en un certain sens avec le couplage de Weil. Soit x et y deux points de m-torsion de $\mathbb{C}^g/\Lambda_\Omega$ (c'est à dire que a, b, c, d appartiennent à $\frac{1}{m}\mathbb{Z}^g/\mathbb{Z}^g$), posons

$$\tilde{e}_m(x,y) = \exp\big(-2i\pi E(x, my)\big) = \exp\big(-2i\pi m({}^t ad - {}^t bc)\big).$$

Un cas particulier de cette formule est

$$\tilde{e}_m\left(\Omega \begin{bmatrix} 1/m \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1/m \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right) = \exp\left(-\frac{2i\pi}{m}\right).$$

Il existe un isomorphisme ϕ entre A et $\mathbb{C}^g/\Lambda_\Omega$ tel que

$$\forall P, Q \in A[m], \qquad e_m(P,Q) = \tilde{e}_m\big(\phi(P), \phi(Q)\big).$$

En effet, il suffit de composer l'isomorphisme $A \to \mathbb{C}^g/\Lambda_\Omega$ par un changement de base symplectique. Dans le cas particulier où A est la jacobienne d'une courbe hyperelliptique, l'application d'Abel-Jacobi $\mathfrak{u}$ est un isomorphisme explicite entre A et $\mathbb{C}^g/\Lambda_\Omega$. L'application $\tilde{e}_m$ correspond exactement au couplage de Weil :

Propriété 2.3.19. *Soient P et Q deux éléments de $\mathrm{Jac}(\mathcal{C})[m]$ alors le couplage de Weil est donné par*

$$e_m(P,Q) = \tilde{e}_m\big(\mathfrak{u}(P), \mathfrak{u}(Q)\big).$$

Une preuve dans le cas elliptique est suggérée dans l'exercice 1.15 de [Sil94] (Notons l'inversion du signe dans l'exponentielle). Dans le cas d'une variété générale, cette formule est encore valide, sa démonstration est faite par exemple dans [Rob10, p. 114] en étudiant les fibrés.

Soit $(P_1, \dots, P_{2g})$ une base symplectique de la m-torsion. C'est à dire que la matrice du couplage de Weil dans la base P_i est

$$\begin{bmatrix} & \zeta_m \operatorname{Id}_g \\ -\zeta_m \operatorname{Id}_g & \end{bmatrix}$$

où ζ_m est une racine primitive m-ième de l'unité fixée. Sauf dans le cas où $\zeta_m = exp\left(\frac{2i\pi}{m}\right)$, il n'existe pas de matrice γ de $\mathrm{Sp}(2g, \mathbb{Z})$ telle que la base $(P_1, \dots, P_{2g})$ corresponde à la base canonique de $\mathbb{C}^g/\Lambda_{\gamma.\Omega}$. Si nous travaillons sur un corps plongé dans $\mathbb{C}$, il faudra alors faire attention à la racine de l'unité ζ_m utilisée. Pour d'autres corps, nous pouvons choisir n'importe quelle racine primitive m-ième de l'unité. En effet, pour les preuves, nous pouvons utiliser le principe de Lefschetz pour plonger le corps dans $\mathbb{C}$ mais nous avons le choix de quelle racine primitive m-ième de l'unité s'envoie sur $exp\left(\frac{2i\pi}{m}\right)$.
Nous ne reviendrons pas sur ce point par la suite : si le corps est naturellement plongé dans $\mathbb{C}$, quand nous parlerons de base symplectique de la m-torsion, nous supposerons que $\zeta_m = e_m(P_1, P_{g+1})$ est égal à $exp\left(\frac{2i\pi}{m}\right)$.

Chapitre 3

Fonctions thêta

Les fonctions thêta sont le principal outil utilisé, dans cette thèse, pour l'étude des variétés abéliennes. Historiquement introduites pour l'étude des surfaces de Riemann, elles ont trouvé de nombreuses applications dans divers domaines des mathématiques. En cryptographie, elles fournissent des systèmes de coordonnées « canoniques » pour les variétés abéliennes.

Des versions algébriques des fonctions thêta ont été introduites par Weil [Wei64] pour étudier les variétés abéliennes générales. Ces dernières ont été étudiées en particulier par Mumford. Contrairement à la théorie analytique des fonctions thêta, les versions algébriques présentent l'avantage d'être des fonctions définies sur d'autres corps que le corps des complexes et les preuves de certains théorèmes énoncés dans ce chapitre font appel de manière fondamentale à la théorie algébrique des fonctions thêta.
Cependant, pour de nombreuses applications, le principe de Lefschetz et la théorie de la réduction permettent de transporter les propriétés obtenues sur $\mathbb{C}$ à d'autres corps. En particulier, il est possible d'utiliser cette méthode pour les variétés ordinaires sur les corps finis (avec certaines limitations sur la caractéristique du corps liées au niveau des fonction thêta).

Pour simplifier l'exposition, nous ne travaillerons que sur $\mathbb{C}$ et nous ne présenterons que la théorie classique. Pour celle-ci on peut se référer aux livres [Mum83, Mum84]. Pour aller plus loin en restant dans le cadre analytique on consultera [BL04, Mum91]. Pour l'étude algébrique, citons [Mum66, Mum67a, Mum67b], et [Rob10] qui généralise certains résultats de cette thèse.

Après avoir défini les fonctions thêta et donné leurs liens avec les variétés abéliennes en 3.1, nous décrirons en détail comment les utiliser pour avoir une arithmétique efficace en 3.2.

3.1 Propriétés théoriques

3.1.1 Définitions et propriétés

Les fonctions thêta sont des fonctions holomorphes de $\mathbb{C}^g$ dans $\mathbb{C}$. Ce sont en fait des translatées de la fonction thêta de Riemann à un facteur exponentiel près.

Définition 3.1.1. *Soient Ω une matrice de $\mathcal{H}_g$ et z un vecteur de $\mathbb{C}^g$. La fonction thêta de Riemann est donnée par*

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

Pour tout élément a et b de $\mathbb{Q}^g$, la fonction thêta de caractéristique a,b est définie par

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega) &= \exp\left(i\pi\, {}^t a\Omega a + 2i\pi\, {}^t a\ (z+b)\right)\theta(z+\Omega a+b,\Omega)\\ &= \sum_{n\in\mathbb{Z}^g} \exp\left(i\pi\, {}^t(n+a)\Omega(n+a) + 2i\pi\, {}^t(n+a)(z+b)\right).\end{aligned}$$

La plupart des auteurs utilisent cette définition. Citons par exemple [Igu72, Mum83, Mum84].

Il existe des définitions différentes pour les fonctions thêta avec caractéristiques : l'une d'elles consiste à diviser par 2 les caractéristiques dans l'exponentielle. Ainsi avec cette définition, les fonctions thêta sont définies par

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \sum_{m\in\mathbb{Z}^g} \exp\left(i\pi\,{}^t\left(m+\frac{a}{2}\right)\Omega\left(m+\frac{a}{2}\right) + 2i\pi\,{}^t\left(m+\frac{a}{2}\right)\left(z+\frac{b}{2}\right)\right).$$

Citons par exemple [Igu62, Wen03, FK80, FK01] qui ont choisi cette définition. Pour les niveaux 2 et $(2,2)$ où a et b appartiennent à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$, cette définition est particulièrement bien adaptée et permet de simplifier les notations. Cependant pour le niveau n quelconque, les caractéristiques à valeurs dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ sont plus agréables à manipuler que s'il fallait les considérer dans $\frac{1}{n/2}\mathbb{Z}^g/2\mathbb{Z}^g$.

Dupont [Dup06] a écrit un programme permettant le calcul efficace et certifié des fonctions thêta. Bien que notre but est d'utiliser les fonctions thêta sur les corps finis pour des applications cryptographiques, il est utile de pouvoir évaluer numériquement les fonctions pour tester la correction des formules. En particulier cela permet d'éviter de faire des erreurs de signes : Mumford reconnaît cette difficulté dans l'introduction de [Mum66].

En revenant à la définition des fonctions thêta en tant que somme d'exponentielles, nous obtenons les relations suivantes qui sont importantes car elles permettent de justifier le fait que les caractéristiques sont principalement considérées modulo $\mathbb{Z}^g$ et la variable z modulo le réseau $\Omega\mathbb{Z}^g + \mathbb{Z}^g$.

Propriété 3.1.2. *Soit $\Omega \in \mathcal{H}_g$ et soit $z \in \mathbb{C}^g$, pour tout k', k'' dans $\mathbb{Z}^g$ et pour tout $a, b \in \mathbb{Q}^g$,*

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\Omega k'+k'',\Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)\exp(-i\pi\,{}^t k'\Omega k' - 2i\pi\,{}^t k' z)\exp(2i\pi({}^t a k'' - {}^t b k')). \tag{3.1}$$

De plus, pour tout α, β dans $\mathbb{Q}^g$,

$$\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z,\Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\Omega\alpha+\beta,\Omega)\exp(i\pi\,{}^t\alpha\Omega\alpha + 2i\pi\,{}^t\alpha(z+\beta))\exp(2i\pi\,{}^t\alpha b). \tag{3.2}$$

En particulier si α, β appartiennent à $\mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z,\Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)\exp(2i\pi\,{}^t a\beta). \tag{3.3}$$

Par ailleurs

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](-z,\Omega) = \theta\left[\begin{smallmatrix} -a \\ -b \end{smallmatrix}\right](z,\Omega).$$

En utilisant ces dernières formules nous obtenons que pour le cas particulier des caractéristiques semi-entières, les fonctions sont soit paires soit impaires : soient a et b deux éléments de $\frac{1}{2}\mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](-z,\Omega) = (-1)^{4\,{}^t a\,b}\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega). \tag{3.4}$$

Avec les caractéristiques η (définition 2.3.14), cette équation se reformule : pour tout sous-ensemble T de $\{1,\ldots,2g+1\}\cup\{\infty\}$,

$$\theta[\eta_{\mathcal{U}\circ T}](-z,\Omega) = (-1)^{4\,{}^t\eta'_T\eta''_T}\theta[\eta_{\mathcal{U}\circ T}](z,\Omega)$$

et la propriété 2.3.18 précise, suivant le cardinal de T, si la fonction est paire ou impaire.

Les fonctions thêta vérifient de nombreuses relations : Koizumi [Koi76] dans le cadre analytique et Kempf [Kem89] dans le cadre algébrique ont prouvé la formule 3.1.3 qui regroupe diverses relations dues à d'autres personnes. Soit un entier m et soient m réels positifs γ_i. Soient K_1, K_2 appartenant à $\mathrm{Mat}_{g,m}(\mathbb{R})$, posons

$$K = \begin{bmatrix} K_1 \\ K_2 \end{bmatrix} \in \mathrm{Mat}_{2g,m}(\mathbb{R}).$$

Soit $Z \in \mathrm{Mat}_{g,m}(\mathbb{C})$, nous définissons alors

$$\Theta^{(m)}[K](Z \mid \gamma_1\Omega,\ldots,\gamma_m\Omega) = \prod_{i=1}^{m}\theta\left[K^{(i)}\right]\left(Z^{(i)},\gamma_i\Omega\right)$$

où $K^{(i)}$ et $Z^{(i)}$ désignent la i-ième colonne de K et de Z. Les colonnes de K codent les caractéristiques des différentes fonctions thêta qui apparaissent dans le produit. De même, les colonnes de Z sont des vecteurs de $\mathbb{C}^g$ sur lesquels les fonctions thêta sont évaluées.

Théorème 3.1.3 (Koizumi-Kempf). *Soit Ω une matrice du demi-espace de Siegel $\mathcal{H}_g$. Soit un entier m et soient m réels positifs γ_i (respectivement m réels positifs δ_i), posons Γ la matrice diagonale des γ_i et Δ celle des δ_i. Supposons qu'il existe une matrice $T \in \mathrm{GL}_m(\mathbb{Q})$ telle que ${}^tT\,\Gamma\,T = \Delta$.*
Soient $K = \begin{bmatrix} K_1 \\ K_2 \end{bmatrix} \in \mathrm{Mat}_{2g,m}(\mathbb{R})$ et $Z \in \mathrm{Mat}_{g,m}(\mathbb{C})$. Posons

$$J = \begin{bmatrix} J_1 \\ J_2 \end{bmatrix} = \begin{bmatrix} K_1\,{}^tT^{-1} \\ K_2 T \end{bmatrix}, \qquad W = ZT.$$

Posons également $L_1 = M = \mathrm{Mat}_{g,m}(\mathbb{Z})$, $L_2 = \mathrm{Mat}_{g,m}(\mathbb{Z})\,{}^tT$ et $L = L_1 + L_2$. L'ensemble L_1 est naturellement un sous-groupe de L et nous notons $[L : L_1]$ le cardinal du quotient. Alors

$$[L : L_1]\,\Theta^{(m)}\,[K]\,(Z \mid \gamma_1\Omega, \ldots, \gamma_m\Omega) = \sum \exp\left(-2i\pi\,\mathrm{Tr}\left({}^tP_2 J_1\right)\right)\Theta^{(m)}\,[J+P]\,(W \mid \delta_1\Omega, \ldots, \delta_m\Omega) \quad (3.5)$$

où la somme porte sur les matrices P_1, P_2 appartenant à $\mathrm{Mat}_{g,m}(\mathbb{C})$, avec P_1 qui décrit un système de représentants de $M\,{}^tT^{-1}/(M \cap M\,{}^tT^{-1})$ et P_2 un système de représentants de $MT/(M \cap MT)$.

3.1.2 Systèmes de coordonnées

Fonctions thêta de niveau n

Les fonctions thêta fournissent des coordonnées agréables à manipuler : chaque fonction thêta peut être vue comme une coordonnée d'un plongement projectif de la variété.

Définition 3.1.4. *Soient $\Omega \in \mathcal{H}_g$ et $n \in \mathbb{N}$. Les fonctions $f : \mathbb{C}^g \to \mathbb{C}$ vérifiant pour tout $z \in \mathbb{C}^g$ et pour tout $m', m'' \in \mathbb{Z}^g$,*

$$f(z + \Omega m' + m'') = f(z)\exp\left(-\pi i\, n\,{}^tm'\Omega m' - 2\pi i\, n\,{}^tzm'\right)$$

sont dites de niveau n. Elles forment un espace vectoriel noté R_n^Ω.

Théorème 3.1.5. *L'espace vectoriel R_n^Ω est de dimension finie n^g.*

Une preuve de ce théorème est donnée dans [Mum83, section II.1]. Par abus de notation on parle de « fonctions de niveau n » pour désigner seulement une famille génératrice de R_n^Ω.

Un intérêt de ces fonctions est de permettre de définir une application holomorphe du tore $\mathbb{C}^g/\Lambda_\Omega$ dans l'espace projectif : $k+1$ fonctions $f_0, \ldots, f_k$ de R_n^Ω, telles qu'il existe pour tout $z \in \mathbb{C}^g$ une fonction f_i non nulle en ce point, définissent une application de $\mathbb{C}^g/\Lambda_\Omega$ dans $\mathbb{P}^k(\mathbb{C})$. Nous étudierons cette propriété dans la section 3.1.3

Propriété 3.1.6. *Si H est un sous-groupe de G, nous notons par $\mathrm{Rpr}(G/H)$ un système de représentants dans G des classes. Une base de R_n^Ω est fournie par les familles suivantes :*

$$\begin{aligned}
& & \mathscr{F}'_n &= \left\{\theta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](nz, n\Omega), \quad a \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\}, \\
& & \mathscr{F}_n &= \left\{\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right), \quad b \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\}, \\
\textit{quand } n = k^2, & & \mathscr{F}_{(k,k)} &= \left\{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](kz, \Omega), \quad a, b \in \mathrm{Rpr}\left(\tfrac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\}, \\
\textit{quand } 2 \mid n, & & \mathscr{F}_{(n/2,2)} &= \left\{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]\left(2z, \frac{4\Omega}{n}\right), \quad a \in \mathrm{Rpr}\left(\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right),\ b \in \mathrm{Rpr}\left(\tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\}, \\
\textit{quand } 2 \mid n, & & \mathscr{F}_{(n,1)^2} &= \left\{\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\left(z, \frac{\Omega}{n/2}\right)^2, \quad b \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\}. \\
& & \mathscr{F}_{(n,1)^n} &= \left\{\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](z, \Omega)^n, \quad b \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right)\right\},
\end{aligned}$$

Plus généralement, des familles génératrices de R_n^Ω sont fournies par

$$\begin{aligned} \text{quand } 2 \mid n, \qquad \mathscr{F}_{(n,2)^2} &= \left\{ \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \left(z, \frac{\Omega}{n/2} \right)^2, \quad a \in \mathrm{Rpr}\left(\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right),\ b \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right) \right\}, \\ \mathscr{F}_{(n,n)^n} &= \left\{ \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (z,\Omega)^n, \quad a,b \in \mathrm{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right) \right\}. \end{aligned}$$

Pour ne pas alourdir les notations, nous omettons Rpr dans la suite. Il faut cependant faire attention car deux représentants de la même classe ne donnent pas forcément la même fonction thêta : une racine de l'unité peut apparaître d'après l'équation 3.3.

La première et la deuxième base sont similaires et nous choisissons d'utiliser plutôt $\mathscr{F}_n$. Ces deux bases sont particulièrement bien adaptées pour le calcul d'isogénies (chapitre 7) : le fait d'avoir du $\frac{\Omega}{n}$ permet d'avoir des formules « simples » reliant les thêta constantes de niveau $n\ell$ de la variété associée à Ω et celles de niveau n de la variété associée à $\frac{\Omega}{\ell}$. De plus ce sont ces familles qui interviennent naturellement dans les formules de changement de niveaux. Pour ces raisons, nous décrirons l'algorithmique avec ces formules dans la partie 3.2.

Dans le cas où le niveau $n = k^2$ est un carré, nous avons à notre disposition la base $\mathscr{F}_{(k,k)}$ (ces fonctions sont parfois appelées de niveau (k,k)). L'intérêt de celle-ci est que les fonctions thêta de niveau (k,k) partent du tore $\mathbb{C}^g/\Lambda_\Omega$ et, si Ω provient d'une courbe, nous pouvons étudier ces fonctions directement à partir des points de la jacobienne. Cette propriété sera utilisée pour les preuves analytiques. Cependant, un avantage à utiliser les bases $\mathscr{F}'_n$ ou $\mathscr{F}_n$ est qu'elles sont symétriques :

$$\theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right] (-z) = \theta \left[\begin{smallmatrix} 0 \\ -b \end{smallmatrix}\right] (z)$$

où des représentants de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ ont été fixés. Cette propriété est utile pour obtenir des formules plus symétriques et donc simplifier les preuves algébriques. De plus deux représentants de la même classe définissent la même fonction thêta.

La base $\mathscr{F}_{(n/2,2)}$ quand n est divisible par 2 sera utilisée pour les formules d'addition de la section 3.2.

Dans le cas où n n'est pas un carré, nous n'avons pas de base agréable analytiquement. Pour $n = 2$, cependant, nous pouvons utiliser les deux dernières familles. La base $\mathscr{F}_{(n,1)^2}$ est particulièrement adaptée pour avoir une arithmétique efficace sans prendre de trop grandes extensions de corps mais comme nous le verrons page 42, les propriétés de rationalité de ses thêta constantes diffèrent de celles des autres bases, de ce fait, la famille $\mathscr{F}_{(n,2)^2}$ qui est seulement génératrice est parfois préférée.

Finalement la base $\mathscr{F}_{(n,1)^n}$ et la famille $\mathscr{F}_{(n,n)^n}$ pour n différent de 2 ne seront utilisées que pour l'étude des formules de Thomae (chapitre 6) où elles apparaissent naturellement. Au niveau de l'arithmétique, nous ne disposons pas de formules efficaces et comme dans le cas précédent, les propriétés des thêta constantes associées à la base $\mathscr{F}_{(n,1)^n}$ diffèrent de celles des autres bases.

Remarque 3.1.7. *Pour prouver que toutes ces familles sont bien des bases, nous pouvons utiliser les formules de changement de coordonnées (page 38) et un résultat de Mumford [Mum83, proposition II.1.3] qui montre que les deux premières familles sont des bases.*

Numérotation

Il existe différentes « numérotations » des fonctions thêta. Nous utiliserons principalement celle par les caractéristiques comme définie précédemment 3.1.6. Celle-ci est également utilisée par Mumford [Mum83, Mum84] ou Igusa [Igu72].

Au lieu d'indicer les fonctions thêta par des éléments de $\mathrm{Rpr}\left(\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right)$, certains auteurs les indicent par $\mathrm{Rpr}\left(\mathbb{Z}^g/n\mathbb{Z}^g\right)$. Par exemple Lubicz et Robert [LR10a, LR10b] définissent $\theta_i(z) := \theta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right] \left(z, \frac{\Omega}{n}\right)$ pour $i \in \mathbb{Z}^g/n\mathbb{Z}^g$.

Dans le même ordre d'idée, pour le niveau $(2,2)$, on fixe des représentants des classes de $\mathbb{Z}^{2g}/2\mathbb{Z}^{2g}$ à coefficients 0 ou 1. Ainsi les fonctions thêta de Jacobi (genre 1) sont définies de la façon suivante.

$$\theta_{00}(z) := \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] (z,\Omega), \qquad \theta_{01}(z) := \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (z,\Omega), \qquad \theta_{10}(z) := \theta \begin{bmatrix} \frac{1}{2} \\ 0 \end{bmatrix} (z,\Omega), \qquad \theta_{11}(z) := \theta \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (z,\Omega).$$

C'est aussi le choix fait par Igusa [Igu62] pour le genre 2.

Toujours pour le niveau $(2,2)$, Van Wamelen [vW98] a introduit des fonctions thêta tordues $t_A(z)$ indicées par les sous-ensembles $A \subset \{1,\dots,2g+1\}$ de cardinaux congrus à $g+1$ modulo 2. Une telle fonction correspond à la fonction thêta $\theta\left[\eta_{\mathcal{U}\circ A}\right](z,\Omega)$ (voir le chapitre 5). Takase [Tak96] et Koizumi [Koi97] utilisent la notation $\theta[T]$ pour la thêta constante $\theta[\eta_T](0,\Omega)$.

Finalement, dans le cas du genre 2, il y a 16 fonctions thêta de niveau $(2,2)$. Les auteurs ont alors proposé différentes numérotations. Ainsi Weng [Wen03] utilise pour les thêta constantes (non nulles) la notation

$$\begin{aligned}
\theta_1 &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](0,\Omega), & \theta_2 &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](0,\Omega),\\
\theta_3 &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](0,\Omega), & \theta_4 &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](0,\Omega),\\
\theta_5 &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](0,\Omega), & \theta_6 &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](0,\Omega),\\
\theta_7 &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](0,\Omega), & \theta_8 &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](0,\Omega),\\
\theta_9 &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](0,\Omega), & \theta_{10} &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](0,\Omega).
\end{aligned}$$

Gaudry [Gau07] introduit la numérotation suivante (noter la permutation de θ_2, θ_3, θ_4 et celle de θ_8, θ_9 par rapport à celle de Weng)

$$\begin{aligned}
\theta_1(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_2(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](z,\Omega),\\
\theta_3(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_4(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](z,\Omega),\\
\theta_5(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_6(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](z,\Omega),\\
\theta_7(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_8(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_9(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_{10}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](z,\Omega),\\
\theta_{11}(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](z,\Omega), & \theta_{12}(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](z,\Omega),\\
\theta_{13}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_{14}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(\frac12\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_{15}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(\frac12\ \frac12)\end{smallmatrix}\right](z,\Omega), & \theta_{16}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ \frac12)\end{smallmatrix}\right](z,\Omega).
\end{aligned}$$

Par ailleurs, Gaudry [Gau07] pose

$$\begin{aligned}
\Theta_1(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,2\Omega), & \Theta_2(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,2\Omega),\\
\Theta_3(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,2\Omega), & \Theta_4(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,2\Omega).
\end{aligned}$$

Les numérotations de Gaudry ont également été utilisées dans l'article [Cos10]. Dupont [Dup06] a préféré introduire la notation suivante qui est plus « logique » mais présente l'inconvénient de mélanger les fonctions paires et impaires. Soient a, b deux vecteurs de $\frac12\mathbb{Z}^g$, posons

$$c = \sum_{i=1}^{g} 2^i b_i + \sum_{i=1}^{g} 2^{g+i} a_i,$$

et notons $\theta_c(z)$ pour $\theta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](z,\Omega)$. L'indice c est la valeur décimale de la concaténation des éléments de $2\,{}^t\!b$ et de $2\,{}^t\!a$ (avec les poids forts à droite). Le choix de commencer la numérotation par les b est cohérent

avec la base $\mathscr{F}_{(n,1)^2}$ du niveau 2 : les 2^g fonctions thêta qui y interviennent sont alors numérotées de 0 à 2^g-1. Dans le cas du genre 2 nous obtenons

$$\begin{aligned}
\theta_0(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_1(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_2(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega), & \theta_3(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega),\\
\theta_4(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_5(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_6(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega), & \theta_7(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega),\\
\theta_8(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_9(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_{10}(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega), & \theta_{11}(z) &= \theta\left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega),\\
\theta_{12}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ 0)\end{smallmatrix}\right](z,\Omega), & \theta_{13}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right](z,\Omega),\\
\theta_{14}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega), & \theta_{15}(z) &= \theta\left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right](z,\Omega).
\end{aligned}$$

Cette dernière notation est également utilisée par Streng [Str10] et c'est celle que nous choisissons pour cette thèse.

Changements de base

Les formules pour changer de bases sont données par les relations suivantes qui découlent de la formule de Koizumi. Entre la base $\mathscr{F}'_n$ et $\mathscr{F}_n$,

$$\forall b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right) = \sum_{a\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} \exp(2i\pi n\, {}^t a\, b)\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](nz,n\Omega), \tag{3.6}$$

$$\forall a \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](nz,n\Omega) = \frac{1}{n^g}\sum_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} \exp(-2i\pi n\, {}^t a b)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right). \tag{3.7}$$

Pour $n=k^2$, entre la base $\mathscr{F}_{(k,k)}$ et $\mathscr{F}_n$,

$$\forall b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right) = \sum_{\alpha\in\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}\alpha\\kb\end{smallmatrix}\right](kz,\Omega), \tag{3.8}$$

$$\forall a,b \in \tfrac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](kz,\Omega) = \frac{1}{k^g}\sum_{\beta\in\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g} \exp(-2i\pi k\, {}^t a\beta)\theta\left[\begin{smallmatrix}0\\\frac{b}{k}+\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right). \tag{3.9}$$

Pour $2 \mid n$, entre la base $\mathscr{F}_{(n/2,2)}$ et $\mathscr{F}_n$,

$$\forall b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right) = \sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}\alpha\\2b\end{smallmatrix}\right]\left(2z,\frac{4\Omega}{n}\right), \tag{3.10}$$

$$\forall a \in \tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ \forall b \in \tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z,\frac{4\Omega}{n}\right) = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} (-1)^{4\,{}^t a\beta}\theta\left[\begin{smallmatrix}0\\\frac{b}{2}+\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right). \tag{3.11}$$

Pour $2 \mid n$, entre la famille $\mathscr{F}_{(n,2)^2}$ et la base $\mathscr{F}_n$,

$$\forall b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right)\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right) = \sum_{a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n/2}\right)^2, \tag{3.12}$$

$\forall a \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ \forall b \in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g,$

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n/2}\right)^2 = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \exp(-2i\pi 2\,{}^t a\beta)\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right)\theta\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right). \tag{3.13}$$

La base $\mathscr{F}_{(n,1)^2}$ étant une sous famille de $\mathscr{F}_{(n,2)^2}$, la dernière équation reste valide. Cependant il n'y a pas d'expression « simple » permettant d'exprimer les fonctions de $\mathscr{F}_n$ en fonction de celle de $\mathscr{F}_{(n,1)^2}$. Le plus simple est de passer par la base $\mathscr{F}_{(n/2,2)}$:

$$\forall b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g, \qquad \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n/2}\right)^2 = \sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}\alpha\\2b\end{smallmatrix}\right]\left(2z,\frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right), \tag{3.14}$$

$\forall a \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ \forall b \in \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g,$

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z,\frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right) = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \exp(-2i\pi 2\,{}^t a\beta)\theta\left[\begin{smallmatrix}0\\\frac{b}{2}+\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n/2}\right)^2. \tag{3.15}$$

Pour des variétés abéliennes absolument simples, les thêta constantes $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)$ et $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)$ intervenant en facteur dans les relations précédentes sont non nulles.
Si la thêta constante $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)$ de l'équation 3.12 est nulle, nous pouvons la remplacer par $\theta\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)$ où β appartient à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$. En effet il existe un β telle que cette thêta constante soit non nulle (car la variété abélienne $\mathbb{C}^g/\left(\frac{\Omega}{n/2}\mathbb{Z}^g+\mathbb{Z}^g\right)$ se plonge dans $\mathbb{P}^{2^g-1}(\mathbb{C})$ par les fonctions de $\mathscr{F}_2$).
De même pour tout a, il existe $\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ tel que $\theta\left[\begin{smallmatrix}a\\\beta\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)$ soit non nulle. Nous pouvons alors remplacer $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)$ dans la formule 3.15 par cette thêta constante.

Exemple 3.1.8. *Plaçons nous en genre* 2 *et en niveau* 2. *Nous utilisons la numérotation de Dupont. Les fonctions thêta des différentes bases sont :*

$$\begin{aligned}
&\textit{Pour } \mathscr{F}_2 : && \left\{\theta_0\left(z,\frac{\Omega}{2}\right)\ ,\ \theta_1\left(z,\frac{\Omega}{2}\right)\ ,\ \theta_2\left(z,\frac{\Omega}{2}\right)\ ,\ \theta_3\left(z,\frac{\Omega}{2}\right)\right\}\\
&\textit{Pour } \mathscr{F}_2' : && \{\theta_0(2z,2\Omega)\ ,\ \theta_4(2z,2\Omega)\ ,\ \theta_8(2z,2\Omega)\ ,\ \theta_{12}(2z,2\Omega)\}\\
&\textit{Pour } \mathscr{F}_{(2,1)^2} : && \left\{\theta_0(z,\Omega)^2\ ,\ \theta_1(z,\Omega)^2\ ,\ \theta_2(z,\Omega)^2\ ,\ \theta_3(z,\Omega)^2\right\}\\
&\textit{Pour } \mathscr{F}_{(2,2)^2} : && \left\{\theta_0(z,\Omega)^2\ ,\ \ldots\ ,\ \theta_{15}(z,\Omega)^2\right\}
\end{aligned}$$

Le changement de variables pour passer de $\mathscr{F}_2'$ à $\mathscr{F}_2$ est

$$\begin{aligned}
\theta_0\left(z,\frac{\Omega}{2}\right) &= \theta_0(2z,2\Omega)+\theta_4(2z,2\Omega)+\theta_8(2z,2\Omega)+\theta_{12}(2z,2\Omega)\\
\theta_1\left(z,\frac{\Omega}{2}\right) &= \theta_0(2z,2\Omega)-\theta_4(2z,2\Omega)+\theta_8(2z,2\Omega)-\theta_{12}(2z,2\Omega)\\
\theta_2\left(z,\frac{\Omega}{2}\right) &= \theta_0(2z,2\Omega)+\theta_4(2z,2\Omega)-\theta_8(2z,2\Omega)-\theta_{12}(2z,2\Omega)\\
\theta_3\left(z,\frac{\Omega}{2}\right) &= \theta_0(2z,2\Omega)-\theta_4(2z,2\Omega)-\theta_8(2z,2\Omega)+\theta_{12}(2z,2\Omega)
\end{aligned}$$

Le changement de variables réciproque pour passer de $\mathscr{F}_2$ à $\mathscr{F}_2'$ s'en déduit. Comme nous n'utilisons pas la base $\mathscr{F}_2'$, nous ne le détaillons pas. Intéressons nous maintenant au changement de variables pour passer de $\mathscr{F}_2$ à $\mathscr{F}_{(2,2)^2}$. Pour simplifier les formules, nous oublions le $\Omega/2$ dans les arguments des fonctions thêta de la base $\mathscr{F}_2$.

$$\begin{aligned}
4\,\theta_0(z,\Omega)^2 &= \theta_0(z)\theta_0(0)+\theta_1(z)\theta_1(0)+\theta_2(z)\theta_2(0)+\theta_3(z)\theta_3(0)\\
4\,\theta_1(z,\Omega)^2 &= \theta_0(z)\theta_1(0)+\theta_1(z)\theta_0(0)+\theta_2(z)\theta_3(0)+\theta_3(z)\theta_2(0)\\
4\,\theta_2(z,\Omega)^2 &= \theta_0(z)\theta_2(0)+\theta_1(z)\theta_3(0)+\theta_2(z)\theta_0(0)+\theta_3(z)\theta_1(0)\\
4\,\theta_3(z,\Omega)^2 &= \theta_0(z)\theta_3(0)+\theta_1(z)\theta_2(0)+\theta_2(z)\theta_1(0)+\theta_3(z)\theta_0(0)\\
&\\
4\,\theta_4(z,\Omega)^2 &= \theta_0(z)\theta_0(0)-\theta_1(z)\theta_1(0)+\theta_2(z)\theta_2(0)-\theta_3(z)\theta_3(0)\\
\vdots &\quad \vdots \qquad\qquad\qquad \vdots\\
4\,\theta_{15}(z,\Omega)^2 &= \theta_0(z)\theta_3(0)-\theta_1(z)\theta_2(0)-\theta_2(z)\theta_1(0)+\theta_3(z)\theta_0(0).
\end{aligned}$$

Rapppelons que nous avons défini les thêta constantes comme étant le vecteur projectif des fonctions d'une famille génératrice de R_n^Ω évaluées en 0. Si nous remplaçons z par 0 dans toutes les formules précédentes, nous pouvons calculer les thêta constantes associées aux nouvelles bases en fonction de celles des anciennes bases.
Supposons connues les fonctions thêta de la famille $\mathscr{F}_{(2,2)^2}$ et faisons l'hypothèse que $\theta_0\left(0,\frac{\Omega}{2}\right)$ n'est pas nulle. La famille $\mathscr{F}_2$ est alors donnée par :

$$\begin{aligned}
\theta_0\left(z,\frac{\Omega}{2}\right)\theta_0\left(0,\frac{\Omega}{2}\right) &= \theta_0(z,\Omega)^2+\theta_4(z,\Omega)^2+\theta_8(z,\Omega)^2+\theta_{12}(z,\Omega)^2\\
\theta_1\left(z,\frac{\Omega}{2}\right)\theta_0\left(0,\frac{\Omega}{2}\right) &= \theta_1(z,\Omega)^2+\theta_5(z,\Omega)^2+\theta_9(z,\Omega)^2+\theta_{13}(z,\Omega)^2\\
\theta_2\left(z,\frac{\Omega}{2}\right)\theta_0\left(0,\frac{\Omega}{2}\right) &= \theta_2(z,\Omega)^2+\theta_6(z,\Omega)^2+\theta_{10}(z,\Omega)^2+\theta_{14}(z,\Omega)^2\\
\theta_3\left(z,\frac{\Omega}{2}\right)\theta_0\left(0,\frac{\Omega}{2}\right) &= \theta_3(z,\Omega)^2+\theta_7(z,\Omega)^2+\theta_{11}(z,\Omega)^2+\theta_{15}(z,\Omega)^2.
\end{aligned}$$

En remplaçant z par 0 nous n'obtenons les thêta constantes de la base $\mathscr{F}_2$ qu'à un facteur projectif près. Supposons maintenant connues les fonctions thêta de la base $\mathscr{F}_{(2,1)^2}$. La formule 3.15 se traduit par

$$\begin{aligned}
\theta_0(2z,2\Omega)\theta_0(0,2\Omega) &= \theta_0(z,\Omega)^2+\theta_1(z,\Omega)^2+\theta_2(z,\Omega)^2+\theta_3(z,\Omega)^2\\
\theta_4(2z,2\Omega)\theta_4(0,2\Omega) &= \theta_0(z,\Omega)^2-\theta_1(z,\Omega)^2+\theta_2(z,\Omega)^2-\theta_3(z,\Omega)^2\\
\theta_8(2z,2\Omega)\theta_8(0,2\Omega) &= \theta_0(z,\Omega)^2+\theta_1(z,\Omega)^2-\theta_2(z,\Omega)^2-\theta_3(z,\Omega)^2\\
\theta_{12}(2z,2\Omega)\theta_{12}(0,2\Omega) &= \theta_0(z,\Omega)^2-\theta_1(z,\Omega)^2-\theta_2(z,\Omega)^2+\theta_3(z,\Omega)^2.
\end{aligned}$$

Si nous faisons l'hypothèse que les thêta constantes sont non nulles, nous obtenons alors les fonctions thêta de la base $\mathscr{F}_2'$. Remarquons par contre que les thêta constantes ne sont pas calculables (nous n'obtenons que leur carré). Les fonctions thêta de la base $\mathscr{F}_2$ s'expriment en fonction de celles de $\mathscr{F}_{(2,1)^2}$ en combinant les changements de bases précédents.

Étudions maintenant la base $\mathscr{F}_{(n,1)^n}$ et la famille $\mathscr{F}_{(n,n)^n}$. Pour obtenir les fonctions de $\mathscr{F}_{(n,n)^n}$ à partir de celles de $\mathscr{F}_n'$, nous avons la relation

$$\forall a,b\in\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g,\qquad \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega)^n=\sum_{\alpha_n\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}\exp\left(2i\pi\, n\,{}^t(a+\alpha_n)b\right)T_{\alpha_n}(0,\Omega)\,\theta\left[\begin{smallmatrix}a+\alpha_n\\0\end{smallmatrix}\right](nz,n\Omega)\quad(3.16)$$

où $T_{\alpha_n}(0,\Omega)$ est définie de la manière suivante

$$T_{\alpha_n}(0,\Omega)=\sum_{\alpha_1\in\mathbb{Z}^g/\mathbb{Z}^g}\ \sum_{\alpha_2\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\cdots\sum_{\alpha_{n-1}\in\frac{1}{n-1}\mathbb{Z}^g/\mathbb{Z}^g}\prod_{i=1}^{n-1}\theta\left[\begin{smallmatrix}\alpha_i-\alpha_{i+1}\\0\end{smallmatrix}\right](0,i(i+1)\Omega).$$

Remarquons que dans la définition de T, nous pouvons prendre α_1 toujours égal au vecteur 0 de $\mathbb{Q}^g$. Son introduction permet cependant de simplifier l'écriture de la formule.
Dans l'autre sens, les formules suivantes permettent de passer des familles $\mathscr{F}_{(n,1)^n}$ ou $\mathscr{F}_{(n,n)^n}$ à la base $\mathscr{F}'_n$: pour tout a et tout α dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$,

$$n^g T_\alpha(0,\Omega)\,\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](nz,n\Omega) = \sum_{\beta\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} \exp\left(-2i\pi n\,{}^t\beta a\right)\theta\left[\begin{smallmatrix}a-\alpha\\\beta\end{smallmatrix}\right](z,\Omega)^n \tag{3.17}$$

$$n^g T_a(0,\Omega)\,\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](nz,n\Omega) = \sum_{\beta\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} \exp\left(-2i\pi n\,{}^t\beta a\right)\theta\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right](z,\Omega)^n. \tag{3.18}$$

Avant de donner la démontration de ces formules, faisons la remarque suivante qui montre que cette famille de fonctions se comporte mal vis à vis des autres bases.

Remarque 3.1.9. *Les constantes $T_{\alpha_n}(0,\Omega)$ ne sont pas directement calculables à partir de la donnée d'une des familles de fonctions thêta considérées. Nous ne pouvons donc pas calculer les coordonnées d'un point avec la famille $\mathscr{F}_{(n,n)^n}$ à partir des coordonnées du point dans une des bases classiques.*

Une solution pour résoudre ce problème pourrait être d'utiliser les isogénies (chapitre 7) pour obtenir les thêta constantes des variétés associées aux différentes matrices Ω qui apparaissent dans les équations. Dans la formule 3.17, la constante $T_\alpha(0,\Omega)$ est un facteur projectif qui n'a pas besoin d'être calculé. Nous pouvons donc calculer les coordonnées de la base $\mathscr{F}'_n$ à partir de celles de la famille $\mathscr{F}_{(n,n)^n}$.

Les formules précédentes se trouvent dans le livre de Krazer et Prym [KP92] au chapitre 5. Nous reformulons la démonstration en utilisant les notations modernes.

Démonstration. Considérons la matrice suivante

$$F = \begin{pmatrix} 1 & 1 & \dots & \dots & 1\\ 0 & 1 & \dots & \dots & \vdots\\ \vdots & \ddots & \ddots & & \\ \vdots & & \ddots & \ddots & \vdots\\ 0 & \dots & \dots & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & \dots & \dots & \dots & 0\\ 1 & 0 & & & \vdots\\ 0 & 2 & \ddots & & \vdots\\ \vdots & \ddots & \ddots & 0 & 0\\ 0 & \dots & 0 & n-1 & 0 \end{pmatrix},$$

nous pouvons vérifier que

$${}^tFF = \begin{pmatrix} 1\cdot 2 & & & & \\ & 2\cdot 3 & & & \\ & & \ddots & & \\ & & & (n-1)n & \\ & & & & n \end{pmatrix}.$$

La formule 3.16 est alors un cas particulier de la formule de Koizumi avec $T = F$. Si les α_i parcourent des représentants de $\frac{1}{i}\mathbb{Z}^g/\mathbb{Z}^g$ alors

$$P_1 = (\alpha_1-\alpha_2, \alpha_2-\alpha_3, \dots, \alpha_{n-1}-\alpha_n, \alpha_n) \in \mathrm{Mat}_{g,n}(\mathbb{Q})$$

décrit $M\,{}^tT^{-1}/M$ où $M = \mathrm{Mat}_{g,n}(\mathbb{Z})$. Par ailleurs,

$$\begin{aligned}(a,\dots,a)\,{}^tT^{-1} &= (0,\dots,0,a),\\ (b,\dots,b)\,T &= (0,\dots,0,nb) \in \mathrm{Mat}_{g,n}(\mathbb{Z}),\\ (z,\dots,z)\,T &= (0,\dots,0,nz).\end{aligned}$$

car b appartient à $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$.

Passons maintenant à la démonstration des équations 3.17 et 3.18. Pour cela, nous utilisons la formule de Koizumi avec la matrice $T = F^{-1}$.

$$d\left(\prod_{i=1}^{n}\theta\left[\begin{smallmatrix}\alpha_i-\alpha_{i+1}\\0\end{smallmatrix}\right](0,i(i+1)\Omega)\right)\theta\left[\begin{smallmatrix}\alpha_n+a\\0\end{smallmatrix}\right](nz,n\Omega) = \sum_{P_2\in MT/M}\exp\left(-2i\pi\,\mathrm{Tr}\left({}^tP_2J_1\right)\right)\Theta^{(n)}\left[\begin{smallmatrix}J_1\\P_2\end{smallmatrix}\right](Z\mid\Omega)$$

où $M = \mathrm{Mat}_{g,n}(\mathbb{Z})$ et d est le cardinal du groupe quotient $M\,{}^tT/M$. Nous avons

$$\begin{aligned} J_1 &:= (\alpha_1-\alpha_2,\ldots,\alpha_{n-1}-\alpha_n,\alpha_n+a)\;{}^tF \\ &= (\alpha_1+a,-\alpha_1+2\alpha_2+a,-2\alpha_2+3\alpha_3+a,\ldots,-(n-1)\alpha_{n-1}+n\alpha_n+a) \\ &\equiv (a,\ldots,a,a+n\alpha_n) \mod \mathbb{Z}^g \end{aligned}$$

où la dernière égalité est vraie si les α_i sont des éléments de $\frac{1}{i}\mathbb{Z}^g/\mathbb{Z}^g$ pour i compris entre 1 et $n-1$. Écrivons $P_2 = (p_1,\ldots,p_n)$ et remarquons que les conditions sur P_2 impliquent que

- np_n appartient à $\mathbb{Z}^g$,
- $i(p_i - p_{i+1})$ appartient à $\mathbb{Z}^g$ pour $1 \leqslant i \leqslant n-1$.

La trace se réécrit de la manière suivante

$$\mathrm{Tr}\left({}^tP_2J_1\right) = \sum_{i=1}^{n-1} i\,{}^t(p_i-p_{i+1})\,\alpha_i + {}^t(p_1+\ldots+p_n)\,a + n\,{}^tp_n\alpha_n.$$

Nous sommons maintenant la formule 3.19 sur les α_i comme dans la définition de T. Nous obtenons, après avoir permuté les sommes,

$$\begin{aligned} dT_{\alpha_n}(0,\Omega)\,\theta\left[\begin{smallmatrix}\alpha_n+a\\0\end{smallmatrix}\right](nz,n\Omega) = \sum_{P_2}\left(\sum_{\substack{\alpha_i\in\frac{1}{i}\mathbb{Z}^g/\mathbb{Z}^g\\1\leqslant i\leqslant n-1}}\exp\left(-2i\pi\sum_{i=1}^{n-1}i\,{}^t(p_i-p_{i+1})\right)\right) \\ \times\exp\left(-2i\pi\left({}^t(p_1+\ldots+p_n)\,a+n\,{}^tp_n\alpha_n\right)\right)\Theta^{(n)}\left[\begin{smallmatrix}J_1\\P_2\end{smallmatrix}\right](Z\mid\Omega). \end{aligned} \quad (3.19)$$

Cette équation est valide car les caractéristiques J_1 sont congrues modulo $\mathbb{Z}^g$ à la caractéristique a qui est indépendante des α_i. Le terme général de la somme est non nulle si les p_i sont tous égaux et nous notons $\beta \in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ la valeur commune. Supposons que α_n appartient à $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$, nous avons donc

$$n^gT_{\alpha_n}(0,\Omega)\,\theta\left[\begin{smallmatrix}\alpha_n+a\\0\end{smallmatrix}\right](nz,n\Omega) = \sum_{\beta\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}\exp\left(-2i\pi\left(n\,{}^t\beta a+n\,{}^t\beta\alpha_n\right)\right)\theta\left[\begin{smallmatrix}a\\\beta\end{smallmatrix}\right](z,\Omega)^n.$$

Un simple renomage sur a et α_n permet d'obtenir les formules voulues. □

Étude des thêta constantes

Soit $\mathscr{F}$ une famille génératrice de R_n^Ω. Par abus de langage nous parlons de thêta constantes de niveau n pour désigner le vecteur (projectif ou affine suivant les cas) de ces fonctions évaluées en 0. Ainsi, pour un élément b de $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$, la constante $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)^2$ est une thêta constante de niveau 2 (pour les familles $\mathscr{F}_{(2,1)^2}$ et $\mathscr{F}_{(2,2)^2}$) mais elle est aussi le carré d'une thêta constante de niveau 4 (pour la famille $\mathscr{F}_{(2,2)}$).

En remplaçant z par 0 dans les formules de changement de base, nous obtenons des relations liant les thêta constantes associées aux différentes familles.

Ainsi, les thêta constantes associées aux quatre premières familles s'expriment les unes en fonction des autres. Remarquons que les équations ne sont pas à coefficients rationnels : des racines n-ièmes de

l'unité apparaissent. C'est la seule obstruction : si nous supposons que les thêta constantes d'une famille sont définies sur un corps k de caractéristique différente de n et contenant les racines n-ièmes de l'unité, alors les thêta constantes des trois autres familles sont aussi définies sur k.

Il n'en est pas de même pour les deux dernières familles : partant des thêta constantes de $\mathscr{F}_n$, nous pouvons calculer celles de $\mathscr{F}_{(n,1)^2}$ et $\mathscr{F}_{(n,2)^2}$ mais l'inverse n'est pas vrai. Le cas de $\mathscr{F}_{(n,2)^2}$ est particulier car même s'il n'est pas possible d'obtenir exactement les thêta constantes de $\mathscr{F}_n$, nous les obtenons à un facteur projectif près.

La base $\mathscr{F}_{(n,1)^2}$ est le seul cas vraiment « problématique » en pratique. Il n'est pas possible d'obtenir les thêta constantes des autres familles à partir de celles de $\mathscr{F}_{(n,1)^2}$. Ainsi, les propositions 3.1.25 et 3.1.26 montreront qu'il existe différents choix de matrices $\Omega \in \mathcal{H}_g$ donnant les mêmes thêta constantes de $\mathscr{F}_{(n,1)^2}$ mais des thêta constantes de $\mathscr{F}_{(n,2)^2}$ différentes. Ces thêta constantes ne vivent pas sur le même corps : il faut prendre une extension de corps de degré 8 en général (4 pour les corps finis). Nous observerons également dans les paragraphes suivants, les conséquences sur la torsion de la variété

3.1.3 Liens avec les variétés abéliennes

Cas général

Le but de cette partie est de commenter l'assertion suivante : les fonctions thêta de niveau n fournissent un système de coordonnées projectives pour les variétés abéliennes principalement polarisées.
Rappelons que sur $\mathbb{C}$, toute variété abélienne principalement polarisée est isomorphe à un tore $\mathbb{C}^g/\Lambda_\Omega$. Cependant les fonctions thêta ne sont pas définies sur $\mathbb{C}^g/\Lambda_\Omega$ mais sur $\mathbb{C}^g$. La propriété 3.1.2 montre que toutes les fonctions de R_n^Ω évaluées en z diffèrent du même facteur que leur évaluation en $z+\lambda$ pour tout $\lambda \in \Lambda_\Omega$. Nous avons alors la propriété suivante dont une preuve se trouve dans [Mum70, p. 29].

Théorème 3.1.10 (Théorème de Lefschetz)**.** *Pour $n \geqslant 3$, une famille génératrice de k fonctions de niveau n fournissent un plongement de $\mathbb{C}^g/\Lambda_\Omega$ dans $\mathbb{P}^{k-1}(\mathbb{C})$.*
Pour $n = 2$, les fonctions de niveau 2 ne permettent de plonger que $\mathbb{C}^g/\Lambda_\Omega/\sim$ où $\sim$ est la relation d'équivalence telle que $z \sim -z$.

Cette propriété montre qu'il est possible d'utiliser des coordonnées thêta pour coder les informations d'une variété abélienne. Par ailleurs, c'est le seul système de coordonnées connu pour une variété abélienne générale (par exemple celles qui ne sont pas des jacobiennes de courbes).

Pour la dimension $g = 2$, l'image de la variété par les fonctions thêta de niveau 2 s'appelle surface de Kummer.

Les coordonnées de l'image du zéro de la variété abélienne (correspondant au vecteur 0 du tore $\mathbb{C}^g/\Lambda_\Omega$) par le plongement de niveau n sont les fonctions thêta de niveau n évaluées en 0 c'est-à-dire les thêta constantes.
De même, l'image des points de n-torsion se lit très facilement sur les thêta constantes de niveau n (sauf pour la base $\mathscr{F}_{(n,1)^2}$). Dans le tore $\mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$, ces points sont donnés par $\Omega\alpha + \beta$ où α et β sont des vecteurs de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$.

Propriété 3.1.11. *Soit $\Omega \in \mathcal{H}_g$ et soient α et β des vecteurs de $\frac{1}{n}\mathbb{Z}^g$. Nous avons alors les relations projectives suivantes : pour la base $\mathscr{F}'_n$,*

$$\left[\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](n(\Omega\alpha+\beta), n\Omega)\right]_{a\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}a+\alpha\\0\end{smallmatrix}\right](0, n\Omega)\exp\left(2i\pi n\,{}^t a\beta\right)\right]_{a\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g},$$

pour la base $\mathscr{F}_n$,

$$\left[\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\Omega\alpha+\beta, \frac{\Omega}{n}\right)\right]_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)\exp\left(-2i\pi n\,{}^t\alpha b\right)\right]_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g},$$

quand $n = k^2$, pour la base $\mathscr{F}_{(k,k)}$,

$$\left[\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](k(\Omega\alpha+\beta), \Omega)\right]_{a,b\in\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}a+k\alpha\\b+k\beta\end{smallmatrix}\right](0,\Omega)\exp\left(-2i\pi k\,{}^t\alpha b\right)\right]_{a,b\in\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g},$$

quand $2 \mid n$*, pour la base* $\mathscr{F}_{(n/2,2)}$*,*

$$\left[\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2\left(\Omega\alpha+\beta\right),\frac{4\Omega}{n}\right)\right]_{\substack{a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\\ b\in\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g}} = \left[\theta\left[\begin{smallmatrix}a+\frac{n}{2}\alpha\\ b+2\beta\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)\exp\left(-2i\pi\frac{n}{2}\,{}^t\alpha b\right)\right]_{\substack{a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\\ b\in\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g}},$$

quand $2 \mid n$*, pour la famille* $\mathscr{F}'_{(n,2)^2}$*,*

$$\left[\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(\Omega\alpha+\beta,\frac{\Omega}{n/2}\right)^2\right]_{\substack{a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\\ b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}} = \left[\theta\left[\begin{smallmatrix}a+\frac{n}{2}\alpha\\ b+\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n/2}\right)^2\exp\left(-2i\pi n\,{}^t\alpha b\right)\right]_{\substack{a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\\ b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}},$$

pour la famille $\mathscr{F}_{(n,n)^n}$*,*

$$\left[\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(\Omega\alpha+\beta,\Omega\right)^n\right]_{a,b\in\ b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}a+\alpha\\ b+\beta\end{smallmatrix}\right]\left(0,\Omega\right)^n\exp\left(-2i\pi n\,{}^t\alpha b\right)\right]_{a,b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Dans ces six cas, les coordonnées des points de n-torsion sont la permutation et la multiplication par une racine n-ième de l'unité des coordonnées du zéro de la variété données par les thêta constantes. Ainsi un point de n-torsion sur une variété abélienne vivra sur la plus petite extension de corps contenant ces thêta constantes et les racines n-ièmes de l'unité.

Pour des raisons arithmétiques nous supposerons que le niveau est pair, ce qui impose, pour ces familles, que tous les points de 2-torsion soient rationnels.

Pour la base $\mathscr{F}_{(n,1)^2}$, seule la $\frac{n}{2}$-torsion et une partie de la n-torsion s'expriment en fonction des thêta constantes : pour $\alpha \in \frac{1}{n/2}\mathbb{Z}^g$ et $\beta \in \frac{1}{n}\mathbb{Z}^g$,

$$\left[\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\Omega\alpha+\beta,\frac{\Omega}{n/2}\right)^2\right]_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}0\\ b+\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n/2}\right)^2\exp\left(-2i\pi n\,{}^t\alpha b\right)\right]_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Pour la base $\mathscr{F}_{(n,1)^n}$, seule la moitié de la n-torsion est rationnelle : pour $\beta \in \frac{1}{n}\mathbb{Z}^g$,

$$\left[\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta,\Omega\right)^n\right]_{b\in\ b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left[\theta\left[\begin{smallmatrix}0\\ b+\beta\end{smallmatrix}\right]\left(0,\Omega\right)^n\right]_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Dans le cas de corps de caractéristique non première avec le niveau, la n-torsion de la variété abélienne se comporte différemment du cas général 2.1.8. Au vu de la propriété 3.1.11 précédente, il est clair qu'il faut modifier les fonctions thêta si nous voulons travailler avec des variétés sur ces corps. On pourra consulter [Car06, Car09, GL09].

Supposons à partir de maintenant que le niveau n est pair. Nous voulons étudier l'image de la variété par le plongement. L'image de la variété abélienne est une variété algébrique de $\mathbb{P}^{n^g-1}(\mathbb{C})$ et doit donc être localement le lieu des zéros d'un système polynomial. La formule de Koizumi 3.5 implique de nombreuses relations entre les fonctions thêta. En particulier,

Propriété 3.1.12 (Équations de Riemann généralisées)**.** *Soit* $\Omega \in \mathcal{H}_g$ *et soient* $z_1, \dots, z_4$ *quatre vecteurs de* $\mathbb{C}^g$*. Posons* $2z = z_1 + z_2 + z_3 + z_4$ *et* $z'_i = z - z_i$*.*
Soient $b_1, \dots, b_4$ *dans* $\frac{1}{n}\mathbb{Z}^g$*, posons* $2b = b_1 + b_2 + b_3 + b_4$ *et supposons que* b *appartienne aussi à* $\frac{1}{n}\mathbb{Z}^g$*. Posons alors* $b'_i = b - b_i \in \frac{1}{n}\mathbb{Z}^g$*.*
Pour tout caractère χ *sur* $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ *(on peut poser* $\chi(\beta) = (-1)^{4\,{}^t\alpha\beta}$ *avec* $\alpha \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$*), nous avons*

$$\begin{aligned}&\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\ b_1+\beta\end{smallmatrix}\right](z_1)\,\theta\left[\begin{smallmatrix}0\\ b_2+\beta\end{smallmatrix}\right](z_2)\right)\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\ b_3+\beta\end{smallmatrix}\right](z_3)\,\theta\left[\begin{smallmatrix}0\\ b_4+\beta\end{smallmatrix}\right](z_4)\right)\\ &=\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\ b'_1+\beta\end{smallmatrix}\right](z'_1)\,\theta\left[\begin{smallmatrix}0\\ b'_2+\beta\end{smallmatrix}\right](z'_2)\right)\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\ b'_3+\beta\end{smallmatrix}\right](z'_3)\,\theta\left[\begin{smallmatrix}0\\ b'_4+\beta\end{smallmatrix}\right](z'_4)\right)\end{aligned}\tag{3.20}$$

où les fonctions thêta correspondent à la matrice Ω/n du demi-espace de Siegel. De même, supposons que $n = k^2$ avec k pair. Posons,

$$T = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Soit Z dans $\mathrm{Mat}_{g,4}(\mathbb{C})$. Pour tout a, b dans $\mathrm{Mat}_{g,4}\left(\frac{1}{k}\mathbb{Z}^g\right)$ tels que aT et bT appartiennent à $\mathrm{Mat}_{g,4}\left(\frac{1}{k}\mathbb{Z}^g\right)$, nous avons

$$2^g \prod_{i=1}^{4} \theta\left[\begin{smallmatrix} a^{(i)} \\ b^{(i)} \end{smallmatrix}\right]\left(Z^{(i)}, \Omega\right) = \sum_{\alpha,\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \exp\left(-4\pi i\, {}^t\beta a^{(1)}\right) \prod_{i=1}^{4} \theta\left[\begin{smallmatrix} (aT)^{(i)}+\alpha \\ (bT)^{(i)}+\beta \end{smallmatrix}\right]\left((ZT)^{(i)}, \Omega\right). \tag{3.21}$$

Quand $4 \mid n$, la formule de Riemann généralisée s'écrit de manière plus simple avec la base $\mathscr{F}_{(n/2,2)}$: pour tout a dans $\mathrm{Mat}_{g,4}\left(\frac{1}{2}\mathbb{Z}^g\right)$ tel que aT appartienne à $\mathrm{Mat}_{g,4}\left(\frac{1}{2}\mathbb{Z}^g\right)$ et pour tout b dans $\mathrm{Mat}_{g,4}\left(\frac{1}{n/2}\mathbb{Z}^g\right)$ tel que aT appartienne à $\mathrm{Mat}_{g,4}\left(\frac{1}{n/2}\mathbb{Z}^g\right)$,

$$2^g \prod_{i=1}^{4} \theta\left[\begin{smallmatrix} a^{(i)} \\ b^{(i)} \end{smallmatrix}\right]\left(2Z^{(i)}, \frac{4\Omega}{n}\right) = \sum_{\alpha,\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \exp\left(-4\pi i\, {}^t\beta a^{(1)}\right) \prod_{i=1}^{4} \theta\left[\begin{smallmatrix} (aT)^{(i)}+\alpha \\ (bT)^{(i)}+\beta \end{smallmatrix}\right]\left(2\,(ZT)^{(i)}, \frac{4\Omega}{n}\right). \tag{3.22}$$

Notons que les formules sont toujours valides avec a et b dans $\mathbb{Q}^g$ mais, dans ce cas, les fonctions qui apparaissent n'appartiennent plus aux bases $\mathscr{F}$ considérées.

Démonstration. Les équations 3.21 et 3.22 s'obtiennent directement à partir de la formule de Koizumi avec la matrice T donnée. Pour obtenir la formule 3.20 il faut utiliser les formules de changements de base page 38 (pour ce faire il faut avoir montré les formules précédentes avec a et b dans $\mathbb{Q}^g$). □

En spécialisant les équations précédentes avec $z_1 = -z_2 = z$ et $z_3 = z_4 = 0$ nous obtenons les équations de Riemann classiques (on ferra attention aux signes devant b_2 et B_1 dans les formules suivantes) :

Propriété 3.1.13 (Équations de Riemann)**.** *Soit $\Omega \in \mathcal{H}_g$, et soit $z \in \mathbb{C}^g$.*
Soient $b_1, \ldots, b_4$ dans $\frac{1}{n}\mathbb{Z}^g$, posons $2b = b_1 + b_2 + b_3 + b_4$ et supposons que b appartienne aussi à $\frac{1}{n}\mathbb{Z}^g$. Posons alors $b_i' = b - b_i$. Pour tout caractère χ sur $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\left(\sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \chi(\beta)\theta\left[\begin{smallmatrix} 0 \\ b_1+\beta \end{smallmatrix}\right](z)\,\theta\left[\begin{smallmatrix} 0 \\ -b_2+\beta \end{smallmatrix}\right](z)\right)\left(\sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \chi(\beta)\theta\left[\begin{smallmatrix} 0 \\ b_3+\beta \end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix} 0 \\ b_4+\beta \end{smallmatrix}\right](0)\right)$$

$$= \left(\sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \chi(\beta)\theta\left[\begin{smallmatrix} 0 \\ -b_1'+\beta \end{smallmatrix}\right](z)\,\theta\left[\begin{smallmatrix} 0 \\ b_2'+\beta \end{smallmatrix}\right](z)\right)\left(\sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \chi(\beta)\theta\left[\begin{smallmatrix} 0 \\ b_3'+\beta \end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix} 0 \\ b_4'+\beta \end{smallmatrix}\right](0)\right)$$

où les fonction thêta correspondent à la matrice Ω/n du demi-espace de Siegel.

Théorème 3.1.14. *Pour $n \geqslant 4$, les équations de Riemann définissent l'image du plongement par les fonctions thêta de $\mathscr{F}_n$ de la variété abélienne dans $\mathbb{P}^{n^g-1}(\mathbb{C})$.*

Ce théorème est prouvé dans Mumford [Mum69, théorème 10]. En spécialisant encore plus avec $z = 0$ nous obtenons des relations entre les thêta constantes :

Propriété 3.1.15. *Pour $2 \mid n$, les thêta constantes de la famille $\mathscr{F}_n$ vérifient les relations de Riemann : avec les notations précédentes,*

$$\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\b_1+\beta\end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix}0\\b_2+\beta\end{smallmatrix}\right](0)\right)\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\b_3+\beta\end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix}0\\b_4+\beta\end{smallmatrix}\right](0)\right)$$

$$=\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\b-b_1+\beta\end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix}0\\b-b_2+\beta\end{smallmatrix}\right](0)\right)\left(\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\chi(\beta)\theta\left[\begin{smallmatrix}0\\b-b_3+\beta\end{smallmatrix}\right](0)\,\theta\left[\begin{smallmatrix}0\\b-_4+\beta\end{smallmatrix}\right](0)\right)$$

où les fonction thêta correspondent à la matrice Ω/n du demi-espace de Siegel. Les thêta constantes vérifient aussi les relations de symétries : pour tout $b \in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$:

$$\theta\left[\begin{smallmatrix}0\\-b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)=\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right).$$

Réciproquement, étant donnés n^g éléments vérifiant les relations précédentes, existe-t'il une variété abélienne principalement polarisée dont ces éléments sont les thêta constantes ? Nous avons le résultat suivant qui répond partiellement à la question

Théorème 3.1.16. *Pour $n > 4$ pair, soit $\overline{\mathscr{M}_n}$ la variété projective définie par les équations de la propriété 3.1.15 précédente et soit $\mathscr{M}_n$ le sous-ensemble de $\overline{\mathscr{M}_n}$ correspondant aux thêta constantes d'une variété abélienne. Alors $\mathscr{M}_n$ est un ouvert de $\overline{\mathscr{M}_n}$.*

Mumford [Mum66] avait conjecturé ce théorème pour $n \geqslant 4$. Pour n divisible pas 8, ce résultat a été prouvé dans [Mum67a] et Kempf [Kem89, théorème 28 p. 92] a étendu la preuve au cas $n > 4$ pair.
En pratique on prendra des « thêta constantes » vérifiant les relations 3.1.15, on définira alors la variété par les équations de Riemann 3.1.13. Les formules d'additions (qui permettent de prouver que la variété algébrique est abélienne) sont données par les formules de Riemann généralisées (proposition 3.1.12, voir aussi la partie 3.2). Étant donné des « thêta constantes » vérifiant les relations 3.1.15, vérifier que nous avons bien obtenu un élément de $\mathscr{M}_n$, n'est pas trivial. Lubicz travaille sur ce sujet dans le but d'obtenir un algorithme certifiant que les « thêta constantes » sont bien un élément de $\mathscr{M}_n$.

Cette discussion montre qu'il est important d'avoir des théorèmes valides sur d'autres corps que $\mathbb{C}$. Ici nous ne pouvons pas utiliser le principe de Lefschetz et la théorie de la réduction car des relations pourraient exister sur $\mathbb{F}_p$ qui n'existent pas sur $\mathbb{C}$. Par ailleurs les variétés abéliennes principalement polarisées pourraient ne pas être toutes « représentables » par des fonctions thêta.

Dans le cas particulier où la variété abélienne est la jacobienne d'une courbe hyperelliptique, nous avons des propriétés plus précises.

3.1.4 Liens avec les courbes hyperelliptiques

Soit $\mathcal{C} : y^2 = f(x)$ une courbe hyperelliptique sur $\mathbb{C}$, nous avons décrit à la section 2.3.3 comment construire l'application $\mathfrak{u}$ d'Abel-Jacobi et obtenir une matrice Ω de $\mathcal{H}_g$ associée à la courbe. La jacobienne $\mathrm{Jac}(\mathcal{C})$ est isomorphe au tore $\mathbb{C}^g/\Lambda_\Omega$ et se plonge donc dans $\mathbb{P}^{n^g-1}(\mathbb{C})$ à l'aide des fonctions thêta de niveau n.

Nous nous intéressons maintenant aux fonctions thêta de niveau $(2,2)$. D'après la propriété 3.1.2, certaines fonctions thêta sont impaires et les thêta constantes associées sont donc nulles. Dans le cas où la matrice Ω provient d'une courbe hyperelliptique, ce ne sont pas les seules. Avec les notations de la section 2.3.3,

Théorème 3.1.17. *Soit Ω une matrice de $\mathcal{H}_g$ correspondant à une courbe hyperelliptique. Alors,*

$$\forall S \subset \{1,\dots,2g+1\},\qquad \#S \notin \{g, g+1\} \Longleftrightarrow \theta\left[\eta_{\mathcal{U}\circ S}\right](0,\Omega) = 0.$$

Cette propriété caractérise les variétés abéliennes principalement polarisées qui sont la jacobienne d'une courbe hyperelliptique.

Ce théorème a été prouvé par Mumford [Mum84, corollaire III.a.6.7]. Une autre preuve a été donnée par Poor [Poo94]. Ce théorème montre en particulier que pour une courbe hyperelliptique, les thêta constantes $\theta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](0,\Omega)$ et $\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](0,\Omega)$ ne sont pas nulles.

Plus généralement il est intéressant de savoir distinguer quand une variété abélienne est la jacobienne d'une courbe : c'est le « problème de Schottky ». À ce sujet on pourra consulter [Deb94, Gru10]. Ce problème a été résolu pour la dimension 4 (premier cas où il existe des variétés abéliennes non jacobiennes de courbes) par Schottky [Sch88] et Schottky et Jung [SJ09]

Dans le cas des courbes hyperelliptiques, le théorème 3.1.17 permet de simplifier les relations de Riemann.

Propriété 3.1.18 (Relations de Frobenius)**.** *Soient z_1, z_2, z_3, z_4 quatre vecteurs de $\mathbb{C}^g$ tels que $\sum_i z_i = 0$. Soient c_1, c_2, c_3, c_4 des vecteurs de $\mathbb{R}^{2g}$, alors*

$$0 = \sum_{j\in\{1,\dots,2g+1\}\cup\{\infty\}} (-1)^{\delta_{\mathcal{U}}(j)} \prod_{i=1}^{4} \theta\left[c_i+\eta_j\right](z_i)$$

où $\delta_{\mathcal{U}}$ est la fonction caractéristique de $\mathcal{U}$ c'est-à-dire que $\delta_{\mathcal{U}}(j)$ est égal à 1 si et seulement si j appartient à l'ensemble $\{1,3,\dots,2g+1\}$ des indices impairs.

Comme les équations de Riemann (théorème 3.1.14), les relations de Frobenius engendrent l'idéal des relations de la variété abélienne.

Une fois que nous avons reconnu qu'une variété abélienne est la jacobienne d'une courbe, nous pouvons essayer d'avoir des formules exprimant les paramètres de la courbe en fonction des thêta constantes et inversement. Dans le cas des courbes hyperelliptiques, nous avons les deux théorèmes suivants :

Théorème 3.1.19 (Thomae)**.** *Soit $\mathcal{C}$: $y^2 = \prod_{i=1}^{2g+1}(x-a_i)$, une courbe hyperelliptique de genre g et soit S un sous-ensemble de $\{1,\dots,2g+1\}$, alors*

$$\theta\left[\eta_{\mathcal{U}\circ S}\right]^4 = \begin{cases} c\prod_{\substack{i<j\\ i,j\in S}}(a_i-a_j)\prod_{\substack{i<j\\ i,j\notin S}}(a_i-a_j) & \text{si } \#S\in\{g,g+1\},\\ 0 & \text{sinon.}\end{cases}$$

De plus la constante c est donnée par $c=\epsilon/\det(\sigma)^2$ où ϵ appartient à $\{\pm1\}$ et σ est la matrice telle que

$$\omega_i = \frac{1}{2\pi i}\frac{\sum_{j=1}^{g}\sigma_{i,j}x^{j-1}\,\mathrm{d}\,x}{y}$$

et ω_i est la i-ième différentielle utilisée dans la construction de l'application d'Abel-Jacobi 2.3.11. En particulier,

$$\left(\frac{\theta\left[\eta_{\mathcal{U}\circ S}\right]}{\theta[0]}\right)^4 = \begin{cases} (-1)^{\#(\mathcal{U}\setminus S)}\dfrac{\prod_{\substack{i\in\mathcal{U}\\ j\notin\mathcal{U}}}(a_i-a_j)}{\prod_{\substack{i\in S\\ j\notin S}}(a_i-a_j)} & \text{si } \#S\in\{g,g+1\},\\ 0 & \text{sinon.}\end{cases}$$

La preuve de ce théorème est due à Thomae [Tho70] sur des idées remontant à Riemann [Rie57] (on pourra consulter la traduction de Laugel de ce dernier article [Lau98]). Dans le cas particulier où l'on ne souhaite pas calculer la constante c, on pourra consulter [Zar28, EF08]. Nous redonnerons la preuve au chapitre 6. Une réciproque aux formules de Thomae est donnée par

Théorème 3.1.20. *Soit i, j, k trois entiers distincts de $\{1,\dots,2g+1\}$. Pour tout sous-ensemble V de $\{1,\dots,2g+1\}\setminus\{k\}$ de cardinal $g+1$ et contenant i, j, nous avons*

$$\frac{a_k-a_j}{a_k-a_i} = (-1)^{4\,{}^t\eta'_k(\eta''_i+\eta''_j)}\,\frac{\theta\left[\eta_{\mathcal{U}\circ V\circ\{j\}}\right](0,\Omega)^2\,\theta\left[\eta_{\mathcal{U}\circ V\circ\{i,k\}}\right](0,\Omega)^2}{\theta\left[\eta_{\mathcal{U}\circ V\circ\{i\}}\right](0,\Omega)^2\,\theta\left[\eta_{\mathcal{U}\circ V\circ\{j,k\}}\right](0,\Omega)^2}.$$

Le cas du genre 2 avait été traité par Rosenhain [Ros95] qui supposait de plus que $a_1 = 0$, $a_2 = 1$. Umemura dans [Mum84, IIIc] donne une version non simplifiée de ce théorème. Différentes preuves de ce théorème se trouvent dans les articles [Tak96, Koi97, vW98]. La formule d'Umemura comme celle du théorème permet d'exprimer les racines d'un polynôme $f(x) \in \mathbb{C}[x]$ par les thêta constantes associées à la courbe d'équation $y^2 = f(x)$.

Quand le tore $\mathbb{C}^g/\Lambda_\Omega$ provient d'une courbe hyperelliptique $\mathcal{C}$ via l'application d'Abel-Jacobi, nous avons des informations supplémentaires sur les fonctions thêta considérées comme fonctions de la surface de Riemann $\mathcal{C}$ dans $\mathbb{C}^g$ [FK80].

Propriété 3.1.21. *Soit $e \in \mathbb{C}^g$, les assertions suivantes sont équivalentes :*
- $\theta(e) = 0$
- $e \in \Theta + \mathcal{K} \bmod \Lambda_\Omega$

où Θ est le diviseur thêta 2.2.2, et $\mathcal{K}$ est la constante de Riemann 2.3.16.

Bien que la fonction thêta de Riemann ne soit pas définie sur $\mathbb{C}^g/\Lambda_\Omega$, son diviseur des zéros y est bien défini. Nous pouvons alors reformuler la proposition précédente pour les fonctions thêta de niveau 2.

Propriété 3.1.22. *Soit $\mathfrak{u}$ l'application d'Abel-Jacobi. Le diviseur des zéros de la fonction (multivaluée)*

$$\begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathbb{C} \\ D & \longmapsto & \theta[\eta_{\mathcal{U}}](\mathfrak{u}(D)) \end{array}$$

est le diviseur Θ (ensemble des diviseurs de poids strictement inférieur à g). Soit E un élément de $\mathrm{Jac}(\mathcal{C})$, la fonction

$$\begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathbb{C} \\ D & \longmapsto & \theta\left[\eta_{\mathcal{U}} + \begin{array}{c} \mathfrak{u}(E)' \\ \mathfrak{u}(E)'' \end{array}\right](\mathfrak{u}(D)) \end{array}$$

a pour diviseur des zéros $\mathrm{T}_{-E}\,\Theta$ où pour tout diviseur D, l'opérateur T_D est la translation par D.

En particulier, soit un sous-groupe S de $\{1, \ldots, 2g+1\} \cup \{\infty\}$, le translaté $\mathrm{T}_{\sum_{l\in S} a_l - sP_\infty}\,\Theta$ est le diviseur des zéros de la fonction $D \mapsto \theta\left[\eta_{\mathcal{U}\circ S}\right](\mathfrak{u}(D))$.

Propriété 3.1.23. *La fonction (multivaluée)*

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathbb{C} \\ P & \longmapsto & \theta(\mathfrak{u}(P) - e) \end{array}$$

est soit identiquement nulle, soit a g zéros $P_1, \ldots, P_g$ qui vérifient

$$e \equiv \mathfrak{u}(P_1 + \ldots + P_g) + \mathcal{K} \mod \Lambda_\Omega.$$

3.1.5 Action du groupe symplectique

Comme il existe plusieurs matrices Ω associées à la même variété abélienne, il existe plusieurs plongements différents de cette variété avec les fonctions thêta. D'après la propriété 2.3.7, les isomorphismes entre deux tores proviennent d'une action de $\mathrm{Sp}(2g, \mathbb{Z})$ sur $\mathbb{C}^g \times \mathcal{H}_g$. Examinons comment cette action se traduit sur le plongement donné par les fonctions thêta de niveau n.

Rappelons que si M est une matrice, nous avons noté $\mathrm{diag}\,(M)$ le vecteur (colonne) des termes diagonaux de M.

Propriété 3.1.24. *Soit une matrice γ de $\mathrm{Sp}(2g, \mathbb{Z})$ donnée par*

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

Posons

$$e' = \frac{1}{2}\,\mathrm{diag}\left({}^tAC\right), \qquad e'' = \frac{1}{2}\,\mathrm{diag}\left({}^tDB\right)$$

Alors pour tous vecteurs a, b de $\mathbb{R}^g$, tout vecteur z de $\mathbb{C}^g$ et toute matrice Ω de $\mathcal{H}_g$, nous avons

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\gamma.z,\gamma.\Omega) &= \zeta_\gamma\sqrt{\det(C\Omega+D)}\exp\left(\pi i\,{}^tz\left(C\Omega+D\right)^{-1}Cz\right)\theta\left[{}^t\gamma\begin{pmatrix}a\\b\end{pmatrix}+\begin{pmatrix}e'\\e''\end{pmatrix}\right](z,\Omega)\\ &\quad \exp\left(-\pi i\,{}^taA\,{}^tBa\right)\exp\left(-\pi i\,{}^tbC\,{}^tDb\right)\exp\left(-2\pi i\,{}^taB\,{}^tCb\right)\\ &\quad \exp\left(-2\pi i\,{}^t\left({}^tAa+\,{}^tCb+e'\right)e''\right)\end{aligned}$$

où ζ_γ est une racine 8-ième de l'unité dépendant uniquement de γ. Si la matrice γ est un élément de Γ_4 alors nous avons de plus que $\zeta_\gamma=\pm1$.
Si γ appartient à $\Gamma_{1,2}$ l'équation précédente se simplifie en

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\gamma.z,\gamma.\Omega) &= \zeta_\gamma\sqrt{\det(C\Omega+D)}\exp\left(\pi i\,{}^tz\left(C\Omega+D\right)^{-1}Cz\right)\theta\left[{}^t\gamma\begin{pmatrix}a\\b\end{pmatrix}\right](z,\Omega)\\ &\quad \exp\left(-\pi i\,{}^taA\,{}^tBa\right)\exp\left(-\pi i\,{}^tbC\,{}^tDb\right)\exp\left(-2\pi i\,{}^taB\,{}^tCb\right).\end{aligned}$$

Si de plus $z=0$,

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\gamma.\Omega) &= \zeta_\gamma\sqrt{\det(C\Omega+D)}\theta\left[{}^t\gamma\begin{pmatrix}a\\b\end{pmatrix}\right](0,\Omega)\\ &\quad \exp\left(-\pi i\,{}^taA\,{}^tBa\right)\exp\left(-\pi i\,{}^tbC\,{}^tDb\right)\exp\left(-2\pi i\,{}^taB\,{}^tCb\right)\end{aligned}$$

et donc $\Omega\to\theta\left(0,\Omega\right)^2$ est une forme modulaire de Siegel de poids 1 et de niveau Γ_4 [Kli90, Mum83].

Démonstration. Cette propriété a été démontrée par Igusa [Igu72, théorème 2 chapitre 5]. Il faut cependant faire attention au fait que Igusa considère les caractéristiques comme des vecteurs horizontaux et que ses actions sont à droite.
Mumford [Mum83, chapitre II.5] a prouvé le cas particulier de $\Gamma_{1,2}$. On peut s'inspirer de cette dernière preuve pour montrer la formule dans le cas général. Commençons par remarquer que la formule principale découle de la formule suivante

$$\begin{aligned}\theta\left(\gamma.y,\gamma.\Omega\right) &= \zeta_\gamma\sqrt{\det(C\Omega+D)}\exp\left(\pi i\,{}^ty\left(C\Omega+D\right)^{-1}Cy\right)\theta(y-\Omega e'+e'',\Omega)\\ &\quad \exp\left(\pi i\,{}^te'\Omega e'\right)\exp\left(-2\pi i\,{}^te'y\right)\end{aligned}$$

où il suffit de poser $y=z+\gamma^{-1}.{}_{\gamma.\Omega}\left((\gamma.\Omega)a+b\right)$ (rappelons que l'action de $\mathrm{Sp}(2g,\mathbb{Z})$ sur $\mathbb{C}^g$ a été définie dans la propriété 2.3.7 et qu'elle dépend d'une matrice de $\mathcal{H}_g$).
Pour prouver cette dernière formule on procède en plusieurs étapes :

- On montre que si cette formule est vraie pour γ_1 et γ_2 dans $\mathrm{Sp}(2g,\mathbb{Z})$, elle est vraie pour $\gamma_1\gamma_2$. Cette étape est très calculatoire.
- On démontre la formule pour les générateurs de $\mathrm{Sp}(2g,\mathbb{Z})$.

De manière plus précise,

- pour $\gamma=\begin{pmatrix}\mathrm{Id}&B\\0&\mathrm{Id}\end{pmatrix}$, en considérant la définition de la fonction thêta comme somme d'exponentielles, on a $\theta\left(\gamma.z,\gamma.\Omega\right)=\theta(z+e'',\Omega)$.
- Pour $\gamma=\begin{pmatrix}A&0\\0&{}^tA^{-1}\end{pmatrix}$, de la même manière, on obtient $\theta\left(\gamma.z,\gamma.\Omega\right)=\theta(z,\Omega)$. Or $\det({}^tA^{-1})=1$ et donc on pose $\zeta_\gamma=\sqrt{\det({}^tA^{-1})}\in\{\pm1\}$.
- Pour $\gamma=\begin{pmatrix}0&\mathrm{Id}\\-\mathrm{Id}&0\end{pmatrix}$, une des méthodes consiste à utiliser la formule de Poisson. Le calcul est fait dans [Mum83, II.5].

□

Nous pouvons maintenant étudier l'action de $\mathrm{Sp}(2g,\mathbb{Z})$ sur les thêta constantes de niveau n. En particulier, nous nous intéressons aux stabilisateurs des thêta constantes de niveau n : nous fixons une base, et nous nous intéressons aux matrices de $\mathrm{Sp}(2g,\mathbb{Z})$ qui fixent projectivement les thêta constantes de

cette base. Dans les chapitres suivants, nous nous autoriserons à prendre des isomorphismes préservant certaines propriétés des thêta constantes. Les propositions suivantes seront utilisées pour caractériser les éléments de $\mathrm{Sp}(2g,\mathbb{Z})$ correspondant aux isomorphismes qui nous intéresseront.

Propriété 3.1.25. *Pour chacun des vecteurs projectifs de thêta constantes suivants*

$$\begin{array}{lllll}
 & \mathscr{F}'_n & : & \left(\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,n\Omega)\right)_a & \text{où } a\in \mathrm{Rpr}\left(\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right),\\
 & \mathscr{F}_n & : & \left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)\right)_b & \text{où } b\in \mathrm{Rpr}\left(\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right),\\
\textit{quand } n=k^2, & \mathscr{F}_{(k,k)} & : & \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)\right)_{a,b} & \text{où } a,b\in \mathrm{Rpr}\left(\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g\right),\\
\textit{quand } 2\mid n, & \mathscr{F}_{(n/2,2)} & : & \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)\right)_{a,b} & \text{où } a\in \mathrm{Rpr}\left(\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right),\ b\in \mathrm{Rpr}\left(\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g\right),\\
\textit{quand } 2\mid n, & \mathscr{F}_{(n,2)^2} & : & \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n/2}\right)^2\right)_{a,b} & \text{où } a\in \mathrm{Rpr}\left(\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right),\ b\in \mathrm{Rpr}\left(\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right),\\
 & \mathscr{F}_{(n,n)^n} & : & \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)^n\right)_{a,b} & \text{où } a,b\in \mathrm{Rpr}\left(\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right),
\end{array}$$

le stabilisateur du vecteur est l'ensemble $\tilde{\Gamma}_{n,2n}$.

Démonstration. Traitons le cas de la famille $\mathscr{F}_n$. L'image de la n torsion est déterminée par les valeurs des thêta constantes de la famille $\mathscr{F}_n$. Une matrice γ fixant ces thêta constantes détermine donc l'image de la n torsion et donc les points de n-torsion modulo les automorphismes du tore. Pour des matrices Ω génériques, le seul automorphisme du tore $\mathbb{C}^g/\Lambda_\Omega$ est l'involution $z\mapsto -z$ et donc γ doit appartenir à $\tilde{\Gamma}_n$. Posons

$$\gamma=\begin{pmatrix} A & B\\ C & D\end{pmatrix}\in\tilde{\Gamma}_n,\qquad \gamma'=\begin{pmatrix} A & B/n\\ nC & D\end{pmatrix}.$$

On vérifie que γ' appartient bien à $\mathrm{Sp}(2g,\mathbb{Z})$. Nous avons alors

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}=\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\gamma'.\left(\frac{\Omega}{n}\right)\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\gamma'.\left(\frac{\Omega}{n}\right)\right)},$$

et en appliquant la formule 3.1.24, nous obtenons

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}=\frac{\theta\left[\begin{smallmatrix}n\,{}^tCb+e'\\ {}^tDb+e''\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}e'\\e''\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}\exp\left(-n\pi i\,{}^tbC\,{}^tDb\right)\exp\left(-2n\pi i\,{}^tbCe''\right)$$

où

$$e'=\frac{n}{2}\operatorname{diag}\left({}^tAC\right),\qquad e''=\frac{1}{2n}\operatorname{diag}\left({}^tDB\right).$$

Comme γ appartient à $\tilde{\Gamma}_n$ et b appartient à $\frac{1}{n}\mathbb{Z}^g$, nous avons les relations

$$n\,{}^tCb\equiv 0 \bmod 1,\qquad {}^tDb\equiv\pm b \bmod 1.$$

De plus, n est pair, nous avons également les relations

$$e'\equiv 0 \bmod 1,\qquad {}^tCe''=\frac{{}^tC}{2}\operatorname{diag}\left(\frac{{}^tDB}{n}\right)\equiv 0 \bmod 1$$

donc

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}=\frac{\theta\left[\begin{smallmatrix}0\\\pm b+e''\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\e''\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}\exp\left(-n\pi i\,{}^tbC\,{}^tDb\right)$$

En examinant les caractéristiques des thêta constantes, nous devons avoir que e'' appartient à $\mathbb{Z}^g$, c'est-à-dire que $\operatorname{diag}\left({}^tDB\right)$ doit être congru à 0 modulo $2n$. Quant à lui, le facteur exponentiel doit être égal

à 1 ce qui implique que la matrice $C\,{}^tD$ (qui est symétrique) soit congru à 0 modulo n et que sa diagonale le soit modulo $2n$. Nous avons donc

$$\operatorname{diag}\left({}^tAC\right) \equiv \operatorname{diag}\left(\pm C\right) \equiv \operatorname{diag}\left(C\,{}^tD\right) \equiv 0 \mod 2n$$

Nous obtenons que γ appartient à $\tilde{\Gamma}_{n,2n}$ et

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{n}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\\pm b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)}.$$

Donc dans le cas où n est pair, nous avons montré que $\tilde{\Gamma}_{n,2n}$ est bien le stabilisateur des thêta constantes de la famille $\mathscr{F}_n$. Les cas n impair et ceux correspondant aux autres familles se traitent de la même façon. □

Propriété 3.1.26. *L'ensemble*

$$\left\{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad \begin{array}{l} C \equiv 0 \bmod 2, \quad A \equiv D \equiv \mathrm{Id} \bmod 2, \\ \operatorname{diag}\left({}^tDB\right) \equiv 0 \bmod 2, \quad \operatorname{diag}\left({}^tAC\right) \equiv 0 \bmod 4 \end{array}\right\}$$

est le stabilisateur du vecteur projectif de thêta constantes

$$\mathscr{F}_{(2,1)^2} : \quad \left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)^2\right)_b \quad \textit{où } b \in \operatorname{Rpr}\left(\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right).$$

Démonstration. Soit $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ une matrice de $\mathrm{Sp}(2g,\mathbb{Z})$ fixant le vecteur. En examinant les caractéristiques, γ doit appartenir à $\Gamma_{1,2}$. Nous avons alors

$$\left(\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)}\right)^2 = \left(\frac{\theta\left[\begin{smallmatrix}{}^tCb\\{}^tDb\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\right)^2 \exp\left(-2\pi i\,{}^tbC\,{}^tDb\right).$$

Pour que cette valeur soit égale à

$$\left(\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\right)^2,$$

nous devons avoir

$$C \equiv 0 \mod 2, \qquad D \equiv \mathrm{Id} \mod 2, \qquad \operatorname{diag}\left(C\,{}^tD\right) \equiv 0 \mod 4.$$

Ces conditions impliquent que γ appartient bien à l'ensemble voulu. Réciproquement, il est clair qu'une matrice de cet ensemble laisse fixes les thêta constantes de $\mathscr{F}_{(2,1)^2}$. □

Remarquons la différence entre la propriété 3.1.25 et la propriété 3.1.26 : l'indice des stabilisateurs est $2^{\frac{g(g+1)}{2}}$ et il est engendré par les matrices :

$$\begin{pmatrix} \mathrm{Id} & E_{i,j}+E_{j,i} \\ 0 & \mathrm{Id} \end{pmatrix} \quad \text{pour } i,j \in \{1,\ldots,g\}.$$

Au niveau de la 2-torsion du tore $\mathbb{C}^g/\Lambda_\Omega$, le stabilisateur des thêta constantes $\mathscr{F}_{(2,1)^2}$ ne laisse fixes que les points $\{\beta, \beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\}$ tandis que Γ_2 qui est contenu dans le stabilisateur des autres familles laisse fixes tous les points de 2-torsion.

Propriété 3.1.27. *L'ensemble*

$$\left\{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad \begin{array}{l} C \equiv 0 \bmod n, \quad A \equiv D \equiv \pm\mathrm{Id} \bmod n, \\ \operatorname{diag}\left({}^tDB\right) \equiv 0 \bmod 2, \quad \operatorname{diag}\left({}^tAC\right) \equiv 0 \bmod 2n \end{array}\right\}$$

est le stabilisateur du vecteur projectifs de thêta constantes

$$\mathscr{F}_{(n,1)^n} : \quad \left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)^n\right)_b \quad \textit{où } b \in \operatorname{Rpr}\left(\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g\right).$$

Nous ne faisons pas la démonstration qui est similaire aux précédentes. Remarquons que la base $\mathscr{F}_{(n,1)^n}$ a un stabilisateur beaucoup plus petit que les autres bases. Explicitons maintenant l'action de $\mathrm{Sp}(2g,\mathbb{Z})$ sur les fonctions thêta de niveau $(2,2)$ ce qui nous sera utile dans la partie 6.2.

Lemme 3.1.28. *Soient a,b dans* $\frac{1}{2}\mathbb{Z}^g$ *et soit* $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *une matrice de* Γ_2*, alors*

$$\begin{aligned}
\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)} &= \frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)} \exp\left(\pi i\, {}^t a A\, {}^t B a\right) \exp\left(-\pi i\, {}^t b C\, {}^t D b\right) \exp\left(-2\pi i\, {}^t a\,(A-\mathrm{Id})\, b\right), \\
\left(\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)}\right)^2 &= \left(\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\right)^2 (-1)^{2\,{}^t a A\, {}^t B a} (-1)^{2\,{}^t b C\, {}^t D b}, \\
\left(\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)}\right)^4 &= \left(\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\right)^4.
\end{aligned}$$

Finalement, pour les fonctions thêta, nous avons la propriété

Propriété 3.1.29. *Soit A une variété abélienne sur* $\mathbb{C}$*. Un de ses plongements par les fonctions thêta de niveau n est entièrement déterminé (à l'involution* $z \mapsto -z$ *près) par les thêta constantes.*

Ce théorème est cohérent avec les équations de Riemann 3.1.13 qui définissent la variété à automorphisme près et qui ne dépendent que des thêta constantes de la famille considérée.

Démonstration. Faisons la preuve pour la famille $\mathscr{F}_n$. Une matrice γ fixant les thêta constantes de cette famille appartient à $\tilde{\Gamma}_{n,2n}$. Soit $\epsilon \in \{\pm 1\}$ tel que $\epsilon\gamma$ appartient à $\Gamma_{n,2n}$. D'après la formule 3.1.24 appliquée avec $\epsilon\gamma$ nous obtenons

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\gamma.z, \frac{\gamma.\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(\gamma.z, \frac{\gamma.\Omega}{n}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\epsilon z, \frac{\Omega}{n}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(\epsilon z, \frac{\Omega}{n}\right)}.$$

Cette dernière formule montre que les coordonnées des images des points de la variété abélienne sont laissées invariantes (à l'involution $z \mapsto -z$ près) par l'action de γ.

La preuve dans le cas des autres familles est similaire. □

3.2 Arithmétique

Après avoir étudié les variétés abéliennes en tant que variétés algébriques via leurs plongements par les fonctions thêta, nous nous intéressons maintenant à la partie abélienne. Nous nous limitons aux cas des niveaux pairs. Comme il y a plusieurs bases de fonction thêta, il a fallu faire un choix et nous laissons au lecteur le soin d'adapter les formules pour les autres bases.

Le fait que le niveau des fonctions thêta soit pair impose que la caractéristique du corps de base soit différente de 2. Pour ces corps, il faut modifier les formules, ce qui est fait en genre 1 et 2 dans [GL09].

Dans un premier temps (section 3.2.1) nous présentons les « vraies » formules d'additions (c'est à dire comment obtenir $z + z'$ à partir de z et de z') dans le cas des niveaux divisibles par 4. Nous nous intéressons ensuite au cas du niveau 2. Puis dans 3.2.3, nous utilisons les additions différentielles pour diverses applications :

- Garder trace des facteurs projectifs dans les coordonnées projectives des points.
- Calculer les puissances des facteurs projectifs associés à des points de ℓ-torsion.
- Calculer le module engendré par des points de ℓ-torsion.

Finalement dans 3.2.4, nous présentons et comparons la complexité des différents algorithmes.

3.2.1 Formules d'addition

Lubicz et Robert [LR10a] ont démontré qu'il était possible d'utiliser les relations de Riemann généralisées 3.1.12 pour obtenir un algorithme d'addition pour les niveaux pairs.

Algorithme 7 add (P, Q, O_A) : addition en coordonnées thêta $\mathscr{F}_{(n/2,2)}$

Entrée: Soit A une variété abélienne donnée par ses thêta constantes $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)$ de niveau n avec n divisible par 4. Supposons données les coordonnées thêta dans la base $\mathscr{F}_{(n/2,2)}$ de niveau n de deux points P et Q associés aux vecteurs z et z'.

Sortie: Les coordonnées du point $P+Q$ correspondant à $z+z'$.

1: Choisir a_2 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_2 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ {On peux mettre un ordre sur $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g \times \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et prendre les premiers}

2: **for** a_1 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_1 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ **do**

3: Choisir a_3, a_4 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_3, b_4 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ tels que

$$-a_1+a_2+a_3+a_4 = 2a, \quad -b_1+b_2+b_3+b_4 = 2b$$

avec $a \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et $b \in \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et tels que $\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)$ soit non nul.

4: Calculer

$$u\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right](z+z') := \theta\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right]\left(2(z+z'), \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)$$

par la formule 3.23.

5: **end for**

6: Vérifier que les $u\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right](z+z')$ ne sont pas tous nuls sinon revenir au point 3 et choisir d'autres a_2, b_2. {Il n'y a qu'un nombre fini de choix de a_2, b_2 et l'un de ces choix convient.}

7: **return** Le vecteur projectif $\left(u\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right](z+z')\right)$ des coordonnées du point $z+z'$.

Nous ne décrivons l'algorithme que dans le cas plus facile où n est divisible par 4. Dans ce cas les formules s'obtiennent naturellement avec les coordonnées $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z, \frac{4\Omega}{n}\right)$ (propriété 3.2.1). L"algorithme 7 reprend ces formules.

Propriété 3.2.1. *Soit n un entier divisible par 4. Pour tout entier $i \in \{1, \ldots, 4\}$, soient $a_i \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et $b_i \in \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ tels que*

$$-a_1+a_2+a_3+a_4 = 2a, \qquad -b_1+b_2+b_3+b_4 = 2b$$

où a et b appartiennent respectivement à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et à $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$. Pour tout z et z' de $\mathbb{C}^g$, nous avons

$$2^g\theta\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right]\left(2(z+z'), \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right) =$$
$$\sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}a_1+a+\alpha\\b_1+b+\beta\end{smallmatrix}\right]\left(2z, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_2-a+\alpha\\b_2-b+\beta\end{smallmatrix}\right]\left(2z, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_3-a+\alpha\\b_3-b+\beta\end{smallmatrix}\right]\left(2z', \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4-a+\alpha\\b_4-b+\beta\end{smallmatrix}\right]\left(2z', \frac{4\Omega}{n}\right). \tag{3.23}$$

Pour pouvoir utiliser ces formules pour faire des additions en coordonnées thêta, il faut justifier qu'il existe des indices tels que la quantité

$$\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)$$

soit non nulle. Remarquons qu'il existe a_2 et b_2 tels que $\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)$ soit non nul car une des coordonnées du point $z-z'$ doit être non nulle (ces fonctions thêta fournissant un plongement de la variété dans $\mathbb{P}^{n^g-1}(\mathbb{C})$). Pour $4 \mid n$ Mumford [Mum66] a montré que pour tout choix de a_1, a_2, b_1, b_2 il existe des indices a_3, a_4, b_3, b_4 vérifiant les conditions du théorème et tels que

$$\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right) \neq 0.$$

Algorithme 8 add (P, Q, O_A) : addition en coordonnées thêta $\mathscr{F}_n$

Entrée: Soit A une variété abélienne donnée par ses thêta constantes $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)$ de niveau n avec n divisible par 4. Supposons données les coordonnées thêta dans la base $\mathscr{F}_n$ de niveau n de deux points P et Q associés aux vecteurs z et z'.

Sortie: Les coordonnées du point $P+Q$ correspondant à $z+z'$.

1: Calculer les thêta constantes suivantes par la formule 3.11 {elles peuvent être pré-calculées}

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right) \quad a \in \tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ b \in \tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g.$$

2: Calculer les fonctions thêta suivantes par la formule 3.11

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z, \frac{4\Omega}{n}\right),\ \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z', \frac{4\Omega}{n}\right) \quad a \in \tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ b \in \tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g.$$

3: Choisir a_2 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_2 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ {On peux mettre un ordre sur $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g \times \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et prendre les premiers}

4: **for** a_1 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_1 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ **do**

5: Choisir a_3, a_4 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_3, b_4 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ tels que

$$-a_1+a_2+a_3+a_4 = 2a, \quad -b_1+b_2+b_3+b_4 = 2b$$

avec $a \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et $b \in \frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et tels que $\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0, \frac{4\Omega}{n}\right)$ soit non nul.

6: Calculer

$$u\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right](z+z') := \theta\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right]\left(2(z+z'), \frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)$$

par la formule 3.23.

7: **end for**

8: Vérifier que les $u\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right](z+z')$ ne sont pas tous nuls sinon revenir au point 3 et choisir d'autres a_2, b_2. {Il n'y a qu'un nombre fini de choix de a_2, b_2 et l'un de ces choix convient.}

9: **return** Les coordonnées projectives $v\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z+z')$ de niveau n du point $z+z'$ obtenues par (voir la formule 3.10)

$$v\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z+z') := \sum_{\alpha \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} u\left[\begin{smallmatrix}\alpha\\2b\end{smallmatrix}\right](z+z'), \qquad b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g.$$

Fixons a_2 et b_2 tels que $\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2(z-z'), \frac{4\Omega}{n}\right)$ soit non nul. Cette quantité apparaît en facteurs de toutes les coordonnées thêta du points $z+z'$ et elle peut donc être omise car nous avons un plongement projectif. Évidement, pour calculer les coordonnées de $z+z'$ nous ne connaissons pas celles de $z-z'$ et nous ne pouvons pas savoir si la coordonnée choisie est non nulle. Il est possible après coup de le vérifier en testant qu'une, au moins, des coordonnées de $z+z'$ n'est pas nulle.

Ces formules ont été obtenues par Baily [Bai62] pour le niveau $(2,2)$. Nous y reviendrons dans la partie 5.5.

Pour $n \neq 4$, les coordonnées $\mathscr{F}_{(n/2,2)}$ sont peu utilisées, c'est pourquoi nous donnons dans l'algorithme 8 les formules d'additions pour les coordonnées dans la base $\mathscr{F}_n$.

3.2.2 En niveau 2

Soit A une variété abélienne. Nous nous intéressons à la variété algébrique $A/\{\pm 1\}$ et aux coordonnées thêta de niveau 2 associées. Il n'est plus possible d'additionner deux points P et Q. En effet nous ne

connaissons que les classes de $\pm P$ et $\pm Q$ dans $A/\{\pm 1\}$ et donc nous ne savons pas discriminer $\pm(P+Q)$ de $\pm(P-Q)$. Il existe cependant un algorithme de doublement et un algorithme de pseudo-addition où nous supposons connue la différence des deux points à additionner.

Remarque 3.2.2. *Une fois obtenu des algorithmes de doublement et de pseudo-addition, nous pouvons calculer le multiple d'un point comme expliqué page 60.*

Plus particulièrement, nous nous intéressons ici aux fonctions thêta de niveau 2 dans le cas particulier des bases suivantes

$$\begin{aligned}\mathscr{F}_2 &= \left\{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{2}\right),\quad b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right\},\\ \mathscr{F}_{(2,1)^2} &= \left\{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z,\Omega)^2,\quad b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right\}.\end{aligned}$$

Nous supposons, pour cette section, que toutes les thêta constantes paires qui apparaissent sont non nulles. Cela est vrai en particulier dans les cas suivants

- variétés génériques,
- courbes hyperelliptique en genre 2 non $(2,2)$-décomposables.

Quand certaines de ces thêta constantes sont nulles, il n'est en général pas possible d'utiliser le niveau 2 et nous devons alors rester en niveau 4. Cependant, même pour ces variétés, il existe des cas où il est possible d'utiliser le niveau 2. Dans le cas des courbes hyperelliptiques de genre plus grand que 3, il existe toujours des thêta constantes paires qui sont nulles (théorème 3.1.17). Cependant, quand les coordonnées de $P-Q$ sont non nulles, il est quand même possible de calculer celles de $P+Q$.

Pour le doublement, nous utilisons les isogénies de Richelot [Ric36, Ric37] :

$$\begin{array}{ccc}\mathbb{C}^g/\Omega\mathbb{Z}^g+\mathbb{Z}^g & \longrightarrow & \mathbb{C}^g/2\Omega\mathbb{Z}^g+\mathbb{Z}^g\\ z & \longmapsto & 2z\\ z & \longleftarrow\!\shortmid & z\end{array}$$

La composition de ces deux isogénies est la multiplication par 2 sur $\mathbb{C}^g/\Omega\mathbb{Z}^g+\mathbb{Z}^g$.

Sur la surface de Kummer, il n'existe pas de formule d'addition. Cependant si les coordonnées des points $\pm P$, $\pm Q$ et $\pm(P-Q)$ sont connues, il est possible de retrouver celles de $\pm(P+Q)$.

Cas particulier

Commençons par traiter le cas particulier où les diverses évaluations des fonctions thêta ne sont pas nulles. L'algorithme est alors beaucoup plus simple. Nous allons utiliser les relations suivantes [Gau07] :

Propriété 3.2.3 (Gaudry). *Pour $\mathscr{F}_2$, quels que soient a et b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,*

$$\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](2z,\Omega) = \frac{1}{2^g}\frac{1}{\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,\Omega)}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t a\beta}\theta\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{2}\right)^2, \tag{3.24}$$

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(2z,\frac{\Omega}{2}\right) = \frac{1}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right)}\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t\alpha b}\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z,\Omega)^2. \tag{3.25}$$

Pour $\mathscr{F}_{(2,1)^2}$, quels que soient a et b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](2z,2\Omega) = \frac{1}{2^g}\frac{1}{\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,2\Omega)}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t a\beta}\theta\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right](z,\Omega)^2, \tag{3.26}$$

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](2z,\Omega)^2 = \frac{1}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)^2}\left(\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t\alpha b}\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z,2\Omega)^2\right)^2. \tag{3.27}$$

Démonstration. Les deux premières formules sont des cas particuliers de la formule de Koizumi 3.5 appliquée respectivement aux matrices T suivantes

$$T = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

□

Dans le cas de la base $\mathscr{F}_2$, supposons que les thêta constantes $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{2}\right)$ et $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,\Omega)$ (respectivement les thêta constantes $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)$ et $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,2\Omega)$ dans le cas de la base $\mathscr{F}_{(2,1)^2}$) ne sont pas nulles. Connaissant les thêta constantes de la base $\mathscr{F}_2$ (respectivement celles de la base $\mathscr{F}_{(2,1)^2}$), il n'est pas possible de calculer les thêta constantes $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,\Omega)$ (respectivement $\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](0,2\Omega)$) mais seulement leurs carrés. En fait dans l'équation 3.25 (respectivement 3.27), nous n'avons besoin que du carré de la formule 3.24 (respectivement 3.26).
Quand les thêta constantes ne sont pas nulles, nous obtenons donc des formules rationnelles permettant de calculer les fonctions thêta de niveau 2 évaluées en $2z$ à partir de celles évaluées en z. Une partie de ces formules se trouvait déjà dans l'article de Chudnovsky et Chudnovsky [CC86]. Pour l'addition différentielle nous avons besoin des formules supplémentaires suivantes :

Propriété 3.2.4 (Gaudry)**.** *Pour tout b dans $\frac{1}{2}\mathbb{Z}^g$, pour tout z, z' dans $\mathbb{C}^g$,*

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z', \frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z', \frac{\Omega}{2}\right) = \sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} (-1)^{4\,{}^t\alpha b}\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z',\Omega), \tag{3.28}$$

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z+z',\Omega)^2\,\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z-z',\Omega)^2 = \left(\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} (-1)^{4\,{}^t\alpha b}\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z,2\Omega)\,\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z',2\Omega)\right)^2. \tag{3.29}$$

En se plaçant dans le cas générique (celui où aucune coordonnée thêta de niveau 2 évaluée en $z-z'$ n'est nulle), nous obtenons des formules permettant de calculer les fonctions thêta évaluées en $z+z'$ en fonction de leurs valeurs en z, z' et $z-z'$.

Avant de poursuivre, il est sans doute utile de remplacer les fonctions thêta par des coordonnées ce qui permet de se rendre compte de la simplicité des formules. Traitons le cas du genre 2 pour la base $\mathscr{F}_{(2,1)^2}$. Il y a 4 fonctions thêta de niveau 2 que nous appelons (X,Y,Z,T) de la façon suivante (cela correspond à la numérotation de Dupont) :

$$\begin{aligned} X &= \theta\begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{bmatrix}(z,\Omega)^2, & Y &= \theta\begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0)\end{bmatrix}(z,\Omega)^2, \\ Z &= \theta\begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2})\end{bmatrix}(z,\Omega)^2, & T &= \theta\begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{bmatrix}(z,\Omega)^2. \end{aligned}$$

Notons $(\alpha,\beta,\gamma,\delta)$ les thêta constantes associées ainsi que (A,B,C,D) celles de la variété isogène :

$$\begin{aligned} A &= \theta\begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ 0)\end{bmatrix}(0,2\Omega)^2, & B &= \theta\begin{bmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ 0)\end{bmatrix}(0,2\Omega)^2, \\ C &= \theta\begin{bmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(0\ 0)\end{bmatrix}(0,2\Omega)^2, & D &= \theta\begin{bmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ 0)\end{bmatrix}(0,2\Omega)^2. \end{aligned}$$

Les algorithmes 9 et 10 permettent de calculer les doublements et les pseudo-additions. Nous avons noté $\mathcal{K}_{(\alpha,\beta,\gamma,\delta)}$ la surface de Kummer sur laquelle nous travaillons.

Algorithme 9 Doublement sur une surface de Kummer avec la base $\mathscr{F}_{(2,1)^2}$ en genre 2

Entrée: un point $P = (X, Y, Z, T)$ sur $\mathcal{K}_{(\alpha,\beta,\gamma,\delta)}$.
Sortie: le point $[2]P = (X_2 : Y_2 : Z_2 : T_2)$.

1:
$$\begin{aligned} X' &= (X+Y+Z+T)^2/A, & Y' &= (X+Y-Z-T)^2/B, \\ Z' &= (X-Y+Z-T)^2/C, & T' &= (X-Y-Z+T)^2/D \end{aligned}$$

2:
$$\begin{aligned} X_2 &= (X'+Y'+Z'+T')^2/\alpha, & Y_2 &= (X'+Y'-Z'-T')^2/\beta, \\ Z_2 &= (X'-Y'+Z'-T')^2/\gamma, & T_2 &= (X'-Y'-Z'+T')^2/\delta \end{aligned}$$

3: **return** (X_2, Y_2, Z_2, T_2)

Algorithme 10 Pseudo-addition sur une surface de Kummer avec la base $\mathscr{F}_{(2,1)^2}$ en genre 2

Entrée: deux points $P = (X_1, Y_1, Z_1, T_1)$ et $Q = (X_2, Y_2, Z_2, T_2)$ sur $\mathcal{K}_{(\alpha,\beta,\gamma,\delta)}$, et le point $R = (x, y, z, t)$ égal à $P - Q$ et tel que $xyzt \neq 0$.
Sortie: le point $P + Q = (X, Y, Z, T)$.

1:
$$\begin{aligned} X' &= (X_1+Y_1+Z_1+T_1)(X_2+Y_2+Z_2+T_2)/A, \\ Y' &= (X_1+Y_1-Z_1-T_1)(X_2+Y_2-Z_2-T_2)/B, \\ Z' &= (X_1-Y_1+Z_1-T_1)(X_2-Y_2+Z_2-T_2)/C, \\ T' &= (X_1-Y_1-Z_1+T_1)(X_2-Y_2-Z_2+T_2)/D \end{aligned}$$

2:
$$\begin{aligned} X &= (X'+Y'+Z'+T')^2/x, \\ Y &= (X'+Y'-Z'-T')^2/y, \\ Z &= (X'-Y'+Z'-T')^2/z, \\ T &= (X'-Y'-Z'+T')^2/t \end{aligned}$$

3: **return** (X, Y, Z, T)

Cas général

Traitons maintenant le cas général : c'est à dire celui où les coordonnées de $z - z'$ peuvent être nulles. Nous ne le traitons que pour la base $\mathscr{F}_2$, le cas de la base $\mathscr{F}_{(2,1)^2}$ étant plus compliqué. De plus cette dernière base n'est pas utilisée dans ce cadre. La méthode suivante (algorithme 11) a été décrite dans [LR10b]. On pourra aussi consulter [Rob10, section 4.8] qui est plus détaillé.

Pour le doublement, nous procédons comme précédemment. Pour la pseudo-addition, il faut utiliser les formules

Propriété 3.2.5. *Pour la base $\mathscr{F}_2$: pour tous vecteurs z et z' dans $\mathbb{C}^g$, quels que soient a et b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,*

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2z, \Omega) = \frac{1}{2^g} \frac{1}{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, \Omega)} \sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} (-1)^{4\,{}^t a\beta} \theta\left[\begin{smallmatrix} 0 \\ b+\beta \end{smallmatrix}\right]\left(z, \frac{\Omega}{2}\right) \theta\left[\begin{smallmatrix} 0 \\ \beta \end{smallmatrix}\right]\left(z, \frac{\Omega}{2}\right), \tag{3.30}$$

$$\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\left(z+z', \frac{\Omega}{2}\right) \theta\left[\begin{smallmatrix} 0 \\ b' \end{smallmatrix}\right]\left(z-z', \frac{\Omega}{2}\right) = \sum_{\alpha \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix} \alpha \\ b+b' \end{smallmatrix}\right](2z, \Omega)\, \theta\left[\begin{smallmatrix} \alpha \\ b-b' \end{smallmatrix}\right](2z', \Omega). \tag{3.31}$$

Il n'est malheureusement pas possible de conclure immédiatement avec les formules précédentes. En effet, il faudrait diviser par $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, \Omega)$. Or, pour tout $b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ non nul, il existe un $a \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ tel

Algorithme 11 Pseudo-addition en coordonnées thêta $\mathscr{F}_2$ (niveau 2) : cas général

Entrée: une variété abélienne donnée par ses thêta constantes $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right)$ de niveau 2. Supposons données les coordonnées de niveau 2 des points correspondant aux vecteurs complexes z, z' et $z-z'$.
Sortie: Les coordonnées du point correspondant au vecteur $z+z'$.

Calculer les thêta constantes suivantes par la formule 3.33 {elles peuvent être pré-calculées}

$$\theta\left[\begin{smallmatrix}a\\b+b'\end{smallmatrix}\right](0,\Omega)\,\theta\left[\begin{smallmatrix}a\\b-b'\end{smallmatrix}\right](0,\Omega)\,,\qquad \forall a,b,b'\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g.$$

if Aucune coordonnée de $z-z'$ n'est nulle **then** {Nous appliquons la méthode de Gaudry [Gau07]}
  Calculer les fonctions thêta suivantes par les formules 3.24

$$\theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](2z,\Omega)\,,\ \theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right](2z',\Omega)\qquad \forall a\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g.$$

  Calculer les produits suivants par la formule 3.28

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)\qquad \forall b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g.$$

  Diviser les coordonnées par $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)$.
  return Les coordonnées $\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\right)_b$.

else
  Calculer par les formules 3.30 les fonctions thêta $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)$ et $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z',\Omega)$ où a et b appartiennent à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et sont tels que $(-1)^{4\,{}^t ab}=1$.
  Pour tout $b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ calculer $\kappa_{b,b}$ grâce à la formule suivante (cas particulier de 3.32) :

$$\kappa_{b,b}=2\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t\alpha b}\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](2z',\Omega)$$

  if $\kappa_{b,b}$ est nul pour tout $b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ **then**
    Soit b_0 tel que $\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)\neq 0$ {Alors $\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)=0$}
    for b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ **do**
      Calculer κ_{b,b_0}. {Nous avons $\kappa_{b,b_0}=\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)$}
      Diviser κ_{b,b_0} par $\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)$ pour obtenir la coordonnée b de $z+z'$.
    end for
  else
    Soit b_0 tel que $\kappa_{b_0,b_0}\neq 0$
    Calculer

$$\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)=\frac{\kappa_{b_0,b_0}}{2\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}.$$

    for b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ **do**
      Calculer κ_{b,b_0}.
      Calculer

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)=\left(2\frac{\kappa_{b,b_0}}{\kappa_{b_0,b_0}}-\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right).$$

    end for
  end if
58
  return Les coordonnées $\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\right)_b$.
end if

que cette thêta constante soit nulle. Si toutes les coordonnées de $z - z'$ sont non nulles, nous pouvons prendre $b' = b$ et obtenir les coordonnées de $z + z'$ (voir la propriété 3.2.4 et l'algorithme 10). Dans le cas général nous remarquons que

$$\begin{aligned}\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right) \quad + \quad \theta\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)\\ = \sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\left(1+(-1)^{4\,{}^t\alpha(b+b')}\right)\theta\left[\begin{smallmatrix}\alpha\\b+b'\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}\alpha\\b-b'\end{smallmatrix}\right](2z',\Omega)\,. \qquad (3.32)\end{aligned}$$

Les thêta constantes $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)$ non nulles ne sont par ailleurs pas calculables à partir des thêta constantes de la base $\mathscr{F}_2$. Par contre nous pouvons calculer le produit de ces constantes qui apparaît lors du calcul du terme $\theta\left[\begin{smallmatrix}\alpha\\b+b'\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}\alpha\\b-b'\end{smallmatrix}\right](2z',\Omega)$ dans l'équation 3.31. En effet, nous avons la formule

$$\theta\left[\begin{smallmatrix}a\\b+b'\end{smallmatrix}\right](0,\Omega)\,\theta\left[\begin{smallmatrix}a\\b-b'\end{smallmatrix}\right](0,\Omega) = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t a\beta}\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b'+\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right). \qquad (3.33)$$

Supposons maintenant que toutes les thêta constantes paires $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)$ ne sont pas nulles (c'est à dire, d'après la formule 3.4, celles pour lesquelles $(-1)^{4\,{}^t ab} = 1$). Alors nous pouvons calculer les quantités suivantes pour tout b et b' dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$:

$$\kappa_{b,b'} := \theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right) + \theta\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right).$$

Si pour tout b, le produit $\kappa_{b,b} = 2\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)$ est nul alors nous obtenons les coordonnées de $z + z'$ (algorithme 11 étapes 10 à 15). Sinon il existe b_0 tel que $\kappa_{b_0,b_0} \neq 0$. Dans ce cas, nous pouvons calculer

$$\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right) = \frac{\kappa_{b_0,b_0}}{2\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}.$$

Nous avons alors

$$\begin{aligned}\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)} &= \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)} + \frac{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}\\ &\quad - \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}\\ &= 2\frac{\kappa_{b,b_0}}{\kappa_{b_0,b_0}} - \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}.\end{aligned}$$

Pour obtenir la thêta constante cherchée il faut donc calculer

$$\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right) = \left(2\frac{\kappa_{b,b_0}}{\kappa_{b_0,b_0}} - \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}{\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)}\right)\theta\left[\begin{smallmatrix}0\\b_0\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right).$$

L'algorithme présenté dans [Rob10, section 4.8 p. 100] est légèrement différent. En effet, on n'y suppose pas connues à priori les coordonnées de $z - z'$. Nous obtenons alors, au prix d'une racine carrée, les coordonnées

$$\left\{\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{2}\right)\right)_{b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}, \left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z-z',\frac{\Omega}{2}\right)\right)_{b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\right\}$$

en fonction de celles des points z et z'.

3.2.3 Formules d'additions différentielles

Additions différentielles classiques

Pour certaines applications (et en particulier le calcul d'isogénies, chapitre 7) il est utile de savoir maîtriser le facteur projectif dans les coordonnées des points. Nous appelons alors relevé affine d'un point P de $\mathbb{P}^{n^g-1}(\mathbb{C})$ un élément $\widetilde{P}$ de $\mathbb{A}^{n^g}(\mathbb{C})$ tel que $\widetilde{P}$ s'envoie sur P par l'application naturelle

$$\mathbb{A}^{n^g}(\mathbb{C}) \to \mathbb{P}^{n^g-1}(\mathbb{C}).$$

Exemple 3.2.6. *Soit la variété $A = \mathbb{C}^g/\Lambda_\Omega$ plongée dans $\mathbb{P}^{n^g-1}(\mathbb{C})$ par les fonctions thêta de niveau n. Ces dernières fournissent naturellement un relevé affine : $\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right)\right)_b \in \mathbb{A}^{n^g}(\mathbb{C})$ est un relevé affine du point $\left(\lambda\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right)\right)_b \in \mathbb{P}^{n^g-1}(\mathbb{C})$.*

Soit P et Q deux points d'une variété abélienne A correspondant aux vecteurs z et z'. Supposons connues les « vraies » coordonnées de niveau 2 des points O_A, $\pm P$, $\pm Q$ et $\pm(P-Q)$ (c'est-à-dire les fonctions thêta évaluées en 0, z, z' et $z-z'$ et non pas ces fonctions à un facteur projectif près). Les algorithmes présentés dans la section précédente permettent alors de calculer les « vraies » coordonnées de niveau 2 du point $\pm(P+Q)$.

Soit un entier 2 pair et supérieur à 3. Supposons connues les « vraies » coordonnées de niveau n des points O_A, P, Q et $P-Q$. Quand $4 \mid n$, nous pouvons modifier l'algorithme 8 pour obtenir un algorithme d'addition différentielle (aussi appelé de pseudo-addition) permettant de retrouver les « vraies » coordonnées du point $P+Q$. Ce nouvel algorithme est l'algorithme 12.

Notons $\text{add\_diff}\left(\widetilde{P}, \widetilde{Q}, \widetilde{P-Q}, \widetilde{O_A}\right)$ le résultat fourni par l'algorithme 12 (respectivement de l'algorithme 11). C'est un relevé affine de $P+Q$ (respectivement de $\pm(P+Q)$).

Il est clair que $\text{add\_diff}\left(\widetilde{P}, \widetilde{Q}, \widetilde{P-Q}, \widetilde{O_A}\right)$ dépend des relevés affines des différents points. La propriété suivante précise cette dépendance. Pour se fixer les idées, on pourra considérer les relevés affines comme étant exacts.

Lemme 3.2.7. *Soit A une variété abélienne de zéro O_A et soient P et Q deux points de A donnés avec les fonctions thêta de niveau n (nous supposons $4 \mid n$). Soient $\widetilde{O_A}$, $\widetilde{P}$, $\widetilde{Q}$, $\widetilde{P-Q}$ des relevés affines des différents points. Soient λ_{O_A}, λ_P, λ_Q, λ_{P-Q} des éléments de $\mathbb{C}^*$, alors*

$$\text{add\_diff}\left(\lambda_P\widetilde{P}, \lambda_Q\widetilde{Q}, \lambda_{P-Q}\widetilde{P-Q}, \lambda_{O_A}\widetilde{O_A}\right) = \frac{\lambda_P^2\lambda_Q^2}{\lambda_{P-Q}\lambda_{O_A}^2}\,\text{add\_diff}\left(\widetilde{P}, \widetilde{Q}, \widetilde{P-Q}, \widetilde{O_A}\right).$$

Chaînes d'additions différentielles

Soit un point P sur une variété abélienne donné par ses coordonnées thêta de niveau n. Nous voulons calculer $[k]P$ pour un entier k en n'utilisant que des doublements et des additions différentielles. L'intérêt est de pouvoir calculer les vraies coordonnées du point $[k]P$ en fonction de celles de P et de O_A. Par ailleurs, en niveau 2, il n'existe pas d'addition, et pour calculer $[k]P$, nous devons utiliser uniquement des doublements et des pseudo-additions.

Nous sommes dans un cas spécial de chaînes d'additions appelées chaînes de Lucas. Ainsi

$$1 \to 2 \to 3 \to 4 \to 7 \to 10 \to 17$$

est une chaîne de Lucas pour 17. Une façon de construire de telles chaînes est de remarquer que si nous connaissons les points $[n]P$ et $[n+1]P$ alors nous pouvons calculer $[2n]P$, $[2n+1]P$ et $[2n+2]P$. Ces chaînes sont appelées binaires : à chaque étape, nous choisissons le point à doubler selon la décomposition binaire de k (algorithme 13). Pour un nombre k donné, il existe une unique chaîne de Lucas binaire. Par exemple, la chaîne suivante est la chaîne binaire pour 17 :

$$1 \to 2 \to 3 \to 4 \to 5 \to 8 \to 9 \to 17.$$

Algorithme 12 add_diff $\left(\widetilde{P},\widetilde{Q},\widetilde{R},\widetilde{O_A}\right)$: additions différentielles en coordonnées thêta $\mathscr{F}_n$

Entrée: Soit A une variété abélienne donnée par ses thêta constantes $\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)$ de niveau n avec n divisible par 4. Supposons donnés des relevés affines $\widetilde{P}$, $\widetilde{Q}$, $\widetilde{R}$ des coordonnées de niveau n des points correspondants aux vecteurs z, z' et $z-z'$.
Sortie: Un relevé affine des coordonnées du point $z+z'$.

1: Calculer les thêta constantes suivantes par la formule 3.11 {elles peuvent être pré-calculées}

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right) \quad a\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ b\in\tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g.$$

2: Calculer les fonctions thêta suivantes par la formule 3.11

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z,\frac{4\Omega}{n}\right),\ \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2z',\frac{4\Omega}{n}\right),\ \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(2\left(z-z'\right),\frac{4\Omega}{n}\right) \quad a\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,\ b\in\tfrac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g.$$

3: Choisir a_2 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_2 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ tels que $\theta\left[\begin{smallmatrix}a_2\\b_2\end{smallmatrix}\right]\left(2\left(z-z'\right),\frac{4\Omega}{n}\right)\neq 0$.
4: **for** a_1 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_1 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ **do**
5: Choisir a_3, a_4 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et b_3, b_3 dans $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ tels que

$$-a_1+a_2+a_3+a_4=2a,\quad -b_1+b_2+b_3+b_4=2b$$

avec $a\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ et $b\in\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et tels que $\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right]\left(0,\frac{4\Omega}{n}\right)$ soit non nul.
6: Par la formule 3.23, calculer

$$\theta\left[\begin{smallmatrix}a_1\\b_1\end{smallmatrix}\right]\left(2(z+z'),\frac{4\Omega}{n}\right).$$

7: **end for**
8: **return** Les coordonnées de niveau n du point $z+z'$ obtenues par (voir la formule 3.10)

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{n}\right)=\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\theta\left[\begin{smallmatrix}\alpha\\2b\end{smallmatrix}\right]\left(2(z+z'),\frac{4\Omega}{n}\right),\qquad b\in\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g.$$

Les chaînes binaires ne sont pas les chaînes de Lucas les plus courtes. L'algorithme PRAC de Montgomery [Mon83] trouve de manière efficace des chaînes de Lucas courtes.

Dans le cadre des fonctions thêta de niveau 2, pour avoir des formules de multiplications efficaces nous n'utilisons que des chaînes binaires. La raison sera expliquée à la page 68.

Nous avons présenté une méthode permettant de calculer un multiple d'un point en n'utilisant que des additions différentielles et des doublements. Cette méthode peut être adaptée pour calculer $[k]P+Q$ à partir de la connaissance de O_A, P, Q et de $P+Q$.

Il est important de noter que le relevé affine de $[k]P+Q$ obtenu à partir d'un relevé des différents points et à l'aide uniquement d'additions différentielles ne dépend pas de la chaîne choisie. Nous pouvons alors noter

$$\text{mult\_add}(k,\widetilde{P},\widetilde{P+Q},\widetilde{Q},\widetilde{O_A})$$

le résultat d'un tel calcul. Dans le cas particulier où $Q=O_A$, nous notons

$$\text{mult}(k,\widetilde{P},\widetilde{O_A})=\text{mult\_add}(k,\widetilde{P},\widetilde{P},\widetilde{O_A},\widetilde{O_A}).$$

C'est le résultat de l'algorithme 13.

Algorithme 13 multiplication binaire

Entrée: un point P et un entier $k > 1$.
Sortie: le point $[k]P$.

if $k = 2$ **then**
  return $[2]P$
else
  Soit $k = \sum_{i=0}^{l} k_i 2^{l-i}$ la décomposition binaire de k avec $k_0 = 1$ le bit de poids fort.
  $P_m = P$; $P_p = [2]P$;
  for i from 2 to l **do**
    $Q = P_p + P_m$ {On remarque que $P_p - P_m = P$}
    if $k_i = 1$ **then**
      $P_p = [2]P_p$; $P_m = Q$;
    else $\{k_i = 0\}$
      $P_m = [2]P_m$; $P_p = Q$;
    end if
  end for
  return P_m
end if

Lemme 3.2.8. *Soit A une variété abélienne de zéro O_A et soit P un point de A donné avec les fonctions thêta de niveau n (où $4 \mid n$). Soient $\widetilde{O_A}$ et $\widetilde{P}$, des relevés affines des deux points. Soient λ_{O_A} et λ_P des éléments de $\mathbb{C}^*$. Alors, pour tout entier $k \geqslant 1$,*

$$\mathrm{mult}(k, \lambda_P \widetilde{P}, \lambda_{O_A} \widetilde{O_A}) = \frac{\lambda_P^{k^2}}{\lambda_{O_A}^{k^2-1}} \mathrm{mult}(k, \widetilde{P}, \widetilde{O_A}).$$

De même, soient $\widetilde{P+Q}$ et $\widetilde{Q}$ des relevés affines des points $P+Q$ et Q et soient λ_{P+Q} et λ_Q des éléments de $\mathbb{C}^*$. Alors

$$\mathrm{mult\_add}(k, \lambda_P \widetilde{P}, \lambda_{P+Q} \widetilde{P+Q}, \lambda_Q \widetilde{Q}, \lambda_{O_A} \widetilde{O_A}) = \frac{\lambda_{P+Q}^{k} \lambda_P^{k(k-1)}}{\lambda_Q^{k-1} \lambda_{O_A}^{k(k-1)}} \mathrm{mult\_add}(k, \widetilde{P}, \widetilde{P+Q}, \widetilde{Q}, \widetilde{O_A}).$$

La preuve de ce lemme se fait par récurrence en utilisant le lemme 3.2.7. Le lemme suivant est utile pour la programmation dans le cadre du genre 1 et 2. Il se montre aussi par récurrence.

Lemme 3.2.9. *Soient P, Q, R trois points d'une variété abélienne A. Supposons connus des relevés affines des points de l'ensemble*

$$\{P,\ Q,\ R,\ P+Q,\ P+R,\ Q+R,\ P+Q+R\}.$$

Pour tout $a, b, c \in \mathbb{N}$, il est possible de calculer $aP + bQ + cR$ en utilisant uniquement des chaînes d'additions différentielles. Le facteur projectif du relevé affine de ce point est alors :

$$\frac{\lambda_{P+Q+R}^{abc} \lambda_P^{a(a-b-c+bc)} \lambda_Q^{b(b-a-c+ac)} \lambda_R^{c(c-a-b+ab)}}{\lambda_{P+Q}^{ab(c-1)} \lambda_{P+R}^{ac(b-1)} \lambda_{Q+R}^{bc(a-1)} \lambda_{O_A}^{a^2+b^2+c^2-ab-ac-bc+abc-1}}.$$

Calcul des puissances des facteurs projectifs

Soient n et ℓ deux entiers avec n pair. Soit z un vecteur de $\mathbb{C}^g$, posons

$$P = \left(\theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] \left(z, \frac{\Omega}{n} \right) \right)_{b \in \frac{1}{n}\mathbb{Z}^g / \mathbb{Z}^g}$$

le point de $\mathbb{P}^{n^g-1}(\mathbb{C})$ correspondant. Supposons que P soit de ℓ-torsion c'est-à-dire ℓz appartient au réseau Λ_Ω. Soit $\widetilde{O_A}$ un relevé affine du zéro de la variété A et soit $\widetilde{P}$ un relevé affine de P : il existe donc des nombres complexes λ_{O_A} et λ_P tels que

$$\widetilde{O_A} = \lambda_{O_A}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}, \qquad \widetilde{P} = \lambda_P\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Supposons connues les coordonnées de $\widetilde{O_A}$ et celles de $\widetilde{P}$. Nous voulons retrouver le facteur λ_P/λ_{O_A}.

En utilisant les additions différentielles, nous pouvons calculer $\widetilde{Q} = \mathrm{mult}\left(\ell, \widetilde{P}, \widetilde{O_A}\right)$ qui est un relevé affine de $Q = [\ell]P$. D'après le lemme 3.2.8, nous avons

$$\widetilde{Q} = \frac{\lambda_P^{\ell^2}}{\lambda_{O_A}^{\ell^2-1}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\ell z,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Cependant comme ℓz appartient au réseau Λ_Ω et d'après les formules 3.1.2 nous obtenons

$$\widetilde{Q} = \frac{\lambda_P^{\ell^2}}{\lambda_{O_A}^{\ell^2-1}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \frac{\lambda_P^{\ell^2}}{\lambda_{O_A}^{\ell^2}}\widetilde{O_A}.$$

Une des coordonnées de $\widetilde{O_A}$ n'est pas nulle et en divisant par celle-ci la coordonnée correspondante de $\widetilde{Q}$, nous obtenons la puissance ℓ^2-ième du facteur λ_P/λ_{O_A}.

En fait, nous pouvons faire mieux et obtenir la puissance 2ℓ-ième si ℓ est pair et ℓ-ième si ℓ est impair. Cette méthode est dûe à Lubicz et Robert [LR10a]. Détaillons ce dernier cas : posons $\ell = 2\ell' + 1$ et

$$\widetilde{Q_+} = \mathrm{mult}\left(\ell'+1, \widetilde{P}, \widetilde{O_A}\right), \qquad \widetilde{Q_-} = \mathrm{mult}\left(-\ell', \widetilde{P}, \widetilde{O_A}\right).$$

D'après le lemme 3.2.8, nous avons

$$\widetilde{Q_+} = \frac{\lambda_P^{(\ell'+1)^2}}{\lambda_{O_A}^{(\ell'+1)^2-1}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left((\ell'+1)\,z,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g},$$

$$\widetilde{Q_-} = \frac{\lambda_P^{(-\ell')^2}}{\lambda_{O_A}^{(-\ell')^2-1}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left((-\ell')\,z,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Comme ℓz appartient à Λ_Ω nous obtenons

$$\widetilde{Q_+} = \frac{\lambda_P^{(\ell'+1)^2}}{\lambda_{O_A}^{(\ell'+1)^2-1}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left((-\ell')\,z,\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \frac{\lambda_P^{(\ell'+1)^2}}{\lambda_{O_A}^{(\ell'+1)^2-1}}\frac{\lambda_{O_A}^{(-\ell')^2-1}}{\lambda_P^{(-\ell')^2}}\widetilde{Q_-} = \frac{\lambda_P^{2\ell'+1}}{\lambda_{O_A}^{2\ell'+1}}\widetilde{Q_-}.$$

Une des coordonnées de $\widetilde{Q_-}$ étant non nulle, nous obtenons bien la puissance $2\ell'+1 = \ell$-ième du facteur projectif.

Soit z' un autre vecteur de $\mathbb{C}^g$ et soit P' le point correspondant. Soient $\widetilde{P'}$ et $\widetilde{P+P'}$ des relevés affines de P' et $P+P'$: il existe donc des nombres complexes $\lambda_{P'}$ et $\lambda_{P+P'}$ tels que

$$\widetilde{P'} = \lambda_{P'}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z',\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}, \qquad \widetilde{P+P'} = \lambda_{P+P'}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z+z',\frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Nous ne faisons aucune hypothèse sur le point P'. Nous calculons un relevé affine $\widetilde{Q}$ de $\ell P + P'$ avec les chaînes d'addition :

$$\widetilde{Q} = \mathrm{mult\_add}(\ell, \widetilde{P}, \widetilde{P+P'}, \widetilde{P'}, \widetilde{O_A}).$$

D'après le lemme 3.2.8 nous avons

$$\widetilde{Q} = \frac{\lambda_{P+P'}^{\ell}\lambda_P^{\ell(\ell-1)}}{\lambda_{P'}^{\ell-1}\lambda_{O_A}^{\ell(\ell-1)}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\ell z + z', \frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$$

et comme ℓz appartient à Λ_Ω, nous obtenons

$$\widetilde{Q} = \frac{\lambda_{P+P'}^{\ell}\lambda_P^{\ell(\ell-1)}}{\lambda_{P'}^{\ell-1}\lambda_{O_A}^{\ell(\ell-1)}}\left(\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z', \frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \frac{\lambda_{P+P'}^{\ell}\lambda_P^{\ell(\ell-1)}}{\lambda_{P'}^{\ell}\lambda_{O_A}^{\ell(\ell-1)}}\widetilde{P'}.$$

Nous pouvons donc calculer la puissance ℓ-ième du facteur projectif $\lambda_{P+P'}/\lambda_{P'}$ en fonction de la puissance ℓ-ième de λ_P/λ_{O_A}.

Dans le chapitre 6, nous aurons besoin du même type de résultat pour la base $\mathscr{F}_{(2,2)}$. Soit un vecteur $z = \Omega\alpha + \beta$ correspondant à un point de ℓ-torsion. Soit P le point correspondant,

$$P = \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Soit $\widetilde{O_A}$ un relevé affine du zéro de la variété et soit $\widetilde{P}$ un relevé affine de P : il existe donc des nombres complexes λ_{O_A} et λ_P tels que

$$\widetilde{O_A} = \lambda_{O_A}\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}, \qquad \widetilde{P} = \lambda_P\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Supposons que $\ell = 2\ell' + 1$ est impair et calculons par l'algorithme 12 les points

$$\widetilde{Q_+} = \mathrm{mult}\left(\ell'+1, \widetilde{P}, \widetilde{O_A}\right), \qquad \widetilde{Q_-} = \mathrm{mult}\left(-\ell', \widetilde{P}, \widetilde{O_A}\right).$$

D'après la formule 3.1, nous avons

$$\widetilde{Q_+} = \exp\left(-2\pi i 2\ell\, {}^t\alpha\Omega\alpha\right)\exp\left(-2\pi i 2\ell\, {}^t\alpha\beta\right)\frac{\lambda_P^{\ell}}{\lambda_{O_A}^{\ell}}\widetilde{Q_-} \tag{3.34}$$

et nous obtenons alors la puissance ℓ-ième du facteur $\exp\left(-4\pi i\, {}^t\alpha\Omega\alpha\right)\lambda_P/\lambda_{O_A}$. Si ℓ est pair, nous ne savons obtenir que la puissance 2ℓ-ième de ce facteur.

Module engendré par des points de ℓ-torsion

Soient k points e_i de ℓ-torsion et un point P quelconque qui sont donnés par des coordonnées thêta de niveau n. Supposons que les points e_i sont linéairement indépendants et notons S et S' les ensembles

$$S = \{e_i,\ i \in \{1,\dots,g\}\} \cup \{e_i + e_j,\ i \neq j \in \{1,\dots,g\}\},$$

$$S' = \{P\} \cup \{P + e_i,\ i \in \{1,\dots,g\}\} \cup S.$$

Nous décrivons ici une méthode 14 permettant de retrouver, à partir de S, tout le $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathscr{M}$ engendré par les e_i et à partir de S', le module affine $P+\mathscr{M}$ en n'utilisant que des additions différentielles. Rappelons que nous avons fait l'hypothèse que ℓ est impair. Ces algorithmes sont des briques de base essentielles pour pouvoir

- passer des coordonnées compressées aux coordonnées normales [LR10a],
- calculer des ℓ-isogénies en montant de niveau ([LR10a] et partie 7.1),
- calculer des ℓ-isogénies sans changer de niveau (section 7.2.2).

Une autre méthode utilisant différemment les équations de Riemann est donnée dans [Rob10].

Dans le cas où $k = 2$, il est relativement facile d'obtenir les points de $\mathscr{M}$ (début de l'algorithme 14). Dans le cas général, par récurrence, nous pouvons calculer toutes les sommes utilisant strictement moins

Algorithme 14 Calcul, avec des additions différentielles, des points du module $\mathscr{M}$ engendrés par des points de ℓ-torsion.

Entrée: Soient k points e_i de ℓ-torsion (avec ℓ impair) supposés linéairement indépendants. Étant données les coordonnées thêta de niveau n de O_A, des points e_i ainsi que celle des points e_i+e_j avec $i \neq j$.

Sortie: Les coordonnées de tous les points engendrés par les e_i en n'utilisant que des additions différentielles.

if k=2 **then**
  for $m = 1$ to $l-2$ **do**
    $(m+1)e_1 :=$ add_diff$(me_1, e_1, (m-1)e_1, O_A)$.
    $(m+1)e_1 + e_2 :=$ add_diff$(me_1 + e_2, e_1, (m-1)e_1 + e_2, O_A)$.
  end for
  for $m_1 = 0$ to $l-1$ **do**
    for $m_2 = 1$ to $l-2$ **do**
      $m_1e_1 + (m_2+1)e_2 :=$ add_diff$(m_1e_1 + m_2e_2, e_2, m_1e_1 + (m_2-1)e_2, O_A)$.
    end for
  end for{Nous avons tout le $\mathbb{Z}/\ell\mathbb{Z}$ module engendré par e_1, e_2}

else
  Appliquer récursivement l'algorithme pour avoir les sommes de strictement moins de k points.
  Utiliser l'algorithme 15 avec $P = e_3 + \ldots + e_k$ pour obtenir $e_1 + \ldots + e_k$.
  for $i = 1$ to k **do**
    for $(m_1 = 1$ to $l-1)$, ... , $(m_{i-1} = 1$ to $l-1)$ **do**
      for $m_i = 1$ to $l-2$ **do**
        Calculer

$$\sum_{j=1}^{i-1} m_j e_j + (m_i+1)e_i + \sum_{j=i+1}^{k} e_j \quad = \quad \text{add\_diff}\left(\sum_{j=1}^{i-1} m_j e_j + m_i e_i + \sum_{j=i+1}^{k} e_j \ , \ e_i \ , \ \sum_{j=1}^{i-1} m_j e_j + (m_i-1)e_i + \sum_{j=i+1}^{k} e_j \ , \ O_A\right)$$

      end for
    end for
  end for
end if

Algorithme 15 Calcul de $P + e_1 + e_2$

Entrée: Soit P un point quelconque et soient e_1, e_2 deux points de ℓ-torsion avec ℓ impair. Supposons données les coordonnées thêta des points $P + e_1$, $P + e_2$, $P - e_2$, $2e_1$ et $e_1 + e_2$.

Sortie: Les coordonnées de niveau n de $P+e_1+e_2$ obtenues en n'utilisant que des additions différentielles.

1: $P + 2e_1 + e_2 = \text{add\_diff}(P + e_1, e_1 + e_2, P - e_2, O_A)$

2: $P + (\ell + 1)e_1 + e_2 = \text{mult\_add}(\frac{\ell+1}{2}\ ,\ 2e_1\ ,\ P + 2e_1 + e_2\ ,\ P + e_2\ ,\ O_A)$

de k points. De plus, si nous avons les points $\sum_{i=1}^{k} \epsilon_i e_i$ avec $\epsilon_i \in \{0, 1\}$, nous pouvons retrouver tous les points de $\mathscr{M}$ (algorithme 14). La partie difficile est d'obtenir ces points (algorithme 15). Nous allons détailler ce dernier calcul dans le cas particulier suivant.

Soit P un point quelconque (dans l'algorithme 14, P est le point $e_3 + \ldots + e_k$), nous voulons calculer les coordonnées du point $P + e_1 + e_2$ à partir de celles des points $P + e_1$, $P + e_2$, $e_1 + e_2$, $2e_1$ et $P - e_1$. Nous commençons par faire

$$P + 2e_1 + e_2 = \text{add\_diff}(P + e_1, e_1 + e_2, P - e_2, O_A)$$

En utilisant des additions différentielles avec le point $2e_1$ nous obtenons le point $P + (\ell + 1)e_1 + e_2$ (car ℓ est impair). Comme e_1 est de ℓ-torsion, le point obtenu est bien $P + e_1 + e_2$.

Remarque 3.2.10. *Dans l'algorithme 14, il faut faire attention aux facteurs projectifs. En effet les facteurs projectifs des points* $e_1 + (l-1)e_2$ *obtenus par 14 et* $\text{add\_diff}(e_1, -e_2, e_1 + e_2, O_A)$ *sont différents. Le plus simple pour la programmation, si avons besoin du facteur projectif, est d'en garder trace tout au long du calcul.*

Pour obtenir le module affine $P + \mathscr{M}$ à partir de S', il suffit de faire une légère adaptation de l'algorithme 14. Finalement, il est possible d'obtenir les points $kP + \mathscr{M}$ en faisant :

$$kP + M = \text{mult\_add}(k, P, P + M, M, O_A)$$

où M appartient à $\mathscr{M}$.

3.2.4 Complexité

Pour calculer la complexité de nos algorithmes, nous allons faire quelques suppositions sur l'arithmétique du corps sur lequel nous travaillons. En premier lieu les additions seront négligées par rapport aux multiplications. Ceci est valide asymptotiquement sur des corps finis de taille cryptographique mais n'est pas forcément vrai pour des corps de petite taille (voir par exemple le tableau 4.3 dans le cas d'une implémentation du niveau 2 en genre 2).
Selon les algorithmes utilisés, calculer un carré peut être moins coûteux que faire une multiplication. Pour l'arithmétique modulaire, suivant la valeur du modulo, on pourra supposer qu'un carré coûte entre 0.81 et 1 multiplication [BZ10, 1.3.6].
Les divisions sont en général coûteuses par rapport aux multiplications. Pour remédier à ce problème les solutions classiques sont de

- transformer les divisions en produits (car nous travaillons avec des coordonnées projectives),
- transformer les divisions en un certain nombre de produits et 1 division par la méthode de Montgomery [BZ10, 2.5.1] (cela peut être utile pour les additions différentielles en niveau 2),
- essayer d'en diminuer le nombre avec des précalculs et en divisant ensuite toujours par la même quantité.

Dans les algorithmes, il y a des multiplications par des constantes. Si ces dernières peuvent être choisies petites alors ces multiplications ont un coût négligeable.

Dans les formules de complexité, nous noterons (par ordre de complexité décroissante)

- par I les inversions,

– par M les multiplications,
– par S les carrés
– par m_P les multiplications qui dépendent d'un point P de la variété (dans le cas où on peut précalculer certaines quantités)
– par m les multiplications qui dépendent des paramètres de la variété.

Pour certaines applications, ces deux dernières opérations peuvent être considérées comme négligeables, tandis que dans d'autres cas, leur coût est celui d'une multiplication normale.

Nous supposons également que le maximum de précalculs ont été effectués et que leur coût est négligeable par rapport à celui des multiples additions ou doublements que nous voulons effectuer sur la variété. C'est en pratique toujours le cas. En particulier nous considérons que les inverses des thêta constantes sont connus.

Complexité des opérations élémentaires sur la variété

Dans le cas du niveau n (divisible par 4) nous utilisons pour l'addition l'algorithme 8. Les changements de bases entre $\mathscr{F}_n$ et $\mathscr{F}_{(n/2,2)}$ n'utilisent que des additions et sont donc négligeables. Il faut alors calculer la quantité

$$\theta \left[\begin{smallmatrix} a_1 \\ b_1 \end{smallmatrix}\right] \left(2(z+z'), \frac{4\Omega}{n}\right) \theta \left[\begin{smallmatrix} a_2 \\ b_2 \end{smallmatrix}\right] \left(2(z-z'), \frac{4\Omega}{n}\right)$$

pour tout a_1 et b_1 dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$. Pour les a_i et b_i fixés, ce calcul prend $4^g 3M$. Dans le cas où nous connaissons les coordonnées de $z-z'$, nous pouvons choisir a_2 et b_2 tels que la coordonnée $\theta \left[\begin{smallmatrix} a_2 \\ b_2 \end{smallmatrix}\right] \left(2(z-z'), \frac{4\Omega}{n}\right)$ soit non nulle. Sinon il faut calculer cette quantité pour tout a_2 et b_2 jusqu'à ce que les coordonnées de $z-z'$ soient non nulles. Nous obtenons donc la complexité $(3(4n^g))^+ M + (n^g-1)m$ où le $^+$ signifie qu'il faut effectuer l'opération au moins une fois et au plus n^g fois.

Dans le cas du niveau 2, le doublement est effectué à l'aide de la propriété 3.2.3. Sa complexité est de $2^{g+1}S + (2^{g+1}-2)m$ pour les bases $\mathscr{F}_2$ et $\mathscr{F}_{(2,1)^2}$.

Pour la pseudo-addition, si nous pouvons utiliser la méthode de Gaudry (première partie de l'algorithme 11), le coût est de

$$2^g M + 2^{g+1}S + (2^g-1)m_{P-Q} + (2^g-1)m$$

pour la base $\mathscr{F}_2$ et de

$$2^g M + 2^g S + (2^g-1)m_{P-Q} + (2^g-1)m$$

pour la base $\mathscr{F}_{(2,1)^2}$ (avec cette dernière, nous gagnons 2^g carrés).

Si nous ne pouvons pas utiliser la méthode de Gaudry, il faut regarder la seconde partie de l'algorithme 11. L'étape 8 coûtera deux fois $(4^g M + 2^{g-1}(2^g+1)m)$. L'étape 9 de l'algorithme consiste à calculer $\kappa_{b,b}$ jusqu'à en obtenir un non nul, elle coûtera donc de $2^g M$ à $2^{g-1}(2^g+1)M$. Dans le cas où ils sont tous nuls, il faut calculer κ_{b,b_0} pour tout b (étape 13) ce qui prend $2^{g-1}(2^g+1)M$. Finalement l'étape 14 est gratuite si lors des précalculs nous nous sommes ramenés à $\theta \left[\begin{smallmatrix} 0 \\ b_0 \end{smallmatrix}\right] \left(z-z', \frac{\Omega}{2}\right) = 1$. Dans le cas où il existe b_0 tel que κ_{b_0,b_0} soit non nul, l'étape 18 coûte $1m_{p-q}$ puis le calcul de tous les κ_{b,b_0} coûte encore $2^{g-1}(2^g+1)M$. Finalement l'étape 21 prend $1I + 2M + 1m_{p-q}$ pour chaque b. La complexité finale est donc de

$$\begin{cases} 2^g(2^g+1)M + 2^{g-1}(2^g+1)m & \text{si } \kappa_{b,b} = 0,\ \forall b, \\ (2^g-1)\,I + \left(5(2^{2g-1}+2^{g-1}) + (2^g)^+ - 2\right) M + (2^g-1)m_{P-Q} + 2^{g-1}(2^g+1)m & \text{sinon.} \end{cases}$$

Soient deux points P et Q de niveau 2 sur la variété. Nous voulons à la fois calculer $2P$ et $P+Q$ (il faut également supposé la connaissance des coordonnées de $P-Q$). Plutôt que de calculer un doublement puis une pseudo-addition, il est possible de partager des calculs. Ceci est notamment utilisé dans les chaînes d'additions binaires.

Nous nous plaçons en niveau 2 et nous supposons que les coordonnées de $P-Q$ ne sont pas nulles pour pouvoir utiliser les formules de Gaudry. Le calcul des fonctions thêta $\theta \left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right] (2z_P, \Omega)$ peut alors être partagé entre l'algorithme de doublement et celui de pseudo-addition. Par ailleurs, si les thêta constantes associées

Tableau 3.1 – Complexité des opérations élémentaires

Opérations	Complexité
Addition en niveau n (base $\mathscr{F}_n$)	$(3(4n)^g)^+ M + (n^g - 1)m$
Doublement en niveau 2 (base $\mathscr{F}_2$ et $\mathscr{F}_{(2,1)^2}$)	$2^{g+1}S + (2^{g+1} - 2)m$
Pseudo-addition en niveau 2 avec la méthode de Gaudry (base $\mathscr{F}_2$)	$2^g M + 2^{g+1}S + (2^g - 1)m_{P-Q} + (2^g - 1)m$
Pseudo-addition en niveau 2 avec la méthode de Gaudry (base $\mathscr{F}_{(2,1)^2}$)	$2^g M + 2^g S + (2^g - 1)m_{P-Q} + (2^g - 1)m$
Pseudo-addition en niveau 2 méthode général cas où $\forall b,\ \kappa_{b,b} = 0$ (base $\mathscr{F}_2$)	$2^g(2^g + 1)M + 2^{g-1}(2^g + 1)m$
Pseudo-addition en niveau 2 méthode général cas où $\exists b_0,\ \kappa_{b_0,b_0} \neq 0$ (base $\mathscr{F}_2$)	$(2^g - 1)\, I + \left(5(2^{2g-1} + 2^{g-1}) + (2^g)^+ - 2\right) M$ $+(2^g - 1)m_{P-Q} + 2^{g-1}(2^g + 1)m$
Doublement + Pseudo-addition en niveau 2 $P, Q, P - Q \longmapsto 2P, P + Q$ (base $\mathscr{F}_2$ et $\mathscr{F}_{(2,1)^2}$)	$2^g M + 3.2^g S + (2^g - 1)m_{P-Q} + 3(2^g - 1)m$ ou selon le coût de m, $(2^{g+1} - 1)M + (2^{g+1} + 1)S + (2^g - 1)m_{P-Q} + 2(2^g - 1)m$

à la variété ne sont pas choisie petite, les multiplications par ces nombres ne seront pas négligeable. Dans ce cas, il est possible de partager des multiplications entre les deux algorithmes. Pour les deux bases $\mathscr{F}_2$ et $\mathscr{F}_{(2,1)^2}$ nous obtenons

- $2^g M + 3.2^g S + (2^g - 1)m_{P-Q} + 3(2^g - 1)m$ si les multiplications m sont petites,
- $(2^{g+1} - 1)M + (2^{g+1} + 1)S + (2^g - 1)m_{P-Q} + 2(2^g - 1)m$ sinon.

Ces différentes complexités sont résumées dans le tableau 3.1.

Multiplication

Intéressons nous maintenant au problème du calcul de $[k]P$ sur la variété. Suivant les opérations autorisées (additions, additions différentielles), la complexité des opérations élémentaires et les propriétés de l'entier k, différents algorithmes peuvent être utilisés : on consultera [BZ10, 2.6] par exemple. Leur complexité est toujours en $O\left(n^g \log(k)\right)$ multiplications sur le corps de base. De ce fait, ce qui est intéressant, en pratique, est la constante dans le O.

Pour se fixer les idées, en niveau 4, si nous appliquons l'algorithme d'exponentiation rapide, nous obtenons une complexité de $3 \cdot 16^g M + (4^g - 1)m$ pour chaque bit de k (plus des opérations négligeables). Nous avons supposé que nous faisons le bon choix de a_2 et b_2 tels que $\theta\left[\begin{smallmatrix} a_2 \\ b \end{smallmatrix}\right]_2 (2(z - z'), \Omega) \neq 0$ dès que nous voulons additionner les points correspondants à z et z'. Ceci est vrai pour des points initiaux génériques.

Quand nous voulons utiliser des pseudo-additions, il faut faire attention au fait que les m_{P-Q} dans 3.1 sont en fait des divisions par les coordonnées de $P - Q$. De ce fait, s'il n'est pas possible de précalculer leurs inverses, la complexité de l'algorithme sera élevée.

Tableau 3.2 – Complexité de la multiplication en niveau 2 par bit du multiplieur

	en genre 1	en genre 2	en genre g quelconque
si $m \ll M$	$2M + 9S$ $+1m_P + 3m$	$4M + 12S$ $+3m_P + 6m$	$2^g M + 3.2^g S$ $+(2^g - 1)m_P + 3(2^g - 1)m$
si $m \approx M$	$5M + 5S$ $+1m_P$	$13M + 9S$ $+3m_P$	$(2^{g+2} - 3)M + (2^{g+1} + 1)S$ $+(2^g - 1)m_P$

Parmi les solutions de la page 66, la meilleure va consister à imposer que la différence des points soient toujours un point connu initialement (et dont nous avons précalculé les inverses des coordonnées). Par exemple, dans les chaînes de Lucas binaires 13, nous précalculons les inverses des coordonnées du point

$$[n+1]\,P - [n]P = P.$$

Un autre avantage à utiliser ces chaînes est que si aucune des coordonnées initiales de P n'est nulle alors les formules de Gaudry 3.2.4 sont toujours utilisables. En effet ces chaînes garantissent que les différences dans l'algorithme de pseudo-addition sont égales au point P initial dont les coordonnées sont inversibles. La complexité de l'algorithme est donc de $2^g M + 3.2^g S + (2^g - 1)m_P + 3(2^g - 1)m$ ou de $(2^{g+1} - 1)M + (2^{g+1} + 1)S + (2^g - 1)m_P + 2(2^g - 1)m$ par bit du multiplieur (voir le tableau 3.2).

On peut comparer ces résultats aux calculs effectués avec l'algorithme de Cantor 2.2.3 ou avec les résultats de [Duq04]. Dans le cas du genre 2, la complexité de la multiplication par bit du multiplieur est

- de $4M + 12S + 3m_P + 6m$ pour les fonctions thêta de niveau 2,
- de $52M$ avec les formules de Duquesne sur la surface de Kummer,
- au alentour de $50M$ avec les coordonnées de Mumford (cette complexité dépend des hypothèses faite sur la forme de la courbe, du coût relatif des différentes opérations...).

En conclusion travailler sur la surface de Kummer en genre 2 avec les fonctions thêta est compétitif par rapport aux autres algorithmes.

3.3 Coordonnées de Mumford versus coordonnées thêta

Nous avons présenté rapidement les coordonnées de Mumford dans la section 2.2.3 du chapitre précédent. Comparons les fonctions thêta aux coordonnées de Mumford :

- Les coordonnées thêta peuvent être utilisées pour toute variété abélienne principalement polarisée tandis que les coordonnées de Mumford sont restreintes aux jacobiennes de courbes hyperelliptiques.
- Il y a n^g coordonnées thêta de niveau n (il faut prendre $n = 2$ (surface de Kummer) ou $n \geqslant 4$ pair). En comparaison, pour les coordonnées de Mumford, il n'y a que $2g$ coordonnées à manipuler. Notons que Lubicz et Robert [LR10a] ont introduit des coordonnées compressées mais celle-ci restent bien supérieures en nombre à celles de Mumford. Pour des variétés de petite dimension (cas intéressants en cryptographie), la différence reste raisonnable par rapport aux gains arithmétiques.
- Pour l'arithmétique, en genre petit, les coordonnées thêta sont compétitives avec les coordonnées de Mumford. En genre 2, sur la surface de Kummer, la multiplication est même plus rapide avec les coordonnées thêta de niveau 2 [Gau07].
- Les coordonnées thêta de niveau n encodent une partie (au moins) de la n-torsion de la variété.
- Les coordonnées thêta ne sont a priori pas rationnelles (les points de n-torsion n'étant pas rationnels en général) tandis que celles de Mumford le sont.
- Certains algorithmes ne s'expriment qu'avec les coordonnées thêta (calcul de ℓ-isogénies par exemple).
- Notons également que [LR10b] donne un algorithme pour calculer le couplage de Weil avec les fonctions thêta. Celui-ci semble compétitif par rapport à ceux qui utilisent les coordonnées de Mumford mais nécessiterait une étude plus détaillée.

Les deux systèmes de coordonnées sont donc complémentaires et nous présenterons au chapitre 5 des formules permettant de passer de l'un à l'autre.

Chapitre 4

Factorisation d'entiers

L'algorithme ECM (elliptic curve method) introduit en 1985 par Lenstra [Len87] joue un rôle important pour factoriser des entiers. L'utilisation principale d'ECM est de trouver des facteurs premiers de taille « moyenne » (jusqu'à une soixantaine de décimales) de grands nombres. Il est ainsi utilisé pour le projet Cunningham [1] ou pour les nombres de Fermat. Parmi les succès de ECM, citons la factorisation des nombres de Fermat F_{10} et F_{11} [Bre99]. À ce jour, le plus grand facteur trouvé par ECM est de 73 chiffres décimaux. Il a été trouvé en 2010 par Bos, Kleinjung, Lenstra et Montgomery et il a permis d'achever la factorisation de $2^{1181} - 1$.

Dans la première section, nous présentons le contexte de la factorisation dans lequel rentre l'algorithme ECM. Dans la section suivante, nous présentons l'algorithme ainsi que diverses améliorations. Dans la section 4.3, nous expliquons comment généraliser ECM en utilisant des variétés abéliennes et en particulier des courbes hyperelliptiques de genre 2 (algorithme HECM : hyperelliptic curve method). Puis nous explicitons et étudions une famille de courbes hyperelliptiques de genre 2 utilisable pour HECM. Pour l'étude pratique, nous avons écrit un logiciel GMP-HECM qui est décrit dans la section 4.4. Finalement, dans la section 4.5, nous donnons quelques pistes de recherche pour améliorer HECM.

L'intérêt de ce chapitre est de présenter et d'analyser une version effective d'un algorithme du type ECM utilisant des variétés abéliennes de dimension 2 et qui soit compétitif par rapport à ECM. Ce chapitre est basé sur l'article [Cos10].

Fixons des notations pour ce chapitre. Nous voulons factoriser un entier N impair sans facteur carré. Posons p un facteur premier de N, ce nombre n'étant pas forcément le plus petit facteur de N.

4.1 Multiplication et factorisation

Multiplier deux nombres entiers est une opération rapide aussi bien en pratique qu'en théorie. Algorithmiquement, suivant la taille n des nombres, différentes méthodes pour les multiplier sont utilisées. La complexité de certaines de ces méthodes est donnée dans le tableau 4.1. On consultera la partie 1.3 du livre [BZ10] pour une description et une analyse de ces méthodes. Asymptotiquement la méthode la plus rapide est quasi-linéaire et est due à Fürer [Fü07].

Combinés à une méthode de réduction, ces algorithmes peuvent être utilisés pour multiplier des nombres dans l'anneau $\mathbb{Z}/N\mathbb{Z}$. En effet, les éléments de cet anneau peuvent être représentés par des entiers entre 0 et $N-1$. En supposant les éléments distribués uniformément, leur taille moyenne est $O(\log_2(N))$, c'est-à-dire la même que celle de N. Si N est de taille n la complexité moyenne des algorithmes dans ce cadre est celle donnée par le tableau 4.1. On consultera le chapitre 2 du livre [BZ10] pour une description plus détaillée des différents algorithmes dans ce cadre. En particulier, les différentes façons de représenter les nombres de $\mathbb{Z}/N\mathbb{Z}$ y sont discutées.

1. La page internet du projet est http://homes.cerias.purdue.edu/~ssw/cun/index.html

Algorithme	Complexité
Multiplication triviale	$O\left(n^2\right)$
Karatsuba	$O\left(n^{\log_2(3)}\right)$
Toom-Cook	$O\left(n^{1+\epsilon}\right)$
algorithme FFT	$O\left(n\log(n)\log\left(\log(n)\right)\right)$
Fürer	$n\log(n)2^{O(\log^*(n))}$

Tableau 4.1 – Complexité des algorithmes de multiplications de deux entiers de taille n

Algorithme	Complexité	Complexité dans le pire des cas
Division à essai	$\pi(p) \sim \frac{p}{\log(p)}$	$\pi(\sqrt{N}) \sim O\left(\frac{\sqrt{N}}{\log(N)}\right)$
rho de Pollard	$\tilde{O}\left(\sqrt{p}\right)$	$\tilde{O}\left(\sqrt[4]{N}\right)$
$p-1$	$O\left(\sqrt{q}\right)$ où q est le plus grand facteur de $p-1$	$O\left(\sqrt{N}\right)$
ECM	$O\left(\mathrm{L}_p\left[\frac{1}{2};\sqrt{2}+o(1)\right]\right)$	$\tilde{O}\left(\mathrm{L}_N\left[\frac{1}{2};1\right]\right)$
Crible quadratique		$\mathrm{L}_N\left[\frac{1}{2};1\right]$
Crible algébrique		$\mathrm{L}_N\left[\frac{1}{3};1.902\right]$

Tableau 4.2 – Complexité des algorithmes de factorisation en terme de nombre d'opérations modulo N

Contrairement à la multiplication, l'opération inverse, la factorisation, est en général une opération difficile. À l'heure actuelle, nous ne connaissons pas d'algorithme polynomial en la taille des nombres pour factoriser les entiers. Cette différence de complexité a été exploitée pour construire des protocoles cryptographiques comme RSA [RSA78]. La factorisation est une brique de base de nombreux algorithmes utilisés en théorie des nombres. Parmi ceux-ci citons

- la construction de racines (carrées ou autres) modulo N,
- la décomposition d'un groupe abélien de type fini,
- le calcul de l'anneau des entiers d'un corps de nombres (factorisation du discriminant),
- ...

Asymptotiquement, la complexité des algorithmes est donnée dans le tableau 4.2 où nous utilisons la fonction $\mathrm{L}_N\left[\alpha;c\right]$ définie par

$$\mathrm{L}_N\left[\alpha;c\right] = \exp\left(c\log(N)^\alpha \log(\log(N))^{1-\alpha}\right)$$

et où $\pi(x)$ est le nombre de premiers inférieurs à x. Pour certains algorithmes, leur complexité dépend de la taille du plus facteur premier p de N (rappelons que p est inconnu). Dans le pire des cas, p est de l'ordre de $\sqrt{N}$.

Étant donné un nombre à factoriser, la méthode classique consiste à utiliser la division triviale puis des algorithmes du type $p-1$, $p+1$ et ECM pour « nettoyer » les petits et moyens facteurs du nombre. En effet, les entiers de très grande taille peuvent avoir des facteurs de petite taille. Une fois ceux-ci « nettoyés », si la taille du nombre restant est raisonnable (le record actuel est la factorisation d'un nombre RSA de 768 bits [KAF+10]) nous utilisons le crible quadratique ou algébrique [Mon94]. Ces derniers ont la meilleure complexité asymptotique connue. Dans le cas où la taille du nombre restant à factoriser est trop élevée, nous continuons d'utiliser des algorithmes du type ECM en espérant que les facteurs premiers du nombre ne soient pas trop grands.

Algorithme 16 $p-1$

Entrée: étant donnés deux entiers positifs N et B_1.
Sortie: S'il existe, un facteur de p tel que $p-1$ soit B_1-friable

1: Choisir au hasard a modulo N premier avec N.
2: Calculer a^k modulo N avec $k = \text{ppcm}\,(2,\ldots,B_1)$.
3: Calculer $\text{pgcd}(a^k-1, N)$

Dans la section suivante, nous présentons plus en détails les algorithmes $p-1$ et ECM et nous étudions leur complexité. Dans la section 4.3.1, nous présentons une généralisation d'ECM utilisant les variétés abéliennes, le but étant d'obtenir un algorithme de complexité similaire. Notons que les algorithmes de crible nécessitent de trouver des nombres friables et pour cela utilisent ECM [Kru08, Kru10]. Dans ce cadre, les nombres à factoriser sont beaucoup plus petits et l'analyse de complexité est très différente : les précalculs ne sont plus négligeables. Nous ne nous sommes pas intéressés à cette application.

4.2 L'algorithme ECM

4.2.1 Contexte

L'algorithme ECM généralise l'algorithme $p-1$ de Pollard [Pol74] dont voici une description. Prenons un entier a premier avec N (nous choisissons a modulo N au hasard et nous calculons $\text{pgcd}(a,N)$, si celui-ci n'est pas égal à 1 alors nous avons un facteur de N). Comme $a^{p-1} \equiv 1\,[p]$ par le petit théorème de Fermat, alors, pour tout multiple k de $p-1$, le calcul de $\text{pgcd}(a^k-1,N)$ donne un facteur de N (sauf dans le cas où a^k est congru à 1 modulo tous les facteurs de N).
En pratique, nous ne connaissons pas p et nous prenons k comme étant le produit d'un grand nombre de facteurs en espérant que ceux de $p-1$ sont parmi ceux-ci. Prenons $k = \text{ppcm}\,(2,\ldots,B_1)$ pour une certaine borne B_1 fixée. La méthode réussit si $p-1$ est B_1-friable c'est-à-dire produit de petits nombres premiers. Si ce n'est pas le cas nous pouvons augmenter B_1 mais cela augmente le temps de calcul.

Définition 4.2.1. *Soit n un entier dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1}\ldots p_r^{\alpha_r}$. Le nombre n est dit B_1-friable si et seulement si les $p_i^{\alpha_i}$ sont inférieurs à B_1.*

Une idée naturelle est d'étendre l'algorithme $p-1$ avec d'autres groupes que $(\mathbb{Z}/N\mathbb{Z})^*$. La méthode $p+1$, introduite par Williams [Wil82], utilise le groupe

$$\mathbb{Z}/N\mathbb{Z}[X]/\left(X^2 - SX + 1\right)$$

où S est un élément quelconque de $\mathbb{Z}/N\mathbb{Z}$. Si le polynôme X^2-SX+1 est scindé alors $p+1$ se comporte comme $p-1$. Sinon, le polynôme est irréductible et nous retrouvons le facteur p si $p+1$ est friable. La probabilité d'être dans chacun des deux cas précédents est de $\frac{1}{2}$.
Bach et Shallit [BS89] ont généralisé ces deux algorithmes en utilisant les polynômes cyclotomiques. Lenstra [Len87] a proposé d'utiliser le groupe des points sur une courbe elliptique. Cet algorithme est appelé ECM pour elliptic curve method.

Définissons les courbes elliptiques sur l'anneau $\mathbb{Z}/N\mathbb{Z}$. Pour plus de détails, on pourra consulter [Len87].

Définition 4.2.2. *Soient n et N deux entiers. L'espace projectif $\mathbb{P}^n(\mathbb{Z}/N\mathbb{Z})$, est*

$$\mathbb{P}^n\left(\mathbb{Z}/N\mathbb{Z}\right) = \left\{(x_0,\ldots,x_n) \in \left(\mathbb{Z}/N\mathbb{Z}\right)^{n+1},\ \textit{tel que l'idéal engendré par les } x_i \textit{ est } \mathbb{Z}/N\mathbb{Z}\right\}/\simeq$$

où $\simeq$ est la relation d'équivalence suivante :

$$(x_0,\ldots,x_n) \simeq (y_0,\ldots,y_n) \iff \exists \lambda \in (\mathbb{Z}/N\mathbb{Z})^*\ \ \forall i,\ x_i = \lambda y_i$$

Algorithme 17 ECM : phase 1

Entrée: Étant donnés deux entiers positifs N et B_1.
Sortie: Un facteur de N.

1: Choisir au hasard une courbe elliptique $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$ et un point P dessus.
2: Calculer $[k]P$ avec $k = \text{ppcm}\,(2, \ldots, B_1)$.
3: Espérer que $[k]P = \mathcal{O}_\mathcal{E} \mod p$ pour obtenir le facteur p.
4: Sinon revenir à la première étape.

Soit p un facteur de N, la réduction modulo p définit une application de $\mathbb{P}^n(\mathbb{Z}/N\mathbb{Z})$ dans $\mathbb{P}^n(\mathbb{F}_p)$. Nous considérons les éléments $(x, y, z) \in \mathbb{P}^2(\mathbb{Z}/N\mathbb{Z})$ qui vérifient $y^2z = x^3 + axz^2 + z^3$. Le discriminant $-16(4a^3 + 27b^2)$ est supposé être un inversible de $\mathbb{Z}/N\mathbb{Z}$ et dans ce cas nous disons que la courbe $\mathcal{E}$ ainsi définie est une courbe elliptique sur l'anneau $\mathbb{Z}/N\mathbb{Z}$.

La réduction modulo p est un morphisme naturel π_p de $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ dans $\mathcal{E}(\mathbb{F}_p)$. Ce morphisme est théorique car nous ne connaissons pas les facteurs de N. Il est possible de définir une « loi d'addition » sur les points de cette courbe : nous la définissons avec les formules classiques quand cela est possible. Cependant la « somme » de deux points n'est plus forcément bien définie. Si la somme $P + Q$ de deux points P et Q de $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ est bien définie alors les images de ces points existent dans $\mathcal{E}(\mathbb{F}_p)$ et la réduction modulo p de $P + Q$ est la somme des réductions modulo p des points P et Q. C'est-à-dire que

$$\pi_p(P + Q) = \pi_p(P) + \pi_p(Q).$$

En pratique, nous travaillons sur $\mathbb{Z}/N\mathbb{Z}$ comme si c'était un corps. La seule opération de corps qui n'existe pas dans $\mathbb{Z}/N\mathbb{Z}$ est l'inversion modulaire. Celle-ci est calculée par l'algorithme d'Euclide étendu et si une inversion échoue, nous obtenons un facteur de N.

Remarque 4.2.3. *Il n'est pas possible de prendre des racines carrées modulo le nombre N à factoriser. En effet prendre une racine carrée modulo N est équivalent à la factorisation de N : si nous savons factoriser N alors il est possible de calculer la racine carrée d'un nombre modulo tous les facteurs de N puis de reconstruire la racine avec des restes chinois. Dans l'autre sens, supposons donné un algorithme permettant de prendre des racines carrées modulo N. Nous appliquons cet algorithme sur $b^2 \mod N$ pour obtenir un élément a tel que $a^2 = b^2 \mod N$. Le calcul de $\gcd(a - b, N)$ a alors une grande probabilité de donner un facteur de N.*

Cette remarque est d'ailleurs utilisée dans les algorithmes de cribles quadratique et algébrique où le but est de construire une relation $a^2 = b^2 \mod N$.

Soit P un point d'une courbe elliptique $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$. L'objectif de l'algorithme, et c'est en ce sens qu'il généralise $p - 1$, est de calculer $[k]P$ dans $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ pour un certain entier k et un certain point P de $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ et nous espérons obtenir le zéro $\mathcal{O}_\mathcal{E}$ de $\mathcal{E}(\mathbb{F}_p)$.

4.2.2 Description générale de l'algorithme ECM

Soit P un point d'une courbe elliptique $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$ et soit $k = \text{ppcm}\,(2, \ldots, B_1)$. Nous calculons le point $[k]P$ dans $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ et nous espérons que ce point s'envoie sur le zéro de la courbe $\mathcal{E}(\mathbb{F}_p)$. Cette étape est appelée phase 1 et est résumée dans l'algorithme 17.
Il existe une extension aux algorithmes de type $p - 1$ qui est appelée « phase 2 » ou « étape 2 ». Cette deuxième phase a été proposée par Brent [Bre86] et Montgomery [Mon87]. En particulier ce dernier article donne une description unifiée de la phase 2 pour les algorithmes $p - 1$, $p + 1$ et ECM.
L'idée générale de la phase 2 est la suivante : soit Q le résultat de la première phase, nous calculons πQ pour tout nombre premier π entre B_1 et B_2 et nous espérons qu'un des πQ est le zéro du groupe dans lequel nous travaillons. De ce fait, nous autorisons le cardinal du groupe à être B_1, B_2-friable :

Définition 4.2.4. *Soit n un entier dont la décomposition en facteur premiers est $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Le nombre n est dit B_1, B_2-friable si et seulement si nous sommes dans un des deux cas suivants*

– $p_i^{\alpha_i} \leq B_1$ *pour tout* $1 \leq i \leq r$,
– $p_i^{\alpha_i} \leq B_1$ *pour tout* $1 \leq i \leq r-1$, $\alpha_r = 1$ *et* $B_1 < p_r \leq B_2$.

Il existe différentes méthodes pour éviter de calculer tous les πQ. Une description générale de ces méthodes se trouve dans [ZD06, Kru10]. Nous ne décrivons pas plus en détail la phase 2 car, pour des raisons données ultérieurement, nous ne l'utilisons pas dans nos algorithmes.

La correction de l'algorithme ECM vient du fait que si $[k]P = \mathcal{O}_{\mathcal{E}} \mod p$ alors, lors de ce calcul, une des divisions va échouer. Les divisions étant calculées par l'algorithme d'Euclide étendu, nous obtenons un diviseur de N si une d'elles échoue.
L'intérêt d'ECM par rapport à $p-1$ est que le cardinal du groupe dans lequel nous travaillons n'est plus totalement déterminé par p. Si le cardinal de la variété abélienne modulo p est friable alors nous obtenons un facteur de N sinon il est possible de recommencer avec une autre courbe. La borne de friabilité B_1 est choisie en fonction de la taille du facteur que nous voulons trouver pour avoir un compromis entre le calcul de $[k]P$ (les autres étapes étant négligeables) et le nombre de fois qu'il faut recommencer l'algorithme. La borne B_2 est telle que le temps de calcul de la phase 2 est approximativement le même que celui de la phase 1.

L'algorithme ECM est un algorithme de factorisation probabiliste dont la complexité est de

$$O\left(\mathrm{L}_p\left[\frac{1}{2}; \sqrt{2}+o(1)\right] M\left(\log(N)\right)\right)$$

et $M(\log(N))$ est la complexité de la multiplication modulo N. La complexité de ECM est dominée par la taille du plus petit facteur p de N plutôt que celle de N. Rappelons que ECM ne trouve pas forcément le plus petit facteur de N. Dans le pire des cas, c'est-à-dire quand p est de l'ordre de $\sqrt{N}$, la complexité de ECM est de $\tilde{O}\left(\mathrm{L}_N\left[\frac{1}{2}; 1\right]\right)$ ce qui est bien plus élevé que le crible algébrique.

La phase 2 permet de gagner un facteur $\log(p)$ dans le O. Asymptotiquement l'utilisation de la phase 2 n'améliore donc pas beaucoup la complexité. Cependant, en pratique, elle permet d'augmenter de manière significative la probabilité de succès d'une courbe.

Le cardinal du groupe dans lequel nous travaillons est donné par les conjectures de Hasse-Weil.

Théorème 4.2.5 (Hasse-Weil)**.** *Soit $\mathcal{C}$ une courbe de genre g sur $\mathbb{F}_q$ alors*

$$\left(\sqrt{q}-1\right)^{2g} \leq \#\operatorname{Jac}_{\mathbb{F}_q}(\mathcal{C}) \leq \left(\sqrt{q}+1\right)^{2g}.$$

Ainsi pour les courbes elliptiques, leur cardinal se trouve dans l'intervalle $\left[p+1-2\sqrt{p}, p+1+2\sqrt{p}\right]$ (page 15, nous avions précisé la distribution de ces nombres).

4.2.3 Améliorations de l'algorithme ECM

Plusieurs améliorations de l'algorithme ECM sont possibles. Tout d'abord, toute amélioration (pratique ou théorique) sur l'arithmétique modulaire permet de diminuer le facteur $O\left(M(\log(n))\right)$; nous n'y reviendrons pas. À l'opposé, les améliorations mathématiques et algorithmiques travaillent sur le facteur $O\left(\mathrm{L}_p\left[\frac{1}{2}; \sqrt{2}+o(1)\right]\right)$. Les principales améliorations consistent à
– Accélérer l'arithmétique sur les courbes.
– Augmenter la probabilité de succès en utilisant des courbes plus « chanceuses ».
Ces deux pistes de recherche sont liées. En effet, améliorer l'arithmétique sur les courbes elliptiques, revient souvent à choisir des modèles particuliers des courbes. Les meilleures courbes pour ECM sont alors différentes suivant les familles.

Différents modèles de courbes elliptiques ont été proposés, et pour chacun d'entre eux, nous disposons de différentes formules pour calculer la loi de groupe. Le site internet EFD [2] rassemble la plupart des

2. http://www.hyperelliptic.org/EFD/index.html

formules de la littérature et donne leur complexité. Dans le cadre d'ECM, deux modèles sont particulièrement intéressants : celui de Montgomery et celui d'Edwards.

Décrivons plus en détail les courbes de Montgomery car leur arithmétique ressemble à celle que nous utilisons. Ces courbes sont en particulier utilisées dans le logiciel GMP-ECM. Pour les courbes d'Edwards, nous renvoyons à [BBLP10]. Une courbe sous forme de Montgomery est une courbe projective d'équation

$$\mathcal{E}: \ by^2z = x\left(x^2 + axz + z^2\right).$$

Il faut supposer que $a^2 \neq 4$ et $b \neq 0$. Le zéro de la courbe est le point à l'infini $(0:1:0)$. En ignorant la coordonnée y des points, nous identifions un point et son opposé, c'est-à-dire que nous travaillons sur $\mathcal{E}/\{\pm 1\}$. Nous avons alors les formules suivantes pour l'arithmétique (où nous posons $d = (a+2)/4$) :

$$x_{2P} = (x_P + z_P)^2, \qquad z_{2P} = 4x_P z_P\left((x_P - z_P)^2 + 4dx_P z_p\right),$$

$$x_{P+Q} = 4z_{P+Q}\left(x_P x_Q - z_P z_Q\right)^2, \qquad z_{P+Q} = 4x_{P-Q}\left(x_P z_Q - z_P x_Q\right)^2$$

Le doublement peut se calculer avec 3 multiplications et 2 carrés. Tandis que la pseudo-addition coûte 4 multiplications et 2 carrés. Pour calculer un multiple d'un point, nous utilisons les chaînes de Lucas avec l'algorithme PRAC de Montgomery. En effet, à la différence des formules de pseudo-additions avec les fonctions thêta 3.2.2, les formules de Montgomery n'utilisent aucune division. Le calcul de $[k]P$ se fait alors en à peu près $6M + 3S$ par bit de k [ZD06].

Une courbe elliptique est « chanceuse » pour ECM si son cardinal est friable. Celui-ci est un entier de l'ordre de p d'après le théorème 4.2.5.
Pour améliorer la probabilité de succès, une solution consiste à forcer l'ordre du groupe des points sur les courbes elliptiques sur $\mathbb{F}_p$ à être divisible par un entier m. La probabilité que le cardinal de la courbe soit friable n'est plus celle qu'un entier de taille $\log(p)$ soit friable mais celle qu'un entier de taille $\log(p/m)$ le soit. De ce fait, la probabilité de succès est un peu plus élevée.

Les courbes elliptiques utilisées dans ECM sont souvent la réduction modulo N de courbes définies sur $\mathbb{Q}$. De même, le point P provient de la réduction d'un point de $\mathcal{E}(\mathbb{Q})$. Le théorème de Mazur limite cependant le groupe de torsion $\mathcal{E}_{tor}(\mathbb{Q})$ d'une courbe elliptique sur $\mathbb{Q}$:

Théorème 4.2.6 (Mazur)**.** *Le groupe de torsion d'une courbe elliptique sur $\mathbb{Q}$ est isomorphe à l'un des groupes suivant :*

$$\mathcal{E}_{tor}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 4 \end{cases}$$

Par exemple, pour la paramétrisation de Suyama [Suy85], nous posons σ aléatoire et nous calculons

$$u = \sigma^2 - 5, \quad v = 4\sigma, \quad a = \frac{(v-u)^3(3u+v)}{4u^3v}, \quad b = u/v^3.$$

Le point

$$P = \left(\frac{u^3}{v^3}, \frac{\left(\sigma^2-1\right)\left(\sigma^2-25\right)\left(\sigma^4-25\right)}{v^3}\right)$$

est alors sur la courbe

$$b\,y^2 = x^3 + a\,x^2 + x.$$

et est d'ordre infini dessus. Cette forme de courbe impose que le cardinal de la courbe sur $\mathbb{F}_p$ soit divisible par 12 pour presque tout p. Les courbes de Suyama sont un cas particulier des courbes de Montgomery et elles sont en particulier utilisées par GMP-ECM [ZD06].
Dans sa thèse [Mon92], Montgomery décrit des paramétrisations donnant des courbes ayant 12 ou 16 points de torsions sur $\mathbb{Q}$. On pourra également consulter [AM93].
Au lieu de chercher à avoir des courbes ayant un groupe de torsion fixé sur $\mathbb{Q}$ ou sur tous les $\mathbb{F}_p$, nous pouvons chercher des courbes ayant une bonne probabilité d'avoir de la torsion modulo p quand ce dernier

varie. Bărbulescu [Băr09] décrit une méthode pour étudier la valuation moyenne modulo p du cardinal des courbes elliptiques.

Pour des nombres N particuliers, nous savons que certains éléments sont des carrés. Par exemple pour $N = a^{2n} + 1$ alors -1 est le carré de a^n modulo tous les facteurs de N. Pour des N de ce type, nous pouvons construire nos courbes comme la réduction modulo N de courbes définies sur des corps de nombres [BC10]. L'équivalent du théorème de Mazur sur les corps de nombres montre qu'il existe des courbes ayant des groupes de torsion plus gros que les courbes sur $\mathbb{Q}$. La probabilité de succès de ECM avec ces courbes est donc plus élevée.

Il n'est pas possible de prendre un point P au hasard sur la courbe $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$. En effet, pour ce faire, il faudrait prendre une racine carrée, ce qui n'est pas possible. Le point P doit donc être construit directement sur $\mathcal{E}(\mathbb{Q})$ et doit être d'ordre infini sur cette courbe. En effet, sinon nous aurions une relation du type $mP = O$ sur $\mathcal{E}(\mathbb{Q})$ et donc sur $\mathcal{E}(\mathbb{F}_p)$ pour tout facteur p de N. De ce fait, nous ne pourrions pas retrouver les facteurs de N. La courbe elliptique sur $\mathbb{Q}$ doit donc être de rang strictement positif.

Signalons que les différentes méthodes utilisées dans la phase 2 demandent de savoir faire de vraies additions sur la courbe elliptique. De ce fait nous demandons que la donnée initiale de la phase 2 soit un vrai point de la courbe elliptique. Montrons comment transformer une classe $(x_1 :: z_1)$ sur la courbe

$$\kappa z y^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3$$

provenant de la phase 1 en un vrai point (x_2, y_2) d'une courbe

$$y^2 = x^3 + Ax + B$$

sans modifier l'ordre du point. Rappelons que la notation $(x :: z)$ signifie que nous avons identifié les points $(x : y : z)$ et son opposé $(x : -y : z)$.

Nous commençons par translater le point par $x \mapsto x - a_2 z/3$ avant de diviser sa coordonnée x par z pour obtenir le point $(x'_1, ?)$ sur la courbe $\kappa y^2 = f(x) = x^3 + a'_4 x + a'_6$. Les points $(x'_1, \pm 1)$ sont alors sur la courbe

$$D y^2 = f(x) = x^3 + a'_4 x + a'_6 \quad \text{avec } D = f(x'_1)\,.$$

Par le changement de variables

$$(x, y) \longmapsto \left(\frac{x}{D}, \frac{y}{D}\right),$$

nous obtenons un point de la courbe $y^2 = x^3 + Ax + B$ où $A = a'_4/D^2$ et $B = a_6/D^3$. Remarquons que le signe ± 1 peut être choisi arbitrairement car un point et son opposé ont le même ordre.

4.3 Algorithme HECM

4.3.1 Généralisation d'ECM avec des variétés abéliennes

Il est possible de généraliser l'algorithme ECM en remplaçant les courbes elliptiques par des variétés abéliennes générales. Cette idée avait été proposée par Lenstra, Pila, Pomerance [LPP93, LPP02, LP92] dans le but d'avoir un algorithme prouvé. En comparant les variétés abéliennes de dimension g et les courbes elliptiques, deux problèmes apparaissent :

- L'arithmétique est plus lente sur les variétés abéliennes générales.
- Le cardinal du groupe dans lequel nous travaillons (donné par les conjectures de Hasse-Weil 4.2.5) est plus élevé et de ce fait la probabilité de succès est moins bonne.

Pour résoudre le premier problème, la meilleure arithmétique sur les variétés abéliennes principalement polarisées est donnée par les fonctions thêta de niveau 2 (voir le tableau 3.1). Nous voyons que la complexité des opérations croît en $O(2^g)$. Contrairement aux autres applications cryptographiques où augmenter la dimension permet de réduire la taille du corps, dans ECM, la taille du « corps » est fixée, et donc augmenter la dimension fait croître le cardinal de la variété.

Les frères Chudnovsky [CC86] proposent de travailler sur des produits de courbes elliptiques : supposons

que la variété A ne soit pas irréductible (ou plus généralement qu'elle ne soit pas simple), c'est-à-dire que nous avons un morphisme

$$A \longrightarrow A_1 \times \ldots \times A_n$$

de la variété A dans un produit de variétés de dimension plus petite. Au lieu de chercher à trouver le zéro de $A(\mathbb{F}_p)$, nous allons essayer de trouver celui d'une des variétés $A_i(\mathbb{F}_p)$. En supposant que les variétés A_i sont indépendantes, la probabilité de succès de l'algorithme ECM sur A sera alors la somme de celles sur les A_i. Il est clair que l'optimal est de prendre des A_i de dimension la plus petite possible, c'est-à-dire des courbes elliptiques. L'algorithme obtenu reviendra à effectuer g algorithmes ECM classiques en parallèle et la probabilité de succès sera alors g fois celle de l'algorithme ECM.
Pour cette variante d'ECM, il faut donc se poser la question du rapport entre la complexité des opérations sur la variété (qui est en $O(2^g)$) et la dimension g. Seuls deux cas sont donc intéressants : la dimension 1 (ECM classique) et la dimension 2.

En dimension 2, toute variété abélienne A principalement polarisée et irréductible est la jacobienne d'une courbe hyperelliptique. La propriété que la variété soit non simple se traduit alors par les cas suivants

- la variété est isomorphe au produit de deux courbes elliptiques,
- la courbe hyperelliptique est décomposable (l'isogénie étant de type (d_1, d_2) avec les $d_i > 1$).

Soit $\Omega \in \mathcal{H}_g$ la matrice des périodes associée à la variété et soient τ_1 et τ_2 celles des courbes elliptiques. Si la variété est isomorphe au produit de ces deux courbes elliptiques, la matrice Ω est de la forme (possiblement, après un isomorphisme) :

$$\Omega = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}.$$

Posons

$$z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{C}^2,$$

les fonctions thêta sur le tore $\mathbb{C}^2/\Omega\mathbb{Z}^2 + \mathbb{Z}^2$ sont alors données comme des produits des fonctions thêta associées aux tores $\mathbb{C}/\tau_i\mathbb{Z} + \mathbb{Z}$. Ainsi,

$$\begin{array}{rcll}
\theta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0) \end{smallmatrix} \right](z,\Omega) & = & \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right](z_1,\tau_1) & \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right](z_2,\tau_2) \\
\theta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2}) \end{smallmatrix} \right](z,\Omega) & = & \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right](z_1,\tau_1) & \theta \left[\begin{smallmatrix} 0 \\ \frac{1}{2} \end{smallmatrix} \right](z_2,\tau_2) \\
\theta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0) \end{smallmatrix} \right](z,\Omega) & = & \theta \left[\begin{smallmatrix} 0 \\ \frac{1}{2} \end{smallmatrix} \right](z_1,\tau_1) & \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right](z_2,\tau_2) \\
\theta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{smallmatrix} \right](z,\Omega) & = & \theta \left[\begin{smallmatrix} 0 \\ \frac{1}{2} \end{smallmatrix} \right](z_1,\tau_1) & \theta \left[\begin{smallmatrix} 0 \\ \frac{1}{2} \end{smallmatrix} \right](z_2,\tau_2)
\end{array}$$

Notons leur carré (c'est-à-dire les fonction thêta de niveau 2) par X, Y, Z, T. Elles vérifient la relation $XY = ZT$. Les fonctions thêta $\theta \left[\begin{smallmatrix} a \\ 0 \end{smallmatrix} \right](2z, 2\Omega)^2$ de la variété isogène dans les formules de Gaudry [Gau07] vérifient le même type d'équation.

De manière générale, pour considérer tous les cas, il faut considérer les classes $(\Omega, 2\Omega)$ modulo isomorphisme (c'est-à-dire la variété et une variété 2-isogène). Il faut donc considérer l'action de $\Gamma_2 \backslash \mathrm{Sp}(4, \mathbb{Z})$ d'après la discussion page 27. Nous obtenons cependant toujours la même équation $xy = zt$ pour la variété et sa variété isogène. Par contre les fonctions thêta de la variété et celles des courbes elliptiques sous-jacentes sont différentes. Il est aisé de se rendre compte qu'il n'est pas possible de tricher :

- la probabilité de succès est la somme de celle des deux courbes.
- L'arithmétique est exactement deux fois plus lente que celle sur les courbes elliptiques (avec les fonctions thêta de niveau 2 sur ces courbes).

Avec les courbes décomposables, nous pouvons espérer avoir plus de marge de manœuvre. Nous appelons l'algorithme ainsi obtenu HECM pour hyperelliptic curve method.

Plusieurs solutions sont possibles pour construire des courbes hyperelliptiques $\mathcal{C}$ telles qu'il existe deux courbes elliptique $\mathcal{E}_i$ avec $\mathrm{Jac}(\mathcal{C})$ isogène aux produit de ces courbes. Nous pouvons construire $\mathcal{C}$ sous forme de Weierstraß $y^2 = f(x)$ et regarder les conditions imposées sur les coefficients de f pour qu'elle soit décomposable. Une autre solution consiste à exprimer les fonctions thêta associées à $\mathrm{Jac}(\mathcal{C})$ en fonction de celles associées aux courbes elliptiques sous-jacentes.

Nous avons choisi la première solution car elle permettait d'utiliser les résultats se trouvant dans la littérature et, de plus, elle impose des conditions sur la torsion des courbes elliptiques. La seconde solution serait sans doute plus adaptée pour une étude exhaustive des différentes possibilités de paramétrisation.

Après avoir présenté plus en détail les courbes décomposables dans la section 4.3.2, nous présentons, dans la section 4.3.3, une paramétrisation permettant d'appliquer l'algorithme HECM. Pour cette paramétrisation, nous étudions alors la torsion sur les courbes elliptiques (section 4.3.4). Une amélioration consiste à utiliser de petits paramètres (section 4.3.5).

4.3.2 Courbes décomposables

Définition 4.3.1. *Une courbe hyperelliptique de genre* 2 *est dite décomposable s'il existe une isogénie* ϕ *de* $\mathrm{Jac}(\mathcal{C})$ *dans le produit de deux courbes elliptiques* $\mathcal{E}_i$ *:*

$$\phi : \quad \mathrm{Jac}\,(\mathcal{C}) \longrightarrow \mathcal{E}_1 \times \mathcal{E}_2.$$

Si le noyau de l'isogénie est $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$*, la courbe est dite* (n, n)*-décomposable.*

De nombreuses études ont été faites sur les courbes (n, n)-décomposables. Citons [Kuh88, Sat01, Sha01, Sha05] qui donnent des méthodes pour les étudier. L'idée générale de ces approches consiste à étudier la ramification des injections entre les corps de fonctions. Pour un entier k fixé, nous obtenons alors la forme que doit avoir une courbe (n, n)-décomposable. En particulier, pour les courbes $(3, 3)$-décomposables, on pourra consulter [Sha02, Sha04].
Nous ne nous intéressons qu'aux courbes $(2, 2)$-décomposables car les conditions sont les plus simples. Dans ce cas, Gaudry et Schost [GS01] ont montré le théorème suivant en utilisant une approche basée sur les automorphismes de la courbe [Igu60].

Théorème 4.3.2. *Soit* $\mathcal{C}$ *une courbe hyperelliptique de genre* 2 *sur un corps* k *donnée par l'équation*

$$\kappa y^2 = x\,(x-1)\,(x-\lambda)\,(x-\mu)\,(x-\nu)$$

où λ*,* μ*,* ν *sont les invariants de Rosenhain de la courbe et où* κ *est un élément de* k*. La courbe* $\mathcal{C}$ *est* $(2, 2)$*-décomposable si et seulement si ses invariants de Rosenhain vérifient*

$$\lambda = \mu \frac{1-\nu}{1-\mu}.$$

Les deux courbes elliptiques sous-jacentes ont alors pour équation

$$\chi\kappa\, y^2 = (x-1)\left(x - x_2^2\right)\left(x - x_3^2\right)$$

avec

$$q = \pm\sqrt{\mu\,(\mu-\nu)}, \qquad x_2 = \frac{\mu+q}{\mu-q}, \qquad x_3 = \frac{1-\mu-q}{1-\mu+q}, \qquad \chi = -q\,\mu\,(\mu-1)\,.$$

L'élément κ permet de traiter la courbe et ses tordues avec la même équation. En effet les tordues quadratiques de la courbe $y^2 = f(x)$ sont les courbes d'équations $\kappa y^2 = f(x)$ où κ décrit un système de représentant de k^*/k^{*2}.
Sur un corps non algébriquement clos, les invariants de Rosenhain peuvent ne pas être rationnels. De ce fait, une courbe $(2, 2)$-décomposable peut avoir différentes équations. Pour avoir une équation plus générale, il faut utiliser plutôt les méthodes reposant sur les corps de fonctions.
Soit $\mathcal{C}$ est une courbe $(2, 2)$-décomposable donnée par le théorème. Les courbes elliptiques sous-jacentes

sont rationnelles si et seulement si $\mu(\mu-\nu)$ est un carré. Les morphismes entre la courbe hyperelliptique et les courbes elliptiques sont définis sur $k(q)$ et donnés par

$$(x,y) \longmapsto \left(\left(\frac{x-\mu-q}{x-\mu+q} \right)^2, \frac{w\,y}{(x-\mu+q)^3} \right) \text{ avec } w = \frac{8q}{(\mu-q)(-1+\mu-q)}.$$

Soit f l'application allant de $\mathcal{C}$ dans le produit des deux courbes elliptiques $\mathcal{E}_1 \times \mathcal{E}_2$. Le morphisme f s'obtient en prenant le produit des deux morphismes donnés précédemment. Le poussé en avant f_* de f est défini par

$$f_* : \quad \begin{cases} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathrm{Jac}(\mathcal{E}_1) \times \mathrm{Jac}(\mathcal{E}_2) \\ \displaystyle\sum_{i=1}^{r} P_i - rP_\infty & \longmapsto & \displaystyle\sum_{i=1}^{r} f(P_i) - r\,f(P_\infty) \end{cases}$$

où nous posons que $f(P_\infty) = (\mathcal{O}_{\mathcal{E}_1}, \mathcal{O}_{\mathcal{E}_2})$ est le couple des zéros des deux courbes elliptiques. Remarquons que les diviseurs sur la jacobienne des courbes elliptiques ne sont pas réduits. Pour une courbe elliptique, la jacobienne de la courbe est isomorphe à l'ensemble des points sur la courbe, de ce fait, nous pouvons identifier $\mathrm{Jac}(\mathcal{E}_i)$ avec $\mathcal{E}_i$. L'application f_* devient

$$f_* : \quad \begin{cases} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathcal{E}_1 \times \mathcal{E}_2 \\ \displaystyle\sum_{i=1}^{r} P_i - rP_\infty & \longmapsto & \displaystyle\sum_{i=1}^{r} f(P_i) \end{cases}$$

Un diviseur générique D appartenant à la jacobienne d'une courbe de genre 2 peut s'écrire comme la somme formelle $D = P_1 + P_2 - 2P_\infty$. En général, nous aurons à additionner les deux points $f(P_1)$ et $f(P_2)$ sur les courbes elliptiques.

Si nous partons de $\mathrm{Jac}(\mathcal{C})/\{\pm 1\}$, alors nous ne pouvons calculer que les coordonnées x des images $f(P_i)$ des points. Rappelons que nous ne voulons pas prendre de racine carrée et donc que nous ne pouvons pas avoir les coordonnées y des points ce qui est nécessaire pour additionner ou doubler deux points en coordonnées de Weierstraß. En pratique, pour faire cette opération, nous pouvons soit utiliser des formules d'addition complètes (ou presque complètes) telles que celles fournies par les courbes d'Edwards ou de Jacobi. Une autre solution consiste à travailler dans une algèbre de dimension 4 sur le « corps » $\mathbb{Z}/N\mathbb{Z}$.

Dans HECM, nous utilisons les fonctions thêta de niveau 2 pour accélérer l'arithmétique de la jacobienne de la courbe hyperelliptique. Soit $\mathcal{K}$ la variété définie par ces fonctions. La surface de Kummer $\mathcal{K}$ est isomorphe à la variété $\mathrm{Jac}(\mathcal{C})/\{\pm 1\}$ sur la clôture algébrique du corps. Posons

$$\psi : \qquad \mathrm{Jac}(\mathcal{C})/\{\pm 1\} \longrightarrow \mathcal{K}$$

Sur des corps finis, soit $\tilde{\mathcal{C}}$ la tordue quadratique de la courbe $\mathcal{C}$. Notons $\tilde{\psi}$ l'application de $\mathrm{Jac}(\tilde{\mathcal{C}})$ dans $\mathcal{K}$. Comme ψ, le morphisme $\tilde{\psi}$ est rationnel sur le corps de base et est un isomorphisme sur la clôture algébrique. Sur le corps de base, nous avons que $\mathrm{Jac}(\mathcal{C})/\{\pm 1\}$ et $\mathrm{Jac}(\tilde{\mathcal{C}})/\{\pm 1\}$ sont toutes les deux incluses dans $\mathcal{K}$:

$$\mathcal{K} = \psi\Big(\mathrm{Jac}(\mathcal{C})/\{\pm 1\}\Big) \bigcup \tilde{\psi}\left(\mathrm{Jac}(\tilde{\mathcal{C}})/\{\pm 1\}\right)$$

avec les points de 2-torsion partagés entre les deux jacobiennes.
Nous ne pouvons récupérer que les coordonnées $(x :: z)$ sur les courbes elliptiques. Ces coordonnées sont invariantes sous l'action de l'isomorphisme identifiant une courbe et sa tordue. Le morphisme global, qui est rationnel, est donc la composition de morphismes non rationnels (en particulier, ces derniers utilisent des racines carrés).

Dans les méthodes utilisées pour la phase 2, il n'est pas possible d'utiliser des additions différentielles : il faut utiliser de vraies additions. Par ailleurs il faut tester si les points πQ sont le zéro modulo p d'une des courbes elliptiques. De ce fait, il faut récupérer les coordonnées $(x :: z)$ de nombreux points. Si nous travaillions sur une variété abélienne non simple, il faudrait calculer à chaque fois les morphismes pour

obtenir les coordonnées $(x :: z)$ sur les courbes elliptiques sous-jacentes. En pratique, ceci serait trop coûteux.
La solution retenue a été de récupérer les résultats de la phase 1 sur les courbes elliptiques sous-jacentes puis d'appliquer pour chacun d'eux la phase 2 et donc travailler avec la phase 2 classique d'ECM sur chacune des courbes elliptiques.

4.3.3 Paramétrisation

Dans cette section nous donnons une famille de courbes utilisables pour HECM. Nous obtenons ces courbes sur $\mathbb{Q}$ et considérons leur réduction modulo N, le nombre à factoriser. Comme nous devons avoir suffisamment de courbes sur $\mathbb{Z}/N\mathbb{Z}$, nous voulons avoir un nombre infini de courbes sur $\mathbb{Q}$.

Notons que, au cours de la construction, nous ne devons jamais avoir à calculer une racine carrée. Nous demandons donc que la paramétrisation soit fournie par des fractions rationnelles en un nombre fini de variables.

Paramétrisation de la courbe hyperelliptique

Explicitons le lien entre les fonctions thêta et les invariants de Rosenhain de la courbe hyperelliptique. Rappelons que nous avons posé

$$\mathcal{C}:\ y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

Avec l'ordonnancement $\{\nu, \mu, \lambda, 1, 0\}$ dans la formule 3.1.20, nous obtenons les équations suivantes

$$\lambda = \frac{\alpha\beta}{\delta\gamma}, \qquad \mu = \frac{\gamma\epsilon}{\delta\phi}, \qquad \nu = \frac{\alpha\epsilon}{\delta\phi} \tag{4.1}$$

où nous avons posé

$$\begin{array}{lllll} \alpha = \theta_0(0)^2 = \theta\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right](0,\Omega)^2, & & \beta = \theta_1(0)^2 = \theta\left[\begin{smallmatrix}0&0\\\frac{1}{2}&0\end{smallmatrix}\right](0,\Omega)^2, \\ \gamma = \theta_2(0)^2 = \theta\left[\begin{smallmatrix}0&0\\0&\frac{1}{2}\end{smallmatrix}\right](0,\Omega)^2, & & \delta = \theta_3(0)^2 = \theta\left[\begin{smallmatrix}0&0\\\frac{1}{2}&\frac{1}{2}\end{smallmatrix}\right](0,\Omega)^2, \\ \epsilon = \theta_{12}(0)^2 = \theta\left[\begin{smallmatrix}\frac{1}{2}&\frac{1}{2}\\0&0\end{smallmatrix}\right](0,\Omega)^2, & & \phi = \theta_{15}(0)^2 = \theta\left[\begin{smallmatrix}\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&\frac{1}{2}\end{smallmatrix}\right](0,\Omega)^2. \end{array}$$

Pour l'arithmétique, nous utiliserons celle fournie par les fonctions thêta de niveau 2 de la base $\mathscr{F}_{(2,0)^2}$. De ce fait, il faut que les thêta constantes de cette base (c'est-à-dire le vecteur projectif $(\alpha, \beta, \gamma, \delta)$) soient rationnelles.

Lemme 4.3.3. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 sur $\mathbb{Q}$ dont tous les points de 2-torsion sur la jacobienne sont rationnels.*
La courbe $\mathcal{C}$ peut être utilisée dans HECM *(c'est-à-dire que $\mathcal{C}$ est $(2,2)$-décomposable avec des courbes elliptiques sous-jacentes rationnelles et une surface de Kummer rationnelle) si et seulement si $\mathcal{C}$ peut se mettre sous la forme*

$$\mathcal{C}: \qquad \chi y^2 = x\,(x-1)\,(x-\lambda)\,(x-\mu)\,(x-\nu)\,.$$

avec

$$\lambda = \mu\frac{1-\nu}{1-\mu}, \qquad \mu\,(\mu-\nu) = \square, \qquad \lambda\mu\nu = \square$$

où $\square$ signifie que la quantité doit être un carré.

Démonstration. Avoir une équation sous forme de Rosenhain est équivalent à ce que tous les points de 2-torsion sur la jacobienne soient rationnels.

Les deux premières conditions impliquent que la courbe est $(2,2)$-décomposable avec des courbes elliptiques sous-jacentes rationnelles 4.3.2. La surface de Kummer est rationnelle si et seulement si les

carrés $(\alpha, \beta, \gamma, \delta)$ des quatre thêta constantes sont rationnels. Ils sont reliés aux invariants de Rosenhain par :

$$\lambda = \frac{\alpha\beta}{\delta\gamma}, \qquad \mu = \frac{\gamma\epsilon}{\delta\phi}, \qquad \nu = \frac{\alpha\epsilon}{\delta\phi}$$

où ϵ et ϕ sont deux autres carrés de thêta constantes. Il découle de ces équations que

$$\frac{\alpha}{\delta} = \frac{\sqrt{\lambda\mu\nu}}{\mu}, \qquad \frac{\beta}{\gamma} = \frac{\sqrt{\lambda\mu\nu}}{\nu}.$$

Donc le produit $\lambda\mu\nu$ doit être un carré dans $\mathbb{Q}$.
Quand nous écrivons l'équation $\lambda = \mu\frac{1-\nu}{1-\mu}$ en fonction des thêta constantes (à l'aide des formules 4.1), nous obtenons $\alpha^2 = \gamma^2$. De plus β, γ, δ sont des fonctions de λ, μ, ν, α et donc sont rationnelles. Cela montre que les conditions sont suffisantes. □

Remarque 4.3.4. *Les invariants de Rosenhain (λ, μ, ν) sont définis à une action de* $\mathrm{PGL}(2,5)$ *près. De ce fait, la relation qui les lie pour qu'une courbe soit $(2,2)$-décomposable n'est pas unique. Une fois la numérotation des racines choisie, notre choix est le seul qui entraîne une égalité entre deux des quatre thêta constantes. Nous avons étudié les équations à résoudre pour des paramétrisations avec un choix différent de numérotation. Nous nous sommes rendus compte que cela impliquait de gérer une racine carrée supplémentaire.*

Comme $(\alpha, \beta, \gamma, \delta)$ est un élément de $\mathbb{P}^3(\mathbb{Q})$, nous pouvons supposer que $\alpha = 1$. Faisons également le choix

$$\gamma = \alpha = 1,$$

l'autre (c'est-à-dire $\gamma = -\alpha = -1$) fournissant une surface de Kummer isomorphe. Prenons

$$\mu = 1 - \frac{\nu(1-\nu)}{s^2}$$

avec $s \in \mathbb{Q}$ de sorte que $\lambda\mu\nu = \mu^2 s^2$. La deuxième équation devient

$$\mu(\mu - \nu) = \frac{1}{s^4}\left(-\nu + \nu^2 + s^2\right)(\nu - 1)\left(\nu - s^2\right) = \square.$$

Supposons que $\frac{\nu - s^2}{\nu - 1}$ est un carré u^2 (alors $\nu = \frac{s^2 - u^2}{1 - u^2}$), l'équation se réécrit

$$1 + (-3/s^2 + 1/s^4)u^2 + u^4/s^2 = \square.$$

Soit v^2 ce carré, le point (u, v) se trouve sur une courbe elliptique sur $\mathbb{Q}(s)$. Celle-ci est sous forme de Jacobi [BJ03, Duq07], est de rang 1 et possède un point $\left(1, 1 - \frac{1}{s^2}\right)$ qui n'est pas de torsion.

Théorème 4.3.5. *Une sous-famille des courbes hyperelliptiques $(2,2)$-décomposables de genre 2 ayant des courbes elliptiques sous-jacentes rationnelles et une surface de Kummer rationnelle est donnée par la paramétrisation*

$$\mathcal{C} : \qquad \chi y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu),$$

$$\lambda = \mu\frac{1-\nu}{1-\mu}, \qquad \mu = 1 - \frac{\nu(1-\nu)}{s^2}, \qquad \nu = \frac{s^2 - u^2}{1 - u^2}$$

où (u, v) est un point de la courbe elliptique

$$1 + (-3/s^2 + 1/s^4)u^2 + u^4/s^2 = v^2.$$

Un point générique sur cette courbe est $(1, 1 - \frac{1}{s^2})$. Les paramètres s, χ, u et v sont des nombres rationnels devant vérifier les deux conditions 4.3.6 et 4.3.6 suivantes.

Condition 4.3.6. *Avec les notations du théorème, la courbe $\mathcal{C}$ est de genre 2 si et seulement si les éléments 0, 1, ∞, λ, μ et ν sont distincts et si χ n'est pas nul. Ceci est équivalent aux conditions*

$$\chi \neq 0, \qquad s \neq 0, \pm 1, \qquad u \neq 0, \pm 1, \qquad v \neq 0,$$

$$s \neq \pm u, \qquad s^2 - 2u^2 + u^4 \neq 0.$$

En particulier la condition 4.3.6 implique que nous ne pouvons pas utiliser le point $(1, 1 - \frac{1}{s^2})$ sur la courbe de Jacobi. Nous devons prendre un multiple de ce point, par exemple son double $(2, 1 + \frac{2}{s^2})$.

Condition 4.3.7. *Pour l'arithmétique sur la surface de Kummer, toutes les thêta constantes doivent être non nulles. Les paramètres doivent alors satisfaire à la condition 4.3.6 et vérifier de plus*

$$s \neq \pm u^2.$$

Les différentes thêta constantes non nulles sont données avec la numérotation de Dupont par

$$\begin{aligned}
\theta_0^2(0) &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ 0) \end{bmatrix} (0,\Omega)^2 &&= \alpha = 1, \\
\theta_1^2(0) &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0) \end{bmatrix} (0,\Omega)^2 &&= \beta = \frac{\sqrt{\lambda\mu\nu}}{\nu} = \frac{\mu s}{\nu}, \\
\theta_2^2(0) &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2}) \end{bmatrix} (0,\Omega)^2 &&= \gamma = 1, \\
\theta_3^2(0) &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{bmatrix} (0,\Omega)^2 &&= \delta = \frac{\mu}{\sqrt{\lambda\mu\nu}} = \frac{1}{s}, \\
\theta_{12}^2(0) &= \theta \begin{bmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ 0) \end{bmatrix} (0,\Omega)^2 &&= \epsilon = \sqrt{\alpha\delta - \beta\gamma}\sqrt{\frac{\sqrt{\lambda\mu\nu}}{\lambda}}, \\
\theta_{15}^2(0) &= \theta \begin{bmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{bmatrix} (0,\Omega)^2 &&= \phi = \frac{\alpha\beta - \gamma\delta}{\epsilon}, \\
\theta_8^2(0) &= \theta \begin{bmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ 0) \end{bmatrix} (0,\Omega)^2 &&= \sqrt{-\phi^2}, \\
\theta_9^2(0) &= \theta \begin{bmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ 0) \end{bmatrix} (0,\Omega)^2 &&= \sqrt{-\epsilon^2}, \\
\theta_4^2(0) &= \theta \begin{bmatrix} {}^t(\frac{1}{2},0) \\ {}^t(0,0)) \end{bmatrix} (0,\Omega)^2 &&= \frac{\beta\epsilon - \gamma\phi}{\theta_9(0)}, \\
\theta_6^2(0) &= \theta \begin{bmatrix} {}^t(\frac{1}{2},0) \\ {}^t(0,\frac{1}{2})) \end{bmatrix} (0,\Omega)^2 &&= \frac{\alpha\gamma - \beta\delta}{\theta_4(0)}.
\end{aligned}$$

Notons que les racines carrées apparaissant ici ne sont jamais calculées en pratique. Cependant travailler dans l'algèbre correspondante permet de simplifier la programmation de l'algorithme.

Le paramètre χ détermine si nous sommes sur la courbe ou sur sa tordue quadratique. Cependant il n'est pas choisi lors de la paramétrisation de la courbe : en effet la courbe comme sa tordue ont toutes les deux la même surface de Kummer. Le choix d'un point sur celle-ci déterminera si nous travaillons sur la courbe ou sur sa tordue. En pratique la coordonnée y des points ne sera jamais utilisée et donc χ n'a pas besoin d'être calculé.

Nous aurions pu utiliser $\frac{\nu - s^2}{\nu - 1} = l\,u^2$ (ici $l = 1$) mais cela aurait mené à des équations plus compliquées. Par exemple, avec $l = -1$, nous trouvons une courbe elliptique avec aucun point rationnel (autre que O). Dans ce dernier cas, pour que la courbe devienne de rang 1 il faut supposer que s se trouve sur une conique.

Remarque 4.3.8. *L'algorithme* ECM *suppose que le cardinal des courbes elliptique sur $\mathbb{F}_p$ se comporte comme un nombre entier aléatoire de taille autour de p avec possiblement des conditions de divisibilité supplémentaires. Dans* HECM*, nous travaillons simultanément sur deux courbes elliptiques. Les cardinaux de ces dernières ne sont pas indépendants : par exemple les points de 4-torsion ne peuvent exister que sur une seule des deux courbes. Cependant expérimentalement, il semble que ce soit l'unique lien entre leurs cardinaux.*

Trouver un point sur la surface de Kummer

Appelons (X, Y, Z, T) les coordonnées thêta de niveau 2, c'est-à-dire :

$$\begin{aligned} X &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ 0) \end{bmatrix} (z,\Omega)^2, & Y &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0) \end{bmatrix} (z,\Omega)^2, \\ Z &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2}) \end{bmatrix} (z,\Omega)^2, & T &= \theta \begin{bmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{bmatrix} (z,\Omega)^2. \end{aligned}$$

Les équations de Riemann 3.1.13 imposent alors la relation suivante entre les coordonnées

$$4E'^2\,\alpha\beta\gamma\delta\,XYZT = \big(F(X^2T^2+Y^2Z^2)+G(X^2Z^2+Y^2T^2)+ \\ +H(X^2Y^2+Z^2T^2)-(X^4+Y^4+Z^4+T^4)\big)^2$$

où

$$\begin{aligned} A' &= \alpha+\beta+\gamma+\delta, & B' &= \alpha+\beta-\gamma-\delta, \\ C' &= \alpha-\beta+\gamma-\delta, & D' &= \alpha-\beta-\gamma+\delta, \end{aligned}$$

$$E' = \frac{A'B'C'D'}{(\alpha\delta-\beta\gamma)(\alpha\gamma-\beta\delta)(\alpha\beta-\gamma\delta)},$$

$$F = \frac{\alpha^2-\beta^2-\gamma^2+\delta^2}{\alpha\delta-\beta\gamma}, \qquad G = \frac{\alpha^2-\beta^2+\gamma^2-\delta^2}{\alpha\gamma-\beta\delta}, \qquad H = \frac{\alpha^2+\beta^2-\gamma^2-\delta^2}{\alpha\beta-\gamma\delta}.$$

Pour ECM, nous avons besoin d'un point générique (c'est-à-dire un point qui n'est pas de torsion sur la courbe définie sur $\mathbb{Q}$) sur la courbe elliptique. Contrairement à la paramétrisation de Brent-Suyama pour les courbes elliptiques, il est possible ici de trouver un point après avoir choisi la courbe hyperelliptique.

Comme dans ECM, le point initial utilisé dans HECM, ne doit pas être un point de torsion du groupe considéré (ici les deux courbes elliptiques sous-jacentes).

Rappelons que prendre des racines carrés ou utiliser une extension de corps n'est pas possible. Il n'est donc pas possible de prendre trois coordonnées thêta au hasard et de résoudre l'équation de la surface de Kummer pour obtenir la dernière.

La première méthode pour trouver un point consiste à mettre une coordonnée à zéro. Dans ce cas les trois autres vivent sur une conique. Supposons qu'il existe un point rationnel, comme les coniques sont birationnellement équivalentes à $\mathbb{P}^1$, nous obtenons un nombre infini de points sur la surface de Kummer. Ces points ne peuvent cependant pas être utilisés directement par l'algorithme de multiplication car une de leurs coordonnées est nulle. Pour résoudre ce problème nous pouvons essayer de doubler le point jusqu'à en obtenir un avec des coordonnées non nulles ; en général un seul doublement suffit.
Il existe cependant une meilleure solution pour trouver des points : nous cherchons des points avec deux coordonnées égales ou opposées. De tels points ont l'avantage d'économiser des multiplications (car nous pouvons partager des calculs dans les algorithmes 9 et 10) : le coût devient $12M + 10S$ par bit du multiplieur. Tous les choix de paires de coordonnées ne sont pas possibles : certains ne conduisent qu'à des points de torsion ou à des équations impossibles à résoudre comme $-1 = \square$. Le choix $T = -X$ conduit à une courbe elliptique ayant de nombreux points. Chacun de ceux-ci conduit à des points sur la surface de Kummer qui sont d'ordre infini sur $\mathbb{Q}$. Par exemple, nous pouvons utiliser

$$\begin{aligned} X &= \frac{u^2\left(u^2-1\right)\left(su^4-3su^2+u^2+s^3-s^2+s\right)}{\left(s-u^2\right)s^4v^2}, & Y &= 1 \\ Z &= \frac{\left(s^2-u^2\right)\left(u^2-1\right)}{s^4v^2}, & T &= -X \end{aligned}$$

Le chapitre 5 décrit le changement de coordonnées entre les coordonnées thêta sur la surface de Kummer et celles de Mumford (u, v^2).

Tableau 4.1 – points de 4-torsion sur les courbes elliptiques sous-jacentes

s^2-u^2	s^2-1	u^2-1	-1	
			□	⊠
□	□	□	$\mathcal{C}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$
		⊠	$\mathcal{C}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$
	⊠	□	$\mathcal{C}$	
		⊠	$\tilde{\mathcal{C}}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$
⊠	□	□	$\tilde{\mathcal{C}}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$
		⊠	$\mathcal{C}$	
	⊠	□	$\mathcal{C}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$
		⊠	$\mathcal{C}$	$\mathcal{C}$ $\tilde{\mathcal{C}}$

4.3.4 Étude de la torsion

La probabilité de succès de l'algorithme ECM dépend de la probabilité que le cardinal de la courbe sur laquelle nous travaillons soit B_1, B_2-friable. Rappelons (page 15) que le cardinal des courbes elliptiques sur $\mathbb{F}_p$, a de meilleures propriétés de divisibilité que les nombres aléatoires.

Pour augmenter la probabilité de succès nous allons essayer de forcer de petits facteurs dans la torsion des courbes elliptiques. Dans notre cas, nous avons imposé que les courbes elliptiques sous-jacentes aient au moins quatre points de 2-torsion ce qui veut dire que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un sous-groupe du groupe de torsion.

En théorie, il est possible de trouver des courbes hyperelliptiques décomposables ayant des courbes elliptiques sous-jacentes avec de grands groupes de torsion [HLP00]. Cependant cela conduit à devoir résoudre des équations plus compliquées lors de la paramétrisation. Une obstruction plus théorique à l'amélioration de la torsion est que pour avoir des points d'ordre supérieur à 2, il faut être capable de trouver un point de base sur la surface de Kummer correspondant à un point de $\mathrm{Jac}(\mathcal{C})$ et non pas de sa tordue $\mathrm{Jac}(\tilde{\mathcal{C}})$. Cette obstruction pourrait être levée si la courbe et sa tordue avaient la même torsion mais ceci augmente encore le nombre d'équations à résoudre lors de la paramétrisation.

En utilisant la paramétrisation présentée à la section 4.3.3, nous obtenons le tableau 4.1 où les lettres indiquent si et où les points de 4-torsion existent : $\mathcal{C}$ pour la courbe et $\tilde{\mathcal{C}}$ pour sa tordue. Avec la même probabilité, nous travaillons sur la courbe ou sa tordue. Supposons que les symboles de Legendre de s^2-u^2, s^2-1 et de u^2-1 sont indépendants (ce qui se vérifie expérimentalement). Nous en déduisons que si $p \equiv 1 \mod 4$, alors nous avons un point de 4-torsion avec probabilité $1/2$ et, si $p \equiv 3 \mod 4$, la probabilité est de $3/4$. Des expériences montrent que pour $p \equiv 1 \mod 4$, la puissance de 2 divisant le cardinal est, en moyenne, de 3,15 (au lieu de 3 pour des entiers « aléatoires » sous ces conditions) et pour $p \equiv 3 \mod 4$ de 3,48 (au lieu de 3,5).

Pour étudier plus en détail la friabilité des cardinaux des courbes considérées, nous allons utiliser une théorie développée par Knuth et Schröppel dans le cadre l'algorithme de factorisation par les fractions continues (voir [Knu81, page 396] ou [Kru10, page 101]). Soit p un nombre premier. Considérons un ensemble $S \subset \mathbb{N}$ de nombres pour lesquels nous allons étudier l'exposant moyen $f(p, S)$ du premier p dans

la décomposition des nombres de S (avec la probabilité uniforme sur S). Nous avons

$$f(p,S) = \sum_{n=1}^{\infty} \frac{1}{p^n} = \frac{1}{p-1}.$$

Soit k un nombre entier et soit un élément s de S. Divisons s par les nombres premiers inférieurs à k et notons r le reste de cette division. La taille de r peut être estimée par la formule

$$\log(r) = \log(s) - \sum_{p\in\mathcal{P},\ p\leqslant k} f(p,S)\log(p)$$

où $\mathcal{P}$ désigne l'ensemble des nombres premiers. Posons

$$\delta = \sum_{p\in\mathcal{P},\ p\leqslant k} \left(f(p,S) - \frac{1}{p-1}\right)\log(p).$$

Le réel δ correspond à la différence attendue entre la taille du cofacteur r provenant des nombres de S par rapport à celle des cofacteurs r provenant des entiers de $\mathbb{N}$. Comme la taille logarithmique du cofacteur est plus petite du facteur δ, le nombre s se comporte (du point de vue de la friabilité) comme un entier aléatoire plus petit d'un facteur de e^{δ}.

Expérimentalement, nous trouvons que $\delta = 2{,}048$. Le cardinal des courbes est donc friable comme un entier aléatoire valant $1/7{,}75$ du cardinal (à comparer avec $1/23{,}7$ pour les courbes de Suyama [ZD06]). Nous avons remarqué que la paramétrisation $s = \frac{3+t^2}{3-t^2}$, $u = 2$, $v = 1 + \frac{2}{s^2}$ fournit une meilleure torsion (la puissance de 2 étant en moyenne de 3,66) mais il y a moins de telles courbes ayant de petits paramètres.

4.3.5 Petits paramètres

Comme nous l'avons remarqué dans la section 3.2.2, lors du calcul de $[k]P$, nous utilisons beaucoup de multiplications par des constantes. Si les constantes sont petites alors ces multiplications vont être négligeables devant les multiplications modulaires classiques. Le coût deviendra alors de $4M + 12S$ par bit du multiplieur et si nous utilisons l'approximation $1S = 0.8M$, le coût est de $13.6M$.

En pratique, nous appelons un nombre une petite constante s'il tient dans un `signed long`. Ceci limite le nombre de courbes que nous pouvons utiliser : si nous travaillons avec un processeur 64 bits, il y a 185.399 courbes hyperelliptiques utilisables ce qui est suffisant pour trouver des facteurs de plus de 65 chiffres décimaux.
Dans l'algorithme de multiplication, les 16 multiplications par des constantes peuvent être réduites à 12 car nous sommes dans l'espace projectif. Cependant, dans ce cas, nous aurions des nombres rationnels qui doivent, modulo N, tenir dans des `signed long`, ce qui est plus compliqué.
Plus spécifiquement, notre paramétrisation donne $(\alpha,\beta,\gamma,\delta)$ et $(1/A : 1/B : 1/C : 1/D)$ en fonction de fractions rationnelles de petits degrés en $(s,u) \in \mathbb{Q}^2$. Comme nous travaillons en projectif, nous pouvons éliminer les dénominateurs. Les constantes utilisées dans l'algorithme de multiplication sont alors :

$$\left(\frac{1}{\alpha} : \frac{1}{\beta} : \frac{1}{\gamma} : \frac{1}{\delta}\right) = \left(s^4v^2 :\ s\left(u^2-s^2\right)\left(u^2-1\right) :\ s^4v^2 :\ s^5v^2\right),$$

$$\begin{aligned}\left(\frac{1}{A} : \frac{1}{B} : \frac{1}{C} : \frac{1}{D}\right) \quad = \quad & \Big((s-1)^2\left(s^2-2u^2+u^4\right)\left(s+u^2\right)^2 :\ -\left(u^2-1\right)\left(s+u^2\right)^2\left(s-u^2\right)^2 : \\ & (s+1)^2\left(s^2-2u^2+u^4\right)\left(s-u^2\right)^2 :\ \left(u^2-1\right)\left(s+u^2\right)^2\left(s-u^2\right)^2\Big).\end{aligned}$$

Comme s est rationnel, posons $s = a/b$ avec des entiers a et b. Après avoir généré une courbe hyperelliptique, nous pouvons tester si les constantes sont petites. Il faut alors trouver un point sur la surface de Kummer tel que les inverses de ses coordonnées soient « petites ». Malheureusement nous n'avons pas trouvé de point tel que ces inverses ont des degrés égaux ou inférieurs à ceux des constantes précédentes. Ceci réduit donc le nombre de courbes utilisables. En pratique, nous avons plusieurs points génériques sur la surface de Kummer et nous pouvons chercher si l'un de ces points convient.

4.4 GMP-HECM

4.4.1 Un exemple numérique

Essayons de factoriser le nombre $N = 4.816.415.081$ avec HECM. Nous utilisons $B_1 = 25$ et $B_2 = 200$ ainsi que les paramètres suivants pour la courbe : $s = \frac{1}{2}$, $u = 2$ et $v = 9$. La surface de Kummer est alors donnée par les paramètres

$$(\alpha, \beta, \gamma, \delta) = \left(1 : \frac{9}{10} : 1 : 2\right).$$

Un point sur cette surface est

$$P = (-272 : 63 : -140 : 272).$$

Nous calculons $[k]\,P$ sur la surface de Kummer avec $k = \text{ppcm}\,(2, \ldots, B_1) = 26.771.144.400$ et envoyons le point qui en résulte sur les deux courbes elliptiques sous-jacentes :

$$(3455587574, 1) \text{ sur } 734346861\,y^2 = (x-1)\left(x - \frac{1}{25}\right)\left(x - \frac{1}{121}\right),$$

$$(3222355131, 1) \text{ sur } 2791313056\,y^2 = (x-1)\,(x-25)\,(x-121).$$

Nous utilisons maintenant la phase 2 d'ECM sur les courbes elliptiques. Sur la première, cela ne renvoie pas de facteur mais la seconde trouve le nombre $p = 83003$ qui est un facteur de

$$N = 4816415081 = 58027 \cdot 83003.$$

Après examen des calculs, nous n'avons pas travaillé sur la courbe hyperelliptique mais sur sa tordue

$$\chi y^2 = x\,(x-1)\left(x - \frac{9}{20}\right)\left(x - \frac{9}{4}\right)\left(x - \frac{5}{4}\right)$$

où χ est un non résidu quadratique modulo N. L'ordre du point initial dans la jacobienne de cette courbe modulo 83003 est $2 \cdot 3 \cdot 5 \cdot 11 \cdot 19 \cdot 73 \cdot 631$. Le cardinal de la première courbe elliptique est $2 \cdot 7 \cdot 631$ et celui de la deuxième de $2 \cdot 3 \cdot 5 \cdot 19 \cdot 73$.

4.4.2 Implémentation

Il existe de nombreuses implémentations de l'algorithme ECM. En particulier, GMP-ECM est un logiciel libre basé sur la bibliothèque GMP. Il est décrit en détail dans [ZD06]. En utilisant de nombreuses fonctions de GMP-ECM, nous avons écrit un nouveau programme appelé GMP-HECM qui utilise les courbes hyperelliptiques. GMP-HECM est distribué avec GMP-ECM [3].

Notre logiciel commence par générer une courbe hyperelliptique décomposable de genre 2 avec des petits paramètres, puis il calcule $[k]\,P$ sur la surface de Kummer et envoie finalement les points sur les courbes elliptiques sous-jacentes. Pour la phase 2, il utilise celle de GMP-ECM. En effet GMP-ECM peut utiliser les résultats d'une phase 1 d'un autre programme : il a juste besoin du paramètre A de la courbe elliptique $y^2 = x^3 + Ax + B$ et des coordonnées d'un point dessus.

Nos courbes elliptique ne peuvent, en général, pas se mettre sous forme de Suyama. Elles n'ont donc pas le même groupe de torsion que celui attendu dans GMP-ECM. Cela modifie la probabilité que leur cardinal soit friable et par voie de conséquence, il faut modifier les paramètres B_1 et B_2. GMP-ECM est capable de choisir le paramètre B_2 de l'étape 2 en fonction de la valeur de B_1. Ce choix n'est pas le même que celui de la continuation standard où $B_2 = 100 \cdot B_1$: GMP-ECM utilise des B_2 beaucoup plus gros pour réduire le nombre de courbes nécessaires pour trouver un facteur (voir le tableau 4.2 pour les valeurs de B_1 et B_2 utilisées dans GMP-ECM).

Le choix de B_1 étant heuristique, nous avons essayé de minimiser le temps moyen de calcul. Le tableau 4.2 fournit les valeurs optimales de B_1 pour différentes tailles (en général inconnues) de facteur. Pour des facteurs de plus de 35 chiffres décimaux, nous utilisons le même B_1 que ECM. Une fois choisis ces B_1,

3. GMP-ECM et GMP-HECM sont téléchargeables à l'adresse http://gforge.inria.fr/projects/ecm/

Tableau 4.2 – Choix optimal des paramètres dans GMP-ECM et GMP-HECM

ordre de grandeur du facteur	GMP-ECM			GMP-HECM		
	B_1 optimal	B_2	nombre moyen de courbes elliptiques	B_1 optimal	B_2	nombre moyen de courbes elliptiques
10^{20}	11,000	2.10^6	74	14,000	2.10^6	75
10^{25}	50,000	16.10^6	214	60,000	16.10^6	214
10^{30}	250,000	130.10^6	430	260,000	130.10^6	491
10^{35}	1.10^6	900.10^6	904	1.10^6	900.10^6	1,116
10^{40}	3.10^6	4.10^9	2,350	3.10^6	4.10^9	2,871
10^{45}	11.10^6	28.10^9	4,480	11.10^6	28.10^9	5,425
10^{50}	43.10^6	200.10^9	7,553	43.10^6	200.10^9	9,003
10^{55}	110.10^6	750.10^9	17,769	110.10^6	750.10^9	21,183
10^{60}	260.10^6	2.10^{12}	42,017	260.10^6	2.10^{12}	49,534
10^{65}	850.10^6	14.10^{12}	69,408	850.10^6	14.10^{12}	81,387

Tableau 4.3 – Fraction du temps pris par les opérations arithmétiques pour différentes tailles de N

ordre de grandeur de N	10^{100}	10^{150}	10^{200}	10^{250}	10^{300}	10^{350}	10^{400}	10^{500}	10^{1000}
M	0.143	0.159	0.194	0.216	0.209	0.219	0.216	0.222	0.234
S	0.428	0.465	0.557	0.597	0.622	0.645	0.65	0.682	0.700
m	0.163	0.127	0.092	0.081	0.070	0.057	0.037	0.031	0.051
additions	0.237	0.179	0.116	0.109	0.074	0.057	0.059	0.041	0.017
S/M	1.00	0.98	0.96	0.93	0.99	0.98	1.04	1.02	1.00
m/M	0.26	0.20	0.12	0.093	0.084	0.066	0.043	0.035	0.055

GMP-ECM nous propose des valeurs de B_2. Nous nous rendons compte que ces valeurs de B_2 sont les mêmes que celles de ECM.

Finalement, le ratio de la différence du nombre moyen de courbes nécessaires décroît avec la taille du facteur.

4.4.3 Résultats et comparaisons

Pour les B_1 de taille suffisante, la complexité théorique et pratique de l'algorithme est linéaire en B_1. Cependant la dépendance en la taille du nombre N à factoriser n'est pas simple : les multiplications modulaires sont quadratiques pour des petits N mais deviennent quasi-linéaires pour les grands N. Il y a de plus de nombreuses autres opérations (multiplications par de petites constantes, additions...) dont la complexité n'est pas négligeable pour les petits N.

Le tableau 4.3 montre le temps pris par les différentes opérations lors du calcul de $[k]P$ pour différentes tailles d'entiers N dans GMP-HECM (nous avons noté par m les multiplications par les petites constantes). Nous pouvons remarquer que les carrés prennent le même temps que les multiplications. Ceci provient du fait que GMP-ECM (et donc GMP-HECM) a du code assembleur spécifique pour les multiplications modulaires mais pas pour les carrés et donc que ces derniers sont calculés avec le même code. Pour les multiplications par de petites constantes, Kruppa a écrit du code assembleur spécifique. Finalement le tableau montre que ni les additions, ni les multiplications par les petites constantes ne sont négligeables pour les petits N.

À la fois parce que les opérations « négligeables » ne le sont pas et parce que le cardinal des courbes elliptiques dans HECM n'est pas autant divisible par de petits facteurs que celles des ECM classiques (du moins avec notre paramétrisation, voir 4.3.4), l'algorithme HECM ne doit pas être utilisé pour factoriser

TABLE 4.4 – Comparaison entre la phase 1 de GMP-ECM et celle de GMP-HECM pour différentes tailles de N avec $B_1 = 10^7$ sur un core 2 à 2.4Ghz.

ordre de grandeur de N	10^{100}	10^{150}	10^{200}	10^{250}	10^{300}	10^{350}	10^{400}	10^{500}	10^{1000}
$\frac{HECM}{2*ECM}$	1.15	1.09	1.03	1.0	0.97	0.94	0.95	0.93	0.89

des nombres de petites tailles.

Théoriquement, la complexité de la phase 1 d'HECM est de $4M+12S$ par bit du multiplieur. Pour une exécution d'ECM avec les coordonnées de Montgomery et l'algorithme PRAC, la complexité est à peu près de $6M+3S$. De ce fait deux sessions d'ECM coûteront $12M+6S$. Si nous utilisons l'approximation $1S = 0.8M$, la complexité de HECM devient $13.6M$ et celle de deux ECM devient $16.8M$. Nous obtenons donc un gain compris entre 11% et 20% selon l'algorithme utilisé pour les carrés modulaires. Bien sûr, ceci n'est valide qu'asymptotiquement.

Le tableau 4.4 compare le temps d'exécution de deux GMP-ECM contre celui d'un GMP-HECM (rappelons qu'une exécution de HECM avec des courbes décomposables est équivalente à deux exécutions de ECM) pour un B_1 fixé et différentes tailles de N. Ce tableau montre que pour les N très grands (au moins 10^{250}), notre programme est plus rapide que GMP-ECM. Comme l'arithmétique avec HECM a plus de carrés que celle avec les courbes de Montgomery, du code assembleur optimisé pour les carrés modulaires permettrait de réduire la frontière à partir de laquelle GMP-HECM est plus intéressant que GMP-ECM. Pour de très grands N le gain entre GMP-HECM et GMP-ECM est de 11% ce qui est concordant avec les résultats théoriques.

L'algorithme EECM (ECM avec les courbes d'Edwards) utilise des « signed sliding window » pour calculer $[k]\,P$ (voir [BBLP10, BBL10]). Cette méthode permet de ne faire qu'un doublement et ϵ addition (sur la courbe elliptique) par bit du multiplieur. Le doublement en coordonnées d'Edwards se fait en $3M+4S$ tandis que l'addition est en $10M+1S+1d$.
En théorie, deux exécutions d'EECM seraient plus rapides qu'une de HECM dès que ϵ est plus petit que $1/12$ (si nous supposons que $1S = 0.8M$ alors ϵ doit être plus petit que $1/20$). Cependant, pour atteindre de tels ϵ, la taille de la fenêtre devient très grande. Les précalculs et l'utilisation mémoire deviennent alors non négligeables.
Les auteurs de [BBLP10] comparent EECM à HECM. Ils écrivent que HECM fait plus de multiplications que EECM mais dans leur comparaison, ils ne comptent pas le coût des précalculs et le font pour un B_1 suffisamment petit ce qui permet d'avoir une taille de fenêtre petite. Par ailleurs, dans leur comparaison, ils précisent le nombre de multiplications par de petites constantes dans HECM et pas dans EECM.
Une comparaison pratique entre les deux algorithmes serait intéressante. Cependant le seul logiciel distribué reposant sur les courbes d'Edwards, EECM-MPFQ [4], ne permet de factoriser que des nombres de moins de 10 mots machines (c'est-à-dire faisant moins de 200 chiffres décimaux). Ces nombres sont trop petits pour HECM. Il serait intéressant de comparer GMP-HECM à une implémentation de EECM permettant de travailler avec des grands nombres et des B_1 élevés.

Finalement, citons une nouvelle factorisation obtenue par HECM. Le nombre impliqué $62^{121}+1$ provient de la table Brent-Montgomery-te Riele [5] [Bt92] :

$$\begin{aligned} 62^{121}+1 &= 3^2 \cdot 7 \cdot 2663 \cdot 369293 \cdot 825977153711699903 \cdot p53 \cdot p137 \\ p53 &= 11.032.894.983.078.909.629.369.066.070.666.992.613.860.028.418.707.083 \end{aligned}$$

4. Disponible à l'adresse : http://eecm.cr.yp.to/mpfq.html
5. Une liste des nombres de ce type qui ont été factorisés et qu'il reste à factoriser se trouve sur le site internet de Brent : http://maths.anu.edu.au/~brent/factors.html

Les premiers facteurs ont été trouvés par d'autres méthodes. Il restait à factoriser un nombre de 189 chiffres décimaux.

4.5 Pistes de recherche

Nous avons vu, à la fois théoriquement et en pratique, que l'utilisation des fonctions thêta de niveau de niveau 2 est compétitive par rapport aux courbes elliptiques sous forme de Weierstraß ou d'Edwards.

La paramétrisation donnée dans ce chapitre n'est sans doute pas optimale. Il serait intéressant d'en explorer d'autres pour obtenir des courbes elliptiques avec une meilleure torsion et/ou de « meilleures » formules d'addition. Explicitons ce que nous entendons par cette dernière expression. Pour certaines configurations de courbes $(2,2)$-décomposables, nous avons la relation suivante entre les fonctions thêta

$$\theta_0^2(z) + \theta_1^2(z) + \theta_2^2(z) + \theta_3^2(z) \quad = \quad 0.$$

Ceci est une relation linéaire entre les fonctions thêta de niveau 2. Le problème de cette relation est qu'elle entraîne $\theta[0](0,2\Omega) = 0$ et nous ne pouvons plus utiliser les formules de Gaudry (algorithmes 9 et 10) pour l'arithmétique. Cependant une telle relation permet d'éviter de « calculer » toutes les coordonnées thêta de niveau 2 : l'une étant fournie comme combinaison linéaire des autres, elle peut donc se calculer uniquement à l'aide d'additions.
Une paramétrisation intéressante au niveau arithmétique serait donc une paramétrisation permettant d'avoir une relation linéaire entre les fonctions thêta de niveau 2 de la variété ou de sa variété isogène mais tout en garantissant que les thêta constantes ne soient pas nulles.

Si nous gardons la méthode consistant à étudier les courbes décomposables via leur équation de Rosenhain

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu),$$

il serait intéressant de regarder l'ordonnancement $\{0,1,\lambda,\mu,\nu\}$ des racines au lieu de $\{\nu,\mu,\lambda,1,0\}$. En effet d'après le chapitre 5, les morphismes entre la variété définie par les fonctions thêta et la jacobienne de la courbe avec les coordonnées de Mumford se comportent différemment. Cela permettrait d'obtenir d'autres conditions pour savoir si nous travaillons sur la courbe ou sur sa tordue.

La méthode d'étude la plus prometteuse selon moi consiste à étudier les propriétés des variétés associées aux matrices $\gamma.\Omega_0$ où nous avons posé

$$\Omega_0 = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} \in \mathcal{H}_2$$

avec τ_1 et τ_2 des éléments du demi-plan de Poincaré. Nous devons les étudier pour les matrices γ du type

$$\gamma = \gamma_2 \begin{pmatrix} 2\,\mathrm{Id}_2 & 0 \\ 0 & \mathrm{Id}_2 \end{pmatrix} \gamma_1, \qquad \text{où } \gamma_1, \gamma_2 \in \Gamma_2 \backslash \mathrm{Sp}(4,\mathbb{Z}).$$

En effet, d'après la section 2.3.2, la matrice γ_1 permet de choisir le noyau de la $(2,2)$-isogénie associée à l'opération $\Omega \to 2\Omega$:

$$\begin{array}{ccc} \mathbb{C}^2/(\gamma_1 \cdot \Omega)\,\mathbb{Z}^2 + \mathbb{Z}^2 & \longrightarrow & \mathbb{C}^2/(2\gamma_1 \cdot \Omega)\,\mathbb{Z}^2 + \mathbb{Z}^2 \\ z & \longmapsto & 2z \end{array}$$

Finalement γ_2 permet de déterminer la variété $(2,2)$-isogène pour les formules de Gaudry. Les $\gamma \cdot \Omega_0$ de ce type fournissent donc des représentants des classes de couples (A,B) modulo isomorphismes où A est la surface de Kummer d'une variété abélienne $(2,2)$-décomposable et B la variété isogène associée à 2Ω (où Ω est la matrice des périodes associée à A).

Notons que nous pouvons exclure certaines matrices γ_1. En effet, si

$$\gamma_1 \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} = \begin{pmatrix} \tau_1' & 0 \\ 0 & \tau_2' \end{pmatrix}$$

où τ_1' et τ_2' sont deux éléments du demi-plan de Poincaré, la variété obtenue ne sera pas simple. De ce fait, nous n'obtiendrons pas d'équations plus intéressantes.

Chapitre 5

Morphismes

Le but de cette partie est d'expliciter les morphismes entre la Jacobienne d'une courbe hyperelliptique, représentée par les coordonnées de Mumford, et la variété abélienne représentée avec les fonctions thêta. Nous nous limitons aux niveaux 2 et 4. Pour les autres niveaux, il est possible d'utiliser les formules de changements de niveaux 7.2.

Les morphismes entre jacobiennes de courbes hyperelliptiques et les fonctions thêta sont une brique de base de l'algorithme de calcul d'isogénies entre courbes hyperelliptiques de genre 2 (section 7.4). Une autre application est fournie par la recherche de lois d'addition complètes 5.5.

Soit $\mathcal{C} : \ y^2 = f(x)$ une courbe hyperelliptique que nous supposerons de modèle imaginaire. Nous voulons avoir des formules de changement de coordonnées entre les systèmes suivants

- les fonctions thêta de niveau 4 données avec la base $\mathscr{F}_{(2,2)}$ et les coordonnées de Mumford (u, v),
- les fonctions thêta de niveau 2 données avec la famille $\mathscr{F}_{(2,2)^2}$ et les coordonnées de Mumford (u, v^2). Remarquons que dans ce dernier cas nous travaillons sur $\mathrm{Jac}(\mathcal{C})/\{\pm 1\}$.

Un problème est que les fonctions thêta (et les thêta constantes) ne sont pas rationnelles sur le corps k définissant la courbe. En particulier le plongement de $\mathrm{Jac}(\mathcal{C})$ par les fonctions de niveau 4 est défini sur le corps $k\left(\{a_i\}, \{\sqrt{a_i - a_j}\}\right)$ où les a_i sont les racines de f. Pour résoudre ce problème Van Wamelen a introduit des fonctions thêta tordues $t_A(z) = f_A(C_A)\theta\left[\eta_{\mathcal{U}\circ A}\right](z)$ où A est un sous-ensemble de $\{1, \ldots, 2g+1\}$. Les nouvelles coordonnées thêta sont alors (avec répétition)

- les $t_A(2z)$ pour le niveau 4,
- les $t_A(z)^2$ pour le niveau 2.

Nous introduisons des fonctions $Y_A(z)$ qui s'expriment de manière simple, à la fois en les polynômes de Mumford (u, v) (et non pas (u, v^2)), et en les fonctions $t_A(z)$ (et non pas en les $t_A(2z)$). Nous utilisons la géométrie algébrique pour prouver l'égalité à une constante près puis nous déterminons la constante. En utilisant la formule de Koizumi, il est ensuite possible d'obtenir les formules de changement de coordonnées voulues.

Les preuves de cette partie reposent sur des calculs analytiques. Cependant le principe de Lefschetz permet de montrer la validité des formules sur des corps parfaits de caractéristique différente de 2. Par ailleurs, les courbes hyperelliptiques et les variétés abéliennes considérées sont supposées génériques dans le sens suivant : aucune thêta constante utilisée n'est nulle. Les cas exclus sont ceux de certaines courbes décomposables. Bien que ce cas ne soit pas traité, il suffit qu'une formule soit bien définie pour qu'elle soit valide sur ces courbes.

Cette partie repose de manière cruciale sur les travaux de Van Wamelen [vW98]. Dans cet article, ce dernier explique comment modifier les fonctions thêta de manière à obtenir une variété définie sur le même corps que les racines du polynôme f. Pour ce faire il explicite une partie des morphismes entre les coordonnées de Mumford et les coordonnées thêta de niveau 4. Notre but est d'obtenir des morphismes totalement explicites dans le cas des niveaux 2 et 4. En particulier nous explicitons les signes dans les équations de Van Wamelen et nous introduisons de nouvelles fonctions, généralisant celles de Van

Wamelen, permettant de calculer les fonctions thêta à partir des polynômes de Mumford. Par ailleurs, nous traitons le cas de diviseurs non génériques.

Pour ce faire il faut introduire et étudier différentes fonctions 5.1. Il est conseillé, en première lecture, de ne pas lire les preuves qui sont souvent lourdes. On pourra ainsi se contenter des énoncés suivant

- section 5.1.1 définissant les fonctions thêta tordues $t_S(z)$ (on utilisera les fonctions $t_S(2z)$ pour le niveau 4 et ${}_S(z)^2$ pour le niveau 2),
- la page 125 qui présente les résultats des études précédentes,
- la discution dans la section 5.1.6.

Il est alors possible de lire les sections 5.2 et 5.3 qui expliquent comment calculer les morphismes. Quelques détails sur l'implémentation pratique de ces formules sont donnés dans la section 5.4. La construction de lois d'addition complètes est une application de ces morphismes (section 5.5).

Dans la suite, on suppose fixée une courbe hyperelliptique $\mathcal{C} : y^2 = f(x)$ avec f de degré $2g+1$. Les racines de f sont notées a_l.

5.1 Étude du plongement de $\mathrm{Jac}(\mathcal{C})$ dans $\mathbb{P}^{4^g-1}$ avec les fonctions thêta

Le but de cette section est d'introduire des fonctions Y'_S de $\mathrm{Jac}(\mathcal{C})$ dans $\mathbb{C}$ qui s'expriment « facilement » en fonction des polynômes de Mumford et des fonctions thêta.
Nous commençons par introduire et étudier les fonctions thêta tordues de Van Wamelen (sections 5.1.1 et 5.1.2) avant d'introduire les fonctions Y_S à la section 5.1.3. Des signes apparaissent alors dans les équations et on les déterminera dans la section 5.1.4. Plusieurs choix doivent être effectués pour définir les fonctions Y_S, nous étudierons leurs impacts dans la section 5.1.6.

5.1.1 Fonctions thêta tordues

Tous les quotients de la forme $(a-b)/(c-d)$ où a, b, c, d sont des racines de f peuvent s'exprimer comme un carré ou comme l'opposé d'un carré d'une fraction rationnelle de thêta constantes (théorème 3.1.20). Il est donc naturel, dans le premier cas, d'essayer de prendre une racine carrée. Pour cela, commençons par ordonner les différences de sorte à être toujours dans le premier cas. Nous utilisons ici les notations η_S de la section 2.3.3.

Définition 5.1.1.

$$< a_j - a_i >=< a_i - a_j >= (-1)^{4\,{}^t\eta'_i\eta''_j}(a_i - a_j) = \begin{cases} a_i - a_j & si\ j < i \\ a_j - a_i & si\ i < j \end{cases}$$

Avec cette convention, nous obtenons une reformulation du théorème 3.1.20 :

Lemme 5.1.2. *Pour tous entiers distincts i, j et k de $\{1,\dots,2g+1\}$ et pour tout sous-ensemble V de $\{1,\dots,2g+1\}$ de cardinal $g+1$, contenant i, j mais pas k,*

$$\frac{< a_k - a_j >}{< a_k - a_i >} = \frac{\theta\left[\eta_{\mathcal{U}\circ V\circ\{j\}}\right]^2 \theta\left[\eta_{\mathcal{U}\circ V\circ\{i,k\}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ V\circ\{i\}}\right]^2 \theta\left[\eta_{\mathcal{U}\circ V\circ\{j,k\}}\right]^2}.$$

Dans la suite nous supposons fixée une racine carrée de $< a_2 - a_1 >$. Nous pouvons alors définir les racines des $< a_i - a_j >$ en fonction de cette dernière.

Définition 5.1.3. *Soit un sous-ensemble V de $\{1,\dots,2g+1\}$ de cardinal $g+1$, contenant $2, j$ mais pas 1, nous posons*

$$\sqrt{< a_j - a_1 >} = \sqrt{< a_2 - a_1 >}\frac{\theta\left[\eta_{\mathcal{U}\circ V\circ\{j\}}\right]\theta\left[\eta_{\mathcal{U}\circ V\circ\{1,2\}}\right]}{\theta\left[\eta_{\mathcal{U}\circ V\circ\{2\}}\right]\theta\left[\eta_{\mathcal{U}\circ V\circ\{1,j\}}\right]}.$$

Soit un sous-ensemble V de $\{1,\dots,2g+1\}$ de cardinal $g+1$, contenant $1,j$ mais pas i, nous posons

$$\sqrt{<a_i-a_j>}=\sqrt{<a_i-a_1>}\frac{\theta\left[\eta_{\mathcal{U}\circ V\circ\{j\}}\right]\theta\left[\eta_{\mathcal{U}\circ V\circ\{1,i\}}\right]}{\theta\left[\eta_{\mathcal{U}\circ V\circ\{1\}}\right]\theta\left[\eta_{\mathcal{U}\circ V\circ\{i,j\}}\right]}.$$

Cette définition ne dépend pas du choix des ensembles V. Par ailleurs, en passant au carré, nous voyons qu'elle est cohérente avec le lemme 5.1.2.

Exemple 5.1.4. *Soit la courbe hyperelliptique de genre 2 suivante*

$$y^2=f(x)=x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

pour laquelle nous choisissons l'ordre $\{0,1,\lambda,\mu,\nu\}$ sur les racines de f et $\sqrt{<1-0>}=\sqrt{1}=1$ pour une racine carrée de $<a_2-a_1>$. Nous avons alors, avec la notation de Dupont (page 37) :

$$\begin{array}{lllllllllll}
\sqrt{<a_2-a_1>} & = & \sqrt{1} & = & 1, & \sqrt{<a_3-a_1>} & = & \sqrt{\lambda} & = & -\dfrac{\theta_0\theta_8}{\theta_4\theta_{12}},\\
\sqrt{<a_4-a_1>} & = & \sqrt{\mu} & = & \dfrac{\theta_2\theta_8}{\theta_6\theta_{12}}, & \sqrt{<a_5-a_1>} & = & \sqrt{\nu} & = & -\dfrac{\theta_0\theta_2}{\theta_4\theta_6},\\
\sqrt{<a_3-a_2>} & = & \sqrt{\lambda-1} & = & -\dfrac{\theta_1\theta_9}{\theta_4\theta_{12}}, & \sqrt{<a_4-a_2>} & = & \sqrt{\mu-1} & = & \dfrac{\theta_4\theta_9}{\theta_6\theta_{12}},\\
\sqrt{<a_5-a_2>} & = & \sqrt{\nu-1} & = & -\dfrac{\theta_1\theta_3}{\theta_4\theta_6}, & \sqrt{<a_4-a_3>} & = & \sqrt{\mu-\lambda} & = & \dfrac{\theta_8\theta_9\theta_{15}}{\theta_4\theta_6\theta_{12}},\\
\sqrt{<a_5-a_3>} & = & \sqrt{\nu-\lambda} & = & -\dfrac{\theta_0\theta_1\theta_{15}}{\theta_4\theta_6\theta_{12}}, & \sqrt{<a_5-a_4>} & = & \sqrt{\nu-\mu} & = & -\dfrac{\theta_2\theta_3\theta_{15}}{\theta_4\theta_6\theta_{12}}.
\end{array}$$

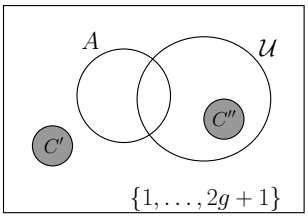
Nous pouvons maintenant introduire de nouvelles coordonnées en « tordant » les fonctions thêta.

Définition 5.1.5. *Soit un sous-ensemble A de $\{1,\dots,2g+1\}$.*
- *Si A est de cardinal plus petit que g, choisissons deux ensembles $C'\subset(A\cup\mathcal{U})^c$ et $C''\subset\mathcal{U}\setminus A$ de cardinaux $n=\lfloor\frac{g+1-\#A}{2}\rfloor$ et posons $C_A=C'\cup C''$.*
- *Si A est de cardinal plus grand que $g+1$, nous poserons $C_A=C_{A^c}$.*

Posons alors

$$f_A(C_A)=\frac{\prod_{\substack{i\in\mathcal{U}\cap A\\ j\in\mathcal{U}\setminus A}}\sqrt{<a_i-a_j>}\prod_{\substack{i\in\mathcal{U}^c\cap A^c\\ j\in A\setminus\mathcal{U}}}\sqrt{<a_i-a_j>}}{\prod_{\substack{i\in(\mathcal{U}\circ C_A)\cap(A\circ C_A)\\ j\in(\mathcal{U}\circ C_A)\setminus(A\circ C_A)}}\sqrt{<a_i-a_j>}\prod_{\substack{i\in(\mathcal{U}\circ C_A)^c\cap(A\circ C_A)^c\\ j\in(\mathcal{U}\circ C_A)\setminus(A\circ C_A)}}\sqrt{<a_i-a_j>}}\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_A}\right]}{\theta\left[\eta_{\mathcal{U}\circ A\circ C_A}\right]}$$

Le choix du sous-ensemble C_A dans la définition précédente peut être résumé par le schéma suivant :



Ensemble C_A dans le cas où $\#A\leqslant g$

Remarque 5.1.6. *Quand il n'y a pas d'ambiguité, nous écrirons C au lieu de C_A, f_A au lieu de $f_A(C_A)$. On pourra se référer à la propriété 5.1.20 et à la discussion page 107 pour l'étude de la dépendance de $f_A(C_A)$ par rapport à C_A : la conclusion de ces études est que différents choix d'ensemble C_A changent seulement le signe de $f_A(C_A)$. Finalement, si $A=\{i\}$ est de cardinal 1, nous écrirons f_i au lieu de $f_{\{i\}}$.*

Remarquons que si $\#A$ n'est pas congru à $g+1$ modulo 2, notre définition de f_A n'est pas la même que celle de Van Wamelen. Pour retrouver cette dernière, on peut regarder A^c qui est de cardinal congru à $g+1$ modulo 2. Notre constante f_A diffère alors de celle de Van Wamelen par un signe.

Définition 5.1.7. *Soit un sous-ensemble A de $\{1,\dots,2g+1\}$, soit C_A un sous-ensemble de $\{1,\dots,2g+1\}$ choisi comme dans la définition 5.1.5. Nous définissons alors la fonction t_{A,C_A} par*

$$t_{A,C_A}(z):\quad \left\{\begin{array}{ccc}\mathbb{C}^g & \longrightarrow & \mathbb{C}\\ z & \longmapsto & f_A(C_A)\,\theta\left[\eta_{\mathcal{U}\circ A}\right](z)\end{array}\right.$$

Remarque 5.1.8. *De même que pour les f_A nous écrirons t_A au lieu de t_{A,C_A} quand il n'y a pas d'ambiguité. De plus, si $A=i$ est de cardinal 1, nous noterons t_i à la place de $t_{\{i\}}$.*

Exemple 5.1.9. *En genre 2 nous obtenons*

A	C_A	$f_A(C_A)$	$t_{A,C_A}(z)$	$\frac{f_{A^c}(C_{A^c})}{f_A(C_A)}$	$\frac{t_{A^c,C_{A^c}}(z)}{t_{A,C_A}(z)}$
$\emptyset$	$\{1,2\}$	$\frac{-1}{\sqrt{a_2-a_1}^3}\frac{\theta_4^2\theta_6^2\theta_{12}^2}{\theta_1\theta_2\theta_3\theta_8\theta_9\theta_{15}}$	$\frac{-1}{\sqrt{a_2-a_1}^3}\frac{\theta_4^2\theta_6^2\theta_{12}^2}{\theta_1\theta_2\theta_3\theta_8\theta_9\theta_{15}}\theta_{14}(z)$	-1	-1
$\{1\}$	$\{2,5\}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_4\theta_6\theta_{12}}{\theta_1\theta_3\theta_9\theta_{15}}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_4\theta_6\theta_{12}}{\theta_1\theta_3\theta_9\theta_{15}}\theta_{10}(z)$	-1	-1
$\{2\}$	$\{1,4\}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_4\theta_6\theta_{12}}{\theta_2\theta_8\theta_{15}}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_4\theta_6\theta_{12}}{\theta_2\theta_8\theta_{15}}\theta_{11}(z)$	1	1
$\{3\}$	$\{1,2\}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_6}{\theta_2\theta_3}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_6}{\theta_2\theta_3}\theta_7(z)$	1	-1
$\{4\}$	$\{1,2\}$	$\frac{1}{\sqrt{a_2-a_1}}\frac{\theta_4}{\theta_1}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_4}{\theta_1}\theta_5(z)$	1	-1
$\{5\}$	$\{1,2\}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_{12}}{\theta_8\theta_9}$	$\frac{-1}{\sqrt{a_2-a_1}}\frac{\theta_0\theta_{12}}{\theta_8\theta_9}\theta_{13}(z)$	-1	-1

Pour les ensembles A de cardinal 2 ou 3, la constante C_A est l'ensemble vide. Nous avons alors

$$f_A(\emptyset)=(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A}\zeta''_g}f_{A^c}(\emptyset)=\frac{\theta\left[0\right]}{\theta\left[\eta_{\mathcal{U}\circ A}\right]},\qquad t_{A,\emptyset}(z)=t_{A^c,\emptyset}(z)=\frac{\theta\left[0\right]}{\theta\left[\eta_{\mathcal{U}\circ A}\right]}\theta\left[\eta_{\mathcal{U}\circ A}\right](z)$$

c'est à dire

A	$f_A(C_A)$	$\frac{f_{A^c}(C_{A^c})}{f_A(C_A)}$	$t_{A,C_A}(z)=t_{A^c,C_{A^c}}(z)$
$\{1,2\}$	$-\frac{\theta_0}{\theta_{15}}$	-1	$\frac{\theta_0}{\theta_{15}}\theta_{15}(z)$
$\{1,3\}$	$\frac{\theta_0}{\theta_3}$	1	$\frac{\theta_0}{\theta_3}\theta_3(z)$
$\{1,4\}$	$\frac{\theta_0}{\theta_1}$	1	$\frac{\theta_0}{\theta_1}\theta_1(z)$
$\{1,5\}$	$\frac{\theta_0}{\theta_9}$	-1	$\frac{\theta_0}{\theta_9}\theta_9(z)$
$\{2,3\}$	$\frac{\theta_0}{\theta_2}$	1	$\frac{\theta_0}{\theta_2}\theta_2(z)$
$\{2,4\}$	1	1	$\theta_0(z)$
$\{2,5\}$	$\frac{\theta_0}{\theta_8}$	-1	$\frac{\theta_0}{\theta_8}\theta_8(z)$
$\{3,4\}$	$\frac{\theta_0}{\theta_{12}}$	-1	$\frac{\theta_0}{\theta_{12}}\theta_{12}(z)$
$\{3,5\}$	$\frac{\theta_0}{\theta_4}$	1	$\frac{\theta_0}{\theta_4}\theta_4(z)$
$\{4,5\}$	$\frac{\theta_0}{\theta_6}$	-1	$\frac{\theta_0}{\theta_6}\theta_6(z)$

Soit $\mathcal{C}: y^2 = f(x)$ une courbe sur un sous-corps k de $\mathbb{C}$. Van Wamelen a montré que les fonctions $t_A(2z)$ pour $A \subset \{1,\dots,2g+1\}$ de cardinal congru à $g+1$ modulo 2 fournissent un plongement projectif de $\mathrm{Jac}(\mathcal{C})$ dans $\mathbb{P}^{4^g-1}(k)$ défini sur le corps $k(a_i)$ où les a_i sont les racines de f.

Nous n'utiliserons pas cette propriété. Cependant les formules s'expriment de manière plus naturelle avec les fonctions t_A que les fonctions thêta : en se basant sur le théorème III.a.7.6 de Mumford [Mum84], Van Wamelen prouve

Théorème 5.1.10. *Soit D un diviseur de $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$. Soit u le polynôme de Mumford associé à D et soit $z = \mathfrak{u}(D)$, l'image de D par l'application d'Abel-Jacobi 2.3.3. Alors, pour tout $k \in \{1,\dots,2g+1\}$,*

$$u(a_k) = (-1)^g \frac{t_k^2(z)}{t_\emptyset^2(z)}.$$

Ce théorème est important car il permet de relier les fonctions thêta au polynôme u de Mumford. Pour les relier au polynôme v, nous allons introduire de nouvelles fonctions Y_S dans la section 5.1.3.

La remarque suivante permettra de faire les calculs dans le cas du niveau 2.

Remarque 5.1.11. *Pour tout ensemble $A \subset \{1,\dots,2g+1\}$, les constantes f_A^2 se calculent en fonction des racines de f et des thêta constantes de niveau 2 :*

$$f_A^2 = \frac{\prod_{\substack{i\in\mathcal{U}\cap A\\ j\in\mathcal{U}\setminus A}}(a_i-a_j)\prod_{\substack{i\in\mathcal{U}^c\cap A^c\\ j\in A\setminus\mathcal{U}}}(a_i-a_j)}{\prod_{\substack{i\in(\mathcal{U}\circ C)\cap(A\circ C)\\ j\in(\mathcal{U}\circ C)\setminus(A\circ C)}}(a_i-a_j)\prod_{\substack{i\in(\mathcal{U}\circ C)^c\cap(A\circ C)^c\\ j\in(\mathcal{U}\circ C)\setminus(A\circ C)}}(a_i-a_j)} \frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]^2}.$$

Dans la suite nous étudions principalement les fonctions t_A avec $\#A \leqslant g$. Les autres peuvent en être déduites par la formule suivante.

Remarque 5.1.12. *Pour tout ensemble A, nous avons les relations*

$$f_{A^c} = f_A(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A\circ C_A}\zeta''_g}, \qquad t_{A^c}(z) = t_A(z)(-1)^{\lfloor\frac{g+1-\#A}{2}\rfloor}(-1)^{2\,{}^t\eta'_{C_A}\zeta''_g}.$$

En particulier si A est de cardinal g ou $g+1$ alors $C_A = \emptyset$ et

$$f_{A^c} = f_A(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A}\zeta''_g}, \qquad t_{A^c}(z) = t_A(z).$$

Les produits $\prod f_{A_i}$ ont des propriétés très intéressantes. En particulier, sous certaines conditions, ils s'expriment uniquement en fonction de produits de racines $\sqrt{<a_i - a_j>}$. Cette étude est effectuée dans la section suivante.

5.1.2 Propriétés des constantes f_A

Le plan général de cette section est le suivant
- Définition d'un ensemble $\mathcal{E}$ (page 95).
- Étude de certaines fractions de 4 thêta constantes (page 96).
- Étude de f_A^2 (page 102).
- Étude de certaines fractions de 8 thêta constantes (page 104).
- Étude de la dépendance de $f_A(C_A)$ par rapport au choix de C_A (page 107).
- Étude de certaines fractions de 4 constantes f_A (page 108).

La plupart des propriétés de cette partie ne sont utiles que pour prouver les théorèmes de la partie 5.1.4. Les preuves, qui consistent en majorité à manipuler des ensembles, peuvent être ignorée en première lecture.

Ensemble $\mathcal{E}$

Nous allons considérer des éléments d'un certain ensemble $\mathcal{E}$ défini comme suit :

Définition 5.1.13. *Soit $\mathcal{E}$ l'ensemble des produits d'un élément de $\bar{\mathbb{Q}}$ et de puissances de $\sqrt{< a_i - a_j >}$. Soit E un élément de $\mathcal{E}$, pour tout $i \neq j$ deux entiers de $\{1, \ldots, 2g+1\}$, notons $p_{i,j}[E]$ la puissance de $\sqrt{< a_i - a_j >}$ dans l'expression E et $s[E]$ la constante de $\bar{\mathbb{Q}}$ apparaissant dans le produit. Ainsi*

$$E = s[E] \prod_{i<j} \sqrt{< a_i - a_j >}^{p_{i,j}[E]}$$

Remarque 5.1.14. *L'ensemble $\mathcal{E}$ ne contient pas les constantes f_A. Cependant lors de l'étude de celles-ci et lors de leur utilisation, les produits de ces constantes qui apparaîtront appartiendront à $\mathcal{E}$.*

Pour montrer qu'un élément E appartient à $\mathcal{E}$, il suffit de vérifier que pour tout i, j dans $\{1, \ldots, 2g+1\}$, la valeur de $p_{i,j}[E]$ est entière ou de manière équivalente que celle de $p_{i,j}\left[E^2\right]$ est paire. Remarquons que pour tout éléments E et F de $\mathcal{E}$ nous avons $p_{i,j}[EF] = p_{i,j}[E] + p_{i,j}[F]$. Pour tout $i \in \{1, \ldots, 2g+1\}$, et $A \subset \{1, \ldots, 2g+1\}$ définissons la fonction $\delta_i(A)$ qui vaut 1 si i appartient à A et 0 sinon. Pour tout ensemble A et B, nous avons

$$\delta_i(A \circ B) = \delta_i(A) + \delta_i(B) - 2\delta_i(A \cap B)$$

et donc

$$(-1)^{\delta_i(A \circ B)} = (-1)^{\delta_i(A)+\delta_i(B)}.$$

Pour prouver des propriétés sur $p_{i,j}$, nous utiliserons plusieurs fois le lemme suivant qui a été prouvé par Van Wamelen, mais peut se redémontrer facilement avec une table de vérité.

Lemme 5.1.15. *Pour tous sous-ensembles A_1, A_2, A_3, A_4 de $\{1, \ldots, 2g+1\} \cup \{\infty\}$ tels que*

$$A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset,$$

la somme

$$\sum_{k=1}^{4} (-1)^{\delta_i(A_k)+\delta_j(A_k)}$$

est divisible par 4.

Fractions avec 4 thêta constantes

Théorème 5.1.16. *Soient V et V' deux sous-ensembles de cardinal $g+1$ de $\{1, \ldots, 2g+1\} \cup \{\infty\}$. Soient deux ensembles $C \subset V \setminus V'$ et $C' \subset V' \setminus V$ de même cardinal. L'expression*

$$E = \frac{\theta[\eta_{\mathcal{U} \circ V}]\, \theta[\eta_{\mathcal{U} \circ V'}]}{\theta\left[\eta_{\mathcal{U} \circ V \circ (C \cup C')}\right]\, \theta\left[\eta_{\mathcal{U} \circ V' \circ (C \cup C')}\right]}$$

appartient à $\mathcal{E}$. De plus $s[E] = 1$ et

$$p_{i,j}[E] = \frac{(-1)^{\delta_i(C)+\delta_j(C)} - (-1)^{\delta_i(C')+\delta_j(C')}}{2} \frac{(-1)^{\delta_i(V \setminus (V' \cup C))+\delta_j(V \setminus (V' \cup C))} - (-1)^{\delta_i(V' \setminus (V \cup C'))+\delta_j(V' \setminus (V \cup C'))}}{2}.$$

La preuve de ce théorème se décompose en plusieurs cas suivant dans quel ensemble se trouve ∞. Si ∞ appartient à un seul des deux ensembles V ou V' alors la preuve avait été faite par Van Wamelen avec l'étude de deux sous-cas suivant que ∞ appartienne à C ou pas. Le cas où ∞ n'appartient à aucun des ensembles V et V' peut se ramener au cas où il appartient aux deux. Pour montrer le théorème dans ce dernier cas, nous allons nous ramener à utiliser trois fois la version prouvée par Van Wamelen.

Démonstration. Dans le cas où $\infty \in V$ mais $\infty \notin V'$, Van Wamelen ([vW98], théorème 2) a montré que

$$\prod_{\substack{l\in(V\setminus V')\setminus C\\ k\in C'}} \sqrt{<a_k-a_l>} \prod_{\substack{l\in(V'\setminus V)\setminus C'\\ k\in C}} \sqrt{<a_k-a_l>}\theta\left[\eta_{\mathcal{U}\circ V}\right]\theta\left[\eta_{\mathcal{U}\circ V'}\right]$$
$$= \prod_{\substack{l\in(V\setminus V')\setminus C\\ k\in C}} \sqrt{<a_k-a_l>} \prod_{\substack{l\in(V'\setminus V)\setminus C'\\ k\in C'}} \sqrt{<a_k-a_l>}\theta\left[\eta_{\mathcal{U}\circ V\circ(C\cup C')}\right]\theta\left[\eta_{\mathcal{U}\circ V'\circ(C\cup C')}\right].$$

Nous obtenons donc dans ce cas que $s\left[E\right]=1$ et

$$p_{i,j}\left[E\right] = p_{i,j}\left[\frac{\prod_{\substack{l\in V\setminus(V'\cup C)\\ k\in C}}\sqrt{<a_k-a_l>}\prod_{\substack{l\in V'\setminus(V\cup C')\\ k\in C'}}\sqrt{<a_k-a_l>}}{\prod_{\substack{l\in V\setminus(V'\cup C)\\ k\in C'}}\sqrt{<a_k-a_l>}\prod_{\substack{l\in V'\setminus(V\cup C')\\ k\in C}}\sqrt{<a_k-a_l>}}\right].$$

Notons que pour tous sous-ensembles disjoints A et B, la puissance de $\sqrt{<a_i-a_j>}$ qui apparaît dans

$$\prod_{\substack{k\in A\\ l\in B}}\sqrt{<a_k-a_l>}$$

est non nulle si et seulement si i appartient à A et j à B ou réciproquement. D'où

$$p_{i,j}\left[\prod_{k\in A,\ l\in B}\sqrt{<a_k-a_l>}\right] = \frac{1-(-1)^{\delta_i(A)}}{2}\frac{1-(-1)^{\delta_j(B)}}{2}+\frac{1-(-1)^{\delta_i(B)}}{2}\frac{1-(-1)^{\delta_j(A)}}{2}.$$

Nous obtenons alors l'expression cherchée.

L'expression étant symétrique, on en déduit immédiatement le cas où $\infty \in V'$ mais $\infty \notin V$.

Le cas où ∞ n'appartient à aucun des deux ensembles V et V' se ramène au cas où il appartient aux deux en considérant les complémentaires de V et V'.

$$E = \frac{\theta\left[\eta_{\mathcal{U}\circ V}\right]\theta\left[\eta_{\mathcal{U}\circ V'}\right]}{\theta\left[\eta_{\mathcal{U}\circ V\circ(C\cup C')}\right]\theta\left[\eta_{\mathcal{U}\circ V'\circ(C\cup C')}\right]} = \frac{\theta\left[\eta_{\mathcal{U}\circ V^c}\right]\theta\left[\eta_{\mathcal{U}\circ V'^c}\right]}{\theta\left[\eta_{\mathcal{U}\circ V^c\circ(C\cup C')}\right]\theta\left[\eta_{\mathcal{U}\circ V'^c\circ(C\cup C')}\right]}\omega$$

où ω est le signe

$$\begin{aligned}
\omega &= (-1)^{2\,{}^t\eta'_{\mathcal{U}\circ V}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ V}\right)}(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ V'}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ V'}\right)}\\
&\quad (-1)^{2\,{}^t\eta'_{\mathcal{U}\circ V\circ(C\cup C')}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ V\circ(C\cup C')}\right)}(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ V'\circ(C\cup C')}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ V'\circ(C\cup C')}\right)}\\
&= (-1)^{2\,{}^t\left(\eta'_{\mathcal{U}\circ V}+\eta'_{\mathcal{U}\circ V'}+\eta'_{\mathcal{U}\circ V\circ(C\cup C')}+\eta'_{\mathcal{U}\circ V'\circ(C\cup C')}\right)\zeta''_g}(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ V}\eta''_{\mathcal{U}\circ V}}(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ V'}\eta''_{\mathcal{U}\circ V'}}\\
&\quad (-1)^{4\,{}^t\left(\eta'_{\mathcal{U}\circ V}+\eta'_{C\cup C'}\right)\left(\eta''_{\mathcal{U}\circ V}+\eta''_{C\cup C'}\right)}(-1)^{4\,{}^t\left(\eta'_{\mathcal{U}\circ V'}+\eta'_{C\cup C'}\right)\left(\eta''_{\mathcal{U}\circ V'}+\eta''_{C\cup C'}\right)}\\
&= (-1)^{4\left({}^t\eta'_{\mathcal{U}\circ V}\eta''_{C\cup C'}+{}^t\eta'_{C\cup C'}\eta''_{\mathcal{U}\circ V}+{}^t\eta'_{\mathcal{U}\circ V'}\eta''_{C\cup C'}+{}^t\eta'_{C\cup C'}\eta''_{\mathcal{U}\circ V'}\right)}\\
&= (-1)^{4\left({}^t\eta'_{V\circ V'}\eta''_{C\cup C'}+{}^t\eta'_{C\cup C'}\eta''_{V\circ V'}\right)}\\
&= e_2\left(\eta_{V\circ V'},\eta_{C\cup C'}\right).
\end{aligned}$$

Le cardinal de $C\cup C'$ est pair (car C et C' sont disjoints et de même cardinal). Par ailleurs,

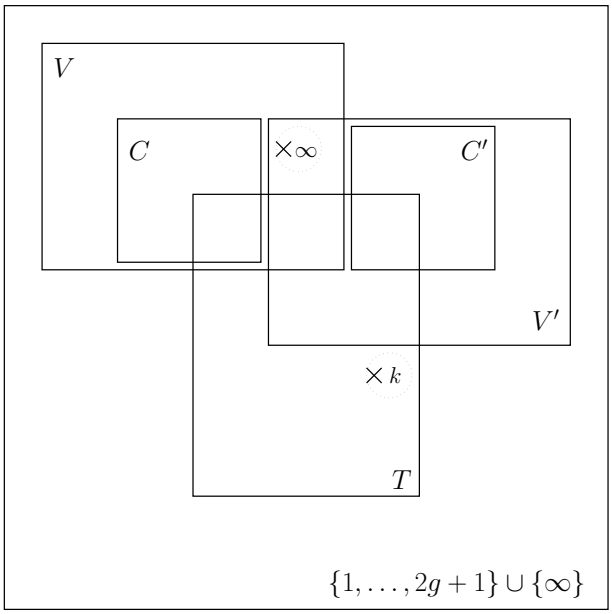
$$\#(V\circ V') = \#V+\#V'-2\#(V\cap V') = 2(g+1)-2\#(V\cap V')\equiv 0 \mod 2.$$

Comme C est inclus dans V et C' dans V', l'intersection de $V\cup V'$ et $C\cup C'$ est de cardinal pair. D'après la propriété 2.3.17, nous obtenons que ω est égal à 1. Remarquons que $C\subset V'^c\setminus V^c$ et $C'\subset V^c\setminus V'^c$ et supposons le théorème prouvé dans le cas où ∞ appartient aux deux ensembles. Nous obtenons alors que $s\left[E\right]=1$ et

$$p_{i,j}\left[E\right] = \frac{(-1)^{\delta_i(C')+\delta_j(C')}-(-1)^{\delta_i(C)+\delta_j(C)}}{2}\frac{(-1)^{\delta_i(V^c\setminus(V'^c\cup C'))+\delta_j(V^c\setminus(V'^c\cup C'))}-(-1)^{\delta_i(V'^c\setminus(V^c\cup C))+\delta_j(V'^c\setminus(V^c\cup C))}}{2}.$$

Or $V^c \setminus (V'^c \cup C') = V' \setminus (V \cup C')$, ce qui donne alors la formule cherchée pour $p_{i,j}[E]$.

Supposons maintenant que ∞ appartient aux deux ensembles V et V'. Il existe alors un élément k de $\{1, \ldots, 2g+1\}$ n'appartenant pas à ces deux ensembles. Soit T un sous ensemble de $\{1, \ldots, 2g+1\}$ de $g+1$ éléments contenant k.



Nous allons décomposer E de la manière suivante :

$$E = \frac{\theta[\eta_{\mathcal{U}\circ V}]\,\theta\left[\eta_{\mathcal{U}\circ V'\circ\{k,\infty\}}\right]}{\theta\left[\eta_{\mathcal{U}\circ V\circ(C\cup C')}\right]\theta\left[\eta_{\mathcal{U}\circ V'\circ\{k,\infty\}\circ(C\cup C')}\right]} \frac{\theta\left[\eta_{\mathcal{U}\circ V'\circ(C\cup C')\circ\{k,\infty\}}\right]\theta\left[\eta_{\mathcal{U}\circ T\circ\{k,\infty\}}\right]}{\theta\left[\eta_{\mathcal{U}\circ V'\circ(C\cup C')}\right]\theta[\eta_{\mathcal{U}\circ T}]} \frac{\theta[\eta_{\mathcal{U}\circ T}]\,\theta[\eta_{\mathcal{U}\circ V'}]}{\theta\left[\eta_{\mathcal{U}\circ T\circ\{k,\infty\}}\right]\theta\left[\eta_{\mathcal{U}\circ V'\circ\{k,\infty\}}\right]}.$$

Sur chacune de ces trois fractions, nous pouvons appliquer le cas particulier précédent du théorème. La figure 5.1 précise les conditions d'application du théorème : les ensembles V et V' du théorème sont ceux avec un bord continu, les ensembles C et C' sont grisés. Il est alors évident que $s[E] = 1$. Pour $p_{i,j}$, nous obtenons la formule suivante en se rappelant que $\delta_i(\infty) = 0$:

$$\begin{aligned} p_{i,j}[E] = {} & \frac{(-1)^{\delta_i(C)+\delta_j(C)} - (-1)^{\delta_i(C')+\delta_j(C')}}{2} \\ & \frac{(-1)^{\delta_i(V\setminus(V'\cup C))+\delta_j(V\setminus(V'\cup C))} - (-1)^{\delta_i((V'\circ\{k,\infty\})\setminus(V\cup C'))+\delta_j((V'\circ\{k,\infty\})\setminus(V\cup C'))}}{2} \\ & - \frac{(-1)^{\delta_i(k)+\delta_j(k)} - 1}{2} \\ & \frac{(-1)^{\delta_i(T\setminus(V'\circ(C\cup C')\cup\{k\}))+\delta_j(T\setminus(V'\circ(C\cup C')\cup\{k\}))} - (-1)^{\delta_i((V'\circ(C\cup C'))\setminus T)+\delta_j((V'\circ(C\cup C'))\setminus T)}}{2} \\ & + \frac{(-1)^{\delta_i(k)+\delta_j(k)} - 1}{2} \frac{(-1)^{\delta_i(T\setminus(V'\cup\{k\}))+\delta_j(T\setminus(V'\cup\{k\}))} - (-1)^{\delta_i(V'\setminus T)+\delta_j(V'\setminus T)}}{2}. \end{aligned}$$

Quand i et j sont différents de k, les termes $(-1)^{\delta_i(k)+\delta_j(k)} - 1$ sont nuls et par conséquent nous obtenons

$$\begin{aligned} p_{i,j}[E] = {} & \frac{(-1)^{\delta_i(C)+\delta_j(C)} - (-1)^{\delta_i(C')+\delta_j(C')}}{2} \\ & \frac{(-1)^{\delta_i(V\setminus(V'\cup C))+\delta_j(V\setminus(V'\cup C))} - (-1)^{\delta_i(V'\setminus(V\cup C'))+\delta_j(V'\setminus(V\cup C'))}}{2}, \end{aligned}$$

FIGURE 5.1 – Les trois applications du cas particuliers du théorème 5.1.16 dans sa preuve

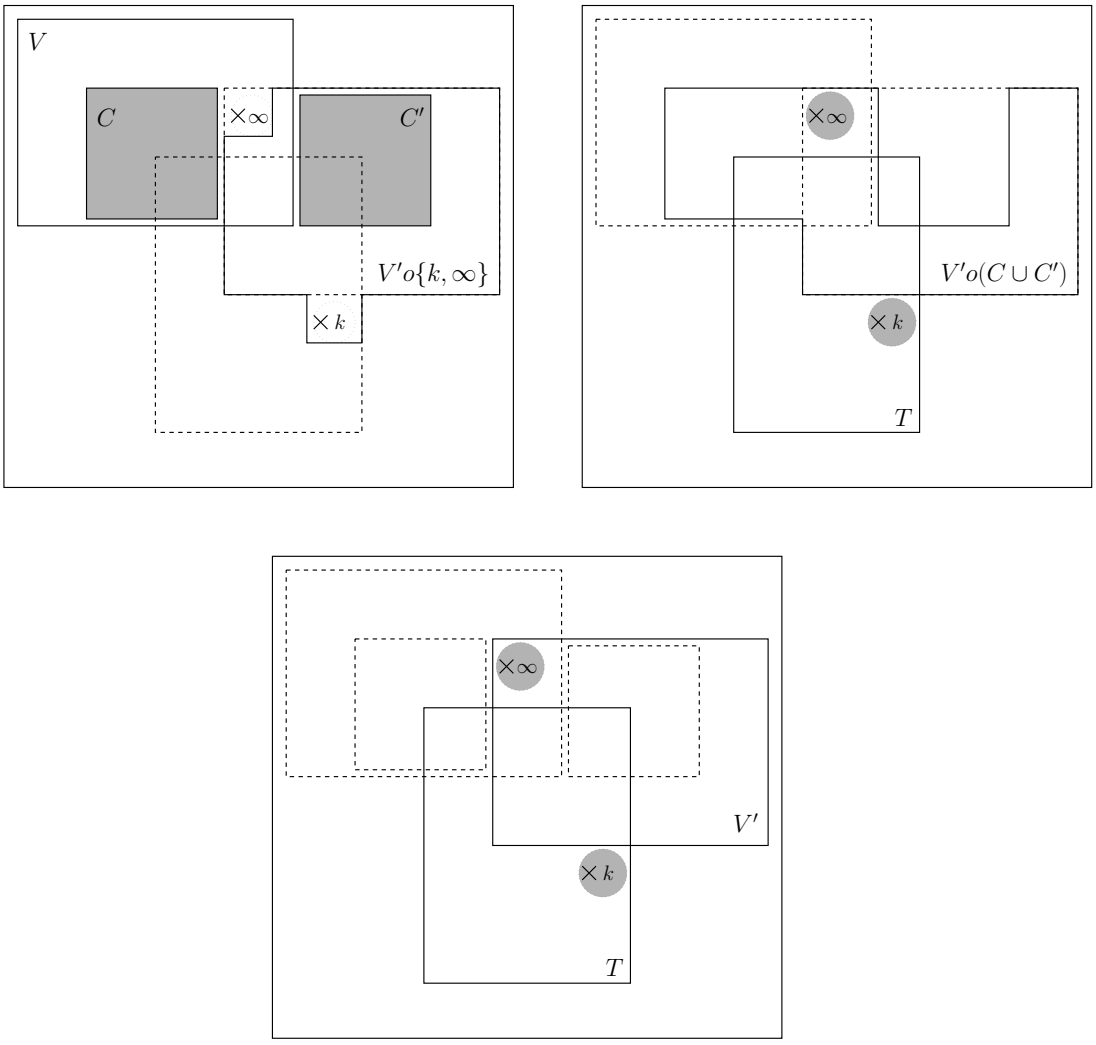


Tableau 5.2 – Table de vérité pour la preuve du théorème 5.1.16

j appartient à	$(-1)^{\delta_j(T\setminus V')}$	$(-1)^{\delta_j(V'\setminus T)}$	$(-1)^{\delta_j(T\setminus(V'\cup C))+\delta_j(T\cap C')}$	$(-1)^{\delta_j((V'\circ(C\cup C'))\setminus T)}$	α
$(T\cup V'\cup C)^c$	1	1	1	1	0
$C\setminus T$	1	1	1	-1	2
$C\cap T$	-1	1	1	1	2
$T\setminus(V'\cup C)$	-1	1	-1	1	0
$(T\cap V')\setminus C'$	1	1	1	1	0
$C'\cap T$	1	1	-1	1	-2
$C'\setminus T$	1	-1	1	1	-2
$V'\setminus(T\cup C')$	1	-1	1	-1	0

ce qui est la valeur cherchée. Supposons maintenant que $i=k$ (et par conséquent j doit être différent de k). Nous voulons montrer que $p_{k,j}[E]=0$. Or

$$\begin{aligned} p_{k,j}[E] &= \frac{(-1)^{\delta_j(C)}-(-1)^{\delta_j(C')}}{2}\frac{(-1)^{\delta_j(V\setminus(V'\cup C))}+(-1)^{\delta_j(V'\setminus(V\cup C'))}}{2} \\ &\quad +\frac{(-1)^{\delta_j(T\setminus(V'\cup C))+\delta_j(T\cap C')}-(-1)^{\delta_j((V'\circ(C\cup C'))\setminus T)}}{2}-\frac{(-1)^{\delta_j(T\setminus V')}-(-1)^{\delta_j(V'\setminus T)}}{2}. \end{aligned}$$

Il est clair que, pour le premier terme,

$$\frac{(-1)^{\delta_j(C)}-(-1)^{\delta_j(C')}}{2}\frac{(-1)^{\delta_j(V\setminus(V'\cup C))}+(-1)^{\delta_j(V'\setminus(V\cup C'))}}{2}=\begin{cases} 0 & j\notin(C\cup C'),\\ -1 & j\in C,\\ 1 & j\in C'.\end{cases}$$

Posons

$$\alpha=-(-1)^{\delta_j(T\setminus V')}+(-1)^{\delta_j(V'\setminus T)}+(-1)^{\delta_j(T\setminus(V'\cup C))+\delta_j(T\cap C')}-(-1)^{\delta_j((V'\circ(C\cup C'))\setminus T)}.$$

Une table de vérité 5.2 permet alors de montrer que $\alpha/2$ est l'opposé du premier terme. Nous avons donc prouvé le théorème dans ce cas. □

Théorème 5.1.17. *Soient T et T' deux sous-ensembles de cardinal $g+1$ de $\{1,\dots,2g+1\}\cup\{\infty\}$. Soient deux ensembles $S\subset(T\cup T')^c$ et $S'\subset T\cap T'$ de même cardinal. L'expression*

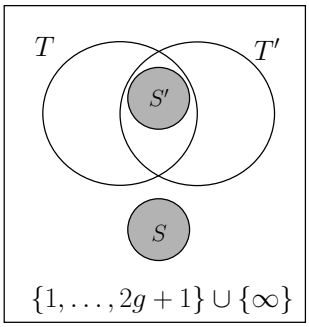
$$E=\frac{\theta\left[\eta_{\mathcal{U}\circ T}\right]\theta\left[\eta_{\mathcal{U}\circ T'}\right]}{\theta\left[\eta_{\mathcal{U}\circ T\circ(S\cup S')}\right]\theta\left[\eta_{\mathcal{U}\circ T'\circ(S\cup S')}\right]}$$

appartient à $\mathcal{E}$. De plus

$$p_{i,j}\left[E\right]=\frac{(-1)^{\delta_i(S)+\delta_j(S)}-(-1)^{\delta_i(S')+\delta_j(S')}}{2}\frac{(-1)^{\delta_i(T\cup T'\cup S)+\delta_j(T\cup T'\cup S)}-(-1)^{\delta_i((T\cap T')\setminus S')+\delta_j((T\cap T')\setminus S')}}{2},$$

$$s\left[E\right]=(-1)^{2\,{}^t\eta'_{S\cup S'}\zeta''_g}.$$

Ce théorème est une reformulation du théorème 5.1.16 précédent. Sa philosophie est de transformer les ensembles T et T' en deux ensembles $T\circ(S\cup S')$ et $T'\circ(S\cup S')$ en retirant des éléments de $T\cap T'$ et en rajoutant des éléments de $(T\cup T')^c$. Il correspond à la figure :



Démonstration. D'après la propriété 3.1.2,

$$E = \frac{\theta\left[\eta_{\mathcal{U}\circ T}\right]\theta\left[\eta_{\mathcal{U}\circ T'}\right]}{\theta\left[\eta_{\mathcal{U}\circ T\circ(S\cup S')}\right]\theta\left[\eta_{\mathcal{U}\circ T'\circ(S\cup S')}\right]} = \frac{\theta\left[\eta_{\mathcal{U}\circ T^c}\right]\theta\left[\eta_{\mathcal{U}\circ T'}\right]}{\theta\left[\eta_{\mathcal{U}\circ T^c o(S\cup S')}\right]\theta\left[\eta_{\mathcal{U}\circ T'\circ(S\cup S')}\right]}\omega$$

avec d'après 2.3.18,

$$\begin{aligned}\omega &= (-1)^{2\,{}^t\eta'_{\mathcal{U}\circ T}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ T}\right)}(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ T\circ(S\cup S')}\left(\zeta''_g-2\eta''_{\mathcal{U}\circ T\circ(S\cup S')}\right)}\\ &= (-1)^{2\,{}^t\eta'_{S\cup S'}\zeta''_g}(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ T}\eta''_{\mathcal{U}\circ T}}(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ T\circ(S\cup S')}\eta''_{\mathcal{U}\circ T\circ(S\cup S')}}\\ &= (-1)^{2\,{}^t\eta'_{S\cup S'}\zeta''_g}.\end{aligned}$$

Pour conclure, nous appliquons le théorème 5.1.16 aux ensembles suivants

$$V = T^c, \quad V' = T', \qquad C = S, \quad C' = S'.$$

Nous obtenons la valeur cherchée de $s[E]$ et

$$p_{i,j}\left[E\right] = \frac{(-1)^{\delta_i(S)+\delta_j(S)} - (-1)^{\delta_i(S')+\delta_j(S')}}{2} \frac{(-1)^{\delta_i(T^c\setminus(T'\cup S))+\delta_j(T^c\setminus(T'\cup S))} - (-1)^{\delta_i(T'\setminus(T^c\cup S'))+\delta_j(T'\setminus(T^c\cup S'))}}{2}.$$

Or $T^c \setminus (T' \cup S)$ est égal à $(T \cup T' \cup S)^c$ donc

$$\delta_i(T^c \setminus (T' \cup S)) = 1 + \delta_i(T \cup T' \cup S)$$

et de même pour δ_j. Par ailleurs nous avons $T' \setminus (T^c \cup S') = (T \cap T') \setminus S'$, ce qui termine la preuve. □

Une application directe de ce théorème est le corollaire suivant dû à Van Wamelen.

Corollaire 5.1.18. *Pour tous sous-ensembles A_1 et A_2 de cardinal $g+1$ de $\{1,\dots,2g+1\}\cup\{\infty\}$, l'expression $\frac{\theta\left[\eta_{\mathcal{U}\circ A_1}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A_2}\right]^2}$ appartient à $\mathcal{E}$ et*

$$p_{i,j}\left[\frac{\theta\left[\eta_{\mathcal{U}\circ A_1}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A_2}\right]^2}\right] = \frac{(-1)^{\delta_i(A_1)+\delta_j(A_1)} - (-1)^{\delta_i(A_2)+\delta_j(A_2)}}{2},$$

$$s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ A_1}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A_2}\right]^2}\right] = (-1)^{2\,{}^t\eta'_{A_1\circ A_2}\zeta''_g}.$$

Démonstration. Appliquons le théorème 5.1.17 à

$$T = T' = A_1, \qquad S = A_2 \setminus A_1, \qquad S' = A_1 \setminus A_2.$$

Posons

$$E = \frac{\theta\left[\eta_{\mathcal{U}\circ A_1}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A_2}\right]^2}.$$

Comme $S \cup S' = A_1 \circ S_2$, nous obtenons la bonne valeur pour $s[E]$. Par ailleurs, nous avons

$$\begin{aligned} p_{i,j}[E] &= \frac{(-1)^{\delta_i(A_2\setminus A_1)+\delta_j(A_2\setminus A_1)} - (-1)^{\delta_i(A_1\setminus A_2)+\delta_j(A_1\setminus A_2)}}{2} \\ &\quad \frac{(-1)^{\delta_i(A_1\cup A_2)+\delta_j(A_1\cup A_2)} - (-1)^{\delta_i(A_1\cap A_2)+\delta_j(A_1\cap A_2)}}{2}. \end{aligned}$$

Avec les bonnes factorisations, nous obtenons :

$$\begin{aligned} p_{i,j}[E] &= (-1)^{\delta_i(A_1\cap A_2)+\delta_j(A_1\cap A_2)} \frac{(-1)^{\delta_i(A_2)+\delta_j(A_2)} - (-1)^{\delta_i(A_1)+\delta_j(A_1)}}{2} \\ &\quad (-1)^{\delta_i(A_1\cap A_2)+\delta_j(A_1\cap A_2)} \frac{(-1)^{\delta_i(A_1\circ A_2)+\delta_j(A_1\circ A_2)} - 1}{2} \\ p_{i,j}[E] &= \frac{(-1)^{\delta_i(A_2)+\delta_j(A_2)} - (-1)^{\delta_i(A_1)+\delta_j(A_1)}}{2} \frac{(-1)^{\delta_i(A_1\circ A_2)+\delta_j(A_1\circ A_2)} - 1}{2}. \end{aligned}$$

Pour les indices i, j tels que $(-1)^{\delta_i(A_2)+\delta_j(A_2)} - (-1)^{\delta_i(A_1)+\delta_j(A_1)}$ n'est pas nul, une table de vérité montre que $(-1)^{\delta_i(A_1\circ A_2)+\delta_j(A_1\circ A_2)} = -1$. Nous obtenons donc

$$p_{i,j}[E] = \frac{(-1)^{\delta_i(A_2)+\delta_j(A_2)} - (-1)^{\delta_i(A_1)+\delta_j(A_1)}}{2} \frac{-1-1}{2} = \frac{(-1)^{\delta_i(A_1)+\delta_j(A_1)} - (-1)^{\delta_i(A_2)+\delta_j(A_2)}}{2}.$$

□

Remarque 5.1.19. *Comme $\eta_\infty = 0$, ce corollaire est toujours valide si A_1 et A_2 sont deux sous-ensembles de $\{1,\dots,2g+1\}$ de cardinal g ou $g+1$.*

Carré de f_A

Le corollaire 5.1.18 permet de montrer la propriété suivante. Notons que cette propriété implique que f_A^2 n'est pas définie sur le corps $\mathbb{Q}(a_i - a_j)$ mais sur le corps $\mathbb{Q}\left(\sqrt{< a_i - a_j >}\right)$.

Corollaire 5.1.20. *Pour tout sous-ensemble A de $\{1,\dots,2g+1\}$, la constante f_A^2 appartient à $\mathcal{E}$ et*

$$p_{i,j}\left[f_A^2\right] = \frac{(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})} - (-1)^{\delta_i(A)+\delta_j(A)}}{2},$$

$$s\left[f_A^2\right] = (-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A}\zeta''_g}.$$

En particulier f_A^2 est indépendant du sous-ensemble C_A choisi dans la définition 5.1.5.

Démonstration. D'après la définition 5.1.5, nous avons

$$f_A = \frac{\prod_{\substack{i\in\mathcal{U}\cap A\\ j\in\mathcal{U}\setminus A}} \sqrt{< a_i - a_j >} \prod_{\substack{i\in\mathcal{U}^c\cap A^c\\ j\in A\setminus\mathcal{U}}} \sqrt{< a_i - a_j >}}{\prod_{\substack{i\in(\mathcal{U}\circ C)\cap(A\circ C)\\ j\in(\mathcal{U}\circ C)\setminus(A\circ C)}} \sqrt{< a_i - a_j >} \prod_{\substack{i\in(\mathcal{U}\circ C)^c\cap(A\circ C)^c\\ j\in(\mathcal{U}\circ C)\setminus(A\circ C)}} \sqrt{< a_i - a_j >}} \frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]}{\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]}.$$

Pour tous sous-ensembles A et B de $\{1,\dots,2g+1\}$, posons $p'_{i,j}(A,B)$ la puissance de $\sqrt{< a_i - a_j >}$ dans

$$\prod_{\substack{k\in A\cap B\\ l\in A\setminus B}} \sqrt{< a_k - a_l >}.$$

Pour que $p'_{i,j}(A,B)$ soit non nul, il faut que l'un des indices i, j appartienne à $A\cap B$ et que l'autre indice se trouve dans A. Dans ce cas, $p'_{i,j}(A,B)$ est égal à 1. Nous avons donc

$$p'_{i,j}(A,B) = \frac{1-(-1)^{\delta_i(A)}}{2} \frac{1-(-1)^{\delta_j(A)}}{2} \frac{1-(-1)^{\delta_i(B)+\delta_j(B)}}{2}.$$

De la même façon,

$$\begin{aligned} p''_{i,j}(A,B) &:= p_{i,j}\left[\prod_{\substack{k\in A^c\cap B^c\\ l\in A\setminus B}}\sqrt{<a_k-a_l>}\right] \\ &= \frac{1+(-1)^{\delta_i(B)}}{2}\frac{1+(-1)^{\delta_j(B)}}{2}\frac{1-(-1)^{\delta_i(A)+\delta_j(A)}}{2}. \end{aligned}$$

Nous obtenons donc que

$$\begin{aligned} p_{i,j}\left[f_A^2\right] &= 2p'_{i,j}(\mathcal{U},A)+2p''_{i,j}(A,\mathcal{U})-2p'_{i,j}(\mathcal{U}\circ C,A\circ C)-2p''_{i,j}(A\circ C,\mathcal{U}\circ C)+p_{i,j}\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]^2}\right] \\ &= 2\frac{1-(-1)^{\delta_i(\mathcal{U})}}{2}\frac{1-(-1)^{\delta_j(\mathcal{U})}}{2}\frac{1-(-1)^{\delta_i(A)+\delta_j(A)}}{2} \\ &\quad +2\frac{1+(-1)^{\delta_i(\mathcal{U})}}{2}\frac{1+(-1)^{\delta_j(\mathcal{U})}}{2}\frac{1-(-1)^{\delta_i(A)+\delta_j(A)}}{2} \\ &\quad -2\frac{1-(-1)^{\delta_i(\mathcal{U}\circ C)}}{2}\frac{1-(-1)^{\delta_j(\mathcal{U}\circ C)}}{2}\frac{1-(-1)^{\delta_i(A\circ C)+\delta_j(A\circ C)}}{2} \\ &\quad -2\frac{1+(-1)^{\delta_i(\mathcal{U}\circ C)}}{2}\frac{1+(-1)^{\delta_j(\mathcal{U}\circ C)}}{2}\frac{1-(-1)^{\delta_i(A\circ C)+\delta_j(A\circ C)}}{2} \\ &\quad +\frac{(-1)^{\delta_i(\mathcal{U}\circ C)+\delta_j(\mathcal{U}\circ C)}-(-1)^{\delta_i(A\circ C)+\delta_j(A\circ C)}}{2} \end{aligned}$$

où nous avons appliqué le corollaire 5.1.18.

$$\begin{aligned} p_{i,j}\left[f_A^2\right] &= \left(1+(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}\right)\frac{1-(-1)^{\delta_i(A)+\delta_j(A)}}{2} \\ &\quad -\left(1+(-1)^{\delta_i(\mathcal{U}\circ C)+\delta_j(\mathcal{U}\circ C)}\right)\frac{1-(-1)^{\delta_i(A\circ C)+\delta_j(A\circ C)}}{2} \\ &\quad +\frac{(-1)^{\delta_i(\mathcal{U}\circ C)+\delta_j(\mathcal{U}\circ C)}-(-1)^{\delta_i(A\circ C)+\delta_j(A\circ C)}}{2} \\ &= \left(1+(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}\right)\frac{1-(-1)^{\delta_i(A)+\delta_j(A)}}{2} \\ &\quad -\left((-1)^{\delta_i(C)+\delta_j(C)}+(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}\right)\frac{(-1)^{\delta_i(C)+\delta_j(C)}-(-1)^{\delta_i(A)+\delta_j(A)}}{2} \\ &\quad +(-1)^{\delta_i(C)+\delta_j(C)}\frac{(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}-(-1)^{\delta_i(A)+\delta_j(A)}}{2}. \end{aligned}$$

En rassemblant les deux premiers termes puis en factorisant,

$$\begin{aligned} p_{i,j}\left[f_A^2\right] &= \frac{(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}-(-1)^{\delta_i(A)+\delta_j(A)}}{2}\left(1-(-1)^{\delta_i(C)+\delta_j(C)}+(-1)^{\delta_i(C)+\delta_j(C)}\right) \\ &= \frac{(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}-(-1)^{\delta_i(A)+\delta_j(A)}}{2}. \end{aligned}$$

Pour le signe, avec le corollaire 5.1.18, nous avons

$$s\left[f_A^2\right]=s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]^2}\right]=(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A}\zeta''_g}.$$

□

Quotient de 8 thêta constantes

Lors des calculs ultérieurs, nous aurons besoin de la propriété suivante

Propriété 5.1.21. *Soient $A_1, \dots, A_4$ quatre sous-ensembles de cardinaux $g+1$ de $\{1, \dots, 2g+1\} \cup \{\infty\}$ tels que $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$, Soit E l'expression $\prod_{k=1}^{4} \frac{\theta[\eta_{\mathcal{U} \circ A_k}]}{\theta[\eta_{\mathcal{U} \circ \mathcal{U}}]}$. Alors E est un élément de $\mathcal{E}$ qui vérifie*

$$p_{i,j}[E] = \frac{1}{4}\left(\sum_{k=1}^{4}(-1)^{\delta_i(A_k)+\delta_j(A_k)}\right) - (-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})},$$

$$s[E] = (-1)^{2\left({}^t\eta'_{A_1\cap A_2\cap A_3\cap A_4} + {}^t\eta'_{A_1\cup A_2\cup A_3\cup A_4}\right)\varsigma''_g}.$$

Notons que comme $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$, la somme $\sum_{k=1}^{4}(-1)^{\delta_i(A_k)+\delta_j(A_k)}$ est congrue à zéro modulo 4. La partie facile de la propriété est la puissance de $\sqrt{< a_i - a_j >}$ dans E. En effet, il suffit de trouver celle dans E^2 par le corollaire 5.1.18 puis de diviser par 2. Pour obtenir le signe, nous devons utiliser le théorème 5.1.17 qui permet de modifier les ensembles A_i pour nous ramener au cas où $A_1 = A_2$ et $A_3 = A_4$.

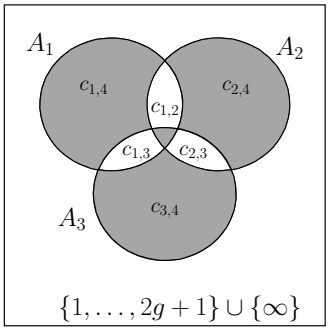
Démonstration. Montrons d'abord que E est un élément de $\mathcal{E}$. D'après le corollaire 5.1.18, E^2 est un élément de $\mathcal{E}$ et la puissance de $\sqrt{< a_i - a_j >}$ dans E^2 est

$$\begin{aligned} p_{i,j}\left[E^2\right] &= \sum_{k=1}^{4} \frac{(-1)^{\delta_i(A_k)+\delta_j(A_k)} - (-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}}{2} \\ &= \frac{1}{2}\left(\sum_{k=1}^{4}(-1)^{\delta_i(A_k)+\delta_j(A_k)}\right) - 2(-1)^{\delta_i(\mathcal{U})+\delta_j(\mathcal{U})}. \end{aligned}$$

Il est donc clair d'après le lemme 5.1.15 que pour tous i, j la puissance de $\sqrt{< a_i - a_j >}$ dans E^2 est paire et donc que $E \in \mathcal{E}$. Intéressons nous maintenant à la constante $s[E]$. Pour tous $i, j, k, l \in \{1, \dots, 4\}$ distincts posons

$$c_{i,j} = (A_i \cap A_j) \setminus (A_k \cup A_l).$$

En toute généralité, nous sommes dans la configuration suivante :



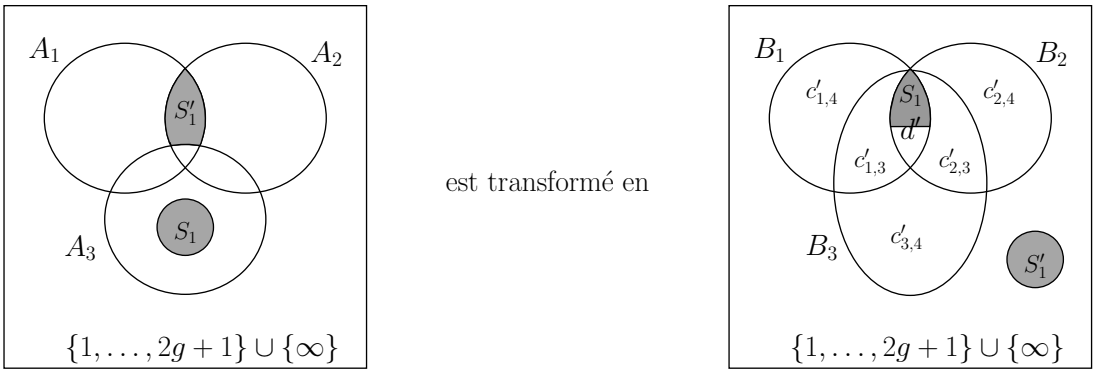
L'ensemble A_4 est grisé

Sans perte de généralité, nous pouvons modifier l'ordre des A_k : supposons que $c_{1,2}$ soit le plus petit des $c_{i,j}$. Appliquons alors le théorème 5.1.17 à

$$T = A_1, \qquad T' = A_2, \qquad S'_1 = A_1 \cap A_2 \setminus A_3, \qquad S_1 \subset A_3 \setminus (A_1 \cup A_2)$$

tels que $\#S_1 = \#S'_1$ (cela est possible car $c_{1,2} \leqslant c_{3,4}$). Nous avons rajouté un indice pour distinguer les ensembles S des applications suivantes du théorème 5.1.17. Posons alors

$$B_1 = A_1 \circ (S_1 \cup S'_1), \qquad B_2 = A_2 \circ (S_1 \cup S'_1), \qquad B_3 = A_3, \qquad B_4 = A_4.$$



Nous obtenons

$$s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ A_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right]=s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ B_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right](-1)^{2\,{}^t\eta'_{S_1\cup S_1'}\zeta''_g}.$$

Les ensembles B_k vérifient les mêmes propriétés que les A_k. Posons

$$c'_{i,j}=(B_i\cap B_j)\setminus(B_k\cup B_l),\qquad d'=\#\left(B_1\cap B_2\cap B_3\cap B_4\right),$$

alors

$$\#\left(B_1\cup B_2\cup B_3\cup B_4\right)=\#\left(B_1\cup B_2\cup B_3\right)=3(g+1)-c'_{1,3}-c'_{2,3}-2d'.$$

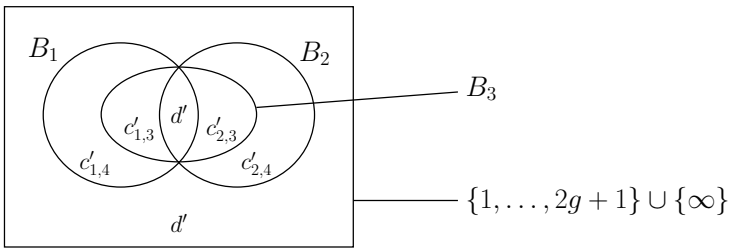
Or B_4' est l'union des parties correspondant à $c'_{1,4}$, $c'_{2,4}$, $c'_{3,4}$, et d' donc

$$g+1=\#B_4'=3(g+1)-2c'_{1,3}-2c'_{2,3}-2d'$$

ce qui implique que $\#\left(B_1\cup B_2\cup B_3\cup B_4\right)=2(g+1)-d'$ et donc que

$$\#\left(B_1\cup B_2\cup B_3\cup B_4\right)^c=d'=\#\left(B_1\cap B_2\cap B_3\cap B_4\right).$$

Par ailleurs, comme $\#A_3=g+1$, nous obtenons $c'_{3,4}=0$ et donc $B_3\subset B_1\cup B_2$. Visuellement, cela se traduit par la modification suivante de la dernière figure



Appliquons le théorème 5.1.17 à

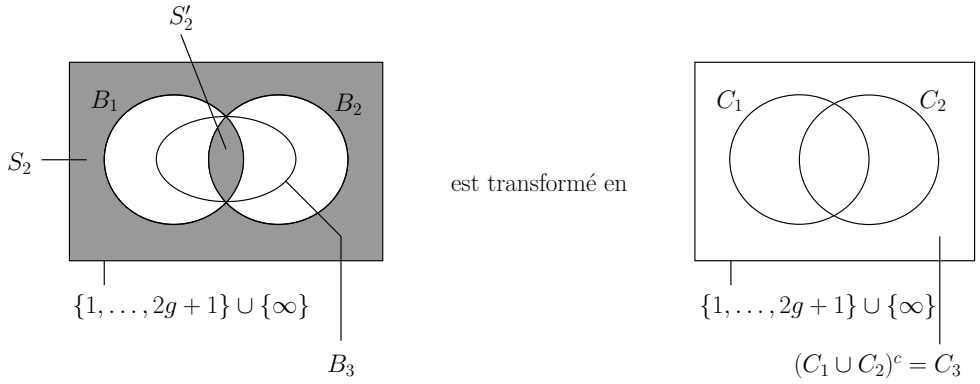
$$T=B_1,\qquad T'=B_3,$$

$$S_2=\left(B_1\cup B_2\cup B_3\cup B_4\right)^c,\qquad S_2'=B_1\cap B_2\cap B_3\cap B_4.$$

Posons

$$C_1=B_1\circ(S_2\cup S_2'),\qquad C_2=B_2,\qquad C_3=B_3\circ(S_2\cup S_2'),\qquad C_4=B_4.$$

Nous obtenons le dessin :



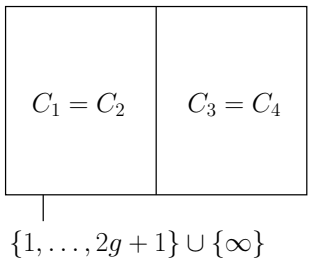
et, par le théorème 5.1.17, cela se traduit par la formule

$$s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ B_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right]=s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ C_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right](-1)^{2\eta'_{S_2\cup S_2'}\zeta''_g}.$$

D'après le dessin, nous avons $C_3=(C_1\cup C_2)^c$. Comme $C_1\circ C_2\circ C_3\circ C_4=\emptyset$, alors

$$C_4=C_3\cup(C_1\setminus C_2)\cup(C_2\setminus C_1),$$

les trois unions étant distinctes. Comme $\#C_3=\#C_4=g+1$, nous obtenons que $C_1\setminus C_2=\emptyset$ et $C_2\setminus C_1=\emptyset$ et donc que $C_1=C_2$. Nous sommes donc dans la configuration suivante



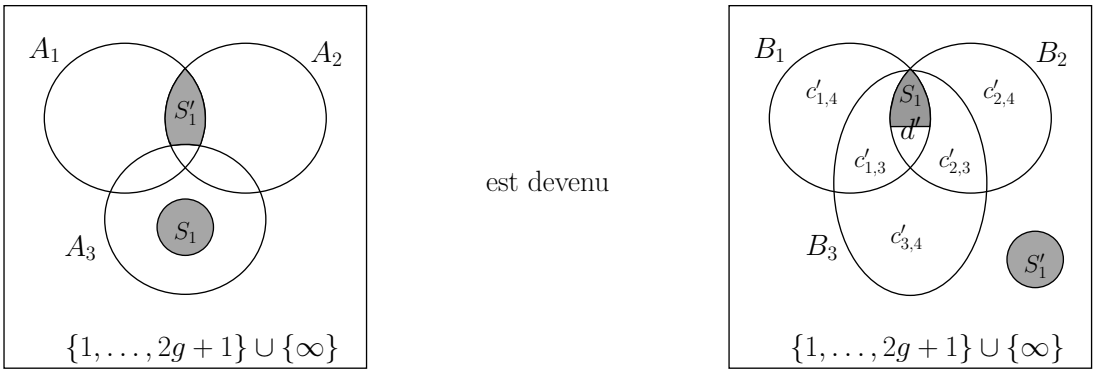
C'est-à-dire que les ensembles C_k vérifient $C_1=C_2=C_3^c=C_4^c$. D'où

$$s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ C_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right]=s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ C_1}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}\frac{\theta\left[\eta_{\mathcal{U}\circ C_1^c}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}\right]=s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ C_1}\right]^4}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^4}\right]=1.$$

En résumé,

$$\begin{aligned}
s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ A_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right] &= s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ B_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right](-1)^{2\,{}^t\eta'_{S_1\cup S_1'}\zeta''_g}\\
&= s\left[\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ C_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right](-1)^{2\eta'_{S_2\cup S_2'}\zeta''_g}(-1)^{2\,{}^t\eta'_{S_1\cup S_1'}\zeta''_g}\\
&= (-1)^{2\eta'_{S_2\cup S_2'}\zeta''_g}(-1)^{2\,{}^t\eta'_{S_1\cup S_1'}\zeta''_g}.
\end{aligned}$$

En reprenant le dessin



ou en travaillant formellement, nous obtenons que

$$\begin{array}{rcl}(B_1\cup B_2\cup B_3\cup B_4)^c & = & (A_1\cup A_2\cup A_3\cup A_4)^c\cup S_1',\\ B_1\cap B_2\cap B_3\cap B_4 & = & (A_1\cap A_2\cap A_3\cap A_4)\cup S_1.\end{array}$$

Donc, par définition de S_2 et S_2',

$$\begin{array}{rcccl}S_2 & = & (B_1\cup B_2\cup B_3\cup B_4)^c & = & (A_1\cup A_2\cup A_3\cup A_4)^c\cup S_1',\\ S_2' & = & B_1\cap B_2\cap B_3\cap B_4 & = & (A_1\cap A_2\cap A_3\cap A_4)\cup S_1\end{array}$$

et donc en remplaçant nous obtenons

$$\begin{array}{rcl}s\left[\displaystyle\prod_{k=1}^{4}\frac{\theta\left[\eta_{\mathcal{U}\circ A_k}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}\right] & = & (-1)^{2\eta'_{(A_1\cup A_2\cup A_3\cup A_4)^c\cup(A_1\cap A_2\cap A_3\cap A_4)\cup S_1\cup S_1'}\zeta_g''}(-1)^{2\,{}^t\eta'_{S_1\cup S_1'}\zeta_g''}\\ & = & (-1)^{2\,{}^t\eta'_{(A_1\cup A_2\cup A_3\cup A_4)^c\cup(A_1\cap A_2\cap A_3\cap A_4)}\zeta_g''}.\end{array}$$

□

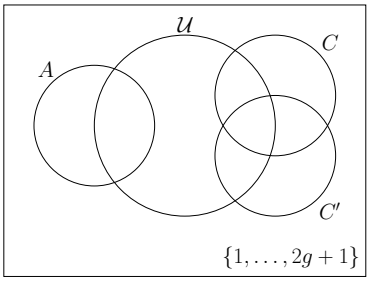
Dépendance de $f_A(C_A)$ par rapport à C_A

Le corollaire suivant précise la dépendance de $f_A(C_A)$ par rapport au choix de C_A dans la définition 5.1.5.

Corollaire 5.1.22. *Soit A un sous-ensemble de $\{1,\dots,2g+1\}$ auquel nous associons les sous-ensembles C et C' (c'est-à-dire que les ensembles C et C' sont deux choix de constantes C_A dans la définition 5.1.5). Les constantes $f_A(C)$ et $f_A(C')$ associées vérifient alors*

$$f_A(C')=\begin{cases}f_A(C)(-1)^{2\,{}^t\eta'_{(C\circ C')\cap\mathcal{U}}\zeta_g''} & \#A\leqslant g,\\ f_A(C)(-1)^{2\,{}^t\eta'_{(C\circ C')\cap\mathcal{U}}\zeta_g''}(-1)^{2\,{}^t\eta'_{(C\circ C')}\zeta_g''} & \#A\geqslant g.\end{cases}$$

Démonstration. D'après le corollaire 5.1.20, f_A^2 est indépendant du choix de C, nous avons donc l'égalité entre $f_A(C)$ et $f_A(C')$ au signe près. De plus, le quotient $f_A(C)/f_A(C')$ appartient à $\mathcal{E}$, déterminons son signe. D'après la remarque 5.1.12, nous pouvons supposer que $\#A\leqslant g$. Comme C et C' sont deux ensembles d'intersection vide avec A, nous sommes dans la configuration suivante :



$$\begin{aligned} s\left[\frac{f_A(C')}{f_A(C)}\right] &= s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]}{\theta\left[\eta_{\mathcal{U}\circ A\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]}\right] \\ &= s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]\theta\left[\eta_{\mathcal{U}\circ A\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]}{\theta\left[\eta_{\mathcal{U}\circ A\circ C'}\right]^2\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]^2}\right] \\ &= s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A\circ C'}\right]^2}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]^2}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C}\right]\theta\left[\eta_{\mathcal{U}\circ A\circ C'}\right]\theta\left[\eta_{\mathcal{U}\circ A\circ C}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^4}\right]. \end{aligned}$$

Nous avons la relation ensembliste suivante

$$(\mathcal{U}\circ C')\circ(\mathcal{U}\circ C)\circ(A\circ C')\circ(A\circ C)=\emptyset.$$

Par ailleurs, d'après les dessins de la page 109 ou grâce à des manipulations algébriques :

$$\begin{aligned} (\mathcal{U}\circ C')\cup(\mathcal{U}\circ C)\cup(A\circ C')\cup(A\circ C) &= A\cup\mathcal{U}\cup C\cup C', \\ (\mathcal{U}\circ C')\cap(\mathcal{U}\circ C)\cap(A\circ C')\cap(A\circ C) &= (A\cap\mathcal{U})\cup((C\cap C')\setminus\mathcal{U}). \end{aligned}$$

Avec le corollaire 5.1.18 et la propriété 5.1.21, nous en déduisons que

$$\begin{aligned} s\left[\frac{f_A(C')}{f_A(C)}\right] &= (-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A\circ C'}\zeta''_g}(-1)^{2\,{}^t\eta'_C\zeta''_g}(-1)^{2\,{}^t\eta'_{A\cup\mathcal{U}\cup C\cup C'}\zeta''_g+2\,{}^t(\eta'_{A\cap\mathcal{U}}+\eta'_{(C\cap C')\setminus\mathcal{U}})\zeta_g} \\ &= (-1)^{2\,{}^t\left(\eta'_{\mathcal{U}}+\eta'_A+\eta'_C+\eta'_{C'}\right)\zeta''_g}(-1)^{2\,{}^t\eta'_{A\cup\mathcal{U}\cup C\cup C'}\zeta''_g}(-1)^{2\,{}^t(\eta'_{A\cap\mathcal{U}}+\eta'_{(C\cap C')\setminus\mathcal{U}})\zeta_g}. \end{aligned}$$

Avec le dernier dessin de la page 109, nous obtenons

$$s\left[\frac{f_A(C')}{f_A(C)}\right]=(-1)^{2\,{}^t\eta'_{(C\circ C')\cap\mathcal{U}}\zeta''_g}.$$

□

Quotient de 4 constantes f_A

Un deuxième corollaire de la propriété 5.1.21 est

Corollaire 5.1.23. *Soient A_1 et A_2 deux sous-ensembles de $\{1,\dots,2g+1\}$ de cardinaux respectifs a_1 et a_2 et associés aux constantes C_1 et C_2 par la définition 5.1.5. Soit D un sous-ensemble de $\{1,\dots,2g+1\}$ tel que les cardinaux de $D\circ A_1$ et de $D\circ A_2$ sont égaux à g ou $g+1$. Alors l'expression*

$$E=\frac{f_{A_1\circ D}f_{A_2\circ D}}{f_{A_1}f_{A_2}}$$

appartient à $\mathcal{E}$ et, pour tous $i\neq j$ deux entiers de $\{1,\dots,2g+1\}$,

$$p_{i,j}[E]=\frac{1-(-1)^{\delta_i(D)+\delta_j(D)}}{2}\,\frac{(-1)^{\delta_i(A_1)+\delta_j(A_1)}+(-1)^{\delta_i(A_2)+\delta_j(A_2)}}{2},$$

$$s[E]=\begin{cases} (-1)^{2\,{}^t\eta'_{D\setminus(A_1\circ A_2)}\zeta''_g+2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g} & si\ a_1\leqslant a_2\leqslant g, \\ (-1)^{2\,{}^t\eta'_{D\setminus(A_1\circ A_2)}\zeta''_g+2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{C_2}\zeta''_g} & si\ a_1\leqslant g\leqslant a_2, \\ (-1)^{2\,{}^t\eta'_{D\setminus(A_1\circ A_2)}\zeta''_g+2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{C_1\circ C_2}\zeta''_g} & si\ g\leqslant a_1\leqslant a_2. \end{cases}$$

Remarque 5.1.24. *Formellement le quotient E s'écrit*

$$E=\frac{f_{A_1\circ D}(\emptyset)f_{A_2\circ D}(\emptyset)}{f_{A_1}(C_1)f_{A_2}(C_2)}.$$

Après avoir trouvé la valeur de $p_{i,j}[E]$ et montré que l'expression E appartient à $\mathcal{E}$, nous étudierons $s[E]$ dans le cas particulier où $\mathcal{U}\circ D$ est de cardinal g ou $g+1$ avant de traiter le cas général.

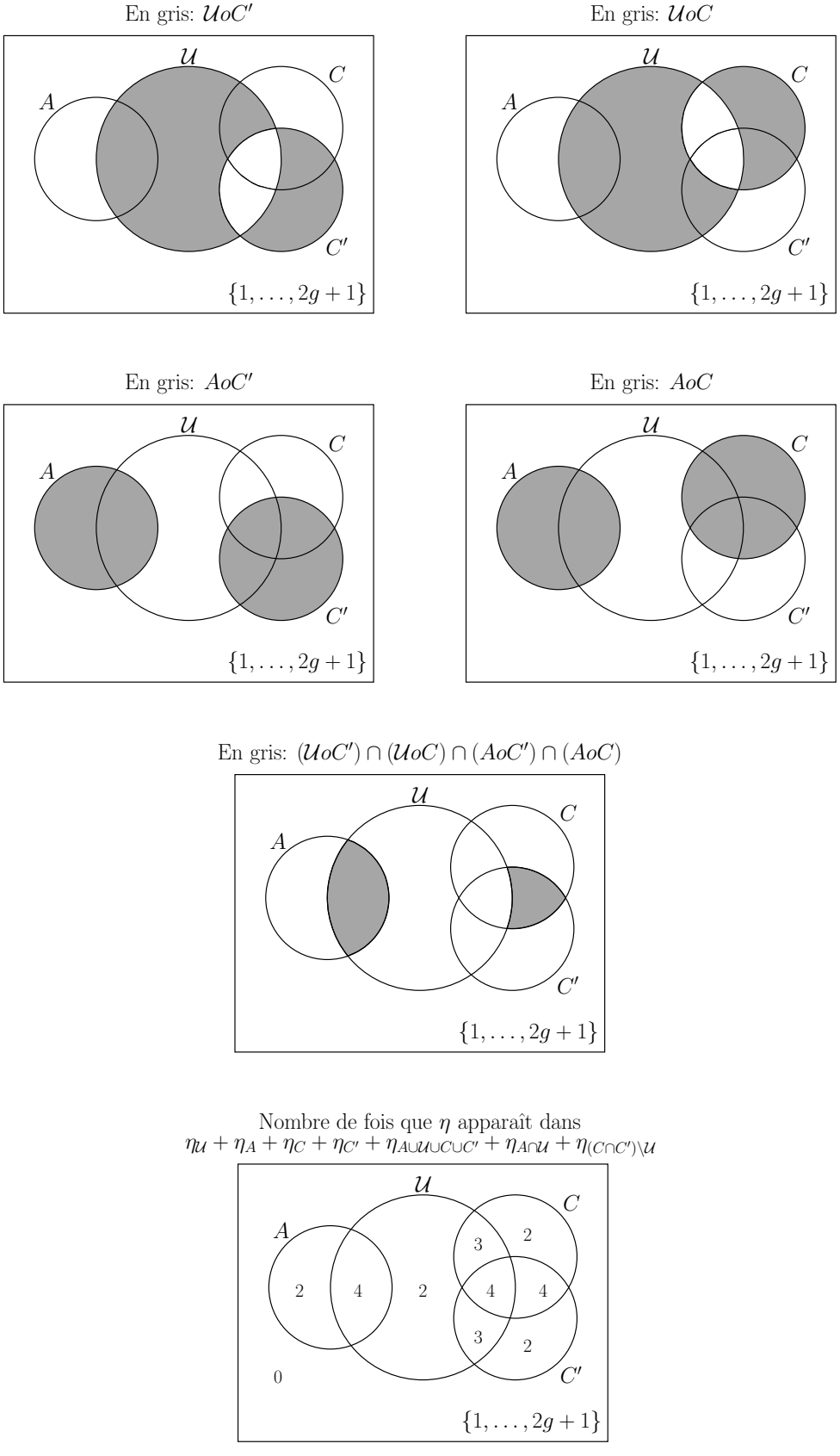


FIGURE 5.3 – Schémas pour le cas particulier de la preuve du corollaire 5.1.22

Démonstration. Grâce à la remarque 5.1.12, nous pouvons nous ramener au cas où $a_1 \leqslant a_2 \leqslant g$. Pour tous $i \neq j$ dans $\{1, \ldots, 2g+1\}$, le corollaire 5.1.20 prouve que le carré de notre expression appartient à $\mathcal{E}$ et que

$$\begin{aligned} p_{i,j}\left[\frac{f^2_{A_1\circ D} f^2_{A_2\circ D}}{f^2_{A_1} f^2_{A_2}}\right] &= \sum_{k=1}^{2} \frac{(-1)^{\delta_i(A_k)+\delta_j(A_k)} - (-1)^{\delta_i(A_k\circ D)+\delta_j(A_k\circ D)}}{2} \\ &= \frac{1-(-1)^{\delta_i(D)+\delta_j(D)}}{2} \sum_{k=1}^{2} (-1)^{\delta_i(A_k)+\delta_j(A_k)}. \end{aligned}$$

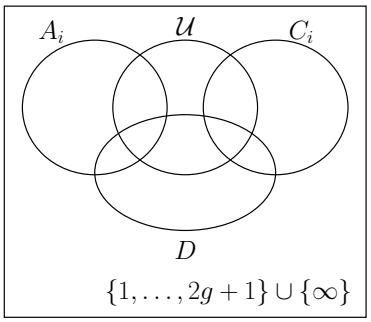
Cette valeur est un multiple de 2 et donc notre expression appartient bien à $\mathcal{E}$. Étudions maintenant la fonction s :

$$s\left[E\right] = s\left[\frac{f_{A_1\circ D} f_{A_2\circ D}}{f_{A_1} f_{A_2}}\right] = s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ A_1\circ C_1}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]\theta\left[\eta_{\mathcal{U}\circ A_2\circ C_2}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_1}\right]\theta\left[\eta_{\mathcal{U}\circ A_1\circ D}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_2}\right]\theta\left[\eta_{\mathcal{U}\circ A_2\circ D}\right]}\right].$$

Supposons, pour commencer, que $\mathcal{U}\circ D$ est de cardinal g ou $g+1$. De ce fait, la thêta constante $\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]$ n'est pas nulle. D'où

$$s\left[E\right] = s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]^2}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]\theta\left[\eta_{\mathcal{U}\circ A_1\circ C_1}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_1}\right]\theta\left[\eta_{\mathcal{U}\circ A_1\circ D}\right]}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]\theta\left[\eta_{\mathcal{U}\circ A_2\circ C_2}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_2}\right]\theta\left[\eta_{\mathcal{U}\circ A_2\circ D}\right]}\right].$$

D'après la définition 5.1.5, les ensembles C_i et A_i sont disjoints et nous sommes donc dans le cas suivant :



Grâce aux propriétés de commutativité de la différence symétrique,

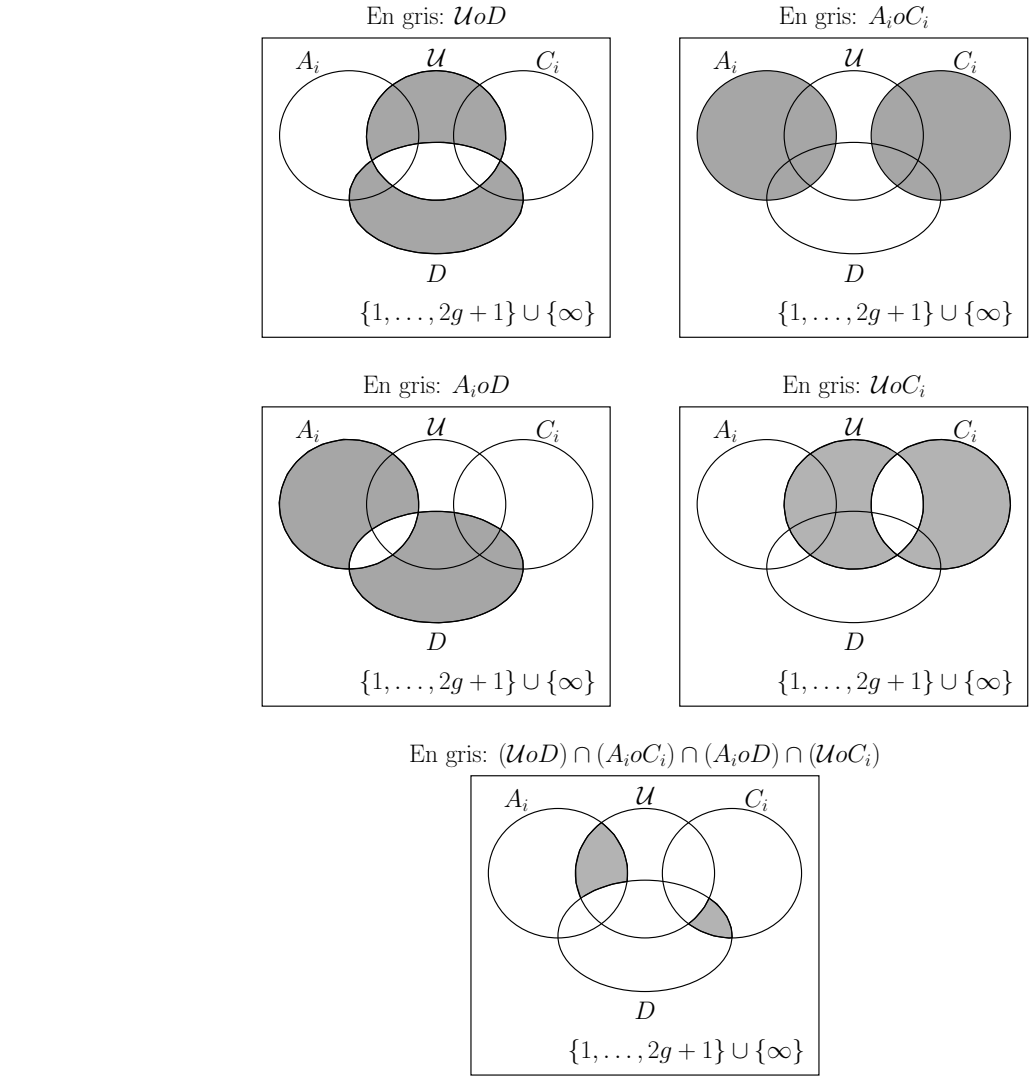
$$(\mathcal{U}\circ D)\circ(A_i\circ C_i)\circ(A_i\circ D)\circ(\mathcal{U}\circ C_i) = \emptyset.$$

Les égalités ensemblistes qui précisent l'union et l'intersection des quatre ensembles peuvent s'obtenir en étudiant les dessins de la page 111.

$$\begin{aligned} (\mathcal{U}\circ D)\cup(A_i\circ C_i)\cup(A_i\circ D)\cup(\mathcal{U}\circ C_i) &= \mathcal{U}\cup D\cup A_i\cup C_i, \\ (\mathcal{U}\circ D)\cap(A_i\circ C_i)\cap(A_i\circ D)\cap(\mathcal{U}\circ C_i) &= ((A_i\cap\mathcal{U})\setminus D)\cup((D\cap C_i)\setminus\mathcal{U}). \end{aligned}$$

Pour tout $i \in \{1,2\}$, le corollaire 5.1.18 et la propriété 5.1.21 montrent les égalités suivantes

$$\begin{aligned} s_i &:= s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]\theta\left[\eta_{\mathcal{U}\circ A_i\circ C_i}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_i}\right]\theta\left[\eta_{\mathcal{U}\circ A_i\circ D}\right]}\right] \\ s_i &= s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_i}\right]^2}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^2}{\theta\left[\eta_{\mathcal{U}\circ A_i\circ D}\right]^2}\right] s\left[\frac{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}\right]\theta\left[\eta_{\mathcal{U}\circ A_i\circ C_i}\right]\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ C_i}\right]\theta\left[\eta_{\mathcal{U}\circ A_i\circ D}\right]}{\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right]^4}\right] \\ s_i &= (-1)^{2\,{}^t\eta'_{C_i}\zeta''_g}(-1)^{2\,{}^t\eta'_{\mathcal{U}\circ A_i\circ D}\zeta''_g}(-1)^{2\,{}^t\eta'_{U\cup D\cup A_i\cup C_i}\zeta''_g}(-1)^{2\,{}^t\eta'_{(A_i\cap\mathcal{U})\setminus D}\zeta''_g+2\,{}^t\eta'_{(D\cap C_i)\setminus\mathcal{U}}\zeta''_g} \\ s_i &= (-1)^{2\,{}^t\left(\eta'_{C_i}+\eta'_{\mathcal{U}}+\eta'_{A_i}+\eta'_D+\eta'_{U\cup D\cup A_i\cup C_i}+\eta'_{(A_i\cap\mathcal{U})\setminus D}+\eta'_{(D\cap C_i)\setminus\mathcal{U}}\right)\zeta''_g}. \end{aligned}$$



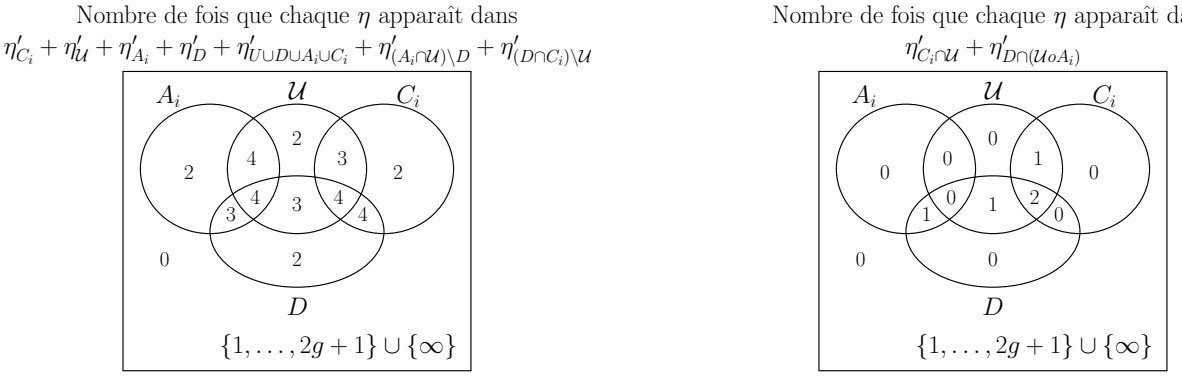


FIGURE 5.4 – Schémas pour le cas particulier de la preuve du corollaire 5.1.23

En reportant le nombre de fois que chaque sous-ensemble apparaît dans les schémas page 111, nous obtenons une expression simplifiée de s_i :

$$s_i = (-1)^{2\,{}^t\eta'_{C_i\cap\mathcal{U}}\zeta''_g + 2\,{}^t\eta'_{D\cap(\mathcal{U}\circ A_i)}\zeta''_g}.$$

Donc

$$\begin{aligned} s[E] &= s\left[\frac{\theta[\eta_{\mathcal{U}\circ\mathcal{U}}]^2}{\theta[\eta_{\mathcal{U}\circ\mathcal{U}\circ D}]^2}\right] s_1 s_2 \\ &= (-1)^{2\,{}^t\eta'_D\zeta''_g}(-1)^{2\,{}^t\eta'_{C_1\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{C_2\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{D\cap(A_1\circ A_2)}\zeta''_g}. \end{aligned}$$

Nous avons donc prouvé le corollaire dans le cas où $\mathcal{U}\circ D$ est de cardinal g ou $g+1$.

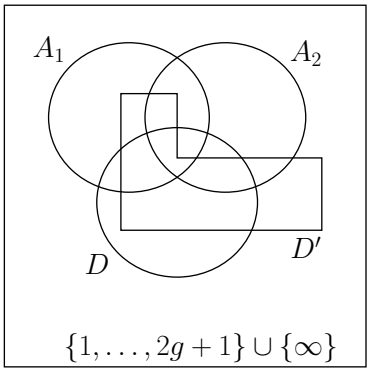
Montrons le cas général. Le lemme 5.1.25 justifiera l'existence d'un sous-ensemble D' de $\{1,\dots,2g+1\}$ tel que les ensembles $\mathcal{U}\circ D'$, $A_1\circ D'$ et $A_2\circ D'$ soient de cardinal g ou $g+1$. Nous avons alors

$$s[E] = s\left[\frac{f_{A_1\circ D} f_{A_2\circ D}}{f_{A_1\circ D'} f_{A_2\circ D'}}\right] s\left[\frac{f_{A_1\circ D'} f_{A_2\circ D'}}{f_{A_1} f_{A_2}}\right]$$

et nous pouvons alors appliquer la version précédente du corollaire sur la deuxième partie de cette expression. Il aurait été agréable de pouvoir l'appliquer aussi sur la première mais $\mathcal{U}\circ D\circ D'$ n'est, a priori, pas de cardinal g ou $g+1$. À la place, procédons comme suit

$$\begin{aligned} s[E] &= s\left[\frac{\theta[\eta_{\mathcal{U}\circ A_1\circ D'}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D'}]}{\theta[\eta_{\mathcal{U}\circ A_1\circ D}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D}]}\right](-1)^{2\,{}^t\eta'_{D'\setminus(A_1\circ A_2)}\zeta''_g}(-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g} \\ &= s\left[\frac{\theta[\eta_{\mathcal{U}\circ\mathcal{U}}]^4}{\theta[\eta_{\mathcal{U}\circ A_1\circ D}]^2\,\theta[\eta_{\mathcal{U}\circ A_2\circ D}]^2}\right](-1)^{2\,{}^t\eta'_{D'\setminus(A_1\circ A_2)}\zeta''_g}(-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g} \\ &\quad s\left[\frac{\theta[\eta_{\mathcal{U}\circ A_1\circ D'}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D'}]\,\theta[\eta_{\mathcal{U}\circ A_1\circ D}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D}]}{\theta[\eta_{\mathcal{U}\circ\mathcal{U}}]^4}\right] \\ &= (-1)^{2\,{}^t\eta'_{A_1\circ A_2}\zeta''_g}(-1)^{2\,{}^t\eta'_{D'\setminus(A_1\circ A_2)}\zeta''_g}(-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g} \\ &\quad s\left[\frac{\theta[\eta_{\mathcal{U}\circ A_1\circ D'}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D'}]\,\theta[\eta_{\mathcal{U}\circ A_1\circ D}]\,\theta[\eta_{\mathcal{U}\circ A_2\circ D}]}{\theta[\eta_{\mathcal{U}\circ\mathcal{U}}]^4}\right]. \end{aligned}$$

Nous nous retrouvons encore une fois avec quatre ensembles A_1, A_2, D, D' mais cette fois en position générique :



Nous avons encore la relation $(A_1\circ D)\circ(A_1\circ D')\circ(A_2\circ D)\circ(A_2\circ D') = \emptyset$. L'union et l'intersection sont précisées par les schéma de la page 113.

$$\begin{aligned} (A_1\circ D)\cup(A_1\circ D')\cup(A_2\circ D)\cup(A_2\circ D') &= (A_1\cup A_2\cup D\cup D')\setminus(A_1\cap A_2\cap D\cap D'), \\ (A_1\circ D)\cap(A_1\circ D')\cap(A_2\circ D)\cap(A_2\circ D') &= ((A_1\cap A_2)\setminus(D\cup D'))\cup((D\cap D')\setminus(A_1\cup A_2)). \end{aligned}$$

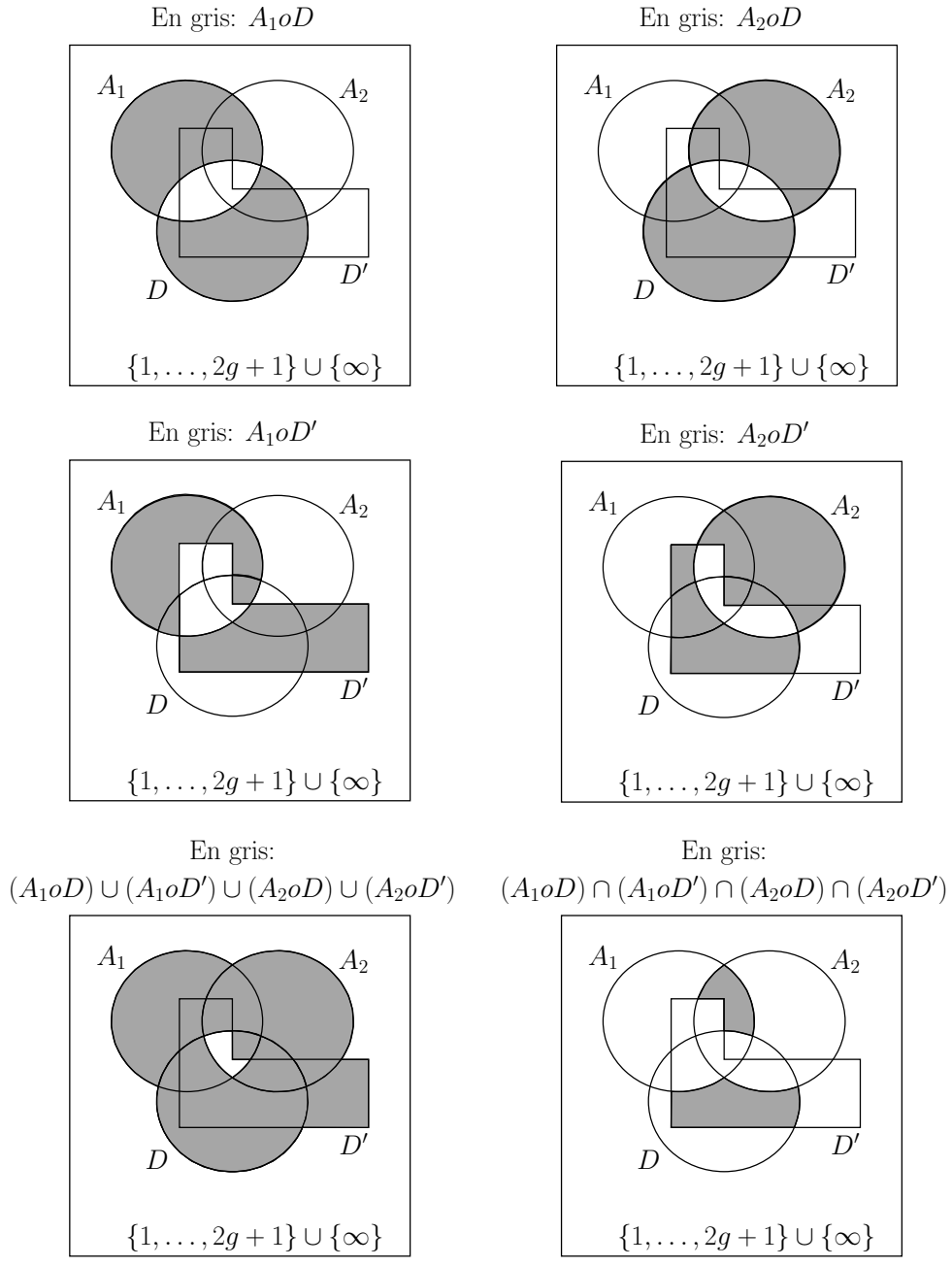


FIGURE 5.5 – Schémas pour le cas général de la preuve du corollaire 5.1.23

Nous obtenons donc

$$\begin{aligned}
s[E] = s\left[\frac{f_{A_1\circ D} f_{A_2\circ D}}{f_{A_1} f_{A_2}}\right] &= (-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{A_1\circ A_2}\zeta''_g}(-1)^{2\,{}^t\eta'_{D'\setminus(A_1\circ A_2)}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\left(\eta'_{((A_1\cap A_2)\setminus(D\cup D'))}+\eta'_{((D\cap D')\setminus(A_1\cup A_2))}\right)\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{(A_1\cup A_2\cup D\cup D')\setminus(A_1\cap A_2\cap D\cap D')}\zeta''_g}\\
&= (-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{(A_1\circ A_2)\cup D'}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{(A_1\cap A_2)\setminus D'}\zeta''_g+2\,{}^t\eta'_{(A_1\cap A_2\cap D)\setminus D'}\zeta''_g+\eta'_{(D\cap D')\setminus(A_1\cup A_2)}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{A_1\cup A_2\cup D\cup D'}\zeta''_g+2\,{}^t\eta'_{A_1\cap A_2\cap D\cap D'}\zeta''_g}\\
&= (-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{A_1\cup A_2\cup D'}\zeta''_g}(-1)^{2\,{}^t\eta'_{(D\cap D')\setminus(A_1\cup A_2)}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{A_1\cup A_2\cup D\cup D'}\zeta''_g}(-1)^{2\,{}^t\eta'_{A_1\cap A_2\cap D}\zeta''_g}\\
&= (-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{(D\cap D')\setminus(A_1\cup A_2)}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{D\setminus(A_1\cup A_2\cup D')}\zeta''_g}(-1)^{2\,{}^t\eta'_{A_1\cap A_2\cap D}\zeta''_g}\\
&= (-1)^{2\,{}^t\eta'_{(C_1\circ C_2)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{D\setminus(A_1\circ A_2)}\zeta''_g}.
\end{aligned}$$

□

Au cours de la preuve précédente, nous avons eu besoin du lemme technique suivant :

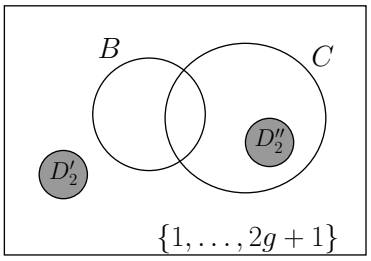
Lemme 5.1.25. *Soit A, B, C trois sous-ensembles de $\{1,\dots,2g+1\}$ de cardinaux inférieurs ou égaux à $g+1$ alors il existe $D \subset \{1,\dots,2g+1\}$ tel que les cardinaux de $A\circ D$, de $B\circ D$ et de $C\circ D$ soient égaux à g ou $g+1$.*

Démonstration. Sans perte de généralité nous pouvons supposer que A, B, C sont ordonnés suivant leur cardinal : $\#A \leqslant \#B \leqslant \#C$. Soit $D_1 \subset C^c$ de cardinal $g+1-\#C$ alors

$$\#C\circ D_1 = g+1, \qquad \#A\circ D_1 \leqslant g+1, \qquad \#B\circ D_1 \leqslant g+1.$$

Nous sommes donc ramenés au cas où $\#A \leqslant \#B \leqslant \#C = g+1$. Soit $n = \lceil \frac{g-\#B}{2} \rceil$, nous pouvons choisir deux ensembles $D'_2 \subset (B\cup C)^c$ et $D''_2 \subset C\setminus B$ de cardinaux n et nous avons alors pour $D_2 = D'_2 \cup D''_2$:

$$\#A\circ D_2 \leqslant g+1, \qquad \#B\circ D_2 \in \{g, g+1\}, \qquad \#C\circ D_2 = g+1.$$

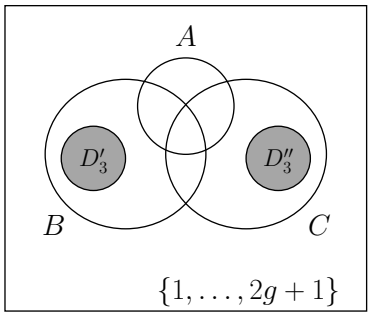


Si $\#A\circ D_2 \geqslant g$, le lemme est prouvé. Sinon nous nous sommes ramenés au cas où

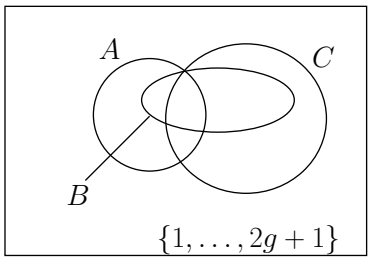
$$\#A < g \leqslant \#B \leqslant \#C = g+1.$$

En prenant $D_3 = D'_3 \cup D''_3$ avec $D'_3 \subset B\setminus(A\cup C)$ et $D''_3 \subset C\setminus(A\cup B)$ de même cardinal n', nous obtenons

$$\#B\circ D_3 = \#B, \qquad \#C\circ D_3 = \#C = g+1, \qquad \#A\circ D_3 = \#A + 2n'.$$



Cela peut ne pas être pas suffisant pour que $\#A \circ D_3$ soit de cardinal g ou $g+1$ et il se peut que nous ne puissions plus continuer le processus. Dans ce cas, cela provient du fait que C est inclus dans $A \cup B$ ou que B est inclus dans $A \cup C$. En réordonnant B et C si besoin, nous sommes ramenés au cas où A est de cardinal strictement plus petit que g, où B est inclu dans $A \cup C$ et les cardinaux de B et de C sont g ou $g+1$. Nous sommes donc dans la configuration suivante :



$$\#(A \cup B \cup C) = \begin{cases} \#A + g - \#(A \cap C) & \text{si } \#C = g \\ \#A + g + 1 - \#(A \cap C) & \text{si } \#C = g+1 \end{cases}.$$

Donc

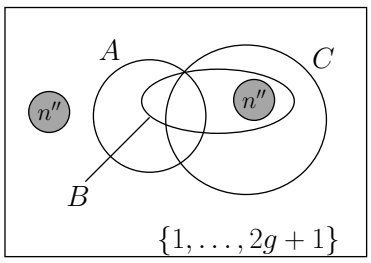
$$\#(A \cup B \cup C)^c \geqslant 2g + 1 - \#A - (g+1) + \#(A \cap C) \geqslant g - \#A.$$

Par définition de l'intersection, nous avons l'inégalité $\#(A \cap B) \leqslant \#A$. Les unions disjointes se traduisent par la somme $\#(A \cap B) + \#((B \cap C) \setminus A) = \#B$ et nous obtenons alors

$$\#((B \cap C) \setminus A) \geqslant \#B - \#A \geqslant g - \#A$$

On peut alors choisir $n'' = \lceil \frac{g - \#A}{2} \rceil$ éléments dans $(A \cup B \cup C)^c$ et n'' dans $(B \cap C) \setminus A$ pour constituer un ensemble D_4 qui vérifiera les propriétés demandées :

$$\#A \circ D_4 \in \{g, g+1\}, \qquad \#B \circ D_4 = \#B \in \{g, g+1\}, \qquad \#C \circ D_4 = \#C \in \{g, g+1\}.$$



□

Nous avons maintenant suffisamment de relations pour être capable de calculer les signes qui apparaîtront dans la suite.

5.1.3 Les fonctions Y_S

Définition 5.1.26. *Soit ϕ le morphisme $\mathcal{C}^g$ dans $\mathrm{Jac}(\mathcal{C})$. Soit $D \in \mathrm{Jac}(\mathcal{C}) \setminus \Theta$, posons $P = (P_i)_{i\in\{1,\dots,g\}}$ un élément de $\phi^{-1}(D)$ et soient x_i et y_i les abscisses et ordonnées des points P_i.*
Pour tout sous-ensemble S de $\{1,\dots,2g+1\}$ de cardinal s tel que $2 \leqslant s \leqslant 2g-1$, posons $n = \lfloor \frac{s}{2} \rfloor$ et définissons la fonction $Y_S :\ \mathrm{Jac}(\mathcal{C}) \to k$ telle que

$$\phi^* Y_S(P) = \sum_{\substack{I\subset\{1,\dots,g\}\\ \#I=n}} \left(\prod_{i\in I} y_i\right) \prod_{\substack{k=1\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k - a_l)}{\prod_{i\in I}(x_i - x_k)}. \tag{5.1}$$

Montrons que cette définition a du sens, c'est-à-dire que Y_S est bien définie. L'expression ne dépendant pas de l'ordre des points P_i, elle définit bien une fraction rationnelle sur $\mathcal{C}^{(g)}$ et donc une fonction sur $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$. En pratique, cela signifie que Y_S peut s'exprimer comme une fraction rationnelle en les coefficients de u et v.

Exemple 5.1.27. *Dans le cas du genre 2, les seuls ensembles S à considérer sont ceux de cardinaux 2 et 3. Nous avons alors*

$$\phi^* Y_{\{k,l\}}(P) = \frac{y_1(x_2 - a_k)(x_2 - a_l) - y_2(x_1 - a_k)(x_1 - a_l)}{x_2 - x_1},$$

$$\phi^* Y_{\{k,l,m\}}(P) = \frac{y_1(x_2 - a_k)(x_2 - a_l)(x_2 - a_m) - y_2(x_1 - a_k)(x_1 - a_l)(x_1 - a_m)}{x_2 - x_1}.$$

Van Wamelen a prouvé le théorème suivant reliant le polynôme v aux fonctions $Y_{\{l,m\}}$.

Théorème 5.1.28. *Soit $l \in \{1,\dots,2g+1\}$, prenons un sous-ensemble V de cardinal g de $\{1,\dots,2g+1\}$ tel que $l \notin V$. Alors*

$$v(a_l) = \sum_{m\in V} \frac{Y_{\{l,m\}}(D)}{\prod_{\substack{k\in V\\ k\neq m}} (a_k - a_m)}.$$

Exemple 5.1.29. *Plaçons nous dans le cas du genre 2. Soit $l \in \{1,\dots,5\}$ et soient m et n deux éléments distincts de $\{1,\dots,5\}$ différents de l. Alors*

$$v(a_l) = \frac{Y_{l,n}(D) - Y_{l,m}(D)}{a_m - a_n}.$$

Le théorème suivant est fondamental pour les calculs des morphismes. En effet, il lie les coordonnées des points sur la courbe aux fonctions thêta. C'est la généralisation de celui prouvé par Van Wamelen dans le cas où $s = 2$.

Théorème 5.1.30. *Soit $z = \mathfrak{u}(D)$, l'image du diviseur D par l'application d'Abel-Jacobi. Alors il existe une constante s_S telle que*

$$Y_S(D) = s_S \frac{t_S(z) \prod_{l\in S} t_l(z)}{t_\emptyset^{s+1}(z)}.$$

La preuve de ce théorème est similaire à celle de Van Wamelen : nous allons étudier les zéros et les pôles des deux fonctions. Nous décomposons cette preuve en plusieurs lemmes. Les fonctions partent de $\mathrm{Jac}(\mathcal{C})$ qui est un espace de dimension g mais il sera plus simple de les étudier sur $\mathcal{C}^g$ en utilisant les tirés en arrière. Soit ϕ l'application naturelle de $\mathcal{C}^g$ dans $\mathrm{Jac}(\mathcal{C})$.

Commençons par remarquer que les variétés $\mathrm{Jac}(\mathcal{C})$ et $\mathcal{C}^g$ sont régulières (la dernière en tant que produit fibré de variétés régulières sur un corps algébriquement clos [Liu02, Exercice 2.12 p. 135]). De ce fait ce sont des variétés normales [Mil09, pp. 94]. Par ailleurs, $\mathrm{Jac}(\mathcal{C})$ étant normale, ses anneaux locaux $\mathcal{O}_P$ sont réguliers et sont donc factoriels [Iit81, théorème 2.11 pp. 120]. En tant que variétés algébriques, ce sont des schémas noetheriens [Liu02, remarque 3.48 p. 55–56] et intègres [Har77, exemple 3.2.1 pp. 84].

L'application $\phi : \mathcal{C}^g \to \mathrm{Jac}(\mathcal{C})$ est un morphisme surjectif. Cette application est la composition du morphisme $\phi : \mathcal{C}^g \to \mathcal{C}^{(g)}$ et de l'application birationnelle $\mathcal{C}^{(g)} \to \mathrm{Jac}(\mathcal{C})$. Ces deux morphismes sont finis (d'après [Liu02, exercice 3.23 pp. 113] pour le premier et car le second est une application birationnelle) donc leur composition ϕ est finie [Iit81, proposition 1.56 pp. 93]. Par ailleurs, ϕ est de degré $g!$.

Iitaka [Iit81, proposition 2.15 pp. 132] montre que pour toute fonction rationnelle $f : \mathrm{Jac}(\mathcal{C}) \to \mathbb{C}$ nous avons $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$. Par ailleurs, Liu [Liu02, théorème 2.18 pp. 271] prouve que pour tout diviseur D sur $\mathrm{Jac}(\mathcal{C})$, nous avons $\phi_*(\phi^* D) = (g!)D$. Ces propriétés permettent de transférer la recherche des zéros et pôles d'une fonction de $\mathrm{Jac}(\mathcal{C}) \to \mathbb{C}$ à celle d'une fonction de $\mathcal{C}^g \to \mathbb{C}$. Ainsi

$$(g!)\,\mathrm{div}(Y_S) = \phi_*(\phi^*\,\mathrm{div}(Y_S)) = \phi_*(\mathrm{div}(\phi^* Y_S)).$$

La fonction Y_S aura donc un pôle ou un zéro en un diviseur premier Γ de $\mathrm{Jac}(\mathcal{C})$ si et seulement si, il existe un diviseur premier F sur $\mathcal{C}^g$ tel que $\phi(F)$ soit dense dans Γ et qui appartienne au support de $\mathrm{div}(\phi^* Y_S)$.

La propriété 3.1.22 décrit le diviseur des zéros de la fonction thêta comme des translatés du diviseur Θ : rappelons que, pour un élément D de $\mathrm{Jac}(\mathcal{C})$, nous avions noté T_D l'opérateur de translation par D. Par abus de notation, nous identifions les racines a_i de f avec les points $(a_i, 0)$ de la courbe $\mathcal{C}$. Ainsi nous écrivons $a_i - P_\infty$ pour le diviseur $(a_i, 0) - P_\infty$ de $\mathrm{Jac}(\mathcal{C})$.

Lemme 5.1.31. *La fonctions* Y_S *a des zéros en les* $\mathrm{T}_{a_l - P_\infty}\,\Theta$ *pour tout* l *dans* S.

Démonstration. Le diviseur premier $T = a_l \times \mathcal{C}^{g-1}$ de $\mathcal{C}^g$ est clairement un zéro de $\phi^* Y_S$ car les $x_i - x_j$ avec $i \neq j$ ne sont pas identiquement nuls sur ces diviseurs. Comme $\phi(T)$ est dense dans $\mathrm{T}_{a_l - P_\infty}\,\Theta$, la fonction Y_S admet $\mathrm{T}_{a_l - P_\infty}\,\Theta$ comme zéro. □

Lemme 5.1.32. *La fonction* Y_S *est régulière sur* $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$.

Rappelons que sur une variété $(X, \mathcal{O}_X)$ normale et localement noethérienne, $\mathcal{O}_X(X \setminus F) = \mathcal{O}_X(X)$ pour tout fermé F de codimension 2 [Liu02, théorème 1.14 pp. 118] (c'est à dire que toute fonction régulière sauf possiblement sur une sous variété fermée de codimension 2, est régulière partout).

Nous allons appliquer cette propriété à la fonction $\phi^* Y_S$ sur $\mathcal{C}^g \setminus \phi^{-1}\Theta$ qui est une sous-variété algébrique et est donc normale et noethérienne.

Démonstration. En revenant à sa définition, la fonction Y_S est trivialement régulière en tout point de $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$ qui n'appartient pas au diviseur premier

$$\mathcal{D} = \{2P_1 + P_2 + \ldots + P_{g-1} - gP_\infty \in \mathrm{Jac}(\mathcal{C})\}\,.$$

Pour montrer que la fraction rationnelle Y_S est régulière en tout point de $\mathcal{D}$, il suffit de montrer que Y_S n'a pas de pôle en le diviseur premier $\mathcal{D}$. En utilisant la fonction ϕ et l'invariance de Y_S sous l'action du groupe $\mathfrak{S}_g$, il suffit de vérifier que le diviseur $F = \Delta \times \mathcal{C}^{g-2}$ (où Δ est le diviseur diagonal sur $\mathcal{C} \times \mathcal{C}$) n'est pas un pôle de $\phi^* Y_S$. En effet F appartient à $\phi^{-1}(\mathcal{D})$ et $\phi(F)$ est dense dans $\mathcal{D}$.

La somme

$$\sum_{\substack{I \subset \{3,\ldots,g\} \\ \#I = n}} \left(\prod_{i \in I} y_i\right) \prod_{\substack{k=1 \\ k \notin I}}^{g} \frac{\prod_{l \in S}(x_k - a_l)}{\prod_{i \in I}(x_i - x_k)}$$

est une fonction régulière sur un ouvert dense de la sous-variété F et donc F n'est pas un pôle de cette fonction (car F est de codimension strictement positive). Il en est de même de la partie où $\{1, 2\} \subset I$:

$$y_1 y_2 \sum_{\substack{I \subset \{3,\ldots,g\} \\ \#I = n-2}} \prod_{i \in I} y_i \prod_{\substack{k=3 \\ k \notin I}}^{g} \left(\frac{1}{(x_1 - x_k)(x_2 - x_k)} \frac{\prod_{l \in S}(x_k - a_l)}{\prod_{i \in I}(x_i - x_k)}\right).$$

Il reste donc à étudier la partie où $1 \in I$ et $2 \notin I$ et celle où $1 \notin I$ et $2 \in I$. Nous regroupons ces éléments par paires avec un élément de la première et son associé dans la seconde. Pour tout sous-

ensemble $I \subset \{3, \dots, g\}$ de cardinal $n-1$,

$$p_I := y_1 \prod_{i\in I} y_i \prod_{\substack{k=1\\ k\notin\{1\}\cup I}}^{g} \frac{\prod_{l\in S}(x_k - a_l)}{(x_1-x_k)\prod_{i\in I}(x_i-x_k)} + y_2 \prod_{i\in I} y_i \prod_{\substack{k=1\\ k\notin\{2\}\cup I}}^{g} \frac{\prod_{l\in S}(x_k - a_l)}{(x_2-x_k)\prod_{i\in I}(x_i-x_k)},$$

$$\begin{aligned} p_I = & \left(\frac{y_1\prod_{l\in S}(x_2-a_l)}{x_1-x_2} - \frac{y_2\prod_{l\in S}(x_1-a_l)}{x_1-x_2}\right)\prod_{i\in I} y_i \frac{1}{\prod_{i\in I}(x_i-x_2)} \prod_{\substack{k=3\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{(x_1-x_k)\prod_{i\in I}(x_i-x_k)} \\ & + y_2 \prod_{i\in I} y_i \prod_{l\in S}(x_1-a_l) \prod_{\substack{k=3\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{\prod_{i\in I}(x_i-x_k)} \\ & \frac{1}{x_1-x_2}\left(\frac{1}{\prod_{i\in I}(x_i-x_2)}\frac{1}{\prod_{\substack{k=3\\ k\notin I}}^{g}(x_1-x_k)} - \frac{1}{\prod_{i\in I}(x_i-x_1)}\frac{1}{\prod_{\substack{k=3\\ k\notin I}}^{g}(x_2-x_k)}\right). \end{aligned}$$

La différence

$$\frac{1}{\prod_{i\in I}(x_i-x_2)}\frac{1}{\prod_{\substack{k=3\\ k\notin I}}^{g}(x_1-x_k)} - \frac{1}{\prod_{i\in I}(x_i-x_1)}\frac{1}{\prod_{\substack{k=3\\ k\notin I}}^{g}(x_2-x_k)}$$

est nulle quand $x_1 = x_2$ et est donc divisible par $x_1 - x_2$. Ceci montre que F (en fait un ouvert dense de F et donc F tout entier) n'est pas un pôle de la seconde partie de p_I . Pour la première partie, le produit est bien défini sur F tandis que la différence se réécrit

$$\frac{y_1\prod_{l\in S}(x_2-a_l) - y_2\prod_{l\in S}(x_1-a_l)}{x_1-x_2} =$$

$$\frac{y_1^2\prod_{l\in S}(x_2-a_l)^2 - y_2^2\prod_{l\in S}(x_1-a_l)^2}{x_1-x_2}\frac{1}{y_1\prod_{l\in S}(x_2-a_l) + y_2\prod_{l\in S}(x_1-a_l)}.$$

Le dénominateur de la première fraction est un polynôme en x_1 et x_2 qui s'annule quand $x_1 = x_2$ et la deuxième partie est régulière sur un ouvert dense de F. Ceci permet de conclure que F n'est pas un pôle de $\phi^* Y_S$ et donc que la fonction Y_S est régulière sur $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$. □

Lemme 5.1.33. *La fonction Y_S a un pôle d'ordre exactement $s+1$ en Θ.*

Encore une fois nous allons raisonner sur $\phi^* Y_S$. Cependant, pour compter les multiplicités il faut utiliser un peu plus de géométrie algébrique. Nous allons nous ramener à étudier la fonction $\phi^* Y_S$ sur le diviseur $T_1 = P_\infty \times \mathcal{C}^{g-1}$ et pour ce faire nous allons séparer la somme en deux, suivant que $i_1 = 1$ ou pas.

Démonstration. Les $T_i = \mathcal{C}^{i-1} \times P_\infty \times \mathcal{C}^{g-i-1}$ sont des diviseurs premiers de $\mathcal{C}^g$ tels que $\phi(T_i)$ est dense dans le diviseur premier Θ de $\mathrm{Jac}(\mathcal{C})$. Comme le degré des morphismes $\phi_{|T_i}$ est $(g-1)!$ et le degré de ϕ égal à $g!$ alors les T_i sont les seuls diviseurs premiers de $\phi^{-1}(\Theta)$ qui sont denses dans Θ et nous avons $\phi^*\Theta = \sum_{i=1}^{g} T_i$ [Iit81]. Comme $\phi^*(\mathrm{div}(Y_S)) = \mathrm{div}(\phi^* Y_S)$, pour montrer que Y_S a un pôle d'ordre $s+1$ en Θ, il suffit de montrer que $\phi^* Y_S$ a un pôle d'ordre $s+1$ en tous les T_i. Par symétrie, il suffit de le vérifier en T_1.

Séparons la somme en deux. Si $1 \in I$,

$$\begin{aligned} & y_1 \sum_{\substack{I\subset\{2,\dots,g\}\\ \#I=n-1}} \left(\prod_{i\in I} y_i\right) \prod_{\substack{k=2\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{(x_1-x_k)\prod_{i\in I}(x_i-x_k)} \\ & \qquad = \frac{y_1}{x_1^{g-n}} \sum_{\substack{I\subset\{2,\dots,g\}\\ \#I=n-1}} \left(\prod_{i\in I} y_i\right) \prod_{\substack{k=2\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{(1-\frac{x_k}{x_1})\prod_{i\in I}(x_i-x_k)}. \end{aligned}$$

La somme est non nulle sur un ouvert dense de T_1. Donc T_1 est un pôle d'ordre exactement

$$2g+1-2(g-n)=2n+1$$

de cette partie de $\phi^* Y_S$. Pour $i_1 \neq 1$, nous avons l'égalité

$$\sum_{\substack{I\subset\{2,\dots,g\}\\ \#I=n}} \left(\prod_{i\in I} y_i\right) \frac{\prod_{l\in S}(x_1-a_l)}{\prod_{i\in I}(x_i-x_1)} \prod_{\substack{k=2\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{\prod_{i\in I}(x_i-x_k)} = \frac{\prod_{l\in S}(x_1-a_l)}{x_1^n}\sigma(z)$$

où

$$\sigma(z)=\sum_{\substack{I\subset\{2,\dots,g\}\\ \#I=n}} \prod_{i\in I} \frac{y_i}{\frac{x_i}{x_1}-1} \prod_{\substack{k=2\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k-a_l)}{\prod_{j=1}^{n}(x_{i_j}-x_k)}.$$

Encore une fois, la somme $\sigma(z)$ est non nulle sur un ouvert dense de T_1 donc T_1 est un pôle d'ordre exactement $2s-2n$ de cette partie.

Comme $2s-2n$ est différent de $2n+1$, l'ordre de T_1 comme pôle de la fonction $\phi^* Y_S$ est exactement $\max(2s-2n, 2n+1)$. Rappelons que $n=\lfloor \frac{s}{2} \rfloor$ donc

$$2n=\begin{cases} s & \text{si } s \text{ est pair,}\\ s-1 & \text{si } s \text{ est impair.}\end{cases}$$

Nous avons donc que $\max(2s-2n, 2n+1)=s+1$ quel que soit la parité de s. Ceci conclut la preuve. □

Lemme 5.1.34. *Avec les notations précédentes,*

$$Y_S(D)=s_S\frac{t_S(z)\prod_{l\in S} t_l(z)}{t_\emptyset^{s+1}(z)}$$

où s_S est une constante.

Démonstration. La fonction $h(z)=t_S(z)\prod_{l\in S} t_l(z)/t_\emptyset^{s+1}(z)$ est bien définie sur $\mathrm{Jac}(\mathcal{C})$ car pour tout élément $\lambda=\Omega\lambda'+\lambda''$ de Λ_Ω, nous avons $h(z+\lambda)=h(z)$ grâce à la formule

$$\theta[\eta_A](z+\Omega\lambda'+\lambda'')=\theta[\eta_A](z)\exp\left(-\pi i\,{}^t\lambda'\Omega\lambda'-2i\pi\,{}^t\lambda' z+2\pi i({}^t\lambda''\eta'_A-{}^t\lambda'\eta''_A)\right).$$

La fonction h a pour diviseur

$$\mathrm{T}_{\sum_{l\in S} a_l - sP_\infty}\Theta+\sum_{l\in S}\mathrm{T}_{a_l-P_\infty}\Theta-(s+1)\Theta.$$

Par ailleurs, nous avons montré dans les lemmes précédents que le diviseur de Y_S est

$$\mathrm{div}(Y_S)\geqslant\sum_{l\in S}\mathrm{T}_{a_l-P_\infty}\Theta-(s+1)\Theta.$$

Donc la fonction Y_S/h appartient à $\mathcal{L}\left(\mathrm{T}_{\sum_{l\in S} a_l - sP_\infty}\Theta\right)$. Cet espace étant de dimension 1 [Lan72, théorème VI.4.1], Y_S/h est une constante. □

Quand le cardinal de S est égal à $2g$ ou $2g+1$, les fonctions Y_S ne sont pas définies. Avec $n=g$, l'équation 5.1 se dérive en $y_1\dots y_g$. Étudions donc la fonction Y associée.

Théorème 5.1.35. *Soit $D=\sum_{i=1}^g P_i - gP_\infty$ un diviseur de $\mathrm{Jac}(\mathcal{C})\setminus\Theta$. Posons (u,v) les coordonnées de Mumford de D et supposons que $z\in\mathbb{C}^g$ soit l'image de D par l'application d'Abel-Jacobi, alors*

$$Y(D):=\mathrm{Res}(u,v)=s\frac{\prod_{l=1}^{2g+1} t_l(z)}{t_\emptyset(z)^{2g+1}}$$

où $s^2=1$. Si nous posons $P=(P_i)\in\mathcal{C}^g$ et y_i les ordonnées des points P_i alors

$$\phi^* Y(P)=y_1\dots y_g.$$

Ce théorème est plus simple à prouver que le précédent. En effet il suffit d'étudier le carré des expressions.

Démonstration. Le théorème 5.1.10 montre que

$$\prod_{l=1}^{2g+1} \frac{t_l^2(z)}{t_\emptyset^2(z)} = (-1)^{g(2g+1)} \prod_{l=1}^{2g+1} u(a_l).$$

Or, pour tout $i \in \{1, \dots, g\}$,

$$y_i^2 = \prod_{l=1}^{2g+1} (x_i - a_l) = (-1)^g \prod_{l=1}^{2g+1} (a_l - x_i)$$

ce qui permet d'obtenir que

$$y_1^2 \dots y_g^2 = (-1)^{g(2g+1)} \prod_{i=1}^{g} \prod_{l=1}^{2g+1} (a_l - x_i) = (-1)^{g(2g+1)} \prod_{l=1}^{2g+1} \prod_{i=1}^{g} (a_l - x_i).$$

Donc

$$y_1^2 \dots y_g^2 = (-1)^{g(2g+1)} \prod_{l=1}^{2g+1} u(a_l).$$

En égalant les deux expressions, nous obtenons que

$$y_1^2 \dots y_g^2 = \prod_{l=1}^{2g+1} \frac{t_l^2(z)}{t_\emptyset^2(z)}$$

ce qui prouve le théorème. □

En résumé, définissons une fonction $Y'_S(D)$ qui rassemble les résultats précédents

Théorème 5.1.36. *Soit $D = \sum_{i=1}^g P_i - gP_\infty$ un diviseur de $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$. Posons (u, v) les coordonnées de Mumford de D et supposons que $z \in \mathbb{C}^g$ soit l'image de D par l'application d'Abel-Jacobi. Pour tout sous-ensemble S de $\{1, \dots, 2g+1\}$, posons*

$$Y'_S(D) = \begin{cases} 1 & \text{si } S = \emptyset, \\ (-1)^g u(a_l) & \text{si } S = \{l\}, \\ \frac{1}{s_S} Y_S(D) & \text{si } 2 \leqslant \#S \leqslant 2g-1, \\ \frac{1}{s}(-1)^{\lfloor \frac{g}{2} \rfloor}(-1)^{2\,{}^t\eta'_{C_l}\zeta''_g} \operatorname{Res}(u,v) & \text{si } S = \{1, \dots, 2g+1\} \setminus \{l\}, \\ \frac{1}{s}(-1)^{\lfloor \frac{g+1}{2} \rfloor}(-1)^{2\,{}^t\eta'_{C_\emptyset}\zeta''_g} \operatorname{Res}(u,v) & \text{si } \#S = 2g+1. \end{cases}$$

Alors

$$Y'_S(D) = \frac{t_S(z) \prod_{l \in S} t_l(z)}{t_\emptyset^{s+1}(z)}.$$

5.1.4 Calcul des constantes s_S

Cette section est consacrée au calcul des constantes s_S. Ces constantes sont en fait des signes ± 1. Van Wamelen a prouvé ce fait dans le cas où l'ensemble S est de cardinal 2 mais la généralisation de sa preuve est triviale : il suffit de calculer

$$\frac{Y_S^2(z)}{\prod_{l \in S} \frac{t_l^2(z)}{t_\emptyset^2(z)}}$$

grâce aux formules

$$\frac{t_l^2(z)}{t_\emptyset^2(z)} = (-1)^g u(a_l) = (-1)^g \prod_{k=1}^{g}(a_l - x_k) = \prod_{k=1}^{g}(x_k - a_l),$$

$$y_i^2 = \prod_{m=1}^{2g+1}(x_i - a_m).$$

Puis il faut évaluer le résultat en un point de 2-torsion ce qui permet d'obtenir alors que $s_S^2 = 1$. Cette preuve ne permet cependant pas de les déterminer.

Dans cette section, nous allons déterminer les constantes s_S en les calculant de proche en proche.

Lemme 5.1.37. *Pour $S \subset \{1,\dots,2g+1\}$ de cardinal pair $2n$ avec $1 \leqslant n \leqslant g-1$ et pour $p \notin S$, posons $S' = S \cup p$. Alors*

$$s_{S'}s_S = \begin{cases} (-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_p\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g} & \text{si } 2n < g, \\ (-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_p\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{C_{S'}\circ C_S}\zeta''_g} & \text{si } 2n \geqslant g. \end{cases}$$

Pour $S \subset \{1,\dots,2g+1\}$ de cardinal pair $2n$ avec $1 \leqslant n \leqslant g-2$ et deux entiers distincts p et q n'appartenant pas à S, posons $S' = S \cup \{p,q\}$. Alors

$$s_{S'}s_Ss_{\{p,q\}} = \begin{cases} (-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_{\{p,q\}}\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g} & \text{si } 2n < g, \\ (-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_{\{p,q\}}\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{C_{S'}\circ C_S}\zeta''_g} & \text{si } 2n \geqslant g. \end{cases}$$

Pour prouver ce lemme, nous reprenons les idées de la preuve de Van Wamelen.

Les seuls points dont on connaît l'expression en coordonnées de Mumford et avec les fonctions thêta sont les points de 2-torsion. Du fait des coordonnées y_i dans l'expression de Y_S, ces points sont des zéros de Y_S. L'idée est alors de multiplier Y_S par d'autres $Y_{S'}$ de façon à ce que au moins un terme de la somme ne comporte que des y_i^2. Il est alors possible d'exprimer ce terme uniquement en fonction de x_i. Il suffit alors de le diviser par $(x_i - a_m)$ pour espérer obtenir un terme non nul.

Cette petite discussion justifie le choix des ensembles dans le lemme : pour chaque somme, il y a des termes ne comportant que des y_i^2 (en particulier dans le dernier cas cela justifie le fait que l'on ne regarde pas $s_{S\cup\{p,q\}}s_{S\cup\{p\}}$ mais $s_{S'}s_Ss_{\{p,q\}}$). Par ailleurs les ensembles sont choisis de façon à maximiser le nombre de $t_l^2(z)/t_\emptyset^2(z)$ ce qui simplifie la preuve. Le point de 2-torsion où nous évaluerons l'expression sera tel que le terme d'indice $I = \{1,\dots,n\}$ soit non nul mais que tous les autres termes soient nuls. L'expression obtenue sera alors très simple et ne fera apparaître que des produits de $a_i - a_j$ et des constantes f_A. On utilisera alors la propriété 5.1.23 pour conclure.

Nous ne prouvons en détail que le premier cas, la preuve de l'autre cas étant très similaire.

Démonstration dans le premier cas. Par définition, pour tout z, la constante $s_{S'}s_S$ est égale à

$$s_{S'}s_S = \frac{Y_S(z)Y_{S'}(z)}{\prod_{l\in S}\frac{t_l(z)^2}{t_\emptyset^2(z)}}\frac{t_\emptyset^3(z)}{t_S(z)t_{S'}(z)t_p(z)}.$$

En développant, nous obtenons

$$s_{S'}s_S = \frac{t_\emptyset^3(z)}{t_S(z)t_{S'}(z)t_p(z)}\left(\sigma_1(z) + \sigma_2(z)\right)$$

avec

$$\begin{aligned} \sigma_1(z) &= \frac{1}{\prod_{k=1}^g\prod_{l\in S}(x_k - a_l)} \sum_{\substack{I\subset\{1,\dots,g\}\\ \#I=n}} \prod_{i\in I} y_i^2 \prod_{\substack{k=1\\ k\notin I}}^{g} \frac{(x_k - a_p)\prod_{l\in S}(x_k - a_l)^2}{\prod_{j=1}^n (x_{i_j} - x_k)^2} \\ &= \sum_{\substack{I\subset\{1,\dots,g\}\\ \#I=n}} \prod_{i\in I}\prod_{m\notin S}(x_i - a_m) \prod_{\substack{k=1\\ k\notin I}}^{g} \frac{\prod_{l\in S'}(x_k - a_l)}{\prod_{i\in I}(x_i - x_k)^2} \end{aligned}$$

et

$$\sigma_2(z) = \sum_{\substack{I \neq I' \subset \{1,\dots,g\} \\ \#I = \#I' = n}} \frac{\prod_{i\in I} y_i \prod_{i\in I'} y_i}{\prod_{k=1}^g \prod_{l\in S}(x_k - a_l)} \prod_{\substack{k=1 \\ k\notin I}}^{g} \frac{\prod_{l\in S'}(x_k - a_l)}{\prod_{i\in I}(x_i - x_k)} \prod_{\substack{k=1 \\ k\notin I'}}^{g} \frac{\prod_{l\in S}(x_k - a_l)}{\prod_{i\in I'}(x_i - x_k)}.$$

Choisissons un sous-ensemble $V \subset S$ de cardinal n et un sous-ensemble $W \subset \{1,\dots,2g+1\} \setminus S'$ de cardinal $g-n$ (ceci est possible car $S' = S \cup \{p\}$ et $1 \leqslant n \leqslant g-1$). Nous allons évaluer l'expression précédente en le diviseur

$$D = \sum_{l\in V} a_l + \sum_{m\in W} a_m - gP_\infty.$$

Pour plus de simplicité, considérons σ_1 et σ_2 comme des fonctions du produit $\mathcal{C}^g$ dans le corps $\mathbb{C}$ ainsi que le point $D = (P_1,\dots,P_n) \in \mathcal{C}^g$ où les n premiers P_i sont les $(a_l, 0)$ avec $l \in V$ numérotés par ordre croissant et les $g-n$ suivant les $(a_m, 0)$ avec $m \in W$ (formellement il faut considérer $\phi^*(\sigma_1)$ et $\phi^*(\sigma_2)$ et le point $(P_1,\dots,P_n)$ qui s'envoie sur D par ϕ).

Le terme général de $\sigma_1(D)$ est non nul si et seulement si pour tout i dans I, x_i est une racine a_l de f avec $l \in S$ et si pour tout $k \in \{1,\dots,g\} \setminus I$, x_k est une racine a_l avec $l \notin S$. Vu le diviseur D considéré, seul le terme $I = \{1,\dots,n\}$ de la somme n'est pas nulle. D'où

$$\begin{aligned}
\sigma_1(D) &= \frac{\prod_{j\in V}\prod_{m\notin S}(a_j - a_m)\prod_{k\in W}\prod_{l\in S'}(a_k - a_l)}{\prod_{k\in W}\prod_{j\in V}(a_j - a_k)^2} \\
&= (-1)^{\#V\#W} \prod_{j\in V}\prod_{m\notin S\cup W}(a_j - a_m) \prod_{k\in W}\prod_{l\in S'\setminus V}(a_k - a_l) \\
&= (-1)^{n(g-n)}(-1)^{4\,{}^t\eta'_V \eta''_{(S\cup W)^c}}(-1)^{4\,{}^t\eta'_W \eta''_{S'\setminus V}} \\
&\quad \prod_{j\in V}\prod_{m\notin S\cup W} < a_j - a_m > \prod_{k\in W}\prod_{l\in S'\setminus V} < a_k - a_l > .
\end{aligned}$$

Montrons que tous les termes de $\sigma_2(D)$ sont nuls. Pour tout $k \in \{1,\dots,g\}$, deux possibilités peuvent se produire

- Si k appartient à $I \cap I'$, alors y_k^2 apparaît au numérateur du terme considéré et donc $\prod_{l\in S}(x_k - a_l)$ divise y_k^2.
- Si k n'appartient pas à une des deux listes I et I' alors $\prod_{l\in S}(x_k - a_l)$ divise le produit de droite correspondant.

Comme $I \neq I'$, il existe un indice $i \in I$ tel que $i \notin I'$. Mais alors y_i se trouve en facteur d'une expression sans pôle en D donc le terme de $\sigma_2(D)$ considéré est nul.

$$\begin{aligned}
\sigma_1(D) + \sigma_2(D) &= (-1)^{n(g-n)}(-1)^{4\,{}^t\eta'_{V\cup W}\eta''_S + 4\,{}^t\eta'_W\eta''_p}(-1)^{4\,{}^t\eta'_V\eta''_W + 4\,{}^t\eta'_W\eta''_V} \\
&\quad \prod_{j\in V}\prod_{m\notin S\cup W} < a_j - a_m > \prod_{k\in W}\prod_{l\in S'\setminus V} < a_k - a_l > .
\end{aligned}$$

Or d'après la propriété 2.3.17,

$$(-1)^{4\,{}^t\eta'_V\eta''_W + 4\,{}^t\eta'_W\eta''_V} = e_2(\eta_V, \eta_W) = \begin{cases} 1 & \text{si } \#V \text{ ou } \#W \text{ est pair,} \\ -1 & \text{sinon.} \end{cases}$$

Donc

$$(-1)^{4\,{}^t\eta'_V\eta''_W + 4\,{}^t\eta'_W\eta''_V} = (-1)^{\#V\#W} = (-1)^{n(g-n)}.$$

Nous obtenons alors

$$\sigma_1(D) + \sigma_2(D) = (-1)^{4\,{}^t\eta'_{V\cup W}\eta''_S + 4\,{}^t\eta'_W\eta''_p} \prod_{j\in V}\prod_{m\notin S\cup W} < a_j - a_m > \prod_{k\in W}\prod_{l\in S'\setminus V} < a_k - a_l > .$$

Travaillons maintenant sur les fonctions thêta. Comme $\mathfrak{u}(D) = \Omega\eta'_{V\cup W} + \eta''_{V\cup W}$, nous avons par définition

$$\frac{t^3_\emptyset(D)}{t_S(D)t_{S'}(D)t_p(D)} = \frac{f^3_\emptyset}{f_S f_{S'} f_p} \frac{\theta\left[\eta_{\mathcal{U}}\right]\left(\Omega\eta'_{V\cup W} + \eta''_{V\cup W}\right)^3}{\theta\left[\eta_{\mathcal{U}\circ S}\right](\mathfrak{u}(D))\ \theta\left[\eta_{\mathcal{U}\circ S'}\right](\mathfrak{u}(D))\ \theta\left[\eta_{\mathcal{U}\circ p}\right](\mathfrak{u}(D))}.$$

Rappelons les résultats de la propriété 3.1.2 : pour tous α, β appartenant à $\mathbb{Q}^g$,

$$\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z,\Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\Omega\alpha+\beta,\Omega)\exp(i\pi\,{}^t\alpha\Omega\beta + 2i\pi\,{}^t\alpha(z+\beta))\exp(2i\pi\,{}^t\alpha b),$$

et si α, β appartiennent à $\mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z,\Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)\exp(2i\pi\,{}^t a\beta).$$

Pour éviter de surcharger les notations, nous notons $S \setminus V \cup W$ pour $(S \setminus V) \cup W$. Nous obtenons

$$\begin{aligned}
\frac{t^3_\emptyset(D)}{t_S(D)t_{S'}(D)t_p(D)} &= \frac{f^3_\emptyset}{f_S f_{S'} f_p} \frac{\theta\left[\eta_{\mathcal{U}} + \eta_{V\cup W}\right]^3}{\theta\left[\eta_{\mathcal{U}\circ S} + \eta_{V\cup W}\right]\theta\left[\eta_{\mathcal{U}\circ S'} + \eta_{V\cup W}\right]\theta\left[\eta_{\mathcal{U}\circ p} + \eta_{V\cup W}\right]}(-1)^{4\,{}^t\eta'_{V\cup W}\eta''_{S'}} \\
&= \frac{f^3_\emptyset}{f_S f_{S'} f_p} \frac{\theta\left[\eta_{\mathcal{U}\circ(V\cup W)}\right]^3}{\theta\left[\eta_{\mathcal{U}\circ(S\setminus V\cup W)}\right]\theta\left[\eta_{\mathcal{U}\circ(S'\setminus V\cup W)}\right]\theta\left[\eta_{\mathcal{U}\circ(\{p\}\cup V\cup W)}\right]} \\
&\quad (-1)^{4\,{}^t\eta'_{V\cup W}\eta''_{S'}}(-1)^{4\,{}^t\eta'_p\eta''_V} \\
&= \frac{f^3_\emptyset}{f_S f_{S'} f_p} \frac{f_{S\setminus V\cup W} f_{S'\setminus V\cup W} f_{\{p\}\cup V\cup W}}{f^3_{V\cup W}}(-1)^{4\,{}^t\eta'_{V\cup W}\eta''_{S'}}(-1)^{4\,{}^t\eta'_p\eta''_V} \\
&= \frac{f^3_\emptyset}{f_S f_{S'} f_p} \frac{f_{S\setminus V\cup W} f_{S'\setminus V\cup W} f_{\{p\}\cup V\cup W}}{f^3_{V\cup W}}(-1)^{4\,{}^t\eta'_{V\cup W}\eta''_S + 4\,{}^t\eta'_W\eta''_p}(-1)^{4\,{}^t\eta'_p\eta''_V + 4\,{}^t\eta'_V\eta''_p}.
\end{aligned}$$

Or

$$(-1)^{4\,{}^t\eta'_p\eta''_V + 4\,{}^t\eta'_V\eta''_p} = e_2\left(\eta_p, \eta_V\right) = (-1)^{\#V} = (-1)^n.$$

Finalement comme

$$s_S s_{S'} = \frac{t^3_\emptyset(D)}{t_S(D)t_{S'}(D)t_p(D)}\left(\sigma_1(D) + \sigma_2(D)\right)$$

nous obtenons

$$\begin{aligned}
s_S s_{S'} &= (-1)^n \prod_{j\in V}\prod_{m\notin S\cup W} < a_j - a_m > \prod_{k\in W}\prod_{l\in S'\setminus V} < a_k - a_l > \\
&\quad \frac{f^4_\emptyset}{f^4_{V\cup W}} \frac{f_{S\circ(V\cup W)} f_{S'\circ(V\cup W)}}{f_S f_{S'}} \frac{f_{\{p\}\circ(V\cup W)} f_{V\cup W}}{f_p f_\emptyset}.
\end{aligned}$$

On vérifie, en utilisant la propriété 5.1.23 que $p_{i,j}\left[s_S s_{S'}\right] = 0$ pour tous $i \neq j \in \{1, \ldots, 2g+1\}$. Par ailleurs, comme $2n < g$, avec cette propriété nous obtenons que

$$\begin{aligned}
s\left[s_S s_{S'}\right] &= (-1)^n(-1)^{2\,{}^t\eta'_{(V\cup W)\setminus(S\circ S')}\zeta''_g + 2\,{}^t\eta'_{(C_S\circ C_{S'})\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{(V\cup W)\setminus\{p\}}\zeta''_g + 2\,{}^t\eta'_{(C_p\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g} \\
&= (-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_p\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g}.
\end{aligned}$$

Ceci conclut la preuve. □

Éléments de démonstration dans le deuxième cas. Par définition,

$$s_{S'} s_S s_{\{p,q\}} = \frac{Y_S(z)Y_{S'}(z)Y_{\{p,q\}}(z)}{\prod_{l\in S'}\frac{t_l(z)^2}{t^2_\emptyset(z)}} \frac{t^3_\emptyset(z)}{t_S(z)t_{S'}(z)t_{\{p,q\}}(z)}.$$

Soient deux sous-ensembles $V \subset S$ et $W \subset \{1, \ldots, 2g+1\} \setminus S'$ de cardinaux n et $g-n-1$ respectivement. Il faut évaluer l'expression précédente en le diviseur

$$D = \sum_{l\in V} a_l + a_p + \sum_{m\in W} a_m - gP_\infty.$$

□

Lemme 5.1.38. *Soit S un sous-ensemble de $\{1,\dots,2g+1\}$ et soient $p\in S$ et $q\in S^c$. Alors*

$$s_S s_{S\circ\{p,q\}} = \begin{cases} (-1)^{2\,{}^t\eta'_{\left(C_S\circ C_{S\circ\{p,q\}}\circ C_p\circ C_q\right)\cap\mathcal{U}}\zeta''_g} & 2n\leqslant g,\\ (-1)^{2\,{}^t\eta'_{\left(C_S\circ C_{S\circ\{p,q\}}\circ C_p\circ C_q\right)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta_{C_S\circ C_{S\circ\{p,q\}}}\zeta''_g} & 2n>g. \end{cases}$$

En particulier, soient l,m,n trois entiers distincts de $\{1,\dots,2g+1\}$ alors

$$s_{\{l,m\}}s_{\{l,n\}} = (-1)^{2\,{}^t\eta'_{\left(C_{\{l,m\}}\circ C_{\{l,n\}}\circ C_m\circ C_n\right)\cap\mathcal{U}}\zeta''_g}.$$

Démonstration. Si $\#S=2n<g$ alors en appliquant le premier cas du lemme 5.1.37 aux ensembles S et $S'=S\cup\{q\}$ d'une part et aux ensembles $S\circ\{p,q\}$ et $S'=(S\circ\{p,q\})\cup p$ d'autre part, nous avons les formules :

$$\begin{aligned} s_{S'} &= s_S(-1)^n(-1)^{2\,{}^t\eta'_{(C_{S'}\circ C_S\circ C_q\circ C_\emptyset)\cap\mathcal{U}}\zeta''_g},\\ s_{S'} &= s_{S\circ\{p,q\}}(-1)^n(-1)^{2\,{}^t\eta'_{\left(C_{S'}\circ C_{S\circ\{p,q\}}\circ C_p\circ C_\emptyset\right)\cap\mathcal{U}}\zeta''_g}. \end{aligned}$$

En égalant ces deux égalités, nous obtenons la propriété dans ce cas. Si $\#S=2n+1<g$ est impair alors en utilisant la même formule que précédemment pour l'ensemble $S\setminus p$ nous avons

$$\begin{aligned} s_{S\setminus p} &= s_S(-1)^n(-1)^{2\,{}^t\eta'_{\left(C_S\circ C_{S\setminus p}\circ C_p\circ C_\emptyset\right)\cap\mathcal{U}}\zeta''_g},\\ s_{S\setminus p} &= s_{(S\setminus p)\cup q}(-1)^n(-1)^{2\,{}^t\eta'_{\left(C_{(S\setminus p)\cup q}\circ C_{S\setminus p}\circ C_q\circ C_\emptyset\right)\cap\mathcal{U}}\zeta''_g}. \end{aligned}$$

En égalant les deux et en remarquant que $(S\setminus p)\cup q = S\circ\{p,q\}$, nous obtenons la formule voulue. Les deux derniers cas (quand n est assez grand), se prouvent de la même façon. □

Une expression des signes s_S s'obtient en utilisant une récurrence basée sur les deux lemmes précédents. Posons

$$\sigma = s_{\{1,2\}}(-1)^{2\,{}^t\eta'_{\left(C_{\{1,2\}}\circ C_1\circ C_2\circ C_\emptyset\right)\cap\mathcal{U}}\zeta''_g}\in\{\pm1\}$$

qui peut se calculer en fonction de $s_{\{1,2\}}$ et inversement.

Théorème 5.1.39. *Soit σ un élément de $\{\pm1\}$, pour tout sous-ensemble S de $\{1,\dots,2g+1\}$ de cardinal $2\leqslant s\leqslant 2g-1$,*

$$s_S = (-1)^{\lfloor\frac{s+1}{4}\rfloor}\sigma^{\lfloor\frac{s}{2}\rfloor}\left((-1)^{2\,{}^t\eta'_{C_\emptyset\cap\mathcal{U}}\zeta''_g}\right)^{s-1}(-1)^{2\,{}^t\eta'_{C_S\cap\mathcal{U}}\zeta''_g}\prod_{l\in S}(-1)^{2\,{}^t\eta'_{C_l\cap\mathcal{U}}\zeta''_g}.$$

Toujours avec la même méthode que pour le lemme 5.1.37, on peut déterminer la valeur de la constante s du théorème 5.1.35 en fonction des autres constantes s_S.

Théorème 5.1.40. *Le signe s est donné par*

$$s=\sigma^g(-1)^{2\,{}^t\eta'_{C_\emptyset\cap\mathcal{U}}\zeta''_g}\prod_{l=1}^{2g+1}(-1)^{2\,{}^t\eta'_{C_l\cap\mathcal{U}}\zeta''_g}.$$

Exemple 5.1.41. *Dans le cas du genre 2 avec les choix d'ensembles C_A de l'exemple 5.1.9, les signes s_S sont égaux à σ si S est de cardinal 2 et $-\sigma$ si S est de cardinal 3. Par ailleurs le signe s est en fait égal à 1.*

5.1.5 Résumé des parties précédentes

En utilisant les fonctions thêta tordues définies à la page 92 nous avons montré le résultat suivant.

Soit ϕ le morphisme $\mathcal{C}^g$ dans $\mathrm{Jac}(\mathcal{C})$. Soit $D \in \mathrm{Jac}(\mathcal{C}) \setminus \Theta$, posons $P = (P_i)_{i\in\{1,\dots,g\}} \in \phi^{-1}(D)$ et soient x_i et y_i les abscisses et ordonnées des points P_i. Posons (u, v) les coordonnées de Mumford de D et supposons que $z \in \mathbb{C}^g$ soit l'image de D par l'application d'Abel-Jacobi.
Pour tout sous-ensemble S de $\{1, \dots, 2g+1\}$ de cardinal vérifiant $2 \leqslant \#S \leqslant 2g-1$, posons $n = \lfloor \frac{\#S}{2} \rfloor$ et définissons la fonction $Y_S :\ \mathrm{Jac}(\mathcal{C}) \to k$ telle que

$$\phi^* Y_S(P) = \sum_{\substack{I\subset\{1,\dots,g\}\\ \#I=n}} \left(\prod_{i\in I} y_i\right) \prod_{\substack{k=1\\ k\notin I}}^{g} \frac{\prod_{l\in S}(x_k - a_l)}{\prod_{i\in I}(x_i - x_k)}$$

La fonction Y'_S est alors définie pour tout sous-ensemble S de $\{1, \dots, 2g+1\}$ par

$$Y'_S(D) = \begin{cases} 1 & \text{si } S = \emptyset \\ (-1)^g u(a_l) & \text{si } S = \{l\} \\ s_S Y_S(D) & \text{si } 2 \leqslant \#S \leqslant 2g-1 \\ \frac{1}{s}(-1)^{\lfloor \frac{g}{2} \rfloor}(-1)^{2\,{}^t\eta'_{C_l}\zeta''_g} \operatorname{Res}(u, v) & \text{si } S = \{1, \dots, 2g+1\} \setminus \{l\} \\ \frac{1}{s}(-1)^{\lfloor \frac{g+1}{2} \rfloor}(-1)^{2\,{}^t\eta'_{C_\emptyset}\zeta''_g} \operatorname{Res}(u, v) & \text{si } \#S = 2g+1 \end{cases}$$

où s_S et s sont donnés par (théorèmes 5.1.39 et 5.1.40)

$$\begin{aligned} s_S &= (-1)^{\lfloor \frac{s+1}{4} \rfloor}\sigma^{\lfloor \frac{s}{2} \rfloor}\left((-1)^{2\,{}^t\eta'_{C_\emptyset\cap\mathcal{U}}\zeta''_g}\right)^{s-1}(-1)^{2\,{}^t\eta'_{C_S\cap\mathcal{U}}\zeta''_g}\prod_{l\in S}(-1)^{2\,{}^t\eta'_{C_l\cap\mathcal{U}}\zeta''_g} \\ s &= \sigma^g(-1)^{2\,{}^t\eta'_{C_\emptyset\cap\mathcal{U}}\zeta''_g}\prod_{l=1}^{2g+1}(-1)^{2\,{}^t\eta'_{C_l\cap\mathcal{U}}\zeta''_g} \end{aligned}$$

et où σ est un élément de $\{\pm 1\}$. Alors les théorèmes 5.1.30 et 5.1.35 montrent que

$$Y'_S(D) = \frac{t_S(z)\prod_{l\in S} t_l(z)}{t_\emptyset^{s+1}(z)}.$$

Par ailleurs les évaluations des polynômes de Mumford en les points de ramifications sont données par les théorèmes 5.1.10 et 5.1.28 : pour tout élément k de $\{1, \dots, 2g+1\}$,

$$u(a_k) = (-1)^g \frac{t_k^2(z)}{t_\emptyset^2(z)},$$

$$v(a_k) = \sum_{m\in V} \frac{Y_{\{k,m\}}(z)}{\prod_{\substack{i\in V\\ i\neq m}}(a_i - a_m)}$$

où V est un sous-ensemble de $\{1, \dots, 2g+1\} \setminus \{k\}$ de cardinal g.

Nous discutons du choix des différentes constantes impliquées dans la partie suivante.

5.1.6 Choix des constantes

Lors de la construction des différentes fonctions nous avons plusieurs choix à faire :
- Choix d'une racine $\sqrt{a_2 - a_1}$.
- Pour tout sous-ensemble A de cardinal plus petit que g, choix de la constante C_A dans la définition 5.1.5.
- Choix du signe σ.

Le but de cette section est de montrer que, quitte à composer l'isomorphisme par l'involution hyperelliptique, on peut les choisir de manière arbitraire.

Il est clair que les sous-ensembles C_A peuvent être choisis de manière arbitraire sans incidence sur les morphismes. En effet, ces ensembles servent uniquement à définir de nouvelles coordonnées. De même le choix de la racine $\sqrt{a_2 - a_1}$ n'est déterminée ni par les valeurs des fonctions thêta, ni par l'équation de la courbe.
Il reste donc à déterminer le signe σ. Ce dernier apparaît dans les formules reliant les fonctions thêta aux fonctions $Y_S(D)$ définies à partir des coordonnées des points dans le support de D. Sur $\mathbb{C}$, nous pouvons évaluer numériquement $z = \mathfrak{u}(D)$, l'image d'un diviseur D par l'application d'Abel-Jacobi. Nous avons donc une valeur numérique pour les deux membres du théorème 5.1.30. Cela détermine le signe de σ. Bien évidement, il va dépendre des autres choix effectués.

La quantité déterminante est, comme nous allons le voir, le produit $\sigma\sqrt{a_2 - a_1}$. Changer le signe de ce produit revient à composer le morphisme par l'involution hyperelliptique. Si nous sommes sur le corps des complexes, le sens des chemins lors du calcul des intégrales hyperelliptiques définissant Ω permet de déterminer ce signe.

Pour justifier ces affirmations, étudions d'abord l'incidence d'un autre choix d'ensemble C_A dans la définition 5.1.5. Supposons choisis pour tout ensemble A deux sous-ensembles C_A et C'_A. Construisons alors les constantes $f_A(C_A)$ (resp. $f_A(C'_A)$) et les fonctions $t_{A,C_A}(z)$ (resp. $t_{A,C'_A}(z)$) associées à C_A (resp. C'_A). De même, soient s_S et s'_S les constantes du théorème 5.1.39 associées aux constantes C_A et σ pour l'une et C'_A et σ' pour l'autre. En utilisant le corollaire 5.1.22 nous obtenons que

$$\begin{aligned} t_{A,C'_A}(z) &= t_{A,C_A}(z)(-1)^{2\,{}^t\eta'_{(C_A\circ C'_A)\cap\mathcal{U}}\zeta''_g} && \#A \leqslant g, \\ t_{A,C'_A}(z) &= t_{A,C_A}(z)(-1)^{2\,{}^t\eta'_{(C_A\circ C'_A)\cap\mathcal{U}}\zeta''_g}(-1)^{2\,{}^t\eta'_{(C_A\circ C'_A)}\zeta''_g} && \#A \geqslant g. \end{aligned}$$

Alors, pour tout ensemble S de cardinal $\#S \geqslant 2$,

$$\frac{s'_S}{\sigma'^n}\frac{t_{S,C'_S}(z)\prod_{l\in S} t_{l,C'_l}(-z)}{t_{\emptyset,C'_\emptyset}(z)^{s+1}} = \frac{s_S}{\sigma^n}\frac{t_{S,C_S}(z)\prod_{l\in S} t_{l,C'_l}(z)}{t_{\emptyset,C_\emptyset}(z)^{s+1}}$$

où $n = \lfloor \frac{\#S}{2} \rfloor$. Comme les fonctions Y'_S sont définies à partir des polynômes de Mumford, elles doivent être invariantes si on change les constantes C_A. Nous en concluons donc que $\sigma = \sigma'$ et nous venons de montrer le lemme suivant :

Lemme 5.1.42. *La constante $\sigma \in \{\pm 1\}$ est indépendante du choix des ensembles C_A dans la définition 5.1.5.*

Regardons maintenant les expressions qui changent selon le choix de la racine de $\sqrt{a_2 - a_1}$. D'après la définition des $\sqrt{< a_i - a_j >}$, ces dernières dépendent du choix $\sqrt{a_2 - a_1}$. Pour toute expression E de $\mathcal{E}$, la parité de $\sum_{i<j} p_{i,j}\,[E]$ permet de savoir si E change de signe quand on change de racine de $\sqrt{a_2 - a_1}$. Un rapide calcul montre que pour tout ensemble $A \subset \{1, \ldots, 2g+1\}$ de cardinal a,

$$\sum_{i<j}(-1)^{\delta_i(A)+\delta_j(A)} = g(2g+1) - 2(2g+1)a + 2a^2$$

et donc que

$$\sum_{i<j} p_{i,j}\left[f_A^2\right] = -g(g+1) + 2g\,a - a(a-1).$$

Par exemple, si $a = g$ ou $g+1$ alors $\sum_{i<j} p_{i,j}\left[f_A^2\right] = 0$, ce qui est cohérent avec le fait que, pour ces sous-ensembles, f_A ne dépend d'aucune racine $\sqrt{< a_i - a_j >}$. D'autres cas particuliers sont

$$\sum_{i<j} p_{i,j}\left[f_\emptyset^2\right] = -g(g+1), \qquad \sum_{i<j} p_{i,j}\left[f_l^2\right] = -g(g-1).$$

Ainsi la quantité $f_l^2/f_\emptyset^2$ est invariante quel que soit le choix de la racine carrée de $\sqrt{a_2-a_1}$. Ceci traduit le fait que $(-1)^g u(a_l) = t_l^2(z)/t_\emptyset^2(z)$ n'en dépende pas. En continuant le calcul, nous obtenons que pour tout sous-ensemble S de cardinal s,

$$\sum_{i<j} p_{i,j}\left[\frac{f_S\prod_{l\in S} f_l}{f_\emptyset^{s+1}}\right] = 2sg - \frac{s(s-1)}{2} \equiv \frac{s(s-1)}{2} \mod 2.$$

La quantité $t_S(z)\prod_{l\in S} t_l(z)/t_\emptyset^{s+1}(z)$ change donc de signe si et seulement si s est congru à 2 ou 3 modulo 4. Cela correspond exactement à l'apparition d'une puissance impaire de σ dans les fonctions Y'_S. De ce fait,

Lemme 5.1.43. *La quantité $\sigma\sqrt{a_2-a_1}$ est indépendante du choix de la racine carrée $\sqrt{a_2-a_1}$ et des choix des constantes C_A.*

Le signe de $\sigma\sqrt{a_2-a_1}$ est fixé par l'isomorphisme ϕ entre $\mathrm{Jac}(\mathcal{C})$ et $\mathbb{C}^g/\Lambda_\Omega$. Montrons cependant que composer ϕ par l'involution hyperelliptique ι ne fait que changer le signe de $\sigma\sqrt{a_2-a_1}$. De ce fait changer ce signe reviendra à dire que, au lieu d'avoir pris l'isomorphisme ϕ, nous avons considéré l'isomorphisme $\phi\circ\iota$.

D'après la définition 5.1.36 de la fonction Y'_S,

$$Y'_S(-D) = (-1)^{\frac{s(s-1)}{2}} Y'_S(D).$$

De ce fait,

$$\frac{t_S(z)\prod_{l\in S} t_l(z)}{t_\emptyset(z)^{s+1}} = (-1)^{\frac{s(s-1)}{2}} Y'_S(-D).$$

Or, nous avons vu que changer le signe de $\sigma\sqrt{a_2-a_1}$ multiplie Y'_S par -1 exactement dans les cas où s est congru à 2 ou 3 modulo 4. De ce fait, considérer le morphisme $\phi\circ\iota$ entre $\mathrm{Jac}(\mathcal{C})$ et $\mathbb{C}^g/\Lambda_\Omega$ au lieu de ϕ, revient bien à faire l'autre choix pour le signe de $\sigma\sqrt{a_2-a_1}$.

En résumé, la première étape du calcul des isomorphismes consiste à choisir arbitrairement des constantes C_A dans la définition 5.1.5 et à choisir une racine de $\sqrt{a_2-a_1}$. Si nous connaissons l'image d'un diviseur qui n'est pas de 2-torsion, à la fois en coordonnées de Mumford et avec les fonctions thêta de niveau 4, alors nous pouvons déterminer la constante σ en évaluant, par exemple, $Y'_{\{1,2\}}$. Ceci est en particulier le cas d'une courbe sur $\mathbb{C}$ où l'application d'Abel-Jacobi a été fixée. Dans le cas contraire, nous choisissons de manière arbitraire σ dans $\{\pm 1\}$.

Par exemple si $\mathcal{C}$ est sous forme de Rosenhain

$$\mathcal{C}:\ y^2 = x(x-1)\prod_{k=3}^{2g+1}(x-a_k),$$

Nous conseillons de numéroter les racines en commençant par 0 puis 1. De ce fait a_2-a_1 est égal à 1 qui est un carré dans tout corps.

En genre 2, Gaudry [Gau07] utilise la numérotation $\{\nu,\mu,\lambda,1,0\}$ où λ,μ,ν sont les invariants de Rosenhain. Avec cette numérotation nous obtenons que a_2-a_1 est l'opposé d'un carré. De ce fait, sur un corps non algébriquement clos, le calcul de l'isomorphisme peut nécessiter de passer dans une extension de degré 2.

5.2 Des fonctions thêta vers les polynômes de Mumford

Avant de commencer à décrire les morphismes, fixons la représentation des coordonnées. En coordonnées de Mumford nous utiliserons la représentation (u,v) et (u,v^2) (sur $\mathrm{Jac}(\mathcal{C})$ et sur $\mathrm{Jac}(\mathcal{C})/\{\pm1\}$). En coordonnées thêta nous utiliserons respectivement les bases suivantes :

$$\begin{array}{ll}\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} & \text{en niveau 4,}\\ \left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega)^2\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} & \text{en niveau 2.}\end{array}$$

5.2.1 En niveau 4

Soit D un diviseur de $\mathrm{Jac}(\mathcal{C})$ n'appartenant pas à Θ, posons $z = \mathfrak{u}(D)$. Supposons connues les fonctions thêta de niveau 4, nous voulons calculer les polynômes de Mumford associés à D.

Pour cela, les polynômes u et v sont calculables par une interpolation de Lagrange sur $g+1$ et g points (u étant unitaire, g points suffisent pour l'interpolation). Les formules 5.1.10 et 5.1.28 donnent l'évaluation de ces polynômes aux points de ramifications : pour tout l dans $\{1,\dots,2g+1\}$,

$$u(a_l) = (-1)^g \frac{t_l^2(z)}{t_\emptyset^2(z)},$$

$$v(a_l) = \sum_{m\in V} \frac{Y_{\{l,m\}}(z)}{\prod_{\substack{k\in V\\ k\neq m}} (a_k - a_m)}$$

où $V \subset \{1,\dots,2g+1\}\setminus\{l\}$ est de cardinal g.

Pour obtenir u, il suffit donc de savoir calculer

$$\frac{t_l^2(z)}{t_\emptyset^2(z)} = \frac{f_l^2}{f_\emptyset^2}\frac{\theta\left[\eta_{\mathcal{U}\circ l}\right](z)^2}{\theta\left[\eta_{\mathcal{U}}\right](z)^2}, \qquad \forall\, l\in\{1,\dots,2g+1\}.$$

Cela est possible en utilisant le doublement :

$$2^g\theta\left[\eta_{\mathcal{U}}\right](z)^4 = \sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S=g}} (-1)^{4\left({}^t\eta'_{\mathcal{U}}\eta''_{\mathcal{U}\circ S}+{}^t\eta'_{\mathcal{U}\circ S}\eta''_{\mathcal{U}}\right)}\theta\left[\eta_{\mathcal{U}\circ S}\right](2z)\theta\left[\eta_{\mathcal{U}\circ S}\right](0)^3,$$

$$2^g\theta\left[\eta_{\mathcal{U}\circ l}\right](z)^2\theta\left[\eta_{\mathcal{U}}\right](z)^2 = \sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S=g}} (-1)^{4\left({}^t\eta'_{\mathcal{U}}\eta''_{S}+{}^t\eta'_{S}\eta''_{\mathcal{U}}+{}^t\eta'_{l}\eta''_{S}\right)}\theta\left[\eta_{\mathcal{U}\circ S\circ l}\right](2z)\theta\left[\eta_{\mathcal{U}\circ S\circ l}\right](0)\theta\left[\eta_{\mathcal{U}\circ S}\right](0)^2.$$

Pour obtenir v, il suffit de calculer pour tous $l\neq m\in\{1,\dots,2g+1\}$,

$$\frac{t_{l,m}(z)t_l(z)t_m(z)}{t_\emptyset^3(z)} = \frac{f_{l,m}(z)f_l(z)f_m(z)}{f_\emptyset^3(z)}\frac{\theta\left[\eta_{\mathcal{U}\circ\{l,m\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ l}\right](z)\theta\left[\eta_{\mathcal{U}\circ m}\right](z)}{\theta\left[\eta_{\mathcal{U}}\right](z)^3}.$$

Pour cela, nous avons la formule

$$2^g\theta\left[\eta_{\mathcal{U}\circ\{l,m\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ l}\right](z)\theta\left[\eta_{\mathcal{U}\circ m}\right](z)\theta\left[\eta_{\mathcal{U}}\right](z) =$$

$$\sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S=g}} (-1)^{4\left({}^t\eta'_{\mathcal{U}}\eta''_{S}+{}^t\eta'_{S}\eta''_{\mathcal{U}}+{}^t\eta'_{\{l,m\}}\eta''_{S}+{}^t\eta'_{l}\eta''_{S\cap m}+{}^t\eta'_{m}\eta''_{S\cap l}\right)}$$

$$\theta\left[\eta_{\mathcal{U}\circ S\circ\{l,m\}}\right](2z)\theta\left[\eta_{\mathcal{U}\circ S\circ l}\right](0)\theta\left[\eta_{\mathcal{U}\circ S\circ m}\right](0)\theta\left[\eta_{\mathcal{U}\circ S}\right](0)$$

où nous avons utilisé le fait que $\theta\left[\eta_{\mathcal{U}\circ S}\right](0) = 0$ si $\#S$ n'est pas égal à g ou $g+1$.

Nous avons donc réussi à calculer les coordonnées de Mumford d'un diviseur générique à partir de ses fonctions thêta de niveau 4.

Exemple 5.2.1. *Poursuivons notre exemple en genre 2. Avec les choix d'ensembles C_A de l'exemple 5.1.9, le théorème 5.1.10 se traduit par*

$$u(a_1) = (a_2-a_1)^2\frac{\theta_0^2\theta_2^2\theta_8^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{10}(z)^2}{\theta_{14}(z)^2}, \qquad u(a_2) = (a_2-a_1)^2\frac{\theta_1^2\theta_3^2\theta_9^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{11}(z)^2}{\theta_{14}(z)^2}.$$

et le polynôme u est alors donné par

$$\begin{aligned} u(x) &= (x-a_1)(x-a_2) + \frac{x-a_2}{a_1-a_2}u(a_1) + \frac{x-a_1}{a_2-a_1}u(a_2)\\ &= (x-a_1)(x-a_2) + \\ &\quad + \frac{a_2-a_1}{\theta_{14}(z)^4\theta_4^2\theta_6^2\theta_{12}^2}\left(-\theta_{10}(z)^2\theta_{14}(z)^2\theta_0^2\theta_2^2\theta_8^2(x-a_2) + \theta_{11}(z)^2\theta_{14}(z)^2\theta_1^2\theta_3^2\theta_9^2(x-a_1)\right) \end{aligned}$$

Les formules de doublement permettent d'obtenir

$$\begin{aligned}4\theta_{14}(z)^4 &= \theta_0(2z)\theta_0^3 - \theta_1(2z)\theta_1^3 - \theta_2(2z)\theta_2^3 + \theta_3(2z)\theta_3^3 + \theta_4(2z)\theta_4^3\\ &\quad -\theta_6(2z)\theta_6^3 - \theta_8(2z)\theta_8^3 + \theta_9(2z)\theta_9^3 - \theta_{12}(2z)\theta_{12}^3 - \theta_{15}(2z)\theta_{15}^3\end{aligned}$$

$$\begin{aligned}4\theta_{10}(z)^2\theta_{14}(z)^2 &= \theta_0(2z)\theta_0\theta_4^2 - \theta_2(2z)\theta_2\theta_6^2 + \theta_4(2z)\theta_4\theta_0^2 - \theta_6(2z)\theta_6\theta_2^2 - \theta_8(2z)\theta_8\theta_{12}^2 - \theta_{12}(2z)\theta_{12}\theta_8^2\\ 4\theta_{11}(z)^2\theta_{14}(z)^2 &= \theta_1(2z)\theta_1\theta_4^2 - \theta_3(2z)\theta_3\theta_6^2 + \theta_4(2z)\theta_4\theta_1^2 - \theta_6(2z)\theta_6\theta_3^2 - \theta_9(2z)\theta_9\theta_{12}^2 - \theta_{12}(2z)\theta_{12}\theta_9^2\end{aligned}$$

Ces formules suffisent pour calculer le polynôme u. Pour v, nous utilisons le théorème 5.1.28 :

$$v(x) = \frac{x-a_2}{a_1-a_2}v(a_1) + \frac{x-a_1}{a_2-a_1}v(a_2),$$

$$v(a_1) = \frac{1}{a_3-a_2}\left(Y_{\{1,2\}}(D) - Y_{\{1,3\}}(D)\right), \qquad v(a_2) = \frac{1}{a_3-a_1}\left(Y_{\{1,2\}}(D) - Y_{\{2,3\}}(D)\right).$$

Les fonctions $Y_{\{l,m\}}$ sont données par (voir l'exemple 5.1.41)

$$\begin{aligned}Y_{\{1,2\}}(D) &= \sigma\frac{t_{\{1,2\}}(z)t_1(z)t_2(z)}{t_\emptyset(z)^3} = -\sigma\sqrt{a_2-a_1}^7\frac{\theta_0^2\theta_1^2\theta_2^2\theta_3^2\theta_8^2\theta_9^2}{\theta_4^4\theta_6^4\theta_{12}^4}\frac{\theta_{10}(z)\theta_{11}(z)\theta_{15}(z)}{\theta_{14}(z)^3},\\ Y_{\{1,3\}}(D) &= \sigma\frac{t_{\{1,3\}}(z)t_1(z)t_3(z)}{t_\emptyset(z)^3} = -\sigma\sqrt{a_2-a_1}^7\frac{\theta_0^3\theta_1^2\theta_2^2\theta_8^3\theta_9^2\theta_{15}^2}{\theta_4^5\theta_6^4\theta_{12}^5}\frac{\theta_3(z)\theta_7(z)\theta_{10}(z)}{\theta_{14}(z)^3},\\ Y_{\{2,3\}}(D) &= \sigma\frac{t_{\{2,3\}}(z)t_2(z)t_3(z)}{t_\emptyset(z)^3} = -\sigma\sqrt{a_2-a_1}^7\frac{\theta_0^2\theta_1^3\theta_3^2\theta_8^2\theta_9^3\theta_{15}^2}{\theta_4^5\theta_6^4\theta_{12}^5}\frac{\theta_2(z)\theta_7(z)\theta_{11}(z)}{\theta_{14}(z)^3}.\end{aligned}$$

Il faut alors utiliser les formules de duplication pour obtenir

$$\begin{aligned}4\theta_{10}(z)\theta_{11}(z)\theta_{14}(z)\theta_{15}(z) &= \theta_5(2z)\theta_0\theta_1\theta_4 - \theta_7(2z)\theta_2\theta_3\theta_6 - \theta_{13}(2z)\theta_8\theta_9\theta_{12},\\ 4\theta_3(z)\theta_7(z)\theta_{10}(z)\theta_{14}(z) &= \theta_5(2z)\theta_1\theta_8\theta_{12} - \theta_{11}(2z)\theta_2\theta_6\theta_{15} - \theta_{13}(2z)\theta_0\theta_4\theta_9,\\ 4\theta_2(z)\theta_7(z)\theta_{11}(z)\theta_{14}(z) &= \theta_5(2z)\theta_0\theta_9\theta_{12} - \theta_{10}(2z)\theta_3\theta_6\theta_{15} - \theta_{13}(2z)\theta_1\theta_4\theta_8.\end{aligned}$$

Nous avons alors toutes les formules pour calculer les polynômes de Mumford (u,v) à partir des fonctions thêta de niveau 4.

5.2.2 En niveau 2

Rappelons que nous nous interessons à un diviseur D de $\mathrm{Jac}(\mathcal{C})$ n'appartenant pas à Θ. Nous avons posé $z = \mathfrak{u}(D)$, l'image de D par l'application d'Abel-Jacobi. Supposons maintenant connues les coordonnées thêta de niveau 2 de D, nous voulons calculer les polynômes de Mumford u et v^2 associés à D. D'après la remarque 5.1.11, les constantes f_A^2 sont calculables à partir des thêta constantes de niveau 2. De ce fait, nous pouvons calculer les valeurs du polynôme u en les points de ramification : pour tout l dans $\{1,\dots,2g+1\}$

$$u(a_l) = (-1)^g\frac{t_l^2(z)}{t_\emptyset^2(z)} = (-1)^g\frac{f_l^2}{f_\emptyset^2}\frac{\theta\left[\eta_{\mathcal{U}\circ l}\right]^2(z)}{\theta\left[\eta_{\mathcal{U}}\right]^2(z)}.$$

Nous obtenons alors u par interpolation de Lagrange. Pour v^2, nous utilisons encore une interpolation de Lagrange (en $2g-1$ points). Pour cela, il faut savoir évaluer pour $l \in \{1,\dots,2g+1\}$,

$$v(a_l)^2 = \sum_{m\in V}\frac{Y_{\{l,m\}}^2(D)}{\prod_{\substack{k\in V\\ k\neq m}}(a_k-a_m)^2} - \sum_{m\neq n\in V}\frac{Y_{\{l,m\}}(D)Y_{\{l,n\}}(D)}{\prod_{\substack{k\in V\\ k\neq m,n}}(a_k-a_m)(a_k-a_n)}$$

où V est un sous-ensemble de $\{1,\dots,2g+1\}$ de cardinal g et ne contenant pas l. Les fonctions $Y_{\{l,m\}}^2(D)$ se calculent trivialement à partir des thêta de niveau 2 :

$$Y_{\{l,m\}}^2(D) = \frac{f_l^2f_m^2f_{\{l,m\}}^2}{f_\emptyset^6}\frac{\theta\left[\eta_{\mathcal{U}\circ l}\right]^2(z)\theta\left[\eta_{\mathcal{U}\circ m}\right]^2(z)\theta\left[\eta_{\mathcal{U}\circ\{l,m\}}\right]^2(z)}{\theta\left[\eta_{\mathcal{U}}\right]^6(z)}.$$

Cependant il faut calculer les produits $Y_{\{l,m\}}(D)Y_{\{l,n\}}(D)$:

$$\begin{aligned} Y_{\{l,m\}}(D)Y_{\{l,n\}}(D) &= s_{\{l,m\}}s_{\{l,n\}}\frac{f_l^2}{f_\emptyset^6}\frac{\theta\left[\eta_{\mathcal{U}\circ l}\right]^2(z)}{\theta\left[\eta_{\mathcal{U}}\right]^6(z)}f_{\{l,m\}}f_{\{l,n\}}f_mf_n \\ &\quad \theta\left[\eta_{\mathcal{U}\circ\{l,m\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ\{l,n\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ m}\right](z)\theta\left[\eta_{\mathcal{U}\circ n}\right](z). \end{aligned}$$

D'après les formules de duplication,

$$2^g\theta\left[\eta_{\mathcal{U}\circ\{l,m\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ\{l,n\}}\right](z)\theta\left[\eta_{\mathcal{U}\circ m}\right](z)\theta\left[\eta_{\mathcal{U}\circ n}\right](z) =$$

$$\sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S=g}}(-1)^g(-1)^{4\left({}^t\eta'_{\mathcal{U}}\eta''_S+{}^t\eta'_S\eta''_{\mathcal{U}}+{}^t\eta'_{\{l\}}\eta''_{S\setminus\{m,n\}}+{}^t\eta_{\{m,n\}}\eta''_{S\setminus\{l\}}\right)}(-1)^{4\left({}^t\eta'_n\eta''_S+{}^t\eta'_S\eta''_n+{}^t\eta'_m\eta''_n\right)}$$

$$\theta\left[\eta_{\mathcal{U}\circ S\circ\{l,m,n\}}\right](2z)\theta\left[\eta_{\mathcal{U}\circ S\circ l}\right](0)\theta\left[\eta_{\mathcal{U}\circ S\circ\{m,n\}}\right](0)\theta\left[\eta_{\mathcal{U}\circ S}\right](0).$$

Dans la somme précédente les ensembles S fournissant des thêta constantes non nulles sont ceux de cardinaux g contenant soit m soit n mais pas l. Nous avons alors $\#S\circ\{l,m,n\}=g+1$ et donc la thêta constante $\theta\left[\eta_{\mathcal{U}\circ S\circ\{l,m,n\}}\right](0)$ est non nulle. Avec une autre application de la formule de duplication nous obtenons

$$2^g\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z)\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0)\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0)^2=\sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t a\beta}\theta\left[\begin{smallmatrix}a+\alpha\\b+\beta\end{smallmatrix}\right](z)^2\theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z)^2.$$

Les formules précédentes montrent que

$$\begin{aligned} Y_{\{l,m\}}(D)Y_{\{l,n\}}(D) &= s_{\{l,m\}}s_{\{l,n\}}\frac{1}{4^g}\frac{f_l^2}{f_\emptyset^2}\frac{\theta\left[\eta_{\mathcal{U}\circ l}\right]^2(z)}{\theta\left[\eta_{\mathcal{U}}\right]^6(z)} \\ &\quad \sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S=g}}\sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\epsilon E\quad\theta\left[\eta_{\mathcal{U}\circ S\circ\{l,m,n\}}+\begin{pmatrix}\alpha\\\beta\end{pmatrix}\right](z)^2\theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z)^2 \end{aligned}$$

où

$$\epsilon=(-1)^g(-1)^{4\left({}^t\eta'_{\mathcal{U}}\eta''_S+{}^t\eta'_S\eta''_{\mathcal{U}}+{}^t\eta'_{\{l\}}\eta''_{S\setminus\{m,n\}}+{}^t\eta_{\{m,n\}}\eta''_{S\setminus\{l\}}\right)}(-1)^{4\left({}^t\eta'_n\eta''_S+{}^t\eta'_S\eta''_n+{}^t\eta'_m\eta''_n\right)}(-1)^{4\,{}^t\eta'_{\mathcal{U}\circ S\circ\{l,m,n\}}\beta},$$

$$E=\frac{f_{\{l,m\}}f_{\{l,n\}}f_mf_n}{f_\emptyset^4}\frac{\theta\left[\eta_{\mathcal{U}\circ S\circ l}\right](0)\theta\left[\eta_{\mathcal{U}\circ S\circ\{m,n\}}\right](0)\theta\left[\eta_{\mathcal{U}\circ S}\right](0)}{\theta\left[\eta_{\mathcal{U}\circ S\circ\{l,m,n\}}\right](0)\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}}\right](0)^2}.$$

Ceci permettrait d'obtenir les produits $Y_{\{l,m\}}(D)Y_{\{l,n\}}(D)$ si nous connaissions les thêta constantes de niveau 4 et la racine $\sqrt{a_2-a_1}$. Comme ce n'est pas le cas, il faut calculer la constante E en fonction des thêta constantes de niveau 2 et des racines de f. La constante E se réécrit

$$\begin{aligned} E &= \frac{f_{\{l,m\}}f_{\{l,n\}}f_mf_n}{f_\emptyset^4}\frac{f_{S\circ\{l,m,n\}}f_{\mathcal{U}}^2}{f_{S\circ l}f_{S\circ\{m,n\}}f_S} \\ E &= \frac{f_{\mathcal{U}}^2f_{S\circ\{l,m,n\}}^2}{f_\emptyset^4}\frac{f_{\{l,m\}}f_{\{n\}}}{f_{\{l,m\}\circ(S\circ\{m\})}f_{\{n\}\circ(S\circ\{m\})}}\frac{f_{\{l,n\}}f_{\{m\}}}{f_{\{l,n\}\circ(S\circ\{l,n\})}f_{\{m\}\circ(S\circ\{l,n\})}}. \end{aligned}$$

La première fraction, en tant que quotient de f_A^2 est calculable sans prendre de racine carrée. Pour l'autre partie, d'après le corollaire 5.1.23 nous avons

$$p_{i,j}\left[\frac{f_{\{l,m\}}f_{\{n\}}}{f_{\{l,m\}\circ(S\circ\{m\})}f_{\{n\}\circ(S\circ\{m\})}}\frac{f_{\{l,n\}}f_{\{m\}}}{f_{\{l,n\}\circ(S\circ\{l,n\})}f_{\{m\}\circ(S\circ\{l,n\})}}\right]=$$

$$=\begin{cases}-2 & \text{si } \#\left(\{i,j\}\cap\{l,m,n\}\right)=0 \text{ et } \#\left(\{i,j\}\cap S\right)=1,\\ 0 & \text{sinon.}\end{cases}$$

Cette dernière expression est clairement un multiple de 2. Par ailleurs, d'après la même propriété,

$$s\left[\frac{f_{\{l,m\}}f_{\{n\}}}{f_{\{l,m\}\circ(S\circ\{m\})}f_{\{n\}\circ(S\circ\{m\})}}\frac{f_{\{l,n\}}f_{\{m\}}}{f_{\{l,n\}\circ(S\circ\{l,n\})}f_{\{m\}\circ(S\circ\{l,n\}}}\right]=$$

$$\begin{aligned}
&= (-1)^{2\,{}^t\eta'_{S\circ\{m\}\setminus\{l,m,n\}}\zeta''_g}(-1)^{2\,{}^t\eta'_{\left(C_{\{l,m\}}\circ C_{\{n\}}\right)\cap\mathcal{U}}\zeta''_g}\\
&\quad (-1)^{2\,{}^t\eta'_{S\circ\{l,n\}\setminus\{l,m,n\}}\zeta''_g}(-1)^{2\,{}^t\eta'_{\left(C_{\{l,n\}}\circ C_{\{m\}}\right)\cap\mathcal{U}}\zeta''_g}\\
&= (-1)^{2\,{}^t\eta'_{\left(C_{\{l,m\}}\circ C_{\{l,n\}}\circ C_{\{m\}}\circ C_{\{n\}}\right)\cap\mathcal{U}}\zeta''_g}.
\end{aligned}$$

Finalement E se calcule bien à partir des racines de f et des thêta constantes de niveau 2.

Exemple 5.2.2. *Toujours avec le même exemple en genre* 2*, les évaluations du polynôme u sont données par*

$$u(a_1) = (a_2-a_1)^2\frac{\theta_0^2\theta_2^2\theta_8^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{10}(z)^2}{\theta_{14}(z)^2},\qquad u(a_2) = (a_2-a_1)^2\frac{\theta_1^2\theta_3^2\theta_9^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{11}(z)^2}{\theta_{14}(z)^2}.$$

Ce qui donne les formules suivantes pour u :

$$\begin{aligned}
u(x) &= (x-a_1)(x-a_2)\\
&\quad +\frac{a_2-a_1}{\theta_{14}(z)^4\theta_4^2\theta_6^2\theta_{12}^2}\left(-\theta_{10}(z)^2\theta_{14}(z)^2\theta_0^2\theta_2^2\theta_8^2(x-a_2)+\theta_{11}(z)^2\theta_{14}(z)^2\theta_1^2\theta_3^2\theta_9^2(x-a_1)\right).
\end{aligned}$$

Pour v^2, nous avons

$$v^2(x)=\frac{(x-a_2)^2}{(a_2-a_1)^2}v(a_1)^2+\frac{(x-a_1)^2}{(a_2-a_1)^2}v(a_2)^2-\frac{(x-a_1)(x-a_2)}{(a_2-a_1)^2}v(a_1)v(a_2)$$

et

$$\begin{aligned}
v(a_1)^2 &= \frac{1}{(a_3-a_2)^2}\left(Y^2_{\{1,2\}}(D)+Y^2_{\{1,3\}}(D)-2Y_{\{1,2\}}(D)Y_{\{1,3\}}(D)\right),\\
v(a_2)^2 &= \frac{1}{(a_3-a_1)^2}\left(Y^2_{\{1,2\}}(D)+Y^2_{\{2,3\}}(D)-2Y_{\{1,2\}}(D)Y_{\{2,3\}}(D)\right),\\
v(a_1)v(a_2) &= \frac{1}{(a_3-a_1)(a_3-a_2)}\left(Y^2_{\{1,2\}}(D)-Y_{\{1,2\}}(D)Y_{\{1,3\}}(D)\right.\\
&\qquad \left.-Y_{\{1,2\}}(D)Y_{\{2,3\}}(D)+Y_{\{1,3\}}(D)Y_{\{2,3\}}(D)\right).
\end{aligned}$$

Or les fonctions $Y^2_{\{l,m\}}(D)$ sont données par

$$\begin{aligned}
Y^2_{\{1,2\}}(D) &= (a_2-a_1)^7\frac{\theta_0^4\theta_1^4\theta_2^4\theta_3^4\theta_8^4\theta_9^4}{\theta_4^8\theta_6^8\theta_{12}^8}\frac{\theta_{10}(z)^2\theta_{11}(z)^2\theta_{15}(z)^2}{\theta_{14}(z)^6},\\
Y^2_{\{1,3\}}(D) &= (a_2-a_1)^7\frac{\theta_0^6\theta_1^4\theta_2^4\theta_8^6\theta_9^4\theta_{15}^4}{\theta_4^{10}\theta_6^8\theta_{12}^{10}}\frac{\theta_3(z)^2\theta_7(z)^2\theta_{10}(z)^2}{\theta_{14}(z)^6},\\
Y^2_{\{2,3\}}(D) &= (a_2-a_1)^7\frac{\theta_0^4\theta_1^6\theta_3^4\theta_8^4\theta_9^6\theta_{15}^4}{\theta_4^{10}\theta_6^8\theta_{12}^{10}}\frac{\theta_2(z)^2\theta_7(z)^2\theta_{11}(z)^2}{\theta_{14}(z)^6}.
\end{aligned}$$

Par ailleurs les produits de deux telles fonctions sont donnés par

$$\begin{aligned}
Y_{\{1,2\}}(D)Y_{\{1,3\}}(D) &= (a_2-a_1)^7\frac{\theta_0^4\theta_1^4\theta_2^4\theta_3^2\theta_8^4\theta_9^4\theta_{15}^2}{\theta_4^{10}\theta_6^8\theta_{12}^{10}}\frac{\theta_{10}(z)^2}{\theta_{14}(z)^6}\theta_3(z)\theta_7(z)\theta_{11}(z)\theta_{15}(z)\theta_0\theta_4\theta_8\theta_{12},\\
Y_{\{1,2\}}(D)Y_{\{2,3\}}(D) &= (a_2-a_1)^7\frac{\theta_0^4\theta_1^4\theta_2^2\theta_3^4\theta_8^4\theta_9^4\theta_{15}^2}{\theta_4^{10}\theta_6^8\theta_{12}^{10}}\frac{\theta_{11}(z)^2}{\theta_{14}(z)^6}\theta_2(z)\theta_7(z)\theta_{10}(z)\theta_{15}(z)\theta_1\theta_4\theta_9\theta_{12},\\
Y_{\{1,3\}}(D)Y_{\{2,3\}}(D) &= (a_2-a_1)^7\frac{\theta_0^4\theta_1^4\theta_2^2\theta_3^2\theta_8^4\theta_9^4\theta_{15}^4}{\theta_4^{10}\theta_6^8\theta_{12}^{10}}\frac{\theta_7(z)^2}{\theta_{14}(z)^6}\theta_2(z)\theta_3(z)\theta_{10}(z)\theta_{11}(z)\theta_0\theta_1\theta_8\theta_9.
\end{aligned}$$

Il faut alors calculer les produits

$$\begin{aligned}
\theta_3(z)\theta_7(z)\theta_{11}(z)\theta_{15}(z)\theta_0\theta_4\theta_8\theta_{12} &= \theta_3(z)^2\theta_{15}(z)^2\theta_0^2\theta_{12}^2 - \theta_0(z)^2\theta_1(z)^2\theta_0^2\theta_1^2 \\
&\quad +\theta_0(z)\theta_1(z)\theta_2(z)\theta_3(z)\theta_0\theta_1\theta_2\theta_3, \\
\theta_2(z)\theta_7(z)\theta_{10}(z)\theta_{15}(z)\theta_1\theta_4\theta_9\theta_{12} &= \theta_2(z)^2\theta_{15}(z)^2\theta_1^2\theta_{12}^2 + \theta_1(z)^2\theta_2(z)^2\theta_1^2\theta_2^2 \\
&\quad +\theta_0(z)\theta_1(z)\theta_2(z)\theta_3(z)\theta_0\theta_1\theta_2\theta_3, \\
\theta_2(z)\theta_3(z)\theta_{10}(z)\theta_{11}(z)\theta_0\theta_1\theta_8\theta_9 &= \theta_2(z)^2\theta_3(z)^2\theta_0^2\theta_1^2 - \theta_0(z)\theta_1(z)\theta_2(z)\theta_3(z)\theta_0\theta_1\theta_2\theta_3.
\end{aligned}$$

Si nous écrivons x, y, z, t pour les fonctions $\theta_0(z), \theta_1(z), \theta_2(z), \theta_3(z)$ et a, b, c, d les thêta constantes associées, nous avons alors

$$2E'\,abcd\,xyzt = F(x^2t^2 + y^2z^2) + G(x^2z^2 + y^2t^2) + H(x^2y^2 + z^2t^2) - (x^4 + y^4 + z^4 + t^4)$$

où

$$\begin{aligned}
A' &= a^2 + b^2 + c^2 + d^2, \qquad B' = a^2 + b^2 - c^2 - d^2, \\
C' &= a^2 - b^2 + c^2 - d^2, \qquad D' = a^2 - b^2 - c^2 + d^2,
\end{aligned}$$

$$E' = \frac{A'B'C'D'}{(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2)},$$

$$\begin{aligned}
F &= (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2), \\
G &= (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2), \\
H &= (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2).
\end{aligned}$$

5.2.3 Cas des diviseurs Θ

Les formules décrites précédemment permettent de calculer les morphismes dans le cas de diviseurs non dégénérés (i.e. la fonction $t_\emptyset$ n'est pas nulle en z). Dans le cas du niveau 4 une méthode naturelle pour calculer l'image d'un diviseur non générique D consiste à calculer l'image de $D + D'$ et de D' où D' est un diviseur générique tel que $D + D'$ l'est aussi. Pour avoir l'image de D, il suffit alors de faire une soustraction.

Cette méthode ne marche malheureusement pas en niveau 2 car on n'y dispose pas d'une vraie addition. Si nous acceptons de travailler dans une extension en prenant une racine carrée, nous pouvons relever le diviseur en niveau 4 et appliquer la méthode précédente. Nous allons décrire une méthode permettant de se ramener au cas d'un diviseur non-thêta en additionnant des points de 2-torsion. Notons que cette méthode marchera aussi en niveau 4.

Soit $D = E - rP_\infty$ un diviseur thêta avec E un diviseur effectif de degré r. Soit $z = \mathfrak{u}(D) \in \mathbb{C}^g$ le vecteur associé à D. Pour $l \in \{1, \ldots, 2g+1\}$, il est facile de savoir si $(a_l, 0)$ appartient au support de E en vérifiant que $t_l(z) = 0$. En niveau 2, il suffit de tester si $\theta\left[\eta_{\mathcal{U}\circ l}\right]^2(z)$ est nul. Il est possible de faire ce test en niveau 4 après avoir utilisé la formule :

$$2^g\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)^4 = \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} (-1)^{4\,{}^t a\beta + 4\,{}^t\alpha b}\theta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](0,\Omega)^3.$$

Additionnons le diviseur $(a_l, 0) - P_\infty$ à D en coordonnée thêta de niveau 2 :

$$\left(\theta\left[\eta_{\mathcal{U}\circ S}\right](z + \mathfrak{u}(a_l), \Omega)^2\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} = \left(\theta\left[\eta_{\mathcal{U}\circ S\circ\{l\}}\right](z,\Omega)^2\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}$$

et en niveau 4 :

$$\left(\theta\left[\eta_{\mathcal{U}\circ S}\right](2(z + \mathfrak{u}(a_l)), \Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} = \left(e_2\left(\eta_{U\circ S}, \eta_l\right)\theta\left[\eta_{\mathcal{U}\circ S}\right](2z,\Omega)\right)_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Algorithme 18 Calcul de l'image d'un diviseur Θ donné par les fonctions thêta

Entrée: Un diviseur D donné par les fonctions thêta de niveau 4.
Sortie: Les coordonnées de Mumford (u, v) de D.

$V := \emptyset$, $l := 1$
while $t_\emptyset(z) = 0$ **do**
  if $t_l(z) \neq 0$ **then**
    Additionner le diviseur $(a_l, 0) - P_\infty$ en coordonnée thêta à D.
    Ajouter l à V.
  end if
end while

Obtenir les coordonnées de Mumford (u, v) du point D ainsi obtenu.

for l dans V **do**
  Diviser u par $x - a_l$.
  $v := v \bmod u$
end for
return (u, v) (resp. (u, v^2)).

Soient u_1 et v_1 les coordonnées de Mumford de $D_1 = E - rP_\infty$ où E est effectif. Supposons que le degré de u soit strictement plus petit que g et que le point $(a, 0)$ n'appartienne pas au support de E, alors les polynômes de Mumford (u_2, v_2) de $D_2 = D_1 + (a, 0) - P_\infty$ sont donnés par

$$u_2(x) = (x - a)u_1(x), \qquad v_2(x) = v_1(x) - \frac{u_1(x)v_1(a)}{u_1(a)}.$$

Remarquons que si nous sommes sur la surface de Kummer,

$$v_2^2(x) = v_1^2(x) + \frac{u_1(x)^2 v_1^2(a)}{u_1(a)^2} - \frac{2u_1(x)v_1(x)v_1(a)}{u_1(a)}$$

et que $v_1(x)v_1(a)$ peut se calculer en fonction de v_1^2 uniquement.

Réciproquement soit $D_2 = E - rP_\infty$ de coordonnées de Mumford (u_2, v_2). Supposons que $(a, 0)$ appartienne au support de E. Alors les coordonnées de Mumford (u_1, v_1) du diviseur $D_1 = D_2 + (a, 0) - P_\infty$ sont données par

$$u_1(x) = \frac{u_2(x)}{x - a}$$
$$v_1(x) = v_2(x) \bmod u_1(x) = v_2(x) - c\, u_1(x)$$

où c est le coefficient de degré $r - 1$ de v_2. Sur la surface de Kummer,

$$v_1^2(x) = v_2^2(x) + c^2 u_1(x)^2 - 2u_1(x)\ c\, v_2(x)$$

où v_2^2, c^2 sont connus et $c\, v_2(x)$ peut se calculer en fonction de v_2^2.

Nous obtenons donc l'algorithme 18 permettant de calculer le morphisme sur un diviseur thêta.

5.3 Des polynômes de Mumford vers les fonctions thêta

5.3.1 Cas des diviseurs génériques

Soit D un diviseur générique de $\mathrm{Jac}(\mathcal{C})$ associé à $z \in \mathbb{C}^g$. Dans cette partie générique signifie que D n'est pas un diviseur thêta et qu'aucun point de ramification n'appartient au support de D. Dans ce cas,

$t_\emptyset(z) \neq 0$ et pour tout $l \in \{1, \dots, 2g+1\}$ nous avons $t_l(z) \neq 0$. Dans le cas du niveau 2, il est trivial de calculer les fonctions thêta à partir des polynômes de Mumford :

$$\frac{t_l^2(z)}{t_\emptyset^2(z)} = (-1)^g u(a_l), \qquad \forall\, l \in \{1, \dots, 2g+1\}$$

$$\frac{t_S^2(z)}{t_\emptyset^2(z)} = (-1)^{g\#S} \frac{Y'_S(D)^2}{\prod_{l\in S} u(a_l)}, \qquad \forall\, S \subset \{1, \dots, 2g+1\},\ 2 \leqslant \#S \leqslant g.$$

Vérifions que $Y_S'^2$ peut se calculer uniquement en fonction de u et v^2. Pour cela, il suffit de voir que $(\phi^* Y_S)^2$ et $(\phi^* Y)^2$ sont
- invariantes par permutation des points de $\mathcal{C}^g$,
- laissées invariantes par l'application $(P_1, \dots, P_g) \longrightarrow \big(\iota(P_1), \dots, \iota(P_g)\big)$.

Exemple 5.3.1. *Dans le cas du genre* 2*, nous obtenons*

$$Y_{\{l,m\}}(D)^2 = \frac{\left(y_1 (x_2 - a_l)(x_2 - a_m) - y_2 (x_1 - a_l)(x_1 - a_m)\right)^2}{(x_2 - x_1)^2}$$

où $D = P_1 + P_2 - 2P_\infty$ *et* $P_i = (x_i, y_i)$*. Nous vérifions bien que l'expression de* $Y_{\{l,m\}}(D)^2$ *est bien invariante si les points* P_i *sont permutés et aussi si on prend l'opposé des deux points* ($y_i \to -y_i$)*. De ce fait* $Y_{\{l,m\}}(D)^2$*, est une fraction rationnelle en les coefficients des polynômes* u *et* v*.*
Pour quelques fonctions thêta, avec la numérotation de Dupont,

$$\begin{array}{rclcl}
\dfrac{1}{t_\emptyset^2(z)}\theta_0^2(z) &=& \dfrac{t_{\{2,4\}}^2(z)}{t_\emptyset^2(z)} &=& \dfrac{Y_{\{2,4\}}(D)^2}{u(a_2)u(a_4)}, \\
\dfrac{1}{t_\emptyset^2(z)}\theta_1^2(z) &=& \dfrac{\theta_1^2}{\theta_0^2}\dfrac{t_{\{1,4\}}^2(z)}{t_\emptyset^2(z)} &=& \dfrac{\theta_1^2}{\theta_0^2}\dfrac{Y_{\{1,4\}}(D)^2}{u(a_1)u(a_4)}, \\
\dfrac{1}{t_\emptyset^2(z)}\theta_2^2(z) &=& \dfrac{\theta_2^2}{\theta_0^2}\dfrac{t_{\{2,3\}}^2(z)}{t_\emptyset^2(z)} &=& \dfrac{\theta_2^2}{\theta_0^2}\dfrac{Y_{\{2,3\}}(D)^2}{u(a_2)u(a_3)}, \\
\dfrac{1}{t_\emptyset^2(z)}\theta_3^2(z) &=& \dfrac{\theta_3^2}{\theta_0^2}\dfrac{t_{\{1,3\}}^2(z)}{t_\emptyset^2(z)} &=& \dfrac{\theta_3^2}{\theta_0^2}\dfrac{Y_{\{1,3\}}(D)^2}{u(a_1)u(a_3)},\ \dots, \\
\dfrac{1}{t_\emptyset^2(z)}\theta_5^2(z) &=& (a_2 - a_1)\dfrac{\theta_1^2}{\theta_4^2}\dfrac{t_4^2(z)}{t_\emptyset^2(z)} &=& (a_2 - a_1)\dfrac{\theta_1^2}{\theta_4^2}u(a_4),\ \dots, \\
\dfrac{1}{t_\emptyset^2(z)}\theta_{14}^2(z) &=& (a_2 - a_1)^3\dfrac{\theta_1^2\theta_2^2\theta_3^2\theta_8^2\theta_9^2\theta_{15}^2}{\theta_4^4\theta_6^4\theta_{12}^4}\dfrac{t_\emptyset^2(z)}{t_\emptyset^2(z)} &=& (a_2 - a_1)^3\dfrac{\theta_1^2\theta_2^2\theta_3^2\theta_8^2\theta_9^2\theta_{15}^2}{\theta_4^4\theta_6^4\theta_{12}^4},\ \dots
\end{array}$$

Supposons maintenant connus les polynômes de Mumford (u, v) d'un diviseur générique D. Les fonctions thêta de niveau 4 associées à D sont de la forme $\theta[\eta_{\mathcal{U}\circ A}](2z)$ avec $\#A \leqslant g$. Pour les calculer, nous allons utiliser les formules de doublement : pour tous $S_1, S_2 \subset \{1, \dots, 2g+1\}$ de cardinal g ou $g+1$,

$$\begin{aligned}
&2^g \theta[\eta_{\mathcal{U}\circ\mathcal{U}\circ S_1\circ S_2}](2z)\,\theta[\eta_{\mathcal{U}\circ S_1}](0)\theta[\eta_{\mathcal{U}\circ S_2}](0)\theta[\eta_{\mathcal{U}\circ\mathcal{U}}](0) \\
&\qquad = \sum_{\substack{S\subset\{1,\dots,2g+1\}\\ \#S\leqslant g}} \omega_S \theta[\eta_{\mathcal{U}\circ S_1\circ S_2\circ S}](z)\,\theta[\eta_{S_1\circ S}](z)\,\theta[\eta_{S_2\circ S}](z)\,\theta[\eta_{\mathcal{U}\circ S}](z) \qquad (5.2)
\end{aligned}$$

où ω_S est égal à

$$\begin{aligned}
\omega_S \;=\;& (-1)^{4\,{}^t\eta'_{\mathcal{U}\circ S_1\circ S_2\circ S}\left(\eta''_{(\mathcal{U}\circ S_1)\cap(\mathcal{U}\circ S_2)}+\eta''_{(\mathcal{U}\circ S_1)\cap(\mathcal{U}\circ S)}+\eta''_{(\mathcal{U}\circ S_2)\cap(\mathcal{U}\circ S)}\right)} \\
& (-1)^{4\,{}^t\eta'_{S_1\circ S}\eta''_{(\mathcal{U}\circ S_2)\cap(\mathcal{U}\circ S)}}(-1)^{4\,{}^t\eta'_{S_2\circ S}\eta''_{(\mathcal{U}\circ S_1)\cap(\mathcal{U}\circ S)}} \\
& (-1)^{4\,{}^t\eta'_{S_1\circ S_2}\eta''_{\mathcal{U}\circ S}}(-1)^{4\,{}^t\eta'_{S_1\circ S_2}\eta''_{(\mathcal{U}\circ S_1)\cap(\mathcal{U}\circ S_2)}}.
\end{aligned}$$

Démonstration. Il suffit d'appliquer la formule du théorème de Koizumi-Kempf 3.1.3 avec la matrice

$$T = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

et les paramètres

$$K = \left[\eta_{\mathcal{U}\circ S_1} + \eta_{\mathcal{U}\circ S_2} | \eta_{\mathcal{U}\circ S_1} | \eta_{\mathcal{U}\circ S_2} | 0\right] \in \mathrm{Mat}_{2g\times 4}\left(\frac{1}{2}\mathbb{Z}\right), \qquad Z = [2z|0|0|0] \in \mathrm{Mat}_{g\times 4}(\mathbb{C}).$$

□

Toutes les fonctions thêta $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z)$ de niveau $(2,2)$ peuvent s'écrire comme $\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ S_1\circ S_2}\right](z)$ avec des ensembles $S_1, S_2 \subset \{1,\dots,2g+1\}$ de cardinaux g ou $g+1$. Par exemple il suffit de les prendre tels que $\eta_{\mathcal{U}\circ S_1} = \begin{pmatrix} a \\ 0 \end{pmatrix}$ et $\eta_{\mathcal{U}\circ S_2} = \begin{pmatrix} 0 \\ b \end{pmatrix}$. Pour ces choix d'ensembles nous avons

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = (-1)^{4\,{}^t\eta'_{S_1\circ S_2}\eta''_{(\mathcal{U}\circ S_1)\cap(\mathcal{U}\circ S_2)}}\theta\left[\eta_{\mathcal{U}\circ\mathcal{U}\circ S_1\circ S_2}\right](z,\Omega).$$

Les fonctions thêta dans la somme de l'équation 5.2 s'expriment comme des quotients $t_A(z)/f_A$. Nous sommes donc ramenés à calculer les produits du type $t_{A_1}(z)t_{A_2}(z)t_{A_3}(z)t_{A_4}(z)$ où les A_i sont quatre sous-ensembles de $\{1,\dots,2g+1\}$ vérifiant $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$. Pour tout $S \subset \{1,\dots,2g+1\}$,

$$\frac{t_S(z)}{t_\emptyset(z)} = \frac{Y'_S(D)}{\prod_{l\in S}\frac{t_l(z)}{t_\emptyset(z)}}.$$

Nous pouvons alors exprimer toutes les fonctions $t_S(z)$ en fonction de (u,v) et des $t_l(z)$ pour l dans S, c'est-à-dire

$$t_{A_1}(z)t_{A_2}(z)t_{A_3}(z)t_{A_4}(z) = t_\emptyset(z)^4\prod_{i=1}^{4}\frac{Y'_{A_i}(D)}{\prod_{l\in A_i}\frac{t_l(z)}{t_\emptyset(z)}}.$$

Comme $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$, la puissance de $t_l(z)/t_\emptyset(z)$ dans le produit précédent est paire et donc s'exprime en fonction de $u(a_l)$. Le facteur projectif $t_\emptyset(z)^4$ n'est pas nul car D n'est pas un diviseur thêta. Nous avons donc réussi à calculer les thêta de niveau 4 à partir des coordonnées de Mumford d'un diviseur.

Exemple 5.3.2. *Nous nous contentons de ne donner le calcul que d'une fonction thêta. La formule de duplication donne*

$$\begin{aligned}\theta_{14}(2z)\theta_0\theta_2\theta_{12} &= \theta_0(z)\theta_2(z)\theta_{12}(z)\theta_{14}(z) + \theta_4(z)\theta_6(z)\theta_8(z)\theta_{10}(z)\\ &\quad -\theta_1(z)\theta_3(z)\theta_{13}(z)\theta_{15}(z) - \theta_5(z)\theta_7(z)\theta_9(z)\theta_{11}(z)\\ &= \frac{t_{\{2,4\}}(z)t_{\{2,3\}}(z)t_{\{3,4\}}(z)t_\emptyset(z)}{f_{\{2,4\}}f_{\{2,3\}}f_{\{3,4\}}f_\emptyset} + \frac{t_{\{3,5\}}(z)t_{\{4,5\}}(z)t_{\{2,5\}}(z)t_{\{2,3,4,5\}}(z)}{f_{\{3,5\}}f_{\{4,5\}}f_{\{2,5\}}f_{\{2,3,4,5\}}}\\ &\quad -\frac{t_{\{1,4\}}(z)t_{\{1,3\}}(z)t_{\{5\}}(z)t_{\{3,4,5\}}(z)}{f_{\{1,4\}}f_{\{1,3\}}f_{\{5\}}f_{\{3,4,5\}}} - \frac{t_{\{4\}}(z)t_{\{3\}}(z)t_{\{1,5\}}(z)t_{\{1,3,4,5\}}(z)}{f_{\{4\}}f_{\{3\}}f_{\{1,5\}}f_{\{2\}}}.\end{aligned}$$

Remarquons que nous n'avons pas forcément choisi l'ensemble A_4 de cardinal le plus petit. En effet, nous

voulons garantir que $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$. *Finalement, nous obtenons*

$$\begin{aligned}\frac{1}{t_\emptyset(z)^4}\theta_{14}(2z)\theta_0\theta_2\theta_{12} &= \frac{Y'_{\{2,4\}}Y'_{\{2,3\}}Y'_{\{3,4\}}Y'_\emptyset}{u(a_2)u(a_3)u(a_4)}\frac{1}{f_{\{2,4\}}f_{\{2,3\}}f_{\{3,4\}}f_\emptyset}\\ &+\frac{Y'_{\{3,5\}}Y'_{\{4,5\}}Y'_{\{2,5\}}Y'_{\{2,3,4,5\}}}{u(a_2)u(a_3)u(a_4)u(a_5)}\frac{1}{f_{\{3,5\}}f_{\{4,5\}}f_{\{2,5\}}f_{\{2,3,4,5\}}}\\ &-\frac{Y'_{\{1,4\}}Y'_{\{1,3\}}Y'_{\{5\}}Y'_{\{3,4,5\}}}{u(a_1)u(a_3)u(a_4)u(a_5)}\frac{1}{f_{\{1,4\}}f_{\{1,3\}}f_{\{5\}}f_{\{3,4,5\}}}\\ &-\frac{Y'_{\{4\}}Y'_{\{3\}}Y'_{\{1,5\}}Y'_{\{1,3,4,5\}}}{u(a_1)u(a_3)u(a_4)u(a_5)}\frac{1}{f_{\{4\}}f_{\{3\}}f_{\{1,5\}}f_{\{1,3,4,5\}}}\end{aligned}$$

où nous avons écrit Y'_S *au lieu de* $Y'_S(D)$. *Cette formule permet de calculer* $\frac{1}{t_\emptyset(z)^4}\theta_{14}(2z)$ *en fonction des polynômes de Mumford.*

5.3.2 Cas des diviseurs non génériques

Les formules décrites précédemment permettent de calculer les morphismes dans le cas de diviseurs génériques (i.e. aucune fonction t_l n'est nulle en z). Encore une fois, dans le cas du niveau 4, la méthode naturelle pour calculer l'image d'un diviseur non générique D consiste à calculer l'image de $D + D'$ et de D' où D' est un diviseur générique tel que $D + D'$ l'est aussi. Pour avoir l'image de D, il suffit alors de faire une soustraction.

Dans le cas du niveau 2, ou si nous ne voulons pas utiliser un diviseur générique D', nous utilisons la méthode suivante. Tout d'abord nous appliquons les formules de la section 5.2.3 pour se ramener au cas d'un diviseur non thêta. Supposons à partir de maintenant que D est un diviseur non thêta, donné par ses coordonnées de Mumford (u, v) (ou (u, v^2) en niveau 2) et supposons que $V \subset \{1, \dots, 2g+1\}$ soit l'ensemble des indices l pour lesquels $u(a_l) = 0$.

Rappelons que, en niveau 2, nous avons $t_S(z)^2 = t_{S^c}(z)^2$. Remarquons que pour tout sous-ensemble S de $\{1, \dots, 2g+1\}$,

$$\begin{array}{lll}\#S < 2\#V \cap S & \Longrightarrow & t_S(z) = 0,\\ \#S \geqslant 2(g+1-\#V) + 2\#V \cap S & \Longrightarrow & t_S(z) = 0.\end{array} \tag{5.3}$$

Pour les autres ensembles S, si aucun élément de V n'appartient à S alors nous pouvons calculer $t_S^2(z)/t_\emptyset^2(z)$, en niveau 2, par la formule :

$$\frac{t_S^2(z)}{t_\emptyset^2(z)} = \frac{Y'_S(D)^2}{\prod_{l\in S}\frac{t_l^2(z)}{t_\emptyset^2(z)}} = (-1)^{g\#S}\frac{Y'_S(D)^2}{\prod_{l\in S}u(a_l)}.$$

Si, au contraire, V est inclus dans S alors en considérant S^c nous nous ramenons au cas précédent. Quels ques soient les ensembles V et S, la fonction

$$\begin{array}{ccc}\mathrm{Jac}(\mathcal{C}) \setminus \Theta & \longrightarrow & \mathbb{C}\\ D & \longmapsto & \dfrac{Y'_S(D)^2}{\prod_{l\in S\cap V}u(a_l)}\end{array}$$

est régulière (il suffit d'utiliser le lemme 5.1.31 pour étudier son diviseur). Si nous ne sommes dans aucun des cas précédents, nous pouvons essayer de trouver une expression de cette fonction qui soit valide sur un ouvert contenant le point D considéré. Nous avons la formule suivante :

Propriété 5.3.3. *Soit* $D = \sum_{i=1}^g P_i - gP_\infty$ *un diviseur de* $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$. *Soient* $W \subset S \subset \{1, \dots, 2g+1\}$ *de cardinal* w *et* s. *Supposons que* $2w \leqslant s \leqslant 2g+1$ *et posons* $n = \lfloor \frac{s}{2} \rfloor$. *Soit* $R \subset \{1, \dots, g\}$, *les indices* i

des P_i qui sont des points de ramifications a_l avec $l \in W$. Alors

$$\frac{Y_S^2(D)}{\prod_{l\in W}(-1)^g u(a_l)} = \sum_{\substack{I,J\subset\{1,\dots,g\}\setminus R\\ \#I=\#J=n-w}} \frac{\prod_{i\in I} y_i \prod_{i\in J} y_i \prod_{l\in W}\prod_{m\notin W} a_l - a_m}{\prod_{l\in W}\prod_{k\in\{1,\dots,g\}\setminus R} x_k - a_l} \prod_{k\in\{1,\dots,g\}\setminus(I\cup R)} \frac{\prod_{l\in S\setminus W} x_k - a_l}{\prod_{i\in I} x_i - x_k} \prod_{k\in\{1,\dots,g\}\setminus(J\cup R)} \frac{\prod_{l\in S\setminus W} x_k - a_l}{\prod_{i\in J} x_i - x_k}.$$

En niveau 2, nous obtenons donc

$$\frac{t_S^2(z)}{t_\emptyset^2(z)} = (-1)^{g\#S}\frac{1}{\prod_{l\in V\setminus S} u(a_l)}\frac{Y_S'(D)^2}{\prod_{l\in S\cap V} u(a_l)}$$

et nous appliquons la formule de la propriété avec $W = V \cap S$. L'hypothèse $2\#W \leqslant \#S$ est vérifiée car d'après 5.3, si nous ne sommes pas dans ce cas, $t_S^2(z)$ est nulle. Ceci résout le problème en niveau 2.

Exemple 5.3.4. *En genre 2, soit $D = P_1 + P_2 - 2P_\infty$ un élément de $\mathrm{Jac}(\mathcal{C})\setminus\Theta$ donné par les polynômes de Mumford (u, v^2). Supposons que P_1 ou P_2 soit un point de Weierstraß. Si les deux le sont, alors D est un élément de 2-torsion et nous pouvons appliquer les formules 3.1.11 pour obtenir les coordonnées thêta de niveau 2 de D.*
Supposons maintenant que $D = P + (a_k, 0) - 2P_\infty$ où P est un point de la courbe et où k appartient à l'ensemble $\{1,\dots,2g+1\}$. Pour tout $l \in \{1,\dots,2g+1\}$ différent de k, le polynôme u ne s'annule pas en a_l. Nous avons alors

$$\begin{aligned}
\frac{1}{t_\emptyset(z)^2}t_\emptyset(z)^2 &= 1\\
\frac{1}{t_\emptyset(z)^2}t_i(z)^2 &= \begin{cases} 0 & i = k\\ \dfrac{1}{u(a_i)} & i \neq k\end{cases}\\
\frac{1}{t_\emptyset(z)^2}t_{\{i,j\}}(z)^2 &= \begin{cases} \dfrac{Y^2_{\{l,m,n\}}(D)}{u(a_l)u(a_m)u(a_n)} & j = k,\ \{l,m,n\} := \{1,\dots,2g+1\}\setminus\{i,j\}\\ \dfrac{Y^2_{\{i,j\}}(D)}{u(a_i)u(a_j)} & i\neq k,\ j\neq k.\end{cases}
\end{aligned}$$

En niveau 4 cela est plus compliqué car dans les formules de doublement 5.2, les fonctions qui apparaissent sont de la forme $t_{A_1}(z)t_{A_2}(z)t_{A_3}(z)t_{A_4}(z)$ avec $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$. Pour pouvoir les calculer, il faut donc savoir calculer les fonctions suivantes :

$$\frac{Y'_{A_1}(D)Y'_{A_2}(D)Y'_{A_3}(D)Y'_{A_4}(D)}{\prod(-1)^g u(a_l)}$$

où le produit porte sur les indices l appartenant à V et à un des ensembles (en le comptant deux fois si l appartient aux quatres). Ceci est possible en développant les formules de la définition des Y'_S comme dans la propriété 5.3.3.

Exemple 5.3.5. *En genre 2, si le diviseur considéré n'est pas de 2-torsion, il n'a qu'un seul point de Weierstraß $(a_k, 0)$ dans son support. Il suffit donc de savoir traiter les fractions du type*

$$\frac{Y'_A(D)Y'_B(D)}{u(a_k)}$$

quand k appartient à A et à B et que ces ensembles sont de cardinal supérieur ou égal à 2 (sinon le produit des thêta est nul). On peut alors donner une formule valide en tout genre comme dans la propriété 5.3.3 mais cela se simplifie encore plus en genre 2. Les seuls ensembles à considérer sont ceux de cardinaux 2, 3 et 5 (d'après la définition de Y'_S).

Supposons que $D = (a_k, 0) + P - 2P_\infty$ *et notons* x_P *l'abscisse de* P*. Si* A *et* B *sont de cardinaux* 2 *ou* 3 *alors*

$$\frac{Y_A(D)Y_B(D)}{u(a_k)} = \frac{\prod_{l\in\{1,\dots5\}\setminus k}(a_l - a_k)\prod_{l\in A\setminus k}(x_P - a_l)\prod_{l\in B\setminus k}(x_P - a_l)}{x_P - a_k}.$$

Si A *est de cardinal* 2 *ou* 3 *et si* B *est de cardinal* 5 *alors*

$$\frac{Y_A(D)Y_B(D)}{u(a_k)} = -\frac{\prod_{l\in\{1,\dots5\}\setminus k}(a_l - a_k)\prod_{l\in A\setminus k}(x_P - a_l)}{x_P - a_k};$$

Si $A = B = \{1, \dots, 2g+1\}$ *alors*

$$\frac{Y(D)^2}{u(a_k)} = \prod_{l\in\{1,\dots5\}\setminus k}(a_l - a_k)\prod_{l\in\{1,\dots5\}\setminus k}(x_P - a_l).$$

5.4 Détails d'implémentation

Les formules de ce chapitre ont été, pour la plupart, testées en Magma. Notre programme n'étant pas spécifique à un genre, il a fallu cependant faire des concessions. Ainsi bien que les fonctions Y_S soient bien définies sur tout $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$ comme le montre le lemme 5.1.32, leur définition 5.1.26 ne fournit pas de formule explicite en tout genre mais une formule pour $\phi^* Y_S$ sur $\mathcal{C}^g \setminus \phi^{-1}\mathcal{D}$ où

$$\mathcal{D} = \{2P_1 + P_2 + \dots + P_{g-1} - gP_\infty \in \mathrm{Jac}(\mathcal{C})\} \subset \mathrm{Jac}(\mathcal{C}).$$

Pour avoir une « expression » de la fonction, valide en tout genre, plusieurs solutions sont possibles :
- Créer une fonction prenant en argument un entier g et qui génère du code résolvant le problème pour le genre g.
- Utiliser des schémas.
- Travailler sur le corps de fonctions $k(\mathcal{C}^g)$.

La première solution a été écartée du fait de sa trop grande complexité de mise en œuvre. Les deux dernières solutions reposent sur des fonctionnalités du langage Magma et sont donc peu coûteuses à programmer. Cependant les calculs deviennent alors très lents. En particulier, dès le genre 3, du fait du nombre important de coordonnées thêta, le temps de calcul des morphismes atteint plusieurs dizaines de secondes.
La solution retenue a été de ne pas traiter le cas général. En utilisant la preuve du lemme 5.1.32, nous avons programmé le cas d'un diviseur « générique » dans $\mathcal{D}$ (i.e. deux points seulement du support sont égaux et pas de points de 2-torsion dedans). Dans le cas d'un diviseur de $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$ ayant des points de 2-torsion dans son support, seul le cas du niveau 2 a été programmé en tout genre. Du code spécifique au genre 2, reposant sur l'exemple 5.3.5 permet de traiter le niveau 4. Ceci permet de gérer la totalité des situations en genre 2 et la majorité en genre plus grand.
En genre quelconque et en niveau 4, il est par ailleurs toujours possible d'additionner un diviseur aléatoire, ce qui a une forte probabilité de rendre le diviseur générique.

Par ailleurs, notre implémentation de ces formules commence en fait par factoriser u pour pouvoir récupérer les coordonnées des points dans le support du diviseur. De même, en niveau 2, la fonction Y_S^2 est théoriquement calculable à partir de (u, v^2) mais nous avons commencé par choisir une racine carrée de v (ce qui peut obliger à prendre une extension de degré 2) avant de travailler dans le corps de décomposition de u.

Pour un genre g fixé, le programme précédent présente de nombreux inconvénients :
- utilisation d'extension de corps ce qui ralentit les calculs.
- Utilisation de « trop » de coordonnées thêta en niveau 2 : 4^g au lieu de 2^g.
- Passage par les diviseurs génériques pour traiter le cas des diviseurs Θ.

En genre fixé, on peut donc considérablement réduire la complexité du programme en trouvant des formules plus spécifiques. En particulier, dans AVIsogenies, il existe du code spécifique au genre 2 en parallèle du code pour les cas génériques.

5.5 Exemple d'application : lois d'additions complètes en genre 2

Soit A_k une variété abélienne sur un corps k, plongée dans un espace projectif $\mathbb{P}^r(k)$:

$$\iota : \ A \hookrightarrow \mathbb{P}^r(k).$$

Rappelons qu'au chapitre 2, nous avions noté μ la loi de groupe sur A :

$$\mu : \begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x + y. \end{array}$$

Sur $\iota(A)$, cette loi de groupe μ sera alors donnée localement par des polynômes.

Notons $k[X_0, \ldots, X_r]/I_X$ l'anneau des fonctions régulières sur $\iota(A)$. L'indice X dans I_X permet de savoir dans quel « espace » l'idéal doit être considéré. L'anneau des fonctions régulières sur le produit $\iota(A) \times \iota(A)$ est

$$R := k[X_0, \ldots, X_r]/I_X \otimes k[Y_0, \ldots, Y_r]/I_Y \simeq k[X_0, \ldots, X_r, Y_0 \ldots, Y_r]/(I_X + I_Y).$$

Définition 5.5.1. *Une loi d'addition $\mathfrak{p}$ de bidegré (m, n) sur $\iota(A) \subset \mathbb{P}^r$ est un ouvert non vide U de $A \times A$ et $r+1$ polynômes p_i appartenant à R bihomogène de degré m en $X_0, \ldots, X_r$ et de degré n en $Y_0, \ldots, Y_r$ et tels que pour tout (x, y) dans $U\left(\overline{k}\right)$,*

$$\iota(\mu(x, y)) = \Big(p_0(\iota(x), \iota(y)) : \ldots : p_r(\iota(x), \iota(y))\Big).$$

C'est à dire que le diagramme suivant doit être commutatif

$$\begin{array}{ccc} U \subset A \times A & \xhookrightarrow{\iota \times \iota} & \mathbb{P}^r \times \mathbb{P}^r \\ \Big\downarrow{\scriptstyle \mu} & & \Big\downarrow{\scriptstyle (p_0, \ldots, p_r)} \\ A & \xhookrightarrow[\iota]{} & \mathbb{P}^r \end{array}$$

Définition 5.5.2. *Un ensemble de lois d'addition est dit k-complet si pour tout point de $A \times A$ il existe une loi d'addition définie sur un ouvert contenant ce point.*
Si cet ensemble est réduit à une seule loi, on parle de loi d'addition k-complète.

Lange et Ruppert [LR85] donnent une caractérisation des lois et des ensembles de lois k-complètes. En particulier ils montrent que le degré minimal d'une loi d'addition est $(2, 2)$. Par ailleurs, il n'existe pas de loi $\overline{k}$-complète, en effet dans [AKR11], il est prouvé que pour qu'un ensemble de lois soit $\overline{k}$-complètes il doit contenir strictement plus de g lois. Sur un corps non algébriquement clos, il peut cependant exister des lois k-complètes.

Exemple 5.5.3. *Il existe des exemples de courbes elliptiques ayant une loi d'addition k-complète : par exemple les courbes d'Edwards [Edw07, BL07] ou les courbes hessiennes tordues [FJ10].*
Pour les courbes d'Edwards, le modèle classique $x^2 + y^2 = 1 + dx^2y^2$ est singulier. Avant de pouvoir l'utiliser avec la théorie précédente il faut considérer le plongement projectif normal associé [Koh11] :

$$X_0^2 + X_1^2 = X_2^2 + dX_3^2, \qquad X_0X_3 = X_1X_2.$$

L'addition classique sur la courbe d'Edwards devient alors

$$\begin{aligned} (X_0, X_1, X_2, X_3) \quad + \quad (Y_0, Y_1, Y_2, Y_3) \quad = \\ \big(X_0^2Y_0^2 - d^2X_3^2Y_3^2, (X_1Y_2 + X_2Y_1)(X_0Y_0 - dX_3Y_3), \\ (X_0Y_3 - X_3Y_0)(X_0Y_0 + dX_3Y_3), (X_1Y_2 + X_2Y_1)(X_0Y_3 - X_3Y_0)\big). \end{aligned}$$

Cette loi est de bidegré $(2, 2)$ et est k-complète si d n'est pas un carré dans k.

Soit k un corps ayant un groupe de Galois absolu $\mathrm{Gal}(\overline{k}/k)$ infini. Cette condition contient les corps finis ou les corps de nombres et elle permet d'éviter les corps algébriquement clos. Arene, Kohel et Ritzenthaler [AKR11] prouvent que pour toute variété abélienne sur k, il existe un plongement projectif de la variété et une loi d'addition k-complète. Dans le cas de la dimension 1, ils montrent que le plongement peut être le modèle de Weierstraß et que pour la dimension 2, il est possible d'utiliser les fonctions thêta de niveau 4 (en supposant que le cardinal de k soit assez grand).

Dans le cas des courbes hyperelliptiques de genre 2, nous allons chercher une loi de bidegré $(2,2)$ qui soit k-complète en utilisant la construction due à Arene, Kohel et Ritzenthaler. La caractérisation de [LR85, lemme 2.1] des lois d'additions sur une variété A est la suivante : $\mathrm{H}^0\left(A\times A, \mathcal{M}_{m,n}\right)$ est isomorphe (l'isomorphisme étant explicite) en tant qu'espace vectoriel aux lois de bidegré (m,n) où $\mathcal{M}_{m,n}$ est un fibré sur $A\times A$ associé au fibré $\mathcal{L}$ sur A (qui détermine le plongement de A dans $\mathbb{P}^r$). Dans le cas où $\mathcal{L}$ est symétrique nous avons $\mathcal{M}_{2,2}=\delta^*\mathcal{L}$ avec δ l'application

$$\delta : \begin{array}{ccc} A\times A & \longrightarrow & A \\ (x,y) & \longmapsto & x-y. \end{array}$$

Soit $\mathcal{C}$ une courbe de la forme $y^2=f(x)$ avec f de degré 5 sur un corps fini k de taille au moins égale à 7. Supposons $\mathrm{Jac}_k(\mathcal{C})$ plongée dans $\mathbb{P}^{15}(k)$ à l'aide des fonctions thêta de niveau $(2,2)$ (c'est à dire que les thêta constantes doivent appartenir à k).
Soit K/k une extension de degré 2 de k et soit $x_0\in K$ n'appartenant pas à k et tel que $f(x_0)$ ne soit pas un carré dans K. Soient $y_0\in L$ tels que $y_0^2=f(x_0)$. Le corps L est donc une extension quadratique de K. Notons $P_0=(x_0,y_0)$ le point de $\mathcal{C}(L)$ correspondant. Posons $\alpha_0=P_0+P_0^\pi-2P_\infty\in\mathrm{Jac}_L(\mathcal{C})$ où π est le Frobenius (élévation à la puissance $q=\#k$). Les conjugués sous l'action de $\mathrm{Gal}(L/k)$ de α_0 sont

$$\begin{array}{lcllcl} \alpha_0 &=& P_0+P_0^\pi-2P_\infty, & \alpha_1 &=& P_0^\pi+\iota(P_0)-2P_\infty, \\ \alpha_2 &=& \iota(P_0)+\iota(P_0)^\pi-2P_\infty & \alpha_3 &=& \iota(P_0)^\pi+P_0-2P_\infty \end{array}$$

où ι désigne l'involution hyperelliptique $\iota((x,y))=(x,-y)$. Posons $\mathrm{T}_{\alpha_i}\,\Theta$ les translatés du diviseur Θ par les α_i et soit $\mathcal{D}$ leur somme :

$$\mathcal{D}=\mathrm{T}_{\alpha_0}\,\Theta+\mathrm{T}_{\alpha_1}\,\Theta+\mathrm{T}_{\alpha_2}\,\Theta+\mathrm{T}_{\alpha_3}\,\Theta.$$

Le diviseur $\mathcal{D}$ est un diviseur sur la variété abélienne $\mathrm{Jac}_k(\mathcal{C})$ (il faut vérifier qu'il est invariant sous l'action de $\mathrm{Gal}(L/k)$) mais il ne possède aucun point rationnel (c'est-à-dire qu'aucun point de $\mathrm{Jac}_k(\mathcal{C})$ n'appartient à $\mathcal{D}$). Par ailleurs ce diviseur est ample et symétrique.
Combiné avec un résultat de [AKR11], ceci démontre qu'il existe une loi k-complète $\mathscr{P}$ de bidegré $(2,2)$ pour le plongement de $\mathrm{Jac}_k(\mathcal{C})$ dans $\mathbb{P}^{15}(k)$ donné par les thêta de niveau $(2,2)$. Formellement il faut considérer le plongement associé à $\mathcal{L}(4\Theta)$ et le loi $\mathscr{P}$ est telle que son ensemble de non-définition (sur $\overline{k}$) soit $\delta^*\mathcal{D}$.

Remarque 5.5.4. *La construction précédente peut être adaptée pour d'autres types de corps, par exemple les corps hilbertiens (voir [AKR11]).*

Pour simplifier la présentation, nous considèrons les fonctions thêta sur le corps de base $\mathbb{C}$. Les résultats suivants s'étendent directement aux sous corps de $\mathbb{C}$ et par le principe de Lefschetz aux corps de caractéristique 0. Pour d'autres types de corps (et en particulier les corps finis), il faut utiliser la théorie algébrique des fonctions thêta. Cependant les preuves restent facilement adaptables dans ce nouveau formalisme.

Reprenons les résultats de la section 3.2.1. Les lois de Baily $\mathscr{P}_{a,b}$ (lois d'addition en niveau $(2,2)$) sont définies pour tous a et b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ par

$$\begin{array}{ccc} A\times A \;\subset\; \mathbb{A}^{4^g}\times\mathbb{A}^{4^g} & \longrightarrow & A\subset\mathbb{A}^{4^g} \\ \left(\theta\left[\begin{smallmatrix}\mathfrak{a}\\ \mathfrak{b}\end{smallmatrix}\right](2z,\Omega)\right)_{\mathfrak{a},\mathfrak{b}},\left(\theta\left[\begin{smallmatrix}\mathfrak{a}\\ \mathfrak{b}\end{smallmatrix}\right](2z',\Omega)\right)_{\mathfrak{a},\mathfrak{b}} & \longmapsto & \left(\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](2(z-z'),\Omega)\,\theta\left[\begin{smallmatrix}\mathfrak{a}\\ \mathfrak{b}\end{smallmatrix}\right](2(z+z'),\Omega)\right)_{\mathfrak{a},\mathfrak{b}} \end{array}$$

où $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$. Pour calculer l'application précédente, nous utilisons les formules suivantes :

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2(z-z'),\Omega)\,\theta\left[\begin{smallmatrix}\mathfrak{a}\\\mathfrak{b}\end{smallmatrix}\right](2(z+z'),\Omega) = \frac{1}{\theta\left[\begin{smallmatrix}a_3\\b_3\end{smallmatrix}\right](0,\Omega)\,\theta\left[\begin{smallmatrix}a_4\\b_4\end{smallmatrix}\right](0,\Omega)}\frac{1}{2^g}\times$$
$$\times \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta\left[\begin{smallmatrix}A+a_1+\alpha\\B+b_1+\beta\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}-A+a_2+\alpha\\-B+b_2+\beta\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}-A+a_3+\alpha\\-B+b_3+\beta\end{smallmatrix}\right](2z',\Omega)\,\theta\left[\begin{smallmatrix}-A+a_4+\alpha\\-B+b_4+\beta\end{smallmatrix}\right](2z',\Omega) \tag{5.4}$$

où a_3, a_4, b_3, b_4 sont choisis dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ de telle sorte que les thêta constantes ne soient pas nulles et que

$$A = \frac{a+\mathfrak{a}+a_3+a_4}{2}, \qquad B = \frac{b+\mathfrak{b}+b_3+b_4}{2}$$

appartiennent à $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$. La propriété 3.2.1 montre que l'équation 5.4 est indépendante du choix des éléments a_3, a_4, b_3, b_4. La différence entre deux équations provenant de choix différents appartient en fait à l'idéal de la variété (engendré par les équations de Riemann 3.1.13) et est donc nulle pour tous z, z'.

Ces lois sont clairement de bidegré $(2,2)$. Leur domaine de non-définition est constitué par le lieux de points z, z' tels que $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2(z-z'),\Omega) = 0$. D'après la propriété 3.1.22 c'est donc le diviseur $\delta^*\,\mathrm{T}_{\mathcal{K}+\Omega a+b}\,\Theta$.

Lemme 5.5.5. *Les lois de Baily sont linéairement indépendantes.*

Une preuve élémentaire sur $\mathbb{C}$ de ce lemme est la suivante.

Démonstration. Supposons qu'il existe des coefficients $\lambda_{a,b}$ tels que

$$\sum_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b}\mathscr{P}_{a,b} = 0.$$

C'est-à-dire que pour tous vecteurs z, z' de $\mathbb{C}^g$,

$$\sum_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b}\mathscr{P}_{a,b}(z,z') = 0.$$

En particulier pour $z' = 0$ et en considérant la coordonnée $\mathfrak{a}, \mathfrak{b}$, nous obtenons

$$\sum_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)\,\theta\left[\begin{smallmatrix}\mathfrak{a}\\\mathfrak{b}\end{smallmatrix}\right](2z,\Omega) = 0.$$

Comme il existe une coordonnée $\mathfrak{a}, \mathfrak{b}$ telle que $\theta\left[\begin{smallmatrix}\mathfrak{a}\\\mathfrak{b}\end{smallmatrix}\right](2z,\Omega)$ soit non nulle, nous avons que pour tout z,

$$\sum_{a,b\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega) = 0.$$

Le théorème 3.1.10 implique alors que les $\lambda_{a,b}$ sont tous nuls. □

Lemme 5.5.6. *Les lois de Baily forment une base des lois d'addition de bidegré* $(2,2)$.

Démonstration. Les lois d'addition de bidegré $(2,2)$ forme un espace vectoriel isomorphe à

$$\mathrm{H}^0\left(A\times A, \mathcal{M}_{2,2}\right) = \mathrm{H}^0\left(A\times A, \delta^*\mathcal{L}\right) \simeq \delta^*\,\mathrm{H}^0\left(A,\mathcal{L}\right).$$

La dimension de ce dernier espace est de 4^g car le plongement est dans $\mathbb{P}^{4^g-1}$. Or le lemme précédent montre que les 4^g lois de Baily forment une famille libre, c'est donc une base. □

Nous allons exprimer la loi $\mathscr{P}$ cherchée comme combinaison linéaire des lois $\mathscr{P}_i$:

$$\mathscr{P} = \sum_{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b} \mathscr{P}_{a,b}.$$

Par abus de notation, si D et D' correspondent aux vecteurs z et z' de $\mathbb{C}^g$, nous notons $\mathscr{P}(z, z')$ au lieu de $\mathscr{P}(D, D')$. Avec la définition précédente des lois de Baily nous avons alors pour tous vecteurs z, z' et toutes coordonnées $(\mathfrak{a}, \mathfrak{b})$

$$\rho_{z,z'} \theta \left[\begin{smallmatrix} \mathfrak{a} \\ \mathfrak{b} \end{smallmatrix}\right] (2(z+z'), \Omega) = \sum_{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (2(z-z'), \Omega)\, \theta \left[\begin{smallmatrix} \mathfrak{a} \\ \mathfrak{b} \end{smallmatrix}\right] (2(z+z'), \Omega)$$

où $\rho_{z,z'}$ est un facteur projectif dépendant uniquement de z, z' et évidement de $\mathscr{P}$. Il existe une coordonnée non nulle et nous avons donc la relation

$$\rho_{z,z'} = \sum_{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (2(z-z'), \Omega)\,.$$

La loi $\mathscr{P}$ n'est pas définie pour les points de $A \times A$ du type (D, O_A) où $D \in \mathcal{D}$. Pour ces points nous avons $\mathscr{P}(D, O_A) = (0)_{a,b}$ qui n'est donc pas un point $\mathbb{P}^{15}$. Pour un tel point, posons z un vecteur de $\mathbb{C}^g$ correspondant à D, nous obtenons

$$0 = \sum_{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \lambda_{a,b} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (2z, \Omega)\,. \tag{5.5}$$

Lemme 5.5.7. *Les coefficients $\lambda_{a,b}$ correspondants aux lois $\mathscr{P}_{a,b}$ impaires (c'est-à-dire les lois pour lesquelles $(-1)^{4\,{}^t ab} = -1$) sont nuls.*

Démonstration. Remarquons que si D appartient à $\mathcal{D}$ alors il en est de même de $\iota(D)$ (par contre $\iota(D)$ n'appartient pas au même $\mathrm{T}_{\alpha_i}\,\Theta$ que D). En comparant l'équation 5.5 pour D et $\iota(D)$ nous obtenons que

$$0 = \sum_{\substack{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g \\ (-1)^{4\,{}^t ab} = -1}} \lambda_{a,b} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (2z, \Omega)\,.$$

Par ailleurs, cette équation est aussi valide pour $z = 0$ car les fonctions sont impaires. Nous avons donc obtenu une équation linéaire valide sur $\mathcal{D} \cup \{0\}$. Comme le plongement de A considéré est associé à $\mathcal{L}(4\Theta)$, cette équation est alors valide sur tout A. Comme les fonctions thêta sont linéairement indépendantes, les coefficients de la relation linéaire doivent être nuls. □

Remarquons finalement que $\mathscr{P}$ n'est définie qu'à un facteur près par le diviseur $\mathcal{D}$, nous cherchons donc à obtenir les $\lambda_{a,b}$ à un facteur projectif près. Pour tout point D de $\mathcal{D}$ nous avons les relations suivantes entre les $\lambda_{a,b}$:

$$0 = \sum_{\substack{a,b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g \\ (-1)^{4\,{}^t ab} = 1}} \lambda_{a,b} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (2z, \Omega)\,. \tag{5.6}$$

Chaque point de $\mathcal{D}$ fournira donc une relation entre les $\lambda_{a,b}$. Les lois de Baily étant génératrices, et la loi $\mathscr{P}$ étant « définie » par $\mathcal{D}$, nous avons suffisamment de relations pour obtenir les $\lambda_{a,b}$ (à un facteur projectif près).

En pratique, les éléments D de $\mathrm{T}_{\alpha_i}\,\Theta$ s'expriment facilement en coordonnées de Mumford : ils sont du type $D = (P - P_\infty) + \alpha_i$ où P est un point de la courbe $\mathcal{C}$. Grâce aux morphismes (section 5.3), nous pouvons alors calculer les coordonnées thêta de niveau $(2, 2)$ correspondant à D pour obtenir des relations 5.6. Nous obtenons un système linéaire de rang 9 (il y a 10 inconnues projectives).

En pratique, nous prenons un i au hasard puis un élément D de Θ_{α_i}. Le système obtenu est presque toujours de rang 9 après avoir généré 9 équations. Pour trouver un élément non nul du noyau, nous pouvons alors utiliser les méthodes classiques d'algèbre linéaire.

Nous avons remarqué qu'avec uniquement des points toujours dans le même Θ_{α_i} alors le rang du système sera strictement inférieur à 9. Cela est cohérent avec la théorie : le fibré $\mathcal{L}$ qui définit le plongement est associé à $\mathcal{D}$. Or il existe plusieurs diviseurs $\mathcal{D}$ ayant les propriétés demandées et partageant une même composante Θ_{α_i}.

Les calculs pratiques (utilisant les morphismes de AVIsogenies) sont relativement efficaces. Cependant, pour des corps de taille cryptographique, le calcul peut prendre quelques minutes.
Théoriquement, cette méthode est valide sur des corps de fonctions, et nous pourrions obtenir une formule rationnelle pour les $\lambda_{a,b}$ en fonction des paramètres de la courbe et des éléments x_0, y_0. Nous avons les paramètres suivants :

- la courbe hyperelliptique est définie par ses trois invariants de Rosenhain (λ, μ, ν).
- Les thêta constantes de niveau $(2, 2)$ associée à la courbe doivent être rationnelles.
- Un point x_0 appartenenant à une extension quadratique du corps de base (mais pas au corps de base) et tel que $f(x_0)$ ne soit pas un carré.
- Une racine carrée y_0 de $f(x_0)$.

Il faut ensuite générer des points P au hasard en coordonnée de Mumford pour résoudre le système. Le corps de fonction considérée serait donc de degré de transcendance supérieure ou égal à 4. Par ailleurs il derait nécessaire de prendre des extensions algébriques de degré

- 2^{13} pour que les theta constantes soient rationnelles,
- 2 pour définir le corps K auquel appartiendra x_0,
- 2 pour construire y_0.

soit une extension algébrique de degré totale 2^{15}. Les calculs sont donc inapplicables en pratique.
Une autre solution pourrait être de calculer les $\lambda_{a,b}$ pour un certain nombre de courbes et d'utiliser des méthodes d'interpolations pour reconnaître des fractions rationnelles. Cependant, le nombre de variables (3 invariants de Rosenhain et les coordonnées (x_0, y_0)) et le degré de ces fractions sont trop élevés pour espérer pouvoir faire les calculs.

Donnons un exemple de loi complète sur la courbe

$$y^2 = f(x) = x^5 + 5782x^4 + 2517x^3 + 2312x^2 + 9402x$$

définie sur le corps $\mathbb{F}_{10007}$. Les thêta constantes (non nulles) associées à cette courbe sont (avec la numérotation de Dupont) :

$$\begin{array}{cccccccccccc} \theta_0 & = & 1, & \theta_1 & = & 7727, & \theta_2 & = & 678, & \theta_3 & = & 5242, & \theta_4 & = & 3926, \\ \theta_6 & = & 7092, & \theta_8 & = & 5628, & \theta_9 & = & 3666, & \theta_{12} & = & 7556, & \theta_{15} & = & 904. \end{array}$$

Posons alors

$$K = \mathbb{F}_{10007}[X]/X^2 + 1 \simeq \mathbb{F}_{10007^2}.$$

Soit $x_0 = 8310 + 2164\sqrt{-1}$, le point $\left(x_0, \sqrt{f(x_0)}\right)$ est alors un point de la courbe $\mathcal{C}\left(\mathbb{F}_{10007^4}\right)$ n'appartenant pas à la courbe $\mathcal{C}\left(\mathbb{F}_{10007^2}\right)$. Les coefficients λ_i (avec la notation de Dupont) non nuls sont alors à un facteur près

$$\begin{array}{cccccccccccc} \lambda_0 & = & 1, & \lambda_1 & = & 1940, & \lambda_2 & = & 9380, & \lambda_3 & = & 6924, & \lambda_4 & = & 5155, \\ \lambda_6 & = & 1278, & \lambda_8 & = & 7239, & \lambda_9 & = & 6859, & \lambda_{12} & = & 1761, & \lambda_{15} & = & 5891. \end{array}$$

Ce calcul a pris une vingtaine de secondes. Nous pouvons vérifier que la loi est $\mathbb{F}_{10007}$-complète. Cette vérification exhaustive prend par contre plusieurs jours. Pour réduire le temps de calcul, nous avons utilisé le fait que d'après [LR85, proposition 2.2], pour tout diviseur D de $\mathrm{Jac}(\mathcal{C})\left(\mathbb{F}_{10007}\right)$, nous devons avoir $\mathscr{P}(D, O_{\mathrm{Jac}(\mathcal{C})}) = D$.

Chapitre 6

Formules à la Thomae

Soit $\mathcal{C}$: $y^2 = \prod_{i=1}^{2g+1}(x - a_i)$ une courbe hyperelliptique. La formule de Thomae (introduite au théorème 3.1.19) exprime les puissances 4-ièmes des thêta constantes de niveau $(2,2)$ de la famille $\mathscr{F}_{(2,2)}$ (ou de manière équivalente, les carrés des thêta constantes de niveau 2 de la famille $\mathscr{F}_{(2,2)^2}$) en fonction des paramètres de la courbe.

Nous souhaitons obtenir les thêta constantes de niveau n (premier avec la caractéristique de corps) associées à un plongement de la jacobienne de la courbe hyperelliptique dans l'espace projectif $\mathbb{P}^{n^g-1}(\mathbb{C})$. C'est-à-dire que nous n'avons pas besoin des valeurs exactes des fonctions thêta évaluées en 0 mais celles de certains quotients. La formule de Thomae se réécrit de la manière suivante : soit un sous-ensemble S de $\{1,\dots,2g+1\}\cup\{\infty\}$

$$\left(\frac{\theta\left[\eta_{\mathcal{U}\circ S}\right]}{\theta[0]}\right)^4 = \begin{cases} (-1)^{\#(\mathcal{U}\setminus S)}\dfrac{\prod_{\substack{i\in\mathcal{U}\\ j\notin\mathcal{U}}}(a_i-a_j)}{\prod_{\substack{i\in S\\ j\notin S}}(a_i-a_j)} & \text{si } \#S\in\{g,g+1\},\\ 0 & \text{sinon.}\end{cases}$$

Des preuves de ce cas particulier sont données dans [Zar28, EF08]. Rappelons que, au signe près, les fonctions thêta associées à S et à S^c (où le complémentaire est pris dans $\{1,\dots,2g+1\}\cup\{\infty\}$) sont les mêmes.

Il existe différents type de généralisation de la formule de Thomae. Par exemple des formules à la Thomae (c'est-à-dire donnant les thêta constantes de niveau n en fonction des paramètres de la courbe) ont été découvertes pour d'autres types de courbes. La principale méthode pour obtenir ces formules consiste à utiliser la géométrie des courbes par rapport à un certain entier n pour obtenir les thêta constantes de niveau n. De ce fait l'entier n est déterminer par la forme de la courbe. Dans notre cas, nous nous intéressons au cas de courbes hyperelliptiques (de genre quelconque) mais nous voulons faire varier le niveau des thêta constantes.

Nous commençons par présenter une méthode analytique. Cette méthode permet de retrouver les formules de Thomae pour le niveau $(2,2)$ et couvre le genre 1. Dans la section 6.2, nous expliquons comment extraire les racines de façon à obtenir les vraies valeurs des thêta constantes. Pour le genre supérieur, nous n'avons pas réussi à conclure par la méthode analytique. Dans la section 6.3, nous proposons une autre méthode qui nécessite d'utiliser les fonctions de niveau $(2,2)$.

6.1 Méthode analytique

6.1.1 Idée générale

Rappelons que l'application d'Abel-Jacobi a été définie par

$$\mathfrak{u} : \begin{cases} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathbb{C}^g/\Lambda_\Omega \\ \sum n_i P_i & \longmapsto & \sum \int_{P_\infty}^{P_i}\omega \mod \Lambda_\Omega \end{cases}$$

où Ω est la matrice des périodes de la courbes. Nous supposons le polynôme f de degré impair et nous donnons un ordre à ses $2g+1$ racines

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

Nous notons $\mathcal{K}$ la constante de Riemann introduite en 2.3.16 :

$$\mathcal{K} = \Omega\eta'_{\mathcal{U}} + \eta''_{\mathcal{U}} = \mathfrak{u}\left(\sum_{l\in\mathcal{U}}(a_l, 0) - (g+1)P_\infty\right)$$

$${}^t\eta'_{\mathcal{U}} = \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right), \qquad {}^t\eta''_{\mathcal{U}} = \left(\frac{g}{2}, \frac{g-1}{2}, \ldots, \frac{1}{2}\right).$$

Notons K le diviseur $\sum_{l\in\mathcal{U}}(a_l, 0) - (g+1)P_\infty$ de $\mathrm{Jac}(\mathcal{C})$. Ainsi, nous avons $\mathcal{K} = \mathfrak{u}(K)$. Par abus de notations, les fonctions thêta étant toujours associées à la matrice Ω, nous écrivons $\theta[e](z)$ au lieu de $\theta[e](z, \Omega)$. Pour tout entier n, nous nous intéressons aux thêta constantes de niveau n de la famille $\mathscr{F}_{(n,n)^n}$:

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0)^n \qquad a, b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g.$$

Rappelons que la formule 3.17 permet alors de calculer projectivement les thêta constantes de niveau n des autres bases.

Pour tout élément $\alpha \in \mathbb{C}^g$ et tout vecteur e de $\frac{1}{n}\mathbb{Z}^{2g}$, la fonction

$$\begin{array}{ccc} \mathbb{C}^g & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ z & \longmapsto & \left(\dfrac{\theta[e](z+\alpha)}{\theta(z+\alpha)}\right)^n \end{array}$$

est invariante sous l'action de Λ_Ω et induit donc en une fonction de $\mathbb{C}^g/\Lambda_\Omega$ dans $\mathbb{C}$. Nous pouvons alors la composer avec l'application d'Abel-Jacobi :

Définition 6.1.1. *Soit D un élément de $\mathrm{Jac}(\mathcal{C})$. Soit un entier $n > 1$ et soit e un vecteur de $\frac{1}{n}\mathbb{Z}^{2g}$. La fonction*

$$q : \left\{ \begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ \delta & \longmapsto & \left(\dfrac{\theta[e](\mathfrak{u}(\delta) - \mathfrak{u}(D) - \mathcal{K})}{\theta(\mathfrak{u}(\delta) - \mathfrak{u}(D) - \mathcal{K})}\right)^n \end{array} \right.$$

est bien définie et est analytique.

Nous notons $q_e(\,\cdot\,; D)$ pour préciser la dépendance de q en D et e. Pour obtenir une puissance de la thêta constante qui nous intéresse, nous voulons calculer

$$q_e(D + K; D) = \left(\frac{\theta[e](0)}{\theta(0)}\right)^n.$$

Supposons que la caractéristique e corresponde à un diviseur $E \in \mathrm{Jac}(\mathcal{C})$, c'est-à-dire que nous supposons que $\mathfrak{u}(E) = \Omega e' + e''$. D'après 3.1.22, la fonction $q_e(\,\cdot\,; D)$ a pour diviseur $n\,\mathrm{T}_{D-E}\,\Theta - n\,\mathrm{T}_D\,\Theta$. D'après [Ser56], il existe une fraction rationnelle que nous notons R qui a le même diviseur que q. De ce fait, il existe une constante B (par rapport à δ mais pouvant dépendre de D et e) telle que

$$q_e(\delta; D) = B_e(D)R_e(\delta; D)$$

où nous avons précisé la dépendance par rapport aux paramètres e et D. En utilisant la propriété 3.1.2 et la parité de la fonction thêta de Riemann, nous pouvons montrer que

$$q_e(\delta - E; D)q_e(-\delta; -D) = \exp\left(2i\pi n\,{}^t e' e''\right).$$

Nous obtenons donc

$$B_e(D)B_e(-D) = \frac{\exp\left(2i\pi n\,{}^t e' e''\right)}{R_e(\delta - E; D)R_e(-\delta; -D)}.$$

Si D est un diviseur de 2-torsion, nous obtenons le carré de B. En particulier, pour $D = O$, nous avons le lemme

Lemme 6.1.2. *Avec les notation précédentes,*

$$\left(\frac{\theta[e]\,(0)}{\theta\,(0)}\right)^{2n} = q_e(K;0)^2 = \exp\left(2i\pi 2n\,{}^t e' e''\right)\frac{R_e\,(K;O)}{R_e\,(K-E;O)}$$

où R est une fraction rationnelle sur $\mathrm{Jac}(\mathcal{C})$ *de diviseur* $n\,\mathrm{T}_E\,\Theta - n\Theta$.

La partie difficile est de construire la fraction R. Ce résultat est atteint dans la section 6.1.2 pour le genre 1 et dans la section 6.1.3 pour le niveau $(2,2)$.

La méthode proposée par Riemann [Rie57, p. 154-155] consiste à étudier la restriction de la fonction q précédente sur la courbe $\mathcal{C}:\ y^2 = f(x)$ vue comme une surface de Riemann compacte. Pour distinguer les deux fonctions nous la notons q' :

$$q' : \left\{\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ \delta & \longmapsto & \left(\dfrac{\theta[e]\,(\mathfrak{u}(\delta)-\mathfrak{u}(D)-\mathcal{K})}{\theta\,(\mathfrak{u}(\delta)-\mathfrak{u}(D)-\mathcal{K})}\right)^n \end{array}\right. .$$

Cette fonction est encore bien définie et est analytique. Pour étudier ses zéros et ses pôles, nous devons supposer que D est de poids g : posons alors $D = D_1 + \ldots + D_g - gP_\infty$. Pour obtenir la thêta constante cherchée, nous voulons alors évaluer la fonction en $\delta = (a_1, 0)$ et $D_i = (a_{2i+1}, 0)$. Soit

$$F = F_1 + \ldots + F_g - gP_\infty$$

le diviseur réduit dans la classe de $D - E$. D'après 3.1.23, le diviseur de q' est alors $nF - nD$ (c'est-à-dire que les points du support de D sont des pôles de degré n de la fonction et que ceux du diviseur réduit F sont ses zéros et sont également d'ordre n). Il existe une fraction rationnelle que nous notons R' qui a le même diviseur que q. De ce fait, il existe une constante B' telle que

$$q'_e(\delta; D) = B'_e(D) R'_e(\delta; D).$$

Cette fois, R' est une fraction rationnelle en (x, y) les coordonnées des points sur la courbe. La fraction R' est facilement constructible avec l'algorithme de Cantor. Par contre nous ne pouvons plus appliquer la méthode précédente pour calculer B' car $\delta - E$ n'est pas un point de $\mathcal{C}$. Dans [Zar28, p. 324], Zariski propose d'exprimer

$$q'_e(F_1; \delta, \iota(F_2), \ldots, \iota(F_g))$$

en fonction de $q'_e(\delta, D)$. L'équation obtenue est

$$q'_e(F_1; \delta, \iota(F_2), \ldots, \iota(F_g)) q'_e(\delta; D_1, \ldots, D_g) = \exp\left(2i\pi n\,{}^t e' e''\right)$$

et donc

$$B'_e\left(\delta, \iota(F_2), \ldots, \iota(F_g)\right) B'_e\left(D_1, \ldots, D_g\right) = \frac{\exp\left(2i\pi n\,{}^t e' e''\right)}{R'_e\left(\delta, \iota(F_2), \ldots, \iota(F_g)\right) R'_e\left(D_1, \ldots, D_g\right)}.$$

Si B' ne dépend pas des points D_i, nous pouvons alors calculer B'^2. De même, si B' ne dépend que d'un seul D_i, il est possible de modifier la preuve précédente pour obtenir une expression de B'^2. Théoriquement, il est possible de modifier R' pour supprimer la dépendance de B' en les D_i. Nous connaissons les zéros et pôles de q' en toutes les variables mais le problème est que lors de la construction de R', des pôles et zéros « parasites » sont créés.

6.1.2 Genre 1

Dans le cas du genre 1, nous identifions la courbe avec sa jacobienne. La fraction rationnelle R est facilement constructible. Rappelons qu'elle a pour diviseur $n\,\iota(E) - nP_\infty$ où E est un point de n-torsion et où ι est l'involution hyperelliptique. De plus, nous devons l'évaluer en le diviseur $\rho(K) - \rho(K - E)$ où $\rho(D)$ désigne le diviseur réduit dans la classe d'un diviseur D.

Ceci peut se faire avec le même type d'algorithme que celui utilisé pour le couplage de Tate en faisant attention au fait que nous n'avons pas le droit de prendre un autre diviseur dans la classe de $\rho(K) - \rho(K-E)$. En effet le résultat doit être exact et non pas modulo une racine de l'unité. Si le support de $\rho(K) - \rho(K-E)$ n'est pas disjoint des supports de $\rho(k\,\iota(E) - kP_\infty)$ pour tout $1 \leq k \leq n$, il faut travailler dans le corps de fonctions de la courbe.

Soit k un corps et soit $\mathcal{E}$ la courbe elliptique $y^2 = x(x-1)(x-\lambda)$ où $\lambda \in k$. Supposons numérotées les racines dans l'ordre suivant $\{0, \lambda, 1\}$. Si k se plonge dans $\mathbb{C}$, nous avons que $\mathcal{E}(\mathbb{C}) \simeq \mathbb{C}/\left(\omega\mathbb{Z} + \mathbb{Z}\right)$ avec ω dans le demi-plan de Poincaré $\mathcal{H}_1$. Nous pouvons supposer que le point $(0,0)$ s'envoie sur le point $\omega/2$, le point $(1,0)$ sur $1/2$ et le point $(\lambda, 0)$ sur $\omega/2 + 1/2$.

Supposons que notre corps n'est pas canoniquement plongé dans $\mathbb{C}$. Dans le cas des niveaux impairs, nous pouvons choisir n'importe quelle base symplectique de la n-torsion de $\mathbb{C}/\omega\mathbb{Z} + \mathbb{Z}$ pour l'image d'une base symplectique de la n-torsion de la courbe. Dans le cas des niveaux pairs, nous ne pouvons pas faire un choix quelconque. En effet, nous avons déjà fixé l'image des points de 2-torsion et le choix doit être compatible. Si le corps de base vient avec un plongement dans $\mathbb{C}$, il faut rajouter les conditions sur le couplage de Weil (page 31). En effet, la valeur du couplage de Weil de points de la base symplectique doit correspondre à la racine de l'unité $\exp(2i\pi/n)$.

Dans le cas des niveaux (n,n) pairs, le groupe Γ_n fixe les puissances n-ièmes des thêta constantes mais seul $\Gamma_{n,2n}$ fixe leurs puissances $2n$-ièmes. De ce fait, il est possible de prendre certaines racines carrées (voir la section 6.2).

Formules pour $n = 3$

Les formules pour le niveau 3 et le genre 1 ont été déjà obtenues par Thomae [Tho73] en utilisant a priori une méthode différente. Soit $P_3 = (x_3, y_3)$ un point générique de 3-torsion. La coordonnée x_3 est racine du polynôme :

$$3X^4 - 4(\lambda+1)X^3 + 6\lambda X^2 - \lambda^2.$$

Comme 2 et 3 sont premiers entre eux, nous pouvons supposer que P_3 s'envoie sur n'importe quel point de 3-torsion du tore $\mathbb{C}/\left(\omega\mathbb{Z} + \mathbb{Z}\right)$ quitte à modifier ω par l'action de $\mathrm{Sp}(2,\mathbb{Z})$. Supposons par exemple que P_3 s'envoie sur le point $\omega/3$. Nous avons alors les thêta constantes suivantes correspondant à P_3 et $2P_3$:

$$\begin{aligned}
\left(\frac{\theta\left[\begin{smallmatrix}1/3\\0\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \frac{3}{4}x_3^2 - \left(\lambda + \frac{1}{4}\right)x_3 + \frac{\lambda}{2} = \left(\frac{\lambda(\lambda-1)}{3x_3^2 + 2(\lambda-2)x_3 - \lambda}\right)^2 \\
\left(\frac{\theta\left[\begin{smallmatrix}2/3\\0\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \left(\frac{\theta\left[\begin{smallmatrix}1/3\\0\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6.
\end{aligned}$$

Soit $Q_3 = (x_3', y_3')$ un autre point de 3-torsion tel que le couplage de Weil $e_3(P_3, Q_3)$ soit une racine primitive 3-ième de l'unité. Si le corps est canoniquement plongé dans $\mathbb{C}$, il faut supposer également que cette racine est $\exp(2i\pi/3)$. La coordonnée x_3' du point Q_3 est une racine du polynôme :

$$\begin{aligned}
&(\lambda-1)X^3 - \left(3x_3^3 - (4\lambda+1)x_3^2 + (2\lambda-1)x_3 + (5\lambda-4)\right)X^2 \\
&+ \left(6x_3^3 - 5(\lambda+1)x_3^2 - 2(2\lambda-1)(\lambda-2)x_3 + 2\lambda(2\lambda-1)\right)X - \left(3x_3^3 - (\lambda+4)x_3^2 - \lambda(\lambda-2)x_3 + \lambda^2\right).
\end{aligned}$$

Nous avons alors

$$\begin{aligned}
\left(\frac{\theta\left[\begin{smallmatrix}0\\1/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \frac{3}{4}x_3'^2 - \left(\lambda+\frac{1}{4}\right)x_3' + \frac{\lambda}{2} = \left(\frac{\lambda(\lambda-1)}{3x_3'^2+2(\lambda-2)x_3'-\lambda}\right)^2,\\
\left(\frac{\theta\left[\begin{smallmatrix}0\\2/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \left(\frac{\theta\left[\begin{smallmatrix}0\\1/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6,\\
\left(\frac{\theta\left[\begin{smallmatrix}1/3\\1/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \Big(\big(9(2\lambda-1)x_3^2x_3'^2 - 6(4\lambda^2-\lambda+1)(x_3+x_3')x_3x_3' + 4(8\lambda^3-9\lambda+8)x_3x_3'\\
&\qquad -4(\lambda-2)(4\lambda^2+3\lambda-4)(x_3+x_3') + \lambda(38\lambda^2-65\lambda+32)\big)\frac{y_3y_3'}{16\lambda^2(\lambda-1)^2}\\
&\qquad +\frac{3}{8}(x_3^2+x_3'^2) - \frac{4\lambda+1}{8}(x_3+x_3') + \frac{\lambda-1}{2}\Big)\exp\left(\frac{2i\pi}{3}\right),\\
\left(\frac{\theta\left[\begin{smallmatrix}2/3\\2/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \left(\frac{\theta\left[\begin{smallmatrix}1/3\\1/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6,\\
\left(\frac{\theta\left[\begin{smallmatrix}1/3\\2/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \Big(\big(9(2\lambda-1)x_3^2x_3'^2 - 6(4\lambda^2-\lambda+1)(x_3+x_3')x_3x_3' + 4(8\lambda^3-9\lambda+8)x_3x_3'\\
&\qquad -4(\lambda-2)(4\lambda^2+3\lambda-4)(x_3+x_3') + \lambda(38\lambda^2-65\lambda+32)\big)\frac{y_3y_3'}{16\lambda^2(\lambda-1)^2}\\
&\qquad -\frac{3}{8}(x_3^2+x_3'^2) + \frac{4\lambda+1}{8}(x_3+x_3') - \frac{\lambda-1}{2}\Big)\exp\left(\frac{2i\pi}{3}\right),\\
\left(\frac{\theta\left[\begin{smallmatrix}2/3\\1/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6 &= \left(\frac{\theta\left[\begin{smallmatrix}1/3\\2/3\end{smallmatrix}\right](0,\omega)}{\theta(0,\omega)}\right)^6.
\end{aligned}$$

6.1.3 Niveau $(2,2)$ pour le genre g

Soit e une caractéristique de niveau $(2,2)$. Nous pouvons écrire $e = \eta_{\mathcal{U}\circ S}$ où $S \subset \{1,\dots,2g+1\}$. De plus nous pouvons faire l'hypothèse que le cardinal de S est congru à $g+1$ modulo 2. Nous cherchons alors une fraction rationnelle R ayant pour diviseur

$$2\,\mathrm{T}_{\sum_{l\in\mathcal{U}\circ S}(a_l,0)-\#(\mathcal{U}\circ S)P_\infty}\,\Theta - 2\Theta$$

et nous voulons évaluer R en les deux points

$$K = \sum_{l\in\mathcal{U}}(a_l,0) - (g+1)P_\infty, \qquad K-E = \sum_{l\in S}(a_l,0) - (\#S)P_\infty.$$

Nous savons que K n'est pas un diviseur thêta. Par ailleurs K n'appartient pas à

$$\mathrm{T}_{\sum_{l\in\mathcal{U}\circ S}(a_l,0)-\#(\mathcal{U}\circ S)P_\infty}\,\Theta$$

si et seulement si S est de cardinal $g+1$. De même, $K-E$ n'appartient jamais à ce dernier diviseur et ce n'est pas un diviseur thêta si et seulement si S est de cardinal $g+1$. Quand S n'est pas de cardinal $g+1$, nous avons alors que $R(K;0)=0$ et $R(K-E;0)=\infty$ et donc le quotient des deux est nul.

Supposons maintenant que S soit de cardinal $g+1$. D'après la section 5.1.3, la fonction suivante

répond aux conditions imposées sur R

$$\phi^* R = \frac{1}{\prod_{l\in\mathcal{U}\circ S} u(a_l)} \left(\sum_{\substack{I\subset\{1,\dots,g\} \\ \#I=\lfloor \frac{\#(\mathcal{U}\circ S)}{2} \rfloor}} \prod_{i\in I} y_i \prod_{\substack{k=1 \\ k\notin I}}^{g} \frac{\prod_{l\in\mathcal{U}\circ S}(x_k - a_l)}{\prod_{i\in I}(x_i - x_k)} \right)^2$$

où les produits sont égaux à 1 si l'ensemble sur lequel nous les prenons est vide. Notons que ce résultat serait faux si nous avions pris S de cardinal non congru à $g+1$ modulo 2 (en particulier pour les S tels que $\mathcal{U}\circ S = \{l\}$ est de cardinal 1, le diviseur de la fonction précédente est $2\Theta - 2\,\mathrm{T}_{(a_l,0)-P_\infty}\,\Theta$).

En procédant de la même façon que dans la preuve du lemme 5.1.37, nous obtenons

$$\begin{aligned} R(K) &= \prod_{l\in S\setminus\mathcal{U}} \prod_{m\in\mathcal{U}\cap S} (a_l - a_m) \prod_{k\in(\mathcal{U}\cup S)^c} \prod_{l\in\mathcal{U}\setminus S} (a_k - a_l)(-1)^{g\#(\mathcal{U}\circ S)}(-1)^{\#(U\cup S)^c\#(S\setminus\mathcal{U})}, \\ R(K-E) &= \prod_{l\in\mathcal{U}\setminus S} \prod_{m\in\mathcal{U}\cap S} (a_l - a_m) \prod_{k\in(\mathcal{U}\cup S)^c} \prod_{l\in S\setminus\mathcal{U}} (a_k - a_l)(-1)^{g\#(\mathcal{U}\circ S)}(-1)^{\#(U\cup S)^c\#(\mathcal{U}\setminus S)}. \end{aligned}$$

Par ailleurs, le facteur exponentiel est trivial. Nous avons alors redémontré le théorème

Théorème 6.1.3 (Thomae)**.** *Soit $\mathcal{C}:\ y^2 = \prod_{i=1}^{2g+1}(x-a_i)$, une courbe hyperelliptique de genre g et soit S un sous-ensemble de $\{1,\dots,2g+1\}$, alors*

$$\left(\frac{\theta\left[\eta_{\mathcal{U}\circ S}\right]}{\theta[0]}\right)^4 = \begin{cases} (-1)^{\#(\mathcal{U}\setminus S)} \dfrac{\prod_{\substack{i\in\mathcal{U} \\ j\notin\mathcal{U}}} (a_i - a_j)}{\prod_{\substack{i\in S \\ j\notin S}} (a_i - a_j)} & \text{si } \#S \in \{g, g+1\}, \\ 0 & \text{sinon.} \end{cases}$$

6.2 Extraction de racines

La formule de Thomae permet d'obtenir les carrés des thêta constantes de niveau 2 de la famille $\mathscr{F}_{(2,2)^2}$ et les puissances 4-ièmes de celles de niveau $(2,2)$ de la famille $\mathscr{F}_{(2,2)}$. En pratique, nous avons besoin d'avoir ces thêta constantes et non pas leur puissance, il faut donc extraire les racines. Sur le corps des complexes, il suffit d'évaluer la somme d'exponentielles numériquement pour savoir quelle racine choisir. Cela n'est bien sûr pas possible sur un corps quelconque.

Les thêta constantes sont indicées par $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ et nous notons $(e_1,\dots,e_{2g})$ la base canonique de cet espace. Nous nous autorisons à changer le plongement par un isomorphisme qui préserve les puissances quatrièmes des thêta constantes. Nous devons étudier l'action du groupe $\mathrm{Sp}(2g,\mathbb{Z})$ sur les thêta constantes de niveau $(2,2)$ et leurs puissances. Pour qu'un élément γ de $\mathrm{Sp}(2g,\mathbb{Z})$ préserve les caractéristiques des thêta, il faut que $\gamma \equiv \mathrm{Id}_{2g} \mod 2$ et donc γ doit appartenir à Γ_2. Rappelons le lemme 3.1.28 :

Lemme 6.2.1. *Soient a,b dans $\frac{1}{2}\mathbb{Z}^g$ et soit $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ une matrice de Γ_2, alors*

$$\begin{aligned} \frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\gamma.\Omega)} &= \frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\Omega)} \exp\left(\pi i\, {}^t a A\, {}^t B a\right) \exp\left(-\pi i\, {}^t b C\, {}^t D b\right) \exp\left(-2\pi i\, {}^t a\,(A - \mathrm{Id})\, b\right), \\ \left(\frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\gamma.\Omega)}\right)^2 &= \left(\frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\Omega)}\right)^2 (-1)^{2\,{}^t a A\, {}^t B a}(-1)^{2\,{}^t b C\, {}^t D b}, \\ \left(\frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\gamma.\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\gamma.\Omega)}\right)^4 &= \left(\frac{\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\Omega)}\right)^4. \end{aligned}$$

Ce lemme montre que Γ_2 fixe les puissances quatrièmes des thêta constantes et $\Gamma_{2,4}$ leurs carrés (rappelons que les matrices $A\,{}^t B$ et $C\,{}^t D$ sont symétriques).

Pour obtenir les carrés des thêta constantes, nous pouvons prendre des racines carrées arbitraires à condition que cette opération corresponde à un isomorphisme défini par une classe de $\Gamma_{2,4}\backslash\Gamma_2$. Nous voyons donc que nous pouvons prendre des racines carrées arbitraires pour toutes les thêta constantes

de caractéristique e_i (où les e_i forment une base de $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$). Une fois cela fait, les carrés de toutes les thêta constantes sont fixés par les isomorphismes.
Supposons prises les racines carrées pour toutes les thêta de caractéristique e_i. En genre 1, nous obtenons les thêta constantes de niveau 2 de la famille $\mathscr{F}_{(2,2)^2}$. En genre 2, les carrés des autres thêta constantes peuvent se calculer grâce aux formules suivantes : soit

$$\mathcal{C}:\ y^2=\prod_{i=1}^{5}(x-a_i)$$

une courbe hyperelliptique de genre 2 de matrice de période Ω. Nous utilisons la formule de Thomae inverse 3.1.20 pour obtenir

$$\frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right]^2}=\frac{a_1-a_5}{a_1-a_2},\qquad \frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(0\ \frac{1}{2})\\ {}^t(0\ 0)\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ \frac{1}{2})\\ {}^t(0\ 0)\end{smallmatrix}\right]^2}=\frac{a_1-a_3}{a_1-a_2},$$

$$\frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right]^2}=-\frac{a_2-a_5}{a_2-a_1},\qquad \frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(0\ \frac{1}{2})\\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ \frac{1}{2})\\ {}^t(0\ 0)\end{smallmatrix}\right]^2}=-\frac{a_2-a_3}{a_2-a_1},$$

$$\frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ \frac{1}{2})\\ {}^t(0\ 0)\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right]^2\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ \frac{1}{2})\\ {}^t(\frac{1}{2}\ \frac{1}{2})\end{smallmatrix}\right]^2}=\frac{a_5-a_2}{a_5-a_4}.$$

L'exemple 6.2.2 donne des formules plus lisibles mais est dans le cas particulier où la courbe est sous forme de Rosenhain. En genre supérieur à 3, nous n'avons pas réussi à trouver une expression donnant les carrés des autres thêta constantes en fonction des racines de f et des carrés des thêta constantes correspondant aux e_i.

Une fois obtenus ces carrés des thêta constantes, nous voulons encore une fois extraire les racines pour obtenir les valeurs des thêta constantes de niveau $(2,2)$. Pour ce faire, nous pouvons prendre un isomorphisme correspondant au choix d'une classe de $\tilde{\Gamma}_{4,8}\backslash\tilde{\Gamma}_{2,4}$. En effet $\tilde{\Gamma}_{2,4}=\Gamma_{2,4}$ laisse fixes les carrés des thêta constantes tandis que $\tilde{\Gamma}_{4,8}$ laisse fixes les thêta constantes elles-mêmes.

Rappelons que les thêta constantes $\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](0,\Omega)$ sont nulles si $(-1)^{4\,{}^tab}=0$. Nous voyons qu'en genre 1 et 2, pour chaque thêta constante non nulle, il existe une matrice γ de $\tilde{\Gamma}_{2,4}$ qui change son signe mais laisse fixe les autres thêta constantes. De ce fait, les racines peuvent être prises de manière arbitraire, un autre choix correspondant à une variété isomorphe.

Exemple 6.2.2. *Soit $\mathcal{C}:\ y^2=x(x-1)(x-\lambda)(x-\mu)(x-\nu)$ une courbe hyperelliptique sous forme de Rosenhain. Choisissons l'ordre suivant $\{0,1,\lambda,\mu,\nu\}$ sur les points de ramifications. Les formules de Thomae donnent*

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(\frac{1}{2}\ 0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]}\right)^4=\frac{\mu(\lambda-1)(\nu-1)}{\lambda\nu(\mu-1)},\qquad \left(\frac{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ \frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]}\right)^4=\frac{\mu(\lambda-1)(\nu-\mu)}{\lambda(\mu-1)(\nu-\lambda)},$$

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]}\right)^4=\frac{\mu}{\lambda\nu},\qquad \left(\frac{\theta\left[\begin{smallmatrix}{}^t(0\ \frac{1}{2})\\ {}^t(0\ 0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0\ 0)\\ {}^t(0\ 0)\end{smallmatrix}\right]}\right)^4=\frac{\mu(\lambda-\mu)(\nu-1)}{\nu(\mu-1)(\lambda-\nu)}.$$

Nous pouvons prendre des racines carrées arbitraires de ces expressions. Les carrés des autres thêta

constantes de niveau $(2,2)$ *non nulles sont alors donnés par*

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&\frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2 = \frac{1}{\nu}\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&\frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2,$$

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&\frac{1}{2})\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2 = \frac{1}{\lambda}\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&\frac{1}{2})\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2,$$

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(\frac{1}{2}&\frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2 = (\nu-1)\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&\frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(\frac{1}{2}&\frac{1}{2})\end{smallmatrix}\right]}\right)^2,$$

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&\frac{1}{2})\\{}^t(\frac{1}{2}&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2 = (\lambda-1)\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&\frac{1}{2})\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2,$$

$$\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&\frac{1}{2})\\{}^t(\frac{1}{2}&\frac{1}{2})\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2 = \frac{\nu-\mu}{\nu-1}\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(\frac{1}{2}&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(\frac{1}{2}&\frac{1}{2})\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}\right)^2\left(\frac{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&0)\end{smallmatrix}\right]}{\theta\left[\begin{smallmatrix}{}^t(0&0)\\{}^t(0&\frac{1}{2})\end{smallmatrix}\right]}\right)^2$$

et nous pouvons encore prendre des racines carrées arbitraires de toutes ces thêta constantes.

6.3 Passage par les fonctions thêta de niveau $(2,2)$

Cas des niveaux $2n$ avec n impair

Soit n un nombre impair, nous allons chercher à calculer les thêta constantes de niveau $2n$ de la famille $\mathscr{F}_{(2n,2n)^{2n}}$ et pour cela, nous allons utiliser les fonctions thêta de niveau $(2,2)$ de la base $\mathscr{F}_{(2,2)}$:

$$[\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z,\Omega)]_{a,b} \qquad \text{où } a,b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g.$$

Nous verrons ensuite comment calculer les thêta constantes de niveau n quelconque.

Remarque 6.3.1. *Nous pourrions vouloir utiliser les fonctions de niveau* 2 *de la famille* $\mathscr{F}_{(2,2)^2}$*. Ceci est possible quand le genre est* 1 *ou* 2*. Cependant, comme nous travaillons avec des courbes hyperelliptiques, dès le genre* 3*, certaines thêta constantes paires sont nulles. Dans ce cas, nous ne pouvons alors pas utiliser les thêta constantes de niveau* 2*.*

Comme les thêta constantes de la famille $\mathscr{F}_{(2n,2n)^{2n}}$ déterminent la $2n$-torsion, nous devons supposer connus les points de n-torsion sur la jacobienne de la courbe. Nous utilisons les morphismes (chapitre 5) pour calculer les coordonnées de ces points avec les fonctions thêta de niveau 4. C'est à dire que nous supposons connus (à un facteur projectif près) les points affines suivants : pour tous α, β dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\widetilde{P}_{\alpha,\beta} := [\lambda_{\alpha,\beta}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2(\Omega\alpha+\beta),\Omega)]_{a,b} \qquad \text{où } a,b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g.$$

Comme n est impair, nous pouvons utiliser la méthode de la page 64 pour calculer

$$\left(\exp\left(-4\pi i\,{}^t\alpha\Omega\alpha\right)\frac{\lambda_{\alpha,\beta}}{\lambda_{0,0}}\right)^n$$

en lien avec la puissance n-ième du facteur projectif $\lambda_{\alpha,\beta}$ associé au vecteur complexe $\Omega\alpha+\beta$. De ce fait, avec l'équation 3.2, nous obtenons la valeur exacte de

$$\frac{\left(\theta\left[\begin{smallmatrix}a+2\alpha\\b+2\beta\end{smallmatrix}\right](0,\Omega)\right)^n}{\left(\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)\right)^n} = \frac{\left(\lambda_{\alpha,\beta}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2(\Omega\alpha+\beta),\Omega)\right)^n}{\left(\lambda_{0,0}\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)\right)^n}\left(\frac{\lambda_{0,0}}{\lambda_{\alpha,\beta}}\exp\left(4\pi i\,{}^t\alpha\Omega\alpha\right)\right)^n\exp\left(2\pi i4n\,{}^t\alpha\beta\right). \qquad (6.1)$$

Algorithme 19 Calcul des thêta constantes de niveau $2n$

Entrée: Une courbe hyperelliptique $\mathcal{C}$ de genre g quelconque. Un entier n impair.

Sortie: Les thêta constantes de niveau $2n$ de la famille $\mathscr{F}_{(2n,2n)^{2n}}$ associées à la courbe. {Cet algorithme donne également les thêta constantes de niveau n. Par ailleurs, en utilisant les formules de changement de bases, il est possible d'obtenir celles des autres bases de niveau n ou $2n$.}

1: Calculer les thêta constantes $\mathscr{F}_{(2,2)}$ par les formulaires de Thomae et extraction des racines.
2: Caluler les coordonnées des points de n-torsion sur la courbe $\mathcal{C}$.
3: Utiliser les morphismes (chapitre 5) pour calculer les coordonnées de ces points avec les fonctions thêta de niveau 4 de la base $\mathscr{F}_{(2,2)}$.
4: Calculer la puissance n-ième des facteurs projectifs : les points de n-torsion pouvant s'écrire

$$[\lambda_{\alpha,\beta}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2(\Omega\alpha+\beta),\Omega)]_{a,b} \qquad \text{où } a,b\in\tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g,$$

et le facteur $\lambda^n_{\alpha,\beta}$ peut se calculer par l'équation 3.34.
5: Utiliser l'équation 6.1 pour caluler

$$\frac{\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)\right)^n}{\left(\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)\right)^n}, \qquad \forall a,b\in\tfrac{1}{2n}\mathbb{Z}^g/\mathbb{Z}^g.$$

6: **return** le carré des expressions précédentes.

Nous procédons de la même façon pour tous les points de n-torsion. Comme n est impair, les $a+2\alpha$ et les $b+2\beta$ génèrent toutes les classes de $\frac{1}{2n}\mathbb{Z}^g/\mathbb{Z}^g$. Nous obtenons donc toutes les thêta constantes des familles $\mathscr{F}_{(n,n)^n}$ et $\mathscr{F}_{(2n,2n)^{2n}}$

$$\mathscr{F}_{(n,n)^n}: \qquad \left[\frac{\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)\right)^n}{\left(\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)\right)^n}\right]_{a,b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g},$$

$$\mathscr{F}_{(2n,2n)^{2n}}: \qquad \left[\frac{\left(\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)\right)^{2n}}{\left(\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)\right)^{2n}}\right]_{a,b\in\frac{1}{2n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Cette méthode est résumée dans l'algorithme 19.

Il existe une variante à cette méthode. Soit $(e_1,\dots,e_{2g})$ une base de la n-torsion, nous pouvons calculer les puissances n-ièmes des facteurs projectifs pour les points de l'ensemble

$$\{e_i,\ 1\le i\le 2g\}\cup\{e_i+e_j,\ 1\le i<j\le 2g\}$$

et ensuite utiliser les additions différentielles pour calculer les coordonnées « exactes » de niveau $(2,2)$ des autres points de n-torsion. En procédant ainsi, nous faisons moins de calculs.

Cas général

Si n est pair, deux problèmes se présentent. Le premier est que nous ne pouvons calculer que les puissances $2n$-ièmes des facteurs projectifs. Le deuxième est que les $a+2\alpha$ et les $b+2\beta$ ne génèrent que $\frac{1}{n/2}\mathbb{Z}^g/\mathbb{Z}^g$ et non plus $\frac{1}{2n}\mathbb{Z}^g/\mathbb{Z}^g$. Il faut alors utiliser la $2n$-torsion et ceci ne permet d'obtenir que les puissances quatrièmes des thêta constantes de niveau n de la base $\mathscr{F}_{(n,n)^n}$.

Remarque 6.3.2. *Si nous sommes en genre* 1 *ou* 2*, nous pouvons utiliser les fonctions de niveau* 2 *de la famille* $\mathscr{F}_{(2,2)}$*. Dans ce cas, nous obtenons les carrés des thêta constantes de niveau* n *de la base* $\mathscr{F}_{(n,n)^n}$*.*

Comparaison avec la méthode analytique

L'avantage de cette méthode par rapport à celle de la section 6.1, est que, si n est impair, nous obtenons directement les thêta constantes de niveau n ou $2n$ et non leurs carrés. Quand n est pair, nous obtenons les carrés des thêta constantes comme dans le cas analytique.

Quand n est impair, nous calculons cependant des thêta constantes de niveau trop élevé dont nous n'avons pas besoin pour avoir les thêta constantes de niveau 2. Par ailleurs, pour les formules de Thomae classiques et pour les morphismes, il faut commencer l'algorithme par prendre une extension de corps où au moins toute la 2-torsion est rationnelle. De plus, l'utilisation des morphismes du chapitre 5 rend cette méthode trop lente pour des courbes sur des corps différents des corps finis.

Nous avons programmé cette méthode en utilisant les fonctionnalités de AVIsogenies. Nous avons ainsi pu retrouver les formules obtenues à la section 6.1.2 dans le cas des courbes elliptiques en spécialisant ces dernières pour des courbes particulières sur des corps finis.

Cas des fonctions de niveau $(2n, 2n)$

Nous nous intéressons maintenant aux thêta constantes de niveau $(2n)^2$. C'est-à-dire que nous voulons connaître le vecteur projectif

$$[\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] (0, \Omega)]_{a,b} \qquad \text{où } a, b \in \tfrac{1}{2n}\mathbb{Z}^g/\mathbb{Z}^g$$

Il serait donc intéressant de savoir extraire les racines n-ièmes des facteurs projectifs calculés précédemment. Supposons que $(e_1, \ldots, e_{2g})$ est une base symplectique de la n-torsion. Nous étudions maintenant l'action du groupe $\tilde{\Gamma}_{2,4}\backslash\tilde{\Gamma}_{n,2n}$ qui préserve les puissances n-ièmes des facteurs projectifs et les thêta constantes de la base $\mathscr{F}_{(2,2)}$. Nous voyons que nous pouvons extraire les racines n-ièmes des facteurs projectifs correspondant au points e_i et aux points $e_i + e_j$ pour $i < j$ et $j \neq i + g$. Il reste donc g puissances n-ièmes à extraire correspondant aux points $e_i + e_{i+g}$.

Si nous savions le faire, nous pourrions utiliser les additions différentielles pour obtenir les facteurs projectifs de tous les points de n-torsion. Cette méthode permettrait d'accélérer grandement les calculs dans le cas des niveaux n divisibles par des carrés.

Chapitre 7

Calcul d'isogénies

Nous avons défini les isogénies dans la section 2.1.2. Ce sont des morphismes entre variétés abéliennes et elles ont beaucoup d'applications (voir la partie 1.2) :

- transfert du logarithme discret,
- comptage de points,
- calcul de polynômes de classes,
- calcul de polynômes modulaires,
- calcul du relevé canonique de la variété,
- calcul des anneaux d'endomorphismes...

Il existe différents problèmes de « calcul d'isogénies ».

1. Étant donné un sous-groupe isotrope maximal de la ℓ-torsion, calculer la variété isogène associée.
2. Calculer toutes les variétés isogènes à une variété donnée.
3. Calculer l'image d'un point par une isogénie.
4. Étant données deux variétés isogènes, calculer l'isogénie allant de l'une à l'autre.

Le second problème peut être résolu grâce aux polynômes modulaires. Les invariants des variétés isogènes s'obtenant comme les zéros de certains polynômes. Clairement, le premier problème permet de résoudre le second car nous disposons d'algorithmes efficaces permettant de calculer les sous-groupes de ℓ-torsion.

Dans les deux premiers problèmes, nous nous autorisons à ne pas avoir les équations définissant l'isogénie. Par exemple nous pouvons demander de calculer uniquement des invariants associés aux variétés. Cependant, dans le premier problème, nous pouvons également demander de calculer l'image d'un point par l'isogénie.

Les variétés initiales et finales peuvent être données de différentes façons :

1. Thêta constantes de niveau n (voir le chapitre 3).
2. Dans le cas où la variété est la jacobienne d'une courbe, par l'équation de Weierstrass de la courbe.

De même le sous-groupe du premier problème peut être défini par

1. une base du sous-groupe en coordonnées thêta de niveau n (ou en coordonnées de Mumford si nous sommes dans le cas d'une jacobienne d'une courbe hyperelliptique),
2. un système d'équations rationnelles définissant le sous-groupe.

Dans ce chapitre, nous supposons données les thêta constantes d'une première variété et une description d'un noyau d'une isogénie. Nous allons calculer alors les thêta constantes de la deuxième variété. Par ailleurs nous expliquons comment calculer l'image d'un point.

Nous nous plaçons en caractéristique différente de 2. Par ailleurs, nous nous intéressons au calcul de d-isogénies séparables étant donnés leurs noyaux. Rappelons qu'elles sont de degré d^g, que leur noyau est un sous-groupe isotrope maximal de la d-torsion qui est isomorphe à $(\mathbb{Z}/d\mathbb{Z})^g$.

Les d qui nous intéressent sont 2 et les nombres premiers impairs différents de la caractéristique du corps. En effet d'après 2.1.2, cela suffit pour calculer des d-isogénies séparables quelconques.

Pour les courbes elliptiques, nous disposons d'algorithmes efficaces pour calculer des isogénies. Ces algorithmes sont principalement basés sur les formules de Vélu [Vél71] ou sur les polynômes modulaires [Sch95, Elk98].

Pour le genre supérieur, les formules de Richelot [Ric36, Ric37], permettent de calculer des $(2,2)$-isogénies entre jacobiennes de courbes hyperelliptiques de genre 2. Plus précisément, étant donnée une courbe de genre 2 d'équation $y^2 = p_1p_2p_3$ avec p_i des polynômes de degré 2, les formules de Richelot permettent de calculer une équation similaire pour la courbe isogène.

Smith [Smi09] donne un algorithme pour calculer des $(2,2,2)$-isogénies pour des jacobiennes de courbes de genre 3. Il utilise ces isogénies pour attaquer le logarithme discret dans les jacobiennes de courbes hyperelliptiques en se ramenant à la jacobienne d'une courbe non-hyperelliptique.

Pour les isogénies de degré différent de 2, l'article [DL08] décrit une méthode permettant le calcul de l'équation des courbes hyperelliptiques $(3,3)$-isogènes à une courbe hyperelliptique de genre 2. Toujours en genre 2, l'article [BGL09] explique comment calculer des graphes de $(3,3)$-isogénies en genre 2 mais ne donne pas la forme explicite de l'isogénie. Les auteurs utilisent entre autre les thêta constantes de niveau 4.

Dans ce chapitre, ℓ désigne un nombre premier impair différent de la caractéristique du corps.

Dans une première section, nous décrivons le travail de Lubicz et Robert [LR10a] qui expliquent comment calculer des ℓ-isogénies en changeant de niveau. Nous donnons alors une formule de changement de niveau et son utilisation pour calculer des ℓ-isogénies. Dans la section 7.3, nous présentons le calcul de 2-isogénies et finalement, nous portons une attention particulière aux courbes hyperelliptiques de genre 2 dans la section 7.4. Ce chapitre repose sur un travail commun avec Damien Robert [CR11].

Nous utilisons exclusivement les fonctions thêta de la base $\mathscr{F}_n$. Pour plus de clarté, nous précisons la variété correspondante en exposant des différentes fonctions thêta.

7.1 Calcul de ℓ-isogénies en changeant de niveaux

Lubicz et Robert [LR10a], expliquent comment prendre des ℓ-isogénies entre variétés abéliennes avec les fonctions thêta de niveaux n et $n\ell$. Notons que, utilisée seule, cette méthode ne permet pas de rester en un niveau n fixé ce qui empêche le calcul de ℓ-isogénies entre jacobiennes de courbes (c'est-à-dire si nous voulons retrouver l'équation de Weierstraß de la courbe isogène).

Les théorèmes présentés dans cette section sont la traduction des isogénies suivantes entre tores :

$$\begin{array}{ccc} A = \mathbb{C}^g/\frac{\Omega}{\ell}\mathbb{Z}^g + \mathbb{Z}^g & \longrightarrow & B = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g \\ z & \longmapsto & \ell z \\ z & \longleftarrow & z. \end{array}$$

Le noyau de la première isogénie est $\left\{\beta,\ \beta \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\right\}$; celui de la seconde est $\left\{\Omega\alpha,\ \alpha \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\right\}$.

7.1.1 En descendant de niveau

L'idée de Lubicz et Robert repose sur le fait qu'en « oubliant » des coordonnées, nous pouvons prendre l'isogénie de B vers A en descendant de niveau.

Théorème 7.1.1. *Soit $B = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$ une variété abélienne donnée par ses thêta constantes de niveau $n\ell$. Soit $A = \mathbb{C}^g/\frac{\Omega}{\ell}\mathbb{Z}^g + \mathbb{Z}^g$, les thêta constantes de niveau n de la variété A sont données par*

$$\left(\theta^A \left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right]\left(0, \frac{\Omega/\ell}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left(\theta^B \left[\begin{smallmatrix}0\\ b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)\right)_{b'\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$$

Au niveau des points, cette isogénie se traduit de la façon suivante :

$$\left(\theta^A \left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega/\ell}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g} = \left(\theta^B \left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(z, \frac{\Omega}{n\ell}\right)\right)_{b'\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

Partant d'une variété, il n'est pas possible par cette méthode de prendre autant d'isogénies que voulu car le niveau est un entier positif et il ne peut donc décroître infiniment. Lubicz et Robert ont expliqué comment prendre l'isogénie duale qui permet de passer du niveau n au niveau $n\ell$.

7.1.2 Calcul de l'isogénie duale (en montant de niveau)

Comme les thêta constantes de niveau $n\ell$ fixent la ℓ-torsion, toute la ℓ-torsion sur la variété B est rationnelle. Par l'isogénie π, une partie de cette ℓ-torsion est connue sur la variété A. Supposons donc connues les thêta constantes de niveau n associées à la variété A ainsi que l'image des points de $\frac{1}{\ell}\mathbb{Z}^g$ par les fonctions thêta de niveau n sur A. C'est-à-dire que nous supposons connues toutes valeurs suivantes

$$\theta^A \left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\Omega/\ell}{n}\right)$$

où b appartient à un système de représentants de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ et où β est un élément de $\frac{1}{\ell}\mathbb{Z}^g$. Nous pouvons alors retrouver les thêta constantes de B : pour b dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ et β dans $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\theta^B \left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right) = \theta^A \left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\Omega}{n\ell}\right).$$

Cependant, en pratique, toutes ces fonctions thêta ne sont pas connues. En effet, ce qui peut être connu ce sont les images de points de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ par l'application

$$\begin{array}{ccc} \mathbb{C}^g & \longrightarrow & \mathbb{P}^{n^g-1}(\mathbb{C}) \\ z & \longmapsto & \left(\theta^A \left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega/\ell}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}. \end{array}$$

Les facteurs projectifs sont différents pour chaque point de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$. Il faut donc une méthode permettant de retrouver ces facteurs de sorte à rendre les fonctions thêta « compatibles » pour obtenir l'équation de B. La méthode proposée par Lubicz et Robert, que nous allons présenter, consiste à retrouver les puissances ℓ-ièmes de ces facteurs pour un certain nombre de points de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$, d'extraire les racines, et d'obtenir les facteurs projectifs des autres points par des formules d'additions différentielles.

Supposons que ℓ soit premier à $2n$ et utilisons la méthode de la page 62 pour récupérer les puissances ℓ-ièmes des facteurs projectifs des points de l'ensemble

$$S = \{e_i,\ i \in \{1,\dots,g\}\} \cup \{e_i + e_j,\ i \neq j \in \{1,\dots,g\}\}$$

où les e_i forment une base $\frac{1}{\ell}\mathbb{Z}^g$. Il faut extraire les racines ℓ-ièmes des facteurs projectifs. Pour cela nous nous reposons sur la propriété

Propriété 7.1.2. *Soient deux entiers n et ℓ avec n pair et ℓ premier à n. Soit une matrice $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ de $\mathrm{Sp}(2g,\mathbb{Z})$ telle que*

$$B \equiv 0 \mod n\ell, \quad A \equiv D \equiv \mathrm{Id} \mod n\ell, \quad \mathrm{diag}\left({}^tDB\right) \equiv 0 \mod 2n\ell,$$

$$C \equiv 0 \mod n, \quad \mathrm{diag}\left(C\,{}^tD\right) \equiv 0 \mod 2n.$$

Alors pour tout $b \in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ *et tout* $\beta \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \exp(-\pi i \ell\, {}^t\beta C\, {}^tD\beta)^n,$$

$$\left(\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)}\right)^{\ell} = \left(\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}\right)^{\ell}.$$

En particulier,

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}.$$

Démonstration. D'après les hypothèses sur γ,

$$\gamma' = \begin{pmatrix} A & B/n\ell \\ n\ell C & D \end{pmatrix}$$

appartient à $\Gamma_{1,2}$. De plus nous avons $\frac{\gamma.\Omega}{n\ell} = \gamma'.\left(\frac{\Omega}{n\ell}\right)$. En utilisant la proposition 3.1.24, nous obtenons

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} = \frac{\theta\left[\begin{smallmatrix}n\ell\, {}^tCb\\ {}^tDb\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \exp\left(-\pi i\, {}^tbn\ell C\, {}^tDb\right).$$

La matrice $C\,{}^tD$ est symétrique, congrue à 0 modulo n et de diagonale congrue à 0 modulo $2n$. De ce fait $n\,{}^tbC\,{}^tDb$ est un entier pair pour tout b dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$. Le facteur exponentiel est donc trivial. Par ailleurs, avec les formules 3.1.2 nous obtenons

$$\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} = \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}.$$

Par le même raisonnement, nous avons

$$\begin{aligned}
\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} &= \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} \\
&= \frac{\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0, \gamma'.\left(\frac{\Omega}{n\ell}\right)\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \gamma'.\left(\frac{\Omega}{n\ell}\right)\right)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \gamma'.\left(\frac{\Omega}{n\ell}\right)\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \gamma'.\left(\frac{\Omega}{n\ell}\right)\right)} \\
&= \frac{\theta\left[\begin{smallmatrix}n\ell\, {}^tC(b+\beta)\\ {}^tD(b+\beta)\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \exp\left(-\pi i\, {}^t\beta n\ell C\, {}^tD\beta\right).
\end{aligned}$$

Comme D est congrue à l'identité modulo $n\ell$, nous obtenons

$$\begin{aligned}
\frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\gamma.\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\gamma.\Omega}{n\ell}\right)} &= \frac{\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \exp\left(-\pi i\, {}^t\beta\ell C\, {}^tD\beta\right)^n \\
&= \frac{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta, \frac{\Omega}{n\ell}\right)}{\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n\ell}\right)} \exp(-\pi i \ell\, {}^t\beta C\, {}^tD\beta)^n.
\end{aligned}$$

Nous avons donc démontré la propriété. □

Soit une matrice γ comme dans la propriété 7.1.2, d'après la dernière équation de cette propriété, les variétés associées à Ω/ℓ et à $(\gamma.\Omega)/\ell$ ont les mêmes thêta constantes de niveau n (projectivement). La deuxième équation implique que les facteurs $(\lambda_P/\lambda_{O_A})^\ell$ sont également les mêmes (rappelons que P est l'image d'un point $\beta \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$). La première équation signifie que les facteurs λ_P/λ_{O_A} sont modifiés par une racine ℓ-ième de l'unité (car n et ℓ sont premiers entre eux).

Considérons les matrices

$$\gamma = \begin{pmatrix} \mathrm{Id} & O \\ nC & \mathrm{Id} \end{pmatrix} \in \Gamma_{n,2n}$$

où $C \in \mathrm{Mat}_{g\times g}(\mathbb{Z})$ est une matrice symétrique de diagonale paire. Ces matrices γ vérifient clairement les conditions de la propriété 7.1.2. Soit ζ_ℓ une racine primitive ℓ-ième de l'unité. Pour tout élément e de S et tout entier k, il existe une matrice C (et donc une matrice γ) qui modifie le facteur λ_e/λ_{O_A} par ζ_ℓ^k mais laisse invariant les autres facteurs $\lambda_{e'}/\lambda_{O_A}$ avec e' dans S.
Nous pouvons donc prendre des racines ℓ-ièmes arbitraires des $(\lambda_e/\lambda_{O_A})^\ell$ pour tous les éléments e de S. Cette opération revient à considérer $\gamma.\Omega$ au lieu de Ω pour une certaine matrice γ.

Supposons « corrigés » les points de S, c'est-à-dire que les points de S sont compatibles. À partir de ces points, il est possible d'obtenir toutes les coordonnées des points de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ et ce en n'utilisant que des additions différentielles (voir l'algorithme 14). Nous avons donc des coordonnées compatibles et nous obtenons alors l'isogénie duale.

Remarque 7.1.3. *Dans l'article de Lubicz et Robert [LR10a], les auteurs utilisent les fonctions thêta algébriques et l'équivalent de la discussion précédente n'utilise pas l'action de* $\mathrm{Sp}(2g,\mathbb{Z})$ *mais l'action des automorphismes du groupe thêta.*

7.1.3 Isogénies de noyau fixé

Nous avons décrit comment prendre les isogénies correspondant aux noyaux $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ et $\Omega\left(\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\right)$. L'action du groupe $\mathrm{Sp}(2g,\mathbb{Z})$ sur les thêta constantes permet d'obtenir des variétés isomorphes (voir la discussion page 25). Après avoir appliqué un tel isomorphisme, les ℓ-isogénies vont correspondre à d'autres noyaux. Ces noyaux ne sont plus ni $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ ni $\Omega\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ mais restent des sous-groupes symplectiques maximaux de la ℓ-torsion.
Réciproquement étant donné un sous-groupe symplectique maximal K de la ℓ-torsion, nous pouvons nous ramener aux cas précédents via un changement de base symplectique : il existe une matrice γ préservant les thêta constantes telle que $\gamma.K$ correspondent à $\{(\gamma.\Omega)\alpha,\ \alpha \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\}$ ou à $\{\beta,\ \beta \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\}$. Nous pouvons alors appliquer les deux méthodes précédentes pour calculer une ℓ-isogénie de noyau K.

Grâce aux algorithmes précédents, il est alors possible de
- calculer une ℓ-isogénie en descendant du niveau $n\ell$ au niveau n,
- calculer une ℓ-isogénie en montant du niveau n au niveau $n\ell$,
- calculer une ℓ^2-isogénie en restant au même niveau.

Ces méthodes de calcul d'isogénies soulèvent le problème de savoir relier les thêta constantes de niveau $n\ell$ à celles de niveau n en restant sur la même variété. Cette question est fondamentale pour certaines applications comme par exemple pour les graphes d'isogénies pour le lien avec les courbes hyperelliptiques. Ainsi, pour les graphes d'isogénies, il faut savoir tester si deux variétés sont isomorphes. Si celles-ci sont fournies par des thêta constantes de même niveau n, ces dernières caractérisent la classe d'isomorphisme de la variété modulo l'action du groupe $\tilde{\Gamma}_{n,2n}\backslash\mathrm{Sp}(2g,\mathbb{Z})$. Dans ce cas, nous pouvons tester si les deux variétés sont isomorphes en testant toutes les matrices de $\tilde{\Gamma}_{n,2n}\backslash\mathrm{Sp}(2g,\mathbb{Z})$ (ce groupe étant fini). Cependant cette méthode ne marche plus si les variétés sont données par des thêta constantes de niveaux différents.
Pour les courbes hyperelliptiques, il est possible grâce aux formules de Thomae de calculer les thêta constantes de niveau 2 ou 4 et réciproquement, étant données ces thêta constantes de revenir à l'équation sous forme de Weierstraß. Cependant il n'existe pas dans la littérature, à notre connaissance, de formules permettant de faire le lien entre l'équation de la courbe et les fonctions thêta de niveau différent de 2 ou 4.
Ces deux exemples montrent donc la nécessité de savoir changer de niveau sans prendre d'isogénie.

7.2 Formules de changement de niveaux et applications

7.2.1 Changer de niveau en restant sur la même variété

Dans cette sous-section uniquement, les entiers positifs non nuls n et ℓ sont quelconques. Pour descendre de niveau sans prendre d'isogénie, nous disposons de la formule suivante qui est un cas particulier du théorème de Koizumi-Kempf 3.1.3.

Théorème 7.2.1. *Soit F une matrice de $\mathrm{Mat}_{r\times r}(\mathbb{Z})$ telle que ${}^tFF = \ell\,\mathrm{Id}$. Posons $T = F^{-1}$.*
Soit Ω une matrice du demi-espace de Siegel $\mathcal{H}_g$ et soit z un vecteur de $\mathbb{C}^g$.
Posons $Z = (z, 0, \ldots, 0) \in \mathrm{Mat}_{g,r}(\mathbb{C})$ et $W = ZT$.
Posons également $M = \mathrm{Mat}_{g,m}(\mathbb{Z})$, $L = \frac{1}{\ell}\mathrm{Mat}_{g,m}(\mathbb{Z})F$ et $L = L_1 + L_2$.
Soient des éléments b et b' de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$, posons $J_2 = (b, b', \ldots, b')\,T$. Nous avons

$$[L : M]\,\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right)\theta\left[\begin{smallmatrix}0\\ b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)^{r-1} = \sum_{P_2 \in MT/M}\prod_{i=1}^{r}\theta\left[\begin{smallmatrix}0\\ J_2^{(i)}+P_2^{(i)}\end{smallmatrix}\right]\left(W^{(i)}, \frac{\Omega}{n\ell}\right).$$

Si nous avons une matrice F de $\mathrm{Mat}_{r\times r}(\mathbb{Z})$ telle que ${}^tFF = \ell\,\mathrm{Id}$, alors les $J_2^{(i)} + P_2^{(i)}$ sont des vecteurs de $\frac{1}{n\ell}\mathbb{Z}^g$ et $W^{(i)}$ est un multiple de z. Par ailleurs, il existe un b' dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ tel que la thêta constante $\theta\left[\begin{smallmatrix}0\\ b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)$ ne soit pas nulle. Nous pouvons donc calculer la valeur de $\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right)$ en fonction des coordonnées de niveau $n\ell$ du point z et de ses multiples. Le nombre $\theta\left[\begin{smallmatrix}0\\ b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)^{r-1}$ apparaît devant toutes les coordonnées et est donc un facteur projectif qui n'est pas calculé. Avec $z = 0$ et en fixant b', nous obtenons (projectivement) les thêta constantes de niveau n en fonction de celles de niveau $n\ell$.

Des matrices convenables pour le théorème 7.2.1 sont données par

$$\begin{aligned}
\text{Pour } \ell = a^2, \qquad & F = (a)\,,\\
\text{Pour } \ell = a^2 + b^2, \qquad & F = \begin{pmatrix} a & -b\\ b & a\end{pmatrix},\\
\text{Pour } \ell = a^2 + b^2 + c^2 + d^2, \qquad & F = \begin{pmatrix} a & -b & -c & -d\\ b & a & -d & c\\ c & d & a & -b\\ d & -c & b & a\end{pmatrix}.
\end{aligned}$$

Ces matrices viennent naturellement : considérons les corps $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$. Dans chaque cas, la matrice F précédente est celle de la multiplication par un élément z tel que $z\bar{z} = \ell$ dans la base canonique du corps considéré comme $\mathbb{R}$ espace vectoriel. Comme la transposée de la matrice de multiplication par un élément z correspond à la matrice de multiplication par $\bar{z}$, le produit ${}^tFF$ est donc la matrice de multiplication par $z\bar{z} = \ell$ et est donc égal à $\ell\,\mathrm{Id}_r$.
La complexité des calculs dépendant fortement de la dimension r, il est intéressant d'essayer de la diminuer. En étudiant les formes quadratiques Id_r et $\ell\,\mathrm{Id}_r$, il est possible de trouver la valeur minimale de r.

Lemme 7.2.2. *Soit un nombre premier $\ell > 2$. La dimension minimale r dans le théorème 7.2.1 est de*
- *2 si ℓ est somme de deux carrés,*
- *4 sinon.*

Démonstration. Comparons les matrices des formes quadratiques $\ell\,\mathrm{Id}_r$ et Id_r. Elles sont équivalentes si elles ont même discriminant sur $\mathbb{Q}$, et même symboles de Hilbert [Ser70, p. 78]. Le discriminant de la première est $\ell^{r \bmod 2}$ donc si ℓ n'est pas carré, r doit être pair. Nous avons, d'après [Ser70, p. 39],

$$\epsilon_\ell\left(\ell\,\mathrm{Id}_2\right) = (\ell, \ell)_\ell = (-1)^{\frac{\ell-1}{2}},$$

$$\epsilon_\ell\left(\mathrm{Id}_2\right) = 1.$$

Donc r peut être pris égal à 2 si et seulement si ℓ est congru à 1 modulo 4 c'est à dire si et seulement si ℓ est la somme de deux carrés. □

Évidement, si ℓ n'est pas un nombre premier, la dimension r associée à ℓ peut être inférieure à celles associées à ses facteurs. De plus, dans le théorème 7.2.1, les constantes $\theta \left[\begin{smallmatrix} 0 \\ b' \end{smallmatrix} \right] \left(0, \frac{\Omega}{n}\right)$ de la partie gauche constituent un facteur projectif. Il n'est donc pas nécessaire qu'elles correspondent à la matrice Ω/n. Ainsi nous pouvons chercher des matrices F telles que

$$ {}^tFF = \begin{pmatrix} \ell & & & \\ & \gamma_2 & & \\ & & \ddots & \\ & & & \gamma_n \end{pmatrix} $$

où les γ_i sont des réels positifs quelconques. Par exemple pour $\ell = 12$ nous avons

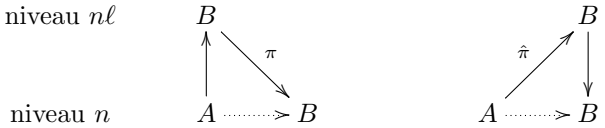
$$ \begin{pmatrix} 2 & 2 & 2 \\ 2 & -1 & -1 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 2 & 0 \\ 2 & -1 & 1 \\ 2 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 12 & & \\ & 6 & \\ & & 2 \end{pmatrix}. $$

Remarque 7.2.3. *Il existe une réciproque au théorème 7.2.1 permettant de monter de niveau sans prendre d'isogénie. Il suffit de considérer la matrice F^{-1} au lieu de F. Notons cependant qu'il faut connaître les coordonnées thêta de niveau n des points de ℓ-torsion. Ceci est cohérent avec la propriété 3.1.11 qui dit que les thêta constantes de la famille $\mathscr{F}_{n\ell}$ codent la $n\ell$-torsion de la variété.*

7.2.2 Calcul de ℓ-isogénies sans changer de niveau

Dans cette section, nous nous intéressons de nouveau aux calculs de ℓ-isogénies entre variétés abéliennes représentées avec des fonctions thêta de niveau n. Rappelons que nous supposons que n est pair (pour des raisons arithmétiques). Pour simplifier l'exposition et parce qu'il est possible de s'y ramener, nous avons fait l'hypothèse que ℓ est un nombre premier qui est premier avec n et avec la caractéristique du corps.

Combinée aux isogénies π et $\hat{\pi}$ de Lubicz et Robert [LR10a] (section 7.1), la formule de changement de niveau permet de calculer une ℓ-isogénie sans changer de niveau. Pour cela nous procédons comme l'un des deux diagrammes suivants :



Cette méthode présente l'inconvénient de devoir prendre des racines ℓ-ièmes et de travailler dans une extension de corps car les variétés en niveau $n\ell$ ne sont à priori pas définies sur le corps de base. Comme la flèche horizontale est rationnelle, il est naturel d'essayer de trouver un algorithme ne nécessitant pas de passer dans une extension. Une modification de la formule de descente de niveau sans isogénie va résoudre ce problème.

Posons $A = \mathbb{C}^g/\frac{\Omega}{\ell}\mathbb{Z}^g + \mathbb{Z}^g$ et $B = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$, l'isogénie de A vers B est donnée par

$$ \begin{array}{ccc} A = \mathbb{C}^g/\frac{\Omega}{\ell}\mathbb{Z}^g + \mathbb{Z}^g & \longrightarrow & B = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g \\ z & \longmapsto & \ell z \end{array} $$

et a pour noyau $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$.

Théorème 7.2.4. *Soit F une matrice de $\mathrm{Mat}_{r\times r}(\mathbb{Z})$ telle que ${}^tFF = \ell\,\mathrm{Id}$. Posons $T = F^{-1}$. Soit Ω une matrice du demi-espace de Siegel $\mathcal{H}_g$ et soit z un vecteur de $\mathbb{C}^g$. Posons*

$$ (w_1, \ldots, w_r) = (\ell z, 0, \ldots, 0)\, T \in \mathrm{Mat}_{g\times r}(\mathbb{C}). $$

Soient des éléments b et b' de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$, posons $(j_1,\dots,j_r) = (b,b',\dots,b')\,T$. Nous avons

$$d\;\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\ell z,\frac{\Omega}{n}\right)\theta^B\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)^{r-1} = \sum_{\substack{t_1,\dots,t_r\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\\(t_1,\dots,t_r)F=0}}\prod_{i=1}^{r}\theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(w_i+t_i,\frac{\Omega/\ell}{n}\right) \tag{7.1}$$

où $d = [\mathrm{Mat}_{g\times r}(\mathbb{Z})\,F : \ell\,\mathrm{Mat}_{g\times r}(\mathbb{Z})]$.

Démonstration. Ce théorème est une réécriture du théorème 7.2.1 où nous avons utilisé la propriété 3.1.2 pour avoir

$$\theta^A\left[\begin{smallmatrix}0\\j_i+P_2^{(i)}\end{smallmatrix}\right]\left(W^{(i)},\frac{\Omega/\ell}{n}\right) = \theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(W^{(i)}+P_2^{(i)},\frac{\Omega/\ell}{n}\right)$$

et le fait que

$$P_2\in\mathrm{Rpr}\,(MT/T)\iff P_2\in\left(\tfrac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\right)^r,\ P_2F=0.$$

□

Remarque 7.2.5. *La matrice $J=(b,b',\dots,b')\,T$ est à coefficients dans $\frac{1}{n\ell}\mathbb{Z}^g$. Rappelons que b et b' sont des représentants dans $\mathbb{Q}^g$ de classes de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$. Comme n et ℓ sont premiers entre eux, nous pouvons modifier b et b' par des éléments de $\mathbb{Z}^g$ de telle sorte que tous leurs numérateurs soient divisibles par ℓ. Dans la suite nous supposons donc que $J=(j_1,\dots,j_r)$ appartient à $\left(\frac{1}{n}\mathbb{Z}^g\right)^r$. D'après la propriété 3.1.2, les fonctions thêta de la base $\mathscr{F}_n$ utilisées ici ne dépendent pas du choix des représentants des classes de $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$.*

Avec la remarque précédente, il est clair que nous pouvons calculer les thêta constantes de niveau n de la variété B, à partir de la connaissance des « vraies » thêta constantes de niveau n de A et des « vraies » coordonnées des points de ℓ-torsion de la variété A :

$$\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta,\frac{\Omega/\ell}{n}\right)\qquad b\in\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g,\ \beta\in\tfrac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g.$$

De même, à partir de ces mêmes points de ℓ-torsion et des « vraies » coordonnées de niveau n d'un point de A, nous pouvons calculer les coordonnées de niveau n de l'image de ce point par l'isogénie.

Nous allons expliquer maintenant comment il est possible d'utiliser en pratique le théorème 7.2.4 pour calculer des ℓ-isogénies. Nous utiliserons le lemme suivant

Lemme 7.2.6. *La matrice F définie une application linéaire sur le $\mathbb{Z}/\ell\mathbb{Z}$ espace vectoriel :*

$$\begin{array}{ccc}(\mathbb{Z}/\ell\mathbb{Z})^r & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^r\\ u & \longmapsto & uF.\end{array}$$

Le noyau de cette application est l'ensemble des $u\,{}^tF$ où $u\in(\mathbb{Z}/\ell\mathbb{Z})^r$ et est de dimension $r/2$.

Calcul des thêta constantes de la variété B

Soit ℓ un nombre premier impair différent de la caractéristique du corps. Nous voulons calculer une ℓ-isogénie de A dans $B=A/K$ où K est un sous-groupe symplectique maximal de la ℓ-torsion sur A. Après un changement de base symplectique, nous pouvons supposer que K correspond à $\{\beta,\beta\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\}$. Finalement supposons que nous connaissons les coordonnées thêta de niveau n (avec n pair) des points de $\frac{1}{\ell}\mathbb{Z}^g$. C'est-à-dire que nous connaissons à un facteur projectif λ_β les coordonnées thêta

$$\lambda_\beta\,\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\beta,\frac{\Omega/\ell}{n}\right)\qquad b\in\tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g,\ \beta\in\tfrac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g.$$

Soit $(e_1,\dots,e_g)$ la base canonique de $\frac{1}{\ell}\mathbb{Z}^g$, nous notons par λ_i et $\lambda_{i,j}$ (pour $i\neq j$) les facteurs associés aux point e_i et e_i+e_j.

Comme ℓ est impair, nous obtenons les puissances ℓ-ièmes des λ_i/λ_{O_A} et $\lambda_{i,j}/\lambda_{O_A}$ en appliquant les résultats de la page 62. D'après les algorithmes 14 et 15, il est possible de calculer les relevés affines de tous les points de $\frac{1}{\ell}\mathbb{Z}^g$ en fonction des coordonnées des points e_i, e_i+e_j et des coefficients λ_i et $\lambda_{i,j}$. Reprenons l'équation 7.1 :

$$[L:L_1]\,\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)\theta\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)^{r-1}=\sum_{\substack{t_1,\dots,t_r\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g\\(t_1,\dots,t_r)F=0}}\prod_{i=1}^{r}\theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(t_i,\frac{\Omega/\ell}{n}\right).$$

Nous avons alors les monômes de la partie droite. Le lemme suivant montre qu'ils ne dépendent que des puissances ℓ-ièmes des facteurs λ_i/λ_{O_A} et $\lambda_{i,j}/\lambda_{O_A}$.

Lemme 7.2.7. *Soient $t_1,\dots,t_r$ des éléments de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ vérifiant la relation $(t_1,\dots,t_r)\,F=(0,\dots,0)$ et soient $j_1,\dots,j_r$ des éléments de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ tels que $(j_1,\dots,j_r)\,F=(b,b',\dots,b')$. Quand nous écrivons le produit*

$$\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1,\frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r,\frac{\Omega/\ell}{n}\right)$$

en terme des λ_i/λ_{O_A}, $\lambda_{i,j}/\lambda_{O_A}$ vues comme indéterminées, il appartient à l'algèbre

$$\mathbb{C}\left[\left(\lambda_i/\lambda_{O_A}\right)^\ell,\left(\lambda_{i,j}/\lambda_{O_A}\right)^\ell\right].$$

Démonstration. Nous voulons montrer que le produit est laissé invariant par toute transformation de

$$\mathbb{C}\left[\lambda_i/\lambda_{O_A},\lambda_{i,j}/\lambda_{O_A}\right]$$

qui agit sur les générateurs par une racine de ℓ-ième l'unité ζ. Ces transformations sont engendrées par les transformations χ_{i_o} et χ_{i_o,j_o} où

$$\chi_{i_o}\left(\frac{\lambda_i}{\lambda_{O_A}}\right)=\begin{cases}\zeta\frac{\lambda_{i_0}}{\lambda_{O_A}} & i=i_o\\ \frac{\lambda_i}{\lambda_{O_A}} & \forall i\neq i_o\end{cases}\qquad \chi_{i_o}\left(\frac{\lambda_{i,j}}{\lambda_{O_A}}\right)=\begin{cases}\zeta\frac{\lambda_{i_0,j}}{\lambda_{O_A}} & i=i_o,\ \forall j\\ \frac{\lambda_{i,j}}{\lambda_{O_A}} & \forall i\neq i_o,\ \forall j\end{cases}$$

$$\chi_{i_o,j_0}\left(\frac{\lambda_i}{\lambda_{O_A}}\right)=\frac{\lambda_i}{\lambda_{O_A}}\quad\forall i\qquad \chi_{i_o,j_0}\left(\frac{\lambda_{i,j}}{\lambda_{O_A}}\right)=\begin{cases}\zeta\frac{\lambda_{i_0,j_o}}{\lambda_{O_A}} & i=i_o,\ j=j_o\\ \frac{\lambda_{i,j}}{\lambda_{O_A}} & \forall i\neq i_o\ \forall j\neq j_o.\end{cases}$$

Les vecteurs t_i appartiennent à $\frac{1}{\ell}\mathbb{Z}^g$, posons $u_i=\ell\,(t_i)_{i_o}\in\mathbb{Z}$ la multiplication par ℓ de la coordonnée i_o de t_i. Nous avons alors

$$\begin{aligned}\chi_{i_0}\left(\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1,\frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r,\frac{\Omega/\ell}{n}\right)\right)&=\zeta^{u_1^2+\dots+u_r^2}\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1,\frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r,\frac{\Omega/\ell}{n}\right)\\&=\zeta^{u\,{}^tu}\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1,\frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r,\frac{\Omega/\ell}{n}\right)\end{aligned}$$

où nous avons écrit u pour le vecteur ligne des u_i. Comme par hypothèse

$$(t_1,\dots,t_r)\,F=(0,\dots,0)\in\tfrac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g,$$

nous avons

$$\begin{gathered}((t_1)_{i_o},\dots,(t_r)_{i_o})\,F\equiv(0,\dots,0)\mod\mathbb{Z}^g\\ uF=(u_1,\dots,u_r)\,F=(0,\dots,0).\end{gathered}$$

D'après 7.2.6, le vecteur u de $(\mathbb{Z}/\ell\mathbb{Z})^r$ doit être de la forme $u'\,{}^tF$ et donc

$$u\,{}^tu=u'\,{}^tFF\,{}^tu'=\ell u'\,{}^tu'=0\in\mathbb{Z}/\ell\mathbb{Z}.$$

De même, pour la transformation χ_{i_o,j_0}, posons

$$u=(\ell(t_1)_{i_0},\dots,\ell(t_r)_{i_0})\in\mathbb{Z}^g/\ell\mathbb{Z}^g,\qquad v=(\ell(t_1)_{j_0},\dots,\ell(t_r)_{j_0})\in\mathbb{Z}^g/\ell\mathbb{Z}^g.$$

Algorithme 20 Calcul d'une ℓ-isogénie sans changer de niveau

Entrée: Soit A une variété abélienne donnée par ses thêta constantes $\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega/\ell}{n}\right)$ de niveau n (avec n pair). Soit un entier ℓ premier et copremier avec n et la caractéristique du corps. Supposons données les coordonnées thêta de niveau n d'une base symplectique $(e_1, \ldots, e_i)$ d'un sous-groupe isotrope maximal de la ℓ-torsion.

Sortie: Les thêta constantes de niveau n de la variété $B = A/K$.

1: Fixer une matrice F de $\mathrm{Mat}_{r\times r}(\mathbb{Z})$ telle que ${}^tFF = \ell\,\mathrm{Id}_r$. {Nous posons $T = F^{-1} = \frac{1}{\ell}F$}
2: Faire un changement de base symplectique de sorte que

$$e_i \quad = \quad (0, \quad \ldots, \quad 0, \quad \overset{i}{\tfrac{1}{\ell}}, \quad 0, \quad \ldots, \quad 0)$$

3: Pour $i \neq j$, calculer $e_i + e_j$ dans A en utilisant des vraies additions (algorithme 8 page 54).
4: Calculer les puissances ℓ-ièmes des λ_i/λ_{O_A}, $\lambda_{i,j}/\lambda_{O_A}$ (voir page 62).
5: Utiliser les additions différentielles pour calculer les coordonnées thêta affines de niveau n de tous les points de $K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ dans $\mathbb{C}\left[\lambda_i/\lambda_{O_A}, \lambda_{i,j}/\lambda_{O_A}\right]$ où les λ_i/λ_{O_A}, $\lambda_{i,j}/\lambda_{O_A}$ sont vues comme des indéterminées.
6: Fixer un b' dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$.
7: **for** Pour tout b dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ **do**
8: soit $(j_1, \ldots, j_r) = (b, b', \ldots, b')\,T$ dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$. Calculer alors

$$u_b(0) := \sum_{\substack{t_1,\ldots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\ldots,t_r)F=0}} \prod_{i=1}^{r} \theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(t_i, \frac{\Omega/\ell}{n}\right)$$

dans l'algèbre

$$\mathbb{C}\left[X_i, X_{i,j}\right]/\left\{X_i^\ell = \left(\lambda_i/\lambda_{O_A}\right)^\ell, X_{i,j}^\ell = \left(\lambda_{i,j}/\lambda_{O_A}\right)^\ell\right\}.$$

9: **end for**
10: Si pour tout b, $u_b(0)$ est nul, retourner à 6.
11: **return** Les coordonnées $(u_b(0))_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$.

Nous avons alors

$$\chi_{i_0,j_o}\left(\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1, \frac{\Omega/\ell}{n}\right)\ldots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r, \frac{\Omega/\ell}{n}\right)\right) = \zeta^{u\,{}^tv}\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(t_1, \frac{\Omega/\ell}{n}\right)\ldots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(t_r, \frac{\Omega/\ell}{n}\right)$$

et par le même raisonnement, $u\,{}^tv = 0$, ce qui conclut la preuve. □

Grâce à ce lemme, n'importe quel choix de racine ℓ-ième pour λ_i/λ_{O_A} et $\lambda_{i,j}/\lambda_{O_A}$ donne le bon résultat. Nous pouvons éviter de prendre ces racines en travaillant dans l'algèbre

$$\mathbb{C}\left[X_i, X_{i,j}\right]/\left\{X_i^\ell = \left(\lambda_i/\lambda_{O_A}\right)^\ell, X_{i,j}^\ell = \left(\lambda_{i,j}/\lambda_{O_A}\right)^\ell\right\}.$$

Nous résumons le calcul des thêta constantes de la variété B dans l'algorithme 20.

Remarque 7.2.8. *Quand la donnée initiale n'est pas tous les points du noyau K mais seulement une base e_i, il faut calculer les points $e_i + e_j$ pour $i \neq j$. Cela ne peut pas être fait en utilisant des additions différentielles. En niveau $n \geq 4$ pair, nous pouvons utiliser les vrais additions et en niveau $n = 2$, il faut utiliser des additions compatibles telles que définies dans [LR10a, Rob10].*

Calcul de l'image d'un point

Nous expliquons maintenant comment calculer l'image d'un point $z \in \mathbb{C}^g/\Lambda_\Omega$ par l'isogénie précédente. Supposons connu un relevé affine des coordonnées thêta de niveau n de z :

$$\mu_0\ \theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right), \qquad b \in \tfrac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g.$$

D'après l'équation 7.1, nous avons la formule

$$[L : L_1]\,\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(\ell z, \frac{\Omega}{n}\right)\theta^B\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)^{r-1} = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)F=0}} \prod_{i=1}^{r} \theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(w_i + t_i, \frac{\Omega/\ell}{n}\right),$$

nous devons calculer les $\theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(w_i + t_i, \frac{\Omega/\ell}{n}\right)$. Comme dans le cas précédent, nous allons les calculer à un facteur inconnu près. Cependant, nous connaîtrons suffisamment d'informations pour être capable d'obtenir la valeur du terme de droite.

Commençons par calculer le point correspondant à $z + e_i$ où $(e_1, \dots, e_n)$ est la base canonique de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ à des facteurs projectifs μ_i inconnus près. Pour cette opération nous avons besoin de vraies additions. Soit k un entier, avec les algorithmes de la section 3.2.3, nous pouvons retrouver tous les points $kz+\beta$ avec $\beta \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ à un facteur projectif près dépendant des μ_i, λ_i et $\lambda_{i,j}$. De plus, d'après la section 3.2.3, nous pouvons calculer les puissances ℓ-ièmes des facteurs μ_i/μ_0 en fonction des coordonnées des points et de $\lambda_i^{\ell(\ell-1)}/\lambda_{O_A}^{\ell(\ell-1)}$. Ces derniers sont les puissances $\ell-1$-ièmes de $(\lambda_i/\lambda_{O_A})^\ell$ qui ont été calculées dans la section précédente.

Lemme 7.2.9. *Soient $t_1, \dots, t_r$ des éléments de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ vérifiant la relation $(t_1, \dots, t_r)\,F = (0, \dots, 0)$ et soient $j_1, \dots, j_r$ des éléments de $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ tels que $(j_1, \dots, j_r)\,F = (b, b', \dots, b')$.*
Posons $(w_1, \dots, w_r) = (z, 0, \dots, 0)\ {}^tF$. Quand nous écrivons le produit

$$\theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(w_1 + t_1, \frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(w_r + t_r, \frac{\Omega/\ell}{n}\right)$$

en terme des μ_i, λ_i et $\lambda_{i,j}$ vues comme indéterminées, il appartient à l'algèbre

$$\mathbb{C}\left[(\mu_i/\mu_0)^\ell, (\lambda_i/\lambda_{O_A})^\ell, (\lambda_{i,j}/\lambda_{O_A})^\ell\right].$$

La preuve est similaire à celle du lemme 7.2.7.

Démonstration. Appelons $\mathscr{P}$ le produit

$$\mathscr{P} := \theta^A\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right]\left(w_1 + t_1, \frac{\Omega/\ell}{n}\right)\dots\theta^A\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]\left(w_r + t_r, \frac{\Omega/\ell}{n}\right).$$

Nous voulons montrer que $\mathscr{P}$ est laissé invariant par toute transformation de

$$\mathbb{C}\left[(\mu_i/\mu_0)^\ell, (\lambda_i/\lambda_{O_A})^\ell, (\lambda_{i,j}/\lambda_{O_A})^\ell\right]$$

qui agit sur les générateurs par une racine ℓ-ième de l'unité ζ. Ces transformations sont engendrées par les transformations χ_{i_o}, χ_{i_o,j_o} et ξ_{i_0} où

$$\chi_{i_o}\left(\frac{\lambda_i}{\lambda_{O_A}}\right) = \begin{cases} \zeta\frac{\lambda_{i_0}}{\lambda_{O_A}} & i = i_o \\ \frac{\lambda_i}{\lambda_{O_A}} & \forall i \neq i_o \end{cases} \qquad \chi_{i_o}\left(\frac{\lambda_{i,j}}{\lambda_{O_A}}\right) = \begin{cases} \zeta\frac{\lambda_{i_0,j}}{\lambda_{O_A}} & i = i_o,\ \forall j \\ \frac{\lambda_{i,j}}{\lambda_{O_A}} & \forall i \neq i_o,\ \forall j \end{cases}$$

$$\chi_{i_o}\left(\frac{\mu_i}{\mu_0}\right) = \begin{cases} \zeta\frac{\mu_{i_0}}{\mu_0} & i = i_o \\ \frac{\mu_i}{\mu_0} & \forall i \neq i_o \end{cases}$$

$$\chi_{i_o,j_0}\left(\frac{\lambda_i}{\lambda_{O_A}}\right)=\frac{\lambda_i}{\lambda_{O_A}}\qquad\forall i,\qquad\qquad \chi_{i_o,j_0}\left(\frac{\lambda_{i,j}}{\lambda_{O_A}}\right)=\begin{cases}\zeta^{\frac{\lambda_{i_0,j_o}}{\lambda_{O_A}}} & i=i_o,\ j=j_o\\ \frac{\lambda_{i,j}}{\lambda_{O_A}} & \forall i\neq i_o\ \forall j\neq j_o\end{cases}$$

$$\chi_{i_o,j_0}\left(\frac{\mu_i}{\mu_0}\right)=\frac{\mu_i}{\mu_0}\qquad\forall i$$

$$\xi_{i_o}\left(\frac{\lambda_i}{\lambda_{O_A}}\right)=\frac{\lambda_i}{\lambda_{O_A}}\qquad\forall i,\qquad\qquad \xi_{i_o}\left(\frac{\lambda_{i,j}}{\lambda_{O_A}}\right)=\frac{\lambda_{i,j}}{\lambda_{O_A}}\qquad\forall i,j,\qquad\qquad \xi_{i_o}\left(\frac{\mu_i}{\mu_0}\right)=\begin{cases}\zeta^{\frac{\mu_{i_0}}{\mu_0}} & i=i_o\\ \frac{\mu_i}{\mu_0} & \forall i\neq i_o\end{cases}$$

Posons

$$u=(\ell(t_1)_{i_0},\ldots,\ell(t_r)_{i_0})\in\mathbb{Z}^g/\ell\mathbb{Z}^g,\qquad v=(\ell(t_1)_{j_0},\ldots,\ell(t_r)_{j_0})\in\mathbb{Z}^g/\ell\mathbb{Z}^g,\qquad m=(1,0,\ldots,0)\ {}^tF,$$

nous avons alors

$$\begin{aligned}\chi_{i_0}(\mathscr{P}) &= \zeta^{u\,{}^tu}\mathscr{P},\\ \chi_{i_0,j_o}(\mathscr{P}) &= \zeta^{u\,{}^tv}\mathscr{P},\\ \xi_{i_0}(\mathscr{P}) &= \zeta^{u\,{}^tm}\mathscr{P}.\end{aligned}$$

Comme $mF=uF=vF=0$ dans $(\mathbb{Z}/\ell\mathbb{Z})^r$, il existe des vecteurs u', v' et m' dans $(\mathbb{Z}/\ell\mathbb{Z})^r$ tels que $u=u'\,{}^tF$, $v=v'\,{}^tF$ et $m=m'\,{}^tF$. D'où

$$u\,{}^tu=u'\,{}^tFF\,{}^tu'=\ell u'\,{}^tu'=0,$$

$$u\,{}^tv=u'\,{}^tFF\,{}^tv'=\ell u'\,{}^tv'=0,$$

$$u\,{}^tm=u'\,{}^tFF\,{}^tm'=\ell u'\,{}^tm'=0.$$

□

L'algorithme 21 permettant de calculer l'image d'un point par l'isogénie est donc correct.

Complexité

Nos algorithmes dépendent de plusieurs paramètres :
- la dimension g de la variété abélienne,
- le corps k où elle est définie,
- le degré ℓ de l'isogénie,
- le niveau n des coordonnées thêta.

La dimension g est fixée ainsi que le corps k. Nous supposons également que n est fixé car en pratique n est égal à 2 ou 4. Nous cherchons donc la complexité en ℓ.

Dans les algorithmes précédents, l'étape la plus coûteuse est le calcul des $O(\ell^g)$ points des modules en utilisant des additions différentielles. Pour le calcul des thêta constantes de B, nous avons besoin de ℓ^g points exactement et pour envoyer un point par l'isogénie, nous avons besoin de $r\ell^g$ points. Soit L le corps où tous les points sont définis. Le nombre de coordonnées d'un point est $O(n^g)$ et est fixe. Par ailleurs, nous travaillons sur une algèbre de dimension au plus $g(g+3)/2$ au dessus de L. De ce fait, nous avons besoin de $O(\ell^g)$ opérations dans L pour calculer les coordonnées des points.

Maintenant, il faut utiliser l'équation 7.1. Le coût est de $O\left(\ell^{\frac{rg}{2}}\right)$ opérations dans L car l'ensemble des éléments $t_1,\ldots,t_r\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ tels que $(t_1,\ldots,t_r)\,F=0$ est un $\mathbb{Z}/\ell\mathbb{Z}$-espace vectoriel de dimension $rg/2$. Nous obtenons donc bien la complexité annoncée.

Algorithme 21 Image d'un point par une ℓ-isogénie sans changer de niveau

Entrée: Soit A une variété abélienne donnée par ses thêta constantes $\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega/\ell}{n}\right)$ de niveau n (avec n pair). Soit un entier ℓ premier et copremier avec n et la caractéristique du corps. Supposons données les coordonnées thêta de niveau n d'une base symplectique $(e_1, \ldots, e_i)$ d'un sous-groupe isotrope maximal de la ℓ-torsion ainsi que celles $\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(z, \frac{\Omega/\ell}{n}\right)$ d'un point P sur la variété.

Sortie: Les coordonnées thêta de niveau n de l'image de P dans la variété $B = A/K$ isogène à A.

1: Fixer une matrice F de $\mathrm{Mat}_{r\times r}(\mathbb{Z})$ telle que ${}^tFF = \ell\,\mathrm{Id}_r$. {Nous posons $T = F^{-1} = \frac{1}{\ell}F$}
2: Faire un changement de base symplectique de sorte que

$$e_i \quad = \quad (0, \quad \ldots, \quad 0, \quad \overset{i}{\tfrac{1}{\ell}}, \quad 0, \quad \ldots, \quad 0)$$

3: Pour $i \neq j$, calculer $e_i + e_j$ dans A en utilisant des vraies additions (algorithme 8 page 54).
4: Pour tout i, calculer $P + e_i$ dans A en utilisant des vraies additions.
5: Calculer les puissances ℓ-ièmes des λ_i/λ_{O_A}, $\lambda_{i,j}/\lambda_{O_A}$, μ_i/μ_0.
6: Utiliser les additions différentielles pour calculer les coordonnées thêta affines de niveau n de tous les points $kz + e$ où $0 \leq k < \ell$ et e appartient à $K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ dans $\mathbb{C}\left[\mu_i/\mu_0, \lambda_i/\lambda_{O_A}, \lambda_{i,j}/\lambda_{O_A}\right]$ où les μ_i/μ_0, λ_i/λ_{O_A}, $\lambda_{i,j}/\lambda_{O_A}$ sont vues comme des indéterminées.
7: Fixer un b' dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ tel que $\theta^B\left[\begin{smallmatrix}0\\b'\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)$ est non nulle.
8: **for** Pour tout b dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ **do**
9: Soit $(j_1, \ldots, j_r) = (b, b', \ldots, b')\,T$ dans $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$. Posons $(w_1, \ldots, w_r) = (z, 0, \ldots, 0)\ {}^tF$. Calculer

$$u_b(z) := \sum_{\substack{t_1,\ldots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\ldots,t_r)F=0}} \prod_{i=1}^{r} \theta^A\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right]\left(w_i + t_i, \frac{\Omega/\ell}{n}\right)$$

dans l'algèbre

$$\mathbb{C}\left[Y_i, X_i, X_{i,j}\right]/\left\{Y_i^\ell = \left(\mu_i/\mu_0\right)^\ell, X_i^\ell = \left(\lambda_i/\lambda_{O_A}\right)^\ell, X_{i,j}^\ell = \left(\lambda_{i,j}/\lambda_{O_A}\right)^\ell\right\}.$$

10: **end for**
11: **return** Les coordonnées $(u_b(z))_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$.

7.3 Calcul de 2-isogénies

Les 2-isogénies s'expriment facilement en considérant les tores :

$$\begin{array}{rcl} A = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g & \longrightarrow & B = \mathbb{C}^g/2\Omega\mathbb{Z}^g + \mathbb{Z}^g \\ z & \longmapsto & 2z. \end{array}$$

Le noyau de l'isogénie est $\left\{\beta,\ \beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\right\}$. Dans la section 3.2, nous avons utilisé cette isogénie et sa duale pour avoir une arithmétique efficace avec les fonctions thêta. Cependant, si nous reprenons les formules, nous voyons que nous n'avons pas réellement calculé l'isogénie. En particulier, les thêta constantes de B ne sont jamais calculées.

Supposons que la variété A soit donnée par ses thêta constantes de niveau n de la base $\mathscr{F}_n$:

$$\left(\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0, \frac{\Omega}{n}\right)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$$

et supposons que n soit pair, les formules suivantes traduisent l'isogénie :

$$\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{2\Omega}{n}\right)^2 = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\theta^A\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right)\theta^A\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right]\left(0,\frac{\Omega}{n}\right),$$

$$\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(2z,\frac{2\Omega}{n}\right)\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{2\Omega}{n}\right) = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\theta^A\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right)\theta^A\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right]\left(z,\frac{\Omega}{n}\right).$$

Nous obtenons donc les carrés des thêta constantes de la variété B. Une fois déterminées ces thêta constantes, nous pouvons calculer l'image des points mais il faut supposer qu'aucune thêta constante de niveau n de la variété B n'est nulle. Remarquons que pour des variétés génériques ceci est le cas.

Pour obtenir les thêta constantes, nous pouvons extraire les racines de manière arbitraire et vérifier que les valeurs obtenues vérifient toujours les équations de Riemann et celles de symétries 3.1.15.

Le lemme suivant est une application du lemme 3.1.28.

Lemme 7.3.1. *Soit γ une matrice de $\Gamma_{2,4}$ alors γ laisse fixes les thêta constantes de niveau 2 de A et les carrés de celles de niveau 2 de B :*

$$\frac{\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{2}\right)}{\theta^A\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\gamma.\Omega}{2}\right)} = \frac{\theta^A\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right)}{\theta^A\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\left(0,\frac{\Omega}{2}\right)}, \qquad \left(\frac{\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta^B\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)}\right)^2 = \left(\frac{\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)}{\theta^B\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\right)^2.$$

Par contre nous avons

$$\frac{\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\gamma.\Omega)}{\theta^B\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\gamma.\Omega)} = \frac{\theta^B\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega)}{\theta^B\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)}\exp\left(-\pi i\,{}^t\!bC\,{}^tDb\right).$$

En dimension 2 et en niveau 2, le lemme précédent montre que nous pouvons prendre des racines carrées arbitraires. En effet, considérons la matrice

$$\gamma = \begin{pmatrix} \mathrm{Id}_2 & 0 \\ \begin{pmatrix} 4c_{1,1} & 2c_{1,2} \\ 2c_{1,2} & 4c_{2,2} \end{pmatrix} & \mathrm{Id}_2 \end{pmatrix} \in \Gamma_{2,4}$$

où les $c_{i,j}$ sont des entiers. Posons ${}^t\!b = (b_1, b_2) \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ alors

$$\exp\left(-\pi i\,{}^t\!bC\,{}^tDb\right) = (-1)^{4b_1^2c_{1,1}+4b_2^2c_{2,2}+4b_1b_2c_{1,2}}.$$

De ce fait, pour chaque caractéristique possible de $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$, il existe une matrice γ qui change la thêta constante de B en son opposée et laisse les autres thêta constantes invariantes.

Toujours en dimension 2, pour le niveau 4, nous pouvons procéder de la même façon en travaillant avec la base $\mathscr{F}_{(2,2)}$. Nous avons alors la formule suivante : pour tous éléments a, b dans $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,

$$\theta^B\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,2\Omega)^2 = \frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}(-1)^{4\,{}^t\!a\beta}\theta^A\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right](0,\Omega)\,\theta^A\left[\begin{smallmatrix}0\\\beta\end{smallmatrix}\right](0,\Omega)$$

et nous pouvons montrer que nous avons le droit d'extraire les racines pour toutes les thêta constantes. On consultera également la section 6.2 qui fait le même genre de travail pour les formules de Thomae.

7.4 Isogénies entre courbes hyperelliptiques en genre 2

Dans cette section, nous appliquons les résultats des parties précédentes pour calculer des isogénies entre les jacobiennes de courbes hyperelliptiques en genre 2. Nous nous plaçons dans le cadre le plus général possible : l'équation d'une courbe $\mathcal{C}_1$ est sous forme de Weierstraß et nous supposons que le noyau de l'isogénie est un sous-groupe globalement rationnel de la ℓ-torsion de $\mathrm{Jac}(\mathcal{C}_1)$. Nous voulons calculer une équation rationnelle de la courbe $\mathcal{C}_2$, isogène à $\mathcal{C}_1$. De même, pour pousser des points, nous supposons que le point initial nous est donné par ses coordonnées de Mumford et nous voulons retrouver les coordonnées de Mumford de son image.

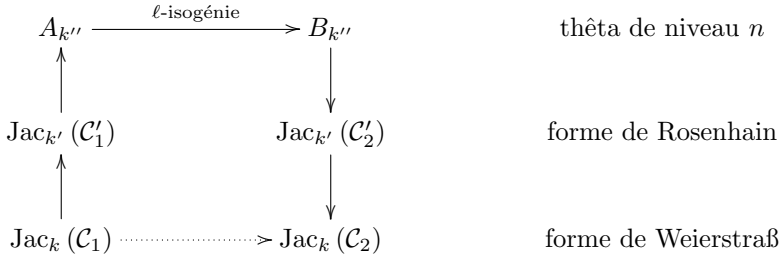
Algorithme 22 Calcul de ℓ-isogénies entre courbes hyperelliptiques de genre 2

Entrée: étant donnée une courbe $\mathcal{C}_1$ sur un corps k et un sous-groupe isotrope maximal K de $\mathrm{Jac}_k(C_1)[\ell]$ où ℓ est un premier impair.
Sortie: Une courbe $\mathcal{C}_2$ sur k telle que $\mathrm{Jac}_k(\mathcal{C}_2) = \mathrm{Jac}_k(C_1)/K$.

1: Trouver une base de K en coordonnées de Mumford. {Si nous utilisons $n = 2$, nous pouvons travailler avec u et v^2 ; cela oblige en général à prendre une extension de corps}
2: Trouver l'équation de Rosenhain $\mathcal{C}_1'$ de la courbe $\mathcal{C}_1$ et y envoyer les points de la base de K. {Cela peut nécessiter de prendre une extension de corps k'/k}
3: Utiliser les formules de Thomae (théorème 3.1.19) pour calculer les puissances 4-ièmes des thêta constantes de niveau $(2,2)$.
4: Extraire les racines (section 6.2) pour obtenir les vraies thêta constantes de niveau n de $A_{k''}$. {Cela peut nécessiter de prendre une extension de corps k''/k'}
5: Calculer les coordonnées thêta des images de la base de K. {Il peut être intéressant de calculer aussi celles des points $e_i + e_j$}
6: Appliquer l'algorithme 20 pour obtenir la variété isogène $B_{k''}$.
7: Calculer une forme de Rosenhain $\mathcal{C}_2'$ de la courbe $\mathcal{C}_2$. {A priori $\mathcal{C}_2'$ est à coefficients dans k''}
8: Si besoin, appliquer l'algorithme de Mestre [Mes91] pour obtenir une équation rationnelle de $\mathcal{C}_2$.

7.4.1 Théorie

Nous calculons le diagramme commutatif suivant. L'entier n est pris égal 2 ou 4 suivant l'objectif poursuivi (nous y reviendrons page 170). De plus, en général, nous avons à prendre des extensions de corps.



L'algorithme décrit dans cette section est résumé plus formellement par l'algorithme 22.

La première étape de l'algorithme consiste à calculer les thêta constantes de niveau n de la variété A. Pour cela, nous devons utiliser les formules de Thomae et il faut donc avoir une courbe $\mathcal{C}_1'$ de la forme $y^2 = f(x)$ avec f un polynôme scindé. Après avoir appliqué la formule de Thomae, nous obtenons les puissances 4-ièmes des thêta constantes de niveau $(2,2)$ et nous utilisons alors la discussion de la section 6.2 pour extraire ces racines et obtenir les thêta constantes de niveau n de A. Pour une courbe initiale $\mathcal{C}_1$ générique, ces deux étapes obligent à prendre des extensions de corps (le degré de ces extensions est borné par $6n$ sur les corps finis).
Même si le noyau K est rationnel, les points de K ne sont a priori pas définis sur le corps de base. De ce fait, nous allons travailler dans une extension de corps L/k où ces points seront définis. Le degré de cette extension est au plus de $\ell^2 - 1$ mais si ℓ est totalement décomposé dans l'anneau d'endomorphismes de la jacobienne, la borne est $\ell - 1$. Nous pouvons maintenant calculer les coordonnées thêta de l'image des points d'une base symplectique du noyau par les morphismes entre $\mathrm{Jac}(\mathcal{C}_1)$ et A (chapitre 5). Comme ℓ est premier avec n, il existe un isomorphisme du tore qui laisse fixes les thêta constantes de niveau n mais transforme le noyau K en $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$. Nous pouvons donc directement appliquer les morphismes en supposant que nous sommes dans ce cas.
Nous appliquons alors l'algorithme 20 permettant de calculer les thêta constantes de niveau n de la variété $B = A/K$. Une fois celles-ci obtenues, nous appliquons les formules de Rosenhain 3.1.20 pour obtenir une courbe sous forme de Rosenhain. Notons que l'équation obtenue correspond à la courbe $\mathcal{C}_2'$ ou à sa

tordue $\widetilde{\mathcal{C}_2'}$. Si nous sommes en niveau 4, nous connaissons les coordonnées thêta d'un point de 4-torsion ce qui permet, après avoir utilisé les morphismes, de déterminer l'équation de $\mathcal{C}_2'$. Pour le niveau 2, nous expliquerons comment retrouver la bonne courbe à la fin de la section.
L'équation de $\mathcal{C}_2$ ainsi obtenue, n'est pas forcément rationnelle sur le corps k. Si la 2-torsion était rationnelle sur la courbe $\mathcal{C}_1/k$ alors elle le sera aussi sur $\mathcal{C}_2$. Dans ce cas, cette dernière admet une équation $y^2 = f(x)$ avec $f \in k[x]$ scindée, à racines simples. Possiblement après un changement de coordonnée $y \to \chi y$, la courbe $\mathcal{C}_2'$ a une équation rationnelle. Si la 2-torsion n'était pas rationnelle, nous calculons les invariants d'Igusa de $\mathcal{C}_2'$ qui appartiennent à k car $\mathcal{C}_2'$ est un modèle de la courbe $\mathcal{C}_2$ définie sur k. Nous appliquons alors l'algorithme de Mestre [Mes91] pour reconstruire un modèle de Weierstraß rationnel de $\mathcal{C}_2$.

Le fait de retrouver une courbe ayant une équation rationnelle est important pour certaines applications. Par exemple, pour les graphes d'isogénies, nous désirons pouvoir calculer toutes les ℓ-isogénies rationnelles partant de $\mathcal{C}_2$. Si nous n'avons pas une équation rationnelle de $\mathcal{C}_2$, il n'est pas possible de déterminer les sous-groupes de ℓ-torsion qui sont globalement rationnels (par rapport au corps de base). Si les thêta constantes de niveau n de A sont définies sur le corps de base, celles de B le sont également. Dans ce cas, si nous voulons calculer des isogénies (rationnelles) partant de $\mathcal{C}_2$, il n'est pas nécessaire de calculer l'équation de la courbe. Remarquons cependant que le calcul des sous-groupes rationnels isotropes maximaux de la ℓ-torsion est plus facile en coordonnées de Mumford qu'en coordonnées thêta. On pourra consulter [FLR09].

En supposant que le corps de base est fixé, nous obtenons

Théorème 7.4.1. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 sur un corps k de caractéristique différente de 2. Soit ℓ un nombre premier impair différent de la caractéristique de k, posons $r = 2$ si $\ell \equiv 1 \mod 4$ et $r = 4$ sinon. Soit K un sous groupe isotrope maximal de $\mathrm{Jac}_k(\mathcal{C})[\ell]$.*
Nous pouvons calculer l'isogénie $\mathrm{Jac}_k(\mathcal{C}) \to \mathrm{Jac}_k(\mathcal{C})/K$ avec les coordonnées de Mumford en utilisant $O(\ell^r)$ opérations arithmétiques dans le corps L/k où les points de K sont définis. En particulier, si k est un corps fini et si K est rationnel alors l'isogénie peut se calculer en $O\left(\ell^{r+2}\right)$ opérations dans k.

Pour accélérer les calculs, le niveau $n = 2$ est très intéressant. En effet, travailler en niveau 2 plutôt que 4 présente de grands avantages :
- extensions de corps moins grandes à prendre (voir les formules de Thomae 6.2),
- moins de coordonnées à manipuler : 4 au lieu de 16,
- arithmétique plus rapide.

Les inconvénients du niveau 2 sont
- nous travaillons sur la courbe et sa tordue en même temps,
- nous identifions un point et son opposé.

Dans la plupart des cas, il est possible de contourner ces inconvénients tout en ayant un algorithme plus rapide que le niveau 4. Cependant, même si nous utilisons le niveau 2, il est intéressant de travailler en coordonnées de Mumford sur A et non sur $A/\{\pm 1\}$. En effet, cela simplifie les calculs et cela permet également de calculer les points $e_i + e_j$ en coordonnées de Mumford, puis leurs images en coordonnées thêta de niveau 2. De ce fait nous n'avons pas besoin d'additions différentielles compatibles [LR10a].
Lors du calcul de la courbe isogène en niveau 2, nous ne pouvons pas déterminer si nous sommes sur la courbe ou sa tordue. Une méthode pour résoudre ce problème sur corps finis consiste à compter le nombre de points de la jacobienne. En effet ce nombre permet de discriminer une courbe de sa tordue. Si nous ne disposons pas d'un algorithme de comptage de points suffisamment rapide, nous pouvons calculer l'image d'un diviseur de $\mathrm{Jac}(\mathcal{C}_1)$ qui n'est pas de 2-torsion. Nous obtenons alors l'élément $\pm f(D)$ de $\mathrm{Jac}(\mathcal{C}_2)$ qui permet de savoir si nous avons obtenu ou pas l'équation de la courbe.
Supposons que nous voulons calculer l'image d'un diviseur D par l'isogénie f, mais en utilisant le niveau 2 pour accélérer les calculs. Dans ce cas, nous avons vu que nous pouvons calculer $\pm f(D)$ et il faut donc trouver un moyen de discriminer entre ces deux points. Quitte à composer l'isogénie par l'involution hyperelliptique nous pouvons choisir arbitrairement une de ces deux images. Le seul cas où il ne sera pas possible de conclure en utilisant le niveau 2 est celui où nous voulons calculer les images de plusieurs points par l'isogénie.

7.4.2 Calculs explicites

Nous avons programmé l'algorithme 22 dans AVIsogenies. Pour avoir un programme plus efficace, du code spécifique a été écrit pour le genre 2 et le niveau 2. Un exemple de calcul d'isogénie de grand degré est le suivant : soit $\mathcal{C}$ la courbe d'équation

$$y^2 = x^5 + 41691x^4 + 24583x^3 + 2509x^2 + 15574x$$

sur $\mathbb{F}_{42179}$. Le cardinal de la jacobienne de cette courbe est $2^{10}1321^2$ et il n'existe qu'un seul sous-groupe isotrope rationnel K de $\ell = 1321$ torsion. Des générateurs de ce sous-groupe sont par exemple les deux diviseurs

$$\left(x^2 + 19580x + 40287, 11802x + 21414\right), \qquad \left(x^2 + 39301x + 3354, 4542x + 23058\right)$$

donnés en coordonnées de Mumford. La courbe isogène (respectivement à K) est

$$y^2 = 33266x^6 + 20155x^5 + 31203x^4 + 9732x^3 + 4204x^2 + 18026x + 29732$$

Le calcul a pris autour de 2 heures sur un core 2 avec 12 GB de RAM. Cet exemple a été choisi de telle sorte que les thêta constantes de niveau 2 soient rationnelles sur le corps de base, ainsi que tous les points de K. Ceci a permis de ne pas calculer certaines extensions de corps. Dans le cas général, prendre des extensions de corps augmente le temps de calcul d'un facteur quadratique ou linéaire selon le type d'algorithme utilisé pour la multiplication.

Notre programme est générique. Pour un genre fixé, il est certain qu'il est possible de l'optimiser à la fois au niveau du temps de calcul et au niveau de la gestion de la mémoire. Ainsi, la structure utilisée pour coder les fonctions thêta de niveau n est valide pour tout n et pour toute dimension. De ce fait elle est peu adaptée aux niveaux et genres petits. Par ailleurs, il faudrait éviter de prendre des extensions de corps. En effet, les calculs sont ensuite plus lents et les précalculs effectués par MAGMA lors de ces créations ne sont pas négligeables.
Pour de petits ℓ (inférieur à 10), l'opération la plus coûteuse n'est plus le calcul de l'isogénie en lui même mais les conversions entre les différents systèmes de coordonnées.

Présentons quelques graphes d'isogénies obtenus sur de petits exemples. Chaque sommet des graphes est une classe d'isomorphisme de courbes hyperelliptiques et chaque arrête représente une (ℓ, ℓ)-isogénie. La structure des graphes peut se lire en étudiant les idéaux dans l'anneau d'endomorphismes. Décrivons ce qui se passe sans rentrer trop en détail dans la théorie de la multiplication complexe pour laquelle on pourra consulter les livres [Shi98, Mil06] et les thèses [Gru08, Str10, Bis11].
Le corps $K = \mathrm{End}(A) \otimes \mathbb{Q}$ est une extension quadratique totalement imaginaire d'un corps de nombre K_0 totalement réel de degré g. De plus $\mathcal{O} = \mathrm{End}(A)$ est un ordre dans ce corps et il doit contenir l'ordre minimal $\mathbb{Z}[\pi, \hat{\pi}]$ où π est le Frobenius et $\hat{\pi}$ le Verschiebung (notons que $\hat{\pi} = q/\pi$ dans K). Pour simplifier l'exposition, nous supposons que nous sommes toujours dans le cas où $\mathcal{O} = \mathrm{End}(A)$ est l'ordre maximal $\mathcal{O}_K$ de K.
Nous nous intéressons aux ℓ-isogénies qui préservent la polarisation. Il en existe de deux types : celles qui préservent l'anneau d'endomorphisme (isogénies horizontales) et les autres (isogénies verticales).

La théorie CM permet de décrire les isogénies horizontales. Elles correspondent à l'action d'un élément $(\mathfrak{a}, \ell)$ du groupe $\mathfrak{C}(\mathcal{O}_K)$ de Shimura. C'est-à-dire que ℓ doit se décomposer dans $\mathcal{O}_K$ en $\ell\mathcal{O}_K = \mathfrak{a}\bar{\mathfrak{a}}$. En genre 2, nous sommes dans un des cas suivants :
- $\ell\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$ avec $\mathrm{N}\,\mathfrak{p} = \mathrm{N}\,\mathfrak{q} = \ell$,
- $\ell\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}$ avec $\mathrm{N}\,\mathfrak{p} = \ell$ et $\mathrm{N}\,\mathfrak{q} = \ell^2$,
- $\ell\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ avec $\mathrm{N}\,\mathfrak{p} = \ell$ et $\mathrm{N}\,\mathfrak{q} = \ell^3$,
- $\ell\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ avec $\mathrm{N}\,\mathfrak{p} = \mathrm{N}\,\mathfrak{q} = \ell^2$,
- $\ell\mathcal{O}_K = \mathfrak{p}$ avec $\mathrm{N}\,\mathfrak{p} = \ell^4$.

Les cas qui nous intéressent sont donc les deux premiers. Quand $\ell\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}$, de chaque courbe partent deux isogénies. Nous avons alors un graphe en forme de cercle, figure 7.1. Quand $\ell\mathcal{O}_K = \mathfrak{p}\mathfrak{q}\bar{\mathfrak{p}}\bar{\mathfrak{q}}$, il existe 4 idéaux $\mathfrak{a}$ tels que $\mathfrak{a}\bar{\mathfrak{a}} = \ell$. Nous obtenons alors une décomposition du tore en quadrilatères (figure 7.2).

FIGURE 7.1 – Graphe de $(3,3)$-isogénies contenant la courbe $y^2 = 3x^5 + 15x^4 + 11x^3 + 3x^2 + 11x + 12$ sur le corps $\mathbb{F}_{19}$

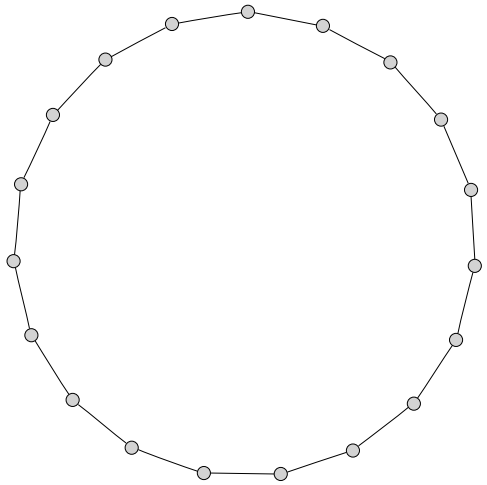


FIGURE 7.2 – Graphe de $(7,7)$-isogénies contenant la courbe $y^2 = 26x^6+21x^5+17x^4+8x^3+22x^2+31x+17$ sur le corps $\mathbb{F}_{41}$

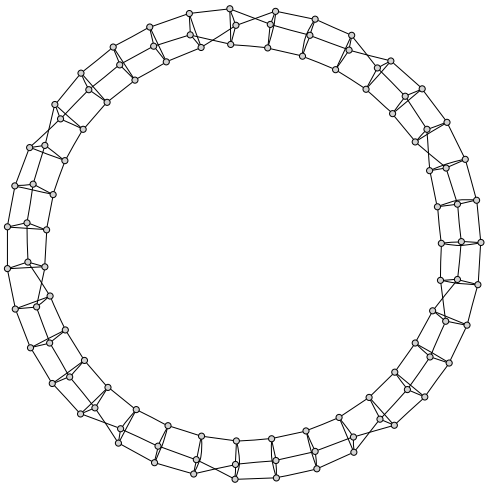


FIGURE 7.3 – Graphe de $(3,3)$-isogénies contenant la courbe $y^2 = 55x^6+29x^5+25x^4+38x^3+56x^2+15x+15$ sur le corps $\mathbb{F}_{61}$

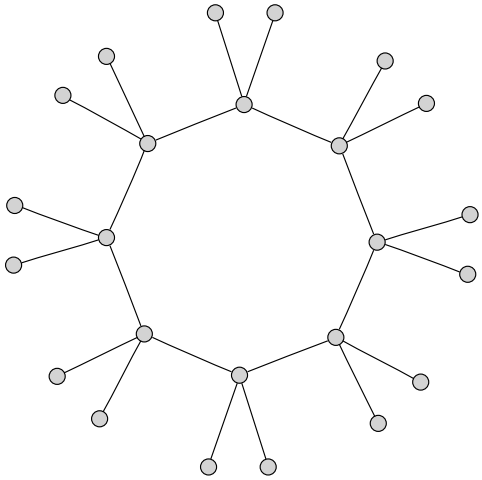


FIGURE 7.4 – Graphe de $(3,3)$-isogénies contenant la courbe $y^2 = 33x^6+7x^5+17x^4+6x^3+52x^2+10x+23$ sur le corps $\mathbb{F}_{61}$

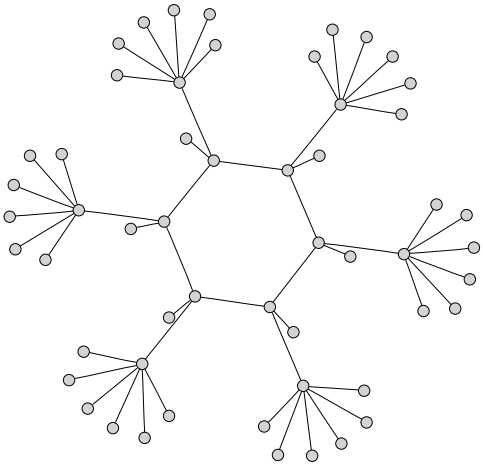
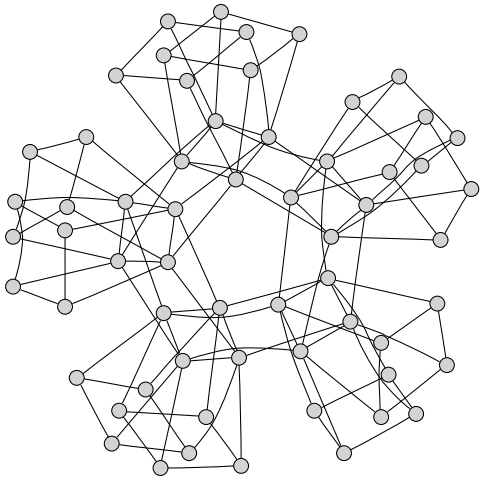


FIGURE 7.5 – Graphe de $(3,3)$-isogénies contenant la courbe $y^2 = 8x^6 + 3x^5 + 7x^4 + 5x^3 + 12x^2 + 5x + 5$ sur le corps $\mathbb{F}_{23}$



Des isogénies verticales apparaissent quand $\ell\mathcal{O}_K$ n'est pas premier au conducteur de $\mathbb{Z}[\pi, \hat{\pi}]$. Il existe une partie du graphe (appelée sommet du volcan dans le cas elliptique) qui correspond aux classes de variétés dont l'anneau d'endomorphismes est l'ordre maximal et aux isogénies horizontales entre ces variétés. Puis nous avons des isogénies qui descendent vers les courbes qui correspondent aux autres ordres. La figure 7.3 ressemble aux cas elliptiques, cependant toutes les branches n'ont pas forcément la même profondeur (figure 7.4).
Par ailleurs, quand ℓ se décompose totalement, nous nous rendons compte en étudiant $\mathfrak{C}(\mathcal{O})$ qu'il peut exister des isogénies entre les courbes ne correspondant pas à l'ordre maximal : figure 7.5.

Perspectives

Au cours de cette thèse nous avons donné quelques pistes de recherche. En particulier à la section 4.5, nous avons expliqué comment rechercher des courbes hyperelliptiques intéressantes pour l'algorithme HECM (c'est-à-dire des courbes décomposables, ayant des thêta constantes de niveau 2 rationnelles, que les paramètres de la surface de Kummer utilisés soient petits et enfin qu'il existe une relation linéaire entre les thêta constantes de niveau 2 de la variété ou de sa variété isogène).

Dans le cadre des formules de Thomae (chapitre 6), il serait intéressant de savoir construire une fraction rationnelle sur la variété $\mathrm{Jac}(\mathcal{C})$ ayant ses zéros et pôles fixés. En effet, nous serions alors capable d'utiliser la formule du lemme 6.1.2 pour obtenir les puissances $2n$-ièmes des thêta constantes de niveau n associées à une courbe hyperelliptique de genre g quelconque.

Dans le cadre du calcul d'isogénies entre courbes hyperelliptiques de genre 2, nous avons expliqué (chapitre 7) comment calculer des (ℓ,ℓ)-isogénies. L'étape suivante est le calcul de $(\ell,1)$-isogénies (et plus généralement de $(\ell,1,\ldots,1)$-isogénies en dimension g). Pour calculer des ℓ-isogénies, nous avons considéré les tores complexes $\mathbb{C}^g/\Lambda_\Omega$. Ces tores sont naturellement munis d'une forme de Riemann c'est-à-dire d'une polarisation. Les fonctions thêta sont également intrinsèquement liées à des polarisations (non principales). Les ℓ-isogénies étudiées au chapitre 7 respectent ces polarisations, or ce n'est pas le cas des $(\ell,1)$-isogénies. Ceci constitue une obstruction pour trouver des formules permettant le calcul de ces isogénies avec les fonctions thêta.

Smith [Smi09] a proposé une méthode permettant d'attaquer le problème du logarithme discret dans la jacobienne d'une courbe de genre 3 hyperelliptique en le transférant, par des isogénies, dans la jacobienne d'une courbe non hyperelliptiques. Les algorithmes permettant de résoudre le problème du logarithme discret dans ce dernier cas nécessitent la connaissance d'une équation de la courbe non hyperelliptique. De ce fait, seules des 2-isogénies sont utilisables ce qui limite le nombre de courbes hyperelliptiques sur lesquelles cette méthode est applicable. On pourrait essayer d'exploiter le calcul de ℓ-isogénies entre variétés abéliennes représentées par les fonctions thêta qui a été présenté au chapitre 7. Par ailleurs, nous avons expliqué comment passer d'une courbe hyperelliptique sous forme de Weierstraß et des coordonnées de Mumford aux fonctions thêta. La brique manquante pour la résolution de ce problème est donc la reconstruction d'une courbe de genre 3 non hyperelliptique à partir des thêta constantes associées. Deux problèmes apparaissent naturellement :

- reconstruire une courbe de genre 3 non hyperelliptique à partir des thêta constantes associées,
- savoir changer de coordonnées (calcul des morphismes).

Une fois ces deux problèmes résolus, nous serions capables de calculer des ℓ-isogénies entre jacobiennes de courbes de genre 3 et donc de généraliser la méthode de Smith.

Dans cette thèse, nous avons utilisé la théorie analytique des fonctions thêta. Le principe de Lefschetz et la théorie de la réduction permettent d'étendre les preuves et les formules aux cas de corps de caractéristiques impaires. Dans le cas de corps de caractéristiques 2, les coordonnées thêta doivent être modifiées (et ce de manière différente suivant le 2-rang de la variété). On pourra consulter [Dia10] pour une description des coordonnées thêta de niveau 2 en genre 2 suivant le 2-rang de la variété. Dans le cas de courbes ordinaires, Gaudry et Lubicz [GL09] ont étudié les formules sur une extension de $\mathbb{Q}_2$. Ils ont désingularisé les équations en 2 avant de réduire les formules. Cette méthode pourrait être utilisée pour obtenir des ℓ-isogénies entre variétés abéliennes ordinaires sur des corps de caractéristique 2 et en particulier dans le cas de courbes hyperelliptiques de genre 2 sur $\mathbb{F}_{2^n}$. Une difficulté est qu'une courbe hyperelliptique sur un tel corps ne peut être mise sous forme de Rosenhain. Cela rend la désingularisation des formules des morphismes plus difficiles à obtenir. Dans [GL09], les auteurs ont expliqué comment

calculer les morphismes en genre 2.

Bibliographie

[ADH94] L. M. Adleman, J. DeMarrais et M.-D. Huang : A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. *In* L. Adleman et M.-D. Huang, éditeurs : *ANTS-I*, volume 877 de *Lecture Notes in Computer Science*, pages 28–40. Springer–Verlag, 1994.

[AKR11] C. Arène, D. Kohel et C. Ritzenthaler : Complete addition laws on abelian varieties. eprint arXiv:1102.2349, Février 2011. http://arxiv.org/abs/1102.2349.

[AM93] A. O. L. Atkin et F. Morain : Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, Janvier 1993.

[Atk92] A. O. L. Atkin : The Number of Points on an Elliptic Curve modulo a Prime. Ensemble d'e-mails à la liste de diffusion `NMBRTHRY`, 1992.

[Bai62] W. L. Baily, Jr. : On the Theory of θ-Functions, the Moduli of Abelian Varieties, and the Moduli of Curves. *Annals of Mathematics. Second Series*, 75(2):342–381, Mars 1962.

[BBL10] D. J. Bernstein, P. Birkner et T. Lange : Starfish on Strike. *In* M. Abdalla et P. Barreto, éditeurs : *Progress in Cryptology – LATINCRYPT 2010*, volume 6212 de *Lecture Notes in Computer Science*, pages 61–80. Springer Berlin / Heidelberg, 2010.

[BBLP10] D. J. Bernstein, P. Birkner, T. Lange et C. Peters : ECM using Edwards curves. Cryptology ePrint Archive, Report 2008/016, Juin 2010. http://eprint.iacr.org/2008/016.

[BC10] É Brier et C. Clavier : New Families of ECM Curves for Cunningham Numbers. *In* Guillaume Hanrot, François Morain et Emmanuel Thomé, éditeurs : *Algorithmic Number Theory*, volume 6197 de *Lecture Notes in Comput. Sci.*, pages 96–109. Springer–Verlag, 2010. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings.

[BF01] D. Boneh et M. K. Franklin : Identity-Based Encryption from the Weil Pairing. *In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK, 2001. Springer–Verlag.

[BGL09] R. Bröker, D. Gruenewald et K. Lauter : Explicit CM-theory in dimension 2. eprint arXiv:0910.1848, Octobre 2009. http://arxiv.org/abs/0910.1848.

[Bir68] B. J. Birch : How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[Bis11] G. Bisson : *Endomorphism rings in cryptography.* Thèse de doctorat, Eindhoven University of Technology, 2011.

[BJ03] O. Billet et M. Joye : The Jacobi Model of an Elliptic Curve and Side-Channel Analysis. *In* M. Fossorier, T. Høholdt et A. Poli, éditeurs : *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 de *Lecture Notes in Computer Science*, pages 34–42. Springer Berlin / Heidelberg, 2003.

[BL04] C. Birkenhake et H. Lange : *Complex abelian varieties*, volume 302 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer–Verlag, Berlin, second édition, 2004.

[BL07] D. J. Bernstein et T. Lange : Faster Addition and Doubling on Elliptic Curves. *In* K. Kurosawa, éditeur : *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 de *Lecture Notes in Computer Science*, pages 29–50. Springer Berlin / Heidelberg, 2007.

[BLS01] D. Boneh, B. Lynn et H. Shacham : Short Signatures from the Weil Pairing. *In* C. Boyd, éditeur : *Advances in Cryptology — ASIACRYPT 2001*, volume 2248 de *Lecture Notes in Computer Science*, pages 514–532. Springer Berlin / Heidelberg, 2001.

[BLS10] R. Bröker, K. Lauter et A.V. Sutherland : Modular polynomials via isogeny volcanoes. eprint arXiv:1001.0402, Janvier 2010. http://arxiv.org/abs/1001.0402.

[Bre86] R. P. Brent : Some integer factorization algorithms using elliptic curves. *Australian Computer Science Communications*, 8:149–163, 1986. Réécrit et appendice ajouté en 1998. http://arxiv.org/abs/1004.3366.

[Bre99] R. P. Brent : Factorization of the tenth and eleventh Fermat numbers. *Mathematics of Computation*, 68(225):429–451, Janvier 1999.

[BS89] E. Bach et J. Shallit : Factoring with cyclotomic polynomials. *Mathematics of Computation*, 52(185):201–219, Janvier 1989.

[BS11] G. Bisson et A. V. Sutherland : Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 131(5):815–831, 2011.

[Bt92] R. P. Brent et H. J. J. te Riele : Factorizations of $a^n \pm 1$, $13 \leq a < 100$. Report nm-r9212, Centrum voor Wiskunde en Informatica, Juin 1992.

[BZ10] R. Brent et P. Zimmermann : *Modern Computer Arithmetic*, volume 18 de *Cambridge Monographs on Applied and Computational Mathematics*. Cambridge University Press, 2010.

[Bă09] R. Bărbulescu : Familles de courbes elliptiques adaptées à la factorisation des entiers, 2009.

[Can87] D. G. Cantor : Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177):95–101, 1987.

[Car06] R. Carls : Canonical coordinates on the canonical lift. eprint arXiv:math/0508007, Juin 2006. http://arxiv.org/abs/math/0508007.

[Car09] R. Carls : Galois theory of the canonical theta structure. eprint arXiv:math/0509092, Novembre 2009. http://arxiv.org/abs/math/0509092.

[CC86] D. V. Chudnovsky et G. V. Chudnovsky : Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986.

[CF05] H. Cohen et G. Frey, éditeurs. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman & Hall / CRC, 2005.

[CH11] W. Castryck et H. Hubrechts : The distribution of the number of points modulo an integer on elliptic curves over finite fields. eprint arXiv:0902.4332, Janvier 2011. http://arxiv.org/abs/0902.4332.

[Cho49] W. L. Chow : On compact complex analytic varieties. *American Journal of Mathematics*, 71:893–914, 1949.

[CKL08] R. Carls, D. Kohel et D. Lubicz : Higher dimensional 3-adic CM construction. *Journal of Algebra*, 319:971–1006, 2008.

[Cos10] R. Cosset : Factorization with genus 2 curves. *Mathematics of Computation*, 79:1191–1208, 2010.

[CR11] R. Cosset et D. Robert : Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. Cryptology ePrint Archive, Report 2011/143, Mars 2011. http://eprint.iacr.org/2011/143.

[CS86] G. Cornell et J. H. Silverman, éditeurs. *Arithmetic Geometry*. Springer–Verlag, 1986.

[Deb94] O. Debarre : The Schottky Problem: An Update. *In* H. Clemens et J. Kollár, éditeurs : *Current Topics in Algebraic Geometry*, volume 28 de *Mathematical Sciences Research Institute Publications*, pages 57–64. Cambridge University Press, 1994.

[DH76] W. Diffie et M. E. Hellman : New directions in cryptography. *IEEE Transactions on Information Theory*, IT–22(6):644–654, Novembre 1976.

[Dia10] O. Diao : *Quelques aspects de l'arithmétique des courbes hyperelliptiques de genre 2*. Thèse de doctorat, Université Rennes 1, Juillet 2010.

[Die06] C. Diem : An index calculus algorithm for plane curves of small degree. *In* S. Pauli F. Hess et M. Pohst, éditeurs : *ANTS-VII*, volume 4076 de *Lecture Notes in Computer Science*, pages 543–557. Springer–Verlag, 2006.

[DL08] I. Dolgachev et D. Lehavi : On isogenous principally polarized abelian surfaces. eprint arXiv:0710.1298, Mars 2008. http://arxiv.org/abs/0710.1298.

[DT08] C. Diem et E. Thomé : Index calculus in class groups of non-hyperelliptic curves of genus three. *Journal of Cryptology*, 21:593–611, 2008.

[Dup06] R. Dupont : *Moyenne arithmético-géométrique, suites de Borchardt et applications*. Thèse de doctorat, École polytechnique, 2006.

[Duq04] S. Duquesne : Montgomery scalar multiplication for genus 2 curves. *In* D. Buell, éditeur : *ANTS-VI*, volume 3076 de *Lecture Notes in Computer Science*, pages 153–168. Springer–Verlag, 2004.

[Duq07] S. Duquesne : Improving the arithmetic of elliptic curve in the Jacobi model. *Information Processing Letters*, 104:101–105, 2007.

[Edw07] H. M. Edwards : A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, Avril 2007.

[EF08] A. Eisenmann et H. Farkas : An Elementary Proof of Thomae's Formulae. *Online Journal of Analytic Combinatorics*, 3, Janvier 2008.

[EGT11] A. Enge, P. Gaudry et E. Thomé : An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves. *Journal of Cryptology*, 24(1):24–41, 2011.

[EJS+07] S. Erickson, M. Jacobson, N. Shang, S. Shen et A. Stein : Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation. *In* Claude Carlet et Berk Sunar, éditeurs : *Arithmetic of Finite Fields*, volume 4547 de *Lecture Notes in Computer Science*, pages 202–218. Springer Berlin / Heidelberg, 2007.

[ElG85] T. ElGamal : A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT–31(4):469–472, Juillet 1985.

[Elk91] N. D. Elkies : Explicit isogenies. Manuscrit, 1991.

[Elk98] N. D. Elkies : Elliptic and modular curves over finite fields and related computational issues. *In* D.A. Buell et J.T. Teitelbaum, éditeurs : *Computational Perspectives on Number Theory*, pages 21–76. AMS/International Press, 1998. Proceedings of a Conference in Honor of A.O.L. Atkin.

[Eng08] A. Enge : Discrete logarithms in curves over finite fields. *In* G. L. Mullen, D. Panario et I. E. Shparlinski, éditeurs : *Eighth International Conference on Finite Fields and Applications - Fq8 Finite Fields and Applications*, volume 461 de *Contemporary Mathematics*, pages 119–139, Melbourne, Australie, 2008. Amer. Math. Soc.

[FJ10] R. Farashahi et M. Joye : Efficient Arithmetic on Hessian Curves. *In* P. Nguyen et D. Pointcheval, éditeurs : *Public Key Cryptography – PKC 2010*, volume 6056 de *Lecture Notes in Computer Science*, pages 243–260. Springer Berlin / Heidelberg, 2010.

[FK80] H.M. Farkas et I. Kra, éditeurs. *Riemann Surfaces*, volume 71 de *Graduate Texts in Mathematics*. Springer–Verlag, 1980.

[FK01] H.M. Farkas et I. Kra, éditeurs. *Theta constants, Riemann surfaces and the modular group*, volume 37 de *Graduate studies in Mathematics*. Amer. Math. Soc., 2001.

[FLR09] J.-C. Faugère, D. Lubicz et D. Robert : Computing modular correspondences for abelian varieties. eprint arXiv:0910.4668, Octobre 2009. http://arxiv.org/abs/0910.4668.

[FM02] M. Fouquet et F. Morain : Isogeny volcanoes and the SEA algorithm. *In* C. Fieker et D. R. Kohel, éditeurs : *Algorihmic Number Theory*, volume 2369 de *Lecture Notes in Computer Science*, pages 276–291. Springer–Verlag, 2002. 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[FR94] G. Frey et H.-G. Rück : A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, Avril 1994.

[Fü07] M. Fürer : Faster integer multiplication. *In Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, STOC '07, pages 57–66, New York, NY, USA, 2007. ACM.

[Gal11] S. Galbraith : Mathematics of Public Key Cryptography. Livre en préparation, 2011.

[Gau00] P. Gaudry : *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* Thèse de doctorat, École Polytechnique, Décembre 2000.

[Gau04] P. Gaudry : Algorithmes de comptage de points d'une courbe définie sur un corps fini. http://www.loria.fr/~gaudry/publis/pano.pdf, 2004.

[Gau07] P. Gaudry : Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1:243–265, 2007.

[Gau09] P. Gaudry : Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic Computation*, 44(12):1690–1702, 2009.

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler et A. Weng : The 2-adic CM method for genus 2 curves with application to cryptography. *In* X. Lai et K. Chen, éditeurs : *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 de *Lecture Notes in Computer Science*, pages 114–129. Springer–Verlag, 2006.

[GHMM08] S. Galbraith, M. Harrison et D. Mireles Morales : Efficient Hyperelliptic Arithmetic Using Balanced Representation for Divisors. *In* Alfred van der Poorten et Andreas Stein, éditeurs : *Algorithmic Number Theory*, volume 5011 de *Lecture Notes in Computer Science*, pages 342–356. Springer Berlin / Heidelberg, 2008.

[GL09] P. Gaudry et D. Lubicz : The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields and Their Applications*, 15:246–260, 2009.

[Gru08] D. Gruenewald : *Explicit Algorithms for Humbert Surfaces.* Thèse de doctorat, University of Sydney, Décembre 2008.

[Gru10] S. Grushevsky : The Schottky problem. eprint arXiv:1009.0369, Septembre 2010. http://arxiv.org/abs/1009.0369.

[GS01] P. Gaudry et É. Schost : On the invariants of the quotients of the Jacobian of a curve of genus 2. *In* S. Boztaş et I. Shparlinski, éditeurs : *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2227 de *Lecture Notes in Computer Science*, pages 373–386. Springer–Verlag, 2001.

[GTTD07] P. Gaudry, E. Thomé, N. Thériault et C. Diem : A double large prime variation for small genus hyperelliptic index calculus. *Mathematics of Computation*, 76:475–492, 2007.

[Har77] R. Hartshorne : *Algebraic Geometry*, volume 52 de *Graduate Texts in Mathematics.* Springer–Verlag, 1977.

[HLP00] E. W. Howe, F. Leprévost et B. Poonen : Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12:315–364, 2000.

[Hon68] T. Honda : Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20(1–2):83–95, 1968.

[How93] E. W. Howe : On the group orders of elliptic curves over finite fields. *Compositio Mathematica*, 85:229–247, 1993.

[How96] E. W. Howe : The Weil pairing and the Hilbert symbol. *Mathematische Annalen*, 305(1):387–392, 1996.

[HSSI99] R. Harasawa, J. Shikata, J. Suzuki et H. Imai : Comparing the MOV and FR Reductions in Elliptic Curve Cryptography. *In* J. Stern, éditeur : *Advances in Cryptology — EUROCRYPT '99*, volume 1592 de *Lecture Notes in Computer Science*, pages 190–205. Springer Berlin / Heidelberg, 1999.

[Hus87] D. Husemöller : *Elliptic curves*, volume 111 de *Graduate Texts in Mathematics*. Springer–Verlag, 1987.

[Igu60] J.-I. Igusa : Arithmetic variety of moduli for genus two. *Annals of Mathematics. Second Series*, 72:612–649, 1960.

[Igu62] J.-I. Igusa : On Siegel modular forms of genus two. *American Journal of Mathematics*, 84:175–200, 1962.

[Igu72] J.-I. Igusa : *Theta functions*, volume 194 de *Grundlehren der mathematischen Wissenschaften*. Springer, 1972.

[Iit81] S. Iitaka : *Algebraic geometry*, volume 76 de *Graduate Texts in Mathematics*. Springer–Verlag, 1981.

[Jou00] A. Joux : A One Round Protocol for Tripartite Diffie–Hellman. *In* W. Bosma, éditeur : *Algorithmic Number Theory*, volume 1838 de *Lecture Notes in Computer Science*, pages 385–393. Springer Berlin / Heidelberg, 2000.

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev et P. Zimmermann : Factorization of a 768-bit rsa modulus. *In Advances in Cryptology – Crypto'2010*, volume 6223 de *Lecture Notes in Computer Science*, pages 333–350. Springer–Verlag, 2010. Proceedings.

[Kem89] G.R. Kempf : Linear systems on abelian varieties. *American Journal of Mathematics*, 111(1):65–94, 1989.

[Kli90] H. Klingen : *Introductory lectures on Siegel modular forms*, volume 20 de *Cambridge studies in advanced mathematics*. Cambridge University Press, 1990.

[Knu81] D. E. Knuth : *The Art of Computer Programming: Seminumerical Algorithms*. Addison-Wesley, 2e edition, 1981.

[Koh96] D. Kohel : *Endomorphism rings of elliptic curves over finite fields*. Thèse de doctorat, University of California, Berkeley, Décembre 1996.

[Koh11] D. Kohel : Addition law structure of elliptic curves. *Journal of Number Theory*, 131(5):894–919, 2011.

[Koi76] S. Koizumi : Theta relations and projective normality of abelian varieties. *American Journal of Mathematics*, pages 865–889, 1976.

[Koi97] S. Koizumi : Remarks on Takase's paper "A generalization of Rosenhain's normal form with an application". *Japan Academy. Proceedings. Series A. Mathematical Sciences*, 73(1):12–13, 1997.

[KP92] A. Krazer et F. Prym : *Neue Grundlagen einer Theorie der allgemeinen Thetafunctionen*. B.G. Teubner, Leipzig, 1892.

[Kru08] A. Kruppa : Factoring into large primes with P-1, P+1 and ECM, 2008. Slides au workshop CADO, disponible à l'adresse http://cado.gforge.inria.fr/workshop/slides/kruppa.pdf.

[Kru10] A. Kruppa : *Speeding up Integer Multiplication and Factorization*. Thèse de doctorat, Université Henri Poincaré - Nancy 1, Janvier 2010.

[KS10] K.S. Kedlaya et A.V. Sutherland : Hyperelliptic curves, l-polynomials, and random matrices. eprint arXiv:0803.4462, Mars 2010. http://arxiv.org/abs/0803.4462.

[Kuh88] R. M. Kuhn : Curves of genus 2 with split jacobian. *Transactions of the American Mathematical Society*, 307(1):41–49, Mai 1988.

[Lan58] S. Lang : Reciprocity and Correspondences. *American Journal of Mathematics*, 80(2):431–440, 1958.

[Lan59] S. Lang : *Abelian varieties*. Numéro 7 de Interscience Tracts in Pure and Applied Mathematics. Interscience Publishers, 1959.

[Lan72] S. Lang : *Introduction to algebraic and abelian functions*. Addison–Wesley, 1972.

[Lan05] T. Lange : Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328, 2005.

[Lau98] L. Laugel : *Oeuvres Mathmatiques de Riemann*. A. Blanchard, 1898.

[Len87] H. W. Lenstra, Jr. : Factoring integers with elliptic curves. *Annals of Mathematics. Second Series*, 126:649–673, 1987.

[Liu02] Q. Liu : *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics, 2002.

[LP92] H. W. Lenstra Jr. et C. Pomerance : A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3):483–516, 1992.

[LPP93] H. W. Lenstra, Jr., J. Pila et C. Pomerance : A hyperelliptic smoothness test, I. *Philos. Trans. Roy. Soc. London Ser. A*, 345:397–408, 1993.

[LPP02] H. W. Lenstra, Jr., J. Pila et C. Pomerance : A hyperelliptic smoothness test, II. *Proc. London Math. Soc.*, 84:105–146, 2002.

[LR85] H. Lange et W. Ruppert : Complete systems of addition laws on abelian variety. *Inventiones Mathematicae*, 79:603–610, 1985.

[LR10a] D. Lubicz et D. Robert : Computing isogenies between abelian varieties. eprint arXiv:1001.2016, Mars 2010. http://arxiv.org/abs/1001.2016.

[LR10b] D. Lubicz et D. Robert : Efficient pairing computation with theta functions. *Algorithmic Number Theory*, 6197, Juillet 2010. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings.

[Mes91] J.-F. Mestre : Construction de courbes de genre 2 à partir de leurs modules. *In* T. Mora et C. Traverso, éditeurs : *Effective methods in algebraic geometry*, volume 94 de *Progress in Mathematics*, pages 313–334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17–21, 1990.

[Mil06] J.S. Milne : *Complex Multiplication*. 2006. http://www.jmilne.org/math/CourseNotes/cm.html.

[Mil08] J.S. Milne : *Abelian varieties*. 2008. http://www.jmilne.org/math/CourseNotes/av.html.

[Mil09] J.S. Milne : *Algebraic Geometry*. 2009. http://www.jmilne.org/math/CourseNotes/ag.html.

[Mon83] P. L. Montgomery : Evaluating recurrences of form $x_{m+n} = f(x_m, x_n, x_{m-n})$ via Lucas chains. Manuscript non publié: ftp://ftp.cwi.nl:/pub/pmontgom/Lucas.ps.gz, 1983.

[Mon87] P. L. Montgomery : Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of Computation*, 48(177):243–264, Janvier 1987.

[Mon92] P. L. Montgomery : *An FFT extension of the Elliptic Curve Method of factorization*. Thèse de doctorat, University of California – Los Angeles, 1992.

[Mon94] P. L. Montgomery : A Survey of Modern Integer Factorization Algorithms. *CWI Quarterly*, 7:337–366, 1994.

[MOV91] A. Menezes, T. Okamoto et S. A. Vanstone : Reducing elliptic curves logarithms to logarithms in a finite field. *In Proc. 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 80–89. ACM Press, 1991. May 6–8, 1991, New Orleans, Louisiana.

[Mum66] D. Mumford : On the Equations Defining Abelian Varieties. I. *Inventiones Mathematicae*, 1:287–354, 1966.

[Mum67a] D. Mumford : On the Equations Defining Abelian Varieties. II. *Inventiones Mathematicae*, 3:75–135, 1967.

[Mum67b] D. Mumford : On the equations defining abelian varieties. III. *Inventiones Mathematicae*, 3:215–244, 1967.

[Mum69] D. Mumford : Varieties defined by quadratic equations. *Questions on Algebraic Varieties (CIME, III Ciclo, Varenna, 1969)*, pages 29–100, 1969.

[Mum70] D. Mumford : *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum83] D. Mumford : *Tata lectures on theta I*, volume 28 de *Progress in Mathematics*. Birkhäuser, 1983.

[Mum84] D. Mumford : *Tata lectures on theta II*, volume 43 de *Progress in Mathematics*. Birkhäuser, 1984.

[Mum91] D. Mumford : *Tata lectures on theta III*, volume 97 de *Progress in Mathematics*. Birkhauser, 1991.

[Odl99] A. Odlyzko : Discrete logarithms: the past and the future. *Designs, Codes, and Cryptography*, 19:129–145, 1999.

[PH78] S. Pohlig et M. E. Hellman : An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, IT–24:106–110, 1978.

[Pol74] J. M. Pollard : Theorems on factorization and primality testing. 76:521–528, 1974.

[Poo94] C. Poor : The Hyperelliptic locus. *Duke Mathematical Journal*, 76(3):809–884, 1994.

[Ric36] F. Richelot : Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes. *Comptes Rendus de l'Académie des Sciences. Série I*, 2:622–627, 1836.

[Ric37] F. Richelot : De transformatione Integralium Abelianorum primiordinis commentation. *Journal fur die Reine und Angewandte Mathematik*, 16:221–341, 1837.

[Rie57] B. Riemann : Theorie des Abelschen Funktionen. *Journal fur die Reine und Angewandte Mathematik*, 54:115, 1857.

[Rob10] D. Robert : *Theta functions and cryptographic applications*. Thèse de doctorat, Université Henri-Poincarré, Nancy 1, France, Juillet 2010.

[Ros95] G. Rosenhain : Abhandlung über die Functionen zweier Variabler mit vier Perioden. *Ostwald's Klassiker der Exacten Wissenschaften*, 65, 1895.

[RSA78] R. L. Rivest, A. Shamir et L. M. Adleman : A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sat00] T. Satoh : The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *Journal of the Ramanujan Mathematical Society*, 15:247–270, 2000.

[Sat01] P. Satgé : Morphismes d'une courbe de genre 2 vers une courbe de genre 1. *In Arithmétique des revêtements algébriques - Actes du colloque de Saint-Étienne*, volume 5 de *Séminaires et Congrès*, pages 133–146. B. Deschamps, 2001.

[Sch88] F. Schottky : Zur Theorie der *Abel*schen Functionen vor vier Variablen. *Journal fur die Reine und Angewandte Mathematik*, 102:304–352, 1888.

[Sch85] R. Schoof : Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[Sch95] R. Schoof : Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[Ser56] J.-P. Serre : Géométrie algébrique et géométrie analytique. *Université de Grenoble. Annales de l'Institut Fourier*, 6:1–42, 1955–1956.

[Ser70] J.-P. Serre : *Cours d'arithmétique*. PUF, 1970.

[Ser89] J.-P. Serre : *Lectures on the Mordell-Weil theorem*. Friedr. Vieweg & Sohn, Braunschweig, 1989. Traduit du français et édité par M. Brown à partir des notes de M. Waldschmidt.

[Sha01] T. Shaska : Curves of genus 2 with (n, n)-split Jacobians. *Journal of Symbolic Computation*, 31:603–617, 2001.

[Sha02] T. Shaska : Genus 2 curves with $(3, 3)$-split Jacobian and large automorphism group. *In ANTS V*, volume 2369 de *Lecture Notes in Computer Science*, pages 100–113. Springer, 2002.

[Sha04] T. Shaska : Genus 2 fields with degree 3 elliptic subfields. *Forum Mathematicum*, 16:263–280, 2004.

[Sha05] T. Shaska : Genus 2 curves covering elliptic curves, a computational approach. *Lecture Notes in Computer Science*, 13:151–195, 2005.

[Shi98] G. Shimura : *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.

[Sil86] J. H. Silverman : *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer–Verlag, 1986.

[Sil94] J. H. Silverman : *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 de *Graduate Texts in Mathematics*. Springer–Verlag, 1994.

[SJ09] F. Schottky et H. Jung : Neue Sätze über Symmetralfunktionen und die Abel'schen Funktionen der Riemann'schen Theorie. *S.-B. Preuss. Akad. Wiss. Berlin; Phys. Math. Kl.*, 1:282–297, 1909.

[Smi09] B. Smith : Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves. *Journal of Cryptology*, 22(4):505–529, Février 2009.

[Sti93] H. Stichtenoth : *Algebraic function fields and codes*. Springer–Verlag, 1993.

[Str10] M. Streng : *Complex multiplication of abelian surfaces*. Thèse de doctorat, Universiteit Leiden, 2010.

[Sut11] A.V. Sutherland : Computing Hilbert class polynomials with the Chinese remainder theorem. *Mathematics of Computation*, 80:501–538, 2011.

[Suy85] H. Suyama : Informal preliminary report (8). Letter to Richard P. Brent, 25 octobre 1985.

[Tak96] K. Takase : A Generalization of Rosenhain's Normal Form for Hyperelliptic Curves with an Application. *Japan Academy. Proceedings. Series A. Mathematical Sciences*, 72(7):162–165, 1996.

[Tat66] J. Tate : Endomorphisms of Abelian varieties over finite fields. *Inventiones Mathematicae*, 2:134–144, 1966.

[Tho70] J. Thomae : Beitrag zur Bestimmung von $\theta\,(0, 0, \ldots 0)$ durch die Klassbmoduln agebraischer Functionnen. *Journal fur die Reine und Angewandte Mathematik*, 70:201–222, 1870.

[Tho73] J. Thomae : Darstellung des Quotienten zweier Thetafunctionen, deren Argumente sich um Drittel ganzer Periodicitätsmoduln unterscheiden, durch algebraische Fiunctionen. *Mathematische Annalen*, 6:603–612, 1873.

[vdGM07] G. van der Geer et B. Moonen : Abelian varieties. Livre en préparation, 2007.

[Vél71] J. Vélu : Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences. Série A*, 273:238–241, Juillet 1971.

[vW98] P. van Wamelen : Equations for the Jacobian of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 350(8):3083–3106, 1998.

[Wei64] A. Weil : Sur certains groupes d'opérateurs unitaires. *Acta Mathematica*, 111(1):143–211, 1964.

[Wen03] A. Weng : Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72:435–458, 2003.

[Wil82] H. C. Williams : A $p+1$ Method of Factoring. *Mathematics of Computation*, 39(159):225–234, Juillet 1982.

[Yos73] H. Yoshida : On an analogue of the Sato conjecture. *Inventiones Mathematicae*, 19(4):261–277, 1973.

[Zar28] O. Zariski : On Hyperelliptic θ-Functions with Rational Characteristics. *American Journal of Mathematics*, 50(3):315–344, Juillet 1928.

[ZD06] P. Zimmermann et B. Dodson : 20 years of ECM. *In ANTS VII*, volume 4076 de *Lecture Notes in Computer Science*, pages 525–542. Springer–Verlag, 2006.

Résumé

Depuis le milieu des années 1980, les variétés abéliennes ont été abondamment utilisées en cryptographie à clé publique: le problème du logarithme discret et les protocoles qui s'appuient sur celles-ci permettent le chiffrement asymétrique, la signature, l'authentification. Dans cette perspective, les jacobiennes de courbes hyperelliptiques constituent l'un des exemples les plus intéressants de variétés abéliennes principalement polarisées.

L'utilisation des fonctions thêta permet d'avoir des algorithmes efficaces sur ces variétés. En particulier nous proposons dans cette thèse une variante de l'algorithme ECM utilisant les jacobiennes de courbes de genre 2 décomposables. Par ailleurs, nous étudions les correspondances entre les coordonnées de Mumford et les fonctions thêta. Ce travail a permis la construction de lois d'additions complètes en genre 2. Finalement nous présentons un algorithme de calcul d'isogénies entre variétés abéliennes.

La majorité des résultats de cette thèse sont valides pour des courbes hyperelliptiques de genre quelconque. Nous nous sommes cependant concentré sur le cas du genre 2, le plus intéressant en pratique. Ces résultats ont été implémentés dans un package Magma appelé AVIsogenies.

Mots-clés: Cryptographie, courbes hyperelliptiques, variétés abéliennes, fonctions thêta, factorisation, isogénies

Abstract

Since the mid 1980's, abelian varieties have been widely used in cryptography: the discrete logarithm problem and the protocols that rely on it allow asymmetric encryption, signatures, authentification... For cryptographic applications, one of the most interesting examples of principally polarized abelian varieties is given by the Jacobians of hyperelliptic curves.

The theory of theta functions provides efficient algorithms to compute with abelian varieties. In particular, using decomposable curves of genus 2, we present a generalization of the ECM algorithm. In this thesis, we also study the correspondences between Mumford coordinates and theta functions. This led to the construction of complete addition laws in genus 2. Finally we present an algorithm to compute isogenies between abelian varieties.

Most of the results of this thesis are valid for hyperelliptic curves of arbitrary genus. More specifically we emphasize on genus 2 hyperelliptic curves, which is the most relevant case in cryptography. These results have been implemented in a Magma package called AVIsogenies.

Keywords: Cryptography, hyperelliptic curves, abelian varieties, theta functions, factorization, isogenies