Fonctions thêta et applications à la cryptographie

Damien Robert

Département de formation doctorale en informatique. École doctorale IAEM Lorraine.
UFR STMIA

Fonctions thêta et applications à la cryptographie

Theta functions and cryptographic applications

THÈSE

présentée et soutenue publiquement le 21 juillet 2010

pour l'obtention du

Doctorat de l'université Henri Poincaré — Nancy 1
(spécialité informatique)

par

Damien Robert

Rapporteurs :

Antoine Chambert-Loir	Prof. Univ. Rennes 1
Kristin Lauter	Microsoft Research

Composition du jury :

Guillaume Hanrot	Prof. ÉNS de Lyon	(directeur)
Jean-Marc Couveignes	Prof. Univ. Toulouse 2	
Didier Galmiche	Prof. Univ. Nancy 1	
Pierrick Gaudry	CR CNRS (LORIA)	
David Kohel	Prof. Univ. Méditerranée	
Kristin Lauter	Microsoft Research	(rapporteur)
François Morain	Prof. École Polytechnique	(président)
Sylvain Petitjean	DR INRIA (LORIA)	(référent)

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

FONCTIONS THÊTA ET APPLICATIONS À LA CRYPTOGRAPHIE

DAMIEN ROBERT

Thèse d'informatique

Juillet 2010

À mes parents.

À ma petite coccinelle.

RÉSUMÉ

Le logarithme discret sur les courbes elliptiques fournit la panoplie standard de la cryptographie à clé publique : chiffrement asymétrique, signature, authentification. Son extension à des courbes hyperelliptiques de genre supérieur se heurte à la difficulté de construire de telles courbes qui soient sécurisées.

Dans cette thèse nous utilisons la théorie des fonctions thêta développée par MUMFORD pour construire des algorithmes efficaces pour manipuler les variétés abéliennes. En particulier nous donnons une généralisation complète des formules de Vélu sur les courbes elliptiques pour le calcul d'isogénie sur des variétés abéliennes. Nous donnons également un nouvel algorithme pour le calcul efficace de couplage sur les variétés abéliennes en utilisant les coordonnées thêta. Enfin, nous présentons une méthode de compression des coordonnées pour améliorer l'arithmétique sur les coordonnées thêta de grand niveau. Ces applications découlent d'une analyse fine des formules d'addition sur les fonctions thêta.

Si les résultats de cette thèse sont valables pour toute variété abélienne, pour les applications nous nous concentrons surtout sur les Jacobiennes de courbes hyperelliptiques de genre 2, qui est le cas le plus significatif cryptographiquement.

ABSTRACT

The discrete logarithm on elliptic curves gives the standard protocols in public key cryptography: asymmetric encryption, signatures, zero-knowledge authentification. To extend the discrete logarithm to hyperelliptic curves of higher genus we need efficient methods to generate secure curves.

The aim of this thesis is to give new algorithms to compute with abelian varieties. For this we use the theory of algebraic theta functions in the framework of MUMFORD. In particular, we give a full generalization of Vélu's formulas for the computation of isogenies on abelian varieties. We also give a new algorithm for the computation of pairings using theta coordinates. Finally we present a point compression method to manipulate more efficiently theta coordinates of high level. These applications follow from the analysis of Riemann relations on theta functions for the addition law.

Whereas the results of this thesis are valid for any abelian variety, for the applications a special emphasis is given to Jacobians of hyperelliptic genus 2 curves, since they are the most significantly relevant case in cryptography.

Mots clefs : Cryptographie, courbes hyperelliptiques, variétés abéliennes, isogénies, couplage, fonctions thêta

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

PUBLICATIONS

Quelques idées et figures de cette thèse sont reprises des publications suivantes :

1. J.-C. Faugère, D. Lubicz et D. Robert. *Computing modular correspondences for abelian varieties*. Mai 2009. arXiv : 0910.4668
2. D. Lubicz et D. Robert. *Computing isogenies between abelian varieties*. Jan. 2010. arXiv : 1001.2016
3. D. Lubicz et D. Robert. *Efficient pairing computation with theta functions*. Sous la dir. de G. Hanrot, F. Morain et E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Jan. 2010. URL : http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf

REMERCIEMENTS

We have seen that computer programming is an art,
because it applies accumulated knowledge to the world,
because it requires skill and ingenuity, and especially
because it produces objects of beauty.

— Donald E. Knuth [Knu74]

A word of warning — and apology. There are several thousand formulas in this paper which allow one or more *''sign-like ambiguities'': i.e., alternate and symmetric but non-equivalent reformulations. [...] I have made a superhuman effort to achieve consistency and even to make* correct *statements: but I still cannot guarantee the result.*

— David Mumford "On the equations defining abelian varieties."

```
$ { IFS='
'; for i in `cat acknowledgements.txt`; do
  printf '%s\a%s\n' `printf "$i" | sha256sum` "$i";
done } | sort | cut -d `printf '\a'` -f 2 > acknowledgements.tex
```

Il y a bien sûr tous les membres de l'équipe Cacao/Caramel ! Son chef grand, beau, fort et surtout chevelu [1], Pierrick Gaudry, qui a toujours réponse à mes questions stupides ; Emmanuel Thomé entre autres pour ses conseils Unixiens et TEXniques, ainsi que Jérémie Detrey pour toutes les explications sur les détails d'implémentation des couplages. De même, je remercie vivement les membres du jury, qui ont accepté de venir malgré la date peu pratique, et en particulier François Morain qui m'a fait l'honneur de présider. Je remercie aussi très vivement Jean-François Mestre pour ses nombreuses questions, ses conseils et ses remarques. Les rapporteurs Kristin Lauter et Antoine Chambert-Loir m'ont fait l'honneur d'accepter de rapporter cette thèse, qui est bien plus longue que ce que je n'espérais. Malgré cela, ils ont effectué un travail en tout point remarquable. Avant tout, je souhaite remercier mon directeur de thèse, Guillaume Hanrot, qui m'a accueilli à Nancy, et a toujours su prendre du temps pour moi. La clarté de ses explications scientifiques, ses conseils avisés, et ses qualités humaines [2] en font un directeur en tout point remarquable. Je remercie également les « jeunes [3] » : Romain Cosset et Gaëtan Bisson pour les remarques et rapports de bug sur mon programme de calcul d'isogénies.

Bien sûr, une thèse ne se limite pas seulement au travail scientifique, et je devrais remercier tous les gens qui m'ont encadré pour mon monitorat, Monique Grandbastien, Lofti Bellalem, Marion Videau et Pierrick Gaudry, ainsi que l'ensemble des personnels administratifs qui simplifient considérablement la vie d'un thésard. Je m'excuse auprès de toutes les personnes que je n'ai pas citées, je ne vous ai pas oubliés !

Les remerciements sont la partie la plus importante d'une thèse (car la plus lue), mais je ne suis pas très fort pour cet exercice…Je préfère faire preuve de ma gratitude à l'oral plutôt qu'à

1. Hum, ça risque de se voir… 2. et culinaires [a] !
3. Je ne citerai pas Nicolas Estibals qui est tellement jeune qu'il fait plutôt partie de la catégorie des bambins…

a. J'espère que j'aurai le droit à une tarte au citron après ma soutenance !

l'écrit, et vous ne trouverez ici qu'un ensemble minimal[1] de remerciements, sur des critères purement scientifiques.

Je tiens également à remercier mes co-auteurs, notamment David Lubicz, qui m'a appris la théorie algébrique des fonctions thêta, et avec qui j'ai eu une collaboration fructueuse. Son enthousiasme communicatif a été une grande source d'inspiration. Enfin, je remercie de tout mon cœur Blandine pour avoir relu attentivement ma thèse !

1. Son existence et unicité sont laissées en exercice au lecteur. Indice : considérer la catégorie duale de l'ensemble des critiques, auquel on applique l'opérateur de Bisson–Brisebarre.

CONVENTIONS TYPOGRAPHIQUES

Le corps du texte est en sérif. J'utilise des notes de marge pour apporter des précisions. *Comme celle-ci* Les notes de bas de page[1] servent à apporter des précisions plus longues. Les incises sont typographiées avec des doubles parenthèses ((ce qui doit être une hérésie typographique…)). Enfin, il m'arrivera de faire des commentaires que l'on pourra sauter en première lecture, ils sont représentés par une police plus petite :

> Tant qu'à parler d'hérésie typographique, j'ai pris une largeur de texte bien supérieure à celle recommandée par Bringhurst [Bri02].

Cette thèse a été produite à l'aide de LaTeX, de la classe KOMA-Script et l'aide de nombreux packages, notamment biber/biblatex, booktabs, cleveref, hyperref, marginnote, mathtools, microtype, ntheorem, tikz. Le style est repris des packages ClassicThesis [Mie07] et ArsClassica [Pan09].

RÉFÉRENCES

[Bri02] R. Bringhurst. *The Elements of Typographic Style*. Version 2.5. Point Roberts, WA, USA : Hartley & Marks, Publishers, 2002. (Cf. p. xi).

[Knu74] D. E. Knuth. « Computer Programming as an Art ». Dans : *Communications of the ACM* 17.12 (déc. 1974), p. 667–673. (Cf. p. ix).

[Mie07] A. Miede. *A Classic Thesis style*. http://www.ctan.org/tex-archive/macros/latex/contrib/classicthesis/ClassicThesis.pdf. 2007. (Cf. p. xi).

[Pan09] L. Pantieri. *Ars Classica*. http://www.ctan.org/tex-archive/macros/latex/contrib/arsclassica/. 2009. (Cf. p. xi).

1. J'utilise le package `bigfoot` pour optimiser l'apparence de ces notes.

TABLE DES MATIÈRES

LISTE DES ALGORITHMES

LISTE DES EXEMPLES ALGORITHMIQUES

LISTE DES FIGURES

LISTE DES TABLEAUX

1 VARIÉTÉS ABÉLIENNES ET CRYPTOGRAPHIE

MATIÈRES

1.1 INTRODUCTION

Dans l'usage moderne de la cryptographie [DH76], la cryptographie à clé publique basée sur le protocole RSA [RSA78] occupe une place prépondérante. Cependant, l'augmentation des puissances de calcul et l'amélioration des attaques contre RSA [CDL+00 ; KAF+10] rendent le besoin d'alternatives prégnant. Or les courbes elliptiques et les variétés abéliennes de dimension 2 permettent d'avoir des niveaux de sécurité équivalent à taille de clé et coût calculatoire bien moindre. De plus, l'existence d'une forme bilinéaire naturelle (pairing) sur ces structures permet des constructions cryptographiques avancées de plus en plus utilisées chez les constructeurs de protocoles.

L'algorithmique des courbes elliptiques sur les corps finis a été étudiée en profondeur : on dispose d'une arithmétique rapide [BBJ+08], on sait calculer efficacement les isogénies, les polynômes de classes de Hilbert, les anneaux d'endomorphismes, et on dispose d'algorithmes efficaces de comptage de points. En revanche, il n'en va pas de même des variétés abéliennes de dimension 2 : si l'arithmétique a été relativement étudiée [Lan05 ; Gau07], les algorithmes plus avancés (comme le calcul d'isogénies, des anneaux d'endomorphismes, ou le comptage de point en grande caractéristique) sont bien plus lents que leurs contreparties sur les courbes elliptiques. De plus, l'utilisation des pairings peut faire intervenir des variétés abéliennes de dimension supérieure (pour des raisons d'efficacité ou pour avoir plus de liberté dans la conception de protocoles).

Le but de cette thèse est de proposer des améliorations à certains de ces algorithmes, pour des variétés abéliennes de dimensions quelconques. Notre stratégie est d'utiliser les fonctions thêta, qui constituent un (des) système(s) de coordonnées canoniques sur les variétés abéliennes. Ces fonctions thêta sont souvent négligées algorithmiquement en raison de la grande dimension de l'espace dans lequel elles plongent la variété. Cependant, Gaudry a montré dans [Gau07] que les fonctions thêta de petit niveau permettaient de disposer d'une arithmétique efficace sur les variétés abéliennes de petite dimension. De plus, nous montrerons que le calcul d'isogénies et le calcul de couplages se décrivent très naturellement dans ce langage, et expliquerons

comment éviter le problème de la dimension de l'espace ambiant en introduisant un système de coordonnées compressées n'utilisant qu'un (petit) sous-ensemble de toutes les fonctions thêta.

La structure de la thèse est la suivante. Les chapitres 2 et 3 introduisent les fonctions thêta sur les variétés abéliennes. Le chapitre 4 introduit les coordonnées thêta compressées. Ce chapitre explique également comment utiliser ces coordonnées compressées pour calculer efficacement l'arithmétique grâce aux fonctions thêta, généralisant les résultats de [Gau07] à tout niveau. Les applications de la première partie seront présentées dans la seconde partie : le chapitre 5 donne un algorithme de calcul de pairings, le chapitre 6 une correspondance modulaire et le chapitre 7 un algorithme de calcul explicite d'isogénies généralisant les formules de Vélu à toute variété abélienne. L'un des objectifs de cette thèse est d'améliorer la compétitivité des (Jacobiennes de) courbes de genre 2 par rapport au genre 1. À ce titre, nous illustrerons souvent nos études de complexité par des exemples plus détaillés en genre 2 (ainsi qu'en genre 1 à titre de comparaison). Cependant, une conséquence d'utiliser les fonctions thêta est que nos résultats sont valables pour des (Jacobiennes de) courbes de genres quelconques, et même pour toutes variétés abéliennes. En particulier, les résultats de cette thèse permettent également d'améliorer les applications cryptographiques offertes par les courbes de genre $g \geqslant 3$ petit ($g = 3$ et $g = 4$), qui sont également intéressantes notamment dans le cadre des pairings (voir la section 1.3.1).

Le présent chapitre donne une courte présentation des variétés abéliennes, et de leur usage en cryptographie. La section 1.2 donne un aperçu des applications en cryptographie à clé publique du logarithme discret dans un groupe cyclique. La section 1.3 introduit les variétés abéliennes, qui constituent le réservoir usuel des groupes abéliens utilisés pour le logarithme discret en cryptographie. La section 1.3.3 présente, en particulier, les applications du pairing sur les variétés abéliennes, qui ont ouvert de nombreux horizons en cryptographie à clé publique. La section 1.4 introduit la notion d'isogénies, qui est un concept central pour l'étude des variétés abéliennes. Le calcul d'isogénies est une brique de base de nombreux algorithmes de calcul formel sur les variétés abéliennes, mais n'était explicite qu'en dimension 1, sur les courbes elliptiques. Dans cette section on regarde d'où vient la difficulté de généraliser la construction explicite d'isogénies, et on explique pourquoi les fonctions thêta, introduites dans la section 1.5, sont de bonnes candidates pour résoudre ces difficultés. Enfin, un plan détaillé de la thèse sera présenté dans la section 1.6.

1.2 LOGARITHME DISCRET ET CRYPTOGRAPHIE

DÉFINITION 1.2.1. Soit G un groupe abélien fini, $g \in G$ un élément du groupe d'ordre n, et $y \in \langle g \rangle$. On note $\log_g(y)$ l'élément $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $y = g^x$. C'est le logarithme de y en base g. ◇

Si l'exponentielle dans un groupe est facile à calculer (pour $g \in G$, g^m peut se calculer en $O(\log(m))$ opérations dans G), le logarithme discret est plus compliqué [Sho97] :

THÉORÈME 1.2.2. *Si $G = \langle g \rangle$ est un groupe cyclique* générique *d'ordre n, alors le coût de calcul du logarithme discret est en $\widetilde{\Omega}(\sqrt{p})$ où p est le plus grand nombre premier divisant n, et la notation $\widetilde{\Omega}$ signifie que l'on néglige les facteurs logarithmiques.*

L'algorithme « pas de bébés, pas de géants » (ou l'algorithme ρ de Pollard, qui a une empreinte mémoire en $O(\log(n))$ au prix de la perte du déterminisme de l'algorithme) combiné

à la méthode de Pohlig-Hellmann [PH78] permet d'atteindre la borne donnée dans le théorème 1.2.2. Il faut faire attention au fait que le théorème 1.2.2 ne s'applique qu'à des groupes *génériques*, c'est-à-dire lorsqu'on se restreint uniquement aux opérations de groupe dans G. Autrement dit, même si tous les groupes cycliques d'ordre n sont isomorphes, la complexité du logarithme discret dans G dépend énormément de la représentation utilisée pour G. Donnons quelques exemples :

- Si $G = (\mathbb{Z}/n\mathbb{Z}, +)$, le logarithme discret est trivialement donné par l'algorithme d'Euclide étendu.
- Si $G = \mathbb{F}_q^*$, le groupe des éléments inversibles d'un corps fini, on peut adapter les idées de crible [LLMP93 ; BLP93] utilisées pour la factorisation des entiers, pour obtenir un algorithme sous-exponentiel (appelé algorithme du calcul d'index) [Pom87 ; AD93 ; Gor93]. On peut également consulter [EG02] pour une description générale de l'algorithme du calcul d'index pour attaquer le logarithme discret dans un groupe G admettant une « base de facteurs » (et qui s'applique notamment aux groupes de classe).
- Si $G = J_C(\mathbb{F}_q)$ est le groupe des points rationnels de la Jacobienne d'une courbe $C_{\mathbb{F}_q}$ sur $\mathbb{F}_q$, alors suivant le genre de $C_{\mathbb{F}_q}$ et sa nature (courbe hyperelliptique, plane), l'algorithme du calcul d'index peut être plus rapide que l'algorithme générique du théorème 1.2.2 (voir la section 1.3.2).

Ainsi l'application exponentielle dans un groupe *générique* est une *fonction à sens unique*. On peut donc l'utiliser pour toute la panoplie standard de la cryptographie à clé publique :

- chiffrement asymétrique ;
- signature ;
- authentification ''Zero-Knowledge''.

De plus, la structure sous-jacente de groupe permet d'implémenter ces algorithmes efficacement, par exemple la majeure partie du chiffrement revient à calculer une exponentiation dans G.

Donnons un exemple d'application (protocole d'échange de clé de Diffie-Hellman) : supposons qu'Alice et Bob veulent communiquer à travers un canal non sûr. Ils veulent échanger une clé commune pour utiliser l'algorithme de chiffrement symétrique `AES 256`. Ils se mettent d'accord sur un groupe cyclique $G = \langle g \rangle$ *générique* de cardinal premier p, où p fait 512 bits. Alice choisit un entier $a \in \mathbb{Z}$, et communique à Bob l'élément g^a. De même, Bob choisit un entier $b \in \mathbb{Z}$, et communique à Alice l'élément g^b. Alice et Bob peuvent alors calculer g^{ab}, ce sera leur clé secrète commune. En revanche, un attaquant Ève doit reconstituer g^{ab} à partir de g^a et g^b, on appelle cela le problème de « Diffie-Helmann calculatoire ». En pratique l'algorithme le plus efficace (dans un groupe générique) consiste à calculer le logarithme discret de g^a ou g^b [MW99].

1.3 VARIÉTÉS ABÉLIENNES

1.3.1 *Logarithme discret sur les variétés abéliennes*

À partir de maintenant nous notons la loi de groupe additivement, et donc l'opération de base pour chiffrer un message est la multiplication par un scalaire.

On a vu que pour le logarithme discret, prendre pour G le groupe multiplicatif d'un corps était sujet aux mêmes attaques sous exponentielles que pour RSA. KOBLITZ a proposé dans [Kob87] de prendre pour G le groupe des points d'une courbe elliptique (donnant lieu à ECC : ''elliptic curve cryptography''), puis a généralisé cette construction dans [Kob89] au cas de la Jacobienne d'une courbe hyperelliptique. Plus généralement, on peut considérer pour G l'ensemble des points d'un groupe algébrique projectif connexe (pour avoir une loi commutative), c'est ce que l'on appelle une variété abélienne. L'avantage de la cryptographie

AES	RSA	ECC
72	1008	144
80	1248	160
96	1776	192
112	2432	224
128	3248	256
256	15424	512

TABLE 1.1 – Comparaison de la taille des clés entre RSA et ECC

basée sur les courbes elliptiques est que l'arithmétique y est rapide, ce qui permet de chiffrer et déchiffrer rapidement un message, alors que la meilleure attaque connue contre le logarithme discret reste l'attaque générique (sauf pour certaines classes de courbes, voir par exemple [Gau08]).

On peut trouver dans `http://www.keylength.com` une comparaison (basée entre autres sur les rapports ECRYPT [Sma09]) des tailles de clé nécessaires pour atteindre une sécurité donnée. Les résultats sont résumés dans le tableau 1.1 (pour AES on recense la taille de la clé en bits, pour RSA la taille du module $N = pq$, et pour ECC la taille du corps sur lequel on travaille). On voit qu'au-delà d'un seuil de sécurité, ECC devient bien plus avantageux que RSA. D'ailleurs, dans sa « suite B », la NSA recommande d'utiliser ECC [NSA09]. ((Le seuil à partir duquel ECC devient plus avantageux que RSA dépend des usages. Par exemple, avec un exposant e petit, le chiffrement et la vérification de signature peuvent rester rapides avec RSA, même avec un module N gros. En pratique, le seuil se situe aux alentours de 80 bits de sécurité, voire beaucoup moins pour les systèmes embarqués.))

Si C est une courbe lisse (projective et géométriquement irréductible) de genre g sur un corps fini $\mathbb{F}_q$, sa Jacobienne J (voir la section 1.3.2) est une variété abélienne, et on peut utiliser pour le logarithme discret le groupe $G = J(\mathbb{F}_q)$ des points rationnels de J. Si $g = 1$, on retrouve le cas des courbes elliptiques. WEIL a démontré [Wei49 ; Wei48] (c'est un cas particulier des conjectures de Weil [Har00, Appendice C]) que $\#G \in [(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$, et donc est de l'ordre de q^g. Ainsi, si l'on arrive à générer efficacement des courbes de genre g telles que le cardinal (des points rationnels) de la Jacobienne est un nombre premier (ou a un petit cofacteur), le coût du logarithme discret via l'attaque générique est en $\widetilde{O}(q^{g/2})$. Cependant, lorsque $g \geqslant 3$, on connaît des attaques plus rapides que l'attaque générique (voir la section 1.3.2). En revanche en genre 2, comme pour les courbes elliptiques, la meilleure attaque connue reste l'attaque générique. Ainsi à niveau de sécurité égal, on peut travailler avec une courbe hyperelliptique de genre 2 dans un corps deux fois plus petit que pour une courbe elliptique. En fonction de l'efficacité de l'arithmétique sur (la Jacobienne d') une telle courbe, le genre 2 peut se révéler plus intéressant en cryptographie que le genre 1. Il s'avère que dans certaines situations, en utilisant l'arithmétique efficace due à la formule de duplication sur les fonctions thêta [Gau07], c'est effectivement le cas ; pour une comparaison détaillée entre le genre 1 et le genre 2, on peut consulter [Ber06 ; Lan06 ; BL07a].

Toute courbe lisse de genre 2 est hyperelliptique.

Enfin, on dispose sur les courbes elliptiques de pairings efficaces à calculer (le pairing de Weil, ainsi que le pairing de Tate ou des versions optimisées du pairing de Tate). Ces pairings peuvent être utilisées à des fins destructrices, puisqu'ils permettent de transférer le problème du logarithme discret d'une courbe elliptique sur $\mathbb{F}_q$, à un problème de logarithme discret dans le groupe multiplicatif $\mathbb{F}_{q^d}^*$, où d est l'embedding degree. Or il s'avère que les courbes elliptiques supersingulières, qui étaient utilisées au début de ECC puisqu'elles disposent d'une arithmétique très efficace, ont un embedding degree très petit ($d = 2, 3, 4$ ou 6 par [RS09]).

Ceci donne une attaque sur ces courbes (surtout lorsque $g = 2$) puisque le logarithme discret dans le groupe multiplicatif d'un corps fini se fait en temps sous-exponentiel. C'est le principe de l'attaque MOV [MOV91]. Cependant, les pairings sont aussi utilisés à des fins constructives, en donnant des nouveaux outils pour les protocoles cryptographiques (c'est ce qu'on appelle la ''pairing based cryptography'', on donne des exemples dans la section 1.3.3). Il y a alors deux stratégies possible pour une implémentation efficace des pairings (à une sécurité fixée). On peut utiliser des courbes elliptiques ordinaires, avec un embedding degree d calibré pour que la sécurité sur la courbe soit équivalente à la sécurité sur $\mathbb{F}_{q^d}^*$. L'autre méthode est d'utiliser des courbes elliptiques supersingulières (avec $d = 6$) afin de profiter de leur arithmétique rapide, en prenant q assez grand pour que la sécurité sur $\mathbb{F}_{q^d}^*$ soit suffisante [PSV06 ; Men07].

Or le pairing de Weil (et de Tate) existe pour toute variété abélienne, et on sait le calculer efficacement grâce à l'algorithme de Miller [Mil04] sur des Jacobiennes de courbes hyperelliptiques. Comme le calcul d'index sur les variétés abéliennes de petite dimension reste exponentiel, RUBIN et SILVERBERG ont eu l'idée de considérer des variétés abéliennes supersingulières dans [RS09]. En effet, ceci permet d'obtenir des embedding degrees plus élevés, ce qui permet de travailler sur des corps bien plus petits. Dans la comparaison entre ECC et HECC, on a vu que passer d'une courbe elliptique à une courbe hyperelliptique de genre g permettait de gagner un facteur g sur la taille de q, facteur qui n'est pas compensé par l'augmentation du coût de la multiplication par un scalaire, à part éventuellement en genre 2, surtout que lorsque $g \geqslant 3$ les algorithmes de calcul d'index font que l'on ne gagne pas un facteur g dans ces cas-là. La situation avec le couplage est très différente, comme la sécurité sur une courbe elliptique supersingulière est sous-exponentielle, le passage à des variétés abéliennes supersingulières de dimensions supérieures (et surtout avec des embedding degree plus grands) permet d'être plus efficace. En particulier, pour $g \leqslant 6$, la situation optimale est atteinte sur des variétés abéliennes supersingulières de dimension 4 [RS09, Tableau 1].

1.3.2 *Variétés abéliennes, Jacobiennes de courbes*

DÉFINITION 1.3.1. Une variété abélienne sur un corps k parfait est un groupe algébrique sur k complet et connexe. ◇

On peut montrer que toute variété abélienne est projective, donc de manière plus terre à terre une variété abélienne est un ensemble de points (géométriques) dans un espace projectif donnés par les zéros communs d'un ensemble de polynômes homogènes, sur lesquels on a une loi de groupe, donnée par une application algébrique.

On peut montrer qu'une telle loi de groupe est forcément abélienne [Mum70, p. 41]. De façon générale, une variété abélienne est un objet extrêmement rigide [Mum70, p. 43-45 ; BL04, Section 4.9]. Par exemple, la loi de groupe sur une variété abélienne A_k est entièrement déterminée par le choix d'un point base $0 \in A_k(\overline{k})$ [Mum70, Corollaire 1 p. 43].

Une classe importante de variétés abéliennes est donnée par les Jacobiennes de courbes. Soit C_k une courbe projective lisse et irréductible sur un corps k. Alors le groupe de Picard $\mathrm{Pic}(C_k)$ est représenté par une variété abélienne, que l'on appelle la Jacobienne J de la courbe C_k. Concrètement, on peut décrire ce groupe ainsi : le groupe (abélien) libre engendré par les points géométriques de C_k est appelé le groupe des diviseurs sur C_k. Formellement un diviseur D est une somme formelle $D = \sum_{x \in C_k(\overline{k})} n_x x$, où chaque $n_x \in \mathbb{Z}$ et la famille $(n_x)_{x \in C_k(\overline{k})}$ est à support fini. À un tel diviseur, on associe son degré $\deg D = \sum_{x \in C_k(\overline{k})} n_x$. Si f est une fonction rationnelle sur $C_{\overline{k}}$, on peut lui associer un diviseur (f) comme étant la somme des zéros et pôles avec multiplicité de f. On dit que deux diviseurs D et D' sont équivalents s'il existe

On note $C_{\overline{k}}$ le changement de base de C_k par le morphisme $\mathrm{Spec}\,\overline{k} \to \mathrm{Spec}\,k$.

une telle fonction rationnelle qui satisfait $(f) = D - D'$. Un diviseur (f) est de degré 0, donc l'application degré descend aux classes d'équivalences des diviseurs. Alors l'ensemble des points géométriques de la Jacobienne J est égal aux classes d'équivalences de diviseurs de degré 0. Si C_k est de genre g, alors J est une variété abélienne de dimension g.

En particulier, on s'intéresse aux Jacobiennes de courbes hyperelliptiques. Une courbe hyperelliptique C_k est (la normalisation du projectivisé d') une courbe plane dans $\mathrm{Spec}\, k[x,y]$ donnée par une équation

$$y^2 = f(x)$$

où f est un polynôme séparable sur k (en caractéristique 2, les courbes hyperelliptiques sont de la forme $y^2 + h(x)y = f(x)$). Si f est de degré $2g+1$ ou $2g+2$, alors C_k est de genre g. L'intérêt de travailler sur des Jacobiennes de courbes hyperelliptiques est que l'on a une représentation très agréable des points de la Jacobienne associée donnée par les coordonnées de Mumford. Si f est de degré $2g+1$, la courbe C_k admet un point à l'infini P_∞, et si $\imath$ représente l'involution canonique de C_k, on a si $P \in C_k(\overline{k})$: $P + \imath(P) - 2P_\infty \sim 0$. On peut montrer en utilisant le théorème de Riemann-Roch [Haro0, Théorème 1.3 p. 295] que tout point géométrique Q de la Jacobienne J admet un unique diviseur représentant de la forme

$$Q = \sum_{i=1}^{d} (P_i - P_\infty)$$

avec $P_i \in C_k(\overline{k})$, $P_i \neq P_\infty$, $d \leqslant g$ et $\imath P_i \neq P_j$ pour tout $i, j \in \{1..d\}$. On appelle cette représentation la forme normale de Cantor de Q, et on a un algorithme explicite pour passer d'un représentant quelconque de Q à une forme normale de Cantor [Can87].

Si $d = g$, et $P_i \neq P_j$ pour $i \neq j$, les coordonnées de Mumford de Q sont donnés par un couple de polynômes univariés (u, v), où $u(X) = \prod_{i=1}^{d}(X - x(P_i))$ et v est l'unique polynôme de degré $d-1$ tel que $v(x_{P_i}) = y_{P_i}$ pour $i \in \{1..d\}$. Plus généralement, les diviseurs sous forme normale de Cantor sont en bijection avec les couples (u, v), où u est un polynôme unitaire de degré $d \leqslant g$, et v un polynôme de degré strictement inférieur à celui de u, tels que $u \mid f - v^2$. Un tel couple (u, v) représente le point de la Jacobienne $D - dP_\infty$, où D est le diviseur associé à l'idéal de dimension 0 : $(U(x), y - V(x))$. (Pour plus de détails, on peut consulter [Mum84, Section 1].) Si on applique l'algorithme de mise en forme normale de Cantor au diviseur $D_1 + D_2$, où D_1 et D_2 sont deux représentations canoniques de points géométriques de la Jacobienne, on obtient donc un algorithme permettant d'exprimer l'addition sur les coordonnées de Mumford.

On peut donc calculer explicitement l'addition sur la Jacobienne J, et se servir de ce groupe pour faire de la cryptographie à clé publique (voir la section 1.2 ou [CFA+06] pour un panorama complet). Cependant, les attaques du type *calcul d'index* font qu'on va plutôt travailler sur des courbes hyperelliptiques de petit genre. Étudions quelques cas (pour plus de détails on peut consulter [Gau08]) :

- Si $g = 1$, on dit que C est une courbe elliptique ; la Jacobienne de C est isomorphe à C, donc C est une variété abélienne. Réciproquement toute variété abélienne de dimension 1 est une courbe elliptique.
  Dans ce cas, si $k = \mathbb{F}_q$, le théorème de Hasse montre que le cardinal de C est d'ordre de grandeur q. Si le cardinal de C est premier (ou a seulement un petit cofacteur), sauf pour certaines classes de courbes elliptiques (courbes supersingulières avec l'attaque MOV [MOV91] ; courbes définies sur $\mathbb{F}_{q^n}$ avec $n > 1$ petit ou composé par la descente de Weil [GHS02 ; Gau09] ; courbes anomales ; …), le meilleur algorithme connu pour le calcul du logarithme discret est l'algorithme générique, en $\widetilde{O}(q^{1/2})$.

- Si $g = 2$, toute variété abélienne (principalement polarisée) de dimension 2 est la Jacobienne[1] d'une courbe hyperelliptique [Wei57]. Dans ce cas, le cardinal de la Jacobienne est de l'ordre de q^2, et (pour une courbe hyperelliptique générale), le meilleur algorithme pour le calcul du logarithme discret est en $\widetilde{O}(q)$.
- Si $g \geqslant 3$, une variété abélienne de dimension g a un cardinal de l'ordre de q^g. L'espace modulaire des variétés abéliennes de dimension g est de dimension $g(g+1)/2$, celui des Jacobiennes de courbes de genre g de dimension $3g-3$, et celui des Jacobiennes de courbes hyperelliptiques de genre g de dimension $2g-1$. Dans ce cas, l'algorithme de calcul d'index est plus rapide que l'algorithme générique, il donne une attaque du logarithme discret en $\widetilde{O}(q^{2-2/g})$ [GTTD07].
  Le cas du genre 3 est particulièrement intéressant car toute variété abélienne (principalement polarisée) de dimension 3 est la Jacobienne[2] d'une courbe de genre 3 [Hoy63 ; OU73]. Si J est la Jacobienne d'une courbe hyperelliptique de genre 3, le calcul d'index donne une attaque en $\widetilde{O}(q^{4/3})$ à comparer à $\widetilde{O}(q^{3/2})$ pour l'algorithme générique. Si J est la Jacobienne d'une courbe non hyperelliptique, il existe un algorithme en $\widetilde{O}(q)$ [Die06 ; DT08].
- Pour l'instant, les attaques en genre moyen $g \geqslant 3$ que nous avons vues restent exponentielles. En genre très grand on a des algorithmes sous-exponentiels pour le logarithme discret [ADH94] : si J est la Jacobienne d'une courbe de genre g définie sur $\mathbb{F}_q$, avec $g > \log(q)$, on a un algorithme en $L_{\frac{1}{2},O(1)}(q^g)$ où L est la fonction sous-exponentielle classique qui intervient sur les questions de friabilité :

  $$L_{\alpha,c}(N) = e^{c(\log N)^{\alpha}(\log\log N)^{1-\alpha}}.$$

  On a même une classe de courbes sur lesquelles l'attaque du logarithme discret est en $L_{\frac{1}{3},O(1)}(q^g)$ [EGT09].

Par ce qui précède, pour faire de la cryptographie à clé publique en utilisant le logarithme discret dans les variétés abéliennes, on se restreint essentiellement à des courbes elliptiques et des Jacobiennes de courbes hyperelliptiques de genre 2.

1.3.3 *Pairing sur les variétés abéliennes*

Un pairing[3] est une application bilinéaire non dégénérée $e : G_1 \times G_2 \to G_3$ entre des groupes abéliens finis. Sur les variétés abéliennes, il existe un pairing se calculant efficacement : le pairing de Weil. Cette découverte a ouvert la porte à de nombreux nouveaux protocoles cryptographiques. Citons par exemple l'échange de clé tripartite [Jou04], les signatures courtes [BLS04], les clés basées sur l'identité [BF03], les certificats anonymes [Ver01], la cryptographie par attributs [SW05 ; GPSW06] et la cryptographie par ''broadcast'' [LS08]. Par exemple, le protocole de Diffie-Hellmann tripartite permet à trois personnes Alice, Bob et Charlie d'échanger

1. Si la variété abélienne n'est pas simple, il y a également des produits de Jacobiennes, qui forment une sous-variété stricte de l'espace des modules.

3. Le terme français est *couplage*. Cependant on fera usage intensif d'un couplage appelé « commutator pairing » par MUMFORD, et dont nous n'avons pas trouvé de traduction consacrée dans la littérature. Plutôt que d'employer une traduction bancale comme « couplage des commutateurs », nous avons préféré employer le terme anglais tout le long. En conséquence, on parle aussi d''‘embedding degree'' plutôt que de « degré de plongement ». Nous prions le lecteur de m'excuser pour ces choix ! Nous ferons d'ailleurs un autre anglicisme, en employant « theta null point » à la place du terme français de « thêta constantes ». La raison en est que si le terme français retranscrit bien que les « thêta constantes » forment un invariant modulaire de la variété abélienne, le terme anglais retranscrit mieux le fait que cet invariant modulaire est simplement donné par les coordonnées thêta du point neutre de la variété abélienne.

une clé commune en une seule passe de communication. Si $G = G_1 = G_2$ est cyclique de générateur g, Alice, Bob et Charlie choisissent une clé a, b, et c respectivement, et envoient sur le canal de communication non sûr l'élément g^a, g^b et g^c respectivement. La clé commune est alors $e(g,g)^{abc} \in G_3$. En effet, Alice peut par exemple retrouver cette clé en calculant $e(g^b, g^c)^a$, par bilinéarité du pairing. Pour d'autres application des pairings, on peut consulter les articles de la conférence Pairing http://www.pairing-conference.org/. Un point clé utilisé dans les applications des pairings est qu'ils permettent de séparer le problème de « Diffie-Hellman décisionnel », du problème de « Diffie-Hellman calculatoire ». En effet, le problème de « Diffie-Hellman décisionnel » consiste étant donné 3 éléments g^a, g^b, g^c de G de décider si $g^c = g^{ab}$. Si on dispose d'un pairing non dégénéré e sur G, il suffit de vérifier que $e(g^c, g)e(g,g) = e(g^a, g)e(g^b, g)$. En revanche, le problème de « Diffie-Hellman calculatoire », qui consiste à déterminer g^{ab} à partir de g^a et g^b est lui supposé rester difficile (si le logarithme discret sur le groupe d'arrivée G_3 reste difficile).

Le pairing de Weil sur une courbe elliptique est défini de la façon suivante (pour plus d'informations sur les pairing sur les variétés abéliennes, en particulier leur lien avec les isogénies, on peut consulter la section 5.2) : soit $E_{\mathbb{F}_q}$ une courbe elliptique définie sur le corps fini $\mathbb{F}_q$ et de point neutre $0_{E_{\mathbb{F}_q}} = P_\infty$, $\ell \in \mathbb{N}^*$ et P, Q des points de $E_{\mathbb{F}_q}(\overline{\mathbb{F}}_q)[\ell]$. Comme P est un point de ℓ-torsion, il existe une fonction f_P telle que $(f_P) \sim \ell(P - 0_{E_{\mathbb{F}_q}})$. De même, il existe une fonction (f_Q) telle que $(f_Q) \sim \ell(Q - 0_{E_{\mathbb{F}_q}})$. Alors le pairing de Weil est donné par[1] (en translatant les cycles $(Q) - (0_{E_{\mathbb{F}_q}})$ et $(P) - (0_{E_{\mathbb{F}_q}})$ de telle sorte que leur supports soient disjoints de f_P et f_Q) :

$$e_\ell(P,Q) = \frac{f_Q((P) - (0_{E_{\mathbb{F}_q}}))}{f_P((Q) - (0_{E_{\mathbb{F}_q}}))}.$$

En fait, il suffit que le cardinal de $E_{\mathbb{F}_q}$ soit un multiple de ℓ par un petit cofacteur.

En pratique, on utilise les pairings sur des courbes elliptiques $E_{\mathbb{F}_q}$ dont le cardinal est un nombre premier ℓ (premier à la caractéristique de $\mathbb{F}_q$). On appelle alors d le plus petit entier tel que $\mu_\ell \subset \mathbb{F}_{q^d}^*$, où μ_ℓ est le groupe des racines ℓ-ièmes de l'unité. Autrement dit, d est le plus petit entier tel que $\ell \mid q^d - 1$, on l'appelle ''l'embedding degree'' de la courbe elliptique $E_{\mathbb{F}_q}$. Le pairing de Weil est alors une application bilinéaire :

$$e_\ell : E_{\mathbb{F}_q}[\ell](\mathbb{F}_q) \times E_{\mathbb{F}_q}[\ell](\mathbb{F}_{q^d}) \to \mathbb{F}_{q^d}^*.$$

L'attaque MOV [MOV91], que l'on a vue dans la section 1.3.1 et qui s'applique lorsque d est très petit (ce qui est notamment le cas des courbes elliptiques supersingulières) fonctionne ainsi : on cherche à calculer le logarithme discret de $P = nP_0 \in E_{\mathbb{F}_q}(\mathbb{F}_q)$ par rapport à un générateur P_0. On prend un point $Q \in E_{\mathbb{F}_q}(\mathbb{F}_{q^d})$ tel que $e_\ell(P,Q) \neq 1$. On a alors $e_\ell(P,Q) = e_\ell(P_0,Q)^n$, ce qui nous donne le transfert au problème du logarithme discret dans le corps multiplicatif $\mathbb{F}_{q^d}^*$.

En général, pour une courbe elliptique, d sera grand, de l'ordre de q, ce qui fait que pour utiliser les applications cryptographiques à base de pairing, il faut rechercher des courbes (que l'on appelle ''pairing-friendly'') avec un d relativement petit (mais suffisamment grand pour que la sécurité du logarithme discret dans $\mathbb{F}_{q^d}^*$ soit suffisante). On peut consulter [MNT01 ; BN06] pour des familles de telles courbes.

En pratique, pour calculer des pairings efficacement sur une courbe elliptique, on préfère utiliser le pairing de Tate défini par :

$$\begin{aligned} e_T : E_{\mathbb{F}_q}(\mathbb{F}_{q^d})/\ell E_{\mathbb{F}_q}(\mathbb{F}_{q^d}) \times E_{\mathbb{F}_q}[\ell](\mathbb{F}_q) &\longrightarrow \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*\,\ell} \\ (P,Q) &\longmapsto f_Q((P) - (0_{E_{\mathbb{F}_q}})). \end{aligned}$$

1. En général, on normalise f_P et f_Q de telle sorte que $e_\ell(P,Q) = f_Q(P)/f_P(Q)$.

Si l'on suppose que $\ell^2 \nmid E_{\mathbb{F}_q}(\mathbb{F}_{q^d})$, on a $E_{\mathbb{F}_q}(\mathbb{F}_{q^d})[\ell] \simeq E_{\mathbb{F}_q}(\mathbb{F}_{q^d})/\ell E_{\mathbb{F}_q}(\mathbb{F}_{q^d})$, et de plus si $q^d - 1 = r\ell$, on normalise le pairing de Tate en l'élevant à la puissance r.

On peut calculer le pairing de Tate (ou de Weil) en utilisant un algorithme dû à Miller [Mil04]. L'idée est la suivante : on veut construire la fonction f_Q normalisée telle que $(f_Q) = \ell(Q - 0_{E_{\mathbb{F}_q}})$. Par définition de l'addition sur une courbe elliptique, si $P_1, P_2 \in E_{\mathbb{F}_q}(\mathbb{F}_q)$, il existe une fonction rationelle f_{P_1,P_2} tel que $(f_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - 0_{E_{\mathbb{F}_q}}$. Explicitement, si $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ et que l'on suppose $x_1 \neq x_2$, on a

$$f_{P_1,P_2} = \frac{Y - \lambda(X - x_1) - y_1}{X + (x_1 + x_2) - \lambda^2}$$

où $\lambda = (y_1 - y_2)/(x_1 - x_2)$. En particulier, on peut ainsi construire via une méthode *diviser pour régner* une fonction f_n de diviseur $nQ - (nQ) - (n-1)0_{E_{\mathbb{F}_q}}$, par $f_{n_1+n_2} = f_{n_1} f_{n_2} f_{n_1 Q, n_2 Q}$. Comme $\ell P = 0_{E_{\mathbb{F}_q}}$, on a $f_Q = f_\ell$, et il suffit de l'évaluer en P (sauf qu'il est plus efficace d'évaluer directement en P les fonctions intermédiaires f_n). On en déduit la version suivante de l'algorithme de Miller :

Algorithme 1.3.2 (Pairing via l'algorithme de Miller) :
Entrée $\ell \in \mathbb{N}$, $Q = (x_1, y_1) \in E_{\mathbb{F}_q}[\ell](\mathbb{F}_q)$, $P = (x_2, y_2) \in E_{\mathbb{F}_q}[\ell](\mathbb{F}_{q^d})$.
Sortie $e_T(P, Q)$.

- ➔ Calculer la décomposition binaire $\ell := \sum_{i=0}^{I} b_i 2^i$. Poser $T = Q$, $f_1 = 1$, $f_2 = 1$.
- ➔ Pour i dans $[I..0]$ calculer
  - λ, la pente de la tangente de $E_{\mathbb{F}_q}$ en T.
  - $T = 2T$. $T = (x_3, y_3)$.
  - $f_1 = f_1^2(y_2 - \lambda(x_2 - x_3) - y_3)$, $f_2 = f_2^2(x_2 + (x_1 + x_3) - \lambda^2)$.
  - Si $b_i = 1$, alors calculer
    - λ, la pente de la droite passant par Q et T.
    - $T = T + P$. $T = (x_3, y_3)$.
    - $f_1 = f_1^2(y_2 - \lambda(x_2 - x_3) - y_3)$, $f_2 = f_2(x_2 + (x_1 + x_3) - \lambda^2)$.
- ➔ Renvoyer

$$\left(\frac{f_1}{f_2}\right)^{\frac{q^d-1}{d}}.$$

♢

Remarque 1.3.3. D'une part, on peut éviter les divisions dans le calcul de λ en utilisant des coordonnées homogènes (x, y, z) pour représenter les points de la courbe elliptique [CSB04]. D'autre part, si l'embedding degree $d = 2d'$ est pair, alors on peut se ramener à un point $P = (x_2, y_2)$ tel que $x_2 \in E_{\mathbb{F}_q}(\mathbb{F}_{q^{d'}})$ puisque $y_2^2 = f(x_2)$ [BKLS02]. Lors de l'exponentiation finale, on a $f_2^{\frac{q^d-1}{d}} = 1$, donc il n'y a pas besoin de calculer f_2. Dans ce cas, à chaque étape de la boucle de Miller, le nombre d'opérations dans le *grand corps* $\mathbb{F}_{q^d}$ est de 1 carré, 1 multiplication, et 1 multiplication par un élément du petit corps $\mathbb{F}_q$. (En genre 2, on peut appliquer la même méthode si P est représenté par un diviseur dégénéré. Si ce n'est pas le cas, toujours si d est pair, lorsqu'on évalue l'exponentiation finale, le dénominateur des fonctions de Miller est égal au conjugué de son inverse, donc dans ce cas on peut remplacer l'inversion par une multiplication plutôt que de garder la variable supplémentaire f_2 [ÓS07]. Pour plus d'informations sur le pairing dans des Jacobiennes de courbes hyperelliptiques, on peut consulter [GHV07 ; BBC+09]).

1.4 ISOGÉNIES SUR LES VARIÉTÉS ABÉLIENNES

Lorsqu'on utilise une variété abélienne A_k sur un corps fini k en vue d'applications cryptographiques, il faut faire attention à ce que son cardinal soit divisible par un grand nombre premier. Pour cela il faut être capable de le calculer rapidement. (Une autre méthode est d'utiliser la théorie de la multiplication complexe pour construire une courbe elliptique avec un nombre de points prescrit.) On peut consulter [Gau04] pour un panorama des algorithmes de comptage de points disponibles. Si Fr est le Frobenius de k, il agit sur A_k, et les points fixes de $A_k(\bar{k})$ par le Frobenius sont exactement les points rationnels $A_k(k)$. On a donc $\#A_k(k) = \deg(\mathrm{Fr} - \mathrm{Id})$. On peut montrer que le polynôme caractéristique[1] χ_{Fr} du Frobenius agissant sur le module de Tate (vectorialisé) $V_\ell(A_k) = T_\ell(A_k) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ (pour ℓ premier à la caractéristique de k), vérifie $\chi_{\mathrm{Fr}}(\lambda) = \deg(\mathrm{Fr} - \lambda\,\mathrm{Id})$ [Mil91, Proposition 10.20], et donc $\#A_k(k) = \chi_{\mathrm{Fr}}(1)$.

Il y a alors deux grandes familles d'algorithmes pour calculer le cardinal de A_k. La première famille (appelée famille p-adique), consiste à calculer un relevé (canonique avec l'algorithme de Satoh [Sat00], ou non, avec l'algorithme de Kedlaya utilisant la cohomologie de Monsky-Washnitzer [Ked01]) de la variété abélienne A_k à un anneau p-adique et calculer le polynôme caractéristique du Frobenius sur ce relevé. Cette famille d'algorithme est surtout efficace lorsque la caractéristique p de k est petite. Par exemple, la complexité de l'algorithme de Kedlaya pour calculer le cardinal d'une courbe de genre g défini sur $\mathbb{F}_{p^n}$ est de $\widetilde{O}(pn^3g^4)$, avec les améliorations de [GG03] (si p est grand par rapport à n, une méthode plus efficace est décrite dans [Har07]). L'algorithme de Satoh (et les améliorations de Mestre, voir la section 8.3) a une plus grande complexité en p, mais meilleure en n.

L'autre famille (appelée aussi famille ℓ-adique), consiste à calculer l'action du Frobenius sur $A_k[\ell]$ (avec ℓ premier à p). En effet, $A_k[\ell]$ est un $\mathbb{Z}/\ell\mathbb{Z}$-espace vectoriel de dimension $2g$, et le polynôme caractéristique du Frobenius sur cet espace est χ_{Fr} mod ℓ par ce qui précède. On calcule alors χ_{Fr} mod ℓ pour beaucoup de petits nombres premiers ℓ, et on reconstitue ensuite χ_{Fr} grâce au théorème des restes chinois. En effet, on a vu dans la section 1.3.1 que l'on a une borne explicite de la taille des coefficients de χ_{Fr} grâce aux conjectures de Weil (prouvées par Weil pour les variétés abéliennes, puis par Deligne pour le cas général). On sait donc que les coefficients de χ_{Fr} sont en $O(q^g)$, il faut donc considérer $O(g \log q)$ nombres premiers de taille $O(g \log q)$.

Prenons par exemple une courbe elliptique $E_k : y^2 = f(x)$ définie sur un corps fini $k = \mathbb{F}_q$. Alors on peut exprimer facilement l'idéal de ℓ-division grâce au polynôme de ℓ-division ψ_ℓ. On peut alors calculer l'action du Frobenius (et en particulier sa trace) dans l'algèbre de dimension 0 et de degré $\ell^2 - 1$: $\mathscr{A} = E_k/(\psi_\ell(x), y^2 - f(x))$. Le coût d'une opération dans $\mathscr{A}$ est en $\widetilde{O}(\ell^2 \log q)$ et donc le calcul du Frobenius dans $\mathscr{A}$ est en $\widetilde{O}((\log q)^2\ell^2)$, donc au final la complexité de l'algorithme de Schoof est en $\widetilde{O}((\log q)^5)$. Une amélioration due à Atkin et Elkies consiste à travailler, non plus sur $\mathscr{A}$, mais sur l'anneau associé à un sous-groupe (rationnel) d'ordre ℓ de la ℓ-torsion dans E_k. Le coût d'une opération dans cet anneau est en $\widetilde{O}(\log q \cdot \ell)$, d'où une complexité (heuristique) en $\widetilde{O}((\log q)^4)$. Or il se trouve que de tels noyaux correspondent exactement aux isogénies rationnelles.

Définition 1.4.1. Une isogénie (séparable) est un morphisme (séparable) fini et surjectif de variétés abéliennes. (Un morphisme de variétés abéliennes est un morphisme de variété qui

1. Si A_k est la Jacobienne d'une courbe C_k, alors $H^{1,\mathrm{etale}}(C_k, \mathbb{Q}_\ell) \simeq H^{1,\mathrm{etale}}(A_k, \mathbb{Q}_\ell) = \mathrm{Hom}(V_\ell(A_k), \mathbb{Q}_\ell)$ [AGV72, SGA 4.3, Corollaire 4.7 p. 35 en passant à la limite projective], et donc la formule des traces de Lefschetz montre que la fonction zeta de C_k est égale à $\frac{P(t)}{(1-t)(1-qt)}$ où P est le polynôme réciproque de χ_{Fr} [Har00, Appendice C].

est également un morphisme de groupe.) ◊

Soit une isogénie $f : A_k \to B_k$ entre deux variétés abéliennes. On peut montrer que f est un morphisme plat, et que A_k et B_k ont la même dimension. De plus, les isogénies séparables (rationnelles) de domaine A_k sont en bijection avec les sous-groupes (rationnels) finis de A_k. En effet, à une isogénie séparable f on associe son noyau $K = \operatorname{Ker} f$. Réciproquement, si K est un sous-groupe rationnel fini de A_k, alors la variété quotient A_k/K est une variété abélienne, et $A_k \to A_k/K$ est une isogénie de noyau K.

Un exemple d'isogénie est la multiplication par ℓ, dont le noyau est formé des points de ℓ-torsion. Un exemple d'isogénie non séparable est donné par le Frobenius.

Il se trouve que l'on dispose d'un algorithme explicite pour calculer des isogénies sur les courbes elliptiques, grâce aux formules de Vélu. Ces formules utilisent de manière fondamentale le fait qu'il existe des coordonnées canoniques (x, y) sur une courbe elliptique.

Si E_k est une courbe elliptique sur un corps quelconque k, on peut caractériser uniquement le système de coordonnées affine (x, y) (à un changement de variable linéaire près) sur E_k ainsi :

$$\begin{aligned} v_{0_{E_k}}(x) &= -2 \qquad v_P(x) \geqslant 0 \quad \text{si } P \neq 0_{E_k} \\ v_{0_{E_k}}(y) &= -3 \qquad v_P(y) \geqslant 0 \quad \text{si } P \neq 0_{E_k} \\ y^2/x^3(0_{E_k}) &= 1, \end{aligned} \tag{1.1}$$

où v_Q représente la valuation de l'anneau local de E_k au point fermé Q. La courbe elliptique E_k a alors pour équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

En faisant un changement de variable $(x, y) \mapsto (ax + b, cx + dy + e)$ avec $a^3 = c^2$, on peut de plus se ramener à une équation de la forme $y^2 = x^3 + a'_4x + a'_6$ lorsque la caractéristique de k est différente de 2 ou 3.

PROPOSITION 1.4.2 (FORMULES DE VÉLU). *Soit $G \subset E_k(k)$ un sous-groupe fini. Alors la courbe elliptique E_k/G est donnée par $Y^2 + a_1XY + a_3Y = g(X)$ (où g est un polynôme unitaire de degré 3) et :*

$$\begin{aligned} X(P) &= x(P) + \sum_{Q \in G \setminus \{0_{E_k}\}} (x(P+Q) - x(Q)) \\ Y(P) &= y(P) + \sum_{Q \in G \setminus \{0_{E_k}\}} (y(P+Q) - y(Q)). \end{aligned}$$

Enfin, on peut retrouver l'équation de g, a_1 et a_3 au prix de $O(\ell)$ additions dans E_k [Vel71].

DÉMONSTRATION : Si $\pi : E_k \to E_k/G$ est la projection canonique, on identifie $k(E_k/G)$ à son image dans $k(E_k)$ par π^*, on a alors $k(E_k)^G = k(E_k/G)$. Alors, X et Y sont dans $k(E_k)^G$, et il est facile de voir que ces coordonnées satisfont les conditions (1.1) pour E_k/G. ■

De plus, la courbe modulaire $X_0(\ell)$ paramétrise les classes d'isomorphismes de courbes elliptiques munies d'un sous-groupe de cardinal ℓ de leur ℓ-torsion. Par exemple, $X_0(1)$ paramètre la droite des invariants j. De plus, le polynôme modulaire d'ordre ℓ, $\Phi_\ell(x, y)$, est l'équation de la courbe $X_0(\ell)$ dans $X_0(1) \times X_0(1)$. Autrement dit, si E_k est la courbe elliptique d'équation $y^2 = x^3 + ax + b$ et de j-invariant

$$j(E_k) = 1728\frac{4a^3}{4a^3 + 27b^2},$$

les racines de $\Phi_\ell(j(E_k), \cdot)$ correspondent aux j-invariants des courbes elliptiques ℓ-isogènes à E_k.

En résumé, étant donné une courbe elliptique E_k de j-invariant j_{E_k}, le calcul de ℓ-isogénies se fait en deux étapes :

- D'abord, trouver les solutions de $\Phi_\ell(j_{E_k}, y)$ où $\Phi_\ell(x, y)$ est le polynôme modulaire d'ordre ℓ. Puis étant donné une solution $j_{E'_k}$, calculer l'équation de Weierstrass de la courbe elliptique correspondante E'_k, qui est ℓ-isogène à E_k. (En pratique, comme la hauteur du polynôme modulaire Φ_ℓ est en $O(\ell \log \ell)$ [BS09 ; Coh08], on considère des polynômes modulaires sur des invariants donnant de plus petits coefficients [Mor95].)
- Ensuite, utiliser l'algorithme de Vélu (proposition 1.4.2) pour calculer l'isogénie : $E_k \to E'_k$.

Le calcul effectif d'isogénies est une brique de base de la boite à outils sur les courbes elliptiques, citons entre autre comme applications :

- le transfert du problème du logarithme discret d'une courbe elliptique à une courbe isogène (voir aussi [Smi09] pour un exemple avec des Jacobiennes de courbes de genre 3) ;
- les algorithmes de comptage ℓ-adique [Sch85 ; Sch95 ; Atk88 ; Elk92] ;
- le calcul du relevé canonique de la courbe elliptique (si elle est ordinaire) [Sat00 ; Mes01] ;
- le calcul de l'anneau d'endomorphisme d'une courbe elliptique [Koh96 ; FM02 ; BS09] ;
- le calcul du polynôme modulaire Φ_ℓ [BLS09].
- le calcul des polynômes de classe de Hilbert[1] [Sut09 ; GHK+06 ; CKL08] ; ce sont ces polynômes de classe qui sont utilisées ensuite par la méthode CM (méthode de la multiplication complexe).

Pour certaines applications (calcul de l'anneau d'endomorphisme par exemple), il suffit de construire des graphes d'isogénies et seule la connaissance du polynôme modulaire Φ_ℓ est nécessaire. Pour d'autres comme le transfert du logarithme discret, il faut savoir calculer explicitement l'isogénie.

La situation en dimension supérieure est nettement moins bonne. Si J est la Jacobienne d'une courbe hyperelliptique de genre 2, on sait calculer des $(2,2)$-isogénies grâce aux formules de Richelot [Ric36 ; Ric37]. De plus, on peut généraliser le polynôme modulaire Φ_ℓ en construisant des polynômes modulaires sur les invariants d'Igusa. Cependant dans ce cas les coefficients de ce polynôme sont rationnels (et non plus entiers) et explosent beaucoup plus rapidement que dans le cas elliptique. Actuellement, seul le polynôme modulaire de degré 2 est connu en dimension 2 (dont les coefficients prennent, même compressés, 26.8 MO d'espace disque [Dup06, p 227]). Enfin en genre 3, Smith a étendu les formules de Richelot pour calculer des $(2,2,2)$-isogénies [Smi09].

La raison pour laquelle les formules de Vélu ne fonctionnent pas en dimension 2 vient du fait que les coordonnées de Mumford sont associées à une courbe hyperelliptique plutôt qu'à sa Jacobienne. Or si l'on part d'une courbe C de genre 2 et de Jacobienne J, et si $J \to J'$ est une isogénie, il n'y a pas de courbe explicitement donnée C' telle que la Jacobienne de C' soit J'. Autrement dit, il n'y a aucune raison que les formules de Vélu appliquées aux coordonnées de Mumford donnent les coordonnées de Mumford sur la courbe isogène, et des expériences effectuées à l'aide du logiciel Magma [BCP97] montre qu'en général ce n'est effectivement pas le cas.

1.5 FONCTIONS THÊTA ET APPLICATIONS

Il est donc naturel d'utiliser un autre système de coordonnées projectives, qui soient en un certain sens *canoniques*. Un tel système nous est fourni par les fonctions thêta (on peut consulter

1. On peut citer d'autres méthodes pour le calcul des polynômes de classe : on peut par exemple utiliser la méthode analytique [Eng09], qui revient à voir le j-invariant comme une fonction modulaire sur le demi-plan

[BL04 ; Igu72 ; Mum83 ; Mum84 ; Mum91] pour une définition analytique des fonctions thêta et [Mum66 ; Mum67a ; Mum67b ; Kem89 ; l'appendice « Lecture on curves and their Jacobians » de Mum99 ; Mor85] pour une définition algébrique) : en effet, tout système de coordonnées projectives vient (à une action de PGL_n près) d'un système de coordonnées thêta d'un certain niveau. Réciproquement, si A_k est une variété abélienne de dimension g et $n \geqslant 3$, les coordonnées thêta de niveau n donnent un plongement vers l'espace projectif $\mathbb{P}_k^{n^g-1}$.

De plus, l'intérêt des fonctions thêta de niveau n sur une variété abélienne A_k est qu'elles encodent toute l'information sur la n-torsion de A_k. En particulier, le théorème de l'isogénie (théorème 3.6.4) permet de relier les fonctions thêta de niveau ℓn sur A_k et les fonctions thêta de niveau n sur une variété ℓ-isogène B_k. Ce théorème n'est pas suffisant pour un calcul explicite d'isogénies[1]. On verra toutefois comment l'utiliser comme brique de base dans le chapitre 7.

On peut effectuer une brève comparaison entre les coordonnées thêta et les coordonnées de Mumford :

- Les coordonnées thêta sont universelles, elles existent pour toute variété abélienne, et même tout plongement projectif d'une variété abélienne. Les coordonnées de Mumford sont restreintes aux Jacobiennes de courbes hyperelliptiques.
- Les coordonnées thêta de niveau n sont de cardinal n^g, à comparer aux $2g$-coordonnées données par les coordonnées de Mumford. Ceci restreint l'usage des fonctions thêta à des variétés abéliennes de petite dimension, mais c'est déjà le cas pour les applications cryptographiques.
- Les coordonnées de Mumford sont rationnelles, en revanche les coordonnées thêta de niveau n peuvent nécessiter de prendre une extension de corps (en effet, elles encodent toute l'information de l'action de translation par la n-torsion).
- En genre 2, la multiplication (qui est l'étape de base pour le logarithme discret) avec les coordonnées thêta de niveau 2 est plus rapide que l'algorithme de Cantor pour les coordonnées de Mumford [Gau07], et compétitive avec les meilleurs algorithmes connus en genre 1 [GL09].

On peut bien sûr passer d'un système de coordonnées à l'autre, par exemple en utilisant les formules de [Wam99].

1.5.1 *Construction des fonctions thêta*

Il y a deux manières de présenter la construction des coordonnées thêta sur une variété abélienne. La première méthode est de les construire sur les variété abéliennes complexes : une variété abélienne complexe X de dimension g est un tore de la forme $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ où Ω appartient au demi-espace $\mathfrak{H}_g$ de Siegel (c'est-à-dire que $\Omega \in \mathrm{M}_g(\mathbb{C})$ est une matrice symétrique de partie imaginaire définie positive). On peut alors définir la fonction thêta de Jacobi-Riemann :

$$\vartheta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i\, {}^t n \Omega n + 2\pi i\, {}^t n z}. \tag{1.2}$$

La fonction ϑ est une fonction analytique sur $\mathbb{C}^g \times \mathfrak{H}_g$, et on peut construire d'autres fonctions thêta (avec caractéristiques) de la même manière. Les relations de Riemann (théorème 4.4.6)

de Poincaré (ou en genre supérieur sur le demi-espace de Siegel), et qui peut d'ailleurs servir également à la construction des polynômes modulaires ; ou encore utiliser les méthodes p-adiques qui passent par le calcul du relevé d'une courbe elliptique ordinaire [Bro06].

1. Tant que l'on a pas à disposition une méthode pour *monter de niveau*, c'est-à-dire passer des coordonnées thêta de niveau n aux coordonnées thêta de niveau ℓn. De plus, par souci d'efficacité, on travaille généralement avec des fonctions thêta de niveau 4 voire même de niveau 2, ce qui ne permet pas d'appliquer ce théorème.

donnent des relations algébriques entre ces fonctions thêta. Ces relations encodent à la fois les formules d'addition sur la variété abélienne, et les équations homogènes de X dans le plongement projectif associé aux coordonnées thêta. Il s'avère alors que ces relations de Riemann encodent toute l'information sur la variété abélienne X (voir le théorème 4.7.2). On peut donc invoquer le principe de Lefschetz pour les utiliser sur des variétés abéliennes définies sur un corps algébriquement clos de caractéristique 0. On peut également, ce qui est plus intéressant cryptographiquement, les considérer sur des variétés abéliennes ordinaires sur un corps fini k, en considérant le relevé canonique sur l'anneau des vecteurs de Witt $W(k)$ et en plongeant $W(k)$ dans $\mathbb{C}$.

L'autre solution est de construire les fonctions thêta algébriquement, comme étant les coordonnées normalisant l'action du groupe de Heisenberg de niveau n (cette construction est due à Weil). Cette construction fait appel à des notions mathématiques plus sophistiquées que la construction analytique, mais a l'avantage de s'appliquer à toute variété abélienne (séparablement polarisée). L'autre avantage est que la construction algébrique permet une compréhension plus fine de la structure géométrique associée aux fonctions thêta par rapport au choix d'une matrice $\Omega \in \mathfrak{H}_g$ comme dans la construction analytique (voir la section 4.7). Dans cette thèse, nous avons fait le choix d'utiliser la construction algébrique, qui permet de mieux analyser la correspondance modulaire du chapitre 6 (voir la section 3.5). Cependant, pour faciliter la lecture, nous commençons d'abord par introduire la construction analytique dans le chapitre 2, et dans la suite, à chaque fois que nous introduisons une nouvelle notion algébrique, nous auront soin d'expliciter son équivalent analytique (et de même quand une notion algébrique a plusieurs interprétation, comme la notion de structure de niveau, nous nous efforçons d'expliquer le lien entre toutes ces interprétations).

1.5.2 *Applications*

Le but de cette thèse est de présenter, en les approfondissant, les résultats obtenus dans les trois articles [FLR09 ; LR10a ; LR10b] sur les applications cryptographiques des coordonnées thêta d'une variété abélienne.

Les résultats algorithmiques principaux sont :

- Un algorithme (algorithme 4.6.8) qui permet de compresser les $(4n)^g$ coordonnées thêta de niveau $4n$, en $(1 + g(g+1)/2) \times 4^g$ coordonnées thêta de niveau 4.
- Un algorithme (algorithme 5.4.2) de calcul de pairing sur les fonctions thêta. À ma connaissance, il s'agit du premier algorithme de calcul de pairing sur des variétés abéliennes qui n'utilise pas l'algorithme de Miller. (Dans l'algorithme 5.4.2, on calcule le ''commutator pairing'', un pairing basé sur le défaut de commutativité des facteurs projectifs lors de l'addition sur une variété abélienne, plutôt que d'utiliser l'évaluation d'une fonction rationnelle en un diviseur.)
- Un algorithme (algorithme 7.2.4) qui, étant donné un point modulaire solution d'une certaine correspondance modulaire (voir le chapitre 6), calcule explicitement l'isogénie associée.
- Un algorithme (algorithme 7.3.2) qui, partant des points géométriques d'un sous-groupe fini K d'une variété abélienne A_k construit le point modulaire correspondant à l'isogénie $A_k \to A_k/K$. Combiné à l'algorithme précédent, on a donc une version explicite des formules de Vélu en dimension quelconque, sur un corps k de caractéristique p quelconque (à condition que p ne divise pas $2 \cdot \#K$).

Tous les algorithmes présentés dans cette thèse ont été implémentés en Magma [BCP97]. Une

telle implémentation a d'ailleurs été cruciale pour mieux comprendre les objets manipulés[1]. Ces algorithmes reposent tous sur les formules d'addition (issues des relations de Riemann) présentées au chapitre 4. Au vu des résultats de cette thèse, on peut continuer la comparaison entre les coordonnées thêta et les coordonnées de Mumford selon la vitesse d'implémentation :

- Les coordonnées thêta (de niveau 2) sont plus intéressantes que les coordonnées de Mumford en genre 2, car on a vu qu'elles permettent de calculer bien plus rapidement la multiplication par un scalaire, qui est l'opération de base en cryptographie à clé publique (pour chiffrer et déchiffrer). En particulier, cela rend les courbes de genre 2 compétitives avec les courbes elliptiques, comme l'ont montré [Ber06 ; Lan06 ; BL07a] analysant l'algorithme de Gaudry [Gau07].
- À ce titre, l'algorithme 5.4.2 de calcul de pairing permet de les calculer directement suivant ces coordonnés, en évitant une étape coûteuse de transformation vers les coordonnés de Mumford. De plus, il s'avère que cet algorithme serait compétitif avec l'algorithme usuel de Miller en genre 1 et bien plus rapide en genre 2 si on arrivait à lui appliquer la technique usuelle de réduction de boucle du pairing de ate optimal (utilisant l'action du Frobenius pour accélérer les calculs, voir par exemple [Ver10]).
- Et finalement, actuellement seules les coordonnées thêta permettent le calcul explicite d'isogénies.

Nous voudrions faire deux remarques sur la généralisation des formules de Vélu obtenues dans le chapitre 7. Premièrement, la correspondance modulaire du chapitre 6 relie des points modulaires de niveaux différents. Autrement dit, choisir un point modulaire solution revient à choisir une ℓ-isogénie, et une structure de niveau ℓn sur la variété isogène compatible avec la structure de niveau n de la variété d'origine. Ceci est différent de la correspondance modulaire utilisant le polynôme modulaire Φ_ℓ pour relier les j-invariants des courbes elliptiques isogènes. En particulier, avec l'algorithme de calcul d'isogénies présenté dans cette thèse, le plus efficace n'est pas de calculer un point modulaire solution, mais d'appliquer les formules à la Vélu de l'algorithme 7.3.2 en calculant toute la ℓ-torsion. Ainsi, comme on calcule déjà modulo toute la ℓ-torsion, on ne peut pas appliquer les améliorations d'Atkin et Elkies au comptage de points[2]. Des idées pour avoir une correspondance modulaire entre points modulaires de même niveau sont présentées au chapitre 8. L'autre remarque est sur la différence entre l'algorithme 7.3.2 et la proposition 1.4.2. Dans les formules de Vélu classiques, on fixe les coordonnées des courbes elliptiques isogènes (en prenant les coordonnées de Weierstrass), et l'on calcule la forme de l'isogénie selon ces coordonnées. Dans les formules à la Vélu présentées dans cette thèse, on fixe la forme de l'isogénie, et on cherche des coordonnées sur les variétés abéliennes correspondantes. On voit ici tout l'intérêt de l'universalité des coordonnées thêta.

1.6 PLAN DÉTAILLÉ DE LA THÈSE

Le plan de cette thèse est le suivant : la première partie est consacré à l'étude des fonctions thêta et aux relations d'addition. Dans le chapitre 2, on étudie les variétés abéliennes complexes. Plutôt que d'introduire directement les coordonnées thêta par la formule analytique de l'équation (1.2), on étudie d'abord les systèmes de coordonnées projectives dans les sections 2.3 et 2.4. Lorsque l'on a un système de coordonnées (très ample) sur une variété abélienne X, on

1. Par exemple, nous avons découvert l'algorithme 5.4.2 de pairing en analysant les équations du noyau d'une isogénie donnée par l'algorithme 7.2.4 (voir la section 7.2.1). Cette découverte n'est pas étonnante étant donné le lien profond entre pairings et isogénies (voir la section 5.2).
2. Sauf éventuellement pour calculer la trace du Frobenius agissant sur la ℓ-torsion, une fois que l'on a calculé une base de Gröbner d'icelle, en la restreignant à un sous-groupe rationnel issu du calcul d'isogénie explicite.

peut regarder le plongement projectif associé $f : X \to \mathbb{P}^N_{\mathbb{C}}$ où $N+1$ est le nombre de variables du système. Le groupe projectif $\mathrm{PGL}_N(\mathbb{C})$ agit alors sur ce système de coordonnées. On peut voir les fonctions thêta comme un représentant canonique sous cette action. Le lien avec la formule explicite de l'équation (1.2) est expliqué dans la section 2.6, qui permet la transition avec la construction algébrique. Dans le chapitre 3 on transpose le chapitre 2 au cas algébrique, en suivant [Mum66]. Les relations de Riemann sont introduites (dans le cadre algébrique) dans le chapitre 4. Ce chapitre est consacré à l'étude des formules d'addition issues des relations de Riemann. Le point crucial est que ces relations encodent plus d'informations que simplement la loi d'addition sur une variété abélienne. Par exemple, si $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$, la loi de groupe de X est issue de la loi de groupe de $\mathbb{C}^g$. Si des points $x, y \in X$ admettent des représentants $\widetilde{x}, \widetilde{y} \in \mathbb{C}^g$, alors les relations de Riemann permettent d'exprimer les coordonnées thêta de $\widetilde{x}+\widetilde{y}$ en fonction de celles de $\widetilde{x}, \widetilde{y}$ (et de $\widetilde{x}-\widetilde{y}$), où ici l'addition est l'addition de $\mathbb{C}^g$. Autrement dit, ces relations permettent de retrouver l'addition sur $\mathbb{C}^g$. Toutes les applications de la seconde partie découlent de ces formules d'addition, d'où l'importance du chapitre 4. ((Le lecteur avant tout intéressé par les applications pourra se contenter de lire le chapitre 2 en omettant la section 2.3, puis de passer directement à la section 4.4, en consultant à la section 4.7 pour savoir comment passer du cas analytique au cas algébrique.))

La seconde partie est consacrée aux applications des fonctions thêta ; le chapitre 5 donne un nouvel algorithme pour le calcul du pairing (de Weil ou de Tate) sur les variétés abéliennes via les fonctions thêta. Une comparaison avec l'algorithme 1.3.2 usuel de Miller est donnée dans la section 5.4.1. Le chapitre 6 décrit une correspondance modulaire qui relie les points modulaires de variétés abéliennes isogènes. À la différence de la correspondance modulaire entre les j-invariants (en dimension 1) ou les invariants d'Igusa (en dimension 2), on peut facilement construire les polynômes de cette correspondance modulaire (leurs coefficients étant ± 1, il n'y a pas d'explosion de la taille des coefficients). Ceci vient du fait que l'on considère ici une correspondance entre des variétés abéliennes marquées, ce qui rajoute de la structure au système. Le chapitre 7 utilise la correspondance modulaire du chapitre 6 pour donner un algorithme explicite de calcul d'isogénies. Enfin on présente une sélection de perspectives dans le chapitre 8.

Nous voudrions conclure le présent chapitre par une remarque d'implémentation : il est crucial d'utiliser les coordonnées thêta en niveau 2 (par rapport au niveau 4). En effet, on gagne sur la représentation des points, en utilisant seulement 2^g coordonnées plutôt que 4^g. On gagne également sur l'addition différentielle. Surtout, le gain le plus important se fait sentir dans l'algorithme 7.5.1 de calcul explicite d'isogénies. On a vu que le plus rapide était d'appliquer les formules de Vélu généralisées, en calculant toute la ℓ-torsion d'une variété abélienne. Or en niveau 2, on travaille sur la variété de Kummer associée à la variété abélienne, où un point est équivalent à son opposé, ce qui fait que l'on diminue par 2 le degré du système à traiter par une base de Gröbner. Cependant, comme on travaille sur la variété de Kummer, les formules d'addition sont plus délicates à utiliser. Étant donné l'importance du niveau 2, pour chaque algorithme de la thèse nous expliquons comment l'adapter, en utilisant les résultats de la section 4.8 qui analyse les coordonnées thêta en niveau 2.

Première partie

FONCTIONS THÊTA

2 VARIÉTÉS ABÉLIENNES COMPLEXES

MATIÈRES

2.1 INTRODUCTION

Le but de ce chapitre est de présenter quelques rappels sur les variétés abéliennes complexes. Cela peut sembler être sans objet avec la cryptographie où l'on s'intéresse à des variétés abéliennes sur des corps finis. Néanmoins, le principe de Lefschetz permet d'étendre les résultats à tout corps algébriquement clos de caractéristique 0. Par exemple, si $A_{\mathbb{F}_q}$ est une variété ordinaire sur $\mathbb{F}_q$, son relevé canonique $A_{\mathbb{Z}_q}$ est défini sur $\mathbb{Q}_q$, et un plongement $\mathbb{Q}_q \hookrightarrow \mathbb{C}$ permet alors d'appliquer les résultats à $A_{\mathbb{Z}_q}$, puis en passant à la fibre spéciale (ce qui n'est pas toujours possible, par exemple quand on veut réduire des polynômes dont le terme de tête est divisible par la caractéristique), à $A_{\mathbb{F}_q}$.

L'intérêt de travailler sur $\mathbb{C}$ vient du fait qu'on peut utiliser les méthodes analytiques : si X est une variété algébrique complexe, il existe une structure analytique canonique X_{hol} sur les points de X. De plus, X est complète si et seulement si X_{hol} est compacte, et dans ce cas, GAGA [Ser56] nous dit qu'il y a une équivalence de catégories entre les faisceaux algébriques cohérents sur X et les faisceaux analytiques cohérents sur X_{hol}, qui induit un isomorphisme canonique sur les groupes de cohomologie. De plus, le théorème de Chow dit que si X est complète, et si Y est un sous-espace analytique fermé de X_{hol}, alors Y est fermé pour la topologie de Zariski. Une application immédiate est que tout morphisme analytique $f_{\text{hol}} : X_{\text{hol}} \to Y_{\text{hol}}$ entre deux variétés algébriques X et Y complètes provient d'un morphisme algébrique $X \to Y$. (Voir [Mum70, p. 33-34] et [BL04, Appendice A].)

En particulier, comme les variétés abéliennes sont projectives, analytiquement les variétés abéliennes sont exactement les groupes de Lie qui admettent un plongement dans l'espace projectif, et tout tel plongement provient d'un plongement algébrique.

Les résultats de ce chapitre proviennent des deux références suivantes : MUMFORD, *Abelian varieties* [Mum70] qui fait admirablement le lien entre la théorie analytique et la théorie algébrique, et BIRKENHAKE et LANGE, *Complex abelian varieties* [BL04] qui utilisent le groupe thêta du point de vue analytique.

Toute variété abélienne complexe est un tore. Cette notion est traitée dans la section 2.2 où l'on étudie les différentes façons de représenter un tore complexe. Comme noté dans l'introduction, on souhaite étudier tous les systèmes de coordonnées sur des variétés algébriques (ainsi que leur comportement par rapport à une isogénie). Pour cela, il faut étudier les fibrés en droites (que l'on peut voir comme un objet géométrique associé à un système de coordonnées projectives) sur une variété abélienne complexe X. C'est l'objet de la section 2.3.

Le théorème d'Appell-Humbert démontré dans cette section dit que tout fibré en droites $\mathcal{L}$ sur X se représente par une forme hermitienne H et un semi-caractère χ pour H via le facteur d'automorphie associé. Cela rend les fibrés en droites sur X très simples à manipuler. Tout tore n'est pas une variété abélienne : on étudie dans la section 2.4 à quelle condition un tore admet un système de coordonnées projectif (et est donc une variété abélienne). Dans cette section, on étudie les variétés abéliennes munies d'un facteur d'automorphie (donc sans exhiber un système de coordonnées explicite), on dit aussi qu'un tel facteur d'automorphie (ample) fournit une polarisation sur la variété abélienne. On étudie alors les résultats de base sur les variétés abéliennes polarisées : on verra qu'il s'agit de la bonne notion géométrique pour comprendre comment sont transformés les systèmes de coordonnées (ou plutôt les facteurs d'automorphie) par rapport à une isogénie (voir la proposition 2.4.7). La section précédente introduit plusieurs structures sur les variétés abéliennes complexes. Les espaces modulaires associés à ces structures sont étudiés dans la section 2.5 ; en particulier, on exhibe une matrice $\Omega \in \mathfrak{H}_g$ dans le demi-espace de Siegel associée à chaque variété abélienne (principalement polarisée). Cette matrice Ω nous permettra de définir les fonctions thêta dans la section 2.6. Ces fonctions thêta nous fournissent des coordonnées « canoniques » que l'on peut associer à un fibré très ample. Il s'avère qu'on peut généraliser la construction des fonctions thêta classiques au cadre algébrique (où l'on ne dispose pas d'une telle matrice Ω) comme l'a montré MUMFORD dans « On the equations defining abelian varieties. I ». Cette construction qui passe par le groupe thêta d'une variété abélienne munie d'une polarisation séparable sur un corps k sera présentée au chapitre 3. Pour faire le lien avec ce chapitre, on introduit le groupe thêta dans le cadre complexe à la fin de la section 2.6.

L'approche algébrique des fonctions thêta a sur l'approche analytique présentée dans ce chapitre, l'avantage de s'appliquer également à des variétés abéliennes non ordinaires sur un corps fini (et même sur un corps quelconque). Dans la suite, on utilise l'approche algébrique de Mumford afin d'avoir des résultats généraux. Nous avons néanmoins fait le choix de l'approche analytique dans ce chapitre pour éclairer l'approche algébrique, l'étude des variétés abéliennes algébriques s'étant historiquement beaucoup inspirée du cas complexe. Ainsi, on illustrera souvent une notion algébrique par son équivalent analytique pour mieux l'expliquer.

2.2 TORES COMPLEXES

Une variété abélienne complexe est un groupe de Lie complexe connexe A qui admet un plongement dans l'espace projectif. En particulier, A est compacte, et la proposition suivante montre que c'est un tore, c'est-à-dire le quotient d'un espace vectoriel complexe par un réseau de dimension maximale.

PROPOSITION 2.2.1. *Soit X un groupe de Lie complexe compact et connexe. Soit V son espace tangent en 0. Alors l'application exponentielle* $\exp : V \to X$ *a pour noyau un réseau*[1] Λ *et induit un isomorphisme* $V/\Lambda \xrightarrow{\sim} X$.

DÉMONSTRATION : Voir [Mum70, p. 2] ou [BL04, Lemme 1.1.1]. ∎

Nous allons donc commencer par examiner les tores complexes. Soit V un espace vectoriel complexe de dimension g et Λ un réseau dans V. Le tore $X = V/\Lambda$ est alors un groupe de Lie complexe de dimension g. Comme V est simplement connexe, c'est le revêtement universel de X ; dans ce chapitre, on note $\pi : V \to X$ le revêtement associé.

1. Λ est un réseau pour V vu en tant que $\mathbb{R}$-espace vectoriel .

PROPOSITION 2.2.2. *Soit $X = V/\Lambda$ et $X' = V'/\Lambda'$ deux tores. Alors toute application analytique de X vers X' est la composée d'un morphisme (de groupes de Lie) et d'une translation, et tout morphisme $f : X \to X'$ provient d'une (unique) application $\mathbb{C}$-linéaire $F : V \to V'$ tel que $F(\Lambda) \subset \Lambda'$.*

DÉMONSTRATION : Voir [BL04, Proposition 1.2.1]. L'application F déduite du morphisme f est simplement l'application tangente de F en $0 \in X$. ∎

Si on fixe une base de V et une $\mathbb{Z}$-base de Λ, l'inclusion $\Lambda \hookrightarrow V$ est représentée par une matrice $\Pi \in \mathrm{M}(g \times 2g, \mathbb{C})$. Réciproquement, une telle matrice Π est associée à un réseau si et seulement si $\begin{pmatrix} \mathrm{Re}\,\Pi \\ \mathrm{Im}\,\Pi \end{pmatrix}$ est inversible. Comme $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est équivalente à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ cela revient à ce que $\begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix}$ soit inversible. On dit que Π est la matrice des périodes du réseau X. Comme Λ est un réseau de V, il existe une base de V qui se complète en une base de Λ ; on peut donc toujours écrire Π sous la forme $\Pi = (\Omega, 1)$, où $\Omega \in \mathrm{M}_g(\mathbb{C})$ et $\mathrm{Im}\,\Omega$ est inversible.

Si l'on a un morphisme $f : X \to X' \simeq V'/\Lambda'$, l'application linéaire F de $V \to V'$ s'appelle la représentation analytique de f, et sa restriction $F_{|\Lambda}$ à Λ sa représentation rationnelle. Si on note A la matrice de F suivant des bases de V et de V', et R la matrice de $F_{|\Lambda}$ suivant des bases de Λ et Λ', on a donc $A\Pi = \Pi' R$ où Π' est la matrice des périodes de X'. On peut donc retrouver A à partir de R via la relation

$$\begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} = \begin{pmatrix} \Pi' \\ \overline{\Pi'} \end{pmatrix} R.$$

On obtient ainsi des représentations $\rho_a : \mathrm{Hom}(X, X') \to \mathrm{Hom}_{\mathbb{C}}(V, V'), f \mapsto F$ et $\rho_r : \mathrm{Hom}(X, X') \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda'), f \mapsto F_\Lambda$.

On peut également adopter un point de vue plus intrinsèque : si on oublie la structure complexe de X, X devient un tore réel de dimension $2g$ et est donc isomorphe à $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$. Une structure complexe J sur $\mathbb{R}^{2g}$ est une application $\mathbb{R}$-linéaire telle que $J^2 = -1$. Une telle application J détermine une structure complexe sur le tore $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$. L'espace des structures complexes sur $\mathbb{R}^{2g}$ est un espace homogène sous l'action par conjugaison de $\mathrm{Gl}_{2g}(\mathbb{R})$, et si J est une structure complexe, son stabilisateur est l'ensemble des $F \in \mathrm{Gl}_{2g}(\mathbb{R})$ tels que $FJ = JF$. Ainsi l'espace des structures complexes est un espace homogène principal sous $\mathrm{Gl}_g(\mathbb{C}) \backslash \mathrm{Gl}_{2g}(\mathbb{R})$ et la proposition 2.2.2 montre que les tores complexes, à isomorphisme près, forment un espace homogène principal sous $\mathrm{Gl}_g(\mathbb{C}) \backslash \mathrm{Gl}_{2g}(\mathbb{R}) / \mathrm{Gl}_{2g}(\mathbb{Z})$.

DÉFINITION 2.2.3. Une isogénie est un morphisme surjectif $f : X \to X'$ de noyau fini.

Ainsi f est une isogénie si et seulement si l'application analytique associée $F = \rho_a(f)$ est inversible. Si $\dim X = \dim X'$, il suffit que f soit surjective ou de noyau fini. Ainsi à isomorphisme près, on peut supposer que $F = \mathrm{Id}$, $\Lambda \subset \Lambda'$ et que f est l'application canonique $V/\Lambda \to V/\Lambda'$. Il y a donc bijection entre isogénies de domaine X et sous-groupes finis de X. Le degré de f est le cardinal de son noyau, c'est donc l'index du sous-groupe $\rho_r(f)(\Lambda)$ dans Λ'.

Si $n \in \mathbb{N}^*$, on note $[n] : X \to X, x \mapsto n.x$ l'isogénie de multiplication par n, et $X[n]$ son noyau. Il est clair que $X[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. Ainsi le groupe $\mathrm{End}(X)$ des endomorphismes de X est sans torsion et peut être plongé dans $\mathrm{End}_{\mathbb{Q}}(X) \coloneqq \mathrm{End}(X) \otimes \mathbb{Q}$.

DÉFINITION 2.2.4. Soit $f : X \to X'$ une isogénie, et e l'exposant de son noyau. L'isogénie contragrédiente de f est l'unique isogénie $g : X' \to X$ telle que $gf = fg = [e]$. Elle a pour noyau $f(X[e])$.

On voit donc que les isogénies définissent une relation d'équivalence sur les tores complexes. De plus, un élément de $\mathrm{End}(X)$ est inversible dans $\mathrm{End}_{\mathbb{Q}}(X)$ si et seulement s'il est une isogénie. (En effet, si $f : X \to X$ est une isogénie, et g l'isogénie contragrédiente, alors $gf = fg = [e]$ est inversible dans $\mathrm{End}_{\mathbb{Q}}(X)$. Réciproquement, on voit facilement qu'un élément de $\mathrm{End}(X)$ inversible dans $\mathrm{End}_{\mathbb{Q}}(X)$ a un noyau fini, et est donc une isogénie.)

2.3 FIBRÉS EN DROITES

Comme on l'a vu dans l'introduction, notre objectif ici est de décrire tous les plongements projectifs d'un tore complexe $X = V/\Lambda$. Si $f : X \to \mathbb{C}$ est une fonction analytique définie sur tout X, on peut visualiser f comme une fonction sur V invariante par Λ. Il est clair qu'une telle fonction est constante (car elle est bornée). Cependant, si on considère une classe de fonctions $f : V \to \mathbb{C}$ qui satisfont

$$f(v + \lambda) = a(v, \lambda) f(v) \tag{2.1}$$

où a est une fonction donnée de $V \times \Lambda \to \mathbb{C}^*$ qui satisfait la condition d'associativité $a(x, \lambda_1 + \lambda_2) = a(x, \lambda_1) a(x + \lambda_1, \lambda_2)$. Alors si les fonctions analytiques $f_1, \ldots, f_{n+1}$ sont dans cette classe, par définition de l'espace projectif $\mathbb{P}^n_{\mathbb{C}}$, l'application $v \in V \mapsto (f_1(v), \ldots, f_{n+1}(v)) \in \mathbb{P}^n_{\mathbb{C}}$ se factorise en une application rationnelle $X \to \mathbb{P}^n_{\mathbb{C}}$. On appelle la fonction a un facteur d'automorphie. Le but de cette section est d'analyser de tels facteurs d'automorphie. En particulier, on montre le théorème d'Appell-Humbert (voir le théorème 2.3.6) qui dit qu'un facteur d'automorphie est de la forme : $a(v, \lambda) = \chi(\lambda) e^{\pi H(v,\lambda) + \frac{\pi}{2} H(\lambda,\lambda)}$ où H est une forme hermitienne sur V qui prend des valeurs entières sur le réseau λ, et χ est un semi-caractère pour H (voir la définition 2.3.5 pour ces notions). Il n'existe pas forcément de fonctions définies sur tout V qui satisfont l'équation (2.1) (on appelle une telle fonction une section pour le facteur d'automorphie). Si $f : V \to \mathbb{C}$ est une fonction, on peut la voir comme une application $V \to V \times \mathbb{C}, v \mapsto (v, f(v))$ qui est une section de la projection canonique $V \times \mathbb{C} \to V$. Or Λ agit sur V par translation, et sur $V \times \mathbb{C}$ par $\lambda.(v, \alpha) \mapsto (v + \lambda, a(v, \lambda)\alpha)$. Ces actions donnent le diagramme commutatif suivant :

$$\begin{array}{ccc} V \times \mathbb{C} & \longrightarrow & (V \times \mathbb{C})/a(\Lambda) \\ \downarrow & & \downarrow p \\ V & \xrightarrow{\pi} & X = V/\Lambda. \end{array}$$

Il y a donc bijection entre les sections pour a définies sur tout V et les applications $f : V/\Lambda \to (V \times \mathbb{C})/a(\Lambda)$ telles que $p \circ f = \mathrm{Id}$. (Ici $(V \times \mathbb{C})/a(\Lambda)$ est le quotient de $V \times \mathbb{C}$ par l'action de Λ donnée par a, et $p : (V \times \mathbb{C})/a(\Lambda) \to V/\Lambda$ est la projection canonique induite par la projection $V \times \mathbb{C} \to V$.) Or comme Λ est un groupe discret qui agit proprement et librement sur V, on a localement pour un ouvert U assez petit de V : $(U \times \mathbb{C})/a(\Lambda) \simeq \pi(U) \times \mathbb{C}$, où π est l'application canonique $\pi : V \to X = V/\Lambda$. Autrement dit, il existe toujours des sections (analytiques) locales pour a. On appelle l'espace géométrique $\mathcal{L} = (V \times \mathbb{C})/a(\Lambda)$ un fibré en droites sur X, et on appelle les sections (locales) des sections (locales) pour $\mathcal{L}$. L'ensemble des sections locales pour $\mathcal{L}$ forment un faisceau qui détermine entièrement l'espace géométrique $\mathcal{L}$. Suivant le cas, on visualise $\mathcal{L}$ comme un espace géométrique ou comme un faisceau. Le reste de la section est consacré à l'étude des fibrés en droites sur X, en particulier on donne (une idée de) la preuve du théorème d'Appell-Humbert. Cette section est technique, et seul

l'énoncé du théorème 2.3.6 nous servira dans la suite. Le lecteur pressé pourra donc sans soucis admettre ce résultat et passer à la section 2.4.

On note $\mathrm{Pic}(X)$ le groupe des fibrés en droites sur X ; on a un isomorphisme canonique $\mathrm{Pic}(X) \simeq H^1(X, \mathcal{O}_X^*)$. Soit $\mathcal{L}$ un fibré en droites analytique sur X. On note $\widetilde{\mathcal{L}} = \pi^*\mathcal{L}$ l'image réciproque[1] de $\mathcal{L}$ sur V. Soit $\mathcal{O}_V$ le fibré des fonctions analytiques sur V et $\mathcal{O}_V^*$ celui des fonctions analytiques inversibles. De la suite exacte $0 \to \mathbb{Z} \to \mathcal{O}_V \xrightarrow{\exp} \mathcal{O}_V^* \to 0$ on en déduit que $H^p(V, \mathcal{O}_V^*) = 0$ pour $p > 0$; en effet $H^p(V, \mathbb{Z}) = H^{p+1}(V, \mathcal{O}_V) = 0$ comme V est simplement connexe. Ainsi tout fibré en droites sur V est trivial, et $\widetilde{\mathcal{L}}$ s'identifie au fibré trivial $V \times \mathbb{C}$. Il existe une action de Λ sur $\widetilde{\mathcal{L}}$ telle que $\mathcal{L}$ soit le quotient de $\widetilde{\mathcal{L}}$ par Λ. Cette action induit donc via l'isomorphisme précédent une action Φ de Λ sur $\mathbb{C} \times V$. L'action Φ est de la forme $(\alpha, v) \mapsto \Phi_u(\alpha, v) = (e_u(v).\alpha, v + u)$ pour $u \in \Lambda$ où $e_u \in \Gamma(\mathcal{O}_V^*)$ est une fonction analytique inversible. Par associativité on trouve de plus que $e_{u+u'}(z) = e_u(z + u')e_{u'}(z)$, ce qui signifie que $u \mapsto e_u$ est un 1-cocyle à valeurs dans $\Gamma(\mathcal{O}_V^*)$. Réciproquement, un tel cocycle permet de définir un fibré sur X comme quotient du fibré trivial par l'action de Λ induite par ce cocycle. Qui plus est, si l'on prend un automorphisme du fibré trivial donné par une section $f \in \Gamma(\mathcal{O}_V^*)$, le cocycle e_u est changé par un cobord : $e'_u(v) = e_u(v)f(v + u)/f(v)$.

On note exp *l'application exponentielle : $x \mapsto e^{2ix}$*

MUMFORD montre dans [Mum70, p. 22] que si on a une action libre et propre d'un groupe G discret sur un espace topologique localement simplement connexe X, on peut étudier les faisceaux sur X/G via l'action de G sur les sections globales de leurs préimages. On se restreint ici au cas $X = V$ et $G = \Lambda$:

THÉORÈME 2.3.1. *Pour tout faisceau $\mathcal{F}$ sur X il existe un morphisme naturel*[2]

$$\Phi : H^p(\Lambda, \Gamma(V, \pi^*\mathcal{F})) \to H^p(X, \mathcal{F}),$$

qui commute aux cup-products. De plus, si

$$0 \longrightarrow \mathcal{F}' \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}'' \longrightarrow 0$$

est une suite exacte telle que

$$0 \longrightarrow \Gamma(V, \pi^*\mathcal{F}') \longrightarrow \Gamma(V, \pi^*\mathcal{F}) \longrightarrow \Gamma(V, \pi^*\mathcal{F}'') \longrightarrow 0$$

soit également exacte, alors Φ commute aux morphismes de connexions dans la suite longue de cohomologie. Enfin si $H^i(X, \pi^*\mathcal{F}) = 0, \forall\, i \geqslant 1$, Φ est un isomorphisme.

Appliquant le théorème précédent à $\mathcal{O}_X^*$, on retrouve le fait que $H^1(X, \mathcal{O}_X^*) \simeq H^1(\Lambda, \Gamma(\mathcal{O}_V^*))$. Si $\mathcal{F}$ est un fibré en droite sur X, on note $a_{\mathcal{F}} : \Lambda \times V \to V$ un cocycle représentant $\mathcal{F}$; on dit que $a_{\mathcal{F}}$ est le facteur d'automorphie associé à $\mathcal{F}$. On voit également que $\Gamma(X, \mathcal{F}) \simeq \Gamma(V, \pi^*\mathcal{F})^\Lambda$, et comme $\pi^*\mathcal{F}$ est trivial, les sections globales de $\mathcal{F}$ sont exactement les fonctions analytiques $\vartheta : V \to \mathbb{C}$ telles que

Si un groupe G agit sur X on note X^G les éléments invariants par G.

$$\vartheta(z + \lambda) = a_{\mathcal{F}}(\lambda, z)\vartheta(z)$$

pour tout $\lambda \in \Lambda$ et $z \in V$.

Enfin, si $\phi : X \to X' = V'/\Lambda'$ est un morphisme de tores complexes, $\mathcal{F}'$ un fibré en droites sur X' de facteur d'automorphie $a_{\mathcal{F}'}$, la naturalité de Φ montre que le facteur d'automorphie associé à $\phi^*\mathcal{F}'$ est $(\rho_r(\phi), \rho_a(\phi))^* a_{\mathcal{F}'}$.

1. En Anglais le terme est ''pullback'', que j'avais traduit par « tiré en arrière », mais Jean-François MESTRE m'a signalé que le terme « image réciproque » était d'usage en Français.
2. En particulier, Φ est fonctoriel sur les $\mathcal{F}$.

Les facteurs d'automorphie nous donnent une description très explicite des fibrés en droites sur un tore complexe. Il nous reste à analyser quelle forme ces facteurs d'automorphie peuvent prendre.

Partons de la suite exacte induite par l'exponentielle

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^* \to 0.$$

On déduit de cette suite exacte un morphisme de connexion $c_1 : H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbb{Z})$. Si $\mathcal{L}$ est un fibré en droites sur X, $c_1(\mathcal{L})$ est appelé la (première) classe de Chern de $\mathcal{L}$. Pour comprendre c_1, on voit qu'il faut analyser les espaces de cohomologie $H^2(X, \mathbb{Z})$ et $H^2(X, \mathcal{O}_V)$.

THÉORÈME 2.3.2. *Soit X un tore complexe. L'algèbre $H^\star(X, \mathbb{Z})$ munie du cup-product est isomorphe à l'algèbre $\bigwedge^\star \Lambda^*$ où $\Lambda^* := \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$.*

L'algèbre $H^\star(X, \mathbb{C})$ est isomorphe à l'algèbre $\bigwedge^\star \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C})$. De plus, si $T = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ est l'espace des formes linéaires sur V et $\overline{T} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, C)$ l'espace des formes antilinéaires, on a $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) = T + \overline{T}$ et donc $H^n(X, \mathbb{C}) = \bigoplus_{p+q=n} \bigwedge^p T \otimes \bigwedge^q \overline{T}$.

L'algèbre $H^\star(X, \mathcal{O}_X)$ est isomorphe à l'algèbre $\bigwedge^\star \overline{T}$.

Enfin, les inclusions $\mathbb{Z} \subset \mathbb{C} \subset \mathcal{O}_X$ induisent des morphismes $H^n(X, \mathbb{Z}) \to H^n(X, \mathbb{C}) \to H^n(X, \mathcal{O}_X)$. Les morphismes correspondants sur les algèbres extérieures sont donnés par $\bigwedge^n \Lambda^* \xrightarrow{\bigwedge^n i} \bigwedge^n (T \oplus \overline{T})$ où i est l'inclusion $\Lambda^* = \mathrm{Hom}(\Lambda, \mathbb{Z}) \to \mathrm{Hom}(\Lambda, \mathbb{Z}) \otimes \mathbb{C} = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C})$ et par $\bigwedge^n (T \oplus \overline{T}) \xrightarrow{\bigwedge^n p} \bigwedge^n \overline{T}$ où p est la projection $T \oplus \overline{T} \to \overline{T}$.

DÉMONSTRATION : Comme V est le revêtement universel de X, on a $\pi_1(X) = \Lambda$ et le théorème du coefficient universel donne $H^1(X, \mathbb{Z}) = \mathrm{Hom}(\Lambda, \mathbb{Z})$. La formule de Künneth donne alors $H^n(X, \mathbb{Z}) = \bigwedge^n \Lambda^*$, et le théorème du coefficient universel donne $H^n(X, \mathbb{C}) = H^n(X, \mathbb{Z}) \otimes \mathbb{C} = \bigwedge^n \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) = \bigoplus_{p+q=n} \bigwedge^p T \otimes \bigwedge^q \overline{T}$.

Le théorème de De Rham permet d'affirmer que $H^n(X, \mathbb{C})$ est isomorphe aux n-formes différentielles closes modulo les formes exactes. Si λ_i est une base de Λ, notons x_i les fonctions coordonnées (réelles) correspondantes. Les formes différentielles dx_i sont invariantes (par translation), donc descendent en des formes différentielles dx_i sur X, qui forment une base de $H^1(X, \mathbb{C})$; car $\int_{\lambda_i} dx_j = \delta_{ij}$. Comme le *cup-product* correspond au produit extérieur des formes différentielles, une base de $H^n(X, \mathbb{C})$ est ainsi donnée par les $dx_{i_1} \wedge \cdots \wedge dx_{i_n}$. On voit donc que $H^n(X, \mathbb{C})$ est isomorphe à l'espace $IF^n(X)$ des formes différentielles de degré n sur X invariantes par translation.

Maintenant, si $v_1, \ldots, v_g$ sont des coordonnées complexes sur V, les formes différentielles $dv_1, \ldots, dv_g, d\bar{v}_1, \ldots d\bar{v}_g$ descendent en une base des formes invariantes sur X. Si $p + q = n$, une forme différentielle de type $dv_1 \wedge \cdots \wedge dv_p \wedge d\bar{v}_1 \wedge \dot{\wedge} d\bar{v}_q$ est dite de type (p, q). Les combinaisons linéaires de telles formes donnent un sous-espace $IF^{p,q}(X)$ de $IF^n(X)$. Il est facile de voir que $IF^n(X) = \bigoplus_{p+q=n} IF^{p,q}(X)$, et que $IF^{p,q}(X) = \bigwedge^p T \otimes \bigwedge^q \overline{T}$.

La décomposition de Hodge s'écrit $H^n(X, \mathbb{C}) = \bigoplus_{p+q=n} H^q(X, \Omega_X^p)$ où Ω_X^p est le faisceau des p-formes holomorphes sur X. On a $\mathcal{O}_X \otimes_{\mathbb{C}} \bigwedge^p T \xrightarrow{\sim} \Omega_X^p$, donc $H^q(X, \Omega_X^p) = H^q(X, O_X) \otimes \bigwedge^p T$. On conclut via des arguments d'analyse harmonique que $H^q(X, O_X) \simeq IF^{0,q}(X) \simeq \bigwedge^q \overline{T}$.

Enfin, la description précédente montre que les morphismes induits sur les algèbres extérieures par les inclusions $\mathbb{Z} \subset \mathbb{C} \subset \mathcal{O}_X$ sont bien les morphismes naturels. Il suffit en fait de le vérifier sur les H^1 et d'utiliser la compatibilité avec le cup-product.

Pour plus de détails, voir [Mum70, p. 3-13] ou [BL04, Section 1.3 et 1.4]. Dans la suite on a juste besoin de la description des groupes $H^n(X,\cdot)$ pour $n = 1, 2$, il n'y aurait donc pas besoin d'invoquer un résultat comme la décomposition de Hodge (même si elle est plus facile à prouver sur les tores complexes). Cependant, comme on donne juste une idée de la preuve, ceci nous permet de faire une description plus complète de la structure des groupes de cohomologie sur X, qui se révèle très intéressante. ■

Dans la suite on note également $\mathrm{Alt}^n_{\mathbb{R}}(V,\mathbb{C})$ le groupe $\bigwedge^n \mathrm{Hom}_{\mathbb{R}}(V,\mathbb{C})$ des $\mathbb{R}$-formes alternées sur $\mathbb{C}$.

En combinant les théorèmes 2.3.1 et 2.3.2 on obtient le diagramme commutatif suivant :

$$\begin{array}{ccccc}
H^1(\Lambda,\Gamma(\mathcal{O}_V^*)) & \longrightarrow & H^2(\Lambda,\mathbb{Z}) & & \\
\downarrow\wr & & \downarrow\wr & & \\
H^1(X,\mathcal{O}_X^*) & \xrightarrow{c_1} & H^2(X,\mathbb{Z}) & \xrightarrow{\gamma} & H^2(X,\mathcal{O}_X) \\
 & & \downarrow\wr & & \downarrow\wr \\
 & & \bigwedge^2\Lambda^* & \longrightarrow & \bigwedge^2\overline{T}.
\end{array}$$

Proposition 2.3.3. *La flèche $H^2(\Lambda,\mathbb{Z}) \xrightarrow{\sim} \bigwedge^2\Lambda^*$ est donnée par*

$$F \in Z^2(\Lambda,\mathbb{Z}) \mapsto ((u,v) \mapsto F(u,v) - F(v,u)).$$

Ainsi si $a_{\mathcal{F}} \in Z^1(\Lambda,\Gamma(\mathcal{O}_V^*))$ est un facteur d'automorphie associé à $\mathcal{F} \in H^1(X,\mathcal{O}_X^*)$, on peut écrire $a_{\mathcal{F}} = \exp(2\pi i g)$ et $c_1(\mathcal{L})$ correspond à la forme alternée sur Λ $E_{\mathcal{L}} : (\lambda_1,\lambda_2) \mapsto g(\lambda_2, v+\lambda_1) + g(\lambda_1, v) - g(\lambda_1, v+\lambda_2) - g(\lambda_2, v)$ pour v quelconque dans V.

L'extension réelle $E_{\mathcal{L}} \in \mathrm{Alt}^2_{\mathbb{R}}(V,\mathbb{C})$ satisfait $E(ix,iy) = E(x,y)$ pour tout $x, y \in V$. Réciproquement, l'image de la classe de Chern c_1 correspond exactement aux formes alternées $E \in \mathrm{Alt}^2_{\mathbb{R}}(V,\mathbb{C})$ telles que $E(\Lambda,\Lambda) \subset \mathbb{Z}$ et $E(ix,iy) = E(x,y)$ pour tout $x, y \in V$.

Démonstration : Voir [Mum70, p. 16] ou [BL04, Théorème 2.1.2] pour la description de l'isomorphisme $H^2(\Lambda,\mathbb{Z}) \to \bigwedge^2\Lambda^*$.

Il reste à déterminer l'image de c_1, ou de manière équivalente le noyau de γ. Or γ se factorise en $H^2(X,\mathbb{Z}) \xrightarrow{i} H^2(X,\mathbb{C}) \xrightarrow{j} H^2(X,\mathcal{O}_X)$, que l'on peut voir via les isomorphismes du théorème 2.3.2 comme le morphisme canonique : $\mathrm{Alt}^2(\Lambda,\mathbb{Z}) \xrightarrow{i} \mathrm{Alt}^2_{\mathbb{R}}(V,\mathbb{C}) \xrightarrow{j} \bigwedge^2\overline{T}$. Ainsi, $i(E_{\mathcal{L}})$ est l'extension réelle de $E_{\mathcal{L}}$, que l'on peut écrire sous la forme $i(E_{\mathcal{L}}) = E_1 + E_2 + E_3$ où $E_1 \in \bigwedge^2 T$, $E_2 \in T \otimes \overline{T}$ et $E_3 \in \bigwedge^2\overline{T}$. Comme $i(E_{\mathcal{L}})$ est à valeurs réelles, $E_1 = \overline{E_3}$, comme $j \circ i(E_{\mathcal{L}}) = E_3$, on voit que $E_{\mathcal{L}}$ est dans le noyau de γ si et seulement si $E_{\mathcal{L}} = E_2$, c'est-à-dire si et seulement si $E(ix,iy) = E(x,y)$ pour tout $x, y \in V$. ■

Ainsi la classe de Chern d'un fibré en droites est une forme alternée $E_{\mathcal{L}}$. Cette forme joue un rôle important par la suite. En particulier elle détermine entièrement la polarisation associée à un fibré ample $\mathcal{L}$. Le lemme suivant montre qu'on peut voir $E_{\mathcal{L}}$ comme une forme hermitienne sur V :

On appelle aussi $E_{\mathcal{L}}$ la forme de Riemann associée à $\mathcal{L}$.

Lemme 2.3.4. *Il y a bijection entre les formes hermitiennes H sur V et les formes alternées réelles E sur V telles que $E(ix,iy) = E(x,y)$ pour tout $x, y \in V$. Cette bijection est donnée par*

$$E(x,y) = \mathrm{Im}\, H(x,y) \quad \text{et} \quad H(x,y) = E(ix,y) + iE(x,y).$$

On appelle groupe de Néron-Severi le noyau de $\gamma : H^2(X,\mathbb{Z}) \to H^2(X,\mathcal{O}_X)$. C'est l'ensemble des classes de Chern des éléments de $\mathrm{Pic}(X)$; on le note $\mathrm{NS}(X)$. Enfin on appelle $\mathrm{Pic}_0(X)$ le noyau de $c_1 : \mathrm{Pic}(X) \to H^2(X,\mathbb{Z})$.

Si $\mathcal{L} \in \mathrm{Pic}(X)$ a pour forme de Chern associée E et forme hermitienne associée H, on peut montrer (voir le théorème 2.3.6) qu'il existe toujours un facteur d'automorphie représentant $\mathcal{L}$ de la forme $a_{\mathcal{L}}(\lambda,v) = \chi(\lambda)e^{\pi H(v,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}$ où $\chi : \Lambda \to \mathbb{C}_1^*$ (où on note $\mathbb{C}_1^*$ le groupe des éléments de norme 1 de $\mathbb{C}$) est un semi-caractère pour E, c'est-à-dire que l'on a $\chi(\lambda_1+\lambda_2) = \chi(\lambda_1)\chi(\lambda_2)e^{i\pi E(\lambda_1,\lambda_2)}$ si $\lambda_1,\lambda_2 \in \Lambda$. Réciproquement, si H est une forme hermitienne telle que $\mathrm{Im}\, H(\Lambda,\Lambda) \subset \mathbb{Z}$ et χ est un semi-caractère pour[1] H, alors $a(\lambda,v) = \chi(\lambda)e^{\pi H(v,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}$ est un facteur d'automorphie.

Définition 2.3.5. Avec les notations précédentes, on note $L(H,\chi)$ le fibré en droites associé au facteur d'automorphie $a(\lambda,v) = \chi(\lambda)e^{\pi H(v,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}$.

Théorème 2.3.6 (Appell-Humbert). *L'ensemble des (H,χ) où H est une forme hermitienne telle que $\mathrm{Im}\, H(\Lambda,\Lambda) \subset \mathbb{Z}$ et χ est un semi-caractère pour H forme un groupe via*

$$(H_1,\chi_1).(H_2,\chi_2) = (H_1+H_2,\chi_1\chi_2).$$

L'application $(H,\chi) \to L(H,\chi)$ est un isomorphisme de ce groupe sur $\mathrm{Pic}\, X$ *qui rend le diagramme suivant commutatif :*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(\Lambda,\mathbb{C}_1^*) & \longrightarrow & \textit{Le groupe des } (H,\chi) & \longrightarrow & \textit{Formes hermitiennes sur } V \textit{ telles que } \mathrm{Im}\, H(\Lambda,\Lambda) \subset \mathbb{Z}. & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \mathrm{Pic}_0(X) & \xrightarrow{c_1} & \mathrm{Pic}(X) & \longrightarrow & \mathrm{NS}(X) & \longrightarrow & 0.
\end{array}$$

Démonstration : Les deux suites horizontales sont exactes, et la proposition 2.3.3 montre que la flèche verticale de droite est un isomorphisme. Il suffit donc de montrer que la flèche verticale de gauche est un isomorphisme, soit $\mathrm{Hom}(\Lambda,\mathbb{C}_1^*) \simeq \mathrm{Pic}_0(X)$ (où $\mathbb{C}_1^*$ est le groupe des unités dans $\mathbb{C}^*$).

Si $\chi \in \mathrm{Hom}(\Lambda,\mathbb{C}_1^*)$, le facteur d'automorphie associé est trival dans $H^1(V,\Gamma(\mathcal{O}_V^*))$ si et seulement s'il existe $g \in \Gamma(\mathcal{O}_V^*)$ tel que $\chi(\lambda) = g(v+\lambda)/g(v)$ pour tout $\lambda \in \Lambda$ et $v \in V$. Cela impose g constant, et donc $\chi = 1$, d'où l'injectivité de $\mathrm{Hom}(\Lambda,\mathbb{C}_1^*) \hookrightarrow \mathrm{Pic}_0(X)$.

Pour la surjectivité, on a le diagramme suivant :

$$\begin{array}{ccccccc}
H^1(\Lambda,\mathbb{C}) & \longrightarrow & H^1(\Lambda,\Gamma(\mathcal{O}_V)) & \xrightarrow{\exp} & \mathrm{Ker}[H^1(\Lambda,\Gamma(\mathcal{O}_V^*)) & \longrightarrow & H^2(\Lambda,\mathbb{Z})] \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
H^1(X,\mathbb{C}) & \longrightarrow & H^1(X,\mathcal{O}_X) & \xrightarrow{\exp} & \mathrm{Ker}[H^1(X,\mathcal{O}_X^*) & \xrightarrow{c_1} & H^2(X,\mathbb{Z})] = \mathrm{Pic}_0(X).
\end{array}$$

1. Par abus de notation on appelle un semi-caractère pour H un semi-caractère pour $\mathrm{Im}\, H$.

On sait que $H^1(X,\mathbb{C}) \twoheadrightarrow H^1(X,\mathcal{O}_X)$ est surjectif ; ainsi tout fibré de $\mathrm{Pic}_0(X)$ est représenté par un facteur d'automorphie à facteurs constants : $a(\lambda,v) = \exp(\alpha(\lambda))$ où $\alpha \in \mathrm{Hom}(\Lambda,\mathbb{C})$. On montre qu'on peut normaliser α pour que a soit à valeurs dans $\mathbb{C}_1^*$, ce qui conclut la preuve.

Pour plus de détails, voir [Mum70, p. 20] ou [BL04, Théorème 2.2.3]. ■

2.4 VARIÉTÉS ABÉLIENNES ET POLARISATION

Le but de cette section est d'étudier quand un tore complexe $X = V/\Lambda$ est une variété abélienne, autrement dit quand X admet un plongement dans l'espace projectif. On a vu dans la section 2.3 qu'un facteur projectif (autrement dit un fibré en droites $\mathcal{L}$) définissait un morphisme (pas forcément défini sur tout X) $X \to \mathbb{P}_{\mathbb{C}}^{\deg \mathcal{L}}$ (réciproquement on peut montrer que tout tel morphisme vient d'un fibré en droites [Haroo, Théorème 7.1 p. 150 ; GD64, ÉGA 2, Chapitre 4]). On dit que le fibré $\mathcal{L}$ est très ample lorsque le morphisme projectif associé est un plongement. De manière plus terre à terre, lorsqu'on a un fibré $\mathcal{L}$, on peut regarder une base $(\vartheta_1,\dots,\vartheta_n)$ des sections globales, qui fournissent alors un système de coordonnées sur X. Alors $\mathcal{L}$ est très ample si ce système de coordonnées induit un plongement de X dans l'espace projectif. Grosso modo, pour qu'un fibré $\mathcal{L}$ soit très ample, il faut donc qu'il admette suffisamment de sections globales. Si $\mathcal{L}$ est un fibré en droites sur X, une idée pour avoir plus de sections globales est de considérer le fibré en droites $\mathcal{L}^n$ (où $n \in \mathbb{N}$), dont le faisceau associé est constitué de sections locales qui sont sommes de n produits de sections locales de $\mathcal{L}$. On dit que $\mathcal{L}$ est ample lorsque $\mathcal{L}^n$ est très ample pour n suffisamment grand. Autrement dit : le tore complexe X est une variété abélienne si et seulement si X admet un fibré en droites ample.

D'après le théorème d'Appell-Humbert précédent, tout fibré en droites sur X est de la forme $\mathcal{L} = L(H,\chi)$ où H est une forme hermitienne sur V et χ un semi-caractère pour H. Les sections de $L(H,\chi)$ sont donc les fonctions holomorphes sur V qui vérifient l'équation fonctionnelle

$$\vartheta(z+\lambda) = \chi(\lambda)e^{\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}.$$

De telles fonctions sont appelées des fonctions thêta pour $L(H,\chi)$.

Si H a une valeur propre strictement négative, il est facile de voir que $\Gamma(L(H,\chi)) = 0$. De même, si H est dégénérée, alors l'espace isotrope $N = \{x \in V \mid H(x,y) = 0 \ \forall y \in V\}$ est tel que $N/(N \cap \Lambda)$ soit un tore, et toute fonction theta pour $L(H,\alpha)$ se factorise via une fonction thêta sur $N/(N\cap\Lambda)$ pour H et χ descendus à V/N. Ainsi si $L(H,\chi)$ est ample, H est définie positive. Réciproquement on a la

PROPOSITION 2.4.1. *Le fibré en droites $L(H,\chi)$ est ample si et seulement si H est définie positive.*

DÉMONSTRATION : Voir [Mum70, p. 30] ou [BL04, Théorème 4.5.1]. ■

Ainsi le tore X est une variété abélienne si et seulement s'il existe une forme symplectique[1] réelle E sur V à coefficients entiers sur Λ et telle que $E(ix,iy) = E(x,y)$ pour tout $x,y \in \Lambda$. À partir de maintenant on se restreint aux variétés abéliennes, et on considère des fibrés algébriques plutôt qu'analytiques.

Un fibré ample $\mathcal{L}$ sur une variété abélienne X induit un morphisme rationnel de X dans $\mathbb{P}^{\deg\mathcal{L}-1}(\mathbb{C})$. Ce morphisme n'est pas nécessairement un plongement (si $\mathcal{L}$ n'est pas très ample). En revanche $\mathcal{L}$ détermine toujours une polarisation, c'est-à-dire une isogénie de X

1. Une forme symplectique est une application bilinéaire alternée et non dégénérée.

sur sa variété duale. Ce concept est très important pour la suite, on va donc l'étudier pour le reste de cette section.

Commençons par un lemme élémentaire concernant les opérations classiques sur les fibrés :

LEMME 2.4.2. *Soit H (resp. H') une forme hermitienne sur V et χ (resp. χ') un semi-caractère pour H (resp. pour H'). On a :*

- $L(H,\chi)\otimes L(H',\chi') = L(H+H',\chi\chi')$. *En particulier,* $L(H,\chi)^n = L(nH,\chi^n)$.
- *Si $L(H,\chi)$ est un fibré en droites sur X, alors pour tout $v\in V$ on a*

Par abus de notation on note t_v le morphisme de translation par $\pi(v)$.

$$t_v^* L(H,\chi) = L(H,\chi\exp(\operatorname{Im} H(v,\cdot))).$$

- *Si $f : X\to X'$ est une isogénie, et $L(H,\chi)$ un fibré en droites sur X', alors $f^*L(H,\chi) = L(\rho_a(f)^*H, \rho_r(f)^*\chi)$.*

DÉMONSTRATION : Il suffit de regarder comment se comporte le facteur d'automorphie associé par ces opérations.

Par exemple, si $a_{\mathcal{L}}$ est le facteur d'automorphie associé à un fibré en droites $\mathcal{L}$ sur X', alors par définition l'espace géométrique associé à $f^*\mathcal{L}$ est le produit fibré :

$$\begin{array}{ccc} V\times\mathbb{C}/a_{f^*\mathcal{L}}(\Lambda) & \longrightarrow & (V\times\mathbb{C})/a_{\mathcal{L}}(\Lambda') \\ \downarrow & & \downarrow \\ X = V/\Lambda & \xrightarrow{\ f\ } & X' = V/\Lambda'. \end{array}$$

On vérifie immédiatement que le facteur d'automorphie $a_{f^*\mathcal{L}}$ associé à $f^*\mathcal{L}$ est donné par

$$a_{f^*\mathcal{L}}(v,\lambda) = a_{\mathcal{L}}(\rho_a(f)(v),\rho_r(f)(\lambda)).$$ ■

REMARQUE 2.4.3. En reprenant les notations du lemme 2.4.2, si $\mathcal{L}$ est un fibré très ample sur X', $f^*\mathcal{L}$ est un fibré très ample sur X. Comme le facteur d'automorphie de $f^*\mathcal{L}$ est l'image réciproque du facteur d'automorphie de $\mathcal{L}$, on peut espérer trouver une relation explicite entre les coordonnées projectives de X' associées à $\mathcal{L}$ et celles de X associées à $f^*\mathcal{L}$. Autrement dit, on peut espérer arriver à expliciter l'isogénie f par rapport à ces systèmes de coordonnées. On verra que c'est effectivement le cas dans la section 3.6. ◇

On en déduit en particulier que les variétés abéliennes sont closes par isogénies. Une autre application est le

COROLLAIRE 2.4.4 (THÉORÈME DU CARRÉ). *Pour tout $x, y\in X$ et fibré $\mathcal{L}\in \operatorname{Pic}(X)$ on a*

$$t_{x+y}^*(\mathcal{L}) \simeq t_x^*\mathcal{L}\otimes t_y^*\mathcal{L}\otimes\mathcal{L}^{-1}.$$

Si $\mathcal{L} = L(H,\chi)$ est un fibré sur X, on dit qu'il est symétrique si $[-1]^*\mathcal{L}\simeq\mathcal{L}$, et antisymétrique si $[-1]^*\mathcal{L}\simeq\mathcal{L}^{-1}$. Si $\mathcal{L}$ appartient à $\operatorname{Pic}_0(X)$, $\mathcal{L}$ est antisymétrique, et le fibré correspondant à $L(H,\chi)$ est symétrique si et seulement si $\chi(\Lambda)\subset\{\pm1\}$. Les fibrés symétriques joueront un grand rôle dans la suite, car la condition de symétrie est indispensable dans la description de l'espace modulaire des thêta null-points. Toujours comme application du lemme 2.4.2, on a le

COROLLAIRE 2.4.5. *Pour tout $n \in \mathbb{Z}$ et fibré $\mathcal{L} \in \mathrm{Pic}(X)$ on a*

$$[n]^*\mathcal{L} = \mathcal{L}^{\frac{n^2+n}{2}} \otimes [-1]^*\mathcal{L}^{\frac{n^2-n}{2}}.$$

Ainsi si $\mathcal{L}$ est symétrique, $[n]^*\mathcal{L} \simeq \mathcal{L}^{n^2}$ et si $\mathcal{L}$ est antisymétrique, $[n]^*\mathcal{L} \simeq \mathcal{L}^n$.

DÉMONSTRATION : Encore une fois, il suffit de regarder le comportement des facteurs d'automorphie. Le détail est dans [BL04, Proposition 2.3.5]. ∎

Une des conséquences du théorème d'Appell-Humbert est le fait que $\mathrm{Pic}_0(X) \simeq \mathrm{Hom}(\Lambda, \mathbb{C}_1^*)$. Or $\mathrm{Hom}(\Lambda, \mathbb{C}_1^*)$ est un tore complexe : $\overline{T} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$, l'espace des applications anti-linéaires, est un espace vectoriel complexe de dimension g, et l'application $\phi : \overline{T} \to \mathrm{Hom}(\Lambda, \mathbb{C}_1^*), l \mapsto \exp(\mathrm{Im}\, l(\cdot))$ induit un isomorphisme $\overline{T}/\overline{\Lambda} \xrightarrow{\sim} \mathrm{Pic}_0(X)$ où $\overline{\Lambda} = \{l \in \overline{T} \mid \mathrm{Im}\, l(\Lambda) \subset \mathbb{Z}\}$ est le noyau de ϕ. Comme la forme $\overline{T} \times V \to \mathbb{R}, (l, v) \mapsto \mathrm{Im}\, l(v)$ est non dégénérée, $\overline{\Lambda}$ est un réseau de $\overline{T}$ et $\mathrm{Pic}_0(X)$ est bien un tore. On appelle $\widehat{X}$ l'espace $\mathrm{Pic}_0(X)$ vu avec sa structure de tore complexe ; on dit que $\widehat{X}$ est la variété abélienne duale de X.

En effet, on va voir que $\widehat{X}$ est isogène à X, donc est une variété abélienne.

PROPOSITION 2.4.6. *Soit $f : X \to X'$ une isogénie de variétés abéliennes. Alors l'application $\widehat{f} : \mathrm{Pic}_0(X') \to \mathrm{Pic}_0(X), \mathcal{L} \mapsto f^*\mathcal{L}$ est une isogénie de noyau $\mathrm{Ker}\,\widehat{f} = \mathrm{Hom}(\mathrm{Ker}\, f, \mathbb{C}_1^*)$. On l'appelle l'isogénie duale.*

DÉMONSTRATION : Si F est la représentation analytique de f, on vérifie que la représentation analytique de $\widehat{f}$ est donnée par F^* où F^* est l'application (anti)-duale de F. ∎

Plus généralement on peut montrer que $X \mapsto \widehat{X}$ est un foncteur exact, et la flèche $X \xrightarrow{\sim} \widehat{\widehat{X}}$ est un isomorphisme canonique.

Si $\mathcal{L} \in \mathrm{Pic}(X)$, le lemme 2.4.2 et le corollaire 2.4.4 montrent qu'il existe un morphisme $\phi_{\mathcal{L}} : X \to \widehat{X}, x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. Via le théorème d'Appell-Humbert, le lemme 2.4.2 montre que $\phi_{\mathcal{L}}(x)$ est le fibré de Pic_0 représenté par le caractère $\chi = e^{2\pi i E(x,\cdot)}$. Il est facile de voir alors que si $\mathcal{L} = L(H, \chi)$, la représentation analytique de $\phi_{\mathcal{L}}$ est $\phi_H : V \to \overline{T}, v \mapsto H(v, \cdot)$. Ainsi $\phi_{\mathcal{L}}$ ne dépend que de la classe de Chern de $\mathcal{L}$, et on peut montrer que deux fibrés en droites sont algébriquement équivalents si et seulement s'ils ont la même classe de Chern [BL04, Proposition 2.5.3]. Réciproquement, une application $f : X \to \widehat{X}$ est de la forme $\phi_{\mathcal{L}}$ pour un fibré en droites $\mathcal{L}$ sur X si et seulement si l'application $H : V \times V \to \mathbb{C}, (v, w) \mapsto \rho_a(f)(v)(w)$ est hermitienne, et H est alors le type de $\mathcal{L}$ [BL04, Théorème 2.5.5]. Enfin, le morphisme $\phi_{\mathcal{L}}$ est une isogénie dès que $\mathcal{L}$ est non dégénéré[1] ; on note $K(\mathcal{L})$ son noyau.

Une variété abélienne polarisée est un couple $(X, \mathcal{L})$ où X est une variété abélienne complexe et $\mathcal{L}$ un fibré ample sur X. Si $H = c_1(\mathcal{L})$ est la classe de $\mathcal{L}$, H est une forme hermitienne définie positive. Le morphisme $\phi_{\mathcal{L}} : X \to \widehat{X}$ est alors une isogénie, on dit que c'est la polarisation associée à $\mathcal{L}$, elle ne dépend que de la classe H de $\mathcal{L}$. Le noyau $K(\mathcal{L})$ de $\phi_{\mathcal{L}}$ est l'ensemble des x dans X tels que $t_x^*\mathcal{L} \simeq \mathcal{L}$. Dit autrement, si on prend une base des fonctions thêta associées à $\mathcal{L}$, $K(\mathcal{L})$ est l'ensemble des éléments de X pour lesquels la translation par x s'écrit linéairement sur cette base. Ce fait a de nombreuses applications, en particulier pour le calcul d'isogénies associées à un sous-groupe de $K(\mathcal{L})$. De même, si $\mathcal{L}$ est symétrique, l'inversion $x \mapsto -x$ s'exprime facilement sur les fonctions thêta.

Si $\mathcal{L} = L(H, \chi)$ est un fibré ample, et $E = \mathrm{Im}\, H$ est la forme symplectique associée, on note $\Lambda(\mathcal{L}) = \{v \in V | E(v, \Lambda) \subset \mathbb{Z}\}$ l'orthogonal de Λ. En revenant aux définitions de $\phi_{\mathcal{L}}$ et de

1. Un fibré $L(H, \chi)$ est dit non dégénéré lorsque H l'est.

$\widehat{X}$, on voit que $K(\mathcal{L}) = \Lambda(\mathcal{L})/\Lambda$. Plus généralement, si on a un réseau $\Lambda_0 \subset V$, on appelle le réseau $\Lambda_0^\perp := \{v \in V \mid E(v, \Lambda_0) \subset \mathbb{Z}\}$ l'orthogonal de Λ_0 par rapport à E (ou par abus de notation par rapport à H). Comme $\Lambda(\mathcal{L})$ est orthogonal à Λ, la forme symplectique (additive) E induit une forme symplectique (multiplicative) $e^{2i\pi E(\cdot,\cdot)}$ sur $K(\mathcal{L})$.

Une décomposition symplectique de Λ est une décomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$ telle que les Λ_i, $i = 1, 2$ soient des sous-espaces isotropes maximaux pour E. Une telle décomposition induit une décomposition symplectique $V = V_1 \oplus V_2$. De plus, comme $\Lambda(\mathcal{L})$ et Λ sont orthogonaux, toute décomposition symplectique de Λ induit une décomposition symplectique de $\Lambda(\mathcal{L})$ et réciproquement. (En effet, si $x \in \Lambda(\mathcal{L})$ s'écrit $x = x_1 + x_2$ par rapport à la décomposition $V = V_1 \oplus V_2$, on a pour tout $\lambda_1 \in \Lambda_1, \lambda_2 \in \Lambda_2$, $E(x_1, \lambda_1 + \lambda_2) = E(x_1, \lambda_2) = E(x, \lambda_2) \in \mathbb{Z}$, donc x_1 appartient à $V_1 \cap \Lambda(\mathcal{L})$.) En particulier, on en déduit une décomposition symplectique $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$; réciproquement toute décomposition de $K(\mathcal{L})$ est induite par une (et même plusieurs) décomposition symplectique de Λ.

Par la suite, on parle souvent de décomposition au lieu de décomposition symplectique.

Comme $\mathcal{L}$ est ample, $\phi_{\mathcal{L}}$ est une isogénie et tout fibré $\mathcal{L}'$ algébriquement équivalent (c'est-à-dire de même classe de Chern) est un translaté de $\mathcal{L}$. Si $\mathcal{L} = L(H, \chi)$, son inverse $[-1]^*\mathcal{L} = L(H, \chi^{-1})$ lui est équivalent, et il existe $c \in X$ tel que $[-1]^*\mathcal{L} \simeq t_c^*\mathcal{L}$. Si x est tel que $c = 2x$, $t_x^*\mathcal{L}$ est symétrique. On voit donc que la classe de $\mathcal{L}$ contient un fibré symétrique. Réciproquement, à une décomposition symplectique $\Lambda = \Lambda_1 \oplus \Lambda_2$, on associe le semi-caractère $\chi_0(\lambda_1 + \lambda_2) = e^{\pi i E(\lambda_1, \lambda_2)}$ où $\lambda = \lambda_1 + \lambda_2$ est la décomposition de $\lambda \in \Lambda$; ce caractère définit un fibré symétrique canonique $\mathcal{L}_0 = L(H, \chi)$. Ainsi l'action $c \in V \mapsto t_c^*\mathcal{L}_0$ montre que la classe de $\mathcal{L}$ est un espace homogène principal sous $X/K(\mathcal{L})$, et les fibrés symétriques dans cette classe sont donnés par l'action de $[2]^{-1}K(\mathcal{L})/K(\mathcal{L}) = \frac{1}{2}\Lambda(\mathcal{L})/\Lambda(\mathcal{L})$. Si c est un élément de V, le semi-caractère du fibré translaté $\mathcal{L} = t_c^*\mathcal{L}_0$ est donné via le lemme 2.3.4 par $\chi = \chi_0 e^{2\pi i E(c,\cdot)}$. On appelle c la caractéristique de $\mathcal{L}$ par rapport à la décomposition de Λ, elle est déterminée à translation près par un élément de $\Lambda(\mathcal{L})$.

L'importance de $K(\mathcal{L})$ peut se voir dans l'énoncé de descente suivant :

PROPOSITION 2.4.7. *Soit $f : X \to X'$ une isogénie de variétés abéliennes, et $\mathcal{L} = L(H, \chi)$ un fibré en droites sur X. Alors il existe un fibré $\mathcal{L}' \in \mathrm{Pic}(X')$ tel que $\mathcal{L} = f^*\mathcal{L}'$ si et seulement si le noyau de f est un sous-groupe isotrope pour $E = \mathrm{Im}\, H$. En particulier dans ce cas* $\ker f$ *est un sous-groupe de $K(\mathcal{L})$.*

DÉMONSTRATION : Si $E = \mathrm{Im}\, H$ est la forme symplectique associée à H, par définition $\ker f$ est isotrope pour E si et seulement si $E(F^{-1}\Lambda', F^{-1}\Lambda') \subset \mathbb{Z}$, où Λ' est le réseau associé à X' et F la représentation analytique de f. Dans ce cas, $F^{-1*}H \in \mathrm{NS}(X')$, il existe donc un fibré $\mathcal{M} \in \mathrm{Pic}(X')$ de classe de Chern $F^{-1*}H$. Le fibré $\mathcal{L} \otimes f^*\mathcal{M}^{-1}$ est dans $\mathrm{Pic}_0(X)$; comme l'application duale $\widehat{X} \to \widehat{X'}$ donne une surjection $\mathrm{Pic}_0(X') \twoheadrightarrow \mathrm{Pic}_0(X)$, on peut corriger $\mathcal{M}$ par un élément de $\mathrm{Pic}_0(X')$ de sorte que $\mathcal{L} \simeq f^*\mathcal{M}$. La réciproque vient immédiatement du lemme 2.4.2. ∎

Dans le cadre de la proposition 2.4.7, si $f : X \to X'$ est une isogénie, $\mathcal{M}$ un fibré en droites sur X' et $\mathcal{L} = f^*\mathcal{M}$, le lien entre la polarisation donnée par $\mathcal{L}$ et celle donnée par $\mathcal{M}$ est donné par le diagramme commutatif suivant :

$$\begin{array}{ccc} X & \xrightarrow{\Phi(\mathcal{L})} & \widehat{X} \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle \hat{f}} \\ X' & \xrightarrow{\Phi(\mathcal{M})} & \widehat{X'}. \end{array}$$

En particulier, $\#K(\mathcal{L}) = (\deg f)^2 \#K(\mathcal{M})$, et l'application $c \in \Lambda(\mathcal{L}) \mapsto t^*_{f(c)}\mathcal{M}$ induit une bijection de $\Lambda(\mathcal{L})/\rho_a(f)^{-1}\Lambda(\mathcal{M})$ sur l'ensemble $\{\mathcal{M} \in \mathrm{Pic}(X') \mid f^*\mathcal{M} \simeq \mathcal{L}\}$. D'après le lemme 2.4.2 et la définition de $\Lambda(\mathcal{L})$ comme l'orthogonal de Λ, on voit que $\Lambda(\mathcal{L})/\rho_a(f)^{-1}\Lambda(\mathcal{M})$ est isomorphe à $K(\mathcal{L})/\operatorname{Ker} f^\perp$.

On peut rendre la proposition 2.4.7 explicite de la manière suivante. Pour simplifier les notations, on suppose que $\rho_a(f)$ est l'identité (on peut toujours se ramener à ce cas, car c'est un isomorphisme puisque f est une isogénie). On a alors une inclusion de réseaux $\Lambda \subset \Lambda' \subset \Lambda(\mathcal{M}) \subset \Lambda(\mathcal{L})$ où Λ est le réseau associé à X et Λ' celui de X' et $\operatorname{Ker} f = \Lambda'/\Lambda$. On suppose donnée une décomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$ qui induit des décompositions de Λ', $\Lambda(\mathcal{M})$ et $\Lambda(\mathcal{L})$. Soit $c \in V$ une caractéristique de $\mathcal{L}$ par rapport à la décomposition de Λ. Par définition d'une caractéristique, le facteur d'automorphie $a_{\mathcal{L}}$ de $\mathcal{L}$ est alors

$$a_c(\lambda, z) \coloneqq e^{\pi i E(\lambda_1,\lambda_2)+2\pi i E(c,\lambda)} e^{\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}.$$

On peut utiliser la même formule pour étendre a_c à $V \times V$. Si Γ est un réseau tel que E soit isotrope sur Γ, a_c restreint à $\Gamma \times V$ est un facteur d'automorphie, et donc définit un fibré sur V/Γ. On a donc une description explicite de la proposition 2.4.7. Par exemple $\Lambda_1(\mathcal{L}) \oplus \Lambda_2$ et $\Lambda_2(\mathcal{L}) \oplus \Lambda_1$ sont des réseaux isotropes maximaux, ce sont donc des réseaux maximaux sur lesquels a_c se restreint en un facteur d'automorphie et $X/K_1(\mathcal{L})$, $X/K_2(\mathcal{L})$ sont des quotients maximaux sur lesquels $\mathcal{L}$ descend. Soit $c' \in V$ une caractéristique de $\mathcal{M}$ par rapport à la décomposition de Λ'. Le lemme 2.4.2 montre que le facteur d'automorphie $a_{c'}$ associé à $\mathcal{M}$ se restreint à $\Lambda \times V$ en le facteur d'automorphie $a_{\mathcal{L}}$. La caractéristique c' est donc également une caractéristique de $\mathcal{L}$, on peut donc prendre $c = c'$ pour caractéristique de $\mathcal{L}$. Si on remplace c par $c + c''$, la restriction de la fonction $a_{c+c''}$ à $\Lambda \times V$ (resp. $\Lambda' \times V$) est identique à celle de a_c si et seulement si $c'' \in \Lambda(\mathcal{L})$ (resp. $\Lambda(\mathcal{M})$). On retrouve l'interprétation de $\Lambda(\mathcal{L})/\Lambda(\mathcal{M})$ précédente.

Corollaire 2.4.8. *Soit $\mathcal{M}$ un fibré en droites sur une variété abélienne X. Alors il existe un fibré en droites $\mathcal{L}$ sur X tel que $\mathcal{M} = \mathcal{L}^n$ si et seulement si $X[n] \subset K(\mathcal{M})$.*

Démonstration : Si $\mathcal{M} = \mathcal{L}^n$, $\Lambda(\mathcal{M}) = \frac{1}{n}\Lambda(\mathcal{L})$ et donc $X[n] \subset K(\mathcal{M})$. Pour la réciproque, si $X[n] \subset K(\mathcal{M})$, alors $X[n]$ est isotrope pour nH. Par la proposition 2.4.7, il existe un fibré $\mathcal{M}'$ tel que $\mathcal{M}^n = [n]^*\mathcal{M}'$. Comme $[n]^*\mathcal{M}'$ et $\mathcal{M}'^{n^2}$ sont analytiquement équivalents (ils ont la même classe de Chern par le corollaire 2.4.5), c'est également le cas de $\mathcal{M}$ et $\mathcal{M}'^n$. Ainsi $\mathcal{M}'^n \otimes \mathcal{M}^{-1} \in \mathrm{Pic}_0(X)$, et comme $\widehat{X}$ est divisible, il existe $N \in \mathrm{Pic}_0(X)$ tel que $\mathcal{M}'^n \otimes \mathcal{M}^{-1} \simeq N^n$. $\mathcal{L} = \mathcal{M}' \otimes N^{-1}$ satisfait $\mathcal{M} = \mathcal{L}^n$. ∎

Si $\mathcal{L}$ est un fibré en droites sur X, il détermine une application rationnelle $\Phi_{\mathcal{L}}$ dans $\mathbb{P}^{\deg \mathcal{L}-1}(\mathbb{C})$. Si $\mathcal{L}$ est une puissance 3-ième d'un fibré $\mathcal{L}'$, ce qui revient par le corollaire 2.4.8 à ce que $K(\mathcal{L})$ contienne la 3-torsion $X[3]$, le théorème de Lefschetz [Mum70, p. 30 ; BL04, p. 84] montre que $\Phi_{\mathcal{L}}$ est un plongement. De manière générale [BL04, p. 75], il existe une décomposition de $\mathcal{L}$ en $\mathcal{L} = \mathcal{M} \otimes \mathcal{N}_1 \otimes \ldots \mathcal{N}_r$ où $\mathcal{M}$ n'a pas de composantes fixes, et $\mathcal{N}_i$ est une polarisation principale irréductible (avec $\mathcal{N}_i \neq \mathcal{N}_j$ lorsque $i \neq j$). De plus, $\mathcal{M}$ est trivial sur $K(\mathcal{M})_0$, la composante connexe de $K(\mathcal{M})$ ($\mathcal{M}$ n'est pas nécessairement défini positif, donc $K(\mathcal{M})$ n'est pas nécessairement fini, sa composante connexe est un sous tore de X) et les $\mathcal{N}_i$ sont triviaux sur $K(\mathcal{N}_i)_0$. Le fibré $\mathcal{M}$ (resp. les $\mathcal{N}_i$) descend alors en un fibré $\overline{\mathcal{M}}$ sur $X_{\mathcal{M}} \coloneqq X/K(\mathcal{M})_0)$ (resp. $\overline{\mathcal{N}}_i$ sur $X_{\mathcal{N}_i} \coloneqq X/K(\mathcal{N}_i)_0$). La variété polarisée $(X, \mathcal{L})$ est isomorphe aux produits de variétés polarisées $(X_{\mathcal{M}}, \overline{\mathcal{M}}) \times (X_{\mathcal{N}_1}, \overline{\mathcal{N}_i}) \times \cdots \times (X_{\mathcal{N}_i}, \overline{\mathcal{N}_i})$. Enfin $\overline{\mathcal{M}}^2$ induit un plongement de $X_{\mathcal{M}}$ dans l'espace projectif, tandis que $\overline{\mathcal{N}}_i^2$ induit un plongement de la variété de Kummer $X_{\mathcal{N}_i}/\pm 1$ [BL04, Théorèmes 4.3.1, 4.5.5 et 4.8.1].

2.5 ESPACES MODULAIRES

Soit $X = V/\Lambda$ un tore complexe. Si l'on décompose X en $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ où $\Omega \in \mathrm{Gl}_g(\mathbb{Z})$ (voir la section 2.2), on peut se demander à quelle condition sur Ω le tore X est une variété abélienne. On verra dans cette section qu'il y a bijection entre les variétés abéliennes et les matrices Ω dans le demi-espace $\mathfrak{H}_g$ de Siegel. De plus, une telle matrice Ω détermine entièrement un fibré principal sur X. Ainsi, l'espace modulaire des tores complexes est de dimension g^2, tandis que celui des variété abéliennes complexes de dimension $g(g+1)/2$.

Soit $\mathcal{L} = L(H, \chi)$ un fibré ample sur X, et $E = \operatorname{Im} H$ la forme symplectique associée. La forme symplectique E est entière sur Λ ; il existe donc une base de Λ telle que E soit donnée par la matrice

$$M_\delta = \begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

où D_δ est la matrice diagonale de coordonnées $\delta = (\delta_1, \delta_2, \dots, \delta_g)$, avec $\delta_1 \mid \delta_2 \mid \dots \mid \delta_g$ et $\delta_i > 0$ pour $i \in [1..g]$. On appelle δ le type de la forme symplectique E (ou par abus de langage du fibré $\mathcal{L}$ ou de sa classe H). Notons que δ est simplement le type du groupe fini $K(\mathcal{L}) \simeq \mathbb{Z}/\delta_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/\delta_g\mathbb{Z}$.

Il est intéressant de regarder les conditions imposées par une polarisation $\mathcal{L} = L(H, \chi)$ de type δ sur la matrice des périodes de X. Soit $\Lambda = \Lambda_1 \oplus \Lambda_2$ une décomposition symplectique pour $E = \operatorname{Im} H$. Il est facile de voir que Λ_1 et Λ_2 engendrent chacun V comme $\mathbb{C}$-espace vectoriel . Il existe donc une matrice de périodes qui respecte cette décomposition. Soit $\{f_1, \dots, f_g, f'_1, \dots f'_g\}$ une base symplectique de Λ pour E, alors $\{e_1 = f'_1, \dots, e_g = f'_g\}$[1] est une base de V, et la matrice de période de X pour ces deux bases s'écrit

$$\Pi = (\Omega', \mathrm{Id}).$$

Un calcul montre alors que la matrice correspondant à H est $D_\delta(\operatorname{Im}\Omega')^{-1}$. (Pour simplifier l'exposition, on note également $D = D_\delta$ quand δ est clair dans le contexte.)

Si on pose $\Omega' = \Omega D$, alors $(\operatorname{Im}\Omega)^{-1}$ est la matrice correspondant à H, ce qui impose que Ω soit symétrique, et $\operatorname{Im}\Omega$ définie positive. Réciproquement, si $\Omega \in \mathfrak{H}_g$, le demi-espace de Siegel des matrices $\mathrm{M}_g(\mathbb{C})$ symétriques de partie imaginaire définie positive, on vérifie que la matrice hermitienne $\operatorname{Im}\Omega$ satisfait les conditions de la proposition 2.3.3 pour le réseau $\Lambda_\Omega \coloneqq \Omega D\mathbb{Z}^g \oplus \mathbb{Z}^g$ et est donc une polarisation pour la variété abélienne $X_\Omega = \mathbb{C}^g/\Lambda_\Omega$.

On a donc montré

PROPOSITION 2.5.1. *Le demi espace de Siegel $\mathfrak{H}_g$ est l'espace modulaire des variétés abéliennes X munies d'une polarisation de type δ et d'une base symplectique sur le réseau associé Λ_X.*

De plus, si $\Omega \in \mathfrak{H}_g$ et X est la variété qui lui correspond, il existe un fibré canonique $\mathcal{L}_0$ sur X qui correspond à la polarisation induite par Ω ; c'est le fibré symétrique de type δ et de caractéristique 0 induit par la décomposition $\Lambda_X = \Omega D\mathbb{Z}^g \oplus \mathbb{Z}^g$.

En terme de structure complexe, la situation est la suivante. Soit A la forme symplectique canonique de type δ sur $\mathbb{Z}^{2g}$, c'est-à-dire que la matrice de A dans la base canonique est $\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$. On a vu qu'il y avait bijection entre le demi-espace de Siegel et les morphismes symplectiques $(\mathbb{Z}^{2g}, A) \to (V, E)$ où $E = \operatorname{Im} H$ est la forme symplectique associée à une forme hermitienne H sur V. Si on étend A en une forme symplectique sur $\mathbb{R}^{2g}$, on voit donc que $\mathfrak{H}_g$ est en bijection avec les structures complexes J telles qu'il existe une forme hermitienne H pour J

1. On appelle une telle base normalisée, car elle normalise la matrice des périodes.

avec $A = \operatorname{Im} H$. Par le lemme 2.3.4, cela revient à demander que J satisfasse $A(Jx, Jy) = A(x, y)$ pour tout $x, y \in \mathbb{R}^{2g}$ et $A(Jx, x) > 0$ pour tout x non nul.

Soit $\mathrm{Sp}_{2g}^D(\mathbb{Z}) = \{M \in M_{2g}(\mathbb{Z}) \mid M\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} {}^tM = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}\}$ le groupe symplectique de type D. Si $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{Sp}_{2g}^D(\mathbb{Z})$, elle induit une nouvelle base symplectique du réseau Λ, et donc une nouvelle base normalisée de V. La matrice de période par rapport à cette nouvelle base s'écrit $\Omega_1'\mathbb{Z}^g + \mathbb{Z}^g$ avec $\Omega_1' = (\Omega' c + d)^{-1}(\Omega' a + b)$. Si $\Omega_1' = \Omega_1 D$, on a donc $\Omega_1 = (\Omega D c + d)^{-1}(\Omega D a + b)D^{-1}$. Les deux tores X_Ω et X_{Ω_1} sont isomorphes en tant que variétés abéliennes polarisées, la représentation rationnelle de cet isomorphisme étant donné par $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$ et la représentation analytique par $(c\Omega D + d)^{-1}$.

On peut montrer que (X_Ω, H_Ω) et $(X_{\Omega'}, H_{\Omega'})$ sont isomorphes en tant que variétés abéliennes polarisées si et seulement si Ω et Ω' sont dans la même orbite par $\mathrm{Sp}_{2g}^D(\mathbb{Z})$ [BL04, Proposition 8.1.3]. Ainsi l'espace modulaire des variétés abéliennes munies d'une polarisation de type δ est isomorphe à $\mathcal{A}_D \coloneqq \mathfrak{H}_g/\Gamma_D$ où on note $\Gamma_D = \mathrm{Sp}_{2g}^D(\mathbb{Z})$.

On peut également normaliser les choses différemment, en prenant pour base de V la base $\{e_1 = f_1'/\delta_1, \dots, e_g = f_g'/\delta_g\}$. La matrice de période de X s'écrit alors

$$\Pi = (\Omega_0, D)$$

avec $\Omega_0 = D\Omega D$, on voit donc que $(\operatorname{Im}\Omega_0)^{-1}$ est la matrice de H pour la nouvelle base. L'action de $\mathrm{Sp}_{2g}^D(\mathbb{Z})$ s'écrit alors

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}.\Omega_0 = (\Omega_0 c D^{-1} + D d D^{-1})^{-1}(\Omega_0 a + D b).$$

On peut rendre cette action plus agréable en considérant l'application $\mathbb{Z}^{2g} \to \mathbb{Z}^{2g}$ donnée par la matrice $\begin{pmatrix} \mathrm{Id} & 0 \\ 0 & D \end{pmatrix}$; elle induit un isomorphisme symplectique entre $(\mathbb{Z}^{2g}, A)$ et $(\mathbb{Z}^g \oplus D\mathbb{Z}^g, A_0)$ où A_0 est la forme symplectique associée à $\begin{pmatrix} 0 & \mathrm{Id} \\ -\mathrm{Id} & 0 \end{pmatrix}$.

On a donc un isomorphisme

$$\sigma_D : \mathrm{Sp}_{2g}^D(\mathbb{Q}) \to \mathrm{Sp}_{2g}(\mathbb{Q}), M \mapsto \begin{pmatrix} \mathrm{Id} & 0 \\ 0 & D \end{pmatrix}^{-1} M \begin{pmatrix} \mathrm{Id} & 0 \\ 0 & D \end{pmatrix}$$

qui induit un isomorphisme de $\mathrm{Sp}_{2g}^D(\mathbb{Z})$ sur $\Gamma_D^0 = \{M \in \mathrm{Sp}_{2g}(\mathbb{Q}) \mid {}^tM\Lambda_D \subset \Lambda_D\}$ où $\Lambda_D = \begin{pmatrix} \mathbb{Z}^g \\ D\mathbb{Z}^g \end{pmatrix}$.

L'action de Γ_D^0 sur $\mathfrak{H}_g$ induite par celle de Γ_D est alors donnée par[1]

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \Gamma_D^0.\Omega_0 = (\Omega_0 c + d)^{-1}(\Omega_0 a + b)$$

1. Comme la matrice $\Omega' = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.\Omega \in \mathfrak{H}_g$ est symétrique, l'action peut s'écrire

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}.\Omega_0 = ({}^t a\Omega_0 + {}^t b)({}^t c\Omega_0 + {}^t d)^{-1},$$

L'espace modulaire $\mathcal{A}_D$ précédent est donc également isomorphe à $\mathfrak{H}_g/\Gamma_D^0$.

On peut en fait voir $\mathfrak{H}_g$ comme un espace modulaire universel. En effet, si $\Omega \in \mathfrak{H}_g$, on note $j_\Omega : \mathbb{R}^{2g} \to \mathbb{C}^g, x \mapsto \left[\begin{smallmatrix}\Omega \\ 1\end{smallmatrix}\right] x$. Alors $j_\Omega \Lambda_D = \Omega\mathbb{Z}^g \oplus D\mathbb{Z}^g$ est le réseau associé à Ω (avec la normalisation précédente). On peut considérer la variété algébrique

$$\mathfrak{X}_D \coloneqq (\mathbb{C}^g \times \mathfrak{H}_g)/\Lambda_D$$

munie de la projection $\mathfrak{X}_D \to \mathfrak{H}_g$, et du fibré $\mathcal{L}_{\mathfrak{X}_D}$ donné par le facteur d'automorphie classique $ac_{(m,n),(z,\Omega)} = e^{-\pi i\, {}^t m\Omega m - 2\pi i\, {}^t zm}$ (voir l'équation (2.5)). Alors si $\Omega \in \mathfrak{H}_g$, la fibre de $(\mathfrak{X}_D, \mathcal{L})$ correspond exactement à $(X_\Omega = \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g), \mathcal{L}_0)$ [BL04, Lemme 8.7.1].

La base symplectique $\{f_1, \dots, f_g, f_1', \dots, f_g'\}$ de Λ donne une base symplectique

$$\{f_1/\delta_1, \dots, f_g/\delta_g, f_1'/\delta_1, \dots, f_g'/\delta_g\}$$

de $\Lambda(\mathcal{L})$ dont la projection sur X donne une base symplectique de $K(\mathcal{L})$. Inversement, comme tout automorphisme symplectique de $K(\mathcal{L})$ provient d'un élément de $\mathrm{Sp}_{2g}^D(\mathbb{Z})$ on voit que toute base symplectique de $K(\mathcal{L})$ est de cette forme. L'espace modulaire $\mathcal{A}_D(D)$ des variétés $(X, \mathcal{L})$ polarisées de type δ et munies d'une base symplectique de $K(\mathcal{L})$ est donné par le sous-groupe de congruence [BL04, Théorème 8.3.1] :

$$\Gamma_D(D) \coloneqq \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \Gamma_D \mid a - \mathrm{Id} \equiv b \equiv c \equiv d - \mathrm{Id} \pmod{D} \right\}. \tag{2.2}$$

De plus, on a une action de $\mathrm{Sp}_{2g}^D(\mathbb{Z})$ sur $\mathfrak{X}_D$ qui donne, quand $3 \mid \delta$, par passage au quotient une famille de variétés abéliennes [BL04, Proposition 8.8.2] :

$$\mathfrak{X}_D/\Gamma_D(D) \to \mathcal{A}_D(D).$$

Enfin l'espace modulaire des variétés polarisées de type δ avec une décomposition symplectique de leur réseau est donné par le sous-groupe de congruence [BL04, Proposition 8.3.3] :

$$\Delta_D \coloneqq \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \Gamma_D \mid b = c = 0 \right\}. \tag{2.3}$$

2.6 FONCTIONS THÊTA

Le but de cette section est d'introduire les fonctions thêta, qui fourniront des coordonnées privilégiées pour le plongement projectif associé à un fibré très ample. On verra que ce sont ces coordonnées thêta « canoniques » qui nous permettront d'exprimer des isogénies. Si les fonctions thêta sont introduites explicitement comme des fonctions analytiques sur $\mathbb{C}^g$, la seconde partie de cette section est consacrée à donner une construction « algébrique » de ces fonctions thêta, ce qui permet dans le chapitre 3 d'adapter cette construction au cas d'une variété abélienne sur un corps quelconque.

Soit $(X, \mathcal{L})$ une variété abélienne polarisée de type δ. Soit $\Lambda = \Lambda_1 \oplus \Lambda_2$ une décomposition symplectique du réseau de X, et $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ la décomposition de $K(\mathcal{L})$ associée.

On peut montrer que si $i > 0$, $H^i(X, \mathcal{L}) = 0$ et $h^0(X, \mathcal{L}) = \det D = \#K_2(\mathcal{L})$. Ainsi il existe une base $(\vartheta_i)_{i \in K_2(\mathcal{L})}$ des fonctions thêta de $\mathcal{L}$. En fait, on peut exhiber une base explicite qui de plus diagonalise l'action par translation de $K_2(\mathcal{L})$.

on retrouve l'action classique décrite dans [Mum83, p. 171-176], en se souvenant que les Anglo-saxons font agir

Si $\mathcal{L} = L(H, \chi)$, on a vu dans la section 2.3 que les fonctions thêta sont les fonctions qui satisfont l'équation fonctionnelle :

$$\vartheta(z+\lambda) = a_{\mathcal{L}}(\lambda, z)\vartheta(z)$$

où $a_{\mathcal{L}}(\lambda, z) = \chi(\lambda)e^{\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}$ est le facteur d'automorphie canonique.

Si $\mathcal{L}' = t_c^*\mathcal{L}$, et ϑ est une fonction thêta pour $\mathcal{L}$, alors

$$\vartheta'(z) = e^{-\pi H(z,c)-\frac{\pi}{2}H(c,c)}\vartheta(z+c) \tag{2.4}$$

est une fonction thêta pour $\mathcal{L}'$. On peut donc se ramener à l'étude des fonctions thêta pour le fibré symétrique $\mathcal{L} = \mathcal{L}_0$ de caractéristique 0 induit par la décomposition symplectique de Λ.

La forme hermitienne H est symétrique sur V_2 (car $E = \operatorname{Im} H = 0$ sur V_2). On note B l'extension bilinéaire de $H \mid V_2$ à $V \times V$. On peut alors définir le facteur d'automorphie classique

$$ac_{\mathcal{L}}(\lambda, v) = a_{\mathcal{L}}(\lambda, v)e^{\frac{\pi}{2}(B(v,v)-B(v+\lambda,v+\lambda))} = \chi(\lambda)e^{\pi(H-B)(v,\lambda)+\frac{\pi}{2}(H-B)(\lambda,\lambda)}.$$

On dit qu'une fonction qui satisfait l'équation fonctionnelle associée au facteur d'automorphie classique est une fonction thêta classique pour $\mathcal{L}$. Ainsi, si f est une fonction thêta classique, alors $z \mapsto e^{\frac{\pi}{2}B(z,z)}f(z)$ est une fonction thêta canonique et réciproquement [BL04, Lemme 8.5.2]. Si $w = w_1 + w_2$ est la décomposition de $w \in V$ suivant $V = V_1 \oplus V_2$, on a pour $v \in V$ $(H-B)(v, w) = -2i\,{}^t v \cdot w_1$ [BL04, Lemme 8.5.1]. Soit $\Lambda = \Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ une décomposition du réseau Λ telle que $\Omega D^{-1} \in \mathfrak{H}_g$. Une fonction thêta classique f doit donc d'après la section 2.3 vérifier les conditions :

$$\begin{aligned} f(z+m) &= f(z) \\ f(z+\Omega m) &= e^{-\pi i\,{}^t m\cdot(D\Omega)\cdot m - 2\pi i\,{}^t z\cdot Dm}f(z). \end{aligned} \tag{2.5}$$

Le facteur d'automorphie des fonctions thêta canoniques est plus facile à manipuler, ce qui explique pourquoi on a considéré ce facteur dans les sections 2.3 et 2.4. L'avantage du facteur classique vient du fait qu'une fonction thêta classique est $\mathbb{Z}$-périodique. On peut donc manipuler ces fonctions plus facilement en considérant leur développement de Fourrier [Mum83, p. 121-122]. Par la suite, pour illustrer un exemple algébrique par le cas complexe, on emploie principalement les fonctions thêta classiques. Cependant il nous arrivera de temps en temps de repasser par les fonctions thêta canoniques (voir par exemple la section 5.3).

Soit $\Omega \in \mathfrak{H}_g$ une matrice dans le demi-espace de Siegel. Si $a, b \in \mathbb{Q}^g$, on définit la fonction thêta avec caractéristiques [Mum83, p. 123]

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) = \sum_{n\in\mathbb{Z}^g} e^{\pi i\,{}^t(n+a)\Omega(n+a)+2\pi i\,{}^t(n+a)(z+b)}. \tag{2.6}$$

Les fonctions $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ sont holomorphes sur $\mathbb{C}^g$, et si $n, m \in \mathbb{Z}^g$ on a l'équation

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\Omega m+n, \Omega) = e^{-2\pi i\,{}^t b\cdot m+2\pi i\,{}^t a\cdot n}e^{-\pi i\,{}^t m\Omega m-2\pi i\,{}^t mz}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z). \tag{2.7}$$

Les fonctions thêta avec caractéristiques sont reliées par

$$\begin{aligned} \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) &= e^{\pi i\,{}^t a\Omega a+2\pi i\,{}^t a\cdot(z+b)}\vartheta(z+\Omega a+b, \Omega) \\ \vartheta\left[\begin{smallmatrix} a+n \\ b+m \end{smallmatrix}\right](z, \Omega) &= e^{2\pi i\,{}^t a\cdot m}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) \end{aligned} \tag{2.8}$$

où $m, n \in \mathbb{Z}^g$ et ϑ est la fonction $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$.

On peut utiliser le développement en série de Fourier des fonctions thêta avec caractéristiques (2.6) pour identifier une base des fonctions thêta classiques :

les matrices à droite.

PROPOSITION 2.6.1. *Soit $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g)$ un tore complexe, tel que $\Omega D^{-1} \in \mathfrak{H}_g$. Les fonctions $(\vartheta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](\cdot, \Omega D^{-1}))_{b\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$ forment une base des fonctions thêta classiques. On les appelle fonctions thêta de niveau D.*

DÉMONSTRATION : Voir [Mum83, p. 124]. ∎

Une autre base est donnée par les fonctions $(\vartheta \left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](D\cdot, D\Omega))_{a\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$. Si $\Omega_0 = \Omega D^{-1}$ et que l'on identifie $X = \mathbb{C}^g/(\Omega_0 D\mathbb{Z}^g + \mathbb{Z}^g)$ au tore $X' = \mathbb{C}^g/(\Omega'\mathbb{Z}^g + D\mathbb{Z}^g)$, via $z \mapsto D.z$, alors $\Omega' = D\Omega_0 D$ et la base précédente s'écrit $(\vartheta \left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](\cdot, \Omega')_{a\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g})$, elle est donc plus adaptée à cette décomposition.

Si on suppose $\mathcal{L}$ principal (et symétrique), on peut écrire la matrice des périodes de X sous la forme $\Lambda = \Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ avec $\Omega \in \mathfrak{H}_g$. Si $n \in \mathbb{N}^*$, $[n]^*\mathcal{L} = \mathcal{L}^{n^2}$, et dans ce cas la base de fonctions thêta classiques pour $[n]^*\mathcal{L}$ la plus commode est donnée par $(\vartheta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](n\cdot, \Omega))_{a,b\in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$. (C'est cette base qui est principalement utilisée, avec $n = 2$ et $\mathcal{L}$ le fibré principal de caractéristique 0, pour plonger le tore complexe X dans l'espace projectif.)

EXEMPLE 2.6.2 (FONCTION THÊTA ET DIVISEUR). Soit Θ le diviseur sur $\mathbb{C}^g$ associé à la fonction thêta $\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \Omega D^{-1})$. L'équation (2.7) montre que Θ est invariant par le réseau $\Omega D^{-1}\mathbb{Z}^g \oplus \mathbb{Z}^g$. En particulier Θ descend en un diviseur (toujours noté Θ) sur X. Alors $\mathcal{L}_0$ (le fibré de niveau δ et de caractéristique 0) est le fibré associé au diviseur Θ. De plus, l'équation (2.8) montre que le diviseur associé à la fonction $\vartheta \left[\begin{smallmatrix} Da \\ b \end{smallmatrix}\right](z, \Omega D^{-1})$ est $\Theta + \Omega a + b$. Ainsi le fibré associé à ce diviseur est de caractéristique $\Omega a + b$.

Si $\mathcal{L}$ est de caractéristique $c = \Omega c_1 + c_2$, alors les fonctions thêta associées à $\mathcal{L}$ sont par l'équation (2.4) :

$$(\vartheta \left[\begin{smallmatrix} Dc_1 \\ c_2+b \end{smallmatrix}\right](\cdot, \Omega D^{-1}))_{b\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}.$$

On retrouve que si $\mathcal{L} = t_c^*\mathcal{L}_0$, $\mathcal{L}$ est associé au diviseur $\Theta + c$.

De plus, si $\Omega a + b \in \Lambda(\mathcal{L}_0)$, l'équation (2.7) montre que $\vartheta \left[\begin{smallmatrix} aD \\ b \end{smallmatrix}\right](z, \Omega D^{-1})/\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \Omega D^{-1})$ est une fonction rationnelle sur X. En effet, on a :

$$(\vartheta \left[\begin{smallmatrix} aD \\ b \end{smallmatrix}\right]/\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right])(z + \Omega m + n, \Omega D^{-1}) =$$
$$e^{-2\pi i\, {}^t b\cdot Dm + 2\pi i\, {}^t a\cdot Dn}(\vartheta \left[\begin{smallmatrix} aD \\ b \end{smallmatrix}\right]/\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right])(z, \Omega D^{-1}) = (\vartheta \left[\begin{smallmatrix} aD \\ b \end{smallmatrix}\right]/\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right])(z, \Omega D^{-1}).$$

Le diviseur $\Theta + \Omega a + b$ est donc équivalent au diviseur Θ, ce qui correspond bien au fait que les fibrés associés soient isomorphes. Enfin, on vérifie que Θ descend en un diviseur principal sur la variété abélienne $\mathbb{C}^g/(\Omega D^{-1}\mathbb{Z}^g + \mathbb{Z}^g)$, ce qui permet de redémontrer que $\mathcal{L}_0$ est le l'image réciproque d'un fibré principal sur une variété isogène à X. ◊

REMARQUE 2.6.3 (PLONGEMENTS PROJECTIFS DES TORES COMPLEXES). Soit $\Omega \in \mathfrak{H}_g$, $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$, et $\mathcal{L}$ le fibré principal de caractéristique 0 associé à Ω. Si $n \in \mathbb{N}$, une base des fonctions thêta classiques de niveau n (donc associées à $\mathcal{L}^n$) est donnée par

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

Si de plus $3 \mid n$, par le théorème de Lefschetz, ces fonctions donnent un plongement de X dans l'espace projectif. Plus généralement, les fonctions thêta avec caractéristiques permettent d'obtenir des plongement explicites de tores complexes isogènes à X. En effet, soit $a_\Omega : \mathbb{R}^g \times \mathbb{R}^g \to \mathbb{C}^g$ la fonction $(x, y) \mapsto \Omega x + y$. Soit $L \subset \mathbb{Z}^{2g}$ un réseau d'indice s, et $L^\perp$ l'orthogonal de L par rapport à la forme symplectique A canonique sur $\mathbb{R}^{2g}$: $A(x, y) = {}^t x_1 y_2 - {}^t y_1 x_2$. Si

$m \in \mathbb{N}^*$, l'application

$$\begin{array}{rccl} \phi_L \colon \mathbb{C}^g/a_\Omega(\frac{1}{m}\cdot L) & \longrightarrow & \mathbb{P}^{s-1}_{\mathbb{C}} & , \\ z & \longmapsto & \left(\vartheta\left[\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right](m\cdot z,\Omega)\right)_{a_i,b_i\in L^\perp/\mathbb{Z}^{2g}} & \diamond \end{array}$$

où $a_i, b_i \in L^\perp$ parcourent un système de représentants de $L^\perp/\mathbb{Z}^{2g}$, est une application rationnelle de $X' = \mathbb{C}^g/a_\Omega(\frac{1}{m}L)$ dans l'espace projectif. De plus, s'il existe $r \in \mathbb{N}$, tel que $L \subset rL^\perp$ et $r \geqslant 3$, alors ϕ_L est un plongement [Mum83, Théorème 1.3, p. 125–134].

On retrouve le plongement précédent en considérant $m = 1$, $L = n\mathbb{Z}^g + \mathbb{Z}^g$, on a $a_{\frac{\Omega}{n}}(L) = \Omega\mathbb{Z}^g + \mathbb{Z}^g$. On peut retrouver de même les autres bases discutées après la proposition 2.6.1, en considérant $m = n$, $L = \mathbb{Z}^g + n\mathbb{Z}^g$, on a bien $\frac{1}{n}a_{n\Omega}(L) = \Omega\mathbb{Z}^g + \mathbb{Z}^g$, et de même si $m = n$, $L = n\mathbb{Z}^g + n\mathbb{Z}^g$, on a $\frac{1}{n}a_\Omega(L) = \Omega\mathbb{Z}^g + \mathbb{Z}^g$, ce qui redonne la base des fonctions thêta de niveau n^2.

La série analytique explicite donnant les fonctions thêta avec caractéristiques ne permet pas de construire ces fonctions « algébriquement ». Soit $c = \Omega c_1 + c_2 \in \mathbb{C}^g$ une caractéristique de $\mathcal{L}$. On peut donner une autre interprétation de la construction de la base $(\vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2+b \end{smallmatrix}\right](\cdot,\Omega D^{-1}))_{b\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$ de la manière suivante : $K_1(\mathcal{L})$ est un sous-groupe isotrope maximal de $K(\mathcal{L})$, le fibré $\mathcal{L}$ descend donc en un fibré principal $\mathcal{L}'$ sur $X' = X/K_1(\mathcal{L})$ par la proposition 2.4.7. Quitte à changer $\mathcal{L}'$ par un fibré équivalent, on peut supposer que c est la caractéristique de $\mathcal{L}'$. Le fibré $\mathcal{L}'$ admet une unique section globale (à multiplication par un élément de $\mathbb{C}^*$ près), qui se relève en une section ϑ_0 sur X. Or la fonction $\vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2 \end{smallmatrix}\right](\cdot,\Omega D^{-1})$ est une section du fibré principal de caractéristique c sur $X' = \mathbb{C}^g/(\Omega D^{-1}\mathbb{Z}^g + \mathbb{Z}^g)$ au vu de l'équation (2.7). On peut donc normaliser ϑ_0 de telle sorte $\vartheta_0 = \vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2 \end{smallmatrix}\right](\cdot,\Omega D^{-1})$. Les autres fonctions $\vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2+b \end{smallmatrix}\right](\cdot,\Omega D^{-1})$ sont obtenues en relevant à $\mathbb{C}^g$ l'action de translation par $b \in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g$ par l'équation (2.8), et en l'appliquant à la fonction $\vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2 \end{smallmatrix}\right](\cdot,\Omega D^{-1})$ par l'équation (2.7). ((On peut aussi voir la fonction $\vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2+b \end{smallmatrix}\right](\cdot,\Omega D^{-1})$ comme une section du fibré équivalent à $\mathcal{L}'$ sur X' de caractéristique $c + b$. Seulement, cela ne définit cette fonction qu'à une constante près, l'intérêt de la construction précédente, c'est qu'elle fixe entièrement la base des fonctions thêta une fois que l'on a fixé la fonction ϑ_0.))

Pour rendre plus précise la notion du relevé de l'action par translation à $\mathbb{C}^g$, pour $\mathcal{L}$ un fibré en droites et $x \in K(\mathcal{L})$, on considère les automorphismes de $\mathcal{L}$ au-dessus de x c'est à dire les automorphismes $\phi : \mathcal{L} \to \mathcal{L}$ tels que le diagramme suivant commute

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{\phi} & \mathcal{L} \\ \downarrow & & \downarrow \\ X & \xrightarrow{t_x} & X. \end{array}$$

On note $\mathcal{G}(\mathcal{L})$ le groupe des automorphismes de $\mathcal{L}$ au-dessus d'un point de $K(\mathcal{L})$, la loi de groupe étant donnée par composition : $(x_1,\phi_1).(x_2,\phi_2) = (x_1+x_2,\phi_1\phi_2)$. Par définition de $K(\mathcal{L})$, la projection $\mathcal{G}(\mathcal{L}) \to K(\mathcal{L}) : (x,\phi) \mapsto x$ est surjective (car si $x \in K(\mathcal{L})$, $t_x^*\mathcal{L} \simeq \mathcal{L}$). Le noyau est l'ensemble des isomorphismes de $\mathcal{L}$, c'est donc $\mathbb{C}^*$, et il est facile de voir que la suite exacte correspondante est centrale :

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathcal{G}(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0.$$

Du point de vue des fonctions thêta, si $W = \Gamma(X, \mathcal{L})$, une base de W est donnée par les fonctions thêta classiques précédentes (si $\mathcal{L} = \mathcal{L}_0$). Si $\lambda \in \Lambda(\mathcal{L})$, on a une action par translation $f \in W \mapsto f(\lambda + \cdot)$. Cette action induit une action projective[1] de $K(\mathcal{L})$ dans W ; cette action n'est pas affine car on n'a pas de relèvement canonique d'un élément de $K(\mathcal{L})$ en un élément de $\Lambda(\mathcal{L})$. Pour avoir une action affine, comme $\mathrm{GL}(W)$ est une extension centrale de $\mathrm{PGL}(W)$ par $\mathbb{C}^*$, on regarde l'extension centrale de $K(\mathcal{L})$ donnée par $\mathcal{G}(\mathcal{L})$. En effet, si $s \in \Gamma(X, \mathcal{L})$ et $(\phi, x) \in \mathcal{G}(\mathcal{L})$, on a le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{\phi} & \mathcal{L} \\ {\scriptstyle s}\uparrow & & \uparrow{\scriptstyle \phi \circ s \circ t_{-x}} \\ X & \xrightarrow{t_x} & X. \end{array}$$

On a donc une action de $\mathcal{G}(\mathcal{L})$ dans $\Gamma(X, \mathcal{L})$ donnée par $(\phi, x).s = \phi s t_{-x}$. On peut décrire explicitement $\mathcal{G}(\mathcal{L})$ (et donc l'action correspondante) de la manière suivante : on a vu que $\mathcal{L}$ est isomorphe à $V \times \mathbb{C}/\Lambda$ où Λ agit via le facteur d'automorphie $a_{\mathcal{L}}(\lambda, z) = \chi(\lambda) e^{\pi H(z,\lambda) + \frac{\pi}{2} H(\lambda,\lambda)}$, avec, si c est une caractéristique de $\mathcal{L}$ pour la décomposition symplectique associée à la matrice des périodes Ω, $\chi(\lambda) = e^{\pi i E(\lambda_1,\lambda_2) + 2\pi i E(c,\lambda)}$ (comme on va manipuler le facteur d'automorphie, on repasse au facteur d'automorphie canonique).

Si $\alpha \in \mathbb{C}^*$ et $w \in V$, on note $[\alpha, w]$ la fonction

$$V \times \mathbb{C} \to V \times \mathbb{C}, [\alpha, w].(v, t) = (v + w, \alpha e^{\pi H(v,w) t})$$

et $\widetilde{\mathfrak{G}}(\mathcal{L}) = \{[\alpha, w] \mid \alpha \in \mathbb{C}^*, w \in V\}$ le groupe donné par ces transformations. La multiplication est donnée par $[\alpha_1, w_1].[\alpha_2, w_2] = [\alpha_1 \alpha_2 e^{\pi H(w_2, w_1)}, w_1 + w_2]$. En fait, $\widetilde{\mathfrak{G}}(\mathcal{L})$ est simplement le groupe des automorphismes du fibré trivial $V \times \mathbb{C}$ au-dessus d'un point de V :

$$\begin{array}{ccc} V \times \mathbb{C} & \xrightarrow{[\alpha, w]} & V \times \mathbb{C} \\ \downarrow & & \downarrow \\ V & \xrightarrow{t_w} & V \end{array}$$

Un élément $[\alpha, w] \in \widetilde{\mathfrak{G}}(\mathcal{L})$ induit un élément de $\mathcal{G}(\mathcal{L})$ si et seulement s'il commute avec l'action de Λ sur $V \times \mathbb{C}$. Or si $\lambda \in \Lambda$, cette action est donnée par $[a_{\mathcal{L}}(\lambda, 0), \lambda]$. On a donc une section $s_\Lambda : \Lambda \to \widetilde{\mathfrak{G}}(\mathcal{L})$ donnée par $\lambda \mapsto [a_{\mathcal{L}}(\lambda, 0), \lambda] = [\chi(\lambda) e^{\frac{\pi}{2} H(\lambda,\lambda)}, \lambda]$, et tout élément du centralisateur de s_Λ dans $\widetilde{\mathfrak{G}}(\mathcal{L})$ induit donc un élément de $\mathcal{G}(\mathcal{L})$. Or par définition de $\Lambda(\mathcal{L}) = \Lambda^\perp$, on voit que ce centralisateur est le groupe $\mathfrak{G}(\mathcal{L}) = \{[\alpha, w] \mid \alpha \in \mathbb{C}^*, w \in \Lambda(\mathcal{L})\}$.

En appliquant le lemme des cinq au diagramme commutatif suivant, on obtient alors que $\mathcal{G}(\mathcal{L}) \simeq \mathfrak{G}(\mathcal{L})/s_{\mathcal{L}}(\Lambda)$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{C}^* & \longrightarrow & \mathfrak{G}(\mathcal{L}) & \longrightarrow & \Lambda(\mathcal{L}) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{C}^* & \longrightarrow & \mathcal{G}(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0. \end{array} \tag{2.9}$$

1. On appelle une action projective un morphisme de $K(\mathcal{L})$ dans $\mathrm{PGL}(W)$.

Enfin, on sait que le facteur d'automorphie $a_{\mathcal{L}}$ s'étend en un facteur d'automorphie sur $\Lambda_1(\mathcal{L})$ et $\Lambda_2(\mathcal{L})$, d'où des sections $s_{K_1(\mathcal{L})} : K_1(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ et $s_{K_2(\mathcal{L})} : K_2(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$. ((L'extension de $a_{\mathcal{L}}$ a $K_1(\mathcal{L})$ et $K_2(\mathcal{L})$ nécessite de fixer la valeur d'une caractéristique $c \in \mathbb{C}^g$ correspondant à $\mathcal{L}$ modulo Λ plutôt que modulo $\Lambda(\mathcal{L})$. On reviendra extensivement dans la section 3.5 sur l'action sur les coordonnées thêta résultant d'un choix différent de caractéristique c.))Soit ϑ_i^c les fonctions thêta canoniques correspondant aux fonctions thêta classiques $\vartheta \begin{bmatrix} Dc_1 \\ D^{-1}i+c_2 \end{bmatrix} (\cdot, \Omega D^{-1})_{i \in K_2(\mathcal{L})}$. La section $s_{K_1(\mathcal{L})}$ détermine exactement le fibré principal sur $X/K_1(\mathcal{L})$ tel que ϑ_0^c soit le tiré en arrière de la section globale de ce fibré principal (à un facteur multiplicatif près). La section $s_{K_2(\mathcal{L})}$ donne un relevé affine des translations par des points de $K_2(\mathcal{L})$ qui permet de retrouver la base des fonctions thêta à partir de ϑ_0^c. On voit qu'on peut retrouver les fonctions thêta grâce à ce groupe $\mathcal{G}(\mathcal{L})$, et c'est l'approche que l'on utilisera pour définir des fonctions thêta pour une variété abélienne algébrique.

En utilisant cette méthode, on obtient la construction suivante des fonctions $(\vartheta_i)_{i \in K_2(\mathcal{L})}$ (modulo une renormalisation). Par définition de l'action de $\mathfrak{G}(\mathcal{L})$, si $[\alpha, w] \in \mathfrak{G}(\mathcal{L})$, alors $[\alpha, w].\vartheta_0^c$ est la fonction faisant commuter le diagramme suivant :

$$\begin{array}{ccc} V \times \mathbb{C} & \xrightarrow{[\alpha,w]} & V \times \mathbb{C} \\ {\scriptstyle (\mathrm{Id}_V, \vartheta_0^c)}\uparrow & & \uparrow{\scriptstyle (\mathrm{Id}_V, [\alpha,w].\vartheta_0^c)} \\ V & \xrightarrow{t_w} & V. \end{array}$$

On calcule immédiatement que

$$[\alpha, w].\vartheta_0^c(z) = \alpha e^{\pi H(z-w,w)} \vartheta_0^c(z-w).$$

On a donc si $b \in K_2(\mathcal{L})$, $s_{K_2(\mathcal{L})}(b) = [a_{\mathcal{L}}(b,0), b] = [e^{\frac{\pi}{2}H(b,b)}, b]$ puisque $\chi(b) = 1$, et donc

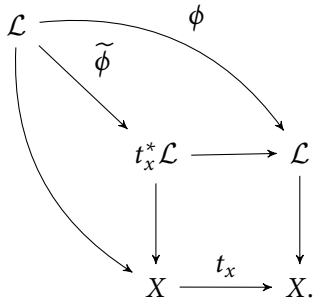
$$\vartheta_b := s_{K_2(\mathcal{L})}(-b).\vartheta_0^c(z) = e^{\frac{\pi}{2}H(b,b)-\pi H(z+b,b)} \vartheta_0^c(z+b) = a_{\mathcal{L}}(b,z)^{-1} \vartheta_0^c(z+b).$$

On vérifie de même [BL04, Proposition 6.4.2] que pour tout $j \in K_2(\mathcal{L})$, on a si $b_2 \in K_2(\mathcal{L})$ et $b_1 \in K_1(\mathcal{L})$:

$$s_{K_2(\mathcal{L})}(-b_2).\vartheta_j^c(z) = a_{\mathcal{L}}(b_2, z)\vartheta_j^c(z+b_2) = \vartheta_{j+b_2}(z)$$
$$s_{K_2(\mathcal{L})}(-b_1).\vartheta_j^c(z) = e^{-2\pi i E(j,b_1)} \vartheta_j(z+b_1).$$

En fait, ces relations déterminent entièrement la base des fonctions thêta canoniques, comme on le verra dans la section 3.4.

Dans la théorie algébrique, on préfère une autre vision de $\mathcal{G}(\mathcal{L})$: Si (x, ϕ) est un automorphisme de $\mathcal{L}$ au-dessus de x, par définition de t_x^* en tant que produit fibré, ϕ induit un unique isomorphisme $\widetilde{\phi} : \mathcal{L} \to t_x^*\mathcal{L}$ qui fait commuter le diagramme :



Le groupe $G(\mathcal{L})$ des isomorphismes $\widetilde{\phi} : \mathcal{L} \to t_x^*\mathcal{L}$ s'appelle le groupe thêta de $\mathcal{L}$. Le groupe thêta est isomorphe à $\mathcal{G}(\mathcal{L})$ via le morphisme $\phi \mapsto \widetilde{\phi}$, et sa structure de groupe induite par cette bijection est donnée par $(\widetilde{\phi}_1, x_1).(\widetilde{\phi}_2, x_2) = ((t_{x_2}^*\widetilde{\phi}_1))\widetilde{\phi}_2, x_1 + x_2)$. L'action induite sur les sections globales est alors donnée par $(\widetilde{\phi}, x).s = t_{-x}^*(\phi(s))$. C'est ce groupe que l'on va considérer dans le chapitre suivant.

3 FONCTIONS THÊTA ALGÉBRIQUES

MATIÈRES

3.1 INTRODUCTION

Ce chapitre est consacré à l'étude des fonctions thêta du point de vue algébrique, suivant la théorie de MUMFORD [Mum66]. Pour l'étude des variétés abéliennes sur un corps, outre le livre [Mum70] de MUMFORD précédemment cité, on peut consulter les notes de MILNE *Abelian varieties* [Mil91], et les résumés « Jacobian varieties » [Mil85] et « Abelian varieties » [Mil86]. Un traitement moderne du sujet est également en cours de rédaction dans GEER et MOONEN, « Abelian varieties » [GM07]. Nous ferons libre usage des résultats standards sur les variétés abéliennes ; en fait dans la mesure où nous nous restreignons à des polarisations et des isogénies séparables, les résultats du chapitre 2 restent vrais (même s'ils sont plus difficiles à démontrer en l'absence du revêtement universel $\mathbb{C}^g$ associé à une variété abélienne complexe de dimension g). Par exemple, une variété abélienne X de dimension g sur un corps algébriquement clos k de caractéristique p est divisible, et si $p \nmid n$ l'isogénie $[n]$ de multiplication par n est séparable, et son noyau $X[n]$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^{2g}$.

On cherche donc à généraliser la construction des fonctions thêta analytiques décrite dans la section 2.6. La section 3.2 introduit la notion de groupe thêta associé à une polarisation. On a vu dans la section 2.6 que c'était l'objet géométrique naturel pour construire les fonctions thêta. Dans le cas algébrique, on n'a plus le revêtement universel $\mathbb{C}^g$ ni la matrice $\Omega \in \mathfrak{H}_g$ pour décrire une variété abélienne. Cependant, même dans le cas complexe, on n'a pas besoin de toute l'information donnée par Ω pour construire les fonctions thêta (voir la discussion à la fin de la section 4.7). L'information nécessaire est encodée par ce qu'on appelle une thêta structure, que l'on peut voir comme un marquage du groupe thêta, et qui est introduite dans la section 3.3. Une thêta structure permet alors de définir des fonctions thêta canoniques, de manière équivalente à la construction donnée dans la seconde partie de la section 2.6. Ces fonctions thêta algébriques seront introduites dans la section 3.4. Une variété abélienne polarisée a de nombreuses thêta structures et il est important de savoir comment passer de l'une à l'autre, c'est l'objet de la section 3.5, qui peut être vue comme le pendant algébrique de la section 2.5.

Si l'on dépense autant d'énergie à construire une base canonique de fonctions thêta, c'est que l'on espère qu'une telle base permet d'exprimer des isogénies (comme on a commencé à le constater dans la section 2.4). On verra dans la section 3.6 que nos efforts sont couronnés de

succès : on peut exprimer des isogénies entre deux variétés abéliennes munies de coordonnées thêta grâce au théorème de l'isogénie. (Mais il faut encore travailler un peu pour l'appliquer en pratique, voir le chapitre 7).

Dans tout ce chapitre on se restreint au cas d'un corps k algébriquement clos, sauf à la section 3.7 où nous introduisons la notion de thêta structure rationnelle. La notion de thêta structure est géométrique et non arithmétique, au sens qu'il n'existe pas forcément de thêta structure rationnelle sur un fibré rationnel d'une variété abélienne rationnelle. Dans cette dernière section nous étudions également les contraintes imposées sur la variété par une thêta structure rationnelle. En particulier, on verra que quitte à prendre une extension finie, il existe toujours une telle thêta structure.

3.2 GROUPE THÊTA

k peut être de caractéristique nulle

Soit X une variété abélienne définie sur un corps algébriquement clos k de caractéristique p. On appelle point géométrique sur X un k-point sur X. Le sous-groupe $\mathrm{Pic}_0(X)$ de $\mathrm{Pic}(X)$ est l'ensemble des fibrés en droites $\mathcal{L}$ sur X tels que $t_x^*\mathcal{L} \simeq \mathcal{L}$ pour tout point géométrique $x \in X$. Comme dans le cas complexe (voir la section 2.4), on peut montrer [Mum70, p. 74] qu'il existe une variété abélienne $\widehat{X}$ sur k telle que $\widehat{X}(k) \simeq \mathrm{Pic}_0(X)$. On l'appelle la variété duale de X. Enfin on dit que deux fibrés en droites $\mathcal{L}$ et $\mathcal{M}$ sur X sont (algébriquement) équivalents si $\mathcal{L} \otimes \mathcal{M}^{-1} \in \mathrm{Pic}_0(X)$.

Soit $\mathcal{L}$ un fibré en droites ample sur X. Si $d = h^0(X, \mathcal{L})$, on dit que d est le degré de $\mathcal{L}$, et on a pour tout $n \in \mathbb{N}$: $h^0(X, \mathcal{L}^n) = dn^g$. Le fibré $\mathcal{L}$ induit une isogénie $\Phi_{\mathcal{L}} : X \to \widehat{X}$ de degré d^2 via l'application $x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ [Mum70, Théorème 1 p. 77]. On dit que $\mathcal{L}$ est un fibré séparable si l'isogénie $\Phi_{\mathcal{L}}$ est séparable. C'est le cas dès que p ne divise pas d, et on se restreint à ce cas par la suite. Le noyau $K(\mathcal{L})$ de $\Phi_{\mathcal{L}}$ est alors un sous-groupe de A_k de cardinal d^2.

DÉFINITION 3.2.1. Si $\mathcal{L}$ est un fibré ample séparable, le groupe thêta $G(\mathcal{L})$ est l'ensemble des couples (x, ϕ) où x est un point géométrique de[1] X et ϕ est un isomorphisme $\mathcal{L} \xrightarrow{\phi} t_x^*\mathcal{L}$. La loi de groupe est donnée, si (x, ϕ) et (y, ψ) sont dans $G(\mathcal{L})$, par la composition $(x, \phi).(y, \psi) = (x + y, t_x^*\psi \circ \phi)$:

$$\mathcal{L} \xrightarrow{\phi} t_x^*\mathcal{L} \xrightarrow{t_x^*\psi} t_x^*(t_y^*\mathcal{L}) = t_{x+y}^*\mathcal{L}$$

◇

Si $(x, \phi) \in G(\mathcal{L})$, on dit que ϕ un morphisme de $\mathcal{L}$ au-dessus de x. En particulier, x est complètement déterminé par ϕ. L'application d'oubli, $\rho_{G(\mathcal{L})} : G(\mathcal{L}) \to X, (x, \phi) \mapsto x$ donne par définition de $K(\mathcal{L})$ une surjection $G(\mathcal{L}) \twoheadrightarrow K(\mathcal{L})$, de noyau les automorphismes de $\mathcal{L}$. On a donc une suite exacte :

$$0 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \xrightarrow{\rho_{G(\mathcal{L})}} K(\mathcal{L}) \longrightarrow 0 .$$

Si $\mathcal{L}'$ est un fibré ample équivalent à $\mathcal{L}$, il existe $c \in X(k)$ tel que $\mathcal{L}' \simeq t_c^*\mathcal{L}$. Le groupe thêta $G(\mathcal{L}')$ de $\mathcal{L}'$ est alors isomorphe au groupe thêta de $\mathcal{L}$ via $t_c^* : (x, \phi) \in G(\mathcal{L}) \mapsto (x, t_c^*\phi) \in G(\mathcal{L}')$. Ainsi le groupe thêta, comme $K(\mathcal{L})$, ne dépend que de la classe d'équivalence de $\mathcal{L}$.

Le groupe thêta est la structure qui permet d'étudier les isogénies. En effet, soit $f : X \to Y$ une isogénie séparable entre variétés abéliennes, $\mathcal{M}$ un fibré ample sur Y et $\alpha : f^*\mathcal{M} \to \mathcal{L}$ un isomorphisme. Alors si $K = \mathrm{Ker}\, f$, K est un sous-groupe fini de l'ensemble des points

1. Comme k est algébriquement clos, les points géométriques de X sont exactement les points fermés.

géométriques sur X, et si $x \in K$, on a un isomorphisme $\mathcal{L} \to t_x^*\mathcal{L}$ donné par $t_x^*\alpha \circ \alpha^{-1}$:

$$\mathcal{L} \xleftarrow{\alpha} f^*\mathcal{M} = (f \circ t_x)^*\mathcal{M} \xrightarrow{t_x^*\alpha} t_x^*\mathcal{L}.$$

Ainsi Ker f est inclus dans $K(\mathcal{L})$, et le morphisme $x \mapsto (x, t_x^*\alpha \circ \alpha^{-1})$ définit une section de $G(\mathcal{L}) \to K(\mathcal{L})$ au-dessus de Ker f. Il est clair que cette section ne dépend pas du choix de α.

Réciproquement, si K est un sous-groupe fini de $K(\mathcal{L})$ on appelle sous-groupe de niveau au-dessus de K un sous-groupe $\widetilde{K} \subset G(\mathcal{L})$ tel que $\rho_{G(\mathcal{L})}$ induise un isomorphisme de $\widetilde{K}$ sur K.

THÉORÈME 3.2.2 (DESCENTE DE GROTHENDIECK). *Soit X une variété abélienne et $\mathcal{L}$ un fibré en droites ample séparable sur X. Soit K un sous-groupe fini de X, et $f : X \to X/K$ l'isogénie associée. Alors il y a bijection entre les fibrés $\mathcal{M}$ sur X/K tels que $f^*\mathcal{M} \simeq \mathcal{L}$ et les groupes de niveau $\widetilde{K}$ au-dessus de K.*

DÉMONSTRATION : Si $k = \mathbb{C}$, c'est le contenu de la proposition 2.4.7. Pour le cas général, voir [Mum66, Proposition 1]. ■

COROLLAIRE 3.2.3. *Soit $\mathcal{L}$ un fibré ample sur X, et n un nombre premier à la caractéristique p de k. Alors $K(\mathcal{L}^n) = [n]^{-1}K(\mathcal{L})$ et $K(\mathcal{L}) = nK(\mathcal{L}^n)$. Ainsi $X[n] \subset K(\mathcal{L}^n)$, réciproquement si $X[n]$ est inclus dans $K(\mathcal{L})$, alors $\mathcal{L}$ est une puissance n-ième d'un fibré $\mathcal{L}_0$.*

DÉMONSTRATION : La polarisation $\phi_{\mathcal{L}^n} : X \to \widehat{X}$ est la composée $\phi_{\mathcal{L}} \circ [n]$ (voir la section 5.2.1). Donc son noyau $K(\mathcal{L}^n)$ est $[n]^{-1}K(\mathcal{L})$, et comme X est divisible $K(\mathcal{L}) = nK(\mathcal{L}^n)$.

Enfin le dernier point découle du théorème 3.2.2 avec la même preuve que le corollaire 2.4.8.■

Dans le cadre de la situation du théorème 3.2.2, on a une description explicite du lien entre le groupe thêta de $\mathcal{L}$ et celui de $\mathcal{M}$. Déjà si $r = \deg f$, alors $r \mid d$ où d est le degré de $\mathcal{L}$, et le degré de $\mathcal{M}$ est d/r, en particulier $\mathcal{M}$ est un fibré séparable.

La situation $k = \mathbb{C}$ a déjà été traitée à la section 2.4, mais il est utile de la réinterpréter avec le vocabulaire algébrique :

EXEMPLE 3.2.4. Soit $X = V/\Lambda$ une variété algébrique complexe, et $\mathcal{L}$ un fibré en droite ample sur X. Soit $\Lambda = \Lambda_1 \oplus \Lambda_2$ une décomposition symplectique de Λ et $c \in V$ une caractéristique de $\mathcal{L}$ pour cette décomposition. Le facteur d'automorphie $a_{\mathcal{L}}$ associé à $\mathcal{L}$ sur $\Lambda \times V$ est alors la restriction de a_c à $\Lambda \times V$ où

$$a_c(\lambda, z) \coloneqq e^{\pi i E(\lambda_1,\lambda_2)+2\pi i E(c,\lambda)} e^{\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}.$$

On a vu dans la section 2.6 que $G(\mathcal{L})$ était isomorphe à $\mathcal{G}(\mathcal{L})$, de plus on une description explicite de $\mathcal{G}(\mathcal{L})$ comme $\mathfrak{G}(\mathcal{L})/s_c(\Lambda)$ où $s_c(\lambda) = [a_c(\lambda, 0), \lambda]$.

Soit $f : X \to X'$ une isogénie. Comme dans la section 2.4 on peut supposer que la représentation analytique de l'isogénie $X \to X'$ est l'identité sur V. On a alors $X' = V/\Lambda'$ où Λ' est un réseau de V qui contient Λ. De plus, on peut supposer qu'on a pris une décomposition symplectique de Λ qui induit une décomposition symplectique de Λ'. Soit $\mathcal{M}$ un fibré en droites sur X' tel que $f^*\mathcal{M} = \mathcal{L}$, et c' la caractéristique de $\mathcal{M}$. Quitte à changer c par un élément de $\Lambda(\mathcal{L})$ (ce qui ne change pas la restriction de a_c à $\Lambda \times V$), on peut supposer que $c = c'$. Le noyau de f est $K = \Lambda'/\Lambda$ et le groupe de niveau associé à Λ' dans $\mathfrak{G}(\mathcal{L})$ est alors simplement $s_c(\Lambda')$. (En effet, a_c est un facteur d'automorphie sur $\Lambda' \times V$, il définit bien une section $\Lambda' \to \mathfrak{G}(\mathcal{L})$ dont l'image est l'image réciproque dans $\mathfrak{G}(\mathcal{L})$ du groupe de niveau associé à $\mathcal{M}$ dans $\mathcal{G}(\mathcal{L})$.)

Or $\mathfrak{G}(\mathcal{L}) = \{[\alpha, w] \mid \alpha \in \mathbb{C}^*, w \in \Lambda(\mathcal{L})\}$; d'autre part on a $\mathcal{G}(\mathcal{M}) = \mathfrak{G}(\mathcal{M})/s_c(\Lambda')$ où $\mathfrak{G}(\mathcal{M}) = \{[\alpha, w] \mid \alpha \in \mathbb{C}^*, w \in \Lambda(\mathcal{M})\}$. On peut caractériser le sous-groupe $\mathfrak{G}(\mathcal{M})$ de $\mathfrak{G}(\mathcal{L})$ ainsi : on a vu dans la section 2.4 que $\Lambda(\mathcal{M})$ est l'orthogonal de Λ' pour la forme symplectique E associée à $\mathcal{L}$. Or si $[\alpha, w_1]$ et $[\beta, w_2]$ sont dans $\mathfrak{G}(\mathcal{L})$, on vérifie immédiatement que leur centralisateur est $[e^{-2\pi i E_{\mathcal{L}}(w_1,w_2)}, 0]$ où $E_{\mathcal{L}}$ est la forme symplectique associée à $\mathcal{L}$. Ainsi $\mathfrak{G}(\mathcal{M})$ est le centralisateur de $s_{\mathcal{L}}(\Lambda')$ dans $\mathfrak{G}(\mathcal{L})$. ◊

Dans le cas général, on a une description identique pour $G(\mathcal{M})$:

Proposition 3.2.5. *Avec les notations précédentes, soit $\widetilde{K}$ un sous-groupe de niveau au-dessus de K, et $\mathcal{M}$ le fibré sur X/K correspondant à $\widetilde{K}$. Soit $\mathcal{Z}(\widetilde{K})$ le centralisateur de $\widetilde{K}$ dans $G(\mathcal{L})$. Alors $G(\mathcal{M})$ est canoniquement isomorphe à $\mathcal{Z}(\widetilde{K})/\widetilde{K}$.*
De plus, $\rho_{G(\mathcal{L})}(\mathcal{Z}(\widetilde{K})) = f^{-1}(K(\mathcal{M}))$.

Démonstration : On vient de voir le cas complexe dans l'exemple 3.2.4. Le cas général découle de la théorie de la descente et est traité dans [Mum66, Proposition 2].

De manière un peu plus explicite, si α_f représente la surjection $\mathcal{Z}(\widetilde{K}) \twoheadrightarrow G(\mathcal{M})$ de noyau $\widetilde{K}$, et si $(y, \psi) \in G(\mathcal{M})$, on peut décrire les éléments de $\alpha_f^{-1}(y, \psi)$ ainsi : soit $x \in f^{-1}(y)$. Alors le morphisme de $\alpha_f^{-1}(y, \psi)$ au-dessus de x est donné par la composition :

$$\mathcal{L} \xrightarrow{\alpha} f^*\mathcal{M} \xrightarrow{f^*\phi} f^*t_y^*\mathcal{M} = t_x^*f^*\mathcal{M} \xrightarrow{(t_x^*\alpha)^{-1}} \mathcal{L}.$$

■

Tout sous-groupe de $K(\mathcal{L})$ n'admet pas forcément un groupe de niveau. Un sous-groupe de niveau est un sous-groupe commutatif de $G(\mathcal{L})$; on a vu dans l'exemple 3.2.4 l'intérêt de la forme $E_{\mathcal{L}}$ pour mesurer le défaut de commutativité d'éléments de $G(\mathcal{L})$. Plus exactement, on a vu que si $X = V/\Lambda$ est une variété abélienne complexe, alors $e^{-2\pi i E_{\mathcal{L}}(\widetilde{x},\widetilde{y})}$ (où $\widetilde{x}, \widetilde{y}$ sont n'importe quels relevés de $x, y \in K(\mathcal{L}) \subset X$ à V) est le commutateur de n'importe quel relevé de x, y à $G(\mathcal{L})$. Dans le même esprit, on peut définir un pairing sur $K(\mathcal{L})$ ainsi : si $x, y \in K(\mathcal{L})$, soit $\widetilde{x}, \widetilde{y}$ n'importe quel relevé de x et y dans $G(\mathcal{L})$. Alors l'élément $e_{\mathcal{L}}(x, y) = \widetilde{x}\widetilde{y}\widetilde{x}^{-1}\widetilde{y}^{-1}$ est un élément de k^* qui ne dépend pas des relevés $\widetilde{x}$ et $\widetilde{y}$. Il est immédiat que $e_{\mathcal{L}}$ est une forme bilinéaire alternée[1], que l'on appelle le ''commutator pairing'' sur $K(\mathcal{L})$.

On peut montrer que la forme $e_{\mathcal{L}}$ sur $K(\mathcal{L})$ est non dégénérée [Mum66, Theorem 1] (ou de manière équivalente que k^* est le centre de $G(\mathcal{L})$) , ainsi c'est une forme symplectique (multiplicative).

Proposition 3.2.6. *Soit K un sous-groupe de $K(\mathcal{L})$. Les conditions suivantes sont équivalentes :*

1. *K admet un groupe de niveau dans $G(\mathcal{L})$.*
2. *$\rho_{G(\mathcal{L})}^{-1}(K)$ est un groupe commutatif.*
3. *K est isotrope pour $e_{\mathcal{L}}$.*

Démonstration : L'équivalence entre les points 2 et 3 est immédiate vu la définition du pairing $e_{\mathcal{L}}$ comme mesurant le défaut de commutativité. Soit $\mathfrak{K} = \rho_{G(\mathcal{L})}^{-1}(K)$; si $\mathfrak{K} \to K$ admet une section, comme $\mathfrak{K}$ est une extension centrale de K par k^*, $\mathfrak{K}$ est commutatif.

Réciproquement, en décomposant K en somme de cycles, et comme $\mathfrak{K}$ est abélien, il suffit d'expliquer comment relever un élément x de K. Si x est d'ordre ℓ, soit $\widetilde{x}$ un relevé quelconque de x, $\widetilde{x}^\ell$ est dans k^*. Si α est une racine ℓ-ième de $\widetilde{x}^\ell$, $\widetilde{x}/\alpha$ est d'ordre ℓ et fournit le relevé cherché. ■

1. C'est-à-dire que $e_{\mathcal{L}}(x, x) = 1$ pour tout $x \in K(\mathcal{L})$.

On note GPAB_{k^*} la catégorie des extensions centrales de groupes abéliens finis par k^*. Un morphisme dans GPAB_{k^*} est un morphisme de groupes qui se restreint en l'identité sur k^*. Ainsi si $\mathfrak{A}, \mathfrak{B} \in \mathsf{GPAB}_{k^*}$ sont des extensions centrales des groupes abéliens A et B, le commutateur sur $\mathfrak{A}$ se restreint en une forme alternée sur A et un morphisme de $\mathfrak{A} \to \mathfrak{B}$ se restreint en un morphisme de $A \to B$ qui respecte les commutateurs. Dans la suite, si on ne le précise pas, les morphismes de groupes thêta sont considérés comme étant dans GPAB_{k^*}.

Un morphisme de variétés abéliennes polarisées $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ est un morphisme $f : X \to Y$ tel que $f^*\mathcal{M} \simeq \mathcal{L}$. Si de plus f est une isogénie, une telle situation est idéale pour étudier f. On verra en effet que si $\mathcal{M}$ est très ample, le théorème de l'isogénie permet de relier les coordonnées associées à $\mathcal{M}$ à celles associées à $\mathcal{L}$. On conclut cette partie par l'étude de cette situation dans le même esprit que la discussion après la proposition 2.4.7. Soit α un isomorphisme $\mathcal{L} \to f^*\mathcal{M}$, K le noyau de f et $\widetilde{K}$ le sous-groupe de niveau au-dessus de K qui correspond à $\mathcal{M}$. Si $\mathfrak{K} = \rho_{G(\mathcal{L})}^{-1}(K)$, $\mathfrak{K}$ est un groupe abélien par la proposition 2.4.7 comme K est isotrope. La donnée de $\widetilde{K}$ équivaut à la donnée d'un caractère χ sur $\mathfrak{K}$ qui se restreint en l'identité sur k^* (à un tel caractère on associe son noyau). Ainsi tout autre groupe de niveau au-dessus de K correspond à un caractère $\chi \circ (\rho_{G(\mathcal{L})}^* \xi)$ où ξ est un caractère sur K. Comme $e_{\mathcal{L}}$ est non dégénérée, il existe $c \in K(\mathcal{L})$, uniquement déterminé modulo $K^\perp$ tel que $\xi = e_{\mathcal{L}}(c, \cdot)$. On peut interpréter géométriquement le fibré correspondant à un tel c ainsi : soit c un point géométrique de X, l'isomorphisme $t_c^* : G(\mathcal{L}) \to G(t_c^*\mathcal{L})$ décrit à la page 42 transporte le groupe de niveau $\widetilde{K}$ de telle sorte que $t_c^*(\widetilde{K})$ correspond à l'isomorphisme $t_c^*\alpha : t_c^*\mathcal{L} \to t_c^* f^*\mathcal{M} = f^* t_{f(c)}^*\mathcal{M}$.

Maintenant, si $\mathcal{L}'$ est un fibré ample sur X isomorphe à $\mathcal{L}$, et $\phi : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ un isomorphisme, on a un isomorphisme entre $G(\mathcal{L})$ et $G(\mathcal{L}')$ donné par $(x, \psi) \mapsto (t_x^*\phi\psi\phi^{-1})$:

$$\mathcal{L}' \xrightarrow{\phi^{-1}} \mathcal{L} \xrightarrow{\psi} t_x^*\mathcal{L} \xrightarrow{t_x^*\phi} t_x^*\mathcal{L}'.$$

Cet isomorphisme ne dépend pas de ϕ. Si $c \in K(\mathcal{L})$, il existe un isomorphisme $\phi : \mathcal{L} \to t_c^*\mathcal{L}$; on peut donc appliquer ce qui précède pour obtenir un isomorphisme $G(t_c^*\mathcal{L}) \xrightarrow{\sim} G(\mathcal{L})$, qui en composant avec l'isomorphisme $t_c^* : G(\mathcal{L}) \xrightarrow{\sim} G(t_c^*\mathcal{L})$ précédent donne un automorphisme de $G(\mathcal{L})$, $(x, \psi) \mapsto (x, t_x^*\phi^{-1}\psi\phi)$:

$$\mathcal{L} \xrightarrow{\phi} t_c^*\mathcal{L} \xrightarrow{t_c^*\psi} t_{c+x}^*\mathcal{L} \xrightarrow{t_x^*\phi^{-1}} t_x^*\mathcal{L}.$$

Cet automorphisme $\mathtt{conj}_c$ de $G(\mathcal{L})$ est donc simplement l'action par conjugaison de n'importe quel relevé ϕ de c dans $G(\mathcal{L})$.

Par définition du commutator pairing, on voit que

$$\mathtt{conj}_c.(x, \psi) = (x, e_{\mathcal{L}}(c, x)\psi). \tag{3.1}$$

L'automorphisme $\mathtt{conj}_c$ laisse $K(\mathcal{L})$ invariant (et on verra dans la section 3.5 que tout tel automorphisme est de ce type). En particulier, $\mathtt{conj}_c(\widetilde{K})$ est le groupe de niveau au-dessus de K correspondant au caractère $\chi \circ (\rho_{G(\mathcal{L})}^* e_{\mathcal{L}}(c, \cdot))$, et par ce qui précède ce groupe de niveau correspond à

$$\mathcal{L} \xrightarrow{\phi} t_c^*\mathcal{L} \longrightarrow t_c^*\alpha^*\mathcal{M} = \alpha^* t_{f(c)}^*\mathcal{M}.$$

Si de plus $f(c) \in K(\mathcal{M})$, $t_{f(c)}^*\mathcal{M} \simeq \mathcal{M}$, mais on a vu que $f^{-1}(\mathcal{M}) = K^\perp$, et si $c \in K^\perp$ l'action $\mathtt{conj}_c$ laisse bien $\widetilde{K}$ invariant.

3.3 THÊTA STRUCTURE

Comme la forme $e_{\mathcal{L}}$ sur $K(\mathcal{L})$ est non dégénérée, il existe une décomposition symplectique $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ où $K_1(\mathcal{L})$ et $K_2(\mathcal{L})$ sont des sous-groupes isotropes maximaux de $K(\mathcal{L})$. En particulier, $K_2(\mathcal{L}) \simeq \mathrm{Hom}(K_1(\mathcal{L}), k^*)$ via le pairing $e_{\mathcal{L}}$. Si $k = \mathbb{C}$, on a vu dans la preuve précédente que $e_{\mathcal{L}}$ était l'exponentielle de la forme symplectique (additive) $E_{\mathcal{L}}$ associée à $\mathcal{L}$, et la décomposition de $K(\mathcal{L})$ pour $e_{\mathcal{L}}$ coïncide donc avec celle de la section 2.4 pour $E_{\mathcal{L}}$.

Par le théorème de décomposition des groupes abéliens finis, on peut écrire $K_1(\mathcal{L}) \simeq \oplus_{i=1}^N \mathbb{Z}/\delta_i\mathbb{Z}$, où $\delta_1 \mid \delta_2 \mid \ldots \mid \delta_N$ sont les diviseurs élémentaires de $K_1(\mathcal{L})$. Comme $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ et que $K_2(\mathcal{L})$ est le dual de $K_1(\mathcal{L})$, les diviseurs élémentaires de $K(\mathcal{L})$ sont donc $(\delta_1, \delta_1, \delta_2, \delta_2, \ldots, \delta_N, \delta_N)$. Or si $d = \vee_{i=1}^N \delta_i$ est le plus petit commun multiple des δ_i, $K(\mathcal{L})$ est un sous-groupe de $X[d]$. Comme ce dernier est de rang $2g$, on a donc $N \leqslant g$.

Il arrive qu'il soit plus simple de manipuler une décomposition cyclique de $Z(\delta)$ qui ne soit pas la décomposition canonique, ce qui explique pourquoi on n'impose pas que $\delta_i \mid \delta_{i+1}$ dans la définition de δ.

Si $\delta = (\delta_1, \ldots, \delta_g)$ (en complétant éventuellement par des 1 pour avoir un vecteur de rang g), on note $Z(\delta) = \oplus_{i=1}^g \mathbb{Z}/\delta_i\mathbb{Z}$. On dit que $\mathcal{L}$ est de type (ou de niveau) δ. Soit $K(\delta) = K_1(\delta) \oplus K_2(\delta)$ l'espace symplectique canonique de type δ. Si $\hat{Z}(\delta) = \mathrm{Hom}(Z(\delta), k^*)$ est le dual de $Z(\delta)$, et $\langle x, l\rangle := l(x)$ représente le pairing canonique entre $Z(\delta)$ et son dual, alors $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$, avec $K_1(\delta) = Z(\delta)$, $K_2(\delta) = \hat{Z}(\delta)$ et le pairing e_δ sur $K(\delta)$ est donné par $e_\delta((x_1, l_1), (x_2, l_2)) = \frac{\langle x_1, l_2\rangle}{\langle x_2, l_1\rangle}$.

Soit $d = \vee_{i=1}^g \delta_i$, et ζ une racine primitive d-ième de l'unité. Soit $Z(\overline{d}) = \mathbb{Z}^g/d\mathbb{Z}^g$, et $(\cdot\,|\,\cdot)$ le produit scalaire canonique sur $Z(\overline{d})$. Ce produit scalaire se restreint alors sur $Z(\delta) \subset Z(\overline{d})$ en l'application

$$(x\,|\,y) = \sum_{i=1}^g \frac{d}{\delta_i} x_i y_i$$

lorsque $x = (x_i)_{i\in[1..g]}$, $y = (y_i)_{i\in[1..g]} \in Z(\delta)$. On peut alors donner une autre description de $K(\delta)$ ainsi : $K(\delta) = Z(\delta) \oplus Z(\delta)$, et le pairing e_δ est donné par

$$e_\delta(x_1 \oplus x_2, y_1 \oplus y_2) = \zeta^{(x_1|y_2)-(y_1|x_2)}.$$

(Il nous arrivera de faire cette identification implicitement, en supposant la racine ζ fixée implicitement.) Enfin, si $x \in K_1(\mathcal{L})$, on appelle le dual de x l'unique élément $y \in K_2(\mathcal{L})$ tel que $e_{\mathcal{L}}(x, y) = \zeta$.

PROPOSITION 3.3.1. *Soit $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ une décomposition de $K(\mathcal{L})$ en sous-espaces isotropes maximaux. Il y a bijection entre les isomorphismes symplectiques $\phi : K(\delta) \to K(\mathcal{L})$ tels que $\phi(K_i(\delta)) \subset K_i(\mathcal{L})$ ($i = 1, 2$) et les isomorphismes $\sigma : Z(\delta) \to K_1(\mathcal{L})$.*

DÉMONSTRATION : En effet, si on fixe un isomorphisme σ de $K_1(\mathcal{L})$ avec $K_1(\delta)$, le pairing $e_{\mathcal{L}}$ permettant d'identifier $K_2(\mathcal{L})$ au dual de $K_1(\mathcal{L})$. On en déduit un isomorphisme $\hat{\sigma}$ de $K_2(\mathcal{L})$ sur $K_2(\delta)$ donné par le dual de σ. On a donc exhibé un isomorphisme symplectique de $(K(\delta), e_\delta)$ sur $(K(\mathcal{L}), e_{\mathcal{L}})$, compatible avec la décomposition de $K(\mathcal{L})$ et $K(\delta)$. Réciproquement à un tel isomorphisme on associe sa restriction σ à $K_1(\delta)$. ∎

Si δ' et δ sont dans $\mathbb{Z}^g$, on dit que $\delta' \mid \delta$ lorsque $\delta'_i \mid \delta_i$ pour chaque $i \in \{1, \ldots, g\}$. On a alors un plongement canonique de $Z(\delta')$ dans $Z(\delta)$ donné par

$$(x_1, \ldots, x_g) \mapsto (\frac{\delta_1}{\delta'_1} x_1, \ldots, \frac{\delta_g}{\delta'_g} x_g),$$

et dans la suite lorsqu'on écrit $Z(\delta') \subset Z(\delta)$ on fait toujours référence à ce plongement. De même, on considère toujours le plongement canonique $\hat{Z}(\delta') \subset \hat{Z}(\delta)$ donné par le dual

de l'épimorphisme canonique $Z(\delta) \twoheadrightarrow Z(\delta')$. Le sous-groupe $\hat{Z}(\delta') \subset \hat{Z}(\delta)$ est le dual symplectique du sous-groupe $Z(\delta') \subset Z(\delta)$. Enfin si $n \in \mathbb{Z}$, on dit que $n \mid \delta$ si $\overline{n} \mid \delta$ où $\overline{n}$ représente le vecteur $(n, \dots, n) \in \mathbb{Z}^g$.

On va chercher une description explicite de $G(\mathcal{L})$ qui étend la description de $(K(\mathcal{L}), e_{\mathcal{L}})$ donnée par $(K(\delta), e_\delta)$. Pour cela on va considérer le groupe de Heisenberg $\mathcal{H}(\delta)$, qui est une extension centrale de $K(\delta)$ par k^*. Du point de vue ensembliste, $\mathcal{H}(\delta) = k^* \times K(\delta)$. Si un élément h de $\mathcal{H}(\delta)$ s'écrit $(\alpha, x) \in k^* \times K(\delta)$, et que $x = (x_1, x_2)$ est la décomposition de x suivant la décomposition canonique $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$, on note aussi cet élément h comme (α, x_1, x_2). La loi de groupe est donnée sur $\mathcal{H}(\delta)$ par

$$(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha\beta\langle x_1, y_2\rangle, x_1 + y_1, x_2 + y_2). \tag{3.2}$$

L'inverse de (α, x_1, x_2) est alors donné par

$$(\alpha, x_1, x_2)^{-1} = (\frac{\langle x_1, x_2\rangle}{\alpha}, -x_1, -x_2) \tag{3.3}$$

et l'exponentiation par

$$(\alpha, x_1, x_2)^n = (\alpha\langle x_1, x_2\rangle^{\frac{n(n-1)}{2}}, nx_1, nx_2).$$

On vérifie aisément qu'on retrouve le pairing e_δ en prenant le commutateur de deux relevés quelconques d'éléments de $K(\delta)$ dans $H(\delta)$. Pour simplifier les notations, pour $G(\mathcal{L})$ et $H(\delta)$, on identifie k^* à son image, ainsi si $\alpha \in k^*$, son image dans $H(\delta)$ est simplement $(\alpha, 0, 0)$. On décompose souvent un élément de $H(\delta)$ ainsi :

$$(\alpha, x_1, x_2) = \alpha(1, 0, x_2).(1, x_1, 0) = \frac{\alpha}{\langle x_1, x_2\rangle}(1, x_1, 0)(1, 0, x_2).$$

Définition 3.3.2. Une thêta structure est un isomorphisme d'extensions centrales $\Theta_{\mathcal{L}}(\delta) : H(\delta) \xrightarrow{\sim} G(\mathcal{L})$.

Une thêta structure $\Theta_{\mathcal{L}}(\delta)$ induit donc un isomorphisme symplectique[1] $\overline{\Theta}_{\mathcal{L}}(\delta) : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ et le diagramme suivant commute :

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & H(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \Theta_{\mathcal{L}}(\delta)} & & \downarrow{\scriptstyle \overline{\Theta}_{\mathcal{L}}(\delta)} & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0.
\end{array}$$

On a une section (ensembliste) canonique de $H(\delta) \to K(\delta)$ donnée par $s_\delta : (x_1, x_2) \mapsto (1, x_1, x_2)$. Cette section se restreint en un morphisme de groupe sur tout sous-groupe isotrope de $K(\delta)$ par définition de e_δ en tant que commutateur. Si $\Theta_{\mathcal{L}}(\delta) : H(\delta) \to G(\mathcal{L})$ est une thêta structure, elle induit donc

- Un isomorphisme symplectique $\overline{\Theta}_{\mathcal{L}}(\delta) : K(\delta) \to K(\mathcal{L})$. Cet isomorphisme transporte la décomposition $K(\delta) = K_1(\delta) \oplus K_2(\delta)$ en une décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.
- Deux sections (de groupe) $s_{K_1(\mathcal{L})} : K_1(\mathcal{L}) \to G(\mathcal{L})$ et $s_{K_2(\mathcal{L})} : K_2(\mathcal{L}) \to G(\mathcal{L})$ comme restrictions de la section (ensembliste) $s_{K(\mathcal{L})} : K(\mathcal{L}) \to G(\mathcal{L})$ induite par s_δ.

1. Par définition de e_δ et $e_{\mathcal{L}}$ comme commutateurs.

PROPOSITION 3.3.3. *Il y a bijection entre les thêta structures $\Theta_{\mathcal{L}}(\delta)$ et les triplets $(\overline{\Theta}_{\mathcal{L}}(\delta), s_{K_1(\mathcal{L})}, s_{K_2(\mathcal{L})})$ où $\overline{\Theta}_{\mathcal{L}}(\delta)$ est un isomorphisme symplectique $K(\delta) \to K(\mathcal{L})$, $K_i(\mathcal{L}) \coloneqq \overline{\Theta}_{\mathcal{L}}(\delta)K(\delta)_i$ et $s_{K_i(\mathcal{L})}$ est une section (de groupe) $K_i(\mathcal{L}) \to G(\mathcal{L})$ pour $i = 1, 2$.*

En particulier, il existe toujours une thêta structure $\Theta_{\mathcal{L}}(\delta) : \mathcal{H}(\delta) \to G(\mathcal{L})$ au-dessus d'un morphisme symplectique $\overline{\Theta}_{\mathcal{L}}(\delta) : K(\delta) \to K(\mathcal{L})$.

DÉMONSTRATION : On a vu qu'une thêta structure induisait un tel triplet. Réciproquement, si $x = (\alpha, x_1, x_2) \in H(\delta)$, on a $x = \alpha.(1, x_1, 0).(1, 0, x_2)$ et on envoie x sur

$$\alpha.s_{K_1(\mathcal{L})}(\overline{\Theta}_{\mathcal{L}}(\delta)(x_1)).s_{K_2(\mathcal{L})}(\overline{\Theta}_{\mathcal{L}}(\delta)(x_2)).$$

Enfin, on a vu dans la proposition 3.2.6 qu'il existait toujours une section de $K(\mathcal{L})_i \to G(\mathcal{L})$ pour $i = 1, 2$, ce qui implique l'existence d'une thêta structure au-dessus de $\overline{\Theta}_{\mathcal{L}}(\delta)$. ■

Dorénavant, étant donné une thêta structure $\Theta_{\mathcal{L}}(\delta)$, on considère toujours la décomposition de $K(\mathcal{L})$ donnée par $K_1(\mathcal{L}) = \overline{\Theta}_{\mathcal{L}}(\delta)(K_1(\delta))$ et $K_2(\mathcal{L}) = \overline{\Theta}_{\mathcal{L}}(\delta)(K_2(\delta))$. De plus, on a des groupes de niveau canoniques au-dessus de $K_1(\delta)$ et $K_2(\delta)$ donnés par $\widetilde{K}_1(\delta) \coloneqq \{(1, i, 0)\}_{i \in K_1(\delta)}$ et $\widetilde{K}_2(\delta) \coloneqq \{(1, 0, j)\}_{j \in K_1(\delta)}$. On appelle les sous-groupes de niveau $\Theta_{\mathcal{L}}(\delta)(\widetilde{K}_i(\delta))$ $(i = 1, 2)$ de $G(\mathcal{L})$ les groupes de niveau induits par la thêta structure $\Theta_{\mathcal{L}}(\delta)$. On note souvent une thêta structure $\Theta_{\mathcal{L}}$ quand on n'a pas besoin de préciser son niveau δ.

Supposons donnée une décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$, on peut associer à cette décomposition le groupe $H(\mathcal{L}) = k^* \times K_1(\mathcal{L}) \times K_2(\mathcal{L})$ muni de la loi de groupe donnée par

$$(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha\beta e_{\mathcal{L}}(x_1, y_2), x_1 + x_2, y_1 + y_2).$$

La proposition 3.3.3 montre qu'une thêta structure $\Theta_{\mathcal{L}}(\delta)$ qui respecte cette décomposition est la composée de deux isomorphismes (dans GPAB_{k^*}) : un isomorphisme $H(\mathcal{L}) \xrightarrow{\sim} G(\mathcal{L})$ qui se restreint en l'identité sur $K(\mathcal{L})$, déterminé entièrement par les sections $s_{K_1(\mathcal{L})}$ et $s_{K_2(\mathcal{L})}$; et un isomorphisme $\mathcal{H}(\delta) \xrightarrow{\sim} H(\mathcal{L})$, déterminé entièrement par un isomorphisme symplectique $\overline{\Theta}_{\mathcal{L}}(\delta) : K(\delta) \to K(\mathcal{L})$ qui respecte la décomposition de $K(\mathcal{L})$.

La proposition 3.3.1 montre que l'isomorphisme $\overline{\Theta}_{\mathcal{L}}(\delta)$ précédent est juste une manière d'énumérer les éléments de $K_1(\mathcal{L})$. L'information géométrique d'une thêta structure est donc contenue dans la section $s_{K(\mathcal{L})} : K(\mathcal{L}) \to G(\mathcal{L})$, ou de manière équivalente dans le choix de groupes de niveau $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ au-dessus de $K_1(\mathcal{L})$ et $K_2(\mathcal{L})$. On appelle un tel choix une structure de niveau sur $G(\mathcal{L})$ au-dessus de la décomposition de $K(\mathcal{L})$. Plus généralement, une structure de niveau sur $G(\mathcal{L})$ est un choix de groupes de niveau $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ tels que $\rho_{G(\mathcal{L})}(\widetilde{K}_1(\mathcal{L}))$ et $\rho_{G(\mathcal{L})}(\widetilde{K}_2(\mathcal{L}))$ forment une décomposition symplectique de $K(\mathcal{L})$.

EXEMPLE 3.3.4. L'interprétation d'une structure de niveau au-dessus d'une décomposition de $K(\mathcal{L})$ peut se voir dans le cas complexe de la manière suivante :

Soit $X = V/\Lambda$ une variété algébrique complexe, $\Lambda = \Lambda_1 \oplus \Lambda_2$ une décomposition symplectique de Λ, $\mathcal{L}$ un fibré en droite ample sur X et $c \in V$ une caractéristique de $\mathcal{L}$ pour cette décomposition. Soit a_c la fonction $a_c(\lambda, z) \coloneqq e^{\pi i E(\lambda_1, \lambda_2) + 2\pi i E(c, \lambda)} e^{\pi H(z, \lambda) + \frac{\pi}{2} H(\lambda, \lambda)}$ qui se restreint en le facteur d'automorphie $a_{\mathcal{L}}$ sur $\Lambda \times V$.

Le groupe thêta $\mathcal{G}(\mathcal{L})$ est égal à $\mathfrak{G}(\mathcal{L})/s_c(\Lambda)$ où $s_c(\lambda) = [a_c(\lambda, 0), \lambda]$. On peut considérer s_c étendu à $\Lambda(\mathcal{L})$, cela donne une section de $\Lambda(\mathcal{L}) \to \mathfrak{G}(\mathcal{L})$. De plus, comme $\Lambda_1(\mathcal{L}) \oplus \Lambda_2$ est un réseau isotrope pour $E_{\mathcal{L}}$, s_c est un morphisme de groupe sur $\Lambda_1(\mathcal{L}) \oplus \Lambda_2$ (et de même sur $\Lambda_1 \oplus \Lambda_2(\mathcal{L})$), donc définit une structure de niveau par passage au quotient sur $\mathcal{G}(\mathcal{L})$.

En outre, changer c en lui additionnant un élément $c' \in \Lambda(\mathcal{L})$ ne change pas a_c restreint à $\Lambda \times V$, mais le change sur $\Lambda(\mathcal{L}) \times V$ (sauf si $c' \in \Lambda = \Lambda(\mathcal{L})^{\perp}$), et donc induit une structure

de niveau différente sur $\mathcal{G}(\mathcal{L})$. En regardant la définition de a_c, on voit que cela revient à changer la section s_c par le facteur $e^{2\pi i E_{\mathcal{L}}(c',\cdot)}$. Sur $\mathcal{G}(\mathcal{L})$, ceci correspond exactement au changement de structure de niveau donné par l'automorphisme $\mathtt{conj}_{\overline{c'}}$ où $\overline{c'}$ est la valeur de c' dans $K(\mathcal{L}) = \Lambda(\mathcal{L})/\Lambda$. On voit donc que toute structure de niveau sur $\mathcal{G}(\mathcal{L})$ vient d'un choix de c modulo Λ. Ainsi la valeur de c modulo $\Lambda(\mathcal{L})$ détermine $\mathcal{L}$ entièrement, et le choix d'une structure de niveau revient à choisir une valeur de c modulo Λ. ◊

Dans le cadre algébrique, le théorème 3.2.2 et la discussion à la fin de la section 3.2 montrent qu'on peut voir une section de groupe $s_{K_1(\mathcal{L})} : K_1(\mathcal{L}) \to G(\mathcal{L})$ comme un groupe de niveau $\widetilde{K}_1(\mathcal{L}) \subset G(\mathcal{L})$ au-dessus de $K_1(\mathcal{L})$; comme un caractère χ sur $\mathfrak{K}_1(\mathcal{L}) \coloneqq \rho_{G(\mathcal{L})}^{-1}(K_1(\mathcal{L}))$ qui se restreint à l'identité sur k^* ou encore comme un fibré en droites $\mathcal{L}_1$ sur $X/K_1(\mathcal{L})$ tel qu'il existe un isomorphisme $\psi : \pi^*\mathcal{L}_1 \to \mathcal{L}$ où π est l'isogénie canonique $X \to X/K_1(\mathcal{L})$. De plus, l'espace des groupes de niveau au-dessus de $K_1(\mathcal{L})$ est un espace homogène principal sous l'action de $K_2(\mathcal{L}) \simeq (K(\mathcal{L})/K_1(\mathcal{L})^\perp)$ via $c \in K_2(\mathcal{L}) \mapsto \mathtt{conj}_c$ où $\overline{c}$ est l'automorphisme de $G(\mathcal{L})$ décrit à la section 3.2.

Comme $K_1(\mathcal{L})$ est un sous-espace isotrope maximal, $K_1(\mathcal{L})^\perp = K_1(\mathcal{L})$.

Si on combine l'action de $K_2(\mathcal{L})$ sur les groupes de niveau au-dessus de $K_1(\mathcal{L})$ et celle de $K_1(\mathcal{L})$ sur les groupes de niveau au-dessus de $K_2(\mathcal{L})$, on trouve que l'espace des structures de niveau au-dessus de la décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ est un espace homogène principal sous l'action de $K(\mathcal{L})$. L'action de $K(\mathcal{L})$ sur la structure de niveau est donnée via l'action induite par l'automorphisme $\overline{c}$ lorsque $c \in K(\mathcal{L})$, autrement dit par la multiplication du caractère $e_{\mathcal{L}}(c, \cdot)$.

3.4 FONCTIONS THÊTA

Supposons que le fibré $\mathcal{L}$ soit très ample sur X. Il induit donc un plongement $X \to \mathbb{P}_k^{d-1}$ où d est le degré de $\mathcal{L}$. Ce plongement est déterminé à une action de $\mathrm{PGL}_d(k)$ près. Pour le fixer, il faut déterminer une base « canonique » de fonctions thêta (c'est-à-dire de sections globales de $\mathcal{L}$) dans l'esprit du chapitre 2. On va voir qu'une thêta structure nous fixe une telle base.

L'espace $V(\delta)$ des fonctions de $K_1(\delta)$ à valeurs dans k admet une représentation irréductible du groupe de Heisenberg $\mathcal{H}(\delta)$ donnée par

$$(\alpha, x_1, x_2).f = y \mapsto \alpha\langle y, -x_2\rangle f(y - x_1). \tag{3.4}$$

Il s'avère qu'une telle représentation est unique :

THÉORÈME 3.4.1. *Le groupe de Heisenberg $\mathcal{H}(\delta)$ admet une unique représentation irréductible telle que k^* agit naturellement. De plus, si V est une représentation de $H(\delta)$ telle que k^* agit naturellement sur V, alors $V \simeq \bigoplus_{i=1}^r V(\delta)$ et r est la dimension de l'espace des invariants de V pour n'importe quel sous-groupe de niveau maximal $\widetilde{K} \subset H(\delta)$.*

DÉMONSTRATION : Voir [Mum66, Proposition 2]. ■

Or si $V = \Gamma(X, \mathcal{L})$ est l'espace des sections globales du fibré $\mathcal{L}$, on a une action de $G(\mathcal{L})$ sur V donnée par

$$(x, \phi).s = t_{-x}^* \phi(s) \tag{3.5}$$

si $(x, \phi) \in G(\mathcal{L})$ et $s \in V$.

REMARQUE 3.4.2. Si $f : X \to Y$ est une isogénie, $\mathcal{M}$ un fibré en droites sur Y tel que $\mathcal{L} = t_f^*\mathcal{M}$, soit $\widetilde{K}$ le groupe de niveau au-dessus de $K = \mathrm{Ker}\, f$ correspondant à $\mathcal{M}$ et $\alpha_f : \mathcal{Z}(\widetilde{K}) \to G(\mathcal{M})$

le morphisme donné dans la proposition 3.2.5. Soit $V = \Gamma(X, \mathcal{L})$ et $W = \Gamma(Y, \mathcal{M})$, si $s \in W$ alors $f^*s \in V$. La preuve de la proposition 3.2.5 montre que si $g \in \mathcal{Z}(\widetilde{K})$, on a :

$$g.f^*s = f^*(\alpha_f(g).s). \qquad \diamond$$

Proposition 3.4.3. *L'action de $G(\mathcal{L})$ sur $V = \Gamma(X, \mathcal{L})$ est irréductible.*

Démonstration : En effet, soit $\widetilde{K}$ un sous-groupe de niveau maximal de $G(\mathcal{L})$, et $K = \rho_{G(\mathcal{L})}(\widetilde{K})$. Si $X' = X/K$, la donnée de $\widetilde{K}$ permet de descendre $\mathcal{L}$ en un fibré $\mathcal{M}$ sur X' par le théorème 3.2.2. De plus, les sections invariantes par $\widetilde{K}$ sont exactement les sections globales de $\mathcal{M}$. Comme K est un sous-groupe isotrope maximal, il est de cardinal $d = \prod_{i=1}^{g} \delta_i$ et $\mathcal{M}$ est un fibré principal. Donc $h^0(X', \mathcal{M}) = 1$ et le théorème 3.4.1 montre alors que l'action de $G(\mathcal{L})$ sur V est irréductible. ■

Ainsi, une fois une théta structure $\Theta_{\mathcal{L}}(\delta)$ choisie, il existe un unique isomorphisme (à multiplication par un scalaire près) $\beta : V(\delta) \to \Gamma(X, \mathcal{L})$ qui commute à l'action de $H(\delta)$ et $G(\mathcal{L})$. Maintenant, $V(\delta)$ a une base canonique donnée par les $\{\gamma_i \mid i \in Z(\delta)\}$ où γ_i est la fonction de Kronecker :

$$\gamma_i(j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j. \end{cases}$$

On note alors $\vartheta_i = \beta(\gamma_i)$ pour $i \in Z(\delta)$. Ainsi la théta structure $\Theta_{\mathcal{L}}(\delta)$ nous fournit la base canonique de fonctions thêta $\{\vartheta_i \mid i \in Z(\delta)\}$ recherchée.

La théta structure $\Theta_{\mathcal{L}}(\delta)$ ne détermine la base des fonctions thêta qu'à une constante près, cependant si $\mathcal{L}$ est très ample, le plongement projectif $\phi_{\Theta_{\mathcal{L}}(\delta)} : X \to \mathbb{P}(\Gamma(X, \mathcal{L}))$ donné explicitement par $x \mapsto (\vartheta_i(x))_{i \in Z(\delta)}$ ne dépend pas de cette constante. En particulier, le point $\phi_{\Theta_{\mathcal{L}}(\delta)}(0_X)$ est uniquement déterminé par $\Theta_{\mathcal{L}}(\delta)$, on l'appelle le thêta null point. La preuve de la proposition 3.4.3 montre qu'on peut retrouver la base $\{\vartheta_i \mid i \in Z(\delta)\}$ de la manière suivante : β permet de transposer l'action de $\mathcal{H}(\delta)$ sur $V(\delta)$ en une action sur $V = \Gamma(X, \mathcal{L})$. De manière explicite si $(\alpha, x, y) \in \mathcal{H}(\delta)$ on a

$$(\alpha, x, y).\vartheta_i = \alpha e_\delta(x + i, -y)\vartheta_{i+x} \tag{3.6}$$

On considère alors le sous-groupe de niveau maximal de $\mathcal{H}(\delta)$ donné par $\widetilde{K} = s_\delta(\hat{Z}(\delta)) = \{(1, 0, j) : j \in \hat{Z}(\delta)\}$. L'espace des éléments de V laissés invariants par $\widetilde{K}$ est de dimension 1 et est engendré par ϑ_0. En transportant $\widetilde{K}$ en un sous-groupe de niveau de $G(\mathcal{L})$ via la théta structure $\Theta_{\mathcal{L}}(\delta)$, on obtient un sous-groupe de niveau au-dessus de $K_2(\mathcal{L})$, et donc une descente de $\mathcal{L}$ en un fibré principal $\mathcal{M}$ sur $X/K_2(\mathcal{L})$. La fonction ϑ_0 s'obtient alors comme le tiré en arrière d'une section globale de $\mathcal{M}$. Ensuite, si $i \in Z(\delta)$, on retrouve $\vartheta_i = (1, i, 0).\vartheta_0$.

Remarque 3.4.4. La base $(\vartheta_i)_{i \in Z(\delta)}$ de $\Gamma(X, \mathcal{L})$ est uniquement déterminée par la structure de niveau sur $G(\mathcal{L})$ induite par la théta structure $\Theta_{\mathcal{L}}(\delta)$. La numérotation $K_1(\delta) \xrightarrow{\sim} K_1(\mathcal{L})$ également induite par $\Theta_{\mathcal{L}}(\delta)$ sert juste à numéroter les fonctions thêta. Il nous arrivera lorsqu'on n'a pas besoin d'une telle numérotation de noter la base précédente comme $(\vartheta_i)_{i \in K_1(\mathcal{L})}$.

L'action de $G(\mathcal{L})$ sur $V = \Gamma(X, \mathcal{L})$ induit une action projective de $K(\mathcal{L})$ sur V, et donc une action de $K(\mathcal{L})$ sur $\mathbb{P}(V)$. Si le fibré $\mathcal{L}$ est très ample, il induit un plongement projectif de X dans $\mathbb{P}(V)$, et l'action de $u \in K(\mathcal{L})$ précédente restreinte à X est simplement la translation par $-u$. Si $x = (\vartheta_i(x)_{i \in K_1(\mathcal{L})}) \in X$, alors l'équation (3.6) donne si $u = u_1 + u_2$ est la décomposition de u :

$$x - u = (e_{\mathcal{L}}(i + u_1, -u_2)\vartheta_{i+u_1}(x)). \tag{3.7}$$

$\diamond$

EXEMPLE 3.4.5. Soit $(X = V/\Lambda, \mathcal{L})$ une variété abélienne complexe munie d'une polarisation de type δ. Soit $\Theta_{\mathcal{L}}$ une thêta structure sur $(X, \mathcal{L})$, et $c \in X(k)$ la caractéristique associé à $\Theta_{\mathcal{L}}$ (voir l'exemple 3.3.4). On peut écrire, si $D = D_\delta$, $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ où $\Omega D^{-1} \in \mathfrak{H}_g$ (voir la section 2.5. On a donc $K_1(\mathcal{L}) = D^{-1}\Omega\mathbb{Z}^g/\mathbb{Z}^g$ et $K_2(\mathcal{L}) = D^{-1}\mathbb{Z}^g/\mathbb{Z}^g$. Alors la discussion précédente et la section 2.6 montrent que l'on a pour $i \in K_2(\mathcal{L})$:

$$\vartheta_i = \vartheta \begin{bmatrix} D_\delta c_1 \\ c_2 + i \end{bmatrix} (\cdot, \Omega D_\delta^{-1})$$

Le lecteur attentif aura remarqué que nous avons inversé le groupe qui numérote les fonctions thêta entre le cas complexe où l'on prend $K_2(\mathcal{L})$ et le cas algébrique où l'on prend $K_1(\mathcal{L})$. C'est pour nous conformer à la tradition qui veut que dans le cas complexe on décompose les réseaux sous la forme $\Omega\mathbb{Z}^g + \mathbb{Z}^g$ plutôt que l'inverse. De plus, dans le cas complexe, par définition des fonctions thêta avec caractéristiques, on a $\vartheta_i = \lambda\vartheta_0(\cdot + i)$, de telle sorte que l'on obtenait ϑ_i en faisant agir $(1, 0, -i)$ sur ϑ_0. ◇

Si $\mathcal{L}$ n'est pas très ample, on peut quand même définir un thêta null point de la manière suivante : on fixe une trivialisation $\gamma_0 : \mathcal{L}(0) \xrightarrow{\sim} k$, alors pour tout $x \in K(\mathcal{L})$ on a une trivialisation $\gamma_x : \mathcal{L}(x) \xrightarrow{\sim} k$ donnée par la composition $\mathcal{L}(x) = t_x^*\mathcal{L}(0) \xrightarrow{\phi_x^{-1}(0)} \mathcal{L}(0) \xrightarrow{\lambda_0} k$ où $(x, \phi_x) = s_{K(\mathcal{L})}(x)$. Si $s \in \Gamma(X, \mathcal{L})$, on peut donc définir la « valeur » de s en x comme étant $\lambda_x(s)$. Par la définition de λ_x, on a $\lambda_x(s) = \lambda_0(s_{K(\mathcal{L})(x)^{-1}}.s)$. Si $s \in \Gamma(X, \mathcal{L})$, et $(x_1, x_2) \in K(\delta)$, on définit $s(x_1, x_2) \coloneqq \lambda_{\overline{\Theta}_{\mathcal{L}}(\delta)(x_1,x_2)}(s)$, la valeur de s au point $\overline{\Theta}_{\mathcal{L}}(\delta)(x_1, x_2)$. Comme la section choisie au-dessus de $\overline{\Theta}_{\mathcal{L}}(\delta)(x_1, x_2)$ correspond via la thêta structure à $(1, x_1, x_2)$, on a donc

$$s(x_1, x_2) = \left((1, x_1, x_2)^{-1}.s\right)(0, 0).$$

On vérifie alors que

$$\begin{aligned} s(x_1, x_2) &= \left((1, y_1, y_2)(1, x_1, x_2)^{-1}.s\right)(y_1, y_2) \\ &= \left((\langle y_1 - x_1, -x_2\rangle, y_1 - x_1, y_2 - x_2).s\right)(y_1, y_2) \end{aligned} \tag{3.8}$$

ce qui correspond à un changement de variable près à la formule donnée par Mumford dans [Mum66, Theorem 3].

En particulier, on peut définir $(q_{\mathcal{L}}(i))_{i\in Z(\delta)} \coloneqq (\vartheta_i(0))_{i\in Z(\delta)}$, le thêta null point associé à la thêta structure, défini modulo l'action de k^*. On retrouve bien le thêta null point précédent défini pour un fibré très ample. L'équation (3.8) montre alors que si $i \in Z(\delta)$, et $(x_1, x_2) \in K(\delta)$ on a en utilisant l'équation (3.6) :

$$\begin{aligned} \vartheta_i(x_1, x_2) &= \left((\langle x_1, x_2\rangle, -x_1, -x_2).\vartheta_i\right)(0) \\ &= \langle i, x_2\rangle.\vartheta_{i-x_1}(0) \\ &= \langle i, x_2\rangle.q_{\mathcal{L}}(i - x_1) \end{aligned} \tag{3.9}$$

Ainsi, si le thêta null point n'est pas identiquement nul (c'est le cas si $\mathcal{L}$ est très ample puisqu'il définit un point projectif), il détermine entièrement la section $s_{K(\mathcal{L})}$. En effet, si $x = \overline{\Theta}_{\mathcal{L}}(\delta)(x_1, x_2)$, soit $i \in Z(\delta)$ un point tel que $q_{\mathcal{L}}(i) \neq 0$, alors $s_{K(\mathcal{L})}(x)$ est l'unique morphisme $\phi : \mathcal{L} \to t_x^*\mathcal{L}$ tel que $\lambda_0(\phi^{-1}\vartheta_i) = \langle i, x_2\rangle.q_{\mathcal{L}}(i - x_1)$.

De plus, si $\mathcal{L}$ est très ample, alors les points de $K(\mathcal{L})$ sont entièrement déterminés par leurs coordonnées $(\vartheta_i(x))_{i\in Z(\delta)}$ lorsque $x \in K(\mathcal{L})$. Mais ces coordonnées se déduisent du thêta null point via l'équation (3.9), et donc le thêta null point détermine $\overline{\Theta}_{\mathcal{L}}(\delta)$. Comme on a vu qu'il déterminait la section au-dessus de $K(\mathcal{L})$, on voit que $\Theta_{\mathcal{L}}(\delta)$ est entièrement déterminée par $(q_{\mathcal{L}}(i))_{i\in Z(\delta)}$. On verra dans le théorème 4.7.1 que si de plus $4 \mid \delta$, les équations projectives du plongement $\phi_{\Theta_{\mathcal{L}}(\delta)}(X)$ dépendent uniquement du thêta null point, donc dans ce cas $(q_{\mathcal{L}}(i))_{i\in Z(\delta)}$ détermine uniquement le triplet $(A, \mathcal{L}, \Theta_{\mathcal{L}}(\delta))$.

3.5 AUTOMORPHISMES DU GROUPE DE HEISENBERG

Soit $(X, \mathcal{L})$ une variété abélienne polarisée de type δ. On a vu qu'il existait des thêta structures sur $(X, \mathcal{L})$, le but de cette section est de toutes les déterminer. Si $\Theta_{\mathcal{L}}(\delta)$ est une telle thêta structure, et ψ un isomorphisme du groupe de Heisenberg $\mathcal{H}(\delta)$ qui se restreint en l'identité sur k^*, alors $\Theta_{\mathcal{L}}(\delta) \circ \psi$ est une thêta structure ; réciproquement si $\Theta_{\mathcal{L}}(\delta)'$ est une thêta structure, $\Theta_{\mathcal{L}}(\delta)^{-1} \circ \Theta_{\mathcal{L}}(\delta)'$ est un automorphisme de $\mathcal{H}(\delta)$ qui se restreint en l'identité sur k^*. Ainsi les thêta structures forment un espace homogène principal sous $\mathrm{Aut}(\mathcal{H}(\delta))$, le groupe des automorphismes de l'extension centrale $\mathcal{H}(\delta)$.

Il nous faut donc déterminer ces automorphismes, ainsi que leur action sur le thêta null point. En effet, (si $4 \mid \delta$), le thêta null point $(\vartheta_i^{\mathcal{L}}(0))_{i \in Z(\delta)}$ détermine le triplet $(X, \mathcal{L}, \Theta_{\mathcal{L}}(\delta))$ où $\Theta_{\mathcal{L}}(\delta)$ est une thêta structure, et donc deux thêta null points correspondent à la même variété polarisée $(X, \mathcal{L})$ si et seulement s'ils différent d'une action de $\mathrm{Aut}(\mathcal{H}(\delta))$.

Soit $\psi \in \mathrm{Aut}(\mathcal{H}(\delta))$; par le même raisonnement que dans la section 3.3 on voit que ψ induit un isomorphisme symplectique $\overline{\psi}$ sur $K(\delta)$ tel que le diagramme suivant commute :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & H(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\ & & \| & & \downarrow \psi & & \downarrow \overline{\psi} & & \\ 1 & \longrightarrow & k^* & \longrightarrow & H(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0. \end{array}$$

PROPOSITION 3.5.1. *Si l'on note* $\mathrm{Sp}(K(\delta))$ *le groupe des isomorphismes symplectiques sur* $K(\delta)$*, on a donc un morphisme d'oubli* $\mathrm{Aut}(\mathcal{H}(\delta)) \to \mathrm{Sp}(K(\delta)), \psi \mapsto \overline{\psi}$*. On a alors une suite exacte :*

$$0 \longrightarrow K(\delta) \longrightarrow \mathrm{Aut}(H(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 0.$$

DÉMONSTRATION : On a déjà vu qu'un automorphisme $\psi \in \mathrm{Aut}(\mathcal{H}(\delta))$ induisait un isomorphisme symplectique $\overline{\psi}$ de $K(\delta)$. Réciproquement, si on a un isomorphisme symplectique $\overline{\psi}$ sur $K(\delta)$, il faut montrer qu'il provient d'un automorphisme ψ du groupe de Heisenberg. Mais en revenant à la preuve de la proposition 3.3.3, on voit qu'il existe des isomorphismes $\psi_1 : \mathcal{H}(\delta) \to \mathcal{H}(\delta)$ et $\psi_2 : \mathcal{H}(\delta) \to \mathcal{H}(\delta)$ au-dessus de $K(\delta) \xrightarrow{\mathrm{Id}} K(\delta)$ et $K(\delta) \xrightarrow{\psi} K(\delta)$ réciproquement. On peut alors poser $\psi = \psi_2 \circ \psi_1^{-1}$. (Une autre manière est d'appliquer la preuve de la proposition 3.2.6 qui montre qu'il existe des groupes de niveau dans $\mathcal{H}(\delta)$ au-dessus de $\overline{\psi}(K_1(\delta))$ et $\overline{\psi}(K_2(\delta))$.

Maintenant, si ψ est un élément du noyau, alors $\overline{\psi}$ laisse $K(\delta)$ invariant. Il existe donc un caractère χ sur $K(\delta)$ tel qu'on ait

$$\psi : (\alpha, x) \mapsto (\alpha\chi(x), x).$$

Comme e_δ est non dégénérée, χ est représenté par un $c \in K(\delta)$, c'est-à-dire que l'on a $\chi(x) = e_\delta(c, x)$ pour tout $x \in K(\delta)$. Si la décomposition de $c \in K(\delta) = K_1(\delta) \oplus K_2(\delta)$ est donnée par $c = c_1 + c_2$, l'automorphisme $\psi_c \in \mathrm{Aut}(H(\delta))$ correspondant est donc donné par

$$\psi_{(c_1,c_2)} : (\alpha, x_1, x_2) \mapsto (\alpha\langle c_1, x_2\rangle\langle c_2, x_1\rangle, x_1, x_2) \tag{3.10}$$

(De plus, la discussion suivant la proposition 3.3.3 montre que l'action de ψ_c sur $\Theta_{\mathcal{L}}(\delta)$ correspond exactement à l'action de $\mathtt{conj}_{\overline{\Theta}_{\mathcal{L}}(\delta)(c)}$ sur $\Theta_{\mathcal{L}}(\delta)$). ∎

REMARQUE 3.5.2. Si l'on veut décrire explicitement un relevé ψ d'un isomorphisme symplectique $\overline{\psi}$ de $K(\delta)$, on peut procéder ainsi : un semi-caractère χ pour $\overline{\psi}$ est une application $\chi : K(\delta) \to k^*$ telle que

$$\chi(i_1 + i_2, j_1 + j_2) = \chi(i_1, j_1)\chi(i_2, j_2)\frac{\langle \overline{\psi}(i_1 + i_2)_1, \overline{\psi}(j_1 + j_2)_2 \rangle}{\langle i_1, j_2 \rangle}.$$

Un tel semi-caractère pour $\overline{\psi}$ donne un relevé ψ par $\psi(\alpha, i, j) = (\alpha\chi(i, j), \overline{\psi}(i + j))$, et il est clair qu'il y a une bijection entre les semi-caractères pour $\overline{\psi}$ et les relevés ψ de $\overline{\psi}$. La proposition 3.5.1 montre qu'il existe toujours un semi-caractère pour $\overline{\psi}$, et de plus, quitte à agir par conjugaison d'un élément $c \in K(\mathcal{L})$, si $(e_1, \dots, e_g, e'_1, \dots, e_g)$ est la base canonique de $K(\delta)$, on peut choisir χ tel que $\chi(e_i) = \mu_i$, $\chi(e'_i) = \mu'_i$ où μ_i et μ'_i sont des racines δ_i-ièmes de l'unité pour $i \in [1..g]$. On pourrait le prouver directement en adaptant la preuve de la proposition 3.2.6. ◇

Il nous faut maintenant étudier l'action de ψ sur un thêta null point quand ψ est un automorphisme du groupe de Heisenberg. Plus généralement, si $\Theta_{\mathcal{L}}(\delta)$ est une thêta structure sur $(X, \mathcal{L})$, on va déterminer l'action d'un tel automorphisme sur la base canonique $(\vartheta_i)_{i \in Z(\delta)}$. On note $(\vartheta'_i)_{i \in Z(\delta)}$ la base canonique de $\Gamma(X, \mathcal{L})$ déterminée par $\Theta'_\delta := \Theta_\delta \circ \psi$.

Si on regarde la construction de la base canonique associée à une thêta structure expliquée dans la section 3.4, on voit qu'il suffit de trouver $\vartheta'_0 \in \Gamma(X, \mathcal{L})$ une fonction invariante (non nulle) par l'action de $\psi(s_\delta(\hat{Z}(\delta)))$, les fonctions ϑ'_i pour $i \in Z(\delta)$ étant alors déterminée par $\psi((1, i, 0)).\vartheta'_0$. Mais si $i \in Z(\delta)$, la fonction $T_i := \sum_{j \in \hat{Z}(\delta)} \psi(s_\delta(j)).\vartheta_i$ est invariante, et comme les fonctions thêta forment une base de $\Gamma(X, \mathcal{L})$, il existe un i tel que T_i soit non nul.

Par exemple $\psi_c \in \mathrm{Aut}(\mathcal{H}(\delta))$ correspond à $c = (c_1, c_2) \in K(\delta)$, l'équation (3.10) montre qu'il faut trouver une fonction invariante par $\{(\langle c_1, j \rangle, 0, j)\}_{j \in \hat{Z}(\delta)}$. On vérifie immédiatement que ϑ_{c_1} est une telle fonction. La nouvelle base est donc donnée par

$$\vartheta'_i = \langle -i, c_2 \rangle \vartheta_{c_1 + i}.$$

Pour donner un autre exemple, si ψ provient d'un automorphisme symplectique $\overline{\psi}$ de $K(\delta)$ tel que $\overline{\psi}(K_2(\delta)) = K_1 \times K_2$, on vérifie immédiatement que $\vartheta'_0 = \sum_{i \in K_1} \vartheta_i$ comme K_2 est orthogonal à K_1. En particulier, on note $\mathfrak{I}$ l'automorphisme qui vient du morphisme symplectique σ consistant à permuter $K_1(\delta)$ et $K_2(\delta)$. On obtient :

$$\vartheta'_i = \sum_{j \in Z(\delta)} \langle -j, \sigma(i) \rangle \vartheta_j. \tag{3.11}$$

3.6 LE THÉORÈME DE L'ISOGÉNIE

Soit $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ une isogénie de noyau K telle que $f^*\mathcal{M} = \mathcal{L}$. On a vu dans le théorème 3.2.2 que $G(\mathcal{M}) \simeq \mathcal{Z}(\widetilde{K})/\widetilde{K}$ où $\widetilde{K}$ est le groupe de niveau de K correspondant à cette isogénie. Soit $\Theta_{\mathcal{L}}$ une thêta structure sur $(X, \mathcal{L})$ et $\Theta_{\mathcal{M}}$ une thêta structure sur $(Y, \mathcal{M})$, on veut définir une notion de compatibilité entre $\Theta_{\mathcal{L}}$ et $\Theta_{\mathcal{M}}$ par rapport à l'isomorphisme $G(\mathcal{M}) \simeq \mathcal{Z}(\widetilde{K})/\widetilde{K}$. Soit α_f le morphisme $\mathcal{Z}(\widetilde{K}) \twoheadrightarrow G(\mathcal{M})$ induit par l'isomorphisme $G(\mathcal{M}) \simeq \mathcal{Z}(\widetilde{K})/\widetilde{K}$. La thêta structure $\Theta_{\mathcal{L}}$ induit une section $s_{\mathcal{L}} : K(\mathcal{L}) \to G(\mathcal{L})$, qui se restreint en une section $s_{\mathcal{L}|K^\perp} : K^\perp \to G(\mathcal{L})$. On a également une section $s^*_{\mathcal{M}} : K^\perp \to G(\mathcal{L})$. Si $x \in K^\perp$, $s^*_{\mathcal{M}}(x)$ est l'unique automorphisme au-dessus de x dans $\alpha_f^{-1}(s_{\mathcal{M}}(f(x)))$:

$$\mathcal{L} \xrightarrow{s^*_{\mathcal{M}}(x)} t_x^*\mathcal{L}$$

$$\mathcal{M} \xrightarrow{s_{\mathcal{M}}(f(x))} t^*_{f(x)}\mathcal{M}.$$

Définition 3.6.1. Avec les notations précédentes, soit $\widetilde{K}_i(\mathcal{L})$ les sous-groupes de niveau maximaux de $G(\mathcal{L})$ associés à la thêta structure $\Theta_{\mathcal{L}}$, et $\widetilde{K}_i(\mathcal{M})$ les sous-groupes de niveau de $G(\mathcal{M})$ associés à $\Theta_{\mathcal{M}}$.

On dit que $\operatorname{Ker} f$ est compatible avec la décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ si on a $\operatorname{Ker} f = (K_1(\mathcal{L}) \bigcap \operatorname{Ker} f) \oplus (K_2(\mathcal{L}) \bigcap \operatorname{Ker} f)$ (comme $\operatorname{Ker} f$ et $\operatorname{Ker} f^\perp$ sont orthogonales, cette condition est équivalente à $\operatorname{Ker} f^\perp = (K_1(\mathcal{L}) \bigcap \operatorname{Ker} f^\perp) \oplus (K_2(\mathcal{L}) \bigcap \operatorname{Ker} f^\perp)$).

Dans ce cas, on dit qu'une décomposition $K(\mathcal{M}) = K_1(\mathcal{M}) \oplus K_2(\mathcal{M})$ est compatible avec la décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ si $f(K_i(\mathcal{L}) \bigcap \operatorname{Ker} f^\perp) \subset K_i(\mathcal{M})$ pour $i = 1, 2$ (on a alors égalité).

On dit qu'une structure de niveau sur $G(\mathcal{L})$ est f-compatible avec $\mathcal{M}$ si $\widetilde{K} = (\widetilde{K} \bigcap \widetilde{K}_1(\mathcal{L})) \oplus (\widetilde{K} \bigcap \widetilde{K}_2(\mathcal{L}))$. Cela équivaut à ce que $\operatorname{Ker} f$ soit compatible avec la décomposition de $K(\mathcal{L})$ et que $s_{\mathcal{L}|K^\perp} = s^*_{\mathcal{M}}$ sur $K = \operatorname{Ker} f$.

Dans ce cas, on a $\mathcal{Z}(\widetilde{K}) \simeq k^* \times (\mathcal{Z}(\widetilde{K}) \bigcap \widetilde{K}_1(\mathcal{L})) \times (\mathcal{Z}(\widetilde{K}) \bigcap \widetilde{K}_2(\mathcal{L}))$ et on dit qu'une structure de niveau sur $G(\mathcal{M})$ est compatible avec celle sur $G(\mathcal{L})$ lorsqu'on a $\alpha_f : \widetilde{K}_i(\mathcal{L}) \bigcap \mathcal{Z}(\widetilde{K}) \subset \widetilde{K}_i(\mathcal{M})$ pour $i = 1, 2$ (on a alors égalité), ou de manière équivalente si $s_{\mathcal{L}|K^\perp} = s^*_{\mathcal{M}}$ sur $K^\perp$.

Enfin on dit qu'une thêta structure $\Theta_{\mathcal{M}}$ sur $G(\mathcal{M})$ est f-compatible avec une thêta structure $\Theta_{\mathcal{L}}$ sur $G(\mathcal{L})$ si les structures de niveau induites sont compatibles. ◊

Proposition 3.6.2. *Soit $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété polarisée munie d'une thêta structure de type δ. Soit K un sous-groupe de $K(\mathcal{L})$ qui s'écrit $K = K_1 \oplus K_2$, avec $K_i \subset K_i(\mathcal{L})$, $Y = X/K$ et f l'isogénie associée. Soit $\widetilde{K}$ le sous-groupe de niveau au-dessus de K donné par*

$$\widetilde{K} = (\rho^{-1}_{G(\mathcal{L})}(K) \bigcap \widetilde{K}_1(\mathcal{L})) \oplus (\rho^{-1}_{G(\mathcal{L})}(K) \bigcap \widetilde{K}_2(\mathcal{L}))$$

et $\mathcal{M}$ un fibré de type δ_0 sur Y induit par $\widetilde{K}$, on a donc $f^*\mathcal{M} = \mathcal{L}$. Soit $K^\perp = K^{\perp,1} \oplus K^{\perp,2}$ la décomposition de $K^\perp$ induite par celle de K. Alors il y a bijection entre les thêta structures de type δ_0 sur $(Y, \mathcal{M})$ compatibles avec $\Theta_{\mathcal{L}}$ et les isomorphismes $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} Z(\delta_0)$. On note $\Theta(\sigma)$ la thêta structure sur $(Y, \mathcal{M})$ associée à un tel σ.

Démonstration : Si $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} Z(\delta_0)$ est un isomorphisme, son dual nous donne un isomorphisme $\hat{\sigma} : K^{\perp,2}/K_2 \xrightarrow{\sim} \hat{Z}(\delta_0)$. On en déduit une thêta structure $\Theta_{\mathcal{M}}$ sur $(Y, \mathcal{M})$ qui rend commutatif le diagramme (dans la catégorie GPAB_{k^*}) :

$$\begin{array}{ccc} k^* \times K^{\perp,1}/K_1 \times K^{\perp,2}/K_2 & \xrightarrow{\Theta_{\mathcal{L}}} & \mathcal{Z}(\widetilde{K})/\widetilde{K} \\ \downarrow{\scriptstyle 1_{k^*} \times \sigma \times \hat{\sigma}} & & \downarrow{\scriptstyle \alpha_f} \\ H(\delta_0) & \xrightarrow{\Theta_{\mathcal{M}}} & G(\mathcal{M}) \end{array} \tag{3.12}$$

La thêta structure $\Theta_{\mathcal{M}}$ est donc compatible avec $\Theta_{\mathcal{L}}$.

Réciproquement, si on a une thêta structure $\Theta_{\mathcal{M}}$ compatible avec celle de $\Theta_{\mathcal{L}}$, alors les groupes de niveau maximaux associés sont forcément $\alpha_f(\widetilde{K} \bigcap \widetilde{K}_1(\mathcal{L}))$ et $\alpha_f(\widetilde{K} \bigcap \widetilde{K}_2(\mathcal{L}))$ et

$\Theta_{\mathcal{M}}$ est alors entièrement déterminée par un isomorphisme symplectique de $K(\delta_0)$ avec $K(\mathcal{M})$ qui respecte la décomposition $K(\mathcal{M}) = K^{\perp,1}/K_1 \times K^{\perp,2}/K_2$. Or un tel isomorphisme vient d'un $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} Z(\delta_0)$ par la proposition 3.3.1. ∎

Pour résumer, pour avoir des thêta structures compatibles, il faut d'abord que $K = \operatorname{Ker} f$ soit compatible avec la décomposition de $K(\mathcal{L})$. Dans ce cas la décomposition de $K(\mathcal{M})$ est fixée, c'est $K(\mathcal{M}) = f(K_1(\mathcal{L})) \oplus f(K_2(\mathcal{L}))$. Il faut de plus que la structure de niveau de $G(\mathcal{L})$ soit compatible avec $\widetilde{K}$. En revenant à la définition 3.6.1, cela revient à demander que $\widetilde{K} = s_{K(\mathcal{L})}(K)$ ou encore que $\alpha_f(\widetilde{K}_i(\mathcal{L}) \cap \rho_{G(\mathcal{L})}^{-1}(K)) \cap k^* = \{1\}$ pour $i = 1, 2$ (car tout élément de $\widetilde{K}_i(\mathcal{L})$ au-dessus d'un élément de K doit être dans $\widetilde{K}$). On peut toujours supposer que c'est le cas, soit en changeant la structure de groupes de niveau de $G(\mathcal{L})$, soit en prenant comme dans la proposition 3.6.2 $\widetilde{K} = s_{K(\mathcal{L})}(K)$, c'est-à-dire en remplaçant $\mathcal{M}$ par un fibré algébriquement équivalent. On voit que la structure de niveau de $G(\mathcal{L})$ fixe $\mathcal{M}$ puisqu'elle fixe le groupe de niveau $\widetilde{K}$. La structure de groupes de niveau de $G(\mathcal{M})$ est alors fixée par celle de $G(\mathcal{L})$, les groupes de niveau étant donnés par $\alpha_f(\widetilde{K}_1(\mathcal{L}))$ et $\alpha_f(\widetilde{K}_2(\mathcal{L}))$. (Réciproquement on a alors $\widetilde{K}_i(\mathcal{L}) \cap \mathcal{Z}(K) = \alpha_f^{-1}(K_i(\mathcal{M}))$ pour $i = 1, 2$). Enfin, quand on a choisi des groupes de niveau compatibles, les thêta structures compatibles sont entièrement déterminées par le choix d'une numérotation de $K_1(\mathcal{L})$ (resp. $K_1(\mathcal{M})$), et le morphisme $\sigma : K_1(\mathcal{L}) \to K_1(\mathcal{M})$ de la proposition 3.6.2 permet de faire le lien entre deux telles numérotations.

L'information géométrique d'une thêta structure vient du choix d'une structure de niveau (c'est cette structure qui détermine la base de fonctions thêta, la numérotation de $K_1(\mathcal{L})$ étant juste une manière de les numéroter). Il est intéressant de regarder ce que devient la notion de compatibilité $f(\widetilde{K}_i(\mathcal{L}) \cap \mathcal{Z}(\widetilde{K})) \subset \widetilde{K}_i(\mathcal{M})$ pour $i = 1, 2$ suivant les différentes caractérisations des sous-groupes de niveau maximaux $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ données dans la section 3.3. Si χ_i et χ_i' sont les caractères correspondant à $\widetilde{K}_i(\mathcal{L})$ et $\widetilde{K}_i(\mathcal{M})$, alors cette condition devient χ_i et $\alpha_f^* \chi_i'$ coïncident sur $\mathfrak{K}_i(\mathcal{L}) \cap \mathcal{Z}(\widetilde{K})$. Si on préfère la vision de $\widetilde{K}_i(\mathcal{L})$ (resp. $\widetilde{K}_i(\mathcal{M})$) comme la donnée d'un fibré $\mathcal{L}_i$ sur $X/K_i(\mathcal{L})$ et d'un isomorphisme $\psi_i : \pi_i^* \mathcal{L}_i \xrightarrow{\sim} \mathcal{L}$ où π_i est l'isogénie $X \to X/K_i(\mathcal{L})$ (resp. d'un fibre $\mathcal{M}_i$ sur $Y/K_i(\mathcal{M})$ et d'un isomorphisme $\psi_i' : \pi_i'^* \mathcal{M}_i \xrightarrow{\sim} \mathcal{M}$ où π_i' est l'isogénie $Y \to X/K_i(\mathcal{M})$), alors le critère de compatibilité devient $\psi_i = f^* \psi_i'$. Chacune de ces descriptions montre que si $\Theta_{\mathcal{L}}$ et compatible avec $\Theta_{\mathcal{M}}$, et qu'on se donne $c \in K(\mathcal{L})$, alors l'action de c sur $\Theta_{\mathcal{L}}$ donne une thêta structure compatible avec l'action de $f(c)$ sur $\Theta_{\mathcal{M}}$. En particulier, si $c \in K$, l'action de $\mathtt{conj}_c$ donne une nouvelle structure de niveau sur $G(\mathcal{L})$ compatible avec celle de $G(\mathcal{M})$.

Exemple 3.6.3. Dans le cas complexe, comme d'habitude on se ramène au cas où $X = V/\Lambda$, $Y = V/\Lambda'$ et l'isogénie $f : X \to Y$ est induite par l'identité sur V. On suppose qu'on a des décompositions compatibles sur Λ et Λ'.

Soit $\mathcal{M}$ un fibré ample sur Y qui se tire en arrière en un fibré $\mathcal{L}$ sur X. Soit c une caractéristique de $\mathcal{L}$, la valeur de c modulo $\Lambda(\mathcal{L})$ détermine entièrement $\mathcal{L}$. On a vu dans l'exemple 3.3.4 qu'une structure de niveau sur $G(\mathcal{L})$ au-dessus de la décomposition de Λ était entièrement caractérisée par le choix d'un représentant de c modulo Λ. De même, si c' est une caractéristique de $\mathcal{M}$, la valeur de c' modulo $\Lambda(\mathcal{M})$ détermine entièrement $\mathcal{M}$ et un choix de représentant de c' modulo Λ' détermine la structure de niveau de $G(\mathcal{M})$.

En terme de ces caractéristiques c et c', on a alors $c = c'$ modulo $\Lambda(\mathcal{L})$ si et seulement si $\mathcal{M}$ se tire en arrière sur $\mathcal{L}$, et $c = c'$ modulo Λ' si les structures de niveau sur $G(\mathcal{M})$ et $G(\mathcal{L})$ sont compatibles. En particulier, dans ce cas on voit qu'on peut altérer la structure de niveau de $G(\mathcal{L})$ par un élément de $\Lambda'/\Lambda = \operatorname{Ker} f$ tout en restant compatible avec celle sur $G(\mathcal{M})$.

Si l'on revient à la situation générale, lorsqu'on a une isogénie $f : X \to Y$, et $\mathcal{M}$ un fibré ample sur Y tel que $f^*\mathcal{M} \simeq \mathcal{L}$, on souhaite déterminer l'application $f^* : \Gamma(Y, \mathcal{M}) \to \Gamma(X, \mathcal{L})$. Si x est un point géométrique de X et $y = f(x)$, on a le diagramme commutatif suivant :

$$\begin{array}{ccc} \Gamma(Y,\mathcal{M}) & \xrightarrow{t_y^*} & \Gamma(Y, t_y^*\mathcal{M}) \\ \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f^*} \\ \Gamma(X,\mathcal{L}) & \xrightarrow{t_x^*} & \Gamma(Y, t_x^*\mathcal{L}). \end{array}$$

On peut donc remplacer $\mathcal{M}$ par un fibré algébriquement équivalent si besoin, pour étudier f^*. (Et si on a des structures de niveau compatibles sur $G(\mathcal{L})$ et $G(\mathcal{M})$, alors l'action t_x^* (resp. t_y^*) transportent ces structures en des structures compatibles sur $G(t_x^*\mathcal{L})$ et $G(t_y^*\mathcal{M})$.)

Si nous avons insisté si longuement sur la caractérisation des thêta structures compatibles, c'est parce qu'on peut facilement exprimer f^* dans ce cadre.

THÉORÈME 3.6.4 (THÉORÈME DE L'ISOGÉNIE). *Soit $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ une isogénie de noyau K, $\Theta_{\mathcal{L}}$, $\Theta_{\mathcal{M}}$ des thêta structures compatibles sur $(X, \mathcal{L})$ et $(Y, \mathcal{M})$, et $\sigma : Z(\delta_0) \to K^{\perp,1}/K_1$ l'isomorphisme induit par $\Theta_{\mathcal{M}}$ (avec les notations de la proposition 3.6.2).*

Soit $(\vartheta^{\Theta_{\mathcal{L}}})_{i\in Z(\delta)}$ la base de $\Gamma(X, \mathcal{L})$ et $(\vartheta^{\Theta_{\mathcal{M}}})_{i\in Z(\delta_0)}$ la base de $\Gamma(Y, \mathcal{M})$, ce sont les bases canoniques associées aux thêta structures $\Theta_{\mathcal{L}}$ et $\Theta_{\mathcal{M}}$.

Ces bases sont canoniques modulo l'action de k^*

Alors il existe $\lambda \in k^*$ tel que tout $i \in Z(\delta_0)$

$$f^*\vartheta_i^{\Theta_{\mathcal{M}}} = \lambda \sum_{j\in\sigma^{-1}(i)} \vartheta_j^{\Theta_{\mathcal{L}}}.$$

DÉMONSTRATION : Soit $\beta_{\mathcal{L}}$ l'isomorphisme canonique de $\Gamma(X, \mathcal{L})$ sur $V(\delta)$ et $\beta_{\mathcal{M}}$ celui de $\Gamma(Y, \mathcal{M})$ sur $V(\delta_0)$ induits par les thêta structures $\Theta_{\mathcal{L}}$ et $\Theta_{\mathcal{M}}$ (voir la section 3.4). Si Φ est la composée $V(\delta_0) \xrightarrow{\beta_{\mathcal{M}}} \Gamma(Y, \mathcal{M}) \xrightarrow{f^*} \Gamma(X, \mathcal{L}) \xrightarrow{\beta_{\mathcal{L}}^{-1}} V(\delta_0)$, il faut montrer qu'il existe un $\lambda \in k^*$ tel que pour tout $g \in V(\delta_0)$ on ait

$$\Phi(g)(x) = \begin{cases} 0 & \text{si } x \notin K_1^{\perp} \\ \lambda g(\sigma x) & \text{si } x \in K_1^{\perp} \end{cases}$$

lorsqu'on est dans la situation du diagramme (3.12). Une preuve est donnée dans [Mum66, Theorem 4].

On peut en donner une démonstration directe en revenant à la construction de la base des fonctions thêta. Il suffit de montrer que

$$f^*\vartheta_0^{\Theta_{\mathcal{M}}} = \lambda \sum_{j\in K_1} \vartheta_j^{\Theta_{\mathcal{L}}}.$$

En effet, on a alors si $i \in Z(\delta_0)$, $\vartheta_i^{\Theta_{\mathcal{M}}} = (1, i, 0).\vartheta_0^{\Theta_{\mathcal{M}}}$ et par compatibilité des thêta structures, si $\sigma(i_0) = i$, on a $f^*(1, i, 0).\vartheta_k = (1, i_0, 0).f^*\vartheta_k$ d'où $f^*\vartheta_i^{\Theta_{\mathcal{M}}} = \lambda \sum_{j\in K_1} \vartheta_{i_0+j}^{\Theta_{\mathcal{L}}}$.

Or $\vartheta_0^{\Theta_{\mathcal{M}}}$ est l'unique fonction (à un scalaire près) invariante par $K_2(\mathcal{M})$, donc $f^*\ \vartheta_0^{\Theta_{\mathcal{M}}}$ est invariante par $K_1 \times K^{\perp,2}$, et c'est l'unique telle fonction (à un scalaire près) car $K_1 \times K^{\perp,2}$ est un sous-groupe isotrope maximal. De plus comme $K^{\perp,2}$ est orthogonal à K_1 on vérifie immédiatement que $\sum_{j\in K} \vartheta_j^{\Theta_{\mathcal{L}}}$ est également invariante par $K_1 \times K^{\perp,2}$ donc ces deux fonctions diffèrent d'un facteur multiplicatif. ∎

EXEMPLE 3.6.5. Si $\mathcal{L}$ est un fibré ample de type δ sur X, et que $\delta = \delta_0\delta'$, on peut considérer le théorème de l'isogénie appliqué à $K = \overline{\Theta}_{\mathcal{L}}(\hat{Z}(\delta')) \subset K_2(\mathcal{L})$ où $\Theta_{\mathcal{L}}$ est une théta structure pour $\mathcal{L}$. On a alors $K_1 = 0$ et $K^{\perp,1} \simeq Z(\delta_0)$ (avec les notations du théorème 3.6.4), on prend alors pour $\sigma : Z(\delta_0) \xrightarrow{\sim} K^{\perp,1}$ le morphisme issu de l'inclusion[1] $Z(\delta_0) \to Z(\delta)$. Si $f : X \to Y = X/K$ est l'isogénie associée et $\mathcal{M}$ est le fibré qui correspond à la descente de $\mathcal{L}$ par $\widetilde{K} = s_{K_2(\mathcal{L})}(K)$, et $\Theta(\sigma)$ est la théta structure sur $\mathcal{M}$ compatible avec $G(\mathcal{L})$ induite par σ on obtient qu'il existe $\lambda \in k^*$ tel que pour tout $i \in Z(\delta_0)$,

On utilise l'identification $Z(\delta_0) \subset Z(\delta)$ dans le membre de droite.

$$f^*(\vartheta_i^{\mathcal{M}}) = \vartheta_i^{\mathcal{L}}$$

On appelle f l'isogénie canonique de type $\hat{Z}(\delta')$ associée à la théta structure $\Theta_{\mathcal{L}}$.

Dans la suite, on est surtout intéressé par le cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$, avec n premier à ℓ. Pour illustrer ce cas lorsque $k = \mathbb{C}$, soit $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ la variété abélienne correspondant à $\Omega \in \mathfrak{H}_g$, et $\mathcal{L} = \mathcal{L}_0^{\ell}$ où $\mathcal{L}_0$ est la polarisation principale associée à Ω (de caractéristique 0). On a vu dans la section 2.6 que la base canonique de fonctions thêta associées à $\mathcal{L}$ était $\vartheta\left[\begin{smallmatrix} 0 \\ i/\ell n \end{smallmatrix}\right](z, \Omega/\ell n)$ où i parcourt $Z(\overline{\ell n})$. Dans cette situation, Y correspond à $\mathbb{C}^g/(\frac{\Omega}{\ell}\mathbb{Z}^g + \mathbb{Z}^g)$, et $\mathcal{M} = \mathcal{M}_0^n$ où $\mathcal{M}_0$ est la polarisation principale associée à Ω/ℓ. On vérifie que si $i \in Z(\overline{n})$ on a bien :

$$\vartheta_i^{\mathcal{M}}(z) = \vartheta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right]\left(z, \frac{\Omega}{\ell}/n\right) = \vartheta\left[\begin{smallmatrix} 0 \\ \ell i/\ell n \end{smallmatrix}\right](z, \Omega/\ell n) = \vartheta_{\ell i}^{\mathcal{L}}(z).$$

Plus généralement si $\mathcal{L}$ et $\mathcal{M}$ sont de caractéristiques c (de telle sorte que les théta structures associées sont compatibles par l'exemple 3.6.3, on a bien :

$$\vartheta_i^{\mathcal{M}}(z) = \vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2 + i/n \end{smallmatrix}\right]\left(z, \frac{\Omega}{\ell}/n\right) = \vartheta\left[\begin{smallmatrix} Dc_1 \\ c_2 + \ell i/\ell n \end{smallmatrix}\right](z, \Omega/\ell n) = \vartheta_{\ell i}^{\mathcal{L}}(z).$$

Si on regarde la même situation en prenant $K = \overline{\Theta}_{\mathcal{L}}(Z(\delta'))$, on obtient cette fois qu'il existe $\lambda \in k^*$ tel que pour tout $i \in Z(\delta_0)$,

$$f^*(\vartheta_i^{\mathcal{M}}) = \sum_{j \in Z(\delta')} \vartheta_{i+j}^{\mathcal{L}}.$$

♢

On appelle f l'isogénie de type $Z(\delta')$.

Ces deux situations seront étudiées en détail dans le chapitre 6. Il est clair que toute isogénie de noyau compatible avec la décomposition de $K(\mathcal{L})$ est une composée de deux isogénies de ce type. En fait, il suffit d'étudier le premier cas, car si on est dans le second cas, on peut se ramener au premier en considérant les théta structures $\mathfrak{I}_{\mathcal{L}} \circ \Theta_{\mathcal{L}}$ et $\mathfrak{I}_{\mathcal{M}} \circ \mathcal{M}$ où $\mathfrak{I}_{\mathcal{L}}$ est l'automorphisme de permutation de la décomposition de $K(\mathcal{L})$ décrit dans la section 3.5. Dans le cas complexe, on peut exprimer $\mathfrak{I}_{\mathcal{L}}$ ainsi : $\mathfrak{I}_{\mathcal{L}}$ transforme la base de fonctions thêta $(\vartheta\left[\begin{smallmatrix} 0 \\ i/\ell n \end{smallmatrix}\right](z, \Omega/\ell n))_{i \in Z(\overline{\ell n})}$ en la base $(\vartheta\left[\begin{smallmatrix} i/\ell n \\ 0 \end{smallmatrix}\right](\ell n z, \ell n \Omega))_{i \in Z(\overline{\ell n})}$ et réciproquement.

REMARQUE 3.6.6. Supposons que l'on prenne un noyau isotrope de $K(\mathcal{L})$ de la forme $K = K_1 \times K_2$, avec $K_i \subset K_i(\mathcal{L})$, et que le fibré $\mathcal{M}$ correspondant à la descente de $\mathcal{L}$ via le groupe de niveau $s_{\mathcal{L}}(K)$ soit très ample. Le fibré $\mathcal{L}$ est alors très ample, et si on se donne des structures de niveau sur $\mathcal{L}$ et $\mathcal{M}$, on peut considérer leurs thêta null points $(\vartheta_i^{\mathcal{L}}(0))_{i \in K_1(\mathcal{L})}$ et $(\vartheta_i^{\mathcal{M}}(0))_{i \in K_1(\mathcal{M})}$. Alors ces structures de niveau sont f-compatibles, où f est l'isogénie $f : X \to X/K$, si et seulement s'il existe $\lambda \in k^*$ tel que pour tout $i \in K_1(\mathcal{M})$ on ait

$$f^*\vartheta_i^{\Theta_{\mathcal{M}}}(0) = \lambda \sum_{j \in f^{-1}(i)} \vartheta_j^{\Theta_{\mathcal{L}}}(0).$$

1. Si $\delta_0 = (d_1, \ldots, d_g)$, on n'a pas forcément $d_i \mid d_{i+1}$, c'est-à-dire que l'on n'a pas forcément pris la décompo-

En effet, si on prend l'unique structure de niveau sur $G(\mathcal{M})$ qui soit f-compatible avec celle de $G(\mathcal{L})$, c'est certainement le cas par le théorème 3.6.4. La réciproque vient du fait que le thêta null point d'un fibré très ample détermine entièrement sa structure de niveau (voir la section 3.4). ◇

Le théorème de l'isogénie est intéressant dans la mesure où il permet d'exhiber des formules explicites pour des isogénies, en revanche on descend de niveau quand on l'utilise. Donc si on veut calculer une isogénie avec un noyau de grand degré, il faut partir d'une thêta structure de grand niveau, et en outre on ne peut pas composer d'isogénies avec cette méthode. Il nous faut un algorithme qui calcule des isogénies en « montant de niveau », qui fait l'objet du chapitre 7.

3.7 STRUCTURE THÊTA RATIONNELLE

Soit k un corps et X_k une variété abélienne sur k. Dans la suite on suppose k parfait et on note $\overline{k}$ une clôture algébrique de k, de sorte qu'un sous schéma réduit Y_k de X_k est entièrement déterminé par ses $\overline{k}$-points[1]. On note $X_{\overline{k}}$ la variété déduite de X_k via le changement de base $\operatorname{Spec}\overline{k} \to \operatorname{Spec} k$, et si $\mathcal{L}$ est un fibré sur X_k, on note $\mathcal{L}_{\overline{k}}$ le fibré $\mathcal{L} \otimes_k \overline{k}$ induit sur $X_{\overline{k}}$.

En général on note souvent $\mathcal{L}_{\overline{k}}$ comme $\mathcal{L}$, quand le contexte est clair.

Si $f : X_k \to Y_k$ est une isogénie séparable, comme son noyau est réduit, on identifie le schéma en groupes $\operatorname{Ker} f$ avec l'ensemble de ses points géométriques. Ainsi la notation $x \in \operatorname{Ker} f$ signifie que x est un point géométrique de $\operatorname{Ker} f$. Si $\mathcal{L}$ est un fibré séparable sur X_k, il induit une isogénie séparable $X_k \xrightarrow{\Phi(\mathcal{L})} \widehat{X}_k$ de noyau $K(\mathcal{L})$. Le groupe thêta $G(\mathcal{L})$ est un schéma en groupes plat et de type fini sur k dont les points géométriques sont donnés par les isomorphismes $t_x^*\mathcal{L}_{\overline{k}} \xrightarrow{\phi} \mathcal{L}_{\overline{k}}$. On a donc $G(\mathcal{L})(\overline{k}) = G(\mathcal{L}_{\overline{k}})$ avec la définition précédente du groupe thêta lorsqu'on travaille sur un corps algébriquement clos.

Si $\mathbb{G}_{m,k}$ représente le schéma en groupes[2] multiplicatif de k, on a une suite exacte

$$0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0$$

et donc $G(\mathcal{L})$ est une extension centrale de $K(\mathcal{L})$. On peut définir le schéma en groupes fini sur k de type δ comme étant $K(\delta)_k = Z(\delta)_k \times_k \hat{Z}(\delta)_k$ où cette fois $Z(\delta)_k = (\mathbb{Z}/\delta_1\mathbb{Z})_k \times_k \cdots \times_k (\mathbb{Z}/\delta_g\mathbb{Z})_k$ ($(\mathbb{Z}/\delta_i\mathbb{Z})_k$ étant vu comme un schéma en groupes constant sur k) et $\hat{Z}(\delta)_k$ est le dual de Cartier de $Z(\delta)_k$. Le schéma en groupes de Heisenberg est $\mathcal{H}(\delta)_k = \mathbb{G}_{m,k} \times K(\delta)$ muni de la loi de groupe

$$(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha\beta y_2(x_1), x_1 + y_1, x_2 + y_2)$$

sur les points géométriques. Le schéma en groupes $\hat{Z}(\delta)_k$ est isomorphe à $\mu_k(\delta_1) \times_k \cdots \times_k \mu_k(\delta_g)$, où $\mu_k(\delta_i)$ est le schéma en groupe des racines δ_i-ièmes de l'unité. La dualité entre $Z(\delta)_k$ et $\hat{Z}(\delta)_k$ s'écrit, si $\zeta = (\zeta_1, \ldots, \zeta_g) \in \hat{Z}(\delta)_k(\overline{k})$ et $x = (x_1, \ldots, x_k) \in Z(\delta)_k(\overline{k})$, par

$$\langle x, \zeta \rangle = \prod_{i=1}^{g} \zeta_i^{x_i}.$$

Les points géométriques de $Z(\delta)_k$ sont rationnels, et si k contient les racines d-ièmes de l'unité, avec $d = \vee_{i=1}^{g} \delta_i$, c'est également le cas pour $\hat{Z}(\delta)_k$. Pour alléger les notations, comme ces

sition canonique de $Z(\delta_0)$, et théoriquement il faudrait composer σ avec l'isomorphisme sur sa décomposition canonique. Comme σ ne sert qu'à numéroter les fonctions thêta, il est bien plus simple de le garder tel quel.

1. On appelle un $\overline{k}$-point un point géométrique
2. On peut consulter [DG70] pour une approche fonctorielle des schémas en groupe.

schémas en groupes sont plats, de type finis, et réduits sur k, on les identifie à l'ensemble de leurs points géométriques, et on note $\mathcal{H}(\delta) = \mathcal{H}(\delta)_k(\overline{k})$, $Z(\delta) = Z(\delta)_k(\overline{k})$ et $\hat{Z}(\delta) = \hat{Z}(\delta)_k(\overline{k})$.

Une thêta structure $\Theta_{\mathcal{L}}$ est alors un isomorphisme d'extensions centrales $\Theta_{\mathcal{L}} : \mathcal{H}(\delta) \xrightarrow{\sim} G(\mathcal{L})$. Elle induit un isomorphisme $\overline{\Theta}_{\mathcal{L}} : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ donné par le diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & H(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \Theta_{\mathcal{L}}} & & \downarrow{\scriptstyle \overline{\Theta}_{\mathcal{L}}} & & \\ 1 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0. \end{array}$$

La décomposition de $K(\delta)$ induit via $\overline{\Theta}_{\mathcal{L}}$ une décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ où $K_2(\mathcal{L})$ est le dual de Cartier de $K_1(\mathcal{L})$. Tous les points géométriques de $K_1(\mathcal{L})$ sont rationnels, mais ce n'est pas forcément le cas des points géométriques de $K_2(\mathcal{L})$ (suivant que k contienne ou non les racines d-ième de l'unité). En revanche, $K_2(\mathcal{L})$ est un sous-groupe rationnel, et de plus si $\delta' \mid \delta$, alors le sous-groupe $K_2(\mathcal{L})[\delta'] \coloneqq \overline{\Theta}_{\mathcal{L}}(\hat{Z}(\delta'))$ est également rationnel car isomorphe à $\oplus_{i=1}^{g} \mu_k(\delta_i')$. Inversement, si on se donne une décomposition rationnelle $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$, alors par la proposition 3.3.1, il est équivalent de se donner un isomorphisme symplectique rationnel $K(\delta) \to K(\mathcal{L})$ et de se donner un isomorphisme rationnel de $K_1(\delta) \to K_1(\mathcal{L})$ ou bien de $K_2(\delta) \to K_2(\mathcal{L})$. En effet, si par exemple $\sigma_1 : K_1(\delta) \to K_1(\mathcal{L})$ est un isomorphisme rationnel, soit $\zeta \in \overline{k}$ une racine primitive d-ième de l'unité. Alors on définit $\sigma_2 : K_2(\delta) \to K_2(\mathcal{L})$ sur les points géométriques par, si $j \in K_2(\delta)(\overline{k})$ est le dual de $i \in K_1(\delta)(\overline{k})$ par rapport à ζ, $\sigma_2(j)$ est l'unique dual de $\sigma_1(i)$ dans $K_2(\mathcal{L})$ (on vérifie immédiatement que σ_2 ne dépend pas du choix de ζ). Si $g \in \mathrm{Gal}(\overline{k}/k)$, on a si $x, y \in K(\mathcal{L})(\overline{k})$, $e_{\mathcal{L}}(g.x, g.y) = g.e_{\mathcal{L}}(x, y)$, ce qui montre que σ_2 est rationnel si σ_1 l'est.

Comme dans le cas algébriquement clos, on peut voir une thêta structure comme la donnée d'un isomorphisme symplectique rationnel entre $K(\delta)$ et $K(\mathcal{L})$ (où la forme symplectique sur les points géométriques de $K(\mathcal{L})$ est simplement le commutator pairing), et de deux sections (de schémas en groupes) rationnelles $s_{K_1(\mathcal{L})} : K_1(\mathcal{L}) \to G(\mathcal{L})$ et $s_{K_2(\mathcal{L})} : K_2(\mathcal{L}) \to G(\mathcal{L})$ de la projection canonique $\rho_{G(\mathcal{L})} : G(\mathcal{L}) \to K(\mathcal{L})$. On a vu qu'une section définie sur $\overline{k}$, $s_{K_1(\mathcal{L})} : K_1(\mathcal{L}) \to G(\mathcal{L}_{\overline{k}})$ était équivalente à la donnée d'un fibré $\mathcal{M}_{\overline{k}}$ sur $X_{\overline{k}}/K_1(\mathcal{L})$. Par la théorie de la descente, cette section provient d'une section rationnelle si et seulement si $\mathcal{M}_{\overline{k}}$ descend en un fibré rationnel $\mathcal{M}$ sur $X_k/K_1(\mathcal{L})$.

Ainsi, même si tous les points géométriques de $K(\mathcal{L})$ sont rationnels, pour avoir une thêta structure rationnelle il faut de plus avoir des sections rationnelles $K_i(\mathcal{L}) \to G(\mathcal{L}_{\overline{k}})$ $(i = 1, 2)$, ce qui peut imposer de prendre une extension (finie) de k. Si on revient à la preuve de la proposition 3.2.6, si $x \in K_i(\mathcal{L})$ est d'ordre ℓ et $\widetilde{x} \in G(\mathcal{L})$ correspond à un isomorphisme rationnel $\mathcal{L} \to t_x^*\mathcal{L}$, alors $\widetilde{x}^\ell \in \mathbb{G}_{m,k}(k)$. Si de plus $\widetilde{x}^\ell = \alpha^\ell$ où $\alpha \in \mathbb{G}_{m,k}(k)$, alors $\widetilde{x}/\alpha$ est un relevé de x d'ordre ℓ. Ainsi le degré de l'extension de k que l'on doit prendre pour avoir des sections rationnelles dépend de la structure galoisienne de k. Par exemple, si k est fini, alors il suffit de prendre une extension de degré d. (Si tous les points géométriques de $K(\mathcal{L})$ sont rationnels, le commutator pairing $e_{\mathcal{L}}$ sur $K(\mathcal{L})$ impose alors que k contienne les racines d-ièmes de l'unité.)

Si $\mathcal{L}$ est très ample sur X_k, la thêta structure $\Theta_{\mathcal{L}}$ induit une thêta structure sur $G(\mathcal{L}_{\overline{k}})$, et on peut lui associer la base de fonctions $(\vartheta_i)_{i \in Z(\delta)}$ correspondante. La construction de la section 3.4 montre, par les remarques précédentes, que les fonctions ϑ_i sont rationnelles. En particulier, le thêta null point associé est un point projectif rationnel. Réciproquement, si k contient les racines d-ièmes de l'unité, supposons donnée une thêta structure sur $G(\mathcal{L}_{\overline{k}})$ telle

que le thêta null point associé soit rationnel. Par l'hypothèse sur k, l'équation (3.9) montre que tous les points géométriques de $K(\mathcal{L})$ sont rationnels, et donc le morphisme $\overline{\Theta}_{\mathcal{L}_{\overline{k}}}$ déduit est rationnel. On a vu dans la section 3.4 que le thêta null point détermine la section $s_{K(\mathcal{L}_{\overline{k}})}$; en revenant à la construction on voit que cette section est rationnelle, et donc la thêta structure sur $G(\mathcal{L}_{\overline{k}})$ provient d'une thêta structure rationnelle sur $G(\mathcal{L})$.

De manière plus générale, si k est parfait, soit $g \in \mathrm{Gal}(\overline{k}/k)$ un élément du groupe de Galois absolu, et soit $\Theta_{\mathcal{L}_{\overline{k}}}$ une thêta structure sur $G(\mathcal{L}_{\overline{k}})$. Alors l'action de g sur $\Theta_{\mathcal{L}_{\overline{k}}}$ induit l'action par conjugaison de g sur les sous-groupes de niveau $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$. Soit $(\vartheta'_i)_{i\in Z(\delta)}$ la base de fonctions thêta induite par la thêta structure $g.\Theta_{\mathcal{L}_{\overline{k}}}$. Par ce qui précède, $\vartheta'_0 = \lambda g.\vartheta_0$, et on peut supposer $\lambda = 1$. On a alors, si $i \in Z(\delta)$ et $\widetilde{i}$ est l'élément de $K_1(\mathcal{L})$ au-dessus de $\overline{\Theta}_{\mathcal{L}_{\overline{k}}}(i)$: $\vartheta'_i = (g.\widetilde{i})\vartheta'_0 = g.(\widetilde{i}.\vartheta_0) = g.\vartheta_i$. En particulier, si $0'_X$ est le thêta null point associé à $\Theta_{\mathcal{L}_{\overline{k}}}$, on a $0'_X = g.0_X$. Comme le thêta null point détermine la thêta structure, on en déduit que $\Theta_{\mathcal{L}_{\overline{k}}}$ descend en une thêta structure rationnelle si et seulement si le thêta null point associé est rationnel.

4 FORMULES D'ADDITION

MATIÈRES

4.1 INTRODUCTION

Le but de ce chapitre est d'étudier les relations d'addition sur une variété abélienne qui découlent des relations de RIEMANN. Comme l'a montré MUMFORD dans [Mum66, Section 3], on peut retrouver les relations de RIEMANN en étudiant, si X est une variété abélienne, l'isogénie

$$\begin{array}{rccc} \xi\colon & X \times X & \longrightarrow & X \times X \\ & (x, y) & \longmapsto & (x + y, x - y) \end{array} .$$

Comme l'isogénie ξ n'est pas séparable en caractéristique 2, on fera ultérieurement l'hypothèse que l'on n'est pas dans ce cas.

MUMFORD utilise ensuite ces relations pour étudier les syzygies de l'anneau des sections homogènes d'un fibré ample $\mathcal{L}$ sur X [Mum66, Section 4] et pour construire l'espace modulaire des variétés abéliennes marquées par une thêta structure (totalement symétrique, cette notion étant définie ultérieurement) dans [Mum67a, Section 6].

Lorsqu'on étudie des isogénies, le concept de thêta structure introduit au chapitre 3 a l'avantage considérable qu'il permet de garder trace des facteurs projectifs. (Par exemple on a discuté longuement dans la section 2.6 de l'avantage d'avoir une action affine de $G(\mathcal{L})$ sur $\Gamma(X, \mathcal{L})$ par rapport à l'action projective de $K(\mathcal{L})$.) Cette idée va se révéler cruciale pour l'étude des formules d'addition. Par exemple, si $X = V/\Lambda$ est une variété abélienne complexe, et que l'on regarde les fonctions thêta comme des fonctions rationnelles sur V plutôt que sur X, les formules d'additions vont relier les valeurs des fonctions thêta sur les points $\{v + w, v - w, v, w, 0\}$ de V. Autrement dit, les formules d'addition permettent de « retrouver » l'addition sur V, pas seulement sur X. Si X est une variété abélienne définie sur un corps algébriquement clos quelconque, on aimerait pouvoir étendre les formules d'addition sur X en des formules « affines ». Pour cela la stratégie habituelle est de choisir une trivialisation du fibré ample $\mathcal{L}$ en 0, ce qui permet en transportant cette trivialisation par la thêta structure $\Theta_{\mathcal{L}}$ d'évaluer les fonctions thêta sur les points géométriques de $K(\mathcal{L})$ (voir la section 3.4). C'est la stratégie utilisée par MUMFORD dans [Mum67a ; Mum67b] lorsqu'il étudie les tours de 2-isogénies sur les variétés abéliennes. Cependant, on a besoin d'évaluer les fonctions thêta en tous les points géométriques de X, donc de fixer une trivialisation en tout point géométrique, de manière compatible avec la thêta structure. Pour cela, si $V = \Gamma(X, \mathcal{L})$, on considère le cône

affine $\widetilde{X}$ de la variété abélienne $X \hookrightarrow \mathrm{Proj}(V)$ dans $\mathrm{Spec}(V)$. Comme les formules d'addition viennent de l'isogénie ξ, et en particulier des relations des fonctions thêta induites par ξ via le théorème de l'isogénie, les formules d'addition pourront être transposées au cône affine $\widetilde{X}$. (Le point crucial étant que le facteur multiplicatif λ qui apparaît dans le théorème de l'isogénie ne dépend pas du point géométrique où on évalue les coordonnées (projectives) thêta, or quitte à renormaliser, ces mêmes coordonnées donnent les coordonnées (affines) sur $\widetilde{X}$). Dans ce cadre, prendre des trivialisations du fibré $\mathcal{L}$ en des points géométriques de X de manière compatible avec la thêta structure s'interprète comme le fait de prendre des sections des points géométriques de X (sous la projection canonique $\widetilde{X}\backslash(0,\dots,0) \to X$) compatibles avec l'action du groupe thêta $G(\mathcal{L})$ sur $\widetilde{X}$.

Toutes les applications que l'on verra dans la seconde partie découlent d'une manière ou d'une autre de ces formules d'addition, ce qui explique la place centrale de ce chapitre.

Avant de commencer à étudier les formules d'addition, on étudie l'isogénie $x \to -x$ dans la section 4.2. On verra dans cette section la notion de thêta structure symétrique (étudiée par Mumford dans [Mum66, Section 2]), qui permet d'assurer la compatibilité des thêta structures avec l'isogénie ξ. Dans la section 4.3, on introduit les formules d'addition générales, qui sont une généralisation des formules d'addition classiques issues des formules de doublement. Ces formules ont été découvertes par Koizumi dans [Koi76], qui en a donné une preuve analytique, et retranscrites dans le cadre algébrique de la théorie de Mumford par Kempf dans [Kem89]. Dans cette section, on donne la preuve algébrique de Kempf, mais comme on se restreint à des fibrés totalement symétriques, on peut considérablement la simplifier. Les formules d'addition classiques (issues des formules d'addition générales en spécialisant à l'isogénie ξ) sur la variété abélienne X et son cône affine sont étudiées dans la section 4.4. On verra que ces formules permettent de définir une notion de pseudo addition (ou d'addition différentielle) sur le cône affine $\widetilde{X}$. On étudie les propriétés de cette pseudo-addition dans la section 4.5. Une première application des sections 4.4 et 4.5 est donnée dans la section 4.6 où l'on donne une méthode de compression des coordonnées, qui permet de manipuler plus efficacement les coordonnées thêta de grand niveau. On retourne à des résultats connus dans la section 4.7 où l'on rappelle la construction de l'espace modulaire des variétés abéliennes marquées de niveau δ (c'est-à-dire des variétés abéliennes polarisées $(X, \mathcal{L})$ munies d'une thêta structure symétrique de niveau δ sur le fibré totalement symétrique $\mathcal{L}$) donnée par Mumford dans [Mum67a, Section 6]. Comme dans le chapitre 3, on supposere dans ce chapitre que l'on travaille sur des variétés abéliennes sur un corps k algébriquement clos. Dans la section 4.7 on explique comment généraliser les résultats au cas d'un corps k parfait quelconque (de caractéristique différente de 2) : voir la proposition 4.7.6. Enfin, on a vu dans l'introduction que pour atteindre une performance optimale, il fallait travailler avec des fonctions thêta de niveau 2. Or de telles fonction thêta ne définissent plus un plongement de la variété abélienne, mais seulement de la variété de Kummer associée. Il nous faut donc adapter les formules d'addition de la section 4.4 à ce cas, ce qui fait l'objet de la section 4.8. Dans [Gau07], Gaudry a montré que les formules d'addition en niveau 2 et genre 2 donnaient l'algorithme le plus efficace pour calculer la multiplication sur les surfaces de Kummer. (Ces résultats furent ensuite étendu au cas de la caractéristique 2, ainsi qu'au genre 1 dans [GL09]). On en profite pour généraliser cet algorithme au cas du genre quelconque et du niveau quelconque, et on pourra trouver une comparaison avec l'algorithme usuel de Cantor dans l'exemple 4.8.9.

4.2 FIBRÉS SYMÉTRIQUES

Lorsqu'on étudie le groupe thêta d'un fibré ample $\mathcal{L}$ sur X via une thêta structure, on peut faire plusieurs choix : on peut remplacer $\mathcal{L}$ par un fibré équivalent, on peut changer la

numérotation de $K(\mathcal{L})$ donnée par $K(\delta)$, on peut changer la structure de niveau de $G(\mathcal{L})$, etc. Si on suppose que le niveau δ de $\mathcal{L}$ est pair, on va montrer dans cette section que l'on peut rigidifier ces choix en prenant pour $\mathcal{L}$ l'unique fibré totalement symétrique dans sa classe d'équivalence, et en prenant pour structure de niveau de $G(\mathcal{L})$ l'unique structure symétrique induite par une numérotation donnée de $K(\mathcal{L}^2)$ par $K(2\delta)$ (voir la proposition 4.3.1). En rigidifiant les choses ainsi, on obtient des thêta structures compatibles avec l'inverse $x \mapsto -x$ ou la duplication $x \mapsto 2x$. Plus généralement, on obtiendra dans la section 4.3 des formules d'addition générales, que l'on appliquera essentiellement à l'isogénie $X \times X \to X \times X$ donnée sur les points géométriques par $(x, y) \mapsto (x + y, x - y)$.

Si $\mathcal{L}$ est un fibré en droites sur X, on dit que $\mathcal{L}$ est symétrique si $[-1]^*\mathcal{L} \simeq \mathcal{L}$, et antisymétrique si $[-1]^*\mathcal{L} \simeq \mathcal{L}^{-1}$. Si $\mathcal{L}$ est un fibré quelconque, $\mathcal{L} \otimes [-1]^*\mathcal{L}$ est symétrique, tandis que $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}$ est antisymétrique. Mais il est facile de voir que $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1} \in \mathrm{Pic}_0(X)$ et que tout élément de $\mathrm{Pic}_0(X)$ est antisymétrique [Mum70, p. 75]. Autrement dit, $\mathcal{L}$ est équivalent à $[-1]^*\mathcal{L}$, comme on l'a déjà constaté dans la section 2.4 pour le cas complexe.

> En fait, on peut montrer que tout fibré antisymétrique est dans $\mathrm{Pic}_0(X)$: si $\mathcal{L}$ est antisymétrique, $\mathcal{L}^2 \in \mathrm{Pic}_0(X)$ par ce qui précède, et on peut montrer que ceci impose $\mathcal{L} \in \mathrm{Pic}_0(X)$. En effet s'il existe $n \in \mathbb{N}$ tel que $\mathcal{L}^n \in \mathrm{Pic}_0(X)$, comme $\mathrm{Pic}_0(X)$ est un groupe divisible étant donné qu'il correspond aux points géométriques d'une variété abélienne, il existe $\mathcal{L}_0 \in \mathrm{Pic}_0(X)$ tel que $\mathcal{L}_0^n = \mathcal{L}^n$. Mais alors $(\mathcal{L} \otimes \mathcal{L}_0^{-1})^n$ est trivial, on est donc ramené à montrer qu'un fibré en droite « de torsion » est dans $\mathrm{Pic}_0(X)$. Or si $\mathcal{L}$ est tel que $\mathcal{L}^n$ soit trivial, alors pour tout point géométrique x de X, $0 = \Phi_{\mathcal{L}^n}(x) = n\Phi_{\mathcal{L}}(x) = \Phi_{\mathcal{L}}(nx)$. Comme X est divisible, on a $\Phi_{\mathcal{L}} = 0$ et donc $\mathcal{L} \in \mathrm{Pic}_0(X)$ par définition.

Soit X une variété abélienne sur un corps algébriquement clos k et $\mathcal{L}$ un fibré en droites ample sur X. Comme $[-1]^*\mathcal{L}$ est équivalent à $\mathcal{L}$, par le même raisonnement que dans la section 2.4, on voit qu'il existe un fibré symétrique dans la classe d'équivalence de $\mathcal{L}$. On peut obtenir tous les autres fibrés symétriques dans cette classe ainsi : si $\mathcal{L}_0$ est un fibré de $\mathrm{Pic}_0(X)$ représenté par un point $x \in \widehat{X}$, le fibré $[-1]^*\mathcal{L}_0$ est représenté par le point $-x$. Ainsi les fibrés symétriques dans $\mathrm{Pic}_0(X)$ sont représentés par les points de 2-torsion $\widehat{X}[2]$. Maintenant, si $\mathcal{L}$ est un fibré en droites symétrique et ample sur X, l'ensemble des fibrés symétriques dans la même classe que $\mathcal{L}$ est donné par $\mathcal{L}_0 \mapsto \mathcal{L} \otimes \mathcal{L}_0$ où $\mathcal{L}_0$ parcourt les fibrés représentés par $\widehat{X}[2]$. Via la polarisation $\phi_{\mathcal{L}} : X \to \widehat{X}$, cette action revient à l'action par translation par un point de $[2]^{-1}K(\mathcal{L})/K(\mathcal{L})$ décrite à la section 2.4. Il existe donc 2^{2g} fibrés symétriques dans la classe d'équivalence de $\mathcal{L}$. Si $2 \mid \delta$, on va voir qu'on peut distinguer un fibré symétrique particulier.

Soit $\mathcal{L}$ un fibré symétrique sur X, il existe donc un isomorphisme $\phi : \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$. Si $x \in X$ est un point fermé, ϕ se restreint en un isomorphisme

$$\phi(x) : \mathcal{L}(x) \xrightarrow{\sim} [-1]^*\mathcal{L}(x) = \mathcal{L}(-x).$$

On dit que ϕ est l'isomorphisme normalisé lorsque $\phi(0) : \mathcal{L}(0) \xrightarrow{\sim} \mathcal{L}(0)$ est l'identité. Dans ce cas, la composée $\mathcal{L} \xrightarrow{\phi} [-1]^*\mathcal{L} \xrightarrow{[-1]^*\mathcal{L}} [-1]^*[-1]^*\mathcal{L} = \mathcal{L}$ est l'identité.

Définition 4.2.1. Soit $\mathcal{L}$ un fibré symétrique et $\phi : \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ l'isomorphisme normalisé. Si $x \in X[2]$ est un point de 2-torsion, on a un isomorphisme $\phi(x) : \mathcal{L}(x) \xrightarrow{\sim} [-1]^*\mathcal{L}(-x) = \mathcal{L}(x)$. On définit alors $e_*^{\mathcal{L}}(x)$ comme le scalaire qui donne (par multiplication) cet isomorphisme

$$\phi(x) : \mathcal{L}(x) \xrightarrow{e_*^{\mathcal{L}}(x)} \mathcal{L}(x).$$

◇

PROPOSITION 4.2.2. *L'application $e_*^{\mathcal{L}} : X[2] \to k^*$ est à valeurs dans $\{\pm 1\}$. De plus, on a les propriétés suivantes :*

- *$e_*^{\mathcal{L}\otimes\mathcal{M}} = e_*^{\mathcal{L}} \times e_*^{\mathcal{M}}$ si $\mathcal{L}$ et $\mathcal{M}$ sont des fibrés symétriques sur X.*
- *Si $f : X \to Y$ est un morphisme, et $\mathcal{L}$ un fibré symétrique sur Y, alors pour tout $x \in X[2]$ $e_*^{f^*\mathcal{L}}(x) = e_*^{\mathcal{L}}(f(x))$.*
- *Si $\mathcal{L}$ est un fibré symétrique dans $\mathrm{Pic}_0(X)$ qui correspond à $y \in \widehat{X}[2]$, on a $e_*^{\mathcal{L}}(x) = e_2(x, y)$ où e_2 est le pairing de Weil sur $X[2] \times \widehat{X}[2]$.*
- *La forme $e_*^{\mathcal{L}}$ est la forme quadratique associée à la forme bilinéaire $e_{\mathcal{L}^2}$ sur $X[2] \times X[2]$.*

DÉMONSTRATION : Les deux premiers points sont évidents. On peut montrer le troisième point en interprétant le pairing de Weil comme donné par le diagramme (5.1) (voir la section 5.2). Pour plus de détails voir [Mum66, p. 304-305]. Enfin le dernier point est montré dans [Mum66, p. 315] ; on peut aussi trouver une preuve analytique dans [BL04, Exercices 4.12 et 4.13]. ■

DÉFINITION 4.2.3. Un fibré symétrique $\mathcal{L}$ sur X est dit totalement symétrique si l'application $e_*^{\mathcal{L}}(x) = 1$ pour tout point $x \in X[2]$. ◇

On peut montrer qu'un fibré $\mathcal{L}$ est totalement symétrique si et seulement s'il descend en un fibré $\mathcal{M}$ sur la variété de Kummer $K_X := X/\pm 1$ associée à X [Mum66, Proposition 1].

PROPOSITION 4.2.4. *Si $\mathcal{L}$ est un fibré ample sur X de type δ, avec $2 \mid \delta$, il existe un unique fibré totalement symétrique dans la classe de $\mathcal{L}$.*

De plus, un fibré $\mathcal{L}$ est totalement symétrique si et seulement s'il est égal au carré d'un fibré symétrique.

DÉMONSTRATION : Si $\mathcal{L}$ est un fibré totalement symétrique, les autres fibrés symétriques sont de la forme $\mathcal{L} \otimes \mathcal{L}_0$ où $\mathcal{L}_0$ est représenté par un point $y \in \widehat{X}[2]$, mais la proposition 4.2.2 montre qu'un tel fibré n'est pas totalement symétrique si $y \neq 0$ car le pairing de Weil e_2 est non dégénéré.

Réciproquement, si $\mathcal{L}$ est un fibré de type δ avec $2 \mid \delta$, le corollaire 3.2.3 montre qu'il existe un fibré $\mathcal{M}$ tel que $\mathcal{L} = \mathcal{M}^2$. Le fibré $\mathcal{M} \otimes [-1]^*\mathcal{M}$ est alors totalement symétrique et est dans la même classe que $\mathcal{L}$.

Si $\mathcal{M}$ est un fibré symétrique, alors il est clair par la proposition 4.2.2 que $\mathcal{M}^2$ est un fibré totalement symétrique. Inversement, si $\mathcal{L}$ est totalement symétrique, la forme $e_{\mathcal{L}^2}$ est triviale sur $X[2] \subset K(\mathcal{L}^2)$ par la proposition 4.2.2. Comme $e_{\mathcal{L}^2}$ est une forme non dégénérée sur $K(\mathcal{L}^2)$, cela impose que $X[4] \subset K(\mathcal{L}^2)$. On a alors $X[2] \subset K(\mathcal{L})$ par le corollaire 3.2.3 et donc $\mathcal{L}$ est le carré d'un fibré $\mathcal{M}$. Si $\mathcal{M}_0$ est un fibré symétrique dans la classe de $\mathcal{M}$, $\mathcal{M}_0^2$ est un fibré totalement symétrique dans la classe de $\mathcal{L}$, par unicité on a $\mathcal{L} = \mathcal{M}_0^2$. ■

EXEMPLE 4.2.5. Lorsque $k = \mathbb{C}$, si $X = V/\Lambda$ est une variété abélienne complexe et $\mathcal{L}$ est un fibré symétrique, son semi-caractère χ est à valeurs dans $\{\pm 1\}$. Le semi-caractère associé à $\mathcal{L}^2$ est alors trivial sur Λ, donc trivial pour toute décomposition symplectique de Λ. Ainsi le fibré totalement symétrique $\mathcal{L}^2$ est de caractéristique 0 pour toute décomposition de Λ.

On vérifie aisément que si $x \in X[2]$ a pour représentant $v \in \frac{1}{2}\Lambda$, on a $e_*^{\mathcal{L}}(x) = \chi(2v)$ [BL04, Remarque 4.7.3]. ◇

DÉFINITION 4.2.6. Si $\mathcal{L}$ est un fibré symétrique et $\psi : \mathcal{L} \to [-1]^*\mathcal{L}$ l'isomorphisme normalisé ;

on note γ_{-1} l'application donnée par[1], si $(x, \phi) \in G(\mathcal{L})$,

$$\gamma_{-1}(x, \phi) = (-x, (t_{-x}^*\psi)^{-1} \circ ([-1]^*\phi) \circ \psi) : \tag{4.1}$$

$$\mathcal{L} \xrightarrow{\psi} [-1]^*\mathcal{L} \xrightarrow{[-1]^*\phi} [-1]^* t_x^*\mathcal{L} = t_{-x}^*[-1]^*\mathcal{L} \xrightarrow{(t_{-x}^*\psi)^{-1}} t_{-x}^*\mathcal{L}. \tag{4.2}$$

On a alors le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \gamma_{-1}} & & \downarrow{\scriptstyle [-1]} & & \\ 1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0. \end{array}$$

Enfin, un élément $g \in G(\mathcal{L})$ est dit symétrique si $\gamma_{-1}(g) = g^{-1}$. ◊

Remarque 4.2.7. La composée de deux éléments symétriques n'est pas forcément symétrique. Si $g_1, g_2 \in G(\mathcal{L})$ sont symétriques, alors $\gamma_{-1}(g_1g_2) = (\gamma_{-1}g_1)(\gamma_{-1}g_2) = g_1^{-1}g_2^{-1}$. Ainsi g_1g_2 est symétrique si et seulement si g_1 et g_2 commutent, c'est-à-dire s'ils sont au dessus de points $x_1, x_2 \in K(\mathcal{L})$ tels que $e_{\mathcal{L}}(x_1, x_2) = 1$.

De plus, si $g \in G(\mathcal{L})$ est symétrique, on a $\gamma_{-1}(g^{-1}) = (\gamma_{-1} \circ \gamma_{-1})(g) = g$, donc g^{-1} est symétrique. Ainsi, si $K \subset K(\mathcal{L})$ est un sous-groupe isotrope, les éléments symétriques au-dessus de K forment un sous-groupe de $G(\mathcal{L})$. ◊

Remarque 4.2.8. Soit $\mathcal{L}$ un fibré sur X, et $\widetilde{K}$ un groupe de niveau au-dessus d'un sous-groupe isotrope $K \subset K(\mathcal{L})$. Comme $\widetilde{K}$ est un groupe de niveau, il est abélien par la proposition 3.2.6. Comme $\widetilde{K}$ est un groupe, si $x \in K$ et $\phi \in \widetilde{K}$ est un morphisme au-dessus de x, pour tout $n \in \mathbb{Z}$, ϕ^n est l'unique élément de $\widetilde{K}$ au-dessus de nx. En particulier, s'il existe $n \in \mathbb{Z}$ tel que $x = ny$ avec y dans K, il existe $\psi \in \widetilde{K}$ tel que $\phi = \psi^n$.

De même, si $\phi, \psi \in \widetilde{K}$ sont des morphismes de $\mathcal{L}$ au-dessus de x et y dans K, alors $\phi \circ \psi$ est l'unique morphisme de $\mathcal{L}$ au-dessus de $x + y$ qui est dans $\widetilde{K}$. ◊

Si $\mathcal{L}$ est un fibré symétrique sur X, on a un morphisme de variétés abéliennes polarisées $(X, \mathcal{L}) \xrightarrow{[-1]} (X, \mathcal{L})$. Soit $\Theta_{\mathcal{L}}$ une thêta structure sur $G(\mathcal{L})$ et $\widetilde{K}_1(\mathcal{L}), \widetilde{K}_2(\mathcal{L})$ la structure de niveau sur $G(\mathcal{L})$ associée. Alors par définition, la thêta structure $\Theta_{\mathcal{L}}$ est $[-1]$-compatible avec elle-même si et seulement si pour tout $\phi \in \widetilde{K}_i(\mathcal{L})$, si ϕ est un automorphisme au-dessus de $x \in K_i(\mathcal{L})$, alors $\gamma_{-1}\phi$ est l'unique automorphisme au-dessus de $-x$ dans $\widetilde{K}_i(\mathcal{L})$ $(i = 1, 2)$. Mais par la remarque 4.2.8, l'unique automorphisme au-dessus de $-x$ dans $\widetilde{K}_i(\mathcal{L})$ est ϕ^{-1}. Autrement dit, $\Theta_{\mathcal{L}}$ est $[-1]$-compatible avec elle-même si et seulement si $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ sont formés d'éléments symétriques.

Si $\mathcal{L}$ est de niveau δ, on peut définir un automorphisme γ_{-1} sur $\mathcal{H}(\delta)$ par

$$\gamma_{-1}.(\alpha, x, y) = (\alpha, -x, -y).$$

Si $(\alpha, x, y) \in \mathcal{H}(\delta)$, on a

$$\gamma_{-1}.(\alpha, x, y) = \frac{\alpha^2}{\langle x, y\rangle}(\alpha, x, y)^{-1}.$$

Les éléments symétriques de $\mathcal{H}(\delta)$ sont donc de la forme $(\pm\langle x, y\rangle^{1/2}, x, y)$.

1. On vérifie facilement que δ_{-1} ne dépend pas du choix de l'isomorphisme $\mathcal{L} \to [-1]^*\mathcal{L}$

PROPOSITION 4.2.9. *Soit $\Theta_{\mathcal{L}}$ une thêta structure sur $\mathcal{L}$, un fibré symétrique de niveau δ. Les assertions suivantes sont équivalentes :*

i) Les sous-groupes de niveau $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ associés à $\Theta_{\mathcal{L}}$ sont symétriques[1].

ii) $\gamma_{-1} \circ \Theta_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \gamma_{-1}$.

iii) L'application induite par $\Theta_{\mathcal{L}}$, $\mathbb{Z}/2\mathbb{Z} \rtimes \mathcal{H}(\delta) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \rtimes G(\mathcal{L})$ où $1 \in \mathbb{Z}/2\mathbb{Z}$ agit par γ_{-1}, est un isomorphisme de groupe.

Si ces assertions sont satisfaites, on dit que $\Theta_{\mathcal{L}}$ est une thêta structure symétrique.

DÉMONSTRATION : L'équivalence entre les points ii) et iii) est immédiate par la propriété universelle du produit semi-direct. Si $\Theta_{\mathcal{L}}$ commute avec γ_{-1}, comme les groupes de niveau canoniques de $\mathcal{H}(\delta)$ sont symétriques, les groupes de niveau associés dans $G(\mathcal{L})$ sont symétriques. Inversement, comme k^* commute toujours avec γ_{-1}, si les groupes de niveau de $G(\mathcal{L})$ commutent avec γ_{-1}, puisqu'ils engendrent $G(\mathcal{L})$ avec k^*, la thêta structure $\Theta_{\mathcal{L}}$ commute avec γ_{-1}. ■

Si $\mathcal{L}$ est un fibré symétrique, il n'existe pas forcément de structure de niveau symétrique sur $G(\mathcal{L})$. Si $\phi \in G(\mathcal{L})$ est un morphisme au-dessus de x, $\gamma_{-1}\phi$ est un morphisme au-dessus de $-x$. On voit facilement qu'il existe exactement deux éléments symétriques dans $G(\mathcal{L})$ au-dessus de x (donnés par $\pm\phi_0$ si ϕ_0 est un élément symétrique au-dessus de x).

LEMME 4.2.10. *Si $\phi \in G(\mathcal{L})$ est un élément au-dessus d'un point x de $K(\mathcal{L})$ d'ordre 2, alors $\gamma_{-1}\phi = e_*^{\mathcal{L}}(x)\phi$.*

DÉMONSTRATION : Voir [Mum66, Proposition 3]. ■

REMARQUE 4.2.11. Ainsi si $\mathcal{L}$ est totalement symétrique, les éléments de $G(\mathcal{L})$ d'ordre 2 sont exactement les éléments symétriques au-dessus d'un point d'ordre 2 de X.

Plus généralement, toujours si $\mathcal{L}$ est totalement symétrique, soit $g \in G(\mathcal{L})$ un élément symétrique au-dessus d'un point x d'ordre n. Alors si $n = 2m$ est pair, g est d'ordre n. En effet, g^m est un élément symétrique (par la remarque 4.2.7), situé au-dessus du point mx d'ordre 2, donc l'élément g^m est d'ordre 2. (Si n est impair, $g^n = \pm 1$ étant donné que g^n est un élément symétrique au-dessus de 0_X, et donc soit g, soit $-g$ est d'ordre n). ◇

PROPOSITION 4.2.12. *Soit $\mathcal{L}$ un fibré symétrique de X, et K un sous-groupe isotrope de $K(\mathcal{L})$. Les conditions suivantes sont équivalentes :*

i) Il existe un groupe de niveau symétrique au-dessus de K.

ii) Pour tout point de 2-torsion $x \in K$, on a $e_*^{\mathcal{L}}(x) = 1$.

iii) Si $Y = X/K$ et $f : X \to Y$ est l'isogénie associée, il existe un fibré symétrique $\mathcal{M}$ sur Y tel que $f^*\mathcal{M} \simeq \mathcal{L}$.

En particulier, si $\mathcal{L}$ est totalement symétrique sur X, et qu'on a une décomposition symplectique $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$, alors il existe toujours une structure de niveau symétrique $s_{\mathcal{L}} : K(\mathcal{L}) \to G(\mathcal{L})$ dans $G(\mathcal{L})$ au-dessus de cette décomposition. Enfin les autres structures de niveau symétriques sont obtenues par l'action de $\mathtt{conj}_c$ sur $s_{\mathcal{L}}$ où c est un point de $X[2]$.

DÉMONSTRATION : Si $\widetilde{K}$ est un groupe de niveau au-dessus de K, et que $\mathcal{M}$ est le fibré sur Y qui lui correspond, alors $[-1]^*\mathcal{M}$ est la descente de $[-1]^*\mathcal{L}$ correspondant au groupe de

1. C'est-à-dire que $\gamma_{-1}(\widetilde{K}_i(\mathcal{L})) = \widetilde{K}_i(\mathcal{L})$ pour $i = 1, 2$.

niveau $\gamma_{-1}(\widetilde{K})$. Ainsi $\mathcal{M}$ est symétrique si et seulement si $\gamma_{-1}(\widetilde{K}) = \widetilde{K}$, c'est-à-dire si $\widetilde{K}$ est un groupe de niveau symétrique.

Maintenant, si $\mathfrak{K} = \rho_{G(\mathcal{L})}^{-1}(K)$, on note $\mathfrak{K}^s$ les éléments symétriques de $\mathfrak{K}$. K admet un groupe de niveau symétrique si et seulement si la suite exacte suivante est scindée :

$$0 \longrightarrow \{\pm 1\} \longrightarrow \mathfrak{K}^s \longrightarrow K \longrightarrow 0.$$

L'obstruction à l'existence d'une section vient des éléments d'ordre 2 dans K. Si z est un élément de $\mathfrak{K}^s$ au-dessus de $x \in K \bigcap X[2]$, alors par le lemme 4.2.10, on a $z^{-1} = \gamma_{-1} z = e_*^{\mathcal{L}}(x) z$. Si $e_*^{\mathcal{L}}(x) = 1$, tout élément de $\mathfrak{K}^s$ au-dessus de x est donc d'ordre 2, et il existe bien une section. (La réciproque est immédiate.)

Enfin, si $\widetilde{K}$ est un groupe de niveau symétrique au-dessus de K et qu'on le modifie par l'action d'un caractère χ sur K, l'image de $\widetilde{K}$ par cette action reste symétrique si et seulement si χ est à valeurs dans $\{\pm 1\}$. Si χ correspond à $e_{\mathcal{L}}(c, \cdot)$ avec $c \in K(\mathcal{L})$, cela impose que c soit d'ordre 2. ■

Exemple 4.2.13. Soit $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ une variété abélienne complexe, $\mathcal{L}$ un fibré sur X de niveau δ, et $c \in X$ une caractéristique pour $\mathcal{L}$. Cette caractéristique c définit alors une thêta structure $\Theta_{\mathcal{L}}$ pour $\mathcal{L}$ (voir l'exemple 3.2.4). Si on revient à la construction de $\Theta_{\mathcal{L}}$ donnée dans la section 2.6, on constate immédiatement que $\Theta_{\mathcal{L}}$ est symétrique si et seulement si $c \in X[2]$. En particulier, les fibrés équivalents à $\mathcal{L}$ admettant une thêta structure symétriques correspondent aux caractéristiques $c \in X[2]/(X[2] \bigcap K(\mathcal{L}))$, et si $\mathcal{L}$ est un tel fibré, les thêta structures symétriques sur $\mathcal{L}$ correspondent aux caractéristiques $c \in X[2] \bigcap K(\mathcal{L})$.

Si $K(\mathcal{L}) \supset X[2]$, on retrouve le fait que l'unique fibré dans la classe de $\mathcal{L}$ qui admet une thêta structure symétrique est le fibré totalement symétrique (de caractéristique 0). ◊

On a vu dans la section 3.5 que le groupe des automorphismes du groupe de Heisenberg était une extension :

$$0 \longrightarrow K(\delta) \longrightarrow \mathrm{Aut}(H(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 0.$$

On note $\mathrm{Aut}^0(\mathcal{H}(\delta))$ le groupe des automorphismes symétriques de $\mathcal{H}(\delta)$ (ce sont les automorphismes qui commutent à γ_{-1}). Si $\overline{\psi} \in \mathrm{Sp}(K(\delta))$, on vérifie immédiatement qu'il existe un élément ψ_0 de $\mathrm{Aut}(\mathcal{H}(\delta))$ symétrique au-dessus de $\overline{\psi}$. (Par exemple si ψ est un relevé de $\overline{\psi}$ correspondant à un semi-caractère χ comme dans la remarque 3.5.2, alors ψ est symétrique si et seulement si χ est à valeurs dans $\{\pm 1\}$.) Donc si $\psi \in \mathrm{Aut}^0(\mathcal{H}(\delta))$, $\psi \circ \overline{\psi}_0^{-1}$ est symétrique et provient d'un automorphisme de conjugaison $\mathtt{conj}_c$. La preuve de la proposition 4.2.12 montre alors que $c \in K(\delta)[2]$, on a donc montré que l'on avait une suite exacte :

$$0 \longrightarrow K(\delta)[2] \longrightarrow \mathrm{Aut}^0(H(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 0.$$

Le théorème de l'isogénie appliqué à $(X, \mathcal{L}) \xrightarrow{[-1]} (X, \mathcal{L})$ nous donne :

Proposition 4.2.14. *Soit $\mathcal{L}$ un fibré totalement symétrique de niveau δ, et $\Theta_{\mathcal{L}}$ une thêta structure symétrique sur $\mathcal{L}$. Soit $(\vartheta_i)_{i \in Z(\delta)}$ la base canonique[1] de $\Gamma(X, \mathcal{L})$. On a pour tout $i \in Z(\delta)$:*

$$[-1]^* \vartheta_i = \vartheta_{-i}.$$

1. Comme d'habitude, cette base n'est canonique qu'à l'action de k^* près.

DÉMONSTRATION : Comme la théta structure $\Theta_{\mathcal{L}}$ est symétrique, elle est $[-1]$-compatible avec elle-même et on peut appliquer le théorème de l'isogénie qui nous dit qu'il existe $\lambda \in k^*$ tel que $[-1]^*\vartheta_i = \lambda\vartheta_{-i}$ pour tout $i \in Z(\delta)$. Comme $[-1]^2 = 1$, on a $\lambda = \pm 1$. Si $\mathcal{L}$ est totalement symétrique on peut de plus montrer que $\lambda = 1$. Voir [Mum66, p. 331] pour le cas $\mathcal{L}$ très ample et [Kem89, Théorème 10] pour le cas général. ■

REMARQUE 4.2.15. Soit $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ une isogénie telle que $f^*\mathcal{M} \simeq \mathcal{L}$, où $\mathcal{M}$ est un fibré symétrique. Soit K le noyau de f, et $\widetilde{K}$ le groupe de niveau au-dessus de K associé. Si $\alpha_f : \mathcal{Z}(\widetilde{K}) \to G(\mathcal{M})$ est le morphisme canonique, α_f envoie un élément symétrique sur un élément symétrique.

En particulier, si $\Theta_{\mathcal{L}}$ est une structure de niveau symétrique sur $(X, \mathcal{L})$, une théta structure $\Theta_{\mathcal{M}}$ sur $\mathcal{M}$ compatible avec $\Theta_{\mathcal{L}}$ est forcément symétrique. On a vu dans la section 3.6 qu'on pouvait toujours trouver des théta structures compatibles sur $(X, \mathcal{L})$ et $(Y, \mathcal{M})$. On peut se demander si c'est toujours le cas quand on impose en plus aux théta structures d'être symétriques.

Supposons $\mathcal{M}$ totalement symétrique, et soit $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ une décomposition de $K(\mathcal{L})$ compatible avec K. Dans ce cas, on a un résultat plus fort : toute structure de niveau symétrique au-dessus de K est compatible avec $\widetilde{K}$.

En effet, si $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$ sont de tels groupes de niveau, par définition la théta structure $\Theta_{\mathcal{L}}$ est compatible avec $\widetilde{K}$ si $\alpha_f(\widetilde{K}_i(\mathcal{L}) \cap \mathfrak{K}) = \{1\}$ pour $i = 1, 2$, où $\mathfrak{K} = \rho_{G(\mathcal{L})}^{-1}(K)$. Mais comme $\widetilde{K}_i(\mathcal{L})$ est composée d'éléments symétriques, $\alpha_f(\widetilde{K}_i(\mathcal{L}) \cap \mathfrak{K}) = \{\pm 1\}$, on a donc au plus un problème de signe. Comme $\mathcal{M}$ est totalement symétrique, $Y[2] \subset K(\mathcal{M})$ par la proposition 4.2.4. Donc si $y \in \widetilde{K}_i(\mathcal{L}) \cap \mathfrak{K}$, il existe un élément $z \in \widetilde{K}_i(\mathcal{L})$ tel que $y = z^2$. L'élément $\alpha_f(z)$ est un élément symétrique au-dessus d'un point d'ordre 2 de Y, donc par le lemme 4.2.10, $\alpha_f(z)$ est d'ordre 2. On a bien $\alpha_f(y) = \alpha_f(z)^2 = 1$. ◇

4.3 FORMULES DE DUPLICATION ET D'ADDITION

À partir de maintenant on suppose que la caractéristique de k est impaire (ou nulle), l'isogénie de duplication est alors séparable. Soit $\mathcal{L}$ un fibré totalement symétrique sur X. On va étudier la situation $(X, [2]^*\mathcal{L}) \xrightarrow{[2]} (X, \mathcal{L})$. Comme $\mathcal{L}$ est symétrique, on a $[2]^*\mathcal{L} \simeq \mathcal{L}^4$. On peut appliquer la remarque 4.2.15 à cette situation pour obtenir :

PROPOSITION 4.3.1. *Soit $\mathcal{L}$ un fibré totalement symétrique sur X. Soit $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ une décomposition de $K(\mathcal{L})$, et $K(\mathcal{L}^4) = K_1(\mathcal{L}^4) \oplus K_2(\mathcal{L}^4)$ une décomposition de $K(\mathcal{L}^4)$ $[2]$-compatible avec celle de $K(\mathcal{L})$. Alors toute structure de niveau symétrique de $G(\mathcal{L}^4)$ au-dessus de la décomposition de $K(\mathcal{L}^4)$ descend en une structure de niveau symétrique sur $G(\mathcal{L})$. De plus, cette structure de niveau symétrique sur $G(\mathcal{L})$ ne dépend que de la décomposition de $[2]^{-1}(K(\mathcal{L}))$ induite par la décomposition de $K(\mathcal{L}^4)$.*

Ainsi une théta structure symétrique $\Theta_{\mathcal{L}}$ sur $G(\mathcal{L})$ revient à choisir un isomorphisme symplectique $\overline{\Theta}_{\mathcal{L}} : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ où δ est le niveau de $\mathcal{L}$, et une décomposition de $[2]^{-1}(K(\mathcal{L})) = K(\mathcal{L}^2)$ compatible avec la décomposition induite par $\overline{\Theta}_{\mathcal{L}}$.

DÉMONSTRATION : On a déjà vu dans la remarque 4.2.15 qu'une structure de niveau symétrique sur $G(\mathcal{L}^4)$ descend en une structure de niveau symétrique sur $G(\mathcal{L})$. De plus, $[2]^{-1}(K(\mathcal{L})) = 2K(\mathcal{L}^4)$. Ainsi si on change la structure de niveau sur $G(\mathcal{L}^4)$ via un caractère $\chi : K(\mathcal{L}^4) \to \{\pm 1\}$, sa restriction sur $[2]^{-1}(K(\mathcal{L}))$ reste inchangée. Donc la structure de

niveau symétrique sur $G(\mathcal{L})$ ne dépend pas du choix de structure de niveau symétrique sur $G(\mathcal{L}^4)$.

Enfin on peut montrer que toute structure de niveau symétrique sur $G(\mathcal{L})$ vient d'un choix de décomposition de $K(\mathcal{L}^2)$, voir [Mum66, Remarque 4 p. 319]. ■

On peut alors complètement rigidifier les structures de niveau sur tous les $G(\mathcal{L}^n)$ ainsi :

DÉFINITION 4.3.2. On appelle une ∞-décomposition[1] de $K(\mathcal{L})$ une décomposition $K(\mathcal{L}^n) = K_1(\mathcal{L}^n) \oplus K_2(\mathcal{L}^n)$ pour tout n premier à la caractéristique p de k de telle sorte que ces décompositions soient compatibles avec les isogénies $[m] : K(\mathcal{L}^{nm}) \to K(\mathcal{L}^n)$ (pour tout m premier à p). ◊

La proposition 4.3.1 montre qu'une ∞-décomposition détermine entièrement une structure de niveau symétrique sur chaque $G(\mathcal{L}^n)$ (n premier à p), de telle sorte que la structure de niveau sur $G(\mathcal{L}^{nm^2})$ est $[m]$-compatible avec celle sur $G(\mathcal{L}^n)$ par la remarque 4.2.15.

REMARQUE 4.3.3. On peut interpréter la remarque 4.2.15 et la proposition 4.3.1 de la façon suivante. Soit $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ une isogénie entre variétés abéliennes polarisées, et $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ une décomposition de $K(\mathcal{L})$ compatible avec le noyau K de f. Soit $\widetilde{K}$ le sous-groupe de niveau correspondant. Supposons que $\mathcal{M}$ soit symétrique, alors $\widetilde{K}$ l'est également par la proposition 4.2.12. On se donne une structure de niveau sur $G(\mathcal{L})$ symétrique compatible avec $\widetilde{K}$. Tout automorphisme symétrique de $G(\mathcal{L})$ fixant $K(\mathcal{L})$ est de la forme $\mathtt{conj}_c$ pour $c \in X[2]$. Si $[2]^{-1}(K) \subset K(\mathcal{L})$ (ce qui est le cas si $\mathcal{M}$ est totalement symétrique, car dans ce cas $Y[2] \subset K(\mathcal{M})$), alors $\mathtt{conj}_c$ laisse $\widetilde{K}$ invariant. Autrement dit, toute structure de niveau symétrique sur $G(\mathcal{L})$ est compatible avec $\widetilde{K}$. Si de plus $[2]^{-1}K^\perp \subset K(\mathcal{L})$ (ce qui est le cas de l'isogénie $[2] : (A_k, \mathcal{L}^4) \to (A_k, \mathcal{L})$), alors $\mathtt{conj}_c$ laisse $\mathcal{Z}(\widetilde{K})$ invariant, c'est-à-dire que toute structure de niveau symétrique sur $G(\mathcal{L})$ induit la même structure de niveau sur $G(\mathcal{M})$. ((Une autre manière de voir les choses est la suivante : l'automorphisme symétrique $\overline{c}$ pour $c \in X[2]$ laisse $\widetilde{K}$ invariant si et seulement si $c \in K^\perp$. Mais $[2]^{-1}(K) \subset K(\mathcal{L})$ équivaut à $X[2] \subset K^\perp$. De même, $[2]^{-1}K^\perp \subset K(\mathcal{L})$ si et seulement si $X[2] \subset K$, et dans ce cas les automorphismes symétriques $\overline{c}$ pour $c \in X[2]$ laissent $\mathcal{Z}(\widetilde{K})$ invariant.))

Et donc, si $\mathcal{M}$ est totalement symétrique, et que l'on considère une ∞-décomposition de $K(\mathcal{L})$ compatible avec K, alors chaque structure de niveau induite sur $G(\mathcal{L}^n)$ ($n \in \mathbb{N}$) est compatible avec le sous-groupe de niveau induit par la descente $f^*\mathcal{M} \simeq \mathcal{L}^n$. De plus, cette ∞-décomposition de $K(\mathcal{L})$ se projette en une ∞-décomposition de $K(\mathcal{M})$, ce qui induit donc une structure de niveau sur chaque $G(\mathcal{M}^n)$, f-compatible avec celle de $G(\mathcal{L}^n)$.

En particulier, la structure de niveau symétrique sur $G(\mathcal{L})$ vient de la décomposition symplectique $K(\mathcal{L}^2) = K_1(\mathcal{L}^2) \oplus K_2(\mathcal{L}^2)$ par la proposition 4.3.1. Comme par hypothèse le noyau K de f est compatible avec cette décomposition, c'est également le cas de $[2]^{-1}K^\perp = f^{-1}(K(\mathcal{M}^2))$ car $[2]^{-1}K^\perp$ est l'orthogonal de K pour $e_{\mathcal{L}^2}$, et donc en poussant la décomposition de $K(\mathcal{L}^2)$ par f, on obtient une décomposition de $K(\mathcal{M}^2)$. La structure de niveau symétrique de $G(\mathcal{M})$ induite par cette décomposition est compatible à celle de $G(\mathcal{L})$, et inversement, une décomposition de $K(\mathcal{M}^2)$ induit une structure de niveau symétrique sur $G(\mathcal{M})$ compatible avec celle de $G(\mathcal{L})$ si et seulement si $K_i(\mathcal{M}^2) = f(K_i(\mathcal{L}^2) \bigcap f^{-1}(K(\mathcal{M}^2)))$ pour $i = 1, 2$. Si $f^{-1}(K(\mathcal{M}^2)) \subset K(\mathcal{L})$, on retrouve le fait que toute les structures de niveau symétriques de $G(\mathcal{L})$ au-dessus de la décomposition de $K(\mathcal{L})$ descendent en la même structure de niveau sur $G(\mathcal{M})$.

1. Une telle ∞-décomposition est facile à construire, il suffit de considérer une décomposition sur chaque module de Tate $T_\ell(X)$, muni de sa forme de Weil par rapport à $\mathcal{L}$ pour chaque ℓ premier à p, et de prendre leur

EXEMPLE 4.3.4. Soit $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$, et $\mathcal{L}$ un fibré symétrique sur X. On suppose qu'il existe une thêta structure symétrique sur chaque $G(\mathcal{L}^n)$ ($n \in \mathbb{N}$), ces thêta structures étant de plus compatibles avec les isogénies de multiplication par $[m]$. Soit $c_n \in X$ la caractéristique correspondant à la thêta structure sur $G(\mathcal{L}^n)$. On a d'une part $c_n \in X[2]$ étant donné que la thêta structure est symétrique, et d'autre part, la compatibilité avec la duplication $[2]$ impose $2c_{4n} = c_n$ (voir la section 3.6). La condition est donc équivalente à $c_n = 0$ pour tout n.

Ceci explique pourquoi le choix d'une caractéristique détermine entièrement un fibré et sa thêta structure. Si $\mathcal{L}$ est le fibré de caractéristique 0, Ω détermine une ∞-décomposition pour $K(\mathcal{L})$, qui détermine uniquement $G(\mathcal{L})$ (et même les $G(\mathcal{L}^n)$). Changer de caractéristique revient à agir par conjugaison par c sur toutes ces données. ♢

Si on a des variétés abéliennes séparablement polarisées $(X_1, \mathcal{L}_1), \ldots, (X_r, \mathcal{L}_r)$, soit $X = X_1 \times \cdots \times X_r$ et $\pi_i : X \to X_i$ la projection quand $i \in \{1 \ldots r\}$. Soit $\mathcal{L} = \pi_1^*\mathcal{L}_1 \otimes \cdots \otimes \pi_r^*\mathcal{L}_r$, la polarisation $\Phi_{\mathcal{L}}$ associée à $\mathcal{L}$ est simplement

$$\begin{pmatrix} \Phi_{\mathcal{L}_1} & & 0 \\ & \ddots & \\ 0 & & \Phi_{\mathcal{L}_r} \end{pmatrix}$$

donc $K(\mathcal{L}) = K(\mathcal{L}_1) \oplus \ldots K(\mathcal{L}_r)$ est une décomposition orthogonale pour $e_{\mathcal{L}}$. Le groupe thêta $G(\mathcal{L})$ est isomorphe à $G(\mathcal{L}_1) \times \cdots \times G(\mathcal{L}_r)$ modulo $\{(\lambda_1, \ldots, \lambda_r) \in k^{*,r} \mid \prod \lambda_i = 1\}$, ainsi il est équivalent de se donner une thêta structure sur $G(\mathcal{L})$ ou sur chaque $G(\mathcal{L}_i)$. Finalement, si δ_i est le niveau de $\mathcal{L}_i$, $\mathcal{L}$ est de niveau $\prod \delta_i$, et si $i = (i_1, \ldots, i_r) \in Z(\delta_1) \times \cdots \times Z(\delta_r)$, la fonction thêta canonique $\vartheta_i^{\mathcal{L}}$ est $\vartheta_i^{\mathcal{L}} = \pi_1^*\vartheta_{i_1}^{\mathcal{L}_1} \otimes \cdots \otimes \pi_r^*\vartheta_{i_r}^{\mathcal{L}_r}$. Pour simplifier les notations, on note également $\vartheta_{i_1}^{\mathcal{L}_1} \star \cdots \star \vartheta_{i_r}^{\mathcal{L}_r}$ la fonction précédente, ainsi que $\mathcal{L} = \mathcal{L}_1 \star \cdots \star \mathcal{L}_r$.

THÉORÈME 4.3.5 (FORMULES D'ADDITION). *Soit $\mathcal{L}_0$ un fibré totalement symétrique sur X, et supposons fixée une ∞-décomposition de $K(\mathcal{L}_0)$. Soit $f : X^r \to X^r$ une isogénie donnée par une matrice F entière $r \times r$ telle que*

$$ {}^tF \begin{pmatrix} m_1 & & 0 \\ & \ddots & \\ 0 & & m_r \end{pmatrix} F = \begin{pmatrix} \ell_1 & & 0 \\ & \ddots & \\ 0 & & \ell_r \end{pmatrix} \tag{4.3} $$

où les entiers m_i et ℓ_i sont premiers à p.

Si π_i est la projection de X^r sur sa i-ième composante, soit $\mathcal{L} = \pi_1^*\mathcal{L}_0^{\ell_1} \otimes \cdots \otimes \pi_r^*\mathcal{L}_0^{\ell_r}$ et $\mathcal{M} = \pi_1^*\mathcal{L}_0^{m_1} \otimes \cdots \otimes \pi_r^*\mathcal{L}_0^{m_r}$. L'équation (4.3) montre que $f^*\mathcal{M} \simeq \mathcal{L}$.

Il existe alors une constante $\lambda \in k^*$ telle que pour tout $(i_1, \ldots, i_r) \in K_1(\mathcal{L}_0^{m_1}) \times \cdots \times K_1(\mathcal{L}_0^{m_r})$,

$$ f^*(\vartheta_{i_1}^{\mathcal{L}_0^{m_1}} \star \cdots \star \vartheta_{i_r}^{\mathcal{L}_0^{m_r}}) = \lambda \sum_{\substack{(j_1,\ldots,j_r) \in K_1(\mathcal{L}_0^{m_1}) \times \cdots \times K_1(\mathcal{L}_0^{m_r}) \\ f(j_1,\ldots,j_r) = (i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}_0^{\ell_1}} \star \cdots \star \vartheta_{j_r}^{\mathcal{L}_0^{\ell_r}} \tag{4.4} $$

DÉMONSTRATION : Si f satisfait l'équation (4.3), le ''seesaw-principle'' montre que $f^*\mathcal{M} \simeq \mathcal{L}$. Si $k = \mathbb{C}$, on le voit immédiatement en utilisant le lemme 2.4.2.

La remarque 4.2.15 montre que les structures de niveau symétriques induites par la ∞-décomposition sur (des produits de) $G(\mathcal{L}_0^n)$ sont f-compatibles. On peut donc appliquer le

somme directe (de leur pullback sur X).

théorème de l'isogénie aux fonctions thêta canoniques déduites de ces structures de niveau, on obtient l'équation (4.4).

On peut aussi consulter [Kem89, Théorèmes 7 et 8] pour une preuve plus générale qui ne suppose pas $\mathcal{L}_0$ totalement symétrique. ■

Ce théorème a d'abord été prouvé analytiquement dans [Koi76], avant d'être étendu dans [Kem89] au cas algébrique. On peut trouver un exposé du cas analytique dans [Mum83, p. 211-216].

Remarque 4.3.6. Dans le théorème de l'isogénie (le théorème 3.6.4), si l'on se fixe des trivialisations en 0 compatibles de $\mathcal{L}$ et $\mathcal{M}$, et que l'on considère les uniques représentants de la base des fonctions théta de $\mathcal{L}$ et $\mathcal{M}$ sous l'action de k^* induits par ces trivialisations (voir la section 3.4), alors $\lambda = 1$. En particulier, dans le théorème 4.3.5, si l'on se fixe une trivialisation de $\mathcal{L}_0$ en 0, et que l'on considère les trivialisations compatibles de $\mathcal{L}$ et $\mathcal{M}$ en 0, on a également $\lambda = 1$. ♢

Un cas particulier du théorème précédent donne les formules de duplication, qui plus généralement sont vraies dès qu'on prend des thêta structures symétriques sur $G(\mathcal{L}_0)$ et $G(\mathcal{L}_0^2)$ qui sont compatibles au sens de [Mum66, p. 317].

Corollaire 4.3.7 (Formules de duplication). *On applique le théorème 4.3.5 à la fonction*

$$\begin{array}{rcl} \xi\colon X \times X & \longrightarrow & X \times X \\ (x, y) & \longmapsto & (x + y, x - y) \end{array}$$

avec $m_1 = m_2 = 1$ et $\ell_1 = \ell_2 = 1$. De plus, si $\mathcal{L}_0$ est de type δ, on suppose choisies des numérotations $Z(\delta) \to K_1(\mathcal{L})$ et $Z(2\delta) \to K_1(\mathcal{L}^2)$ telles que $Z(\delta) \subset Z(2\delta)$ respecte l'inclusion $K_1(\mathcal{L}) \subset K_1(\mathcal{L}^2)$. Comme les structures de niveau de $G(\mathcal{L})$ et $G(\mathcal{L}^2)$ sont fixées par la ∞-décomposition de $K(\mathcal{L})$, les numérotations compatibles de $Z(\delta)$ et $Z(2\delta)$ fixent des thêta structures symétriques sur $G(\mathcal{L})$ et $G(\mathcal{L}^2)$. On appelle de telles thêta structures des thêta structures compatibles[1].

On obtient qu'il existe une constante $\lambda \in k^*$ telle que pour tout $(i_1, i_2) \in Z(\delta) \times Z(\delta)$,

$$\xi^*(\vartheta_{i_1}^{\mathcal{L}_0} \star \vartheta_{i_2}^{\mathcal{L}_0}) = \lambda \sum_{\substack{(j_1,j_2)\in Z(\delta^2)\times Z(\delta^2) \\ j_1+j_2=i_1 \\ j_1-j_2=i_2}} \vartheta_{j_1}^{\mathcal{L}_0^2} \star \vartheta_{j_r}^{\mathcal{L}_0^2}$$

4.4 PSEUDO ADDITION SUR LE CÔNE AFFINE D'UNE VARIÉTÉ ABÉLIENNE

Soit $\mathcal{L}$ un fibré très ample de type δ sur une variété abélienne X. Si $V = \Gamma(X, \mathcal{L})$, on a un plongement $X \to \mathbb{P}(V)$ induit par $\mathcal{L}$. L'action de $G(\mathcal{L})$ sur V induit une action projective sur $X \subset \mathbb{P}(V)$. Si $(x, \phi) \in G(\mathcal{L})$ cette action est simplement la translation par $-x$ (voir la section 3.4). On perd donc toute l'information supplémentaire contenue dans $G(\mathcal{L})$. Pour remédier à cette situation, on a vu dans la section 2.6 que si X était une variété abélienne complexe, on considérait les éléments de V (les fonctions thêta) comme des fonctions sur $\mathbb{C}^g$

1. La notion habituelle de thêta structures symétriques compatibles sur $G(\mathcal{L}^2)$ et $G(\mathcal{L})$ est définie par Mumford comme des thêta structures qui commutent aux actions de η_2 et ϵ_2 [Mum66, p. 309-320]. Mais si $\phi \in G(\mathcal{L}^2)$, $\eta_2(\phi) = \alpha_{[2]}(\phi^{\otimes 2})$, il s'agit donc juste d'une manière de reformuler la [2]-compatibilité de $G(\mathcal{L}^4)$ et $G(\mathcal{L})$ au-dessus de $K(\mathcal{L}^2)$ et les deux notions coïncident. (Voir le diagramme dans [Mum66, p. 317])

et pas seulement sur X. Pour imiter ce procédé, si $p_X : \mathbb{A}(V) \smallsetminus \{0\} \to \mathbb{P}(V)$ est le morphisme canonique, on considère le cône affine $\widetilde{X} \coloneqq p_X^{-1}(X)$. Le choix d'un point $\widetilde{x} \in \widetilde{X}$ au-dessus de $x \in X$ peut se voir comme le choix d'un morphisme de trivialisation $\mathcal{L}(x) \to k$. La base de fonction thêta canoniques $(\vartheta_i)_{i\in Z(\delta)}$ n'est définie qu'à une action de k^* près. Cela ne change rien quand on voit les ϑ_i comme des coordonnées projectives sur X, mais il faut faire un choix quand on les voit comme coordonnées affines sur X. Il s'avère qu'on a un deuxième choix à faire modulo l'action de k^*, à savoir le choix d'un relevé de $x \in X$ dans $\widetilde{X}$. On peut donc fixer une fois pour toute un choix quelconque de fonctions $(\vartheta_i)_{i\in Z(\delta)}$, et se concentrer sur le choix des relevés affines des points géométriques de X.

Pour ne pas alourdir l'exposé, quand on parle d'un point affine au-dessus d'un point géométrique $x \in X$, on le note par défaut $\widetilde{x}$.

L'action de $G(\mathcal{L})$ sur V décrite dans la section 3.4 nous donne une action (affine) sur $\widetilde{X}$. La forme explicite de cette action sur la base donnée par les fonctions thêta est fournie par l'équation (3.6). De manière concrète, si l'on transporte via $\Theta_{\mathcal{L}}$ l'action de $G(\mathcal{L})$ sur $\widetilde{X}$ en une action de $\mathcal{H}(\delta)$ sur $\widetilde{X}$, et si $\widetilde{x} \in \widetilde{X}$ a pour coordonnées $\widetilde{x} = (\vartheta_i(\widetilde{x}))_{i\in Z(\delta)} = (x_i)_{i\in Z(\delta)}$, alors si $(\alpha, i, j) \in \mathcal{H}(\delta)$, on a

$$(\alpha, i, j).\widetilde{x} = (\alpha\langle i + l, -j\rangle x_{i+l})_{l\in Z(\delta)}. \tag{4.5}$$

On note $\widetilde{0}_X$ un relevé affine du thêta null point de X. Un tel choix de relevé correspond à un morphisme de trivialisation : $\gamma_0 : \mathcal{L}(0) \xrightarrow{\sim} k$. On a vu dans la section 3.4 que la thêta structure $\Theta_{\mathcal{L}}$ nous donnait alors des morphismes de trivialisations canoniques $\gamma_x : \mathcal{L}(x) \xrightarrow{\sim} k$ lorsque $x \in K(\mathcal{L})$. On a alors un relevé affine $\widetilde{x}$ de x associé à γ_x donné par $\widetilde{x} = (\gamma_x(\vartheta_i))_{i\in Z(\delta)}$. Si on revient à la définition de γ_x, on voit que $\widetilde{x} = s_{K(\mathcal{L})}(x).\widetilde{0}_X$. Ainsi le choix d'un relevé affine $\widetilde{0}_X$ du thêta null point nous donne une section de $\widetilde{X} \to X$ au-dessus de $K(\mathcal{L})$ dont l'image est

$$\{(1, i, j).\widetilde{0}_X \mid i \in Z(\delta), j \in \hat{Z}(\delta)\}.$$

Le théorème de l'isogénie est pleinement adapté aux cônes affines : si $f : (X, \mathcal{L}) \to (Y, \mathcal{M})$ est une isogénie de variétés abéliennes polarisées, et que l'on a choisi des thêta structures f-compatibles $G(\mathcal{L})$ et $G(\mathcal{M})$, la relation entre les thêta fonctions de $G(\mathcal{L})$ et $G(\mathcal{M})$ est décrite par

$$f^*\vartheta_i^{\Theta_{\mathcal{M}}} = \lambda \sum_{j\in\sigma^{-1}(i)} \vartheta_j^{\Theta_{\mathcal{L}}}$$

avec $i \in Z(\delta_0)$ où δ_0 est le niveau de $\mathcal{M}$, en reprenant les notations du théorème 3.6.4. Comme λ ne dépend pas du point x où on évalue les fonctions thêta, si on a fixé un choix de coordonnées affines sur $\widetilde{X}$ et $\widetilde{Y}$, les cônes affines de X et Y, on peut définir un relevé affine $\widetilde{f}$ de f ainsi :

$$\widetilde{f}^*\vartheta_i^{\Theta_{\mathcal{M}}} = \sum_{j\in\sigma^{-1}(i)} \vartheta_j^{\Theta_{\mathcal{L}}}.$$

On appelle $\widetilde{f}$ le relevé canonique de f par rapport au système de coordonnées affines sur $\widetilde{X}$ et $\widetilde{Y}$, et on a le diagramme commutatif suivant :

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{p_X} & X \\ \downarrow{\scriptstyle \widetilde{f}} & & \downarrow{\scriptstyle f} \\ \widetilde{Y} & \xrightarrow{p_Y} & Y. \end{array}$$

Remarque 4.4.1 (Fibres de $\widetilde{f}$). Soit K le noyau de f, et $\widetilde{K} \subset G(\mathcal{L})$ le relevé de K associé à l'isomorphisme $f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$, et $\alpha_f : \mathcal{Z}(\widetilde{K}) \to G(\mathcal{M})$ l'application canonique de la proposition 3.2.5. On peut alors étendre la remarque 3.4.2 au cas affine. En effet, la preuve du

théorème 3.6.4 montre qu'il existe λ tel que si $\widetilde{x}$ est un point géométrique de $\widetilde{X}$, et $g \in G(\mathcal{L})$ est un élément de $\mathcal{Z}(\widetilde{K})$, on a $\widetilde{f}(g.\widetilde{x}) = \lambda\alpha_f(g).\widetilde{f}(\widetilde{x})$. De plus, comme on a pris des coordonnées affines $\widetilde{f}$-compatibles, on a $\lambda = 1$.

En particulier, si $\widetilde{x}$ est un point géométrique de $\widetilde{X}$, les points géométriques de $\widetilde{f}^{-1}(\widetilde{f}(\widetilde{x}))$ forment un espace homogène principal sous l'action de $\widetilde{K}$. Autrement dit, si $K_0 \subset K(\delta)$ est le sous-groupe correspondant à K via $\overline{\Theta}_{\mathcal{L}}$, alors les antécédents de $\widetilde{f}(\widetilde{x})$ sont donnés par

$$\{(1,i,j).\widetilde{x} \mid (i,j) \in K_0\}.$$

En effet, si $i \in K$, $s_{K(\mathcal{L})}(i)$ est dans le groupe de niveau $\widetilde{K}$, et donc

$$\widetilde{f}(s_{K(\mathcal{L})}(i).\widetilde{x}) = \alpha_f(s_{K(\mathcal{L})}(i)).\widetilde{f}(\widetilde{x}) = \mathrm{Id}\,.\widetilde{f}(\widetilde{x}).$$

> On peut aussi le vérifier directement : si $g \in \widetilde{K}$ et $x = p_X(\widetilde{x})$, on a $f(g.x) = f(x)$, donc pour montrer que $\widetilde{f}(g.\widetilde{x}) = \widetilde{f}(\widetilde{x})$, il suffit de vérifier que $\vartheta_0^{\mathcal{M}}(\widetilde{f}(g.\widetilde{x})) = \vartheta_0^{\mathcal{M}}(\widetilde{f}(\widetilde{x}))$. Si $K = K_1 \oplus K_2$ est la décomposition symplectique de K induite par la décomposition symplectique $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$, on sait par le théorème 3.6.4 que le relevé canonique $\widetilde{f}$ vérifie la formule $\vartheta_0^{\mathcal{M}}(\widetilde{f}(\widetilde{x})) = \sum_{i\in K_1}\vartheta_i^{\mathcal{L}}(\widetilde{x})$. Or il est clair que la somme du membre de droite est inchangée par l'action d'un élément de $\widetilde{K}_1$, et comme K est isotrope, K_2 est orthogonal à K_1, donc cette somme est également invariante par l'action d'un élément de $\widetilde{K}_2$ par l'équation (3.6). Comme $\widetilde{K}$ est engendré par $\widetilde{K}_1$ et $\widetilde{K}_2$, ceci conclut la remarque. ◇

Exemple 4.4.2 (L'isogénie de multiplication par ℓ). Soit $\mathcal{L}$ un fibré symétrique de niveau δ sur une variété abélienne X. Alors $[\ell]^*\mathcal{L} \simeq \mathcal{L}^{\ell^2}$ est un fibré symétrique de niveau $\ell^2\delta$. Soit $\Theta_{\mathcal{L}^{\ell^2}}$ et $\Theta_{\mathcal{L}}$ des théta structures sur $(X,\mathcal{L}^{\ell^2})$ et sur $(X,\mathcal{L})$ respectivement, qui soient $[\ell]$-compatibles. Soit $(\vartheta_i^{\mathcal{L}^{\ell^2}})_{i\in Z(\ell^2\delta)}$ et $(\vartheta_i^{\mathcal{L}})_{i\in Z(\delta)})$ des coordonnées théta canoniques associées sur $(X,\mathcal{L}^{\ell^2})$ et $(X,\mathcal{L})$. Alors le relevé canonique $\widetilde{[\ell]}$ et $[\ell]$ par rapport à ces coordonnées est donné par le théorème 3.6.4 :

$$\widetilde{[\ell]}^*\vartheta_i^{\mathcal{L}} = \sum_{j\in Z(\overline{\ell})}\vartheta_{i+j}^{\mathcal{L}^{\ell^2}}.$$

Le noyau K de $[\ell]$ est égal à $X[\ell]$, et le relevé canonique $\widetilde{K}$ est donné par $\Theta^{-1}_{\mathcal{L}^{\ell^2}}(\widetilde{K}) = \{(1,i,j) \mid i \in Z(\overline{\ell}), j \in \hat{Z}(\overline{\ell})\} \subset \mathcal{H}(\ell^2\delta)$. ◇

On dit que deux relevé affines $\widetilde{0}_X$ et $\widetilde{0}_Y$ des théta null points de X et Y sont compatibles si $\widetilde{f}(\widetilde{0}_X) = \widetilde{0}_Y$. Par la suite, on considère toujours des relevés affines compatibles.

On commence par appliquer le corollaire 4.3.7 au cône affine de X : on verra que l'on peut ainsi retrouver la loi de groupe sur X, mais aussi définir une pseudo loi de groupe sur $\widetilde{X}$ au-dessus de celle de X, qui est crucial pour la suite.

Supposons donc que k est de caractéristique différente de 2, et soit X une variété abélienne sur k avec un fibré $\mathcal{L}$ totalement symétrique. On se donne une théta structure symétrique $\Theta_{\mathcal{L}}$ sur $G(\mathcal{L})$, ainsi qu'une théta structure sur $G(\mathcal{L}^2)$ compatible avec celle de $G(\mathcal{L})$. (C'est-à-dire que l'on prend une ∞-décomposition de $K(\mathcal{L})$ compatible avec la structure de niveau de $G(\mathcal{L})$, ce qui est toujours possible par la proposition 4.3.1. Cette ∞-décomposition fixe une structure de niveau symétrique sur $G(\mathcal{L}^2)$, et on se fixe ensuite une numérotation de $K(\mathcal{L}^2)$ par $K(\delta^2)$ compatible avec la numérotation de $K(\mathcal{L})$ par $K(\delta)$.)

Déjà, on a vu dans la proposition 4.2.14 que dans le cas d'une théta structure symétrique on avait $[-1]^*\vartheta_i = \vartheta_{-i}$. Le relevé affine canonique de $[-1]$ est donc donné sur les coordonnées théta par

$$\widetilde{[-1]} : \widetilde{X} \to \widetilde{X}, (\vartheta_i(x))_{i\in Z(\delta)} \mapsto (\vartheta_{-i}(x))_{i\in Z(\delta)} \tag{4.6}$$

On voit donc que l'inverse est très agréable à manipuler. Pour alléger les notations, si $\widetilde{x} \in \widetilde{X}$, on note son inverse $-\widetilde{x}$.

Le corollaire 4.3.7 nous donne alors que pour tout points géométriques x, y sur X, si l'on note $\widetilde{x}$, $\widetilde{y}$, $\widetilde{x-y}$ et $\widetilde{x+y}$ des relevé affines à $\widetilde{X}$ de x, y, $x-y$ et $x+y$ respectivement, il existe $\lambda \in k^*$ tel que pour tout $i, j \in K(\delta)$ on ait :

$$\vartheta_i^{\mathcal{L}}(\widetilde{x+y})\vartheta_j^{\mathcal{L}}(\widetilde{x-y}) = \lambda \sum_{\substack{u,v \in Z(2\delta) \\ u+v=i \\ u-v=j}} \vartheta_u^{\mathcal{L}^2}(\widetilde{x})\vartheta_v^{\mathcal{L}^2}(\widetilde{y}) \tag{4.7}$$

On peut inverser l'équation (4.7) en considérant un changement de variable. Si $\chi \in \hat{Z}(\overline{2})$ et $i \in Z(\delta)$, on pose

$$U_{\chi,i}^{\mathcal{L}} = \sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}^{\mathcal{L}}.$$

(Comme $\mathcal{L}$ est totalement symétrique, $2 \mid \delta$ et on peut considérer $Z(\overline{2})$ comme un sous-groupe de $Z(\delta)$ via le plongement $Z(\overline{2}) \subset Z(\delta)$ canonique). Si $t \in Z(\overline{2})$, on vérifie immédiatement que $U_{\chi,i+t}^{\mathcal{L}} = \chi(t)U_{\chi,i}^{\mathcal{L}}$ donc on peut essentiellement considérer que les $U_{\chi,i}^{\mathcal{L}}$ sont indicés par $\hat{Z}(\overline{2}) \times Z(\delta)/Z(\overline{2})$. Le changement de variable $\vartheta^{\mathcal{L}} \mapsto U^{\mathcal{L}}$ est simplement une transformation de Fourrier dans $Z(\overline{2})$, ce qui va nous permettre de passer de la convolution dans l'équation (4.7) à un produit :

THÉORÈME 4.4.3. *Soit $\widetilde{x}, \widetilde{y}$ des points géométriques de $\widetilde{X}$. Il existe $\lambda_1, \lambda_2 \in k^*$ tels que pour tout $i, j \in Z(2\delta)$ tels que i et j soient congruents modulo $Z(\delta)$, on ait*

$$\vartheta_{i+j}^{\mathcal{L}}(\widetilde{x+y})\vartheta_{i-j}^{\mathcal{L}}(\widetilde{x-y}) = \frac{\lambda_1}{2^g} \sum_{\chi \in \hat{Z}(\overline{2})} U_{\chi,i}^{\mathcal{L}^2}(\widetilde{x})U_{\chi,j}^{\mathcal{L}^2}(\widetilde{y}) \tag{4.8}$$

$$U_{\chi,i}^{\mathcal{L}^2}(\widetilde{x})U_{\chi,j}^{\mathcal{L}^2}(\widetilde{y}) = \lambda_2 \sum_{t \in \hat{Z}(\overline{2})} \chi(t)\vartheta_{i+j+t}^{\mathcal{L}}(\widetilde{x+y})\vartheta_{i-j+t}^{\mathcal{L}}(\widetilde{x-y}) \tag{4.9}$$

DÉMONSTRATION : On peut supposer que $\widetilde{x+y}, \widetilde{x-y}$ sont choisis de telle sorte que $\lambda_1 = 1$, $\lambda_2 = 1$. On fera toujours cette hypothèse par la suite. Si i et j sont congruents modulo $Z(\delta)$, alors clairement $i+j$ et $i-j$ sont dans $Z(\delta)$. Inversement, comme $Z(\delta) = 2Z(2\delta)$, tout couple d'éléments de $Z(\delta)$ est de cette forme. De plus, l'ensemble des $u, v \in Z(2\delta)$ tels que $u+v = i+j$ et $u-v = i-j$ est donné par $u = i+t$ et $v = j+t$ où $t \in Z(\overline{2})$ est un point d'ordre 2 de $Z(2\delta)$. On a donc :

$$\vartheta_{i+j}^{\mathcal{L}}(\widetilde{x+y})\vartheta_{i-j}^{\mathcal{L}}(\widetilde{x-y}) = \sum_{t \in Z(\overline{2})} \vartheta_{i+t}^{\mathcal{L}^2}(\widetilde{x})\vartheta_{j+t}^{\mathcal{L}^2}(\widetilde{y}).$$

Et d'autre part on a

$$\begin{aligned}\sum_{\chi \in \hat{Z}(\overline{2})} U_{\chi,i}^{\mathcal{L}^2}(\widetilde{x})U_{\chi,j}^{\mathcal{L}^2}(\widetilde{y}) &= \sum_{\substack{\chi \in \hat{Z}(\overline{2}) \\ t_1,t_2 \in Z(\overline{2})}} \chi(t_1+t_2)\vartheta_{i+t_1}^{\mathcal{L}^2}(\widetilde{x})\vartheta_{j+t_2}^{\mathcal{L}^2}(\widetilde{y}) \\ &= 2^g \sum_{t \in Z(\overline{2})} \vartheta_{i+t}^{\mathcal{L}^2}(\widetilde{x})\vartheta_{j+t}^{\mathcal{L}^2}(\widetilde{y})\end{aligned}$$

ce qui montre l'équation (4.8).

Pour l'équation (4.9), pour tout $\chi \in \hat{Z}(\overline{2})$ on calcule

$$\begin{aligned}\sum_{t\in Z(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(\widetilde{x+y})\vartheta^{\mathcal{L}}_{i-j+t}(\widetilde{x-y}) &= \sum_{\substack{t\in Z(\overline{2})\\ u,v\in Z(\overline{2ln})\\ u+v=i+j+t\\ u-v=i-j+t}} \chi(t)\vartheta^{\mathcal{L}^2}_{u}(\widetilde{x})\vartheta^{\mathcal{L}^2}_{v}(\widetilde{y})\\ &= \sum_{t_1,t_2\in Z(\overline{2})} \chi(t_1+t_2)\vartheta^{\mathcal{L}^2}_{i+t_1}(\widetilde{x})\vartheta^{\mathcal{L}^2}_{j+t_2}(\widetilde{y})\\ &= \left(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{i+t}(\widetilde{x})\right)\cdot\left(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{j+t}(\widetilde{y})\right)\\ &= U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{y}).\end{aligned}$$

On retrouve l'équation (4.9). ∎

On peut utiliser le théorème 4.4.3 pour calculer $\vartheta_i(\widetilde{x+y})$ ainsi : supposons par exemple que $\vartheta_i(\widetilde{x-y}) \neq 0$, on obtient :

$$\vartheta^{\mathcal{L}}_i(\widetilde{x+y})\vartheta^{\mathcal{L}}_i(\widetilde{x-y}) = \frac{1}{2^g}\sum_{\chi\in\hat{Z}(\overline{2})} U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,0}(\widetilde{y}).$$

Il reste à calculer les $U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,0}(\widetilde{y})$. On utilise l'équation (4.9) pour obtenir

$$U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{0}_X) = \sum_{t\in\hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(\widetilde{x})\vartheta^{\mathcal{L}}_{i-j+t}(\widetilde{x}).$$

On peut donc calculer $U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})$ s'il existe $j \in Z(\delta)$ tel que $U^{\mathcal{L}^2}_{\chi,j}(\widetilde{0}_X) \neq 0$.

THÉORÈME 4.4.4. *Si $\mathcal{L}$ est un fibré totalement symétrique de niveau δ, et que δ est divisible par un nombre pair $n \geqslant 4$, alors pour tout $\chi \in \hat{Z}(\overline{2})$, et tout $i \in Z(2\delta)$, il existe $j \in Z(\delta)$ tel que $U^{\mathcal{L}^2}_{\chi,i+j}(\widetilde{0}_X) \neq 0$.*

DÉMONSTRATION : Soit $\xi : X \times X \to X \times X$ la fonction donnée sur les points géométriques par $(x, y) \mapsto (x + y, x - y)$ du corollaire 4.3.7. Si $\Delta : X \to X \times X$ est l'application diagonale, donnée sur les points géométriques par $\Delta : x \mapsto (x, x)$ et $S : X \to X \times X$ est donnée sur les points géométriques par $x \mapsto (x, 0)$, on a le diagramme commutatif suivant de variétés abéliennes polarisées :

$$\begin{array}{ccc}(X,\mathcal{L}^2) & & \\ \downarrow{\scriptstyle S} & \searrow^{\Delta} & \\ (X\times X,\mathcal{L}^2\star\mathcal{L}^2) & \xrightarrow{\xi} & (X\times X,\mathcal{L}\star\mathcal{L}).\end{array}$$

L'appliquation $\Delta^* : \Gamma(X,\mathcal{L})\otimes\Gamma(X,\mathcal{L}) \to \Gamma(X,\mathcal{L}^2)$ est donnée sur les fonctions thêtas par $\vartheta^{\mathcal{L}}_i \star \vartheta^{\mathcal{L}}_j \mapsto (\vartheta^{\mathcal{L}}_i \otimes \vartheta^{\mathcal{L}}_j)$, l'appliquation $\xi^* : \Gamma(X,\mathcal{L})\otimes\Gamma(X,\mathcal{L}) \to \Gamma(X,\mathcal{L}^2)\otimes\Gamma(X,\mathcal{L}^2)$ a été vue au corollaire 4.3.7. Enfin l'identification de $S^*(\mathcal{L}^2 \star \mathcal{L}^2)$ à $\mathcal{L}^2$ vient d'un morphisme de trivialisation $\gamma_0 : \mathcal{L}^2(0) \to k$ appliquée au membre de droite de $\mathcal{L}^2 \star \mathcal{L}^2$, et via cette

identification, $S^*\Gamma(X,\mathcal{L}^2)\otimes\Gamma(X,\mathcal{L}^2)\to\Gamma(X,\mathcal{L}^2)$ est donnée sur les fonctions thêta par $\vartheta_i^{\mathcal{L}^2}\star\vartheta_j^{\mathcal{L}^2}\mapsto\vartheta_i^{\mathcal{L}^2}\vartheta_j^{\mathcal{L}^2}(0)$.

Au final, la formule de multiplication $\Gamma(X,\mathcal{L})\otimes\Gamma(X,\mathcal{L})\to\Gamma(X,\mathcal{L}^2)$ est donnée par

$$\vartheta_i^{\mathcal{L}}\star\vartheta_j^{\mathcal{L}}\mapsto\sum_{\substack{u,v\in Z(2\delta)\\ u+v=i\\ u-v=j}}\vartheta_u^{\mathcal{L}^2}\vartheta_v^{\mathcal{L}^2}(0)$$

Cette équation peut se réécrire via le changement de variable du théorème 4.4.3 comme

$$\sum_{t\in\hat{Z}(\delta)}\chi(t)\vartheta_{i+t}^{\mathcal{L}}\star\vartheta_{j+t}^{\mathcal{L}}\mapsto U_{\chi,u}^{\mathcal{L}^2}U_{\chi,v}^{\mathcal{L}^2}(0). \tag{4.10}$$

où $i,j\in Z(\delta)$, et $u,v\in Z(2\delta)$ sont tels que $i=u+v$ et $j=u-v$.

Il y a donc équivalence entre l'assertion $\Gamma(X,\mathcal{L})\otimes\Gamma(X,\mathcal{L})\to\Gamma(X,\mathcal{L}^2)$ est surjective, et pour tout $u\in Z(2\delta)$, $\chi\in\hat{Z}(\delta)$, il existe $v\in Z(2\delta)$ congru à u modulo $Z(\delta)$ tel que $U_{\chi,v}^{\mathcal{L}^2}(0)\neq 0$.

Mumford a montré directement que c'était le cas lorsque $4\mid\delta$ dans [Mum66, p. 339], et en déduit que si $\mathcal{L}_0$ est un fibré, $\Gamma(X,\mathcal{L}_0^n)\otimes\Gamma(\mathcal{L}_0^n)\to\Gamma(X,\mathcal{L}_0^{2n})$ est surjectif lorsque $4\mid n$. Koizumi a étendu ce résultat dans [Koi76, Théorème 4.6] en montrant analytiquement que $\Gamma(X,\mathcal{L}_0^n)\otimes\Gamma(\mathcal{L}_0^m)\to\Gamma(X,\mathcal{L}_0^{n+m})$ est surjectif dès que $n\geqslant 2$ et $m\geqslant 3$. Une preuve algébrique de ce résultat est donnée par Kempf dans [Kem88], on en déduit que $\Gamma(X,\mathcal{L}_0^n)\otimes\Gamma(\mathcal{L}_0^n)\to\Gamma(X,\mathcal{L}_0^{2n})$ est surjectif dès que $n\geqslant 4$ est un nombre pair, ce qui termine la démonstration car $\mathcal{L}$ est de la forme $\mathcal{L}_0^n$ si $n\mid\delta$ d'après le corollaire 2.4.8. ■

Remarque 4.4.5 (Projectivé normale). Si $\mathcal{L}$ est un fibré très ample sur une variété projective lisse X, on dit que le plongement de X dans $\mathbb{P}_N$ est projectivement normal si l'anneau homogène de X associé à ce plongement est intégralement clos. Cette condition est équivalente à demander que $S^n\Gamma(X,\mathcal{L})\to\Gamma(X,\mathcal{L}^n)$ soit surjectif pour tout $n\geqslant 2$ [Haroo, Exercice 5.14 p. 126] (et suffit à imposer que $\mathcal{L}$ soit très ample par [Mum69, p. 38]). De manière équivalente [BL04, p. 187], il suffit de vérifier que $\Gamma(X,\mathcal{L}^n)\otimes\Gamma(X,\mathcal{L})\to\Gamma(X,\mathcal{L}^{n+1})$ est surjectif pour $n\geqslant 1$. La preuve du théorème 4.4.4 montre que si $\mathcal{L}$ est un fibré totalement symétrique de type δ sur une variété abélienne, et que $n\mid\delta$ avec $n\geqslant 4$ pair, alors $(X,\mathcal{L})$ est projectivement normal. ♢

Le problème des formules de duplications du théorème 4.4.3 est qu'elles font intervenir des fonctions thêta sur $\mathcal{L}^2$. On peut combiner les équations (4.8) et (4.9) pour obtenir des relations qui ne font intervenir que les $(\vartheta_i^{\mathcal{L}})_{i\in Z(\delta)}$.

Théorème 4.4.6. *Soit x_1,y_1,u_1 et v_1 des points géométriques de X et $z\in X(\overline{k})$ tel que $x_1+y_1+u_1+v_1=2z$. On pose $x_2=z-x_1$, $y_2=z-y_1$, $u_2=z-u_1$ et $v_2=z-v_1$. Il existe des relevé affines de ces points tels qu'on a : pour tout $\chi\in\hat{Z}(\overline{2})$ et $i,j,k,l,m\in Z(\delta)$ avec $i+j+k+l=2m$, si $i'=m-i$, $j'=m-j$, $k'=m-k$ et $l'=m-l$, alors*

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{i+t}(\widetilde{x}_1)\vartheta_{j+t}(\widetilde{y}_1)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k+t}(\widetilde{u}_1)\vartheta_{l+t}(\widetilde{v}_1)\Big)=$$
$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{i'+t}(\widetilde{x}_2)\vartheta_{j'+t}(\widetilde{y}_2)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k'+t}(\widetilde{u}_2)\vartheta_{l'+t}(\widetilde{v}_2)\Big). \tag{4.11}$$

On dit que ces points satisfont les relations de Riemann.

En particulier, on a les formules (ou relations) d'addition suivantes (où χ, i, j, k, l sont comme précédemment) :

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{k+t}(\widetilde{0}_X)\vartheta_{l+t}(\widetilde{0}_X)\Big) = \Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{-i'+t}(\widetilde{y})\vartheta_{j'+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{k'+t}(\widetilde{x})\vartheta_{l'+t}(\widetilde{x})\Big). \quad (4.12)$$

Inversement, si $\mathcal{L}$ est de type δ, et qu'il existe un entier pair $n \geqslant 4$ qui divise δ, alors si on se fixe des relevé affines $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x-y}$ de x, y et $x-y$, il existe un unique point $\widetilde{x+y}$ de $\widetilde{X}$ qui satisfait les formules d'addition (4.12). On voit que dans ce cas on a une loi de pseudo-addition sur $\widetilde{X}$ (que l'on appelle aussi addition différentielle) au-dessus de la loi d'addition de X. On note

$$\widetilde{x+y} \coloneqq \texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y}).$$

(Il nous arrive également de la noter

$$\widetilde{x+y} \coloneqq \texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y},\widetilde{0}_X)$$

lorsqu'on veut préciser par rapport à quel thêta null point $\widetilde{0}_X$ on calcule cette addition différentielle.)

Démonstration : En utilisant l'équation (4.9), si i, j, k, l sont des éléments de $Z(2\delta)$ congruents modulo $Z(\delta)$, et x, y, u, v sont des points géométriques de X on trouve :

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(\widetilde{x+y})\vartheta^{\mathcal{L}}_{i-j+t}(\widetilde{x-y})\Big)\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta^{\mathcal{L}}_{k+l+t}(\widetilde{u+v})\vartheta^{\mathcal{L}}_{k-l+t}(\widetilde{u-v})\Big) = U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{y})U^{\mathcal{L}^2}_{\chi,k}(\widetilde{u})U^{\mathcal{L}^2}_{\chi,l}(\widetilde{v}).$$

Or on a de même

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta^{\mathcal{L}}_{i+l+t}(\widetilde{x+v})\vartheta^{\mathcal{L}}_{i-l+t}(\widetilde{x-v})\Big)\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta^{\mathcal{L}}_{k+j+t}(\widetilde{u+y})\vartheta^{\mathcal{L}}_{k-j+t}(\widetilde{u-y})\Big) = U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,l}(\widetilde{v})U^{\mathcal{L}^2}_{\chi,k}(\widetilde{u})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{y}).$$

En combinant ces deux identités, on trouve que les deux membres de gauche de ces équations sont égaux. Un changement de variable nous donne alors trivialement l'équation (4.11) ((En effet, on a $(x+y)+(x-y)+(u+v)+(u-v) = 2(x+u)$, on peut donc prendre $z = x+y$. Le seul point à vérifier est que le membre de droite de l'équation (4.11) ne change pas quand on remplace z par $z+t$ où t est un point de 2-torsion. Mais si $t = \overline{\Theta}_{\mathcal{L}}(c_1, c_2)$, en utilisant l'équation (3.6) on voit que le membre de droite change par $(\chi(t_1)\langle i'+c_1,-c_2\rangle\langle j'+c_1,-c_2\rangle)(\chi(t_1)\langle k'+c_1,-c_2\rangle\langle l'+c_1,-c_2\rangle) = \langle 2z,-c_2\rangle = 1$.))On fait le même changement de variable sur i, j, k et l.

L'équation (4.12) est juste un cas particulier de l'équation (4.11) appliqué à $(x+y), (x-y), 0_X, 0_X$, on trouve qu'on peut prendre $z = x$. On utilise l'équation (4.6) pour calculer les coordonnées de $-\widetilde{y}$.

Pour l'unicité, en utilisant le théorème 4.4.4, on voit qu'on peut calculer $\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})$ pour tout $i, j \in Z(\delta)$ et $\chi \in \hat{Z}(\bar{2})$. En effet, si on prend k et l quelconques dans $Z(\delta)$ tels que $i+j+l+k = 2m$, alors

$$\sum_{t\in Z(\bar{2})}\chi(t)\vartheta^{\mathcal{L}}_{k+t}(\widetilde{0}_X)\vartheta^{\mathcal{L}}_{l+t}(\widetilde{0}_X) = U^{\mathcal{L}^2}_{u}(\widetilde{0}_X)U^{\mathcal{L}^2}_{v}(\widetilde{0}_X)$$

où $u, v \in Z(2\delta)$ vérifient $u+v=k$, $u-v=l$. Alors par le théorème 4.4.4, il existe $u', v' \in Z(\delta)$ tels que $U^{\mathcal{L}^2}_{u+u'}(\widetilde{0}_X)U^{\mathcal{L}^2}_{v+v'}(\widetilde{0}_X) \neq 0$. On peut alors appliquer l'équation (4.12) avec $k'=k+u'+v'$ et $l'=l+u'-v'$ et $m'=m+u'$ pour calculer $\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})$. Il suffit d'inverser une matrice pour retrouver $\vartheta_i(\widetilde{x+y})\vartheta_j(\widetilde{x-y})$. ■

Dans le reste du chapitre on suppose que δ est divisible par un nombre pair $n \geqslant 4$, afin d'avoir des chaînes d'addition bien définies. (On verra dans la section 4.8 que généralement, comme on a juste $2 \mid \delta$ puisque $\mathcal{L}$ est totalement symétrique, on ne peut plus forcément calculer l'addition normale sur X, par contre on peut toujours calculer la pseudo-addition sur $\widetilde{X}$, sauf cas dégénéré.)

REMARQUE 4.4.7. Si on ne connait pas $\widetilde{x-y}$, on peut dans ce cas toujours prendre $j=0$, et trouver $\widetilde{x+y}$ à un facteur projectif près, autrement dit on peut calculer l'addition dans X (on l'appelle l'addition « normale »). Cependant, la méthode la plus efficace pour calculer une addition « normale » est de revenir aux formules du théorème 4.4.3 ; voir l'analyse de complexité 4.4.11 suivant l'algorithme 4.4.10. ◊

REMARQUE 4.4.8. Les formules d'addition prennent une forme plus agréable lorsqu'on utilise le changement de variable $U^{\mathcal{L}}$ [Mum66, p. 334-335] :

$$U^{\mathcal{L}}_i(\widetilde{x+y})U^{\mathcal{L}}_j(\widetilde{x-y})U^{\mathcal{L}}_k(\widetilde{0}_X)U^{\mathcal{L}}_l(\widetilde{0}_X) = \frac{1}{2^{2g}}\sum_{\substack{\xi\in\hat{Z}(\bar{2})\times Z(\delta)\\ 2\xi\in\{0\}\times Z(\bar{2})}}(m_2+\xi_2)(2\xi_1)U^{\mathcal{L}}_{i-m+\xi}(\widetilde{y})U^{\mathcal{L}}_{m-j+\xi}(\widetilde{y})U^{\mathcal{L}}_{m-k+\xi}(\widetilde{x})U^{\mathcal{L}}_{m-l+\xi}(\widetilde{x}). \quad (4.13)$$

Pour montrer que l'équation (4.13) détermine $\widetilde{x+y}$ uniquement, il faut juste vérifier que pour tout $(\chi_1,k)\in\hat{Z}(\bar{2})\times Z(\delta)$ et $(\chi_2,l)\in\hat{Z}(\bar{2})\times Z(\delta)$, il existe $\chi\in\hat{Z}(\bar{2})$, et $k',l'\in Z(\delta)$ tels que $k'+l'=2m'$, vérifiant : $U^{\mathcal{L}}_{\chi_1\chi,k+k'}(\widetilde{0}_X)U^{\mathcal{L}}_{\chi_2\chi,l+l'}(\widetilde{0}_X)\neq 0$. Si ce n'est pas le cas, on calcule pour tout $\chi\in\hat{Z}(\bar{2})$:

$$0 = U^{\mathcal{L}}_{\chi_1\chi,k}(\widetilde{0}_X)U^{\mathcal{L}}_{\chi_2\chi,l}(\widetilde{0}_X) = \sum_{t_1,t_2\in Z(\bar{2})}\chi(t_1+t_2)\chi_1(t_1)\chi_2(t_2)\vartheta_{k+t_1}(\widetilde{0}_X)\vartheta_{l+t_1}(\widetilde{0}_X)$$

En sommant sur $\chi\in\hat{Z}(\bar{2})$ on obtient :

$$\begin{aligned}0 &= \sum_{t_1,t_2\in Z(\bar{2})}\chi_1(t_1)\chi_2(t_2)\vartheta_{k+t_1}(\widetilde{0}_X)\vartheta_{l+t_1}(\widetilde{0}_X)\Big(\sum_{\chi\in\hat{Z}(\bar{2})}\chi(t_1+t_2)\Big)\\ &= 2^g\sum_{t\in Z(\bar{2})}\chi_1(t)\chi_2(t)\vartheta_{k+t}(\widetilde{0}_X)\vartheta_{l+t}(\widetilde{0}_X)\end{aligned}$$

Mais le théorème 4.4.4 montre qu'il existe $k',l'\in Z(\delta)$ tels que

$$\sum_{t\in Z(\bar{2})}\chi_1(t)\chi_2(t)\vartheta_{k+k'+l'+t}(\widetilde{0}_X)\vartheta_{l+k'-l'+t}(\widetilde{0}_X)\neq 0,$$

ce qui conclut (voir la preuve du théorème 4.4.6). ◊

EXEMPLE 4.4.9 (FORMULES D'ADDITION ANALYTIQUES). Soit $X=\mathbb{C}^g/(\Omega\mathbb{Z}^g+\mathbb{Z}^g)$ une variété abélienne complexe correspondant à $\Omega\in\mathfrak{H}_g$. Dans ce cas, on travaille sur le revêtement universel $\mathbb{C}^g$ plutôt que sur $\widetilde{X}$. Si $\mathcal{L}_0$ est le fibré principal canonique de caractéristique 0

associé à Ω, soit $\mathcal{L} = \mathcal{L}_0^n$ avec n un entier pair, $\mathcal{L}$ est de type $\overline{n}$. On a vu dans la section 2.6 qu'une base canonique de fonctions thêta était donnée par

$$\vartheta_i = \vartheta \begin{bmatrix} 0 \\ \frac{i}{n} \end{bmatrix} (\cdot, \frac{\Omega}{n})$$

On peut généraliser le changement de base donné dans la discussion suivant la proposition 2.6.1 ainsi : si $n = m_1 m_2$, une base des fonctions thêta est donnée par

$$\vartheta \begin{bmatrix} \frac{a}{m_1} \\ \frac{b}{m_2} \end{bmatrix} (m_1 z, m_1 \frac{\Omega}{m_2})$$

où $a \in Z(m_1), b \in Z(m_2)$. De plus, le changement de variable est donné, si on plonge $Z(m_1)$ et $Z(m_2)$ dans $Z(\overline{n})$, par

$$\vartheta \begin{bmatrix} \frac{a}{m_1} \\ \frac{b}{m_2} \end{bmatrix} (m_1 z, m_1 \frac{\Omega}{m_2}) = \sum_{j \in Z(m_1)} e^{2\pi i m_1^{-1}\, {}^t a(b+j)} \vartheta_{b+j}.$$

(Voir la remarque 2.6.3. Pour le changement de base, il suffit de reprendre la preuve de [Mum83, p. 124-125]).

En particulier, on trouve que $U^{\mathcal{L}}_{\chi,i}(z) = \vartheta \begin{bmatrix} \frac{\chi}{2} \\ \frac{i}{n} \end{bmatrix} (2z, 4\frac{\Omega}{n})$. Or on a $\vartheta_i^{\mathcal{L}^2}(z) = \vartheta \begin{bmatrix} 0 \\ \frac{i}{2n} \end{bmatrix} (z, \frac{\Omega}{2n})$, donc $U^{\mathcal{L}^2}_{\chi,i}(z) = \vartheta \begin{bmatrix} \frac{\chi}{2} \\ \frac{i}{2n} \end{bmatrix} (2z, 2\frac{\Omega}{n})$.

Dans ce cadre, la formule de duplication de l'équation (4.7) est donnée par [Igu72, Théorème 2 p. 139, p. 141] :

$$\vartheta \begin{bmatrix} 0 \\ \frac{i}{n} \end{bmatrix} (z_1 + z_2, \frac{\Omega}{n}) \vartheta \begin{bmatrix} 0 \\ \frac{j}{n} \end{bmatrix} (z_1 - z_2, \frac{\Omega}{n}) = \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \vartheta \begin{bmatrix} \frac{t}{2} \\ \frac{i+j}{2n} \end{bmatrix} (2z_1, 2\frac{\Omega}{n}) \vartheta \begin{bmatrix} \frac{t}{2} \\ \frac{i-j}{2n} \end{bmatrix} (2z_2, 2\frac{\Omega}{n})$$

$$\vartheta \begin{bmatrix} \chi/2 \\ i/(2n) \end{bmatrix} (2z_1, 2\frac{\Omega}{n}) \vartheta \begin{bmatrix} \chi/2 \\ j/(2n) \end{bmatrix} (2z_2, 2\frac{\Omega}{n}) =$$
$$\frac{1}{2^g} \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{-2i\pi\, {}^t \chi \cdot t} \vartheta \begin{bmatrix} 2\chi \\ \frac{i+j}{2n} + t \end{bmatrix} (z_1 + z_2, \frac{\Omega}{n}) \vartheta \begin{bmatrix} 0 \\ \frac{i-j}{2n} + t \end{bmatrix} (z_1 - z_2, \frac{\Omega}{n}).$$

Ainsi la pseudo-addition sur $\mathbb{C}^g$ est simplement l'addition dans $\mathbb{C}^g$!

De plus, i, j sont congruents modulo $Z(\overline{2})$, on peut interpréter les fonctions $\vartheta \begin{bmatrix} 0 \\ \frac{i+j}{2n} + t \end{bmatrix} (\frac{z_1+z_2}{2}, \frac{\Omega}{2n})$ soit comme des fonctions thêta de niveau $2n$ sur X, soit comme des fonctions thêta de niveau n sur $X' := \mathbb{C}^g/(\frac{1}{2}\Omega\mathbb{Z}^g + \mathbb{Z}^g)$. Ainsi les formules de duplication, outre l'addition et le doublement, permettent d'exprimer des 2-isogénies. On étendra ces idées dans la section 7.8.

Enfin, si par exemple $n = 4$, les variables $U_i^{\mathcal{L}}$ correspondent aux fonctions thêta [Mum83, p. 124-125] : $\vartheta \begin{bmatrix} i/2 \\ j/2 \end{bmatrix} (2\cdot, \Omega)$. Les formules d'addition correspondent aux classiques relations de Riemann [Mum83, p. 214] :

$$\vartheta \begin{bmatrix} a' \\ e' \end{bmatrix} (x+y) \vartheta \begin{bmatrix} b' \\ f' \end{bmatrix} (x-y) \vartheta \begin{bmatrix} c' \\ g' \end{bmatrix} (0) \vartheta \begin{bmatrix} d' \\ h' \end{bmatrix} (0) =$$
$$\frac{1}{2^g} \sum_{t_1, t_2 \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{2\pi i \beta'(a+b+c+d)} \vartheta \begin{bmatrix} a+t_1 \\ e+t_2 \end{bmatrix} (x) \vartheta \begin{bmatrix} b+t_1 \\ f+t_2 \end{bmatrix} (x) \vartheta \begin{bmatrix} c+t_1 \\ g+t_2 \end{bmatrix} (y) \vartheta \begin{bmatrix} d+t_1 \\ h+t_2 \end{bmatrix} (y)$$

Avec

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

$$a, b, c, d, e, f, g, h \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$$

$$(a', b', c', d') = A(a, b, c, d), (e', f', g', h') = A(e, f, g, h). \qquad \diamond$$

On vérifie immédiatement en regardant les relations d'addition (4.12) que $\widetilde{0}_X$ est un point neutre pour les pseudo-additions : si $\widetilde{x} \in \widetilde{X}$ est un point géométrique affine, alors

$$\texttt{chain\_add}(\widetilde{x}, \widetilde{0}_X, \widetilde{x}) = \widetilde{x}.$$

(De manière plus surprenante, un point géométrique quelconque de l'espace projectif où est plongé X par $\mathcal{L}$ satisfait ces relations si et seulement s'il est dans X, voir la section 4.7.)

L'équation (4.13) est commode pour l'étude théorique des pseudo-additions, mais l'équation (4.12) est mieux adaptée pour le calcul effectif (on somme sur 2^g éléments au lieu de 4^g). La formule de l'équation (4.12) nous permet de calculer les sommes $\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_i(x+y)\vartheta_i(x-y)$, que l'on peut combiner pour retrouver $\vartheta_i(x+y)\vartheta_i(x-y)$. En terme d'implémentation, le plus efficace pour calculer ainsi l'addition différentielle (ou l'addition normale) est de revenir aux formules de duplications du théorème 4.4.3. En effet, on peut voir la combinaison des équations (4.8) et (4.9) comme une manière de factoriser les relations d'addition. Pour obtenir la pseudo-addition sur le cône affine, il suffit d'utiliser les formules du théorème 4.4.3 avec $\lambda_1 = \lambda_2 = 1$ (ce qui explique pourquoi nous les avons énoncées sous cette forme).

ALGORITHME 4.4.10 (PSEUDO-ADDITION) :
On suppose qu'on a déjà effectué les précalculs suivants :

Précalculs Pour tout $\chi \in \hat{Z}(\overline{2})$:

$$U^{\mathcal{L}^2}_{\chi,0}(\widetilde{0}_X)^{-2} = \left(\sum_{t \in \hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_t(\widetilde{0}_X)\vartheta^{\mathcal{L}}_t(\widetilde{0}_X)\right)^{-1}.$$

Entrées Soit $\widetilde{x}, \widetilde{y}, \widetilde{x-y}$ des points géométriques de $\widetilde{X}$.
Sortie $\widetilde{x+y} := \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}_X)$.

➔ Pour tout $i \in Z(\delta)$

- Calculer pour tout $\chi \in \hat{Z}(\overline{2})$:

$$U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,0}(\widetilde{y}) = \frac{1}{U^{\mathcal{L}^2}_{\chi,0}(\widetilde{0}_X)^2}\left(\sum_{t \in \hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+t}(\widetilde{x})^2\right)\left(\sum_{t \in \hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_t(\widetilde{y})^2\right).$$

- Retourner

$$\vartheta^{\mathcal{L}}_i(\widetilde{x+y}) = \frac{1}{2^g\vartheta^{\mathcal{L}}_i(\widetilde{x-y})}\sum_{\chi \in \hat{Z}(\overline{2})} U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,0}(\widetilde{y}).$$

$\diamond$

ANALYSE DE COMPLEXITÉ 4.4.11. On a supposé dans l'algorithme que pour tout $\chi \in \hat{Z}(\overline{2})$,

$U^{\mathcal{L}^2}_{\chi,0}(\widetilde{0}_X) \neq 0$ et que pour tout $i \in Z(\delta)$, $\vartheta^{\mathcal{L}}_i(\widetilde{x-y}) \neq 0$. Dans le cas général, on peut procéder ainsi : pour tous $i, j \in Z(2\delta)$ congrus modulo $Z(\delta)$, alors par le théorème 4.4.4, pour tout $\chi \in \hat{Z}(\overline{2})$, il existe $u, v \in Z(2\delta)$ congrus à i, j modulo $Z(\delta)$ $U^{\mathcal{L}^2}_{\chi,u}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,v}(\widetilde{0}_X) \neq 0$. On peut alors calculer l'algorithme 4.4.10 en calculant

$$U^{\mathcal{L}^2}_{\chi,u}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,v}(\widetilde{0}_X) = \sum_{t\in\hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{u+v+t}(\widetilde{0}_X)\vartheta^{\mathcal{L}}_{u-v+t}(\widetilde{0}_X)$$

$$U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{y}) = \frac{1}{U^{\mathcal{L}^2}_{\chi,u}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,v}(\widetilde{0}_X)}$$
$$\left(\sum_{t\in\hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+u+t}(\widetilde{x})\vartheta^{\mathcal{L}}_{i-u+t}(\widetilde{x})\right)\left(\sum_{t\in\hat{Z}(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{j+v+t}(\widetilde{y})\vartheta^{\mathcal{L}}_{j-v+t}(\widetilde{y})\right).$$

$$\vartheta^{\mathcal{L}}_{i+j}(\widetilde{x+y})\vartheta^{\mathcal{L}}_{i-j}(\widetilde{x-y}) = \frac{1}{2^g}\sum_{\chi\in\hat{Z}(\overline{2})} U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x})U^{\mathcal{L}^2}_{\chi,j}(\widetilde{y})$$

On peut donc retrouver tous les $\vartheta^{\mathcal{L}}_i(\widetilde{x+y})\vartheta^{\mathcal{L}}_j(\widetilde{x-y})$, $i, j \in Z(\delta)$, et donc toujours calculer la pseudo-addition ou même l'addition normale.

Cependant la version de l'algorithme 4.4.10 est la plus efficace. Par exemple, en niveau n, pour calculer $\widetilde{x+y}$, on calcule les carrés des coefficients de $\widetilde{x}$, ainsi que les coefficients $\vartheta^{\mathcal{L}}_t(\widetilde{y})^2/U^{\mathcal{L}^2}_{\chi,0}(\widetilde{0}_X)^2$. Pour chaque coordonnée, on effectue ensuite une multiplication et une inversion, donc au total on a $n^g + 2^g$ carrés, $n^g + 2^g$ multiplications et n^g inversions (en niveau δ il suffit de remplacer n^g par $\#Z(\delta)$). Si on peut travailler sur les carrés des coordonnées (par exemple si on fait une multiplication, voir l'algorithme 4.4.12), on a juste n^g carrés, $n^g + 2^g$ multiplications et n^g inversions à prendre. On effectue également $O((4n)^g)$ additions. Enfin, la mémoire requise est en $O(n^g)$, donc linéaire en la taille de l'entrée et de la sortie.

Si on veut juste calculer une addition normale, on applique la méthode précédente pour calculer (par exemple) les $\vartheta^{\mathcal{L}}_i(\widetilde{x+y})\vartheta^{\mathcal{L}}_0(\widetilde{x-y})$, $i \in Z(\delta)$. Cette fois ci, comme $i \neq j$, il faut calculer les produits $\vartheta_{i+t}(\widetilde{x})\vartheta_t(\widetilde{x})$, $\vartheta_{i+t}(\widetilde{y})\vartheta_t(\widetilde{y})$ pour $i \in Z(\delta)$, $t \in Z(\overline{2})$, et 2 multiplications par coordonnée soit au total $2n^g(2^g+1)$ multiplications. (À comparer aux $3\cdot 2^g n^g$ multiplications et n^g multiplications par des constantes pour l'addition normale en utilisant l'équation (4.13)).

Une analyse plus fine sera effectuée dans l'exemple 4.8.9, où l'on prend en compte l'addition mixte. ♢

La pseudo-addition sur $\widetilde{X}$ permet de définir une multiplication par un scalaire au-dessus de la multiplication habituelle sur X. En effet, si on s'est fixé des points géométriques $\widetilde{x}$ et $\widetilde{y}$ dans X et un point $\widetilde{x+y}$ au-dessus de $x+y$, on peut définir récursivement pour $m \geqslant 1$:

$$\widetilde{mx+y} \coloneqq \texttt{chain\_add}((\widetilde{m-1)x}+y, \widetilde{x}, (\widetilde{m-2)x}+y)$$

On note $\texttt{chain\_multadd}(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y}) \coloneqq \widetilde{mx+y}$, la multiplication est alors donnée par :

$$m.\widetilde{x} \coloneqq \texttt{chain\_mult}(m, \widetilde{x}) \coloneqq \texttt{chain\_multadd}(m, \widetilde{x}, \widetilde{x}, \widetilde{0}_X).$$

(On peut étendre ces définitions à $m \in \mathbb{Z}$ en posant $\texttt{chain\_multadd}(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y}) \coloneqq \texttt{chain\_multadd}(-m, -\widetilde{x+y}, -\widetilde{x}, -\widetilde{y})$ si $m < 0$.) Il n'est pas clair que la multiplication par un scalaire affine soit associative. Tout ce qu'on peut dire, puisqu'elle releve la multiplication sur X, c'est qu'elle est associative à un facteur scalaire près. On verra qu'elle est effectivement associative dans le corollaire 4.5.6, et donc qu'on peut la calculer à partir de n'importe quelle

chaine de Lucas[1] de m.

On en déduit un algorithme du type « Montgomery » pour calculer la multiplication affine, en prenant une chaine de Lucas de la forme

$$L = \{0, 1, \dots, i, i+1, \text{soit } 2i, 2i+1, \text{soit } 2i+1, 2i+2, \dots, m\}$$

ALGORITHME 4.4.12 (MULTIPLICATION AFFINE) :
Entrée $m \in \mathbb{N}, \widetilde{x+y}, \widetilde{x}, \widetilde{y} \in \widetilde{A}_k$.
Sortie `chain_multadd`$(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y})$.

➔ Calculer la décomposition binaire $m := \sum_{i=0}^{I} b_i 2^i$. Faire $m' := 0$, $\mathsf{xy}_0 := \widetilde{y}$, $\mathsf{xy}_{-1} :=$ `chain_add`$(\widetilde{y}, -\widetilde{x}, \widetilde{x+y})$, $\mathsf{x}_0 := \widetilde{0}_{A_k}$ et $\mathsf{x}_1 := \widetilde{x}$.
➔ Pour `i` dans $[I..0]$ faire
Si $b_i = 0$ alors calculer

$$\begin{aligned} \mathsf{x}_{2m'} &:= \texttt{chain\_add}(\mathsf{x}_{m'}, \mathsf{x}_{m'}, \mathsf{x}_0) \\ \mathsf{x}_{2m'+1} &:= \texttt{chain\_add}(\mathsf{x}_{m'+1}, \mathsf{x}_{m'}, \mathsf{x}_1) \\ \mathsf{xy}_{2m'} &:= \texttt{chain\_add}(\mathsf{xy}_{m'}, \mathsf{x}_{m'}, \mathsf{xy}_0) \\ m' &:= 2m'. \end{aligned}$$

Sinon calculer

$$\begin{aligned} \mathsf{x}_{2m'+1} &:= \texttt{chain\_add}(\mathsf{x}_{m'+1}, \mathsf{x}_{m'}, \mathsf{x}_1) \\ \mathsf{x}_{2m'+2} &:= \texttt{chain\_add}(\mathsf{x}_{m'+1}, \mathsf{x}_{m'+1}, \mathsf{x}_0) \\ \mathsf{xy}_{2m'+1} &:= \texttt{chain\_add}(\mathsf{xy}_{m'}, \mathsf{x}_{m'}, \mathsf{xy}_{-1}) \\ m' &:= 2m' + 1. \end{aligned}$$

➔ Retourner xy_m. ◊

ANALYSE DE COMPLEXITÉ 4.4.13. Comme une pseudo-addition nécessite de diviser par les coordonnées de la différence, on prend une chaine de Mongomery afin que la différence soit toujours $\widetilde{y}$ ou $\widetilde{x+y}$, ce qui permet de minimiser le nombre d'inversions à calculer.

L'algorithme nécessite au plus $2\log(m)$ pseudo-additions de niveau δ, et de plus on peut travailler tout le long sur le carré des coordonnées, sauf à la dernière étape. Voir aussi la section 4.6 pour une amélioration de cet algorithme en remplaçant les pseudo-additions de niveau δ par des pseudo additions de niveau plus petit.

Enfin l'empreinte mémoire est linéaire en la taille de l'entrée ou de la sortie. ◊

4.5 ACTION DU GROUPE THÊTA SUR LES PSEUDO-ADDITIONS

Le but de cette section est d'étudier les propriétés de la pseudo-addition sur le cône affine $\widetilde{X}$ d'une variété abélienne polarisée $(X, \mathcal{L})$. Par exemple, comme on l'a remarqué à la section 4.4, montrer que la multiplication affine est associative directement s'avère très calculatoire (mais bien plus simple dans le cas complexe puisque la pseudo-addition est l'addition sur $\mathbb{C}^g$). De fait, nous adoptons la stratégie suivante : nous étudions l'effet de l'action du groupe thêta

1. Une chaine de Lucas pour m est un sous-ensemble $L \subset [0..m]$ tel que $\{0, 1, m\} \subset L$, et pour tout $I \in L$, il

sur les formules d'addition, ce qui me permettra de déterminer les relations d'addition sur des relevé affines canoniques de points de $K(\mathcal{L})$. Pour étendre cette étude à n'importe quel point de torsion de X, nous montrons ensuite que les formules d'addition commutent aux isogénies compatibles avec la thêta structure symétrique $\Theta_{\mathcal{L}}$ sur $\mathcal{L}$. Il suffit alors d'appliquer ce qui précède à des (relevé affines de) points de $K([\ell]^*\mathcal{L})$ et de les descendre par (un relevé affine de) $[\ell]$ pour obtenir des informations sur des (relevé affines de) points dans $K(\mathcal{L}^\ell)$.

Mais l'action de $G(\mathcal{L})$ est essentiellement de deux types différents (en plus de l'action de k^*) : il y a l'action de $\widetilde{K}_1(\mathcal{L})$ et l'action de $\widetilde{K}_2(\mathcal{L})$. De même, les isogénies compatibles avec $\Theta_{\mathcal{L}}$ sont des composées d'isogénies de type $\hat{Z}(\delta')$ et d'isogénies de type $Z(\delta')$ (voir l'exemple 3.6.5). Or si on change la thêta structure $\Theta_{\mathcal{L}}$ via l'automorphisme $\mathfrak{I}$ décrit à la section 3.5 qui permute les groupes de niveau $\widetilde{K}_1(\mathcal{L})$ et $\widetilde{K}_2(\mathcal{L})$, on transforme une isogénie de type $\hat{Z}(\delta')$ en une isogénie de type $Z(\delta')$ et réciproquement, et on permute les deux types d'action de $G(\mathcal{L})$ puisque $s_{K_2(\mathcal{L})} = \mathfrak{I} \circ s_{K_1(\mathcal{L})} \circ \mathfrak{I}$. On va donc se concentrer sur l'action de $\widetilde{K}_1(\mathcal{L})$, ainsi que sur l'action de $\mathfrak{I}$, ce qui nous permet d'appliquer les résultats précédents à l'action de $\widetilde{K}_2(\mathcal{L})$.

Tout d'abord, la relation entre l'action de $G(\mathcal{L})$ et l'inversion $\widetilde{[-1]}$ est facile :

LEMME 4.5.1. *Soit $(\alpha, i, j) \in \mathcal{H}(\delta)$ et $\widetilde{x}$ un point géométrique de $\widetilde{X}$. On a : $-((\alpha, i, j).\widetilde{x}) = (\alpha, -i, -j).(-\widetilde{x})$.*

DÉMONSTRATION : C'est une conséquence directe du fait qu'on ait une thêta structure symétrique, et que donc l'action de γ_{-1} commute avec la thêta structure. On peut aussi le vérifier directement : si $\widetilde{x} = (x_i)_{i\in Z(\delta)}$, on a donc $-\widetilde{x} = (x_{-i})_{i\in Z(\delta)}$. On vérifie alors lorsque $u \in Z(\delta)$, en utilisant l'équation (3.6) : $((\alpha, i, j).\widetilde{x})_u = \alpha\langle -u-i, j\rangle x_{u+i}$ tandis que $((\alpha, -i, -j).(-\widetilde{x}))_u = ((\alpha, -i, -j).\widetilde{x})_{-u} = \alpha\langle u+i, -j\rangle \widetilde{x}_{-u-i}$. ∎

On passe maintenant à l'étude de $\mathfrak{I}$ sur les relations d'addition. En fait on va l'étudier directement sur les relations de Riemann, ce qui nous donnera l'action de $\mathfrak{I}$ sur les formules d'addition comme corollaire immédiat comme il s'agit d'un cas particulier des relations de Riemann.

PROPOSITION 4.5.2. *Si on se donne des points géométriques affines $x, y, u, v, x', y', u', v' \in \widetilde{X}$ qui satisfont les relations de Riemann de l'équation (4.11), alors $\mathfrak{I}.x$, $\mathfrak{I}.y$, $\mathfrak{I}.u$, $\mathfrak{I}.v$, $\mathfrak{I}.x'$, $\mathfrak{I}.y'$, $\mathfrak{I}.u'$, et $\mathfrak{I}.v'$ satisfont également les relations de Riemann.*

DÉMONSTRATION : Si $x = (x_i)_{i\in Z(\delta)}$, on a vu que l'action de $\mathfrak{I}$ était donnée par l'équation (3.11) :

$$\mathfrak{I}.x = \Big(\sum_{j\in Z(\delta)} e_\delta(-i, j)x_j\Big)_{i\in Z(\delta)}.$$

(Ici nous nous sommes fixé une identification $Z(\delta) \xrightarrow{\sim} \hat{Z}(\delta)$, ce qui revient à choisir une racine primitive $d = \vee_{i=1}^g \delta_i$-ième de l'unité, et on note e_δ l'image du pairing canonique $\langle\cdot,\cdot\rangle$ sur $Z(\delta) \times Z(\delta)$, e_δ est un pairing symplectique de type δ).

Par hypothèse, pour tout $i, j, k, l \in Z(\delta)$ tels que $i + j + k + l = 2m$, on a :

$$\Big(\sum_{t\in Z(\bar{2})} \vartheta_{i+t}(x)\vartheta_{j+t}(y)\Big).\Big(\sum_{t\in Z(\bar{2})} \vartheta_{k+t}(u)\vartheta_{l+t}(v)\Big) = \Big(\sum_{t\in Z(\bar{2})} \vartheta_{i'+t}(x')\vartheta_{j'+t}(y')\Big).\Big(\sum_{t\in Z(\bar{2})} \vartheta_{k'+t}(u')\vartheta_{l'+t}(v')\Big). \quad (4.14)$$

existe $i, j \in L$ tels que $I = i + j$ et $i - j \in L$

On note $A_{\chi,x,y,i,j} = \big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{i+t}(x)\vartheta_{j+t}(y)\big)$. Si I, J, K, L, M sont dans $Z(\delta)$ et vérifient $I + J + K + L = 2M$, on calcule :

$$\begin{aligned} A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J} &= \sum_{T\in Z(\bar{2})} \chi(T)\Big(\sum_{i\in Z(\delta)} e_\delta(-I+T,i)\vartheta_i(x)\Big)\Big(\sum_{j\in Z(\delta)} e_\delta(-J+T,j)\vartheta_j(x)\Big) \\ &= \sum_{\substack{T\in Z(\bar{2})\\ i,j\in Z(\delta)}} \chi(T)e_\delta(T,i+j)e_\delta(I,i)e_\delta(J,j)\vartheta_i(x)\vartheta_j(y) \end{aligned}$$

Donc si on prend le produit on trouve :

$$\begin{aligned} A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J}A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L} &= \sum_{\substack{T_1,T_2\in Z(\bar{2})\\ i,j,k,l\in Z(\delta)}} \chi(T_1+T_2)e_\delta(T_1,i+j)e_\delta(T_2,k+l) \\ &\qquad e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l)\vartheta_i(x)\vartheta_j(y)\vartheta_k(u)\vartheta_l(v) \\ &= \sum_{i,j,k,l\in Z(\delta)} e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l)\vartheta_i(x)\vartheta_j(y)\vartheta_k(u)\vartheta_l(v) \\ &\qquad \Big(\sum_{T_1,T_2\in Z(\bar{2})} \chi(T_1+T_2)e_\delta(T_1,i+j)e_\delta(T_2,k+l)\Big) \quad (4.15) \end{aligned}$$

Or on a :

$$\Big(\sum_{T_1,T_2\in Z(\bar{2})} \chi(T_1+T_2)e_\delta(T_1,i+j)e_\delta(T_2,k+l)\Big) = \begin{cases} 4^g & \text{si } e_\delta(\cdot,i+j) = e_\delta(\cdot,k+l) = \chi \\ 0 & \text{sinon} \end{cases}$$

et de plus les caractères sur $Z(\bar{2})$, $e_\delta(\cdot, i+j)$ et $e_\delta(\cdot, k+l)$ sont égaux si et seulement si il existe $m \in Z(\delta)$ tel que $i+j+k+l = 2m$. Comme par hypothèse on a $I+J+K+L = 2M$, on a donc $e_\delta(I+J,\cdot) = e_\delta(K+L,\cdot)$, et si on regarde des tranches par $Z(\bar{2})$ de la somme (4.15) on trouve en utilisant l'équation (4.14) :

$$\lambda \sum_{t_1,t_2\in Z(\bar{2})} e_\delta(I,i+t_1)e_\delta(J,j+t_1)e_\delta(K,k+t_2)e_\delta(L,l+t_2)\vartheta_{i+t_1}(x)\vartheta_{j+t_1}(y)\vartheta_{k+t_2}(u)\vartheta_{l+t_2}(v) =$$

$$\lambda e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l)\sum_{t_1,t_2\in Z(\bar{2})} e_\delta(I+J,t_1)e_\delta(K+L,t_2)\vartheta_{i+t_1}(x)\vartheta_{j+t_1}(y)\vartheta_{k+t_2}(u)\vartheta_{l+t_2}(v) =$$

$$\lambda e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l)\sum_{t_1,t_2\in Z(\bar{2})} e_\delta(I+J,t_1)e_\delta(K+L,t_2)\vartheta_{i'+t_1}(x')\vartheta_{j'+t_1}(y')\vartheta_{k'+t_2}(u')\vartheta_{l'+t_2}(v') =$$

$$\lambda e_\delta(I',i')e_\delta(J',j')e_\delta(K',k')e_\delta(L',l')\sum_{t_1,t_2\in Z(\bar{2})} e_\delta(I+J,t_1)e_\delta(K+L,t_2)\vartheta_{i'+t_1}(x')\vartheta_{j'+t_1}(y')\vartheta_{k'+t_2}(u')\vartheta_{l'+t_2}(v') =$$

$$\lambda \sum_{t_1,t_2\in Z(\bar{2})} e_\delta(I',i'+t_1)e_\delta(J',j'+t_1)e_\delta(K',k'+t_2)e_\delta(L',l'+t_2)\vartheta_{i'+t_1}(x')\vartheta_{j'+t_1}(y')\vartheta_{k'+t_2}(u')\vartheta_{l'+t_2}(v')$$

où $\lambda = 4^g$ si $i+j+k+l = 2m$ et $\lambda = 0$ sinon. En effet, on a $I'+J'-I-J = 2M$ donc $e_\delta(I'+J',t_1) = e_\delta(I+J,t_1)$ et de même $e_\delta(K'+L',t_2) = e_\delta(K+L,t_2)$, et de plus

$$\begin{aligned} e_\delta(I',i')e_\delta(J',j')e_\delta(K',k')e_\delta(L',l') &= e_\delta(M,m)^4 \\ e_\delta(-M,i+j+k+l)e_\delta(I+J+K+L,-m)e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l)l &= \\ e_\delta(I,i)e_\delta(J,j)e_\delta(K,k)e_\delta(L,l). \end{aligned}$$

En combinant ces relations, on trouve donc

$$A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J}A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L} = A_{\chi,\mathfrak{I}.x',\mathfrak{I}.y',I',J'}A_{\chi,\mathfrak{I}.u',\mathfrak{I}.v',K,L}. \qquad \blacksquare$$

ce qui conclut la preuve.

On passe maintenant à l'étude de l'action $G(\mathcal{L})$ sur les relations d'addition. Si on prend comme dans la proposition 4.5.2 des points géométriques affines $x, y, u, v, x', y', u', v' \in \widetilde{X}$ qui satisfont les relations de Riemann, alors si $g \in G(\mathcal{L})$, $g.x, g.y, g.u, g.v, g.x', g.y', g.u'$, $g.v'$ satisfont toujours les relations de Riemann comme on le constate facilement par un changement de variable. On a donc une compatibilité entre les relations de Riemann et l'action du groupe thêta (qui n'est pas surprenante puisque les relations de Riemann sont obtenues via les formules de duplication qui résultent du théorème de l'isogénie). Cependant cette forme n'est pas suffisante pour étudier les relations d'addition car on doit fixer le point $u = v = \widetilde{0}_X$ dans ce cas.

L'action de k^* sur les relations d'addition est immédiate :

LEMME 4.5.3. *Soit $\widetilde{x}, \widetilde{y}$ des points affines sur $\widetilde{X}$, et $\lambda_0, \lambda_x, \lambda_y, \lambda_{x-y} \in \overline{k}^*$, on a :*

$$\texttt{chain\_add}(\lambda_x\widetilde{x}, \lambda_y\widetilde{y}, \lambda_{x-y}\widetilde{x-y}, \lambda_0\widetilde{0}_X) = \frac{\lambda_x^2\lambda_y^2}{\lambda_{x-y}\lambda_0^2}\,\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}_X), \tag{4.16}$$

$$\texttt{chain\_multadd}(n, \lambda_{x+y}\widetilde{x+y}, \lambda_x\widetilde{x}, \lambda_y\widetilde{y}, \lambda_0\widetilde{0}_X) = \frac{\lambda_x^{n(n-1)}\lambda_{x+y}^n}{\lambda_y^{n-1}\lambda_0^{n(n-1)}}\,\texttt{chain\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y}, \widetilde{0}_X), \tag{4.17}$$

$$\texttt{chain\_mult}(n, \lambda_x\widetilde{x}, \lambda_0\widetilde{0}_X) = \frac{\lambda_x^{n^2}}{\lambda_0^{n^2-1}}\,\texttt{chain\_mult}(n, \widetilde{x}, \widetilde{0}_X). \tag{4.18}$$

DÉMONSTRATION : L'équation (4.16) découle immédiatement des formules d'addition (4.12), et le reste découle par induction. ∎

Ce qui va se révéler plus intéressant est la compatibilité des formules d'addition avec l'action des groupes de niveau induits par la thêta structure :

PROPOSITION 4.5.4. *Soit $\widetilde{x}, \widetilde{y}, \widetilde{x-y}$ dans $\widetilde{X}$, et (i_1, i_2) et $(j_1, j_2) \in K(\delta)$. On a :*

$$(1, i_1 + j_1, i_2 + j_2).\,\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}) = \texttt{chain\_add}((1, i_1, i_2).\widetilde{x}, (1, j_1, j_2).\widetilde{y}, (1, i_1 - j_1, i_2 - j_2).\widetilde{x-y}). \tag{4.19}$$

Et plus généralement si $g_1 = \Theta_{\mathcal{L}}(\alpha, i_1, i_2)$ et $g_2 = \Theta_{\mathcal{L}}(\beta, j_1, j_2)$ on a

$$g_1g_2.\,\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}) = \frac{\langle j_1, j_2\rangle}{\beta^2}\,\texttt{chain\_add}(g_1.\widetilde{x}, g_2.\widetilde{y}, g_1g_2^{-1}\widetilde{x-y}). \tag{4.20}$$

DÉMONSTRATION : Soit $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y})$. Les formules d'addition (4.12) nous disent que pour tous $a, b, c, d, e \in Z(\delta)$ tels que $a + b + c + d = 2e$:

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{a+t}(\widetilde{x+y})\vartheta_{b+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big) = \Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{-e+a+t}(\widetilde{y})\vartheta_{e-b+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{e-c+t}(\widetilde{x})\vartheta_{e-d+t}(\widetilde{x})\Big). \tag{4.21}$$

Si l'on fait le changement de variable $a = a' + i + j, b = b' + i - j, c = c', d = d', e = e' + i$

dans l'équation (4.21) on trouve

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+j+a+t}(\widetilde{x+y})\vartheta_{b+i-j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big) = \Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{-j-e+a+t}(\widetilde{y})\vartheta_{j+e-b}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+e-c+t}(\widetilde{x})\vartheta_{i+e-d+t}(\widetilde{x})\Big). \quad (4.22)$$

Et donc les points $(1, i+j, 0).\widetilde{x+y}$, $(1, i, 0).\widetilde{x}$, $(1, j, 0).\widetilde{y}$ et $(1, i-j, 0).\widetilde{x-y}$ satisfont les relations d'addition.

Maintenant, en appliquant la proposition 4.5.2, on obtient également que les points

$$(1, 0, i+j).\widetilde{x+y}, (1, 0, i).\widetilde{x}, (1, 0, j).\widetilde{y} \text{ et } (1, 0, i-j).\widetilde{x-y}$$

satisfont les relations d'addition. L'équation (4.19) découle de ces deux relations appliquées successivement puisqu'on a $(1, i, j) = (1, 0, j).(1, i, 0)$.

Finalement, l'équation (4.20) découle des équations (4.16) et (4.19) puisque

$$(\alpha, i_1, i_2).(\beta, j_1, j_2) = (\alpha\beta\langle i_1, j_2\rangle, i_1+j_1, i_2+j_2) \text{ et}$$
$$(\alpha, i_1, i_2).(\beta, j_1, j_2)^{-1} = (\frac{\alpha}{\beta}\langle j_1-i_1, j_2\rangle, i_1-j_1, i_2-j_2).$$ ■

En appliquant la même méthode, on trouve que les formules d'addition sont compatibles avec les isogénies :

PROPOSITION 4.5.5. *Soit $\pi : (X, \mathcal{L}) \to (Y, \mathcal{M})$ une isogénie entre variétés abéliennes polarisées et totalement symétriques, munies de thêta structures $\Theta_{\mathcal{L}}$ et $\Theta_{\mathcal{M}}$ symétriques et π-compatibles. Supposons fixé un système de coordonnées affines sur $\widetilde{X}$ et $\widetilde{Y}$, les cônes affines de X et Y et soit $\widetilde{\pi}$ le relevé canonique de π. Supposons de plus qu'on ait choisi les thêtas null points affines $\widetilde{0}_X$ et $\widetilde{0}_Y$ de telle sorte que $\widetilde{0}_Y = \widetilde{\pi}(\widetilde{0}_X)$.*

Alors si on prend des points affines $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x-y}$ dans $\widetilde{X}$, on a

$$\widetilde{\pi}(\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y})) = (\texttt{chain\_add}(\widetilde{\pi}(\widetilde{x}), \widetilde{\pi}(\widetilde{y}), \widetilde{\pi}(\widetilde{x-y}))).$$

DÉMONSTRATION : Soit $\delta = \delta_0\delta'$, et supposons que π soit de type $\hat{Z}(\delta')$ (voir l'exemple 3.6.5). Alors $\mathcal{M}$ est de niveau δ_0 et si $\widetilde{x} = (x_i)_{i\in Z(\delta)}$, on a $\widetilde{\pi}(\widetilde{x}) = (x_i)_{i\in Z(\delta_0)}$.

Si on se donne des points géométriques $x, y, u, v, x', y', u', v'$ sur $\widetilde{X}$, les relations de Riemann sur $\widetilde{\pi}(x), \widetilde{\pi}(y), \widetilde{\pi}(u), \widetilde{\pi}(v), \widetilde{\pi}(x'), \widetilde{\pi}(y'), \widetilde{\pi}(u'), \widetilde{\pi}(v')$, forment un sous-ensemble des relations de Riemann sur $x, y, u, v, x', y', u', v'$. Donc si $x, y, u, v, x', y', u', v'$ satisfont ces relations, $\widetilde{\pi}(x), \widetilde{\pi}(y), \widetilde{\pi}(u), \widetilde{\pi}(v), \widetilde{\pi}(x'), \widetilde{\pi}(y'), \widetilde{\pi}(u'), \widetilde{\pi}(v')$ également.

Maintenant, si π est de type $Z(\delta')$, alors π est de type $\hat{Z}(\delta')$ par rapport aux thêta structures $\Theta_{\mathcal{L}} \circ \mathfrak{I}_\delta$ et $\Theta_{\mathcal{M}} \circ \mathfrak{I}_{\delta_0}$ (où $\mathfrak{I}_\delta$ signifie qu'on prend l'automorphisme de permutation de $Z(\delta)$ et $\hat{Z}(\delta)$ sur $K(\delta)$). Par la proposition 4.5.2, on en déduit que $\widetilde{\pi}$ est encore compatible aux relations de Riemann, et en considérant les composées de deux isogénies on voit que c'est encore le cas pour des isogénies compatibles quelconques, ce qui finit la preuve puisque les formules d'addition sont un cas particulier des relations de Riemann (mais on voit l'importance de bien prendre $\widetilde{0}_Y = \widetilde{\pi}(\widetilde{0}_X)$). ■

COROLLAIRE 4.5.6. *Soit $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x+y}$ des points affines dans $\widetilde{X}$, et tels que x soit un point de ℓ-torsion, où ℓ ne divise pas la caractéristique p de k. Pour tout $n \in \mathbb{Z}$, on pose $\widetilde{nx} =$ $\texttt{chain\_mult}(n, \widetilde{x})$ et $\widetilde{nx+y} = \texttt{chain\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y})$.*

1. *Pour tout $n \in \mathbb{Z}$, on a*

$$-\widetilde{nx+y} = \texttt{chain\_add}(n, -(\widetilde{x+y}), -\widetilde{x}, -\widetilde{y})$$

2. *Pour tous $n_1, n_2 \in \mathbb{Z}$, on a*

$$(\widetilde{n_1+n_2})x = \texttt{chain\_add}(\widetilde{n_1 x}, \widetilde{n_2 x}, (\widetilde{n_1-n_2})x), \tag{4.23}$$

$$(\widetilde{n_1+n_2)x}+y = \texttt{chain\_add}(\widetilde{n_1 x+y}, \widetilde{n_2 x}, (\widetilde{n_1-n_2)x}+y). \tag{4.24}$$

En particulier, on voit que le calcul de $\widetilde{nx+y}$ et $\widetilde{nx}$ ne dépend pas de la séquence de Lucas utilisée pour les calculer via `chain_add`.

Démonstration : On prend une thêta structure sur $(X, [\ell]^*\mathcal{L})$ compatible avec la thêta structure $\Theta_{\mathcal{L}}$ sur $(X, \mathcal{L})$. On choisit un système de coordonnées affines sur $(X, \mathcal{L}^{\ell^2})$, et si $\widetilde{[\ell]}$ représente l'extension canonique de $[\ell]$ par rapport à ce système de coordonnées, on prend pour relevé affine du thêta null point sur $(X, \mathcal{L}^{\ell^2})$ l'unique relevé $\widetilde{0}_{X,\ell}$ tel que $\widetilde{[\ell]}\widetilde{0}_{X,\ell} = \widetilde{0}_X$. Le fibré $\mathcal{L}^{\ell^2}$ est de niveau $\ell^2\delta$, et si $\widetilde{x}_0$ est dans $\widetilde{[\ell]}^{-1}(\widetilde{x})$, comme x est un point de ℓ-torsion, il existe $(\alpha, i, j) \in H(\ell^2\delta)$ tels que $\widetilde{x}_0 = (\alpha, i, j).\widetilde{0}_{X,\ell}$. De plus, $\langle i, j\rangle = 1$.

Soit $\widetilde{y}_0$ un point de $\widetilde{[\ell]}^{-1}(\widetilde{y})$, et $\widetilde{x+y}_0$ un point de $\widetilde{[\ell]}^{-1}(\widetilde{x+y})$. Le lemme 4.5.3 montre que les formules du corollaire 4.5.6 sont homogènes sous l'action de k^*. On peut donc supposer que $\alpha = 1$ et $\widetilde{x+y}_0 = (1, i, j).\widetilde{y}_0$. En combinant les propositions 4.5.4 et 4.5.5, une récurrence immédiate nous donne, si $n > 0$ que $\widetilde{nx+y} = \widetilde{[\ell]}(1, ni, nj).\widetilde{y}_0$. Mais le lemme 4.5.1 montre que c'est également valable pour $n < 0$.

On calcule donc, toujours en utilisant les propositions 4.5.4 et 4.5.5 :

$$\begin{aligned}
&\texttt{chain_add}(\widetilde{n_1x+y}, \widetilde{n_2x}, (\widetilde{n_1-n_2)x}+y) = \\
&\quad \widetilde{[\ell]}\,\texttt{chain_add}((1, n_1i, n_1j).\widetilde{y}_0, (1, n_2i, n_2j).\widetilde{0}_{X,\ell}, (1, n_1-n_2i, n_1-n_2j).\widetilde{y}_0) = \\
&\qquad \widetilde{[\ell]}(1, (n_1+n_2)i, (n_1+n_2)j)\,\texttt{chain_add}(\widetilde{y}_0, \widetilde{0}_{X,\ell}, \widetilde{y}_0) = \\
&\qquad\qquad \widetilde{[\ell]}(1, (n_1+n_2)i, (n_1+n_2)j)\widetilde{y}_0 = (\widetilde{n_1+n_2)x}+y.
\end{aligned}$$

De même, en utilisant de plus le lemme 4.5.1 :

$$\begin{aligned}
-\widetilde{nx+y} &= -\widetilde{[\ell]}\,((1, ni, nj).\widetilde{y}_0) \\
&= \widetilde{[\ell]}\,(-(1, ni, nj).\widetilde{y}_0) \\
&= \widetilde{[\ell]}\,((1, -ni, -nj). -\widetilde{y}_0) \\
&= -\widetilde{nx-y}.
\end{aligned}$$

(Dans le cas général, des essais avec Magma montrent que le corollaire 4.5.6 reste vrai. Si $k = \mathbb{C}$, il est facile de le montrer : si on prend pour $\widetilde{x}$ et $\widetilde{y}$ et $\widetilde{x+y}$ les relevés donnés par les fonctions thêta analytiques, alors les relations de Riemann donnent l'addition sur $\mathbb{C}^g$, et on obtient bien l'associativité. Il suffit ensuite de vérifier grâce au lemme 4.5.3 que l'associativité reste vérifiée lorsqu'on introduit des facteurs projectifs.) ■

4.6 COMPRESSION DES COORDONNÉES

Soit $(X, \mathcal{L})$ une variété abélienne polarisée totalement symétrique de type δ munie d'une théta structure symétrique $\Theta_{\mathcal{L}}$. Si $\delta = \delta'\delta_0$, on va appliquer les résultats de la section 4.5 à l'isogénie de type $\hat{Z}(\delta')$ de l'exemple 3.6.5.

Soit $\pi : (X, \mathcal{L}) \to (Y, \mathcal{M})$ l'isogénie de type $\hat{Z}(\delta')$, $\Theta_{\mathcal{M}}$ la théta structure sur $\mathcal{M}$ π-compatible avec $\Theta_{\mathcal{L}}$, et $\widetilde{\pi} : \widetilde{X} \to \widetilde{Y}$ le relevé canonique de π par rapport à un système de coordonnées affines sur $\widetilde{X}$ et $\widetilde{Y}$. Le théorème 3.6.4 nous dit que

$$\widetilde{\pi}((x_i)_{i\in Z(\delta)}) = (x_i)_{i\in Z(\delta_0)}.$$

Enfin, on se fixe des relevés affines des théta null points $\widetilde{0}_X$ et $\widetilde{0}_Y$ tels que $\widetilde{\pi}(\widetilde{0}_X) = \widetilde{0}_Y$. Soit $(a_i)_{i\in Z(\delta)}$ les coordonnées de $\widetilde{0}_X$ et $(b_i)_{i\in Z(\delta_0)}$ celles de $\widetilde{0}_Y$.

Le noyau K de π est donné par $\overline{\Theta}_{\mathcal{L}}(\hat{Z}(\delta'))$, son orthogonal dans $K(\mathcal{L})$ est donc $\overline{\Theta}_{\mathcal{L}}(Z(\delta_0)\times \hat{Z}(\delta))$. Explicitement, on a en utilisant l'équation (3.6),

$$K = \{(\langle i, -j\rangle a_i)_{i\in Z(\delta)}\}_{j\in\hat{Z}(\delta')}.$$

Si $(i, j) \in Z(\delta_0) \times \hat{Z}(\delta)$, on a par compatibilité de $\Theta_{\mathcal{L}}$ avec $\Theta_{\mathcal{M}}$

$$\widetilde{\pi}((\alpha, i, j).\widetilde{x}) = (\alpha, i, \sigma(j)).\widetilde{\pi}(\widetilde{x}) \tag{4.25}$$

où $\sigma : \hat{Z}(\delta) \to \hat{Z}(\delta_0)$ de noyau $\hat{Z}(\delta')$ est le dual de l'inclusion $Z(\delta_0) \to Z(\delta)$. On pose alors, si $i \in Z(\delta)$, et $\widetilde{x}$ est un point géométrique de $\widetilde{X}$:

$$\widetilde{\pi}_i(\widetilde{x}) = \widetilde{\pi}((1, i, 0).\widetilde{x}). \tag{4.26}$$

Et de même on note si x est un point géométrique de X, $\pi_i(x) = \pi((1, i, 0).x) = \pi(x + \overline{\Theta}_{\mathcal{L}}(i, 0))$.

L'équation (4.25) montre que la connaissance des $(\widetilde{\pi}_i(\widetilde{x}))_{i\in Z(\delta)}$ permet de retrouver $\widetilde{\pi}(g.\widetilde{x})$ où g est un élément quelconque de $G(\mathcal{L})$ via

$$\widetilde{\pi}((\alpha, i, j).\widetilde{x}) = (\alpha, 0, \sigma(j)).\widetilde{\pi}_i(\widetilde{x}) = (\alpha\langle l, -j\rangle_\delta \vartheta_l(\widetilde{\pi}_i(\widetilde{x}))_{l\in Z(\delta_0)}.$$

De plus, si $i_0 \in Z(\delta_0)$, on a

$$\widetilde{\pi}_{i+i_0}(\widetilde{x}) = (1, i_0, 0).\widetilde{\pi}_i(\widetilde{x}) = (\vartheta_{l+i_0}(\widetilde{\pi}_i(\widetilde{x})))_{l\in Z(\delta_0)}. \tag{4.27}$$

Donc si δ' est premier avec δ_0 (c'est-à-dire que leurs indices sont premiers entre eux), on a juste besoin de connaître $(\widetilde{\pi}_i(\widetilde{x}))_{i\in Z(\delta')}$ pour retrouver tous les $(\widetilde{\pi}_i(\widetilde{x}))_{i\in Z(\delta)}$.

EXEMPLE 4.6.1. Prenons $g = 1$, $\delta = 12$ et $\delta_0 = 4$, donc $\delta' = 3$. Le sous-groupe $\mathbb{Z}/3Z \subset \mathbb{Z}/12\mathbb{Z}$ est donné par $\{0, 4, 8\}$. Si $\widetilde{x} = (\widetilde{x}_0, \widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3, \widetilde{x}_4, \widetilde{x}_5, \widetilde{x}_6, \widetilde{x}_7, \widetilde{x}_8, \widetilde{x}_9, \widetilde{x}_{10}, \widetilde{x}_{11})$, on a

$$\begin{aligned}
\widetilde{\pi}_0(\widetilde{x}) &= (\widetilde{x}_0, \widetilde{x}_3, \widetilde{x}_6, \widetilde{x}_9)\\
\widetilde{\pi}_4(\widetilde{x}) &= (\widetilde{x}_4, \widetilde{x}_7, \widetilde{x}_{10}, \widetilde{x}_1)\\
\widetilde{\pi}_8(\widetilde{x}) &= (\widetilde{x}_8, \widetilde{x}_{11}, \widetilde{x}_2, \widetilde{x}_5)
\end{aligned}$$ ◇

On voit qu'on peut entièrement reconstituer $\widetilde{x}$ à partir de $(\widetilde{\pi}_i(\widetilde{x}))_{i\in Z(\delta')}$. En revanche, si $x = p_X(\widetilde{x})$, la connaissance seule des $\pi_i(x)$ ne permet pas de reconstituer x à cause des facteurs projectifs. C'est là tout l'intérêt de travailler sur le cône affine et de considérer l'action du groupe thêta $G(\mathcal{L})$ plutôt que la simple action par translation de $K(\mathcal{L})$: on garde trace de l'action de k^*.

L'exemple 4.6.1 se généralise bien.

PROPOSITION 4.6.2. *En gardant les mêmes notations, on a :*

1. *Les points géométriques $\widetilde{y} \in \widetilde{X}$ tels que $\widetilde{\pi}(\widetilde{y}) = \widetilde{\pi}(\widetilde{x})$, sont donnés par l'ensemble*

$$\{(1,0,j).x\}_{j\in\hat{Z}(\delta')}.$$

En particulier, pour un tel $\widetilde{y}$ qui correspond à un $j \in \hat{Z}(\delta')$, on a si $i \in Z(\delta)$:

$$\widetilde{\pi}_i(\widetilde{y}) = \langle i, j\rangle \widetilde{\pi}_i(\widetilde{x})$$

et donc $\widetilde{\pi}_i(\widetilde{y})$ et $\widetilde{\pi}_i(\widetilde{x})$ diffèrent par une racine ℓ-ième de l'unité, où $\ell = \vee_{i=1}^{g}\delta'_i$.

2. *Soit $\mathcal{S}$ un sous-ensemble de $Z(\delta)$ tel que $\mathcal{S} + Z(\delta_0) = Z(\delta)$. Si δ' est premier avec δ_0, on peut prendre pour $\mathcal{S}$ le sous-groupe $Z(\delta') \subset Z(\delta)$. Alors si $\widetilde{x} \in \widetilde{X}$ est un point géométrique, il est uniquement déterminé par*

$$\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathcal{S}}.$$

DÉMONSTRATION : On prouve les deux points :

1. C'est un cas particulier de la remarque 4.4.1. Comme la forme de $\widetilde{\pi}$ est simple, on peut aussi le vérifier directement. Si $\widetilde{\pi}(y) = \widetilde{\pi}(x)$, alors $\pi(x) = \pi(y)$ où $x = p_X(\widetilde{x})$ et $y = p_X(\widetilde{y})$, donc $x - y \in K = \operatorname{Ker}\pi$. Il existe alors $j \in \hat{Z}(\delta')$ et $\alpha \in k^*$ tel que $\widetilde{y} = (\alpha, 0, j).\widetilde{x}$. Or comme $\widetilde{\pi}((1,0,j).\widetilde{x}) = \widetilde{\pi}(\widetilde{x})$ comme le montre l'équation (4.25), on a $\alpha = 1$. Le reste découle directement de l'équation (4.25).
2. Sur les coordonnées affines de $\widetilde{x}$, on a $\widetilde{\pi}_i((\vartheta_j^{\widetilde{X}}(\widetilde{x}))_{j\in Z(\delta)}) = (\vartheta_{i+j}^{\widetilde{Y}}(\widetilde{x}))_{j\in Z(\delta_0)}$. Donc si on connait $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathcal{S}}$, on retrouve les valeurs $\left\{\vartheta_j^{\widetilde{X}}(\widetilde{x})\right\}_{j\in\mathcal{S}+Z(\delta_0)}$. Si $\mathcal{S} + Z(\delta_0) = Z(\delta)$, on récupère donc $\widetilde{x} = (\vartheta_j^{\widetilde{X}}(\widetilde{x}))_{j\in Z(\overline{\ell n})}$. ■

Dans le cas général où δ' n'est pas premier avec δ_0, on prend usuellement $\mathcal{S} = [0, \delta'_1 - 1] \times [0, \delta'_2 - 1] \times \cdots \times [0, \delta'_g - 1]$. Visualiser $\widetilde{x}$ comme $(\widetilde{\pi}_i(\widetilde{x}))_{i\in\mathcal{S}}$ peut ne pas sembler intéressant, étant donné que la deuxième écriture est juste une permutation des coordonnées de $\widetilde{x}$. Cependant, tout l'intérêt du terme de droite vient de la

PROPOSITION 4.6.3. *Toujours en conservant les mêmes notations, si $\widetilde{x}$ est un point géométrique de $\widetilde{X}$, et $i, j \in Z(\overline{\ell n})$, on a :*

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_X), \widetilde{\pi}_{i-j}(\widetilde{x}), \widetilde{0}_X).$$

DÉMONSTRATION : Il suffit d'appliquer la proposition 4.5.4 à l'équation

$$\widetilde{x} = \texttt{chain\_add}(\widetilde{x}, \widetilde{0}_X, \widetilde{x}, \widetilde{0}_X).$$ ■

Pour exploiter la proposition 4.6.3, on introduit la terminologie suivante :

DÉFINITION 4.6.4. Soit $S \subset G$ un sous-ensemble d'un groupe fini abélien G tel que l'élément neutre 0_G soit dans S. On note S' le plus petit sous-ensemble de G qui contient S et vérifie la propriété $S' = S' \bigcup \{x + y | x \in S', y \in S', x - y \in S'\}$. On dit que S est une base différentielle de G si $S' = G$.

Si G' est un sous-groupe de G, on dit que S est une base différentielle de G relativement à G' si $S' + G' = G$. ◇

Exemple 4.6.5. Si $\{e_1, \dots, e_g\}$ est la base canonique de $Z(\delta)$, une base différentielle de $Z(\delta)$ est donnée par

$$\mathfrak{S} \coloneqq \{ \sum_{\epsilon \in \{0,1\}^g} \epsilon_i e_i \}.$$

Si toutes les coordonnées de δ' sont impaires (on dit que δ' est totalement impair), une base différentielle de $Z(\delta)$ relativement à $Z(\delta_0)$ est donnée par

$$\mathfrak{S} \coloneqq \{e_1, \dots, e_g, e_1 + e_2, \dots, e_1 + e_g, e_2 + e_3, \dots, e_{g-1} + e_g\}.$$

Si δ' est premier à δ_0, on préfère considérer des bases différentielles pour $Z(\delta')$ (qui seront donc différentielles pour $Z(\delta)$ relativement à $Z(\delta_0)$) données par

$$\mathfrak{S} \coloneqq \{ \sum_{\epsilon \in \{0,1\}^g} \epsilon_i d_i \}$$

dans le cas général et par

$$\mathfrak{S} \coloneqq \{d_1, \dots, d_g, d_1 + d_2, \dots, d_1 + d_g, d_2 + d_3, \dots, d_{g-1} + d_g\}$$

si δ' est totalement impair. Ici, $d_i = \delta_{0,i} e_i$ pour $i \in [1..g]$, donc $(d_i)_{i \in [1..g]}$ est la base canonique de $Z(\delta') \subset Z(\delta)$. ◇

On en déduit donc le

Corollaire 4.6.6 (Compression des coordonnées). *Soit $\mathfrak{S}$ une base différentielle de $Z(\delta)$ relativement à $Z(\delta_0)$. Alors un point géométrique $\widetilde{x} \in \widetilde{X}$ est entièrement déterminé par $\widetilde{0}_X$ et $(\widetilde{\pi}_i(\widetilde{x}))_{i \in \mathfrak{S}}$. Le thêta null point affine $\widetilde{0}_X$ est entièrement déterminé par $(\widetilde{\pi}_i(\widetilde{0}_X))_{i \in \mathfrak{S}}$.*

Démonstration : Si on connait $\widetilde{\pi}_i(\widetilde{x})$, on connait $\widetilde{\pi}_{i+i_1}(\widetilde{x})$ pour tout $i_0 \in Z(\delta_0)$ par l'équation (4.27). Si on connait $\widetilde{\pi}_i(\widetilde{x})$, $\widetilde{\pi}_j(\widetilde{0}_X)$ et $\widetilde{\pi}_{i-j}(\widetilde{x})$, on connait $\widetilde{\pi}_{i+j}(\widetilde{x})$ par la proposition 4.6.3. Le corollaire 4.6.6 s'en déduit immédiatement par définition de $\mathfrak{S}$. ■

On en déduit les algorithmes suivants pour compresser/décompresser les points :

Algorithme 4.6.7 (Compression des coordonnées) :
Entrée $\widetilde{x} = (\widetilde{\vartheta}_i(\widetilde{x}))_{i \in Z(\delta)} \in \widetilde{X}$
Sortie Les coordonnées compressées $(\widetilde{\pi}_i(\widetilde{x}))_{i \in \mathfrak{S}}$.

- ➔ Pour tout $i \in \mathfrak{S}$, calculer $\widetilde{\pi}_i(\widetilde{x}) = (\widetilde{\vartheta}_{ni+\ell j}(\widetilde{x}))_{j \in Z(\delta_0)}$.
- ➔ Retourner $(\widetilde{\pi}_i(\widetilde{x}))_{i \in \mathfrak{S}}$. ◇

Algorithme 4.6.8 (Décompression des coordonnées) :
Soit $\mathcal{S}$ comme défini dans la proposition 4.6.2.

Entrée Les coordonnées compressées $\widetilde{\pi}(\widetilde{x})_{i \in \mathfrak{S}}$ de $\widetilde{x} \in \widetilde{X}$.
Sortie $\widetilde{x} = (\widetilde{\vartheta}_i(\widetilde{x}))_{i \in Z(\delta)}$.

- ➔ Soit $\mathcal{S}' \coloneqq \mathfrak{S}$.
- ➔ Tant que $\mathcal{S}' \neq \mathcal{S}$.
  - Choisir $i, j \in \mathcal{S}'$ tels que $i + j \in \mathcal{S} \setminus \mathcal{S}'$ et $i - j \in \mathcal{S}'$.
  - Calculer $\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_X), \widetilde{\pi}_{i-j}(\widetilde{x}))$.
  - $\mathcal{S}' \coloneqq \mathcal{S}' \cup \{i + j\}$.

➔ Pour tout $i \in Z(\delta)$, écrire $i = i_0 + i_1$ où $i_0 \in Z(\delta_0)$ et $i_1 \in \mathcal{S}$ et retourner $\vartheta_i(x) = (\widetilde{\pi}_{i_1}(\widetilde{x}))_{i_0}$. ◇

ANALYSE DE COMPLEXITÉ 4.6.9. La décompression nécessite $\#\mathcal{S} - \#\mathfrak{S} = O(\#Z(\delta))$ pseudo additions de niveau δ_0.

Le point compressé $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathfrak{S}}$ est donné par $\#\mathfrak{S} \times \#Z(\delta_0)$ coordonnées, à comparer avec les $\#Z(\delta) = \#\mathcal{S} \times \#Z(\delta_0)$ coordonnées pour $\widetilde{x}$. ◇

REMARQUE 4.6.10 (ADDITION SUR LES COORDONNÉES COMPRESSÉES). Les coordonnées compressées sont très pratiques car elles sont suffisantes pour calculer les pseudo-additions. En effet, si on prend $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x-y}$ des points géométriques de $\widetilde{X}$, et que l'on a les coordonnées compressées $(\widetilde{\pi}_i(\widetilde{x}))_{i\in\mathfrak{S}}$, $(\widetilde{\pi}_i(\widetilde{y}))_{i\in\mathfrak{S}}$, $(\widetilde{\pi}_i(\widetilde{x-y}))_{i\in\mathfrak{S}}$, alors en utilisant la proposition 4.6.3, on trouve si $i \in \mathfrak{S}$:

$$\widetilde{\pi}_i(\widetilde{x+y}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_0(\widetilde{y}), \widetilde{\pi}_i(\widetilde{x-y})). \tag{4.28}$$

En fait, utiliser les formules d'addition de niveau δ du théorème 4.4.6 pour calculer $\widetilde{x+y}$ revient à utiliser $\#\mathcal{S}$ formules d'addition en niveau δ_0 pour calculer tous les $\widetilde{\pi}_i(\widetilde{x+y})$, $i \in \mathcal{S}$. On fait exactement les mêmes pseudo-additions quand on calcule les coordonnées compressées de $\widetilde{x+y}$ (les $\widetilde{\pi}_i(\widetilde{x+y})$ pour $i \in \mathfrak{S}$) puis quand on décompresse les coordonnées. Cependant, lorsqu'on calcule une multiplication, il est bien plus efficace de travailler sur les coordonnées compressées tout le long et de ne décompresser qu'à la fin.

Par exemple, si $\delta = \overline{n}$, avec $2 \mid n$, et $\delta_0 = \overline{2}$ (on verra dans la section 4.8 qu'on peut toujours calculer les pseudo-additions en niveau 2, sauf cas dégénérés), on a alors $\#\mathfrak{S} = g(g+1)/2$ si $4 \nmid n$ et $\#\mathfrak{S} = 2^g$ sinon[1], et donc une multiplication en niveau n se ramène à $\#\mathfrak{S}$ multiplications en niveau 2 (plus une décompression de coordonnées).

On peut bien sûr appliquer la même méthode pour calculer l'addition normale sur les points compressés, en calculant seulement les coefficients nécessaires aux points compressés dans l'algorithme 4.4.10 et l'analyse de complexité 4.4.11. (Il faut quand même vérifier que l'on peut trouver des relations de Riemann qui ne font intervenir que les coordonnées compressées des points x et y que l'on veut additionner, et de telle sorte que $\left(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{k+t}(0_X)\vartheta_{l+t}(0_X)\right) \neq 0$, en reprenant les notations du théorème 4.4.6. On verra que c'est effectivement le cas dans la section 4.6.1.) ◇

4.6.1 *Compression des coordonnées avec les relations de Riemann*

Pour l'instant, dans le corollaire 4.6.6, on s'est restreint à expliquer comment retrouver des coordonnées de $\widetilde{x} \in \widetilde{X}$ à l'aide des relations d'addition entre les $\widetilde{\pi}_i(\widetilde{x})$ sur $\widetilde{Y}$. Cependant, on a vu dans la proposition 4.5.5 que ces relations d'addition formaient un sous-ensemble des relations de Riemann. En particulier, si on regarde les relations de Riemann entre $(\widetilde{x}, \widetilde{x}, \widetilde{0}_X, \widetilde{0}_X; \widetilde{0}_X, \widetilde{0}_X, \widetilde{x}, \widetilde{x})$, comme les relations de Riemann somment sur les points de 2-torsion de X, et que $2 \mid \delta_0$, on voit qu'elles sont données exactement par les relations de Riemann entre

$$(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{x}), \widetilde{\pi}_k(\widetilde{0}_X), \widetilde{\pi}_l(\widetilde{0}_X); \widetilde{\pi}_{i'}(\widetilde{0}_X), \widetilde{\pi}_{j'}(\widetilde{0}_X), \widetilde{\pi}_{k'}(\widetilde{x}), \widetilde{\pi}_{l'}(\widetilde{x}))$$

où $i, j, k, l \in Z(\delta)$ satisfont $i + j + k + l = 2m$ avec $m \in Z(\delta)$, et $i' = m - i$, $j' = m - j$, $k' = m - k$, $l' = m - l$ (voir le théorème 4.4.6). La proposition 4.6.3 est un cas particulier des

1. De manière surprenante, on a besoin de moins de coordonnées compressées pour représenter un point de

relations de Riemann appliqué à $(i+j, i-j, 0, 0; -j, j, i, i)$, afin de retrouver des relations d'addition dans Y (et par exemple, déjà pour pouvoir calculer l'addition normale sur les points compressés, on va considérer les relations de Riemann avec $(i, 0, i, 0; 0, i, 0, i)$, quitte à translater par un élément j de $Z(\overline{4})$ pour s'assurer, en utilisant la proposition 4.6.11, que $\big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+j+t}(0_X)\vartheta_{j+t}(0_X)\big) \neq 0$).

Le but de cette section est de généraliser le corollaire 4.6.6 en utilisant toutes les relations de Riemann. Soit $(x_i)_{i\in Z(\delta)}$ les coordonnées de $\widetilde{x}$ et $(a_i)_{i\in Z(\delta)}$ celles de $\widetilde{0}_X$. Les relations de Riemann sont données par

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)x_{i+t}x_{j+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)a_{k+t}a_{l+t}\Big) = \Big(\sum_{t\in Z(\overline{2})} \chi(t)a_{i'+t}a_{j'+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)x_{k'+t}x_{l'+t}\Big).$$

Donc si l'on connait $\widetilde{\pi}_j(\widetilde{x})$, $\widetilde{\pi}_{k'}(\widetilde{x})$ et $\widetilde{\pi}_{l'}(\widetilde{x})$, ainsi que les coordonnées de $\widetilde{0}_X$, on peut retrouver $\widetilde{\pi}_i(\widetilde{x})$ si $\sum_{t\in Z(\overline{2})} \chi(t)a_{k+t}a_{l+t} \neq 0$. Or on a $U^{\mathcal{L}^2}_{\chi,k_0}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,l_0}(\widetilde{0}_X) = \sum_{t\in Z(\overline{2})} \chi(t)a_{k+t}a_{l+t}$ par l'équation (4.9), où $k_0, l_0 \in Z(2\delta)$ vérifient $k = k_0 + l_0$, $l = k_0 - l_0$. Si k et l sont dans $Z(\delta_0)$, comme $\widetilde{\pi}(\widetilde{0}_X) = \widetilde{0}_Y$, on peut appliquer le théorème 4.4.4. Pour le cas général, il nous faut une version plus fine de ce théorème, donnée par

PROPOSITION 4.6.11. *Soit $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété abélienne marquée de niveau δ, telle que $4 \mid \delta$. Alors pour tout $\chi \in \hat{Z}(\overline{2})$ et tout $i \in Z(2\delta)$, il existe $j \in Z(\overline{4})$ tel que*

$$U^{\mathcal{L}^2}_{\chi,i+j}(0_X) \neq 0.$$

DÉMONSTRATION : Voir [Mum66, p. 340], où MUMFORD prouve la version suivante : soit Z un sous-groupe de $Z(2\delta)$ tel que $Z(\overline{2}) \subset Z \subset 2Z(2\delta)$. On considère le changement de variable donné, si $l \in \hat{Z}$ et $i \in Z(2\delta)$, par :

$$V_{l,i} = \sum_{j\in Z} l(j)\vartheta_{i+j}.$$

(On retrouve exactement le changement de variable de l'exemple 4.4.9, et si $Z = Z(\overline{2})$ on retombe sur les variables $U^{\mathcal{L}^2}$). Alors pour tout $l \in \hat{Z}$, $i \in Z(2\delta)$, il existe $j \in \frac{1}{2}Z$, et $l' \in \hat{Z}(\overline{2})$ tels que

$$V_{l,i+j}(0_X) \neq 0,\ V_{l+l',i}(0_X) \neq 0.$$ ∎

En appliquant la proposition 4.6.11, on constate que quitte à changer k_0 et l_0 par des éléments k_1, l_1 de $Z(\overline{4})$, on a $U^{\mathcal{L}^2}_{\chi,k_0}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,l_0}(\widetilde{0}_X) \neq 0$. Or ce changement remplace m par $m + k_1$, et donc i', l', k', l', par des éléments de $Z(\overline{4})$. Mais si $4 \mid \delta_0$, si l'on connaît $\widetilde{\pi}_{k'}(\widetilde{x})$, on connaît également $x_{k'+k_1}$.

THÉORÈME 4.6.12 (COMPRESSION DES COORDONNÉES AVEC LES RELATIONS DE RIEMANN). *Avec les notations précédentes, supposons que $4 \mid \delta_0$, et soit $\{e_1, \dots, e_g\}$ la base canonique de $Z(\delta)$. Alors un point géométrique $\widetilde{x} \in \widetilde{X}$ est entièrement déterminé par $\widetilde{0}_X$ et*

$$(\widetilde{\pi}_0(\widetilde{x}), \widetilde{\pi}_{e_1}(\widetilde{x}), \dots, \widetilde{\pi}_{e_g}(\widetilde{x})).$$

Le point $\widetilde{0}_X$ est entièrement déterminé par

$$(\widetilde{\pi}_0(\widetilde{0}_X), \widetilde{\pi}_{e_1}(\widetilde{0}_X), \dots, \widetilde{\pi}_{e_g}(\widetilde{0}_X), \widetilde{\pi}_{e_1+e_2}(\widetilde{0}_X), \dots, \widetilde{\pi}_{e_1+e_g}(\widetilde{0}_X), \widetilde{\pi}_{e_2+e_3}(\widetilde{0}_X) \dots \widetilde{\pi}_{e_{g-1}+e_g}(\widetilde{0}_X).$$

niveau 6 qu'un point de niveau 4.

DÉMONSTRATION : En effet, si $i, j, k \in Z(\delta)$ et que l'on connaît $\widetilde{\pi}_0(\widetilde{0}_X)$, $\widetilde{\pi}_i(\widetilde{0}_X)$, $\widetilde{\pi}_j(\widetilde{0}_X)$, $\widetilde{\pi}_k(\widetilde{0}_X)$, $\widetilde{\pi}_{i+j}(\widetilde{0}_X)$, $\widetilde{\pi}_{j+k}(\widetilde{0}_X)$, $\widetilde{\pi}_{i+k}(\widetilde{0}_X)$, alors en regardant les relations de Riemann sur

$$\left(\widetilde{\pi}_{i+j+k}(\widetilde{0}_X), \widetilde{\pi}_i(\widetilde{0}_X), \widetilde{\pi}_j(\widetilde{0}_X), \widetilde{\pi}_k(\widetilde{0}_X); \widetilde{\pi}_0(\widetilde{0}_X), \widetilde{\pi}_{j+k}(\widetilde{0}_X), \widetilde{\pi}_{i+k}(\widetilde{0}_X), \widetilde{\pi}_{i+j}(\widetilde{0}_X)\right),$$

on retrouve $\widetilde{\pi}_{i+j+k}(\widetilde{0}_X)$ par la proposition 4.6.11. Ceci permet de retrouver tous les $\widetilde{\pi}_{e_{i_1}+e_{i_2}+\ldots e_{i_n}}(\widetilde{0}_X)$, et donc de retrouver $\widetilde{0}_X$ par le corollaire 4.6.6.

On peut appliquer le même raisonnement à $\widetilde{x}$, sachant de plus qu'on peut retrouver les $\widetilde{\pi}_{e_i+e_j}(\widetilde{x})$ en considérant les relations de Riemann sur :

$$\left(\widetilde{\pi}_{i+j}(\widetilde{x}), \widetilde{\pi}_0(\widetilde{x}), \widetilde{\pi}_i(\widetilde{0}_X), \widetilde{\pi}_j(\widetilde{0}_X); \widetilde{\pi}_{i+j}(\widetilde{0}_X), \widetilde{\pi}_0(\widetilde{0}_X), \widetilde{\pi}_j(\widetilde{x}), \widetilde{\pi}_i(\widetilde{x})\right). \qquad \blacksquare$$

REMARQUE 4.6.13. On peut se demander pourquoi nous n'avons pas énoncé le théorème 4.6.12 directement plutôt que de mettre en valeur le corollaire 4.6.6. En effet, ce théorème offre une meilleure compression, et est plus satisfaisant (le nombre de coordonnées pour retrouver $\widetilde{x}$ et $\widetilde{0}_X$ ne dépend que de δ_0, pas de δ). La raison est la suivante : en pratique, la meilleure compression est atteinte en prenant $\delta_0 = \overline{2}$. Or si $i \in Z(2\delta_0)$ et $\chi \in \hat{Z}(\overline{2})$, on a $U^{\mathcal{L}^2}_{\chi,i} = U^{\mathcal{L}^2_0}_{\chi,i}$. (En effet, $\pi : (X, \mathcal{L}^2) \to (Y, \mathcal{L}^2_0)$ est une $\hat{Z}(2\delta')$ isogénie). Or la section 4.8 montre que $U^{\mathcal{L}^2_0}_{\chi,i}(0_X) = 0$ si $\chi(2i) = -1$. On ne peut donc jamais appliquer le théorème 4.6.12 dans ce cadre. En revanche, on a génériquement $U^{\mathcal{L}^2_0}_{\chi,0}(0_X) \neq 0$, donc on peut appliquer le corollaire 4.6.6. Or il est plus efficace de représenter un point par (au pire) 2^g points à coordonnées dans $Z(\overline{2})$, que par $1 + g$ points à coordonnées dans $Z(\overline{4})$. Ceci explique pourquoi nous avons donné les algorithmes 4.6.7 et 4.6.8 dans le cadre précédent, même s'il est trivial de les adapter au théorème 4.6.12.

On introduit la notation suivante pour prendre en compte toutes les possibilités de compression/décompression : nous appellons $\mathfrak{S} \subset Z(\delta)$ une base de décompression par rapport à $Z(\delta_0)$ lorsque

- Si $4 \mid \delta_0$, $\mathfrak{S} = \{0, e_1, \ldots, e_g, e_1 + e_2, \ldots, e_{g-1} + e_g\}$. De plus, dans ce cas, on appelle l'ensemble $\mathfrak{S}_0 = \{0, e_1, \ldots, e_g\}$ (qui est suffisant pour décompresser les coordonnées d'un point $\widetilde{x} \in \widetilde{X}$ si on connaît $\widetilde{0}_X$) une base de décompression spéciale.
- $\mathfrak{S}$ est une base différentielle de $Z(\delta)$ relativement à $Z(\delta_0)$ sinon. $\diamond$

4.7 L'ESPACE MODULAIRE DES THÊTA STRUCTURES

Dans cette section, on suppose seulement k parfait, et on note $\overline{k}$ sa clôture algébrique. Soit $(A_k, \mathcal{L})$ une variété abélienne sur k munie d'un fibré très ample totalement symétrique $\mathcal{L}$. Supposons qu'on s'est fixé une thêta structure symétrique $\Theta_{\mathcal{L}}$ sur $G(\mathcal{L})$ (une thêta structure est dite symétrique lorsque son extension à $\overline{k}$ l'est) de type δ. On peut définir comme dans la section 4.4 le cône affine $\widetilde{X}_k$ associé à la thêta structure $\Theta_{\mathcal{L}}$, et on se fixe des coordonnées thêta affines sur $\widetilde{X}_k$ (c'est-à-dire que l'on prend un représentant de l'orbite sous l'action de $\mathbb{G}_{m,k}$ des coordonnées thêta canoniques), et un relevé affine rationnel $\widetilde{0}_{X_k}$ du thêta null point associé à la thêta structure $\Theta_{\mathcal{L}}$. Alors les formules d'addition du théorème 4.4.6 sont rationnelles, donc en particulier on a toujours la pseudo-addition `chain_add` sur $\widetilde{X}_k$. De plus, si $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x-y}$ sont des points rationnels de $\widetilde{X}_k$, $\widetilde{x+y} \coloneqq \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}_{X_k})$ est dans $\widetilde{X}_k(k)$.

En particulier, tout point géométrique $x \in X(\overline{k})$ satisfait les relations d'addition :

$$x = \texttt{chain\_add}(x, 0_{X_k}, x, 0_{X_k}). \tag{4.29}$$

Ces relations suffisent pour déterminer l'image de X dans $\mathbb{P}_k(\Gamma(X,\mathcal{L}))$:

THÉORÈME 4.7.1. *Avec les notations du paragraphe précédent, soit $(\vartheta_i)_{i\in Z(\delta)}$ une base canonique pour la thêta structure $G(\mathcal{L})$ de $V=\Gamma(X,\mathcal{L})$. Soit $(a_i)_{i\in Z(\delta)}$ les coordonnées dans $\mathbb{P}_k(V)$ du thêta null point $0_{X_k}\in X$. Supposons que δ soit divisible par un nombre pair $n\geqslant 4$. Alors l'image de X_k dans $\mathbb{P}_k(V)$ est l'espace projectif défini par les équations de Riemann :*

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+t}\vartheta_{j+t}\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)a_{k+t}a_{l+t}\Big)= \Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i'+t}\vartheta_{j'+t}\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)a_{k'+t}a_{l'+t}\Big), \quad (4.30)$$

pour tout $\chi\in\hat{Z}(\bar{2})$, $i,j,k,l,m\in Z(\delta)$ tels que $i+j+k+l=2m$, avec $i'=m-i$, $j'=m-j$, $k'=m-k$ et $l'-l$.

DÉMONSTRATION : Une preuve est donnée par MUMFORD dans [Mum66, p. 336-349] lorsque $4\mid n$. Le cas général est donné dans [Mum69]. ∎

On voit donc que le thêta null point $(a_i)_{i\in Z(\delta)}$ détermine entièrement le triplet $(X_k,\mathcal{L},\Theta_{\mathcal{L}})$ (en effet on a vu dans la section 3.4 qu'il détermine $\Theta_{\mathcal{L}}$, de plus le théorème 4.7.1 montre qu'il détermine X_k, et $\mathcal{L}$, comme l'image réciproque de $\mathcal{O}_{\mathbb{P}_k(V)}(1)$).

On peut expliquer l'importance du thêta null point ainsi : on peut spécialiser l'équation (4.29) en posant $\widetilde{x}=0_{X_k}$: on obtient des équations pour le thêta null point de toute variété abélienne marquée (par une structure thêta symétrique de type δ) : $0_{X_k}=\texttt{chain\_add}(0_{X_k},0_{X_k},0_{X_k},0_{X_k})$.

Soit d le degré de δ ($d=\prod_{i=1}^{g}\delta_i$). Si R est un anneau au-dessus de $\mathbb{Z}[d^{-1}]$, et A_R une variété abélienne sur R, on peut définir des R-schémas en groupes $K(A_R)$ et $G(A_R)$ qui étendent la définition des foncteurs $K(\cdot)$ et $G(\cdot)$ définis au-dessus des variétés abéliennes A_k lorsque k est un corps (il faut faire un peut attention dans la définition de $K(A_R)$ lorsque R n'est pas connexe.) On peut alors définir une thêta structure comme un isomorphisme entre le schéma en groupes de Heisenberg de type δ sur R et $G(A_R)$ (pour les détails, voir [Mum67a, p. 76-84]). On peut alors définir l'espace modulaire $\mathscr{M}_\delta$ des variétés abéliennes avec un δ-marquage comme étant le foncteur qui à R associe l'ensemble des triplets $(A_R,\mathcal{L},\Theta_{\mathcal{L}})$ où $A_R\to R$ est une variété abélienne, $\mathcal{L}$ un fibré (relativement) ample et totalement symétrique et $\Theta_{\mathcal{L}}$ une thêta structure symétrique sur $G(\mathcal{L})$.

THÉORÈME 4.7.2 (L'ESPACE MODULAIRE DE NIVEAU δ). *Soit $V_\delta=\mathrm{Hom}_{\mathbb{Z}[d^{-1}]}(Z(\delta),\mathbb{Z}[d^{-1}])$ le $\mathbb{Z}[d^{-1}]$-module libre de base les fonctions de Dirac $(Q_i)_{i\in Z(\delta)}$. Soit $\overline{\mathscr{M}}_\delta$ la variété projective de $\mathbb{P}(V_\delta)$ donnée par les équations de Riemann :*

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)Q_{i+t}Q_{j+t}\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)Q_{k+t}Q_{l+t}\Big)= \Big(\sum_{t\in Z(\bar{2})}\chi(t)Q_{i'+t}Q_{j'+t}\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)Q_{k'+t}Q_{l'+t}\Big), \quad (4.31)$$

(avec χ,i,j,k,l comme dans le théorème 4.7.1) et les relations de symétrie (pour tout $i\in Z(\delta)$) :

$$Q_i=Q_{-i}.$$

Supposons que δ soit divisible par un nombre pair $n>4$. Alors le foncteur, qui associe à un point $(A_R,\mathcal{L},\Theta_{\mathcal{L}})$ de $\mathscr{M}_\delta(R)$ le thêta null point associé dans $\mathbb{P}(V_\delta)(R)$, est une immersion ouverte de $\mathscr{M}_\delta$ sur $\overline{\mathscr{M}}_\delta$. En particulier, $\mathscr{M}_\delta$ est représentable.

DÉMONSTRATION : Soit k un corps de caractéristique non divisible par d. Si δ est divisible par un nombre pair $n \geqslant 4$, et $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ est un point de $\mathscr{M}_\delta(k)$, son thêta null point est dans $\overline{\mathscr{M}}_\delta(k)$ par le théorème 4.7.1. Or par hypothèse sur δ, le thêta null point détermine $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ d'après la section 3.4 et le théorème 4.7.1. Ainsi le foncteur $\mathscr{M}_\delta$ restreint aux corps est un sous-foncteur de $\overline{\mathscr{M}}_\delta$. Il est facile de vérifier que c'est également le cas sur les $\mathbb{Z}[d^{-1}]$-algèbres R [Mum66, p. 82].

Il reste à vérifier que la flèche $\mathscr{M}_\delta \to \overline{\mathscr{M}}_\delta$ est une immersion ouverte. Ce théorème (difficile !) est prouvé par MUMFORD dans [Mum67a, p. 83-99] lorsque $8 \mid n$, et a été étendu par KEMPF dans le cas où $n > 4$ dans [Kem89, p. 92]. (MUMFORD conjecture que le théorème 4.7.2 est également vrai avec $n = 4$ dans [Mum66, p. 288]). ■

Bien sûr, nous nous contenterons d'appliquer le théorème 4.7.2 à des corps. Soit k un corps, de caractéristique non divisible par d. On appelle un élément $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ dans $\mathscr{M}_\delta(k)$ une variété abélienne marquée. Ainsi, $\mathcal{L}$ est un fibré totalement symétrique de type δ et $\Theta_{\mathcal{L}}$ est une thêta structrure symétrique sur $\mathcal{L}$.

DÉFINITION 4.7.3 (L'ESPACE MODULAIRE $\mathcal{M}_\delta$ SUR k). Soit k un corps de caractéristique p non divisible par d. On note $\mathcal{M}_\delta = \mathscr{M}_\delta \times_{\mathbb{Z}[d^{-1}]} k$ l'espace modulaire des variétés abéliennes sur k marquées par une thêta structure symétrique de type δ. On note $\overline{\mathcal{M}}_\delta = \overline{\mathscr{M}}_\delta \times_{\mathbb{Z}[d^{-1}]} k$, $\overline{\mathcal{M}}_\delta$ est un schéma projectif sur k. Lorsque δ est divisible par un nombre pair $n \geqslant 4$, on identifie $\mathcal{M}_\delta$ à son image (isomorphe par le théorème 4.7.2) dans $\overline{\mathcal{M}}_\delta$. (Ainsi, si $n > 4$, $\mathcal{M}_\delta$ est un sous-schéma ouvert de $\overline{\mathcal{M}}_\delta$). ◊

EXEMPLE 4.7.4. Supposons que l'on ait une courbe (irréductible, lisse) C de genre g sur k (où k est de caractéristique différente de 2). On peut se demander s'il est possible de calculer un thêta null point (disons de niveau 4) associé à la Jacobienne $\mathrm{Jac}(C)$ de C. Si C est une courbe hyperelliptique, la réponse est donnée par les formules de Thomae [Mum84, Théorème 8.1] (voir aussi l'algorithme 4.7.5). De plus, la correspondance entre les coordonnées de Mumford (u, v) sur $\mathrm{Jac}(C)$ et les fonctions thêta de niveau 4 sur $\mathrm{Jac}(C)$ est donnée dans [Wam99] (voir aussi [Mum84, Théorème 7.6]). On renvoie au travail de Romain COSSET pour une implémentation efficace de la conversion entre coordonnées de Mumford et coordonnées thêta en genre 2.

Si C est de la forme $y^2 = f(x)$, les formules de Thomae ne donnent que la puissance 4-ième des coordonnées du thêta null point, en fonction des racines de f. Cependant, si on fait attention au choix de racine 4-ième (de manière à obtenir un point géométrique de $\mathscr{M}_{Z(\overline{4})}$), en raisonnant comme dans la section 6.3 on constate que l'on a bien le thêta null point de niveau 4 correspondant à $\mathrm{Jac}(C)$. On peut ensuite utiliser les formules de duplication (voir le théorème 4.4.3) pour calculer le thêta null point de niveau 2 correspondant à $\mathrm{Jac}(C)$. Réciproquement, on peut aussi inverser les formules de Thomae pour reconstituer la courbe à partir du thêta null point.

ALGORITHME 4.7.5 (FORMULES DE THOMAE) :
Entrées $y^2 = \prod_{i=1}^{2g+2}(x - \alpha_i)$ une courbe hyperelliptique de genre g.
Sortie $(U^{\mathcal{L}^4}_{\chi,i}(0)^4)_{\chi \in \hat{Z}(\overline{2}), i \in Z(\overline{2})}$ [1] le thêta null point de niveau 4 associé à $(\mathrm{Jac}(C), \mathcal{L}^4)$ où $\mathcal{L}$ est le fibré principal canonique sur $\mathrm{Jac}(C)$.

➔ Soit $U = \{1, 3, 5, \ldots, 2g+1\}$. Si $S \subset \{1, 2, \ldots, 2g+2\}$, on définit η_S comme la matrice

1. Techniquement les coordonnées $U^{\mathcal{L}^4}$ sont indicées par $\hat{Z}(\overline{2}) \times Z(\overline{4})$, mais on a $U^{\mathcal{L}^4}_{\chi,i+t} = \chi(t) U^{\mathcal{L}^4}_{\chi,i}$, ce qui nous permet d'indicer par $\hat{Z}(\overline{2}) \times Z(\overline{2})$ (en faisant attention que cette fois l'application $Z(\overline{2}) \to Z(\overline{4})$ n'est pas le plongement canonique).

$\eta_S = \sum_{i\in S}\eta_i \in \mathrm{M}_{2\times 2g}(\mathbb{Z}/2\mathbb{Z})$, avec

$$\eta_{2i-1} = \begin{pmatrix} 0 & \dots & 0 & \overset{i}{1} & 0 & \dots & 0 \\ 1 & \dots & 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$
$$\eta_{2i} = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 1 & \dots & 1 & 1 & 0 & \dots & 0 \end{pmatrix}$$

➔ Pour tout $S \subset \{1, 2, \dots, 2g+2\}$

- Si $\#(S \triangle U) = g+1$, alors

$$U^{\mathcal{L}^4}_{\eta_S}(0)^4 = (-1)^{\#(S\cap U)} \prod_{\substack{i\in S\cap U \\ j\notin S\cap U}} (\alpha_i - \alpha_j)^{-1}$$

- Sinon

$$U^{\mathcal{L}^4}_{\eta_S}(0)^4 = 0$$

➔ Retourner $(U^{\mathcal{L}^4}_{\eta_S}(0)^4)_{S\subset\{1\dots 2g+2\}}$. ♢

On peut visualiser l'espace modulaire $\mathscr{M}_\delta$ comme un équivalent algébrique de l'espace modulaire analytique $\mathcal{A}_D(D)$ de la section 2.5 (sauf qu'on impose une structure de niveau en plus de la décomposition symplectique de $K(\mathcal{L})$). On peut généraliser la variété abélienne universelle $\mathfrak{X}_D/\Gamma_D D \to \mathcal{A}_D(D)$ ainsi : Soit $\overline{\mathfrak{A}}_\delta \subset \mathbb{P}(V_\delta) \times \overline{\mathscr{M}}_\delta$ la variété définie par les équations

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)X_{i+t}X_{j+t}\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)Q_{k+t}Q_{l+t}\Big) = \Big(\sum_{t\in Z(\overline{2})}\chi(t)X_{i'+t}X_{j'+t}\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)Q_{k'+t}Q_{l'+t}\Big)$$

où $(X_i)_{i\in Z(\delta)}$ est la base canonique de V_δ et les i, j, k, l comme dans le théorème 4.7.1. Alors le pullback $\mathfrak{A}_\delta \to \mathscr{M}_\delta$ de $\overline{\mathfrak{A}}_\delta \to \overline{\mathscr{M}}_\delta$ est la variété universelle des variété abéliennes munies d'un δ-marquage [Mum67a, p. 84].

On peut également préciser les remarques de la section 3.7 :

Proposition 4.7.6. *Soit k est un corps parfait. Une thêta structure symétrique $\Theta_{\mathcal{L}}$ sur A_k est rationnelle si et seulement si la décomposition symplectique de $K(\mathcal{L}^2) = K_1(\mathcal{L}^2) \oplus K_2(\mathcal{L}^2)$ associée à $\Theta_{\mathcal{L}}$ par la proposition 4.3.1 est rationnelle (c'est à dire que les sous-groupes $K_1(\mathcal{L}^2)$ et $K_2(\mathcal{L}^2)$ sont rationnels) et l'isomorphisme symplectique $\overline{\Theta}_{\mathcal{L}} : K(\delta) \to K(\mathcal{L})$ est rationnel.*

Démonstration : Soit k un corps parfait, et $g \in \mathrm{Gal}(\overline{k}/k)$. Soit $\Theta_{\mathcal{L}}$ une thêta structure (symétrique), et $K(\mathcal{L}^2) = K_1(\mathcal{L}^2) \oplus K_2(\mathcal{L}^2)$ la décomposition symplectique associée. On prend une thêta structure quelconque sur $\mathcal{L}^4$ qui soit compatible avec la décomposition symplectique de $K(\mathcal{L}^2)$, et si $y \in K(\mathcal{L}^2)$, on sait que l'élément (symétrique) canonique de $G(\mathcal{L})$ au-dessus de $x = [2]y$ associé à $\Theta_{\mathcal{L}}$ est donné par $\phi_x = \alpha_{[2]}(\phi_y)$, où ϕ_y est l'élément canonique de $G(\mathcal{L}^4)$ associé à la thêta structure sur $\mathcal{L}^4$. De plus, ϕ_x dépend uniquement de la décomposition de $K(\mathcal{L}^2)$ (proposition 4.3.1). On a $[2](g.y) = g([2].y) = g.x$, et donc $g.\phi_x = \alpha_{[2]}(g.\phi_y) = \alpha_{[2]}(\phi_{g.y}) = \phi_{g.x}$. La thêta structure $g.\Theta_{\mathcal{L}}$ est donc la thêta structure symétrique associée à $g.\overline{\Theta}_{\mathcal{L}}$ ainsi qu'à la décomposition symplectique $K(\mathcal{L}^2) = g.K_1(\mathcal{L}^2) \oplus g.K_2(\mathcal{L}^2)$. La proposition en découle immédiatement.

Si tous les points géométriques de $K(\mathcal{L}^2)$ sont rationnels, on peut même montrer que tous les points géométriques symétriques de $G(\mathcal{L})$ sont rationnels. Soit $x \in K(\mathcal{L})$, $y \in K(\mathcal{L}^2)$ tel que $x = 2y$, et $h \in G(\mathcal{L}^2)(k)$ un élément quelconque au-dessus de y. Soit $\alpha \in \mathbb{G}_{m,k}(k)$ tel que $\gamma_{-1}h = \alpha h^{-1}$. L'élément $h^{\otimes 2}$ est dans $G(\mathcal{L}^4)$, et l'on a $\gamma_{-1}(h^{\otimes 2}) = \alpha^2 h^{\otimes 2^{-1}}$ [Mum66, Proposition 5 p. 311]. Soit $g' = (h^{\otimes 2}/\alpha)$, g' est un élément symétrique de $G(\mathcal{L}^4)(k)$ au-dessus de y. Si $\alpha_{[2]} : G(\mathcal{L}^4) \to G(\mathcal{L})$ est le morphisme de descente associé à l'isogénie $[2]$, alors $g = \alpha_{[2]}(g')$ est un élément symétrique rationnel de $G(\mathcal{L})$ au-dessus de x. De plus, la remarque 4.2.11 montre que si x est d'ordre n, alors g (ou $-g$) est d'ordre n. En reprenant la preuve de la proposition 3.2.6, cela redonne l'existence d'une section (symétrique) rationnelle $K(\mathcal{L}) \to G(\mathcal{L})$. ■

Ainsi, toute la théorie développée par MUMFORD rend les variétés abéliennes très agréables à manipuler. En effet, on part d'un point $(a_i)_{i\in Z(\delta)}$ k-rationnel qui vérifie les équations du théorème 4.7.2, c'est-à-dire que $(a_i)_{i\in Z(\delta)} \in \overline{\mathscr{M}}_\delta(k)$. On peut lui associer la variété projective A_k définie dans le théorème 4.7.1. Si de plus $(a_i)_{i\in Z(\delta)} \in \mathscr{M}_\delta$ (on dit que le thêta null point $(a_i)_{i\in Z(\delta)}$ est non dégénéré), alors A_k est une variété abélienne de point neutre $(a_i)_{i\in Z(\delta)}$. La loi d'addition sur A_k est donnée par le théorème 4.4.6. De plus, tout plongement projectif d'une variété abélienne issue d'un fibré totalement symétrique est donné par les équations de Riemann, modulo un changement de variable projectif ! Donc on retrouve toutes les manières de représenter une variété abélienne par des équations projectives[1].

On aurait pu éviter d'introduire la notion algébrique de thêta structure dans le chapitre 3, en continuant à travailler sur le corps $\mathbb{C}$, en montrant analytiquement les relations de Riemann du théorème 4.4.6, et en en déduisant les équations satisfaites par une variété algébrique complexe X et son thêta null point comme dans les théorèmes 4.7.1 et 4.7.2. Ces équations étant définies sur $\mathbb{Z}$, on peut ensuite les considérer sur n'importe quel corps, et on aurait pu admettre qu'on obtenait toute variété abélienne ainsi (au moins si la caractéristique de k est différente de 2 pour avoir des formules d'addition).

Cependant nous voudrions faire la remarque suivante : lorsque l'on fait le choix de travailler sur le corps complexe, on utilise le fait que les variétés abéliennes complexes polarisées de niveau δ sont de la forme

$$X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$$

avec $\Omega D_\delta^{-1} \in \mathfrak{H}_g$ (voir le chapitre 2). De plus, on a vu dans le chapitre 3 et la section 4.2 que le choix d'une caractéristique $c \in X$ détermine entièrement un fibré $\mathcal{L}$ (dans la classe de polarisation donnée par $\mathrm{Im}(\Omega D_\delta)^{-1}$; $\mathcal{L}$ est en fait déterminé uniquement par la valeur de c modulo $K(\mathcal{L})$), et une structure de niveau sur $G(\mathcal{L})$. En particulier, on a un fibré canonique et une structure de niveau (symétrique) canonique associés à la caractéristique $c = 0$. Cependant, on a besoin de beaucoup moins d'informations qu'une décomposition symplectique du réseau Λ associé à X pour fixer une telle thêta structure canonique, et donc pouvoir avoir des coordonnées thêta canoniques. Déjà si $2 \mid \delta$, on peut considérer l'unique fibré totalement symétrique $\mathcal{L}_0$ dans sa classe d'équivalence. De plus, une structure de niveau symétrique sur $\mathcal{L}_0$ est entièrement déterminée par le choix d'une décomposition symplectique de $K(\mathcal{L}_0^2)$. Or une décomposition de Λ donne une décomposition de chaque $K(\mathcal{L}_0^n)$ (autrement dit une ∞-décomposition), donc fixe bien plus qu'une simple décomposition de $K(\mathcal{L}_0^2)$.

Nous n'avons énoncé la proposition 4.3.1 que pour des fibrés totalement symétriques, étant donné que c'est dans ce cadre que l'on utilise les formules d'addition. On peut cependant la généraliser. Si $2 \nmid \delta$, et $\mathcal{L}$ est un fibré symétrique de type δ, supposons donné une décomposition symplectique de $K(\mathcal{L}^2)$. On prend une structure de niveau symétrique du fibré totalement symétrique $\mathcal{L}^4$ au-dessus

1. Ou presque puisque l'on a besoin d'un fibré totalement symétrique. Disons que l'on retrouve tous les plongements où l'inverse $[-1]$ s'exprime linéairement sur la base.

de cette décomposition, alors en descendant cette structure de niveau par l'isogénie de duplication $[2]$, on obtient un fibré symétrique $\mathcal{L}_0$ équivalent à $\mathcal{L}$ et une structure de niveau symétrique associé, qui dépendent uniquement de la décomposition choisie de $K(\mathcal{L}^2)$. Pour plus de détails, on peut consulter [Mum66, Section 2] et [Kem89, Section 2]. On obtient alors les autres fibrés et thêta structures correspondant aux autres caractéristiques $c \in X$ en faisant agir c par conjugaison $\mathtt{conj}_c$ sur $\mathcal{L}_0$.

De même, si $\Lambda' \subset \mathbb{C}^g$ est un réseau au-dessus de Λ, soit $f : X = \mathbb{C}^g/\Lambda \to X' = \mathbb{C}^g/\Lambda'$ l'isogénie associée, et on considère des décompositions symplectiques compatibles de Λ et Λ'. Alors si $c \in X$ est une caractéristique, correspondant à un fibré $\mathcal{L}_c$ et une structure de niveau sur $G(\mathcal{L}_c)$, $f(c) \in X'$ est une caractéristique qui correspond à un fibré $\mathcal{L}'_c$ tel que $f^*\mathcal{L}'_c = \mathcal{L}_c$ et une structure de niveau sur $G(\mathcal{L}'_c)$ compatible avec celle de $G(\mathcal{L}_c)$. Là encore, on n'a pas besoin de choisir une décomposition compatible sur Λ et Λ', il suffit de projeter via f une décomposition symplectique de $K(\mathcal{L}_0^2)$, ce qui donne une décomposition symplectique de $K({\mathcal{L}'_0}^2)$ telle que la structure de niveau associé sur $G(\mathcal{L}'_0)$ soit compatible avec celle sur $G(\mathcal{L}_0)$.

Autrement dit, une thêta structure (symétrique) est une structure intermédiaire entre le choix d'une base symplectique de $K(\mathcal{L})$ et le choix d'une base symplectique de $K(\mathcal{L}^2)$, en particulier elle ne nécessite qu'un nombre fini de choix. Ce n'est pas le cas du choix d'une décomposition du réseau Λ. D'ailleurs, on voit bien la différence lorsqu'on regarde les actions des sections 2.5 et 3.5 : deux matrices de périodes correspondent à la même variété abélienne si elles différent d'une action du groupe symplectique infini $\mathrm{Sp}_\delta(\mathbb{Z}^{2g})$, tandis que si on regarde seulement les thêta null points de niveau δ, ils vont représenter la même variété abélienne s'ils diffèrent d'un automorphisme symétrique du groupe fini de Heisenberg $\mathcal{H}(\delta)$.

4.8 VARIÉTÉS DE KUMMER

Pour avoir une représentation compacte des points, et des formules d'addition rapides, il est important de travailler avec un fibré de niveau δ minimal. Comme $\mathcal{L}$ est totalement symétrique (ce qui est indispensable pour les formules d'addition), on a $2 \mid \delta$. De plus si $4 \mid \delta$, on sait que $\mathcal{L}$ est très ample. On pourrait donc travailler en niveau 4, dans cette section on explique comment faire pour travailler en niveau 2 (qui est donc le niveau de degré minimal pour lequel on puisse avoir un fibré totalement symétrique), ce qui nous fait gagner 2^g coordonnées par rapport au niveau 4. L'inconvénient est que l'on n'a plus un plongement projectif de la variété abélienne X, mais seulement de la variété de Kummer associée à X.

Soit $\mathcal{L}$ un fibré totalement symétrique de niveau 2 sur une variété abélienne X. Par le corollaire 3.2.3, il existe un fibré principal symétrique $\mathcal{L}_0$ tel que $\mathcal{L} = \mathcal{L}_0^2$. Soit $K_X \coloneqq X/\pm 1$ la variété de Kummer associée à X, et $p_X : X \to K_X$ la projection. De manière imagée, si $x \in X(k)$, on note $\pm x$ son image dans K_X. Le morphisme p_X induit une bijection de $X[2]$ sur son image. D'autre part, l'action de $[-1]$ est libre et propre sur X en-dehors de $X[2]$, donc K_X est lisse en-dehors de $p_X(X[2])$. Comme $\mathcal{L}$ est totalement symétrique, il descend en un fibré $\mathcal{M}$ sur K_X. Si $n \in \mathbb{N}$, l'automorphisme $[-1]$ induit une décomposition de $\Gamma(X, \mathcal{L}_0^n) = \Gamma(X, \mathcal{L}_0^n)^+ \oplus \Gamma(X, \mathcal{L}_0^n)^-$ suivant les vecteurs propres 1 et -1. Un élément de $\Gamma(X, \mathcal{L}_0^n)^+$ est appelé une fonction thêta (de niveau n) paire, tandis qu'une fonction thêta dans $\Gamma(X, \mathcal{L}_0^n)^-$ est appelée une fonction thêta impaire. Par construction de K_X, on a $\Gamma(K_X, \mathcal{M}^n) = \Gamma(X, \mathcal{L}_0^{2n})^+$, et [Kem92] montre que $\bigoplus_{n\geqslant 0} \Gamma(K_X, \mathcal{M}^{2n})$ est engendré par $\Gamma(K_X, \mathcal{M}^2)$ et donc que $(K_X, \mathcal{M}^2)$ est projectivement normal (voir la remarque 4.4.5).

Si on prend une thêta structure symétrique sur $(X, \mathcal{L})$, les fonctions thêta canoniques associées vérifient pour tout $i \in Z(\overline{2})$: $\gamma_{-1}\vartheta_i = \vartheta_{-i} = \vartheta_i$, donc toute fonction thêta sur $\mathcal{L}$ est

paire. Autrement dit, le morphisme projectif induit par $\mathcal{L}$ se factorise par K_X, et pour tout $x \in \widetilde{X}$, on a $(\vartheta_i(x))_{i\in Z(\bar{2})} = (\vartheta_i(-x))_{i\in Z(\bar{2})}$. De plus, si $\mathcal{L}_0$ est irréductible, on a vu dans la section 2.4 que $\mathcal{L}$ induit un plongement de K_X dans l'espace projectif.

Si on connaît $\pm x, \pm y \in K_X$, on peut retrouver au mieux l'ensemble $\{\pm(x+y), \pm(x-y)\}$, mais il n'est pas possible de calculer l'addition normale en niveau 2. Cependant, si on connait également $\pm(x-y)$, on peut identifier $\pm(x+y)$ dans l'ensemble précédent, et on a donc une pseudo-addition sur K_X, que l'on peut espérer calculer via les formules de la section 4.8.

Si on revient aux formules du théorème 4.4.3, on constate que le critère important pour avoir des formules de pseudo-addition consiste en la non annulation des fonctions

$$\{U^{\mathcal{L}^2}_{\chi,i}(0_X) \mid i \in Z(\bar{4}), \chi \in \hat{Z}(\bar{2})\}.$$

Mais si $\widetilde{x} \in \widetilde{X}$, on a

$$\begin{aligned} U^{\mathcal{L}^2}_{\chi,i}(-\widetilde{x}) &= \sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{i+t}(-\widetilde{x}) = \sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{-i+t}(\widetilde{x}) \\ &= \chi(2i)\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{i+t}(\widetilde{x}) = \chi(2i)U^{\mathcal{L}^2}_{\chi,i}(\widetilde{x}). \end{aligned}$$

Ainsi, une base des fonctions thêta paires de $\mathcal{L}^2$ est donnée par les $U^{\mathcal{L}^2}_{\chi,i}$ avec $\chi(2i) = 1$, et une base des fonctions thêta impaires par les $U^{\mathcal{L}^2}_{\chi,i}$ avec $\chi(2i) = -1$. En particulier, si $\chi(2i) = -1$, on a $U^{\mathcal{L}^2}_{\chi,i}(0_X) = 0$.

Si $U^{\mathcal{L}^2}_{\chi,0}(0_X) \neq 0$ pour tout $\chi \in \hat{Z}(\bar{2})$, alors on peut calculer la pseudo-addition de $\widetilde{x}$ et $\widetilde{y}$ si les coordonnées de $\widetilde{x-y}$ ne s'annulent pas comme dans l'algorithme 4.4.10.

Définition 4.8.1. On dit que les thêta null points pairs ne s'annulent pas lorsque $U^{\mathcal{L}^2}_{\chi,i}(0_X) \neq 0$ pour tout $\chi \in \hat{Z}(\bar{2})$ et $i \in Z(\bar{4})$ tels que $\chi(2i) = 1$.

Exemple 4.8.2. Si $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ est une variété abélienne complexe, et que $\mathcal{L}_0$ est le fibré canonique de caractéristique 0, on peut visualiser les fonctions $U^{\mathcal{L}^2}$ comme les fonctions

$$\{\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2\cdot, \Omega) \mid a, b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\}$$

et l'équivalent de $\chi(2i)$ est donné par $(-1)^{4\,{}^t a\cdot b}$. Par définition de $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$, on a $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, \Omega) = 0$ si et seulement si le point de 2-torsion $a\Omega + b$ de X est dans le diviseur Θ associé à $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\cdot, \Omega)$.

De plus, si $e^{\mathcal{L}_0}_*$ est la forme quadratique associée à $\mathcal{L}_0^2$ de la section 4.2, on a $e^{\mathcal{L}_0}_*(a\Omega + b) = (-1)^{4\,{}^t a\cdot b}$ [Mum83, Définition 3.13 p. 167], donc les thêta null points pairs sont exactement les points de $X[2]$ tels que $e^{\mathcal{L}_0}_*(x) = 1$. ◇

Remarque 4.8.3. (Interprétation géométrique de la non annulation des thêta null points pairs). On peut généraliser l'exemple 4.8.2 ainsi : on a $[2]^*\mathcal{L}_0 = \mathcal{L}^2$. Quitte à changer $\mathcal{L}_0$ par un fibré symétrique équivalent, on peut supposer que $\mathcal{L}_0$ est $[2]$-compatible avec $\mathcal{L}^2$, et l'exemple 4.4.2 montre que la duplication $[2] : (X, \mathcal{L}^2) \to (X, \mathcal{L}_0)$ est donnée par

$$[2].(x_i)_{i\in Z(\bar{4})} = (\sum_{t\in Z(\bar{2})} x_{j+t})_{j\in Z(\bar{2})}. \tag{4.32}$$

Soit x un point de 2-torsion, x est donc dans $K(\mathcal{L})$. Soit y un point quelconque tel que

$x = [2]y$, $y \in K(\mathcal{L}^2)$ donc il existe $(i,j) \in K(\overline{4})$ tel que $y = \overline{\Theta}^{\mathcal{L}^2}(i,j)$. On a alors en combinant les équations (3.6) et (4.32) :

$$\vartheta_0^{\mathcal{L}_0}(x) = \sum_{t \in Z(\overline{2})} e_{\overline{4}}(i+t,-j)\vartheta_{i+t}^{\mathcal{L}^2}(0_X) = e_{\overline{4}}(i,-j)U_{\chi,i}^{\mathcal{L}^2}(0_X)$$

si χ est le caractère $t \in Z(\overline{2}) \mapsto e_{\overline{4}}(t,-j)$. Ainsi, $U_{\chi,i}^{\mathcal{L}^2}(0_X)$ s'annule si et seulement si le point de 2-torsion $x = \overline{\Theta}^{\mathcal{L}}(2i,2j)$ est dans le diviseur Θ associé à $\vartheta_0^{\mathcal{L}_0}$. De plus, on a $\chi(2i) = e_{\overline{4}}(2i,-j) = e_{\overline{2}}(2i,2j)$, donc les thêta null points pairs sont exactement les éléments $\{\overline{\Theta}_{\mathcal{L}}(i,j) \mid (i,j) \in Z(\overline{2}) \times \hat{Z}(\overline{2}), j(i) = 1\}$. Ceci explique la condition de la définition 4.8.1.

On sait que les fonctions thêta de $\Gamma(X,\mathcal{L})$ sont paires, et donc le morphisme de multiplication $\Gamma(X,\mathcal{L})^2 \to \Gamma(X,\mathcal{L}^2)$ est à valeurs dans $\Gamma(X,\mathcal{L}^2)^+$. Mumford a montré (sans le publier) que la non annulation des thêta null points pairs équivaut à $\Gamma(X,\mathcal{L}^2)^+ = \Gamma(X,\mathcal{L})^2$. Une preuve est donnée dans [Kem88, Théorème 4 et Corollaire 5]. On vérifie aisément que ce résultat implique $\Gamma(X,\mathcal{L}).\Gamma(X,\mathcal{L}^n)^+ = \Gamma(X,\mathcal{L}^{n+1})^+$ [Koi76, Corollaire 4.5.2], autrement dit que l'anneau $\oplus_{n\geqslant 0}\Gamma(K_X,\mathcal{M}^n)$ des sections homogènes de K_X est engendré par $\Gamma(K_X,\mathcal{M})$, et donc que $(K_X,\mathcal{M})$ est projectivement normal. ◇

Théorème 4.8.4 (Heuristique). *Génériquement, si $(a_i)_{i\in Z(\overline{2})} \in \mathcal{M}_{\overline{2}}(k)$ est un thêta null point correspondant à une variété abélienne $(A_k,\mathcal{L},\Theta_{\mathcal{L}})$, alors les thêta null points pairs $U_{\chi,i}^{\mathcal{L}^2}((a_i)_{i\in Z(\overline{2})})$, pour $\chi \in \hat{Z}(\overline{2})$ et $i \in Z(\overline{4})$ avec $\chi(2i) = 1$, ne s'annulent pas.*

Démonstration (Heuristique) : Il nous faut montrer que si $\chi \in \hat{Z}(\overline{2})$ et $i \in Z(\overline{4})$ sont tels que $\chi(2i) = 1$, alors la fonction $(a_i)_{i\in Z(\overline{4})} \in \overline{\mathcal{M}}_{\overline{4}} \mapsto U_{\chi}^{\mathcal{L}^2}((a_i)_{i\in Z(\overline{4})})$ n'est pas identiquement nulle. Si c'est le cas, comme $\mathcal{M}_{\overline{4}}$ est ouvert[1] dans $\overline{\mathcal{M}}_{\overline{4}}$, la fonction $U_{\chi}^{\mathcal{L}^2}$ s'annule sur un sous schéma propre de $\mathcal{M}_{\overline{4}}$ de codimension 1.

On a $U_{\chi,i}^{\mathcal{L}^2}(0_X) = \sum_{t\in Z(\overline{2})} \vartheta^{\mathcal{L}^2}\chi(t)\vartheta_{i+t}(0_X)$. Cette somme n'est pas combinaison linéaire des relations de symétrie $\vartheta_i^{\mathcal{L}^2}(0_X) = \vartheta_{-i}^{\mathcal{L}^2}(0_X)$ si et seulement si $\chi(2i) = 1$. Pour conclure, il faut montrer que les relations de symétrie sont les seules relations de degré 1 sur les coordonnées $\vartheta_i^{\mathcal{L}^2}$ de $\overline{\mathcal{M}}_{\overline{4}}$. Pour cela il faudrait analyser les syzygies des équations du théorème 4.7.2 à l'instar de l'analyse des équations du théorème 4.7.1 effectuée dans [Mum69 ; Kem89, Théorème 24]. par le théorème 4.7.2. ■

Remarque 4.8.5. Si A_k est la Jacobienne d'une courbe hyperelliptique de dimension g, alors le théorème de Frobenius [Mum83, Corollaire 6.7 p. 3.102] montre que si $g \geqslant 3$, il existe toujours des thêta null points pairs nuls pour A_k. En particulier, on ne peut pas appliquer les résultats de cette section à cette classe de variété abéliennes. ◇

Avec la condition de la définition 4.8.1, on va voir qu'on va pouvoir calculer l'addition normale au prix d'une racine carrée. Comme une telle opération est très coûteuse, pour les variétés de Kummer encore plus que pour les variétés abéliennes, on voit qu'il faut minimiser le nombre d'additions normales que l'on effectue par rapport aux pseudo-additions.

Proposition 4.8.6. *Si les thêta null points pairs ne s'annulent pas, pour tous points géométriques $\widetilde{x},\widetilde{y}$ dans $\widetilde{X}$, on peut calculer (modulo un facteur projectif)*

$$\vartheta_i(\widetilde{x+y})\vartheta_j(\widetilde{x-y}) + \vartheta_j(\widetilde{x+y})\vartheta_i(\widetilde{x-y}),$$

1. Comme on l'a vu dans le théorème 4.7.2, ce résultat est seulement conjecturé pour $n = 4$. Mais on a une

pour tout $i, j \in Z(\overline{2})$. En particulier, étant donné $\pm x$ et $\pm y$ dans K_X, on peut calculer l'ensemble $\{\pm(x+y), \pm(x-y)\}$ en utilisant des additions, multiplications, divisions dans k et en calculant une racine carrée.

DÉMONSTRATION : Soit $\widetilde{x+y}$ et $\widetilde{x-y}$ choisis tels que le facteur projectif des formules d'addition soit 1. On a en reprenant les notations du théorème 4.4.6 :

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(\widetilde{0}_X)\vartheta_{l+t}(\widetilde{0}_X)\Big) = \Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(\widetilde{y})\vartheta_{j'+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(\widetilde{x})\vartheta_{l'+t}(\widetilde{x})\Big).$$

Mais le théorème 4.4.3 donne, si k' et $l' \in Z(\overline{4})$ vérifient $k = k' + l'$ et $l = k' - l'$:

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(\widetilde{0}_X)\vartheta_{l+t}(\widetilde{0}_X)\Big) = U^{\mathcal{L}^2}_{\chi,k'}(\widetilde{0}_X)U^{\mathcal{L}^2}_{\chi,l'}(\widetilde{0}_X).$$

De plus, $\chi(2k') = \chi(k+l) = \chi(i+j)$ puisque $i+j+k+l = 0$. Donc si les thêta null points pairs ne s'annulent pas, on peut calculer

$$\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})$$

pour tout $\chi \in \hat{Z}(\overline{2})$ tel que $\chi(i+j) = 1$. En sommant sur ces caractères, on obtient la valeur $\kappa_{i,j}$ de $\vartheta_i(\widetilde{x+y})\vartheta_j(\widetilde{x-y}) + \vartheta_j(\widetilde{x+y})\vartheta_i(\widetilde{x-y})$.

On peut supposer que $\kappa_{0,0} \neq 0$ (quitte à changer d'indice), et que de plus $\widetilde{x-y}$ est choisi de sorte que $\vartheta_0(\widetilde{x-y}) = 1$. On a donc $\vartheta_0(\widetilde{x+y}) = \kappa_{0,0}/2$.

Si $i \in Z(\overline{2})$, on note $P_i = X^2 - 2\frac{\kappa_{i,0}}{\kappa_{0,0}}X + \frac{\kappa_{i,i}}{\kappa_{0,0}}$, le polynôme de racines $\frac{\vartheta_i(\widetilde{x+y})}{\vartheta_0(\widetilde{x+y})}$, $\frac{\vartheta_i(\widetilde{x-y})}{\vartheta_0(\widetilde{x-y})}$. Si x ou y est un point de 2-torsion, $x+y = x-y$ et chaque P_i a une racine double, qui donne le coefficient correspondant de $\vartheta_i(\widetilde{x+y})$. Sinon, il existe $i_0 \in Z(\overline{2})$ tel que la matrice

$$\begin{pmatrix} \vartheta_0(\widetilde{x+y}) & \vartheta_0(\widetilde{x-y}) \\ \vartheta_{i_0}(\widetilde{x+y}) & \vartheta_{i_0}(\widetilde{x-y}) \end{pmatrix}$$

soit inversible.

On peut calculer $\{\vartheta_{i_0}(z_P + z_Q), \vartheta_{i_0}(z_P - z_Q)\}$ grâce aux racines de P_1 (ce qui nécessite de calculer une racine carrée[1]). On se fixe un ordre arbitraire $(\vartheta_{i_0}(\widetilde{x+y}), \vartheta_{i_0}(\widetilde{x-y}))$ de ces racines. Suivant l'ordre que l'on choisit, on calculera soit le couple $(\widetilde{x+y}, \widetilde{x-y})$, soit le couple $(\widetilde{x-y}, \widetilde{x+y})$.

Pour tout $i \in Z(\overline{2})$, on peut alors calculer $(\vartheta_i(\widetilde{x+y}), \vartheta_i(\widetilde{x-y})\}$ en résolvant le système :

$$\begin{pmatrix} \vartheta_0(\widetilde{x+y}) & \vartheta_0(\widetilde{x-y}) \\ \vartheta_{i_0}(\widetilde{x+y}) & \vartheta_{i_0}(\widetilde{x-y}) \end{pmatrix}\begin{pmatrix} \vartheta_i(\widetilde{x-y}) \\ \vartheta_i(\widetilde{x+y}) \end{pmatrix} = \begin{pmatrix} \kappa_{i,0} \\ \kappa_{i,i_0} \end{pmatrix}. \tag{4.33}$$

■

Si l'on veut calculer en pratique l'addition normale $\{\pm(x+y), \pm(x-y)\}$, d'après la proposition 4.8.6, il suffit de calculer les points géométriques de A_k qui satisfont la relation d'addition $x + y = \texttt{chain\_add}(x, y, x-y)$. Un tel système peut être résolu au moyen d'une base de Gröbner, mais la preuve de la proposition 4.8.6 nous donne une méthode directe et plus efficace :

application $\phi_1 : \mathcal{M}_{\overline{8}} \to \mathcal{M}_{\overline{4}}$ (voir le chapitre 6 avec $n = 4$, $\ell = 2$) et on peut appliquer le raisonnement suivant sur $\phi_1^* U^{\mathcal{L}^2}_{\chi}$ dans $\overline{\mathcal{M}_{\overline{8}}}$.

1. Si jamais on travaille sur un corps k non algébriquement clos, et que x, y sont dans $X(k)$, alors $x+y$ et $x-y$

ALGORITHME 4.8.7 (ADDITION SUR LES VARIÉTÉS DE KUMMER) :
Entrées $x = (x_i)_{i\in Z(\overline{2})}, y = (y_i)_{i\in Z(\overline{2})}$ des points géométriques de K_X. Soit $\widetilde{0}_X = (a_i)_{i\in Z(\overline{2})}$ les coordonnées du point neutre de K_X.
Sortie $\{\pm(x+y), \pm(x-y)\}$

➔ Pour tout $i, j \in Z(\overline{2})$, calculer

$$\kappa_{i,j} = \frac{1}{2^{g-1}} \sum_{\chi\in\hat{Z}(\overline{2})|\chi(i+j)=1} \frac{\left(\sum_{t\in Z(\overline{2})} \chi(t) y_{i+t} y_{j+t}\right).\left(\sum_{t\in Z(\overline{2})} \chi(t) x_{i+t} x_{j+t}\right)}{\left(\sum_{t\in Z(\overline{2})} \chi(t) a_{i+t} a_{j+t}\right)}.$$

➔ On se fixe $i_0 \in Z(\overline{2}) \setminus \{0\}$, et on calcule les racines α et β dans k du polynôme

$$X^2 - 2\frac{\kappa_{i_0,0}}{\kappa_{0,0}} X + \frac{\kappa_{i_0,i_0}}{\kappa_{0,0}}.$$

On se fixe $a, b, c, d \in k$ tels que $2ab = \kappa_{0,0}$, $2cd = \kappa_{i_0,i_0}$ et $c/a = \alpha$, $d/b = \beta$.
➔ Pour tout $i \in Z(\overline{2})$, on calcule

$$\begin{pmatrix} \pm(x-y)_i \\ \pm(x+y)_i \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \kappa_{i,0} \\ \kappa_{i,i_0} \end{pmatrix}. \tag{4.34}$$

➔ Retourner $\{(\pm(x+y)_i)_{i\in Z(\overline{2})}, (\pm(x-y)_i)_{i\in Z(\overline{2})}\}$. ◇

REMARQUE 4.8.8. L'algorithme 4.8.7 retourne des points affines $\{X, Y\}$ qui vérifient

$$X = \texttt{chain\_add}(x, y, Y)$$
$$Y = \texttt{chain\_add}(x, y, X)$$

On peut donc l'utiliser pour calculer des pseudo-additions affines sur la variété de Kummer, d'autant plus que si l'on connaît (par exemple) les coordonnées de $\pm(x-y)$, alors on a une racine du polynôme $X^2 - 2\frac{\kappa_{i_0,0}}{\kappa_{0,0}} X + \frac{\kappa_{i_0,i_0}}{\kappa_{0,0}}$, ce qui évite de calculer une racine carré. Bien sûr, si les coordonnées de $\pm(x-y)$ ne s'annulent pas, il est bien plus efficace d'appliquer directement l'algorithme 4.4.10.

Lorsqu'on utilise l'algorithme 4.8.7 pour calculer une addition « normale » sur la variété de Kummer, il faut extraire une racine carré. Si $k = \mathbb{F}_q$, avec $q \equiv 3 \mod 4$, et que $x \in \mathbb{F}_q$ est un carré, alors la racine carré de x est donnée par $x^{\frac{q+1}{4}}$. Dans le cas général, on a toujours un algorithme polynomial en $\log(q)$ pour calculer une racine carré de x, voir [Coh93, Section 1.5 ; Sch85 ; et les améliorations de WNM05 ; BKLS02].

Dans l'algorithme 4.8.7, même si les points x et y de K_X sont rationnels, il peut arriver que les racines α et β ne le soient pas. En effet, si k est parfait, $G = \mathrm{Gal}(\overline{k}/k)$ le groupe de Galois absolu, soit x un point géométrique de X_k vérifiant $G.x = \{x, -x\}$. Alors x n'est pas un point rationnel de X_k, mais sa projection dans K_X l'est. Si $y \in X_k(k)$, alors $G.(x+y) = \{x+y, -x+y\}$, et donc si y n'est pas un point de 2-torsion, comme x ne l'est pas non plus, le point $x + y \in X_k(\overline{k})$ n'est pas rationnel. Ainsi, il peut arriver que la somme de deux points rationnels dans K_X ne soit pas rationnelle. L'exemple typique d'une telle situation est le cas d'une courbe elliptique E d'équation $y^2 = f(x)$. La variété de Kummer associée à E est la droite projective $\mathbb{P}^1_k$, et la projection $E \to \mathbb{P}^1_k$ est donnée sur les points géométriques par $(x, y, z) \mapsto (x, z)$, où z est une variable d'homogénéisation. Alors si $x \in k$ est un point tel que $y = (f(x))^{1/2} \notin k$, le point (x, y) donne un exemple de point non rationnel dans E dont la projection sur la variété de Kummer est rationnelle. ◇

sont dans k, et la racine que l'on calcule est dans k.

EXEMPLE 4.8.9 (MULTIPLICATION DANS UNE VARIÉTÉ ABÉLIENNE). Le but de cet exemple est de montrer comment se combinent l'algorithme 4.4.12 et la remarque 4.6.10 pour calculer la multiplication sur une variété abélienne en se ramenant aux formules de niveau 2. Soit $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété abélienne marquée de niveau δ telle que $2 \mid \delta$. On pose alors $\delta = 2\delta'$. Soit π l'isogénie de type $\hat{Z}(\delta')$ (voir la section 4.6). Soit $x \in A_k$ un point géométrique, et $n \in \mathbb{N}$; on veut calculer les coordonnées compressées de x. Si $\mathfrak{S}$ est une base de décompression (de cardinal au plus 2^g où g est la dimension de A_k), les coordonnées compressées de $n.x$ sont données par

$$(\widetilde{\pi}_i(n.x))_{i\in\mathfrak{S}} = (\texttt{chain\_multadd}(n, \widetilde{\pi}_0(x), \widetilde{\pi}_i(x), \widetilde{\pi}_i(\widetilde{0}_{A_k})))_{i\in\mathfrak{S}}.$$

On suppose que les coordonnées de $\widetilde{\pi}_i(x)$ et $\widetilde{\pi}_i(\widetilde{0}_{A_k})$ sont non nulles pour $i \in \mathfrak{S}$, ainsi que les fonctions $U^{\mathcal{L}^2}_{\chi,0}(\widetilde{0}_{A_k})$ pour $\chi \in \hat{Z}(\bar{2})$, ce qui nous permet de calculer des pseudo-additions via l'algorithme 4.4.10. On peut expliciter cet algorithme en dimension 1 et 2 :

ALGORITHME 4.8.10 (PSEUDO-ADDITION EN DIMENSION 1 ET NIVEAU 2 [GL09]) :
Soit $\widetilde{\pi}_0(\widetilde{0}_{A_k}) = (a, b)$, et $(U^{\mathcal{L}^2}_{\chi,0})_{\chi\in\hat{Z}(\bar{2})} = (A, B)$. Les formules de duplication (théorème 4.4.3) montrent que $2A^2 = a^2 + b^2$ et $2B^2 = a^2 - b^2$.

Entrées $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P - Q = (x_3, y_3)$.
Sortie $P + Q$.

- ➔ $x_0 = (x_1^2 + y_1^2)(x_2^2 + y_2^2)/A^2$.
- ➔ $y_0 = (x_1^2 - y_1^2)(x_2^2 - y_2^2)/B^2$.
- ➔ $x = (x_0 + y_0)/x_3$.
- ➔ $y = (x_0 - y_0)/y_3$.
- ➔ Retourner (x, y) ◇

ALGORITHME 4.8.11 (PSEUDO ADDITION EN DIMENSION 2 ET NIVEAU 2 [GAU07]) :
Soit $\widetilde{\pi}_0(\widetilde{0}_{A_k}) = (a, b, c, d)$, et

$$\begin{aligned} 4A^2 &= a^2 + b^2 + c^2 + d^2 \\ 4B^2 &= a^2 + b^2 - c^2 - d^2 \\ 4C^2 &= a^2 - b^2 + c^2 - d^2 \\ 4D^2 &= a^2 - b^2 - c^2 + d^2 \end{aligned}$$

Entrées $P = (x_1, y_1, z_1, t_1)$, $Q = (x_2, y_2, z_2, t_2)$, $P - Q = (x_3, y_3, z_3, t_3)$.
Sortie $P + Q$

- ➔ $x_0 = (x_1^2 + y_1^2 + z_1^2 + t_1^2)(x_2^2 + y_2^2 + z_2^2 + t_2^2)/A^2$.
- ➔ $y_0 = (x_1^2 + y_1^2 - z_1^2 - t_1^2)(x_2^2 + y_2^2 - z_2^2 - t_2^2)/B^2$.
- ➔ $z_0 = (x_1^2 - y_1^2 + z_1^2 - t_1^2)(x_2^2 - y_2^2 + z_2^2 - t_2^2)/C^2$.
- ➔ $t_0 = (x_1^2 - y_1^2 - z_1^2 + t_1^2)(x_2^2 - y_2^2 - z_2^2 + t_2^2)/D^2$.
- ➔ $x = (x_0 + y_0 + z_0 + t_0)/x_3$.
- ➔ $y = (x_0 + y_0 - z_0 - t_0)/y_3$.
- ➔ $z = (x_0 - y_0 + z_0 - t_0)/z_3$.
- ➔ $t = (x_0 - y_0 - z_0 + t_0)/t_3$.
- ➔ Retourner (x, y, z, t) ◇

Maintenant, pour calculer la multiplication par $[\ell]$, si on revient à l'algorithme 4.4.12, à chaque étape, on va ajouter le même point $\widetilde{\pi}_0(m\widetilde{x})$ aux points $(\widetilde{\pi}_i(m\widetilde{x}))_{i\in\mathfrak{S}}, \widetilde{\pi}_0((m-1)\widetilde{x})$

	Niveau 2	Cas général
$g = 1$	$2M + 6S + 1m + 3m_0$	$6M + 10S + 3m + 6m_0$
$g = 2$	$4M + 12S + 3m + 9m_0$	$28M + 36S + 15m + 28m_0$
g général	$2^g M + 3.2^g S +$ $(2^g - 1)m + 3(2^g - 1)m_0$	$(2^{2g+1} - 2^g)M + (2^{2g+1} + 2^g)S +$ $(2^{2g} - 1)m + (2^{2g+1} - 2^g)m_0$

TABLE 4.1 – Coût d'une étape de la multiplication

(ou aux points $(\widetilde{\pi}_i((m+1)\widetilde{x})_{i\in\mathfrak{S}}, \widetilde{\pi}_0(m\widetilde{x})$ suivant la décomposition binaire de ℓ). Donc à chaque étape on effectue 1 doublement et $2\#\mathfrak{S} - 1$ pseudo-additions, en réutilisant les calculs faits pour le doublement. De plus, on peut travailler sur les carrés des coordonnées (sauf à la dernière étape) ; et les différences qui apparaissent sont les $\widetilde{\pi}_i(\widetilde{x})$, $\widetilde{\pi}_i(\widetilde{0}_{A_k})$, $i \in \mathfrak{S}$, donc on peut calculer au début de la multiplication les $2^g\#\mathfrak{S}$ inverses des coordonnées des $\widetilde{\pi}_i(\widetilde{x})$.

On utilise les notations suivantes : S représente un carré, M une multiplication, m une multiplication par une constante qui ne dépend que du point que l'on veut multiplier, et m_0 une multiplication qui ne dépend que du thêta null point. Le doublement coûte $2.2^g S + 2.2^g m_0$, tandis que chaque pseudo-addition coûte $2^g M + 2^g S + 2^g m_0 + 2^g m$. De plus, on peut supposer que $a = 1$ (en reprenant les notations de l'algorithme 4.8.10), ce qui fait gagner $1m_0$. Si l'on est juste intéressé par la valeur projective du résultat, on peut de plus supposer que $A = 1$, et qu'une coordonnée de $\widetilde{x}$ est égale à 1, ce qui fait gagner $1m_0 + 1m$.

En faisant ces hypothèses, on obtient que le coût d'un doublement en niveau 2 est donc de $2^{g+1}S + 2(2^g - 1)m_0$, et celui d'une addition différentielle mixte de $2^g M + 2^g S + (2^g - 1)m + (2^g - 1)m_0$, pour un coût total par étape de multiplication de $2^g M + 3.2^g S + (2^g - 1)m + 3(2^g - 1)m_0$. En niveau $n = 2n_0$, le doublement coûte $(n^g - 2^g)M + (n^g + 2^g)S + (2.n^g - n_0^g - 1)m_0$, et une addition différentielle mixte $n^g M + n^g S + (n^g - 1)m + (n^g - n_0^g)m_0$. Enfin, en utilisant des coordonnées compresées, en prenant $\#\mathfrak{S} = 2^g$, le doublement coûte $(2^{2g} - 2^g)M + (2^{2g} + 2^g)S + (2^{2g} - 1)m_0$ et l'addition différentielle mixte coûte $2^{2g}M + 2^{2g}S + (2^{2g} - 1)m + (2^{2g} - 2^g)m_0$. On trouvera un résumé dans le tableau 4.1 du coût d'une étape de la multiplication (il y en a $O(\log_2(\ell))$). Nous avons fait l'hypothèse dans ce tableau que $a = A = 1$. On trouvera le cas du niveau 2 (avec $\#\mathfrak{S} = 1$) et le cas général où l'on a pris $\#\mathfrak{S} = 2^g$.

Si les coordonnées du thêta null point ne sont pas assez petites pour être négligées, alors il est plus efficace de stocker en mémoire les multiplications par une constante lorsqu'on calcule le doublement, ce qui fait que le doublement coûte $2^g M + 2^g S + 2.2^g m_0$ (si l'on suppose $A = a = 1$, on gagne $1m_0 + 1M - 1S$), et une pseudo-addition coûte $2^g M + 2^g S + 2^g m$ ou $2^g M + 2^g S + 2^g m_0$ suivant les cas. On remplace ainsi des carrés par des multiplications, mais on diminue le nombre de multiplications par une constante, ce qui peut être rentable si ces constantes sont grandes.

Dans ce cas, et toujours avec l'hypothèse $a = A = 1$, on obtient que le coût d'un doublement en niveau 2 est de $(2^g - 1)M + (2^g + 1)S + 2(2^g - 1)m_0$, et celui d'une addition différentielle mixte de $2^g M + 2^g S + (2^g - 1)m$, pour un coût total par étape de multiplication de $(2^{g+1} - 1)M + (2^{g+1} + 1S) + (2^g - 1)m + 2(2^g - 1)m_0$. En niveau $n = 2n_0$, le doublement coûte $(n^g - 1)M + (n^g + 1)S + (n^g + 2^g - 2)m_0$, et une addition différentielle mixte $n^g M + n^g S + (n^g - 1)m$. Enfin, en utilisant des coordonnées compresées, en prenant $\#\mathfrak{S} = 2^g$, le doublement coûte $(2^{2g} - 1)M + (2^{2g} + 1)S + (2^{2g} + 2^g - 2)m_0$ et l'addition différentielle mixte coûte $2^{2g}M + 2^{2g}S + (2^{2g} - 1)m$. Le coût d'une étape (il y en a $O(\log_2(\ell))$) est résumé dans le tableau 4.2.

On peut comparer cette méthode avec la multiplication en effectuant des additions nor-

	Niveau 2	Cas général
$g = 1$	$3M + 5S + 1m + 2m_0$	$7M + 9S + 3m + 4m_0$
$g = 2$	$7M + 9S + 3m + 6m_0$	$31M + 33S + 15m + 18m_0$
g général	$(2^{g+1}-1)M + (2^{g+1}+1)S +$ $(2^g-1)m + (2^{g+1}-2)m_0$	$(2^{2g+1}-1)M + (2^{2g+1}+1)S +$ $(2^{2g}-1)m + (2^{2g}+2^g-2)m_0$

TABLE 4.2 – Coût d'une étape de la multiplication, lorsque les constantes liées à la variété abélienne sont grandes

males, qui à chaque étape fait un doublement ou un doublement et une addition. Avec les mêmes hypothèses que pour le tableau 4.2, si l'on travaille sur les carrés des coordonnées, un doublement en niveau n coûte : $(n^g-1)M + (n^g+1)S + (n^g+2^g-2)m_0$, tandis qu'une addition normale coûte $n^g(2^{g+1}+1)M + n^gS + (n^g-1)m_0$. (Si l'on calcule une addition mixte, c'est-à-dire qu'un des points a une coordonnée égale à 1, on gagne n^gM.) On voit que même en niveau 4, suivant la proportion de bits égaux à 1 dans le développement binaire de ℓ, il peut être plus rapide de calculer la multiplication en utilisant des pseudo-additions (si l'on est prêt à prendre des inversions au début) qu'en faisant des additions normales.

À titre de comparaison, l'addition en coordonnées de MUMFORD (Jacobiennes) en genre 2 nécessite $7S + 47M$, l'addition mixte (un point à une coordonnée égale à 1, on peut supposer que c'est le cas pour le calcul de la multiplication) $6S + 37M$, et le doublement $7S + 34M$ [Lano5]. On voit dans ce cas que le niveau 2 est bien meilleur[1], mais le niveau 4 est moins bon. En genre 1, sur une courbe elliptique d'équation de Weierstrass $y^2 = x^3 + ax + b$, la formule d'addition la plus rapide vient de la représentation des points par les coordonnées Jacobiennes (étendues) (X, Y, Z, T) avec $x = X/Z^2$, $y = Y/Z^3$ et $T = Z^2$ [ALNR09]. L'addition coûte $11M + 7S$, l'addition mixte coûte $7M + 6S$ et le doublement $3M + 5S$ [BL07b]. Là encore, la multiplication via les fonctions thêta reste compétitive, surtout en niveau 2 si on peut choisir de petites constantes. Il serait intéressant de regarder si les formules d'addition en niveau 3 donnent un meilleur résultat que l'algorithme de Cantor en dimension 2. (On peut consulter [Gau07] pour une discussion du cas du genre 2 niveau 2, et [GL09] pour une généralisation au genre 1 et à la caractéristique 2, toujours en niveau 2.) ◇

On a besoin d'un troisième type d'addition, que l'appelle addition « compatible », afin de pouvoir appliquer les résultats de la seconde partie au cas du niveau 2. Comme on le verra, le niveau 2 permet d'atteindre la plus grande efficacité dans les algorithmes (notamment ceux du chapitre 7), il est donc crucial de savoir les étendre à ce cas-là.

L'idée est la suivante : on se donne trois points géométriques x, y, z de la variété de Kummer K_X. On suppose qu'on s'est fixé deux choix $\pm(x+z) \in \{\pm(x+z), \pm(x-z)\}$, et $\pm(y+z) \in \{\pm(y+z), \pm(y-z)\}$. Alors on peut identifier $\pm(x+y) \in \{\pm(x+y), \pm(x-y)\}$. En effet, si on effectue une addition normale entre $\pm(x+y)$ et $\pm(x+z)$ on obtient $\{\pm(2x+y+z), \pm(y-z)\}$, tandis qu'une addition normale entre $\pm(x-y)$ et $\pm(x+z)$ nous donne $\{\pm(2x+z-y), \pm(y+z)\}$. Ceci nous permet bien d'identifer $\pm(x+y)$ si $2x \neq 0_X$, $2y \neq 0_X$, $2z \neq 0_X$, $2(x+y+z) \neq 0_X$.

De plus, on peut calculer une telle addition compatible sans avoir à calculer explicitement une racine carrée dans k. Le principe est le suivant : dans l'algorithme 4.8.7, si $P = X^2 - 2\frac{\kappa_{i_0,0}}{\kappa_{0,0}}X + \frac{\kappa_{i_0,i_0}}{\kappa_{0,0}}$, au lieu de calculer les racines de P, on travaille dans l'extension $k[X]/P$ (cette extension n'est pas un corps, mais si l'on tombe sur un élément non inversible on a trouvé une racine de

1. Surtout qu'un grand nombre de multiplications sont des multiplications par des constantes dépendant uniquement de la variété abélienne, et que l'on peut les choisir pour les rendre négligeables, voir [Ber06].

P, donc algorithmiquement on peut supposer que l'on travaille sur un corps). On applique le reste de l'algorithme en travaillant sur cette extension, on obtient alors $\{\pm(x+y), \pm(x-y)\}$ formellement. On applique à nouveau l'algorithme 4.8.7 avec $\pm(x+y)$ et $\pm(x+z)$, on obtient encore une fois un polynôme P' lors de l'étape 2. Cependant on connaît une racine de P' car on connaît les coordonnées de $\pm(y-z)$. En évaluant P' en cette racine, on obtient un élément $\alpha X + \beta$ de $k[X]/P$ qui doit être nul lorsqu'on remplace X par la racine de P associée à $\pm(x+y)$. Ceci permet de retrouver une racine de P.

Exemple 4.8.12 (Addition compatible). Soit C la courbe hyperelliptique sur $\mathbb{F}_{1937419401974319377}$, donnée par le polynôme

$$f = X^5 + 718435286390965184X^4 + 1636958131611282564X^3 + 716356054668642674X^2 + 803089331277748331X.$$

Un point modulaire de niveau 2 associé à la Jacobienne J de C est donné par

$$(1492460524295988209 : 1248528113709005802 : 1267036383052999682 : 1).$$

L'équation de la variété de Kummer K associée à J est donnée (dans les coordonnées thêta de niveau 2) par (voir la section 8.2.2) :

$$\begin{aligned}\vartheta_{(0,0)}^4 + 1105030489589048648\vartheta_{(0,0)}^2\vartheta_{(1,0)}^2 + 1732746955641783324\vartheta_{(0,0)}^2\vartheta_{(0,1)}^2 \\ +1216540098502427636\vartheta_{(0,0)}^2\vartheta_{(1,1)}^2 + 1437304177842156509\vartheta_{(0,0)}\vartheta_{(1,0)}\vartheta_{(0,1)}\vartheta_{(1,1)} + \vartheta_{(1,0)}^4 \\ +1216540098502427636\vartheta_{(1,0)}^2\vartheta_{(0,1)}^2 + 1732746955641783324\vartheta_{(1,0)}^2\vartheta_{(1,1)}^2 \\ +\vartheta_{(0,1)}^4 + 1105030489589048648\vartheta_{(0,1)}^2\vartheta_{(1,1)}^2 + \vartheta_{(1,1)}^4 = 0.\end{aligned}$$

Soit

$$\begin{aligned}x &= (1744570601175213633 : 516530529869770602 : 166020876972545982 : 1),\\ y &= (1720232358604880385 : 1630976880928650471 : 39870385966558281 : 1),\\ z &= (446623626639573423 : 1069727519312660209 : 884054351179222982 : 1),\end{aligned}$$

des points géométriques (pris au hasard) de K.

On calcule en utilisant l'algorithme 4.8.7 :

$$\begin{aligned}&\{\pm(x+y), \pm(x-y)\} = \\ &\quad\{(1444193261424216265 : 753441823061122476 : 843978741775952645 : 1),\\ &\quad\ (1459935953994389014 : 719628298264142569 : 392430493374322185 : 1)\}\\ &\{\pm(x+z), \pm(x-z)\} = \\ &\quad\{(407392633335168336 : 280748078208728888 : 1704551696537067073 : 1),\\ &\quad\ (522618946729802140 : 287904973270212123 : 1095362825794512973 : 1)\}\\ &\{\pm(y+z), \pm(y-z)\} = \\ &\quad\{(1377715090095818289 : 1482477747003475569 : 136714468218104728 : 1),\\ &\quad\ (624672390117217104 : 421157184463500556 : 1224771828998559052 : 1)\}\end{aligned}$$

On fixe

$$\begin{aligned}\pm(x+y) &= (1444193261424216265 : 753441823061122476 : 843978741775952645 : 1),\\ \pm(x+z) &= (407392633335168336 : 280748078208728888 : 1704551696537067073 : 1)\end{aligned}$$

et on calcule :

$$\begin{aligned}&\{\pm(x+y+x+z), \pm(x+y-x-z)\} = \\ &\quad\{(1445688298181394734 : 20359819254574917 : 810717515165735860 : 1),\\ &\quad\ (624672390117217104 : 421157184463500556 : 1224771828998559052 : 1)\}\end{aligned}$$

Donc les points

$$(1444193261424216265 : 753441823061122476 : 843978741775952645 : 1),$$
$$(407392633335168336 : 280748078208728888 : 1704551696537067073 : 1),$$
$$(1445688298181394734 : 20359819254574917 : 810717515165735860 : 1)$$

sont compatibles. ◊

Deuxième partie

APPLICATIONS

5 PAIRINGS

MATIÈRES

5.1 INTRODUCTION

On a vu l'importance dans le chapitre 2 de la forme de Riemann d'une variété abélienne complexe $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$. Lorsqu'on a une variété abélienne $(A_k, \mathcal{L})$ polarisée sur un corps k, on n'a plus de forme de Riemann, par contre le pairing de Weil donne un pairing alterné sur les modules de Tate $T_\ell(A_k)$ pour ℓ premier à la caractéristique p de k par [Mum70, Section 20]. De plus, dans le cadre complexe, si E est la forme de Riemann principale sur le réseau Λ associé à une variété complexe X, le pairing de Weil sur $T_\ell X$ est l'extension $Z(\overline{\ell})$-linéaire de E par [Mum70, Section 24] (voir aussi [Del69, p. 239] pour le lien entre le pairing de Weil sur le module de Tate d'une variété abélienne ordinaire sur un corps fini, et la forme de Riemann du complexifié de son relèvement canonique).

On a vu dans la section 1.3.3 l'importance du pairing pour les applications cryptographiques. On peut se demander s'il est possible de le calculer efficacement avec les coordonnées thêta, sans utiliser une transformation coûteuse vers les coordonnées de MUMFORD. La réponse est donnée par l'algorithme 5.4.2, qui de manière surprenante n'utilise pas l'algorithme de Miller. La raison en est la suivante : dans ce chapitre on explique comment calculer le commutator pairing (étendu), que l'on peut voir comme une forme plus générale du pairing de Weil. Si $(A_k, \mathcal{L})$ est une variété polarisée, et que l'on se fixe un entier ℓ (qui est premier pour les applications), le commutator pairing (étendu) est simplement le pairing $e_{\mathcal{L}^\ell}$ sur $K(\mathcal{L}^\ell)$. Le pairing e_ℓ de Weil, lui, est défini sur $A_k[\ell] \times \widehat{A}_k[\ell]$. Le lien entre les deux est donné dans la section 5.2.2 : si $\phi_{\mathcal{L}}$ est la polarisation associée à $\mathcal{L}$, alors $e_{\mathcal{L}^\ell}(x, y) = e_\ell(x, \phi_{\mathcal{L}}(y))$ si x et y sont des points de ℓ-torsion. L'article [LR10b] étudie l'algorithme 5.4.2 dans le cadre analytique, une version algébrique est donnée dans [LR10a]. Dans ce chapitre, nous généralisons l'algorithme donné dans ces articles au calcul du commutator pairing étendu sur tout $K(\mathcal{L}^\ell)$, et non uniquement sur $K(\mathcal{L}^\ell)[\ell]$.

On rappelle le lien entre pairings et isogénies dans la section 5.2 : la dualité de Cartier associe un pairing à chaque isogénie. Nous appliquons cela à deux types d'isogénies : l'isogénie associée à une polarisation dans la section 5.2.1, qui redonne le commutator pairing de la polarisation, et l'isogénie de multiplication par $[n]$ dans la section 5.2.2, qui donne le pairing

de Weil. On introduit ensuite rapidement dans la section 5.2.3 le pairing de Tate, qui est pour des raisons algorithmique le plus pratique pour des applications cryptographiques. Dans la section 5.3, nous regardons le lien entre ces pairings et la forme de Riemann d'une variété abélienne complexe, et nous donnons une méthode pour calculer le pairing de Tate ou de Weil uniquement en évaluant des fonctions thêta sur des points bien choisis. Nous étendons ces résultats au cadre algébrique dans la section 5.4, où nous donnons un algorithme pour calculer le commutator pairing étendu $e_{\mathcal{L}^\ell}$ sur une variété abélienne polarisée $(A_k, \mathcal{L})$ qui utilise uniquement les formules d'addition du chapitre 4. Une comparaison avec l'algorithme de Miller est donnée dans la section 5.4.1. On peut déjà noter un intérêt de l'algorithme 5.4.2 par rapport à l'algorithme 1.3.2 : il s'applique à toutes les variétés abéliennes, tandis que l'algorithme de Miller est restreint aux jacobiennes de courbes hyperelliptiques. Or il existe des variétés abéliennes supersingulières de dimension 4 optimales pour le pairing [RS09] qui ne sont pas des jacobiennes de courbes hyperelliptiques. (Elles apparaissent comme la sous-variété de trace 0 de la descente de Weil d'une courbe elliptique supersingulière définie sur une extension de degré 5. Pour calculer le couplage avec l'algorithme de Miller, il faut alors remonter à cette courbe elliptique.)

Enfin, nous introduisons dans la section 5.5 un pairing symétrique sur les variétés de Kummer, et expliquons comment le calculer grâce aux résultats précédents. On peut visualiser ce pairing symétrique comme une manière de calculer le pairing de Weil ou le commutator pairing étendu sur des points représentés par des coordonnées compressées en niveau 2 (voir la section 4.6).

5.2 PAIRINGS ET ISOGÉNIES

Soit $f : A_k \to B_k$ une isogénie entre deux variétés abéliennes définies sur un corps k. On a alors le diagramme suivant

$$0 \longrightarrow K \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$

$$0 \longleftarrow \hat{A} \xleftarrow{\hat{f}} \hat{B} \longleftarrow \hat{K} \longleftarrow 0.$$

où K est le noyau de f et $\hat{K}$ celui de l'isogénie duale $\widehat{f}$ [GM07, Theorem 7.5].

Le noyau $\hat{K}$ est le dual de Cartier de K. Ainsi l'isogénie f donne un pairing (usuellement appelé le pairing de Cartier) [GM07, Definition 11.11] :

$$e_f : K \times \hat{K} \to \mathbb{G}_{m,k}.$$

De plus, si $K \subset A_k[\ell]$, e_f prend ses valeurs dans $\mu_\ell \subset \mathbb{G}_{m,k}$. On peut calculer ce pairing sur les points géométriques ainsi : soit $Q \in \hat{K}(\overline{k})$. Q est un fibré en droites sur $B_{\overline{k}}$, et $\widehat{f}(Q) = f^*Q = 0 \in \mathrm{Pic}_0(A_{\overline{k}})$, donc f^*Q est isomorphe au fibré trivial $\mathcal{O}_{A_{\overline{k}}}$ sur $A_{\overline{k}}$. Autrement dit $\mathcal{O}_{A_{\overline{k}}}$ descend via f sur le fibré Q : on est donc dans la situation de la section 3.3 et on a une section $K \to G(\mathcal{O}_{A_{\overline{k}}})$ associée à un isomorphisme $\psi_Q : f^*Q \to \mathcal{O}_{A_{\overline{k}}}$. Alors la multiplication

par $e_f(P,Q)$ fait commuter ce diagramme :

$$\begin{array}{ccc} f^*Q & \xrightarrow{\psi_Q} & \mathscr{O}_A \\ \| & & \| e_f(P,Q) \\ \tau_P^* f^* Q & \xrightarrow{\tau_P^*\psi_Q} & \tau_P^*\mathscr{O}_A. \end{array} \tag{5.1}$$

On peut voir les choses ainsi : comme $\mathcal{O}_{A_{\overline{k}}} \in \mathrm{Pic}_0(A_{\overline{k}})$, $G(\mathcal{O}_{A_{\overline{k}}}) = A_{\overline{k}} \times \overline{k}$ est commutatif (car $e_{\mathcal{O}_{A_{\overline{k}}}}$ est trivial sur $A_{\overline{k}}$). L'action de $G(\mathcal{O}_{A_{\overline{k}}})$ sur le fibré trivial $A_{\overline{k}} \times \mathbb{A}^1_{\overline{k}}$ est donnée par $(x,\lambda).(y,\gamma) = (x+y, \lambda\gamma)$. Ainsi la section $K \to G(\mathcal{O}_{A_{\overline{k}}})$ nous donne un caractère χ tel que K agit sur le fibré trivial par $x.(y,\gamma) = (y+x, \chi(x)\gamma)$ et Q est le quotient de $A_{\overline{k}} \times \mathbb{A}^1_{\overline{k}}$ par cette action. On a alors [Mum70, p. 183 ; GM07, (11.12)] :

$$e_f(P,Q) = \chi(P).$$

De manière plus géométrique, si D est un diviseur qui représente Q, f^*D est trivial donc est le diviseur d'une fonction rationnelle g_Q. Alors $g_Q/t_P^* g_Q = \chi(P)$ et donc [Mum70, p. 184 ; GM07, (11.13)]

$$e_f(P,Q) = g_Q(X)/g_Q(X+P) \tag{5.2}$$

où X est un point géométrique quelconque de $A_{\overline{k}}$ tel que $g(X+P)$ soit bien défini.

Enfin e_f est fonctoriel en f, si on a des isogénies $\alpha : U_k \to A_k$ et $\beta : B_k \to V_k$, alors lorsque $P \in \alpha^{-1}(K(\overline{k}))$ et $Q \in \hat{\beta}^{-1}\hat{K}(\overline{k})$ on a

$$e_{\alpha\circ f\circ\beta}(P,Q) = e_f(\alpha P, \hat{\beta} Q).$$

5.2.1 *Pairings et polarisations*

Si $\mathcal{L}$ est un fibré ample sur A_k, et qu'on regarde le pairing associé à la polarisation $\phi_{\mathcal{L}} : A_k \to \widehat{A}_k$, comme $\hat{\phi}_{\mathcal{L}} = \phi_{\mathcal{L}}$ canoniquement, on obtient un pairing $e_{\phi(\mathcal{L})}$ sur $K(\mathcal{L}) \times K(\mathcal{L})$.

Si on regarde le diagramme (5.1), on voit facilement que le diagramme suivant est commutatif à une multiplication par $e_{\phi(\mathcal{L})}(P,Q)$ près :

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{\psi_P} & \tau_P^*\mathcal{L} \\ \downarrow \psi_Q & & \downarrow \tau_P^*\psi_Q \\ \tau_Q^*\mathcal{L} & \xrightarrow{\tau_Q^*\psi_P} & \tau_{P+Q}^*\mathcal{L}. \end{array}$$

(Dans ce diagramme, on suppose que P et Q sont des points rationnels de $K(\mathcal{L})$. Si P et Q sont des points géométriques, il suffit de considérer le même diagramme en étendant $\mathcal{L}$ par extension des scalaires.)

Ainsi si $g_P = (P, \psi_P) \in G(\mathcal{L})$ et $g_Q = (Q, \psi_Q) \in G(\mathcal{L})$, on a

$$e_{\phi(\mathcal{L})}(P,Q) = g_P g_Q g_P^{-1} g_Q^{-1} = e_{\mathcal{L}}(P,Q).$$

Les propriétés fonctorielles de $e_{\mathcal{L}}$ sont données par [Mum70, p. 228] :

1. Si $f : A_k \to B_k$ est une isogénie et $\mathcal{M}$ un fibré ample sur B_k,
$$e_{f^*\mathcal{M}}(x, y) = e_{\mathcal{M}}(f(x), f(y))$$
pour tous $x, y \in f^{-1}(K(\mathcal{M}))$.
2. Si $\mathcal{L}_1$ et $\mathcal{L}_2$ sont des fibrés sur A_k, on a $e_{\mathcal{L}_1\otimes\mathcal{L}_2}(x, y) = e_{\mathcal{L}_1}(x, y)e_{\mathcal{L}_2}(x, y)$ pour tous $x, y \in K(\mathcal{L}_1) \cap K(\mathcal{L}_2)$.
3. $e_{\mathcal{L}^\ell}(x, y) = e_{\mathcal{L}}(x, \ell y)$ pour tous $x \in K(\mathcal{L})$ et $y \in [\ell]^{-1}(K(\mathcal{L}))$.

Si $x, y \in [\ell]^{-1}(K(\mathcal{L}))$, on peut aussi donner la définition suivante de $e_{\mathcal{L}^\ell}(x, y)$ qui est très importante par la suite : soit $x', y' \in A_k$ tels que $x = \ell x'$ et $y = \ell y'$. Alors

$$e_{\mathcal{L}^\ell}(x, y) = e_{[\ell]^*\mathcal{L}}(x', y) = e_{[\ell]^*\mathcal{L}}(x, y') = e_{[\ell]^*\mathcal{L}}(x', y')^\ell.$$

En effet, comme $e_{\mathcal{L}}$ ne dépend que de la polarisation associée à $\mathcal{L}$, on peut supposer $\mathcal{L}$ symétrique, et alors $[\ell]^*\mathcal{L} = \mathcal{L}^{\ell^2}$. On a alors $e_{\mathcal{L}^{\ell^2}}(x', y) = e_{\mathcal{L}^\ell}(\ell x', y) = e_{\mathcal{L}^\ell}(x, y)$ par le point 3.

5.2.2 *Le pairing de Weil*

Le signe de $e_W(P, Q)$ a changé par rapport à l'équation (5.2) pour être cohérent avec les définitions usuelles du pairing de Weil.

Le pairing de Weil est le pairing e_ℓ associé à l'isogénie $[\ell] : A_k \to A_k$. C'est un pairing défini sur $A_k[\ell] \times \widehat{A}_k[\ell]$. Si on revient à la définition de la section 5.2, si P est un point de ℓ-torsion de A_k et $Q \in \widehat{A}_k[\ell]$ est représenté par un diviseur D, les diviseurs $[\ell]^*D$ et $\ell.D$ sont triviaux et donc représentés par des fonctions g_Q et f_Q. Le pairing de Weil $e_W(P, Q)$ est donné par $e_W(P, Q) = g_Q(X + P)/g_Q(X)$ [Sil86, Section 8]. De plus, comme $\ell.[\ell]^*D = [\ell]^*\ell.D$, on a $[\ell]^*f_Q = g_Q^\ell$, on vérifie donc bien que $e_W(P, Q)^\ell = f_Q(X + \ell.P)/f_Q(X) = 1$. Comme $\widehat{\widehat{A}}_k$ est canoniquement isomorphe à A_k, on peut voir P comme un fibré en droites sur $\widehat{A}_k$, représenté par un diviseur D', et il existe donc une fonction rationnelle f_P qui représente le diviseur $\ell.D'$. La réciprocité de Weil [Sil86, Exercice 2.11] (que l'on peut utiliser si A_k est une Jacobienne, sinon il faut utiliser la réciprocité de Lang [Lan58, Théorème 6]) nous donne alors [Sil86, Exercice 3.16] :

$$e_W(P, Q) = \frac{f_Q((P) - (0))}{f_P((Q) - (0))}.$$

((Si le support de f_Q n'est pas disjoint du support de $(P) - (0)$, on remplace dans la formule précédente $(P) - (0)$ par un cycle équivalent [Lan58, Appendice]. Plus généralement, à chaque fois que l'on évalue une fonction rationnelle f sur un cycle, on fait toujours l'hypothèse que le support de (f) est disjoint du cycle.))

Maintenant, si $\mathcal{L}$ est une polarisation sur A_k, on peut considérer l'isogénie $[\ell] \circ \phi_{\mathcal{L}}$

$$A_k \xrightarrow{[\ell]} A_k \xrightarrow{\mathcal{L}} \widehat{A}_k.$$

Si $x \in A_k(\overline{k})$, comme $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \in \mathrm{Pic}_0(A_k)(\overline{k})$, on a $t_x^*(t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}) \simeq t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. On a alors $t_{2x}^*\mathcal{L} \otimes \mathcal{L}^{-1} = t_x^*(t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}) \otimes t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \simeq t_x^*\mathcal{L}^2 \otimes \mathcal{L}^{-2}$. Plus généralement on a un isomorphisme (que l'on peut aussi obtenir via le théorème du square du corollaire 2.4.4) : $t_{\ell x}^*\mathcal{L} \otimes \mathcal{L}^{-1} \simeq t_x^*\mathcal{L}^\ell \otimes \mathcal{L}^{-\ell}$ et donc l'isogénie $[\ell] \circ \phi_{\mathcal{L}}$ est simplement la polarisation $\mathcal{L}^\ell$.

Le lien entre le pairing associé à cette polarisation et le pairing de Weil est donc donné par [Mum70, p. 236] :

$$e_{\mathcal{L}^\ell}(x, y) = e_\ell(x, \phi_{\mathcal{L}}(y))$$

pour tous $x \in A_k[\ell]$ et $y \in [\ell]^{-1}K(\mathcal{L}) = \phi_{\mathcal{L}}^{-1}(\widehat{A}_k[\ell])$.

EXEMPLE 5.2.1. Soit $X = V/\Lambda$ une variété abélienne complexe, et $\mathcal{L} = L(H, \chi)$ un fibré sur X. Soit $\pi : V \to X$ la projection, on a vu dans l'exemple 3.2.4 que $e_{\mathcal{L}}(x, y) = e^{-2\pi i \operatorname{Im} H(\widetilde{x},\widetilde{y})}$, pour $x, y \in K(\mathcal{L})$ et $\widetilde{x}, \widetilde{y}$ sont des représentants de x et y dans V. Si $E = \operatorname{Im} H$, on a donc $e_{\mathcal{L}^\ell}(x, y) = e^{-2\pi i \ell E(\widetilde{x},\widetilde{y})}$ par le lemme 2.4.2.

D'autre part, on constate immédiatement que le pairing de Weil $e_\ell : X[\ell] \times \widehat{X}[\ell] \to \mu_\ell$ est donné par $e_\ell(x, \mathcal{L}_0) = \chi(\ell x)$ lorsque $\mathcal{L}_0 = L(0, \chi)$ est un fibré de $\mathrm{Pic}_0(X)$ tel que $\mathcal{L}_0^\ell \simeq \mathrm{Id}$ [BL04, Exercice 4.13].

Or on a vu dans la section 2.4 que si $y \in K(\mathcal{L})$, $\phi_{\mathcal{L}}(y) \in \mathrm{Pic}_0(X)$ correspond au fibré $L(0, e^{2\pi i E(y,\cdot)})$, on retrouve $e_\ell(x, \phi_{\mathcal{L}}(y)) = e^{-2\pi i E(\ell x, y)} = e_{\mathcal{L}^\ell}(x, y)$. ♢

5.2.3 *Pairing de Tate*

Le pairing de Tate est différent des pairings présentés directement au sens qu'il est de nature arithmétique plutôt que géométrique et n'est pas le pairing de Cartier associé à une isogénie. On peut trouver la définition originelle du pairing de Tate dans [Lan58]. La forme utilisée en cryptographie est due à LICHTENBAUM dans [Lic69], qui se restreint cependant à des Jacobiennes de courbes. Enfin on peut consulter [Bru09] pour des extensions du pairing de Tate à des isogénies autres que la multiplication par $[\ell]$. Pour la présentation du pairing de Tate, on se restreint un cas très particulier pour la simplicité de l'exposition ; on peut consulter [CFA+06, Chapitre 6] pour le cas général.

On a la suite exacte de Kummer de $G = \mathrm{Gal}(\overline{k}/k)$ modules : $1 \to \mu_\ell \to \overline{k}^* \to \overline{k}^* \to 1$, d'où la suite longue de cohomologie $H^0(G, \mu_\ell) \to k^* \to k^* \to H^1(G, \mu_\ell) \to H^1(G, \overline{k}^*)$.

Or $H^1(G, \overline{k}^*) = 0$ par Hilbert 90 [Ser68, Proposition 2 p. 158], et si on suppose que $\mu_\ell \subset k$ on a $H^0(G, \mu_\ell) = \mu_\ell$ et $H^1(G, \mu_\ell) = \mathrm{Hom}(G, \mu_\ell)$. D'où un isomorphisme canonique $\mathrm{Hom}(G, \mu_\ell) \simeq k^*/k^{*\ell}$, que l'on peut écrire explicitement : si $x \in k^*$, soit $y \in \overline{k}^*$ tel que $x = y^\ell$. Alors on associe à x l'élément $\gamma_x : \sigma \mapsto \sigma y/y$. On a bien $(\sigma y/y)^\ell = \sigma x/x = 1$, donc $\gamma_x \in \mathrm{Hom}(G, \mu_\ell)$.

De même, si on considère la suite exacte :

$$0 \to A_k[\ell](\overline{k}) \to A_k(\overline{k}) \xrightarrow{[\ell]} A_k(\overline{k}) \to 0$$

et qu'on suppose $A_k[\ell](\overline{k}) = A_k[\ell](k)$, on obtient :

$$A_k[\ell](k) \to A_k(k) \xrightarrow{[\ell]} A_k(k) \to H^1(G, A_k[\ell]) = \mathrm{Hom}(G, A_k[\ell]),$$

la dernière égalité venant de l'hypothèse de rationalité des points de ℓ-torsion.

On a donc un morphisme de connexion $\gamma : A_k(k)/\ell A_k(k) \to \mathrm{Hom}(G, A_k[\ell])$ donné explicitement par : si $P \in A_k(k)$ et $P' \in A_k(\overline{k})$ est tel que $P = \ell P'$, alors $\gamma_P : \sigma \mapsto \sigma P' - P'$.

On obtient un pairing en composant avec le pairing de Weil :

$$\begin{array}{rcl} e_T \colon A_k(k)/\ell A_k(k) \times \widehat{A}_k[\ell] & \longrightarrow & \mathrm{Hom}(G, \mu_\ell) \simeq k^*/k^{*\ell} \\ (P, Q) & \longmapsto & \sigma \mapsto e_\ell(\gamma_P(\sigma), Q). \end{array}$$

Il s'agit du pairing de Tate.

Si on le calcule explicitement, soit $Q \in \widehat{A}_k[\ell]$, f_Q la fonction associée au diviseur trivial $\ell.Q$, et g_Q celle associée à $[\ell]^*Q$, on obtient la fonction

$$\sigma \mapsto \frac{g_Q(X + \sigma P' - P')}{g_Q(X)}$$

(où X est un point géométrique quelconque qui rend le membre de droite bien défini). Si on prend $X = P'$, on trouve donc que $e_T(P, Q)$ est la fonction

$$\sigma \mapsto \frac{g_Q(\sigma P')}{g_Q(P')} = \frac{\sigma(g_Q(P'))}{g_Q(P')},$$

et donc correspond via l'isomorphisme $\mathrm{Hom}(G, \mu_\ell) \to k^*/k^{*\ell}$ à la valeur $g_Q(P')^\ell = f_Q([\ell]P') = f_Q(P)$. De plus, on a $f_Q(0) = f_Q([\ell]0) = g_Q(0)^\ell$. Si Q est rationnel, la fonction g_Q l'est, donc $g_Q(0)^\ell \in k^{*\ell}$. Ainsi dans $k^*/k^{*\ell}$, le pairing de Tate est donné par (et c'est cette forme là que l'on utilise dans le cas général, puisqu'il faut évaluer f_Q sur un cycle, voir [Lan58, Section 5]) :

$$e_T(P, Q) = f_Q((P) - (0)).$$

Comme pour le pairing de Weil, en pratique on compose le pairing de Tate avec une polarisation pour avoir un pairing défini sur des points de A_k. Pour les applications cryptographiques du pairing de Tate, on se place en général dans la situation suivante : soit C une courbe hyperelliptique de genre g définie sur un corps fini $\mathbb{F}_q$ telle que si J est sa Jacobienne, alors $\ell \mid \#J(\mathbb{F}_q)$ mais $\ell^2 \nmid \#J(\mathbb{F}_q)$. Soit d l'embedding degree de ℓ sur $\mathbb{F}_q$. Alors en composant avec la polarisation principale canonique sur J, le pairing de Tate est un pairing non dégénéré définit sur [CFA+06, Chapitre 6 et Chapitre 16] :

$$\begin{array}{rcl} e_T \colon J(\mathbb{F}_{q^d})/\ell J(\mathbb{F}_{q^d}) \times J(\mathbb{F}_q)[\ell] & \longrightarrow & \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*\ell} \\ (P, Q) & \longmapsto & f_Q((P) - (0)). \end{array}$$

De plus, avec les hypothèses précédentes, $\ell^2 \nmid \#J(\mathbb{F}_{q^d})$, et donc $J(\mathbb{F}_{q^d})/\ell J(\mathbb{F}_{q^d}) \simeq J(\mathbb{F}_{q^d})[\ell]$ [CFA+06, p. 390].

5.3 FORME DE RIEMANN

Soit X une variété abélienne complexe, de la forme $X = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ avec $\Omega \in \mathfrak{H}_g$. On note aussi Λ_X le réseau $\Omega\mathbb{Z}^g + \mathbb{Z}^g$ associé à X. Soit $\mathcal{L}_0$ le fibré principal canonique de caractéristique 0 associée à X. Si $z \in \mathbb{C}^g$, on note $z = \Omega z_1 + z_2$ sa décomposition induite par l'identification $\mathbb{R}^{2g} \xrightarrow{\sim} \mathbb{C}^g, (z_1, z_2) \mapsto \Omega z_1 + z_2$. La forme symplectique associée à X est alors donnée par $e_\Omega(x, y) = e^{-2\pi i({}^t x_1 y_2 - {}^t y_1 x_2)}$ pour $x, y \in \mathbb{C}^g$ (voir la section 2.5). On l'appelle la forme de Riemann sur X. De plus, si $\mathcal{L} = \mathcal{L}_0^\ell$, pour un $\ell \in \mathbb{N}$, la forme symplectique associée à $\mathcal{L}$ est $e_{\Omega,\ell}(x, y) = e_\Omega(x, y)^\ell$. On a vu dans la section 3.2 que $e_{\Omega,\ell}$ donnait le commutator pairing $e_{\mathcal{L}}$ sur $X[\ell]$.

Le but de cette section est de donner un algorithme pour le calcul du pairing de Weil (associé à la polarisation $\mathcal{L}$) sur $X[\ell]$ lorsque $\ell \in \mathbb{N}$ grâce aux fonctions thêta de niveau n. Soit Θ_n le diviseur thêta de niveau n associé à la fonction $\vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\cdot, \Omega/n)$. Le fibré $\mathcal{L}$ est alors isomorphe à $\mathcal{O}_X(\Theta_n)$. On a vu dans la section 5.2 qu'une définition du pairing de Weil était la suivante : si $P, Q \in X[\ell] \times X[\ell]$, soit $D = t_Q^*\Theta_n - \Theta_n$, comme Q est un point de ℓ-torsion, la classe du diviseur D est dans $\mathrm{Pic}_0(X)[\ell]$. Il existe donc f_Q et g_Q dans $k(X)$ telles que $(f_Q) = \ell.D$ et $(g_Q) = [\ell]^*D$ (où si $f \in K(X)$, (f) représente le diviseur associé à f sur X). On définit de même une fonction f_P qui représente le diviseur $\ell.(t_P^*\Theta_n - \Theta_n)$. Alors le pairing de Weil est donné par

$$e_W(P, Q) = \frac{g_Q(X + P)}{g_Q(X)} = \frac{f_Q((P) - (0))}{f_P((Q) - (0))}$$

(pour la dernière égalité on suppose que le support de f_P est distinct de $(Q) - (0)$, où (Q) représente le cycle associé à Q, et de même pour f_Q).

Soit $\pi : \mathbb{C}^g \to X$ la projection canonique, on note z_P (resp. z_Q) un représentant de P (resp. Q) dans $\mathbb{C}^g$. Le point z_Q se décompose en $z_Q = \Omega z_{Q,1} + z_{Q,2}$, et de même pour le point z_P.

PROPOSITION 5.3.1. *Les fonctions g_Q et f_Q sont données (à une constante près) pour tout $z \in \mathbb{C}^g$ par :*

$$\begin{aligned} g_Q(z) &= \frac{\vartheta\left[\begin{smallmatrix} nz_{Q,1} \\ z_{Q,2}\end{smallmatrix}\right](\ell.z, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](\ell.z, \frac{\Omega}{n})} \\ f_Q(z) &= \frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z + \ell.z_Q, \frac{\Omega}{n})} \cdot \left(\frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z + z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z, \frac{\Omega}{n})}\right)^{\ell}. \end{aligned} \tag{5.3}$$

DÉMONSTRATION : Les fonctions rationnelles f_Q et g_Q de la proposition 5.3.1 sont définies sur $\mathbb{C}^g$, mais on vérifie immédiatement en utilisant l'équation (2.7) qu'elles sont périodiques par rapport au réseau Λ_Ω, et donc sont des fonctions rationnelles sur X.

Comme le diviseur $\pi^*\Theta_n$ sur $\mathbb{C}^g$ est le diviseur associé à la fonction $\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z, \frac{\Omega}{n})$, le diviseur π^*D est associé à la fonction $g'(z) = \frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z+z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z, \frac{\Omega}{n})}$. Ainsi, le diviseur de $g'(\ell z)$ est égal à $\pi^*[\ell]^*D$, tandis que la fonction $g'(z)^\ell$ a pour diviseur π^*D^ℓ. Cependant, la fonction g' n'est pas périodique par rapport à Λ, donc il faut corriger les fonctions précédentes pour obtenir une fonction rationnelle descendant sur X.

La fonction $g(z) = \exp[\pi i^t z_{Q1}\Omega z_{Q1} + 2\pi i^t z_{Q1}(z + z_{Q2})]g'(z)$ a le même diviseur que $g'(z)$, et on vérifie que $g(\ell z)$ est périodique par rapport à Ω, donc descend en la fonction recherchée g_Q sur X. De même, comme $\ell z_Q \in \Lambda$, le terme correctif $\frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z+\ell.z_Q, \frac{\Omega}{n})}$ est égal à l'inverse du facteur d'automorphie (classique) $ac(\ell z_Q, z)$, qui ne s'annule jamais. On vérifie immédiatement que f_Q est périodique, donc descend bien en une fonction rationnelle sur X.■

COROLLAIRE 5.3.2. *Soit $P, Q \in X[\ell]$, et $a, b \in \mathbb{Q}^g$. Alors le pairing de Weil est donné par :*

$$e_W(P,Q) = \frac{\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](\ell.z_P + z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](z_Q, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](\ell.z_P, \frac{\Omega}{n})} \frac{\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](z_P, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](\ell.z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} a \\ b\end{smallmatrix}\right](z_P + \ell.z_Q, \frac{\Omega}{n})} \tag{5.4}$$

Soit K un corps de nombres, A_K une variété abélienne de dimension g définie sur K et $X = A_K \otimes_K \mathbb{C}$. Soit Ω une matrice des périodes pour X, $P \in A(K)/\ell A(K)$, et $Q \in A[\ell](K)$. On suppose que la polarisation principale associée à Ω descend en une polarisation K-rationnelle sur A_K. On se donne des représentants z_P et z_Q dans $\mathbb{C}^g$ de P et $Q \in X$ tels que

$$\left(\frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z_Q, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z_P, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](0, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z_P + z_Q, \frac{\Omega}{n})}\right)^{\ell} \in K^*.$$

Alors un représentant dans $K^*/K^{*\ell}$ du pairing de Tate e_T est donné par :

$$e_T(P,Q) = \frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](z_P, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](\ell.z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](\ell.z_Q + z_P, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0\end{smallmatrix}\right](0, \frac{\Omega}{n})}. \tag{5.5}$$

DÉMONSTRATION : Si $a = b = 0$, la preuve est une conséquence directe de la proposition 5.3.1 et de la formule

$$e_W(P,Q) = \frac{f_Q((P) - (0))}{f_P((Q) - (0))}.$$

Le cas général vient du fait que si $t \in \mathbb{C}^g$, alors pour tout $z \in \mathbb{C}^g$, on a

$$\frac{\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+t, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \frac{\Omega}{n})} = \frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z+t+\frac{\Omega}{n}a+b, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z+\frac{\Omega}{n}a+b, \frac{\Omega}{n})}$$

par l'équation (2.7). Or ici on a par exemple $\ell.z_P \in \Lambda_X$ puisque P est un point de ℓ-torsion, et donc la fonction $\frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z+\ell.z_P+z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z+z_Q, \frac{\Omega}{n})}$ est constante, et ne dépend pas des caractéristiques utilisées.

On applique le même raisonnement pour le pairing de Tate $e_T(P,Q) = f_Q((P)-(0))$. On obtient

$$e_T(P,Q)^{-1} = \frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z_P+\ell.z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\ell.z_Q, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z_P, \frac{\Omega}{n})} \cdot \left(\frac{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z_Q, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z_P, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z_P+z_Q, \frac{\Omega}{n})} \right)^{\ell}. \quad (5.6)$$

Ce qui donne bien le résultat cherché comme $e_T(P,Q) \in K^*/K^{*\ell}$. ∎

Remarque 5.3.3. On peut donner une interprétation du pairing de Tate ainsi : comme les facteurs d'automorphie sont plus simple à manipuler avec les fonctions thêta canoniques, on repasse dans ce cadre pour cette remarque. La fonction thêta canonique de caractéristique 0 est donnée par (voir la discussion précédent la proposition 2.6.1, et [BL04, sec. 3.2]) :

$$\vartheta_c^0(z) = \exp(\frac{\pi}{2}\,{}^t z(\operatorname{Im}\Omega)z)\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \frac{\Omega}{n}).$$

On vérifie facilement que remplacer $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$ par ϑ_c^0 dans l'équation (5.5) ne change pas la valeur du pairing dans $K^*/K^{*\ell}$. On a alors

$$e_T(P,Q) = \frac{a(\ell z_Q, 0)}{a(\ell z_Q, z_P)} = e^{-\pi H(z_P, \ell z_Q)}.$$

On en déduit que

$$e_W(P,Q) = e^{\pi\ell[H(z_P,z_Q)+H(z_Q,z_P)]} = e^{-2\pi i\ell(\operatorname{Im} H)(z_P,z_Q)}$$

et on retrouve bien que le pairing de Weil est associé à la forme de Riemann $E = \operatorname{Im} H$.

Il faut néanmoins faire attention qu'à la différence de l'interprétation du pairing de Weil, l'interprétation du pairing de Tate est basée sur des hypothèses de rationalité. Par exemple, en calculant le pairing de Tate avec la fonction thêta classique $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\cdot, \frac{\Omega}{n})$, on obtient

$$e_T(P,Q) = \frac{ac(\ell z_Q, 0)}{ac(\ell z_Q, z_P)} = e^{-2\pi i\ell\, {}^t z_{Q,1}\cdot z_P}.$$

(On constate que cette formule donne un pairing dégénéré, ce qui est normal car le pairing de Tate sur $\mathbb{C}$ est trivial.) Si $\mathcal{L}$ est une polarisation principale sur X définie sur K, le fibré $\mathcal{L}^n$ est isomorphe (sur $\mathbb{C}$) mais non égal en général au fibré $\mathcal{L}_0^n$, où $\mathcal{L}_0$ est le fibré canonique associée à la matrice de périodes Ω. En particulier, la condition du corollaire 5.3.2 pour le pairing de Tate n'est pas vérifiée en général. On suppose qu'il existe une thêta structure K-rationnelle sur $\mathcal{L}^n$. Soit ϑ' une section sur $\mathbb{C}^g$ du fibré $\mathcal{L}^n$. Comme $\mathcal{L}^n$ et $\mathcal{L}_0^n$ sont isomorphes, il existe une fonction $\gamma \in \Gamma(\mathbb{C}^g, \mathbb{C}^*)$ telle que $\vartheta' = \gamma\vartheta(\cdot, \frac{\Omega}{n})$. Il suffit alors de remplacer $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\cdot, \frac{\Omega}{n})$ par ϑ' dans les équations (5.5) et (5.6). De plus, puisque ϑ' et $\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\cdot, \frac{\Omega}{n})$ satisfont les même formules d'addition, on a par le lemme 4.5.3

$$\frac{\gamma(\ell z_Q + z_P)}{\gamma(\ell z_Q)} = \left(\frac{\gamma(z_Q+z_P)\gamma(0)}{\gamma(z_Q)\gamma(z_P)} \right)^{\ell}.$$

En particulier, l'équation (5.6) reste vraie, et il faut corriger l'équation (5.5) en

$$e_T(P,Q) = \frac{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q, \frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q + z_P, \frac{\Omega}{n})\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0, \frac{\Omega}{n})} \cdot \left(\frac{\gamma(z_Q + z_P)\gamma(0)}{\gamma(z_Q)\gamma(z_P)}\right)^{\ell}. \tag{5.7}$$

On peut également calculer explicitement $e_W(P,Q)$ en utilisant $e_W(P,Q) = g_Q(X+P)/g_Q(X)$. Si on décompose z_Q en $z_Q = \Omega z_{Q,1} + z_{Q,2}$, on calcule alors grâce à l'équation (2.7) :

$$\begin{aligned}\vartheta\left[\begin{smallmatrix}nz_{Q,1}\\z_{Q,2}\end{smallmatrix}\right](z + \ell.z_P, \frac{\Omega}{n}) &= e_{\frac{\Omega}{n}}(\frac{\Omega}{n}.n\ell z_{P,1} + \ell z_{P,2}, \frac{\Omega}{n}.nz_{Q,1} + z_{Q,2})\\ &\exp[(\pi i\ell^2 n^2({}^t z_{P1}.\frac{\Omega}{n}.z_{P1}) - 2\pi i n\ell\, {}^t z_{P1}.z]\vartheta\left[\begin{smallmatrix}nz_{Q1}\\z_{Q2}\end{smallmatrix}\right](z,\Omega)\\ \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z + \ell.z_P, \frac{\Omega}{n}) &= \exp[(\pi i\ell^2 n^2({}^t z_{P1}.\frac{\Omega}{n}.z_{P1}) - 2\pi i n\ell\, {}^t z_{P1}.z]\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega).\end{aligned}$$

En combinant ces deux équations, on retrouve que le pairing de Weil est exactement la forme de Riemann : $e_W(P,Q) = e_{\Omega,\ell}(z_P, z_Q)$. ◇

La base canonique de fonctions thêta de niveau n associées à Ω est donnée par $\vartheta_i = \vartheta\left[\begin{smallmatrix}0\\i/n\end{smallmatrix}\right](\cdot, \Omega/n)$ pour $i \in Z(\overline{n})$. La forme du pairing de Weil donnée dans le corollaire 5.3.2 est intéressante car elle montre comment le calculer grâce aux formules de multiplication :

THÉORÈME 5.3.4. *Soit $\widetilde{0}_X = (\vartheta_i(0)_{i\in Z(\overline{n})}) \in \mathbb{C}^g$ le thêta null point associé à Ω. Soit P et Q des points de la variété abélienne complexe X, tel que P soit un point de ℓ-torsion. Soit $\widetilde{P}$, $\widetilde{Q}$ et $\widetilde{P+Q}$ des relevés affines quelconques à $\mathbb{C}^g$. Il existe $\lambda_x^0, \lambda_x^1 \in \mathbb{C}$ tels que*

$$\begin{aligned}\texttt{chain\_mult}(\ell, \widetilde{P}, \widetilde{0}_X) &= \lambda_x^0 \widetilde{0}_X,\\ \texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}, \widetilde{0}_X) &= \lambda_x^1 \widetilde{Q}.\end{aligned}$$

On pose $\texttt{comm}(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}, \widetilde{0}_X) = \lambda_x^1/\lambda_x^0$.

On a alors, si P et Q sont des points de ℓ-torsion :

$$e_W(P,Q) = \frac{\texttt{comm}(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \widetilde{0}_X)}{\texttt{comm}(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}, \widetilde{0}_X))},$$

Si P est un point de ℓ-torsion et que de plus les relevés $\widetilde{0}_X, \widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$ sont K-rationnels, on a :

$$e_T(P,Q) = \texttt{comm}(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \widetilde{0}_X).$$

DÉMONSTRATION : Supposons que l'on ait choisi $\widetilde{P}$, $\widetilde{Q}$ et $\widetilde{P+Q}$ de telle sorte qu'ils soient l'image des points z_P, z_Q et $z_P + z_Q \in \mathbb{C}^g$ par la base canonique $(\vartheta_i)_{i\in Z(\overline{n})}$. On a vu que la pseudo-addition sur $\widetilde{X}$ venait de l'addition sur $\mathbb{C}^g$ (voir la section 4.3), donc

$$\begin{aligned}\texttt{chain\_mult}(\ell, \widetilde{P}, \widetilde{0}_X) &= (\vartheta_i(\ell z_P))_{i\in Z(\overline{\ell n})},\\ \texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}, \widetilde{0}_X) &= (\vartheta_i(\ell z_P + z_Q))_{i\in Z(\overline{\ell n})}.\end{aligned}$$

Les formules pour e_W et e_T découlent alors immédiatement du corollaire 5.3.2.

Dans le cas général, on vérifie grâce au lemme 4.5.3 que si on change $\widetilde{P}$, $\widetilde{Q}$, $\widetilde{P+Q}$ et $\widetilde{0}_X$ par des facteurs projectifs α, β, γ et $\delta \in \mathbb{C}^*$ respectivement, on a par récurrence

$$\texttt{comm}(\alpha\widetilde{P}, \beta\widetilde{Q}, \gamma\widetilde{P+Q}, \delta\widetilde{0}_X) = \frac{\gamma^\ell\delta^\ell}{\alpha^\ell\beta^\ell}\texttt{comm}(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}). \tag{5.8}$$

Ainsi $e_W(P,Q)$ est inchangé, de même pour la classe de $e_T(P,Q)$ dans $K^*/K^{*\,\ell}$ (si $\alpha,\beta,\gamma,\delta \in K^*$), et les formules du théorème 5.3.4 restent valables dans le cas général.

Pour le cas du pairing de Tate, il faut faire attention à prendre des relevés z_P et z_Q de telle sorte que $\vartheta_i(X) \in K$ pour $i \in Z(\overline{n})$ et $X = z_P, z_Q, z_{P+Q}$. Ce n'est pas toujours possible si on prend pour ϑ_i les fonctions thêta classiques, mais par la remarque 5.3.3, le théorème 5.3.4 reste vrai si on prend pour fonctions thêta la base canonique associé à un thêta null point K-rationnel de niveau n de X. D'ailleurs en reprenant les notations de cette remarque, si on note X^{an} le point analytique $\vartheta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](X,\frac{\Omega}{n})_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$, on a $z_P^{\mathrm{an}} = \gamma(z_P)\widetilde{P}$, $z_Q^{\mathrm{an}} = \gamma(z_Q)\widetilde{Q}$, $(z_P+z_Q)^{\mathrm{an}} = \gamma(z_P+z_Q)\widetilde{P+Q}$ et $0_X^{\mathrm{an}} = \gamma(0_X)\widetilde{0}_X$. Les équations (5.7) et (5.8) nous donnent alors

$$\begin{aligned} e_T(P,Q) &= \mathtt{comm}(z_Q^{\mathrm{an}}, z_P^{\mathrm{an}}, (z_P+z_Q)^{\mathrm{an}}, 0_X^{\mathrm{an}}).\left(\frac{\gamma(z_Q+z_P)\gamma(0)}{\gamma(z_Q)\gamma(z_P)}\right)^{\ell} \\ &= \mathtt{comm}(\gamma(z_Q)\widetilde{Q}, \gamma(z_P)\widetilde{P}, \gamma(z_P+z_Q)\widetilde{P+Q}, \gamma(0_X)\widetilde{0}_X).\left(\frac{\gamma(z_Q+z_P)\gamma(0)}{\gamma(z_Q)\gamma(z_P)}\right)^{\ell} \\ &= \mathtt{comm}(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \widetilde{0}_X). \end{aligned}$$

Autrement dit, pour calculer le pairing de Tate, il suffit d'utiliser les formules d'addition sur des relevés affines de $0_X, P, Q, P+Q$ définis sur K. ■

Remarque 5.3.5. On peut également calculer le pairing de Tate et de Weil avec les coordonnées thêta en utilisant la stratégie de Miller décrite dans la section 1.3.3. En reprenant les notations de cette section, la fonction f_m de diviseur $mQ-(mQ)-(m-1)0_X$ est donnée par (il suffit de reprendre la même preuve que la proposition 5.3.1) :

$$f_m = \frac{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+m.z_Q,\frac{\Omega}{n})}\cdot\left(\frac{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+z_Q,\frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\frac{\Omega}{n})}\right)^m.$$

On en déduit en particulier que la fonction f_{m_1Q,m_2Q} de diviseur $(m_1Q)+(m_2Q)-((m_1+m_2)Q)-0_X$ est donnée par

$$f_{m_1Q,m_2Q} = \frac{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+m_1Q,\frac{\Omega}{n})\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+m_2Q,\frac{\Omega}{n})}{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+(m_1+m_2)Q,\frac{\Omega}{n})\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\frac{\Omega}{n})}.$$

Si $n \geqslant 4$, on peut calculer cette fonction explicitement en utilisant des additions « normales », en faisant attention de l'évaluer ensuite sur le cycle $(P)-(0_X)$ plutôt que directement en P car avec cette méthode, la fonction f_ℓ ainsi construite n'est pas normalisée. En pratique, pour les fonctions thêta, cette méthode est moins efficace que la méthode du théorème 5.3.4. ✧

5.4 CALCUL DU COMMUTATOR PAIRING ÉTENDU

Soit $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété abélienne marquée de niveau δ. Si ℓ est un entier, l'objectif de cette section est de donner un algorithme pour calculer le pairing $e_{\mathcal{L}^\ell}$ en utilisant uniquement les formules d'addition de la section 4.3.

Soit $x, y \in K(\mathcal{L}^\ell) = [\ell]^{-1}(K(\mathcal{L}))$. Comme $\mathcal{L}$ est totalement symétrique, on a $[\ell]^*\mathcal{L} \simeq \mathcal{L}^{\ell^2}$, et on a vu dans la section 5.2.1 que

$$e_{\mathcal{L}^\ell}(x,y) = e_{\mathcal{L}^{\ell^2}}(x',y')^\ell$$

où x' et y' sont des points géométriques de X tels que $x = \ell x'$ et $y = \ell y'$.

Pour calculer $e_{\mathcal{L}^\ell}(x,y)$ on adopte une stratégie similaire à la section 4.5 : on prend une thêta structure $\Theta_{\mathcal{L}^{\ell^2}}$ sur $(A_k, [\ell]^*\mathcal{L})$ compatible avec la thêta structure $\Theta_{\mathcal{L}}$ sur $(A_k,\mathcal{L})$, on choisit un système de coordonnées affines sur $(A_k,\mathcal{L}^{\ell^2})$, et si $\widetilde{[\ell]}$ représente l'extension canonique de $[\ell]$ par rapport à ce système de coordonnées, on prend un relevé affine $\widetilde{0}_{A_k,\ell}$ $\widetilde{[\ell]}$-compatible avec $\widetilde{0}_{A_k}$. On va user de l'action de $G(\mathcal{L}^{\ell^2})$ pour calculer $e_{\mathcal{L}^{\ell^2}}(x',y')^\ell$, et on montrera ensuite comment la formule qu'on obtient peut s'obtenir à l'aide des formules d'addition.

Déjà, on a la méthode suivante de calcul de $e_{\mathcal{L}}(x,y)$ où $x,y \in K(\mathcal{L})$: si $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x+y}$ sont des relevés affines de x, y et $x+y$ respectivement, on peut écrire $\widetilde{x} = (\alpha, i_1, j_1).\widetilde{0}_X$ où $(\alpha, i_1, j_1) \in \mathcal{H}(\delta)$, et de même $\widetilde{y} = (\beta, i_2, j_2).\widetilde{0}_X$. On écrit alors $\widetilde{x+y}$ de deux manières différentes : $\widetilde{x+y} = (\gamma_1, i_1, j_1).\widetilde{y}$ et $\widetilde{x+y} = (\gamma_2, i_2, j_2).\widetilde{x}$. Un calcul immédiat montre qu'on a $\widetilde{x+y} = (\gamma_1\beta\langle i_1, j_2\rangle, i_1+i_2, j_1+j_2).\widetilde{0}_{A_k} = (\gamma_2\alpha\langle i_2, j_1\rangle, i_1+i_2, j_1+j_2).\widetilde{0}_{A_k})$. On trouve alors $e_{\mathcal{L}}(x,y) = \frac{\langle i_1,j_2\rangle}{\langle i_2,j_1\rangle}\frac{\gamma_2\alpha}{\gamma_1\beta}$.

On va combiner cette idée et la méthode de la section 5.3 :

THÉORÈME 5.4.1. *Soit $\widetilde{x},\widetilde{y}$ et $\widetilde{x+y} \in \widetilde{A}_k$ des relevés affines de $x, y, x+y \in K(\mathcal{L}^\ell)$. Comme $\ell x \in K(\mathcal{L})$ (et de même pour $\widetilde{y}$ et $\widetilde{x+y}$) on peut écrire :*

$$\begin{aligned}
\texttt{chain_mult}(\ell,\widetilde{x}) &= (\lambda_x^0, i_1, i_2)\widetilde{0}_{A_k,\ell}\\
\texttt{chain_mult}(\ell,\widetilde{y}) &= (\lambda_y^0, j_1, j_2)\widetilde{0}_{A_k,\ell}\\
\texttt{chain_multadd}(\ell,\widetilde{x+y},\widetilde{x},\widetilde{y}) &= (\lambda_x^1, i_1, j_1)\widetilde{y}\\
\texttt{chain_multadd}(\ell,\widetilde{x+y},\widetilde{y},\widetilde{x}) &= (\lambda_y^1, i_2, j_2)\widetilde{x}
\end{aligned}$$

avec $\lambda_x^0,\lambda_y^0,\lambda_x^1,\lambda_y^1 \in \overline{k}^*$ et $(i_1,i_2),(j_1,j_2) \in K(\delta)$. Alors

$$e_{\mathcal{L}^\ell}(x,y) = \frac{\lambda_y^1\lambda_x^0}{\lambda_x^1\lambda_y^0}.$$

DÉMONSTRATION : Par le même raisonnement que dans la preuve du théorème 5.3.4, on peut supposer qu'on a choisi $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x+y}$ de telle sorte qu'ils soient de la forme :

$$\widetilde{x} = \widetilde{[\ell]}(1,\alpha_1,\beta_1)\widetilde{0}_{A_k,\ell},\ \widetilde{y} = \widetilde{[\ell]}(1,\alpha_2,\beta_2)\widetilde{0}_{A_k,\ell},\ \widetilde{x+y} = \widetilde{[\ell]}(1,\alpha_1+\alpha_2,\beta_1+\beta_2)\widetilde{0}_{A_k,\ell}.$$

Soit $\alpha_{[\ell]} : \mathcal{Z}(K(\mathcal{L}^\ell)) \to G(\mathcal{L})$ l'isomorphisme canonique associé à l'isogénie $[\ell]$, et $(1,i_1',i_2') \in G(\mathcal{L}^{\ell^2})$ un antécédent de $(1,i_1,i_2) \in G(\mathcal{L})$ par $\alpha_{[\ell]}$. Par les propositions 4.5.4 et 4.5.5, on calcule $\ell.\widetilde{x} = \widetilde{[\ell]}(1,\ell\alpha_1,\ell,\beta_1).\widetilde{0}_{A_k,\ell}$. Comme $\ell.\widetilde{x} = \widetilde{[\ell]}(\lambda_x^0,i_1',i_2').\widetilde{0}_{A_k,\ell}$ par définition, on a $(\ell\alpha_1 - i_1', \ell\alpha_2 - i_2') \in K(\ell^2\delta)[\ell]$ et donc $(1,\ell\alpha_1-i_1',\ell\alpha_2-i_2') \in \mathrm{Ker}(\alpha_{[\ell]})$.

On calcule alors :

$$\ell.\widetilde{x} = \langle \ell\alpha_1 - i_1', -i_2'\rangle\widetilde{[\ell]}(1,\ell\alpha_1-i_1',\ell\alpha_2-i_2')(1,i_1',i_2').\widetilde{0}_{A_k,\ell} = (\langle\ell\alpha_1-i_1',-i_2'\rangle,i_1,i_2).\widetilde{0}_{A_k}.$$

Donc $\lambda_x^0 = \langle\ell\alpha_1 - i_1', -i_2'\rangle$. De même, on calcule :

$$\begin{aligned}
\texttt{chain_multadd}(\ell,\widetilde{x+y},\widetilde{x},\widetilde{y}) &= \widetilde{[\ell]}(1,\ell\alpha_1+\beta_1,\ell\alpha_2+\beta_2).\widetilde{0}_{A_k,\ell}\\
&= \langle\ell\alpha_1-i_1',-i_2'-\beta_2\rangle\langle i_1',-\beta_2\rangle\\
&\qquad \widetilde{[\ell]}(1,\ell\alpha_1-i_1',\ell\alpha_2-i_2').(1,i_1',i_2').(1,\beta_1,\beta_2).\widetilde{0}_{A_k,\ell}\\
&= (\langle\ell\alpha_1-i_1',-i_2'-\beta_2\rangle\langle i_1',-\beta_2\rangle,i_1,i_2).\widetilde{y},
\end{aligned}$$

pour trouver $\lambda_x^1 = \langle \ell\alpha_1 - i_1', -i_2' - \beta_2\rangle\langle i_1', -\beta_2\rangle$. Et donc $\lambda_x^1/\lambda_x^0 = \langle \ell\alpha_1, -\beta_2\rangle$.

Au final, on trouve bien :

$$\frac{\lambda_y^1\lambda_x^0}{\lambda_x^1\lambda_y^0} = \frac{\langle \ell\alpha_1, \beta_2\rangle}{\langle \ell\beta_1, \alpha_2\rangle} = e_{\mathcal{L}^\ell}(x, y).$$

■

Bien sûr, le théorème 5.4.1 nous intéresse en pratique lorsque x et y sont des points de ℓ-torsion. Soit $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{x+y}$ des relevés affines quelconques de x, y et $x+y$. On peut calculer les points suivants grâce à des pseudo-additions :

$$\begin{array}{llll}
\widetilde{0}_{A_k} & \widetilde{x} & 2\widetilde{x} & \ldots \quad \ell\widetilde{x} = \lambda_x^0\widetilde{0}_{A_k} \\
\widetilde{y} & \widetilde{x+y} & 2\widetilde{x}+\widetilde{y} & \ldots \quad \ell\widetilde{x}+\widetilde{y} = \lambda_x^1\widetilde{y} \\
2\widetilde{y} & \widetilde{x}+2\widetilde{y} & & \\
\ldots & \ldots & & \\
\ell\widetilde{y} = \lambda_y^0\widetilde{0}_{A_k} & \widetilde{x}+\ell\widetilde{y} = \lambda_y^1\widetilde{x} & &
\end{array}$$

Et on a alors $e_{\mathcal{L}^\ell}(x, y) = \frac{\lambda_y^1\lambda_x^0}{\lambda_x^1\lambda_y^0}$.

On a donc l'algorithme suivant pour calculer $e_{\mathcal{L}^\ell}(x, y)$:

ALGORITHME 5.4.2 (COMMUTATOR PAIRING ÉTENDU) :
Entrées $x, y \in A_k[\ell]$
Sortie $e_{\mathcal{L}^\ell}(x, y)$

➔ Calculer $\lambda_x^0, \lambda_x^1, \lambda_y^0, \lambda_y^1 \in k^*$ tels que :

$$\lambda_x^0\widetilde{0}_{A_k} = \texttt{chain\_mult}(\ell, \widetilde{x}) \quad \lambda_y^0\widetilde{0}_{A_k} = \texttt{chain\_mult}(\ell, \widetilde{y})$$
$$\lambda_x^1\widetilde{y} = \texttt{chain\_multadd}(\ell, \widetilde{x+y}, \widetilde{x}, \widetilde{y}) \quad \lambda_y^1\widetilde{x} = \texttt{chain\_multadd}(\ell, \widetilde{x+y}, \widetilde{y}, \widetilde{x}).$$

➔ Retourner

$$e_{\mathcal{L}^\ell}(x, y) = \frac{\lambda_y^1\lambda_x^0}{\lambda_y^0\lambda_x^1}.$$

De plus, le pairing de Tate est donné par

$$e_T(x, y) = \frac{\lambda_y^1}{\lambda_y^0},$$

par le théorème 5.3.4. ◊

ANALYSE DE COMPLEXITÉ 5.4.3. On peut calculer le pairing $e_{\mathcal{L}^\ell}$ à l'aide de 4 multiplications rapides : l'algorithme coûte donc $O(\log(\ell))$ pseudo-additions, et une addition normale pour calculer $x+y$. Il faut noter que l'on peut réutiliser beaucoup de calculs intermédiaires, lorsqu'on fait les pseudo-additions pour calculer $\texttt{chain\_mult}(\ell, \widetilde{x})$ et $\texttt{chain\_multadd}(\ell, \widetilde{x+y}, \widetilde{x}, \widetilde{y})$. Enfin, comme on a juste besoin de récupérer les coefficients projectifs, une fois qu'on a fait le calcul de $x+y$, on peut très bien projeter les points en niveau 2 et faire le calcul des pseudo-additions en niveau 2. (D'ailleurs, on peut aussi projeter x et y en niveau 4 pour calculer $x+y$.) ◊

EXEMPLE 5.4.4 (PAIRING DE TATE). On donne des formules explicites pour le calcul du pairing de Tate avec $g = 1$ et $g = 2$. On suppose que l'on a calculé P, Q et $P+Q$ en niveau 2 (par exemple en calculant $P + Q$ en niveau 4 puis en prenant les coordonnées de niveau 2. (On obtient bien le même résultat par le point 1 de la section 5.2.1, page 113.) On calcule les multiplications par une chaîne de Montgomery : à partir de $nQ, (n+1)Q, (n+1)Q + P$ on calcule soit $(2n)Q, (2n+1)Q, (2n+1)Q + P$, soit $(2n+1)Q, (2n+2)Q, (2n+2)Q + P$, donc à chaque étape on a un doublement, et deux additions différentielles, de différences P et Q ou P et $P+Q$.

Si $X = \mathbb{C}/(\Omega\mathbb{Z} + \mathbb{Z})$ est une variété abélienne complexe de dimension 1, les fonctions thêta de niveau 2 sont données par $\vartheta\left[\begin{smallmatrix}0\\ i/2\end{smallmatrix}\right](\cdot, \Omega/2)$ et les formules de duplication du théorème 4.4.6 s'écrivent

$$\begin{cases} a\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega/2) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](2z,\Omega)^2 + \vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](2z,\Omega)^2, \\ b\vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](z,\Omega/2) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](2z,\Omega)^2 - \vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](2z,\Omega)^2. \end{cases}$$

$$\begin{cases} 2A\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](2z,\Omega) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega/2)^2 + \vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](z,\Omega/2)^2, \\ 2B\vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](2z,\Omega) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega/2)^2 - \vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](z,\Omega/2)^2. \end{cases}$$

(On interprète les $\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](2z,\Omega)$ comme des fonctions thêta de niveau 2 sur la variété abélienne 2-isogène $X' = \mathbb{C}^g/(\frac{\Omega}{2}\mathbb{Z}^g + \mathbb{Z}^g)$ plutôt que comme des fonctions thêta de niveau 4 sur X.) On a posé

$$a = \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega/2), \quad b = \vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0,\Omega/2), \quad A = \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega), \quad B = \vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0,\Omega)$$

et donc $2A^2 = a^2 + b^2$ et $2B^2 = a^2 - b^2$.

De plus, on peut changer les points le thêta null point (a, b) par un facteur projectif, de même pour les points P, Q et $P + Q$ (voir la preuve du théorème 5.3.4), donc on peut supposer que $P = (x_P, 1)$, $Q = (x_Q, 1)$ et $P + Q = (x_{P+Q}, 1)$. Une autre amélioration est la suivante : on peut remplacer (A, B) par $(1, B/A)$ (si $A \neq 0$). Ceci modifie chaque addition différentielle par le facteur A^2. Cependant, comme on utilise la même séquence de Lucas pour calculer ℓQ et $\ell Q + P$, ces facteurs se compensent.

On en déduit qu'une étape du pairing de Tate est de la forme :

ALGORITHME 5.4.5 (PAIRING DE TATE) :
Calcul d'une étape intermédiaire du pairing de Tate en genre 1, niveau 2.

Entrées $nQ = (x_n, z_n)$; $(n+1)Q = (x_{n+1}, z_{n+1})$, $(n+1)Q + P = (x'_{n+1}, z'_{n+1})$.
Sortie $2nQ = (x_{2n}, z_{2n})$; $(2n+1)Q = (x_{2n+1}, z_{2n+1})$; $(2n+1)Q + P = (x'_{2n+1}, z'_{2n+1})$.

- ➔ $\alpha = (x_n^2 + z_n^2)$; $\beta = \frac{A^2}{B^2}(x_n^2 - z_n^2)$.
- ➔ $X_n = \alpha^2$; $X_{n+1} = \alpha(x_{n+1}^2 + z_{n+1}^2)$; $X'_{n+1} = \alpha(x'^2_{n+1} + z'^2_{n+1})$;
- ➔ $Z_n = \beta(x_n^2 - z_n^2)$; $Z_{n+1} = \beta(x_{n+1}^2 - z_{n+1}^2)$; $Z'_{n+1} = \beta(x'^2_{n+1} + z'^2_{n+1})$;
- ➔ $x_{2n} = X_n + Z_n$; $x_{2n+1} = (X_{n+1} + Z_{n+1})/x_P$; $x'_{2n+1} = (X'_{n+1} + Z'_{n+1})/x_Q$;
- ➔ $z_{2n} = \frac{a}{b}(X_n - Z_n)$; $z_{2n+1} = X_{n+1} - Z_{n+1}$; $z'_{2n+1} = X'_{n+1} - Z'_{n+1}$;
- ➔ Retourner (x_{2n}, z_{2n}) ; (x_{2n+1}, z_{2n+1}) ; (x'_{2n+1}, z'_{2n+1}).

(Le passage à $(2n+1)Q, (2n+2)Q, (2n+2)Q + P$ est similaire). ◇

Si l'on travaille avec les carrés des coordonnées (sauf à la dernière étape), on voit qu'une étape intermédiaire coûte 8 carrés, 4 multiplications par une constante, et 4 multiplications. Bien sûr, si on veut calculer plusieurs pairings $e_T(P_i, Q)$ avec le même Q et des P_i qui changent, on peut garder les résultats intermédiaires du calcul des multiples de Q.

On a vu que l'on pouvait supposer que $A = 1$, ce qui nous permet d'utiliser les formules du tableau 4.2. Dans le cadre des pairings, le choix des variétés abéliennes utilisées est très limité,

	Pairing initial $e(P,Q)$	Pairings suivants $e(P',Q)$
Dimension 1	$5\mathbf{M}+7\mathbf{S}+2\mathbf{m}+2\mathscr{M}_0$	$2\mathbf{M}+2\mathbf{S}+1\mathbf{m}$
Dimension 2	$11\mathbf{M}+13\mathbf{S}+6\mathbf{m}+6\mathscr{M}_0$	$4\mathbf{M}+4\mathbf{S}+3\mathbf{m}$
Dimension g	$(3.2^g-1)\mathbf{M}+(3.2^g+1)\mathbf{S}+$ $2(2^g-1)\mathbf{m}+2(2^g-1)\mathscr{M}_0$	$2^g\,\mathbf{M}+2^g\mathbf{S}+(2^g-1)\mathbf{m}$

TABLE 5.1 – Coût d'une étape du calcul du pairing de Tate, $P, Q \in A_{\mathbb{F}_q}(\mathbb{F}_{q^d})$

	Pairing initial $e(P,Q)$	Pairings suivants $e(P',Q)$
Dimension 1	$2\mathbf{S}+1\mathbf{m}+2\mathscr{M}+3M+5S+3m$	$2\mathbf{S}+1\mathbf{m}+2\mathscr{M}$
Dimension 2	$4\mathbf{S}+3\mathbf{m}+4\mathscr{M}+7M+9S+9m$	$4\mathbf{S}+3\mathbf{m}+4\mathscr{M}$
Dimension g	$2^g\mathbf{S}+(2^g-1)\mathbf{m}+2^g\mathscr{M}+$ $(2.2^g-1)M+(2.2^g+1)S+3(2^g-1)m$	$2^g\mathbf{S}+(2^g-1)\mathbf{m}+2^g\mathscr{M}$

TABLE 5.2 – Coût d'une étape du calcul du pairing de Tate, $P \in A_{\mathbb{F}_q}(\mathbb{F}_q)$, $Q \in A_{\mathbb{F}_q}(\mathbb{F}_{q^d})$

ce qui fait que l'on ne peut pas les choisir pour que les thêta null points associés soient petits. Ceci explique que l'on n'utilise pas la version du tableau 4.1. Pour le calcul du pairing, P et Q seront dans une extension k_2 du corps de définition k_1 de la variété abélienne. Le tableau 5.1 donne le coût d'une étape du calcul du pairing de Tate en genre 1 et 2, où **M** représente une multiplication dans k_2, **S** un carré dans k_2, **m** une multiplication par une constante dans k_2 et $\mathscr{M}_0$ une multiplication d'un élément de k_2 par une coordonnée du thêta null point (qui vit dans k_1).

Cependant, pour aller plus vite, lorsqu'on calcule le pairing de Tate, on choisit Q dans le corps k_1 et P dans l'extension k_2 de k_1. (Voir la discussion à la fin de la section 5.2.3.) Lors du calcul d'une étape du pairing de Tate, les opérations qui font intervenir des coefficients dans k_2 sont le calcul de $nQ+P$: à chaque étape on a deux carrés dans k_2, une multiplication par deux éléments dans k_2, et deux multiplications entre un élément de k_2 et un élément de k_1. Le tableau 5.2 résume le coût s d'une étape du calcul du pairing de Tate sous cette hypothèse, ici M représente une multiplication dans k_1, S un carré dans k_1 et m une multiplication par une constante dans k_1 (c'est-à-dire une coordonnée du thêta null point, de P, de Q ou de $P+Q$, nous n'avons pas distingué m de m_0 ici car on a vu que les coordonnées du thêta null point ne peuvent être choisies petites). Par soucis de lisibilité, nous avons supposé que $k_1 = k_2$ lorsque $g = 1$ et $g = 2$.

EXEMPLE 5.4.6 (CALCUL EXPLICITE DU PAIRING DE WEIL). Soit E la courbe elliptique définie sur $\mathbb{F}_{59}$ par :

$$y^2 = x^3 + 12x + 43.$$

Un point modulaire de niveau 4 associé à E est donné par $(51:1:21:1)$ (on peut le calculer en utilisant les formules de Thomae de l'algorithme 4.7.5). L'équation de E dans la base donnée par les fonctions thêta de niveau 4 associées à ce point modulaire est donnée comme intersection de quadriques (voir le théorème 4.7.1) :

$$0 = \vartheta_0\vartheta_2 + 25\vartheta_1^2 + 25\vartheta_3$$
$$0 = \vartheta_0^2 + 26\vartheta_1\vartheta_3 + \vartheta_2^2.$$

L'embedding degree est $d = 6$. Soit P et Q les points de 7-torsion donnés par

$$P = (42 : 3 : 39 : 1)$$
$$Q = (31t^5 + 20t^4 + 20t^3 + 52t^2 + 15t + 32 : 42t^5 + 51t^4 + 50t^3 + 4t^2 + 31t + 20 : 45t^5 + 2t^4 + 54t^3 + 36t^2 + 40t + 22 : 1)$$

où t est une racine du polynôme primitif $X^6 + 5X^5 + 28X^4 + 32X^3 + 41X^2 + 4X + 22$. Le point P correspond au point $(54, 34)$ sur E (dans les coordonnées (x, y) de Weierstrass), tandis que le point Q correspond au point $(10t^5 + 3t^4 + 21t^3 + 2t^2 + 4t + 9, 31t^5 + 5t^4 + 24t^3 + 12t^2 + 55t + 24 : 1)$.

On calcule

$$P + Q = (50t^5 + 50t^4 + 43t^3 + 17t^2 + 21t + 47 : 20t^5 + 24t^4 + 15t^3 + 50t^2 + 12t + 17 : 26t^5 + 3t^4 + 50t^3 + 37t^2 + 25t + 3 : 1)$$

ce qui nous permet de déterminer :

$$\ell\widetilde{P} = 27\widetilde{0_E},$$
$$\ell\widetilde{Q} = (57t^5 + 46t^3 + 5t^2 + 31t + 21)\widetilde{0_E},$$
$$\texttt{chain\_multadd}(7, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}) = (36t^5 + 58t^4 + 38t^3 + 29t^2 + 7t + 18)\widetilde{Q}$$
$$\texttt{chain\_multadd}(7, \widetilde{P+Q}, \widetilde{Q}, \widetilde{P}) = (41t^5 + 31t^4 + 51t^3 + 42t^2 + 21t + 53)\widetilde{P}$$

D'où l'on en tire $e_7(P, Q) = 32t^5 + 30t^4 + 2t^3 + 15t^2 + 26t + 4$. (On vérifie que l'on a bien $e_7(P, Q)^7 = 1$.) ◇

5.4.1 *Comparaison avec l'algorithme de Miller*

On peut se demander si l'algorithme 5.4.2 est plus efficace que l'algorithme 1.3.2. Cependant, il faut faire attention au fait que l'algorithme de Miller a été extrêmement amélioré ces dernières années par rapport à ce qui est décrit dans l'algorithme 1.3.2. Par exemple, pour le cas des pairings sur une courbe elliptique $E_{\mathbb{F}_q}$, si d est l'embedding degree, on va calculer des pairings de Tate de la forme $e_T(P, Q)$, où $Q \in E_{\mathbb{F}_q}(\mathbb{F}_q)$ et $P \in E_{\mathbb{F}_q}(\mathbb{F}_{q^d})$. On a déjà vu dans la section 1.3.3 des méthodes pour éviter une division si d est pair. De plus, on peut réduire la longueur de la boucle de Miller en remplaçant le pairing de Tate par le pairing Eta [BGÓS07] (sur des variétés abéliennes supersingulières), ou le pairing de Ate optimal [HSV06 ; Ver10 ; Hes08, pour les courbes elliptiques ; et GHO+07, pour les courbes hyperelliptiques].

L'idée du pairing de Ate est la suivante : on considère des sous-groupes de la ℓ-torsion G_1 et G_2 où G_1 est l'espace propre du Frobenius associé à 1 et G_2 l'espace propre associé à q. Si $P \in G_2$, alors $\mathrm{Fr}(P) = [q]P$, et on peut s'en servir pour accélérer le pairing. Il serait intéressant d'utiliser cette méthode pour accélérer également l'algorithme 5.4.2.

Dans la suite, on compare uniquement une étape de la boucle de Miller par rapport à une étape de l'algorithme 5.4.2. Dans [FGJ09], les auteurs donnent des formules efficaces en genre 2 sur des coordonnées de Mumford projectives qui permettent de retrouver la fonction de Miller

$$\frac{y - l(x)}{(x - x_1)(x - x_2)}$$

sans surcoût (où l est un polynôme unitaire de degré 3). Le coût est le suivant : une addition mixte (un des deux points a une coordonnée égale à 1) coûte $36M + 5S$ et un doublement $38M + 6S$ (où les multiplications et les carrés se font sur $\mathbb{F}_p$). Enfin dans leur exemple, $d = 2$, une

	Miller		Theta coordinates
	Doubling	Addition	One step
d even	$1\mathbf{M} + 1\mathbf{S} + 1\mathbf{m}$	$1\mathbf{M} + 1\mathbf{m}$	$1\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$
d odd	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}$	$2\mathbf{M} + 1\mathbf{m}$	

TABLE 5.3 – Comparaison avec l'évaluation dans l'algorithme de Miller en genre 1

multiplication dans $\mathbb{F}_{p^2}$ nécessite 3 multiplications dans $\mathbb{F}_p$ grâce à l'algorithme de Karatsuba, et une multiplication entre un élément de $\mathbb{F}_p$ et un élément de $\mathbb{F}_{p^2}$ nécessite 2 multiplications dans $\mathbb{F}_p$. Pour évaluer la fonction de Miller sur le point P (qui vit dans $J_{\mathbb{F}_p}(\mathbb{F}_{p^2})$) ils ont besoin de $6M$ si $P = [x - x_2, y_2]$ représente un diviseur dégénéré avec $x_2 \in \mathbb{F}_p$ (car on peut appliquer la technique d'élimination des diviseurs dans ce cas), et $51M + 3S$ sinon.

Si l'on compare avec le tableau 5.2, comme on a ici $\mathbf{m} = 2m$, $\mathbf{S} = 2S + 1M$ et $\mathscr{M} = 2M$, on a (avec $m = M$) un coût par étape de $33M + 17S$. L'algorithme 5.4.2 est donc bien plus rapide dans ce cas.

En genre 1, dans [CSB04] les auteurs utilisent des formules d'addition sur les coordonnées Jacobiennes (voir l'exemple 4.8.9) qui encapsulent la pente de la ligne donnant la fonction de Miller. Le coût d'une addition mixte est de $11M + 3S$, et le doublement de $8M + 6S$. Enfin, l'évaluation de la fonction de Miller nécessite $2M$, et pour mettre à jour la valeur actuelle de l'évaluation du diviseur construit, il faut $1S + 1M$ pour un doublement et $1M$ pour une addition (on suppose ici que tous les points sont dans le même corps de base). On voit donc que là encore, l'algorithme 5.4.2 serait compétitif si on pouvait réduire le nombre d'étapes comme pour le pairing Eta (même si actuellement on dispose de formules un peu meilleures avec les coordonnées Jacobiennes étendues ou en travaillant sur les courbes d'Edwards [ALNR09]).

La comparaison précédente n'est pas très réaliste : en effet, en genre 1 on prend en général un embedding degree d relativement grand, ce qui fait que les opérations dans le corps $\mathbb{F}_{q^d}$ sont plus coûteuses. Pour l'algorithme de Miller, les seules opérations dans l'extension de corps $\mathbb{F}_{q^d}$ résultent de l'évaluation de la fonction de Miller en le point P, et pour l'algorithme 5.4.2 lors du calcul de $mQ + P$. On pourra trouver dans les tableaux 5.3 et 5.4 une comparaison entre l'algorithme de Miller et l'algorithme 5.4.2 où l'on compte uniquement les opérations faisant intervenir le grand corps (on pourra se reporter au tableau 5.2 pour les notations).

Le tableau 5.3 correspond au cas du genre 1, il y a alors deux situations, soit d est pair et on peut appliquer les techniques d'élimination du dénominateur dans Miller, soit d est impair et dans ce cas il faut calculer le numérateur et le dénominateur séparément. Dans le tableau 5.4, qui correspond au genre 2, on peut encore appliquer l'élimination du dénominateur lorsque $d = 2$, ce qui impose de supposer que Q soit un diviseur dégénéré. Par rapport au cas général, il y a le cas intermédiaire Q dégénéré mais pas d'élimination des dénominateurs, que nous n'avons pas considéré ici (la seule différence par rapport au cas général étant le nombre de multiplications $\mathbf{m}$, en effet lorsque Q n'est pas dégénéré, évaluer la fonction de Miller en Q demande un calcul coûteux de résultant.

On voit que même dans le cas favorable à Miller, l'algorithme 5.4.2 reste compétitif en fonction de la proportion de bits égaux à 1 dans le développement binaire de ℓ (en effet, pour chaque tel bit, l'algorithme de Miller doit effectuer une addition en plus du doublement, alors que l'algorithme 5.4.2 effectue un doublement et deux additions dans tous les cas).

	Miller		Theta coordinates
	Doubling	Addition	One step
Q degenerate + denominator elimination	1**M** + 1**S** + 3**m**	1**M** + 3**m**	3**M** + 4**S** + 4**m**
General case	2**M** + 2**S** + 18**m**	2**M** + 18**m**	

TABLE 5.4 – Comparaison avec l'évaluation dans l'algorithme de Miller en genre 2

5.5 LE PAIRING SYMÉTRIQUE SUR LES SURFACES DE KUMMER

Soit A_k une variété abélienne sur k, et $\mathcal{L}_0$ un fibré irréductible symétrique sur A_k. Soit $\mathcal{L} = \mathcal{L}_0^2$, $\mathcal{L}$ est un fibré totalement symétrique de niveau 2, qui donne un plongement de la variété de Kummer K_{A_k} associée à A_k par la section 4.8. Soit $\Theta_{\mathcal{L}}$ une thêta structure symétrique sur $\mathcal{L}$; on suppose que les thêta null points pairs ne s'annulent pas pour $\mathcal{L}$, ce qui permet de calculer les pseudo-additions sur la variété de Kummer, et les additions normales modulo une racine carrée.

La variété de Kummer K_{A_k} est munie d'une structure de $\mathbb{Z}$-module, et si $\pm x$ et $\pm y$ sont des points de ℓ-torsion de K_{A_k}, et que l'on connaît de plus $\pm(x+y)$, on peut calculer $e_{\mathcal{L}^\ell}(x,y)$ exactement comme dans l'algorithme 5.4.2. Dans le cas général on peut calculer uniquement l'ensemble $\{\pm(x+y), \pm(x-y)\}$ à partir de $\pm x$ et de $\pm y$ en faisant une addition normale sur K_{A_k}.

Cependant, le pairing $e_{\mathcal{L}^\ell}$ sur $A_k[\ell]$ descend en un pairing

$$e_{\mathcal{L}^\ell,\mathtt{sym}} : K_{A_k}[\ell] \times K_{A_k}[\ell] \to \overline{k}^{*,\pm 1}, (\pm x, \pm y) \mapsto e_{\mathcal{L}^\ell}(x,y)$$

où $\overline{k}^{*,\pm 1}$ est le quotient de $\overline{k}^*$ par l'automorphisme $x \mapsto x^{-1}$, ce qui fait que $e_{\mathcal{L}^\ell,\mathtt{sym}}$ est bien défini. (Cette idée d'utiliser un pairing symétrique sur la variété de Kummer est très naturelle, elle a par exemple été utilisé dans [GL08].) Dans la suite, on représente un élément de $\{x, x^{-1}\} \in \overline{k}^{*,\pm 1}$ par $x + 1/x \in \overline{k}^*$. Le pairing $e_{\mathcal{L}^\ell,\mathtt{sym}}$ est alors représenté par

$$e_{\mathcal{L}^\ell,\mathtt{sym}}(\pm x, \pm y) = e_{\mathcal{L}^\ell}(x,y) + e_{\mathcal{L}^\ell}(-x,y) = e_{\mathcal{L}^\ell}(x,y) + \frac{1}{e_{\mathcal{L}^\ell}(x,y)}.$$

L'ensemble $\overline{k}^{*,\pm 1}$ est muni d'une structure de $\mathbb{Z}$-module, induite par l'exponentiation sur $\overline{k}$. En fait, exactement comme avec les variétés de Kummer, on a une pseudo-multiplication donnée par la formule

$$(x + \frac{1}{x})(y + \frac{1}{y}) = (xy + \frac{1}{xy})(\frac{x}{y} + \frac{y}{x}). \tag{5.9}$$

Ceci nous donne l'algorithme suivant pour calculer une exponentiation dans $\overline{k}^{*,\pm 1}$ en utilisant une chaîne de Montogmery.

ALGORITHME 5.5.1 (EXPONENTIATION SYMÉTRIQUE) :
Soit $\{x, x^{-1}\} \in \overline{k}^{*,\pm 1}$ représenté par $x + 1/x$. On calcule les $i.x$ pour $i \in \mathbb{N}$ via une chaine de Montgomery :

Doublement :

Entrées $i.x \in \overline{k}^{*,\pm 1}$
Sortie $2i.x \in \overline{k}^{*,\pm 1}$

➔ Retourner $(i.x)^2 - 2$.

Pseudo-addition :

Entrées $i.x, j.x, (i-j).x \in \overline{k}^{*,\pm 1}$
Sortie $(i+j).x \in \overline{k}^{*,\pm 1}$

➔ Retourner $(i.x) \times (j.x) - (i-j).x$. ◊

Le pairing symétrique $e_{\mathcal{L}^\ell,\mathtt{sym}}$ est compatible avec la structure de $\mathbb{Z}$-module de K_{A_k} et la structure de $\mathbb{Z}$-module sur $\overline{k}^{*,\pm 1}$, ce qui permet d'utiliser la plupart des applications cryptographiques des pairings, qui n'utilisent pas la bilinéarité mais seulement la structure de $\mathbb{Z}$-module. Si on a besoin de la bilinéarité, au prix d'une racine carrée, on peut calculer l'ensemble $\{x, 1/x\}$ à partir de $x+1/x$, et donc calculer l'ensemble $\{xy+\frac{1}{xy}, \frac{x}{y}+\frac{y}{x}\}$ à partir de $x+1/x$ et de $y+1/y$.

De même, on peut définir un pairing de Tate symétrique à valeurs dans $\overline{k}^{*,\pm 1}/\overline{k}^{*,\pm \ell}$, et utiliser l'algorithme 5.5.1 pour calculer l'exponentiation finale du pairing de Tate afin d'avoir un représentant dans $\overline{k}^{*,\pm 1}$.

Le pairing symétrique se calcule immédiatement grâce à l'algorithme 5.4.2 : si on a x et y des points de ℓ-torsions de A_k, on calcule $\{x+y, x-y\}$ via une addition normale (voir la section 4.8), ce qui nous permet ensuite de calculer $e_{\mathcal{L}^\ell}(x,y)+e_{\mathcal{L}^\ell}(x,-y)$ en faisant les pseudo-additions de l'algorithme 5.4.2. On procède de même pour le pairing de Tate.

L'inconvénient de cette méthode est qu'elle nécessite une racine carrée. Une autre méthode consiste à travailler dans l'algèbre $\mathcal{A} \coloneqq k[X]/P_{i_0}$ où $P_{i_0} = X^2 - 2\frac{\kappa_{i_0,0}}{\kappa_{0,0}}X + \frac{\kappa_{i_0,i_0}}{\kappa_{0,0}}$, en reprenant les notations de la preuve de la proposition 4.8.6. En reprenant cette preuve, on voit que $\{\vartheta_{i_0}(\widetilde{x+y}), \vartheta_{i_0}(\widetilde{x-y})\}$ sont les deux racines de P_{i_0}. De plus, si σ est l'automorphisme de $\mathcal{A}$ qui permute ces deux racines, on peut utiliser l'équation (4.34) formellement en remplaçant $\vartheta_{i_0}(\widetilde{x+y})$ par X et $\vartheta_{i_0}(\widetilde{x-y})$ par $\sigma(X)$ pour obtenir formellement $\vartheta_i(\widetilde{x+y}) = \alpha_i X + \beta_i$ lorsque $i \in Z(\delta)$. On peut alors calculer formellement $e_{\mathcal{L}^\ell}(x,y)$ dans $\mathcal{A}$ grâce à l'algorithme 5.4.2 (les coefficients des points seront dans $\mathcal{A}$), on retrouve alors :

$$e_{\mathcal{L}^\ell,\mathtt{sym}}(x,y) = e_{\mathcal{L}^\ell}(x,y) + \sigma(e_{\mathcal{L}^\ell}(x,y)).$$

En fait, on n'a pas besoin de faire tous les calculs dans $\mathcal{A}$ pour $e_{\mathcal{L}^\ell,\mathtt{sym}}$. Prenons l'exemple du pairing de Tate et de Weil complexes de la section 5.3. On a en reprenant les notations de cette section, si z_P et z_Q sont des points représentant P et Q, et que $\vartheta_i = \vartheta\left[\begin{smallmatrix}0\\ i/n\end{smallmatrix}\right](\cdot, \Omega/n)$:

$$e_{T,\mathtt{sym}}(P,Q) = \frac{[\vartheta_i(\ell.z_Q+z_P)+\vartheta_i(-\ell.z_Q+z_P)]\vartheta_i(0)}{\vartheta_i(z_P)\vartheta_i(\ell.z_Q)} \tag{5.10}$$

$$e_{W,\mathtt{sym}}(P,Q) = \frac{\vartheta_i(z_Q)\vartheta_i(\ell.z_P)[\vartheta_i(\ell.z_Q+z_P)\vartheta_i(z_Q-\ell z_P)+\vartheta_i(\ell.z_Q-z_P)\vartheta_i(z_Q+\ell z_P)]}{\vartheta_i(z_P)\vartheta_i(\ell.z_Q)\vartheta_i(z_Q+\ell.z_P)\vartheta_i(z_Q-\ell.z_P)} \tag{5.11}$$

Pour le pairing de Tate, il suffit de calculer $R = \mathtt{chain\_multadd}(\ell, P+Q, Q, P)$ dans $\mathcal{A}$, on a alors $R+\sigma R = \mathtt{chain\_multadd}(\ell, P+Q, Q, P) + \mathtt{chain\_multadd}(\ell, P-Q, Q, P)$ dans k. Le calcul de $\ell.z_Q$ se fait lui directement (en considérant les coefficients des points) dans k. De même, pour le pairing de Weil, il suffit de faire le calcul de

$$\vartheta_i(\ell.z_Q+z_P)\vartheta_i(z_Q-\ell z_P)+\vartheta_i(\ell.z_Q-z_P)\vartheta_i(z_Q+\ell z_P)$$

dans $\mathcal{A}$, par exemple $\vartheta_i(z_Q+\ell.z_P)\vartheta_i(z_Q-\ell.z_P)$ se calcule directement grâce aux formules d'addition du théorème 4.4.6.

Exemple 5.5.2 (Pairing en genre 2). Soit H la courbe hyperelliptique au-dessus du corps fini $\mathbb{F}_p$, $p = 331$, d'équation :

$$Y^2 = X^5 + 204X^4 + 198X^3 + 80X^2 + 179X.$$

Soit J la Jacobienne de H. Le cardinal de $J(\mathbb{F}_p)$ est $2^6 \cdot 1889$ (H a été choisie de telle sorte que son polynôme de définition soit scindé sur $\mathbb{F}_p$, de telle sorte que les points de 2-torsion

sur J sont rationnels). On pose $\ell = 1889$, l'embedding degree d correspondant à ℓ est $d = 4$. Un thêta null point de niveau 2 associé à J est donné par $0_J = (328 : 213 : 75 : 1)$. Soit $P = (255 : 89 : 30 : 1)$, P est un générateur de $J(\mathbb{F}_p)[\ell]$. Soit $\mathbb{F}_{p^d} \simeq \mathbb{F}_p(t)/(t^4 + 3t^2 + 290t + 3)$, t est un élément primitif de $\mathbb{F}_{p^d}/\mathbb{F}_p$.Soit Q le $\mathbb{F}_{p^d}$-point de ℓ-torsion dont les coordonnées sont données par :

$$(158t^3 + 67t^2 + 9t + 293 : 290t^3 + 25t^2 + 235t + 280 : 155t^3 + 84t^2 + 15t + 170 : 1).$$

On calcule à l'aide de l'algorithme 4.8.7 (en fixant un ordre arbitraire sur $\{\pm(P+Q), \pm(P-Q)\}$) :

$$P + Q = (217t^3 + 271t^2 + 33t + 303 : 308t^3 + 140t^2 + 216t + 312 : 274t^3 + 263t^2 + 284t + 302 : 1)$$
$$P - Q = (62t^3 + 16t^2 + 255t + 129 : 172t^3 + 157t^2 + 43t + 222 : 258t^3 + 39t^2 + 313t + 150 : 1).$$

Enfin, soit $r = \frac{p^d-1}{\ell} = 6354480$ et $\zeta = t^r$ une racine primitive ℓ-ième de l'unité.

On calcule alors en utilisant l'algorithme 4.4.12 :

$$\ell\widetilde{P} = (12, 141, 31, 327) = 327.\widetilde{0}_J$$
$$\ell\widetilde{Q} = (21t^3 + 280t^2 + 101t + 180, 164t^3 + 311t^2 + 111t + 129,$$
$$137t^3 + 282t^2 + 123t + 134, 324t^3 + 17t^2 + 187t + 271) = (324t^3 + 17t^2 + 187t + 271).\widetilde{0}_J$$
$$\texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{Q}, \widetilde{P}) = (45t^3 + 118t^2 + 219t + 308, 152t^3 + 97t^2 + 166t + 40,$$
$$200t^3 + 267t^2 + 201t + 192, 117t^3 + 42t^2 + 106t + 205) = (117t^3 + 42t^2 + 106t + 205).\widetilde{P}$$
$$\texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}) = (50t^3 + 31t^2 + 84t + 309, 168t^3 + 196t^2 + 275t + 234,$$
$$67t^3 + 186t^2 + 159t + 102, 243t^3 + 320t^2 + 222t + 200) = (243t^3 + 320t^2 + 222t + 200).\widetilde{Q}.$$

On obtient alors (en gardant l'ordre précédent sur $\{\pm(P+Q), \pm(P-Q)\}$) :

$$e_W(P,Q) = \frac{243t^3 + 320t^2 + 222t + 200}{327} \cdot \frac{324t^3 + 17t^2 + 187t + 271}{117t^3 + 42t^2 + 106t + 205} = \zeta^{-1}$$
$$e_T(P,Q) = \left(\frac{117t^3 + 42t^2 + 106t + 205}{324t^3 + 17t^2 + 187t + 271}\right)^r = \zeta^{1068}$$
$$e_T(Q,P) = \left(\frac{243t^3 + 320t^2 + 222t + 200}{327}\right)^r = \zeta^{1184}.$$

(Les pairing de Tate sont normalisés en les mettant à la puissance $r = (p^k - 1)/\ell$.)

Les pairing symétriques sont alors $e_{W,\mathtt{sym}}(P,Q) = 61t^3 + 285t^2 + 196t + 257$ et $e_{T,\mathtt{sym}}(P,Q) = 194t^3 + 163t^2 + 97t + 164$. ◇

6 CORRESPONDANCE MODULAIRE

MATIÈRES

6.1 INTRODUCTION

Le but de ce chapitre est de donner un équivalent du polynôme modulaire (du genre 1) Φ_ℓ où l'on considère les invariants donnés par le thêta null point plutôt que par les j-invariants (voir la section 1.4).

On peut visualiser le polynôme modulaire Φ_ℓ ainsi : Si $N \in \mathbb{N}^*$, la courbe modulaire $X_0(N)$ paramétrise les classes d'isomorphismes de courbes elliptiques munies d'un sous-groupe cyclique de N-torsion. Si p est premier à N, et (E, G) est un point de $X_0(pN)$, G est un sous-groupe cyclique d'ordre pN de la courbe elliptique E. On peut alors considérer G_1 l'unique sous-groupe d'ordre N de G, et G_2 l'unique sous-groupe d'ordre p de G. On en déduit une application $\phi_p : X_0(pN) \to X_0(N) \times X_0(N), (E, G) \mapsto ((E, G_1), (E/G_2, G/G_2))$ (voir [Koh03]). En particulier, si $N = 1$, on a une correspondance modulaire

$$\phi_p : X_0(p) \to X_0(1) \times X_0(1)$$

et comme $X_0(1)$ est une courbe de genre 0 (c'est la ligne projective donnée par les j-invariants), l'image de $X_0(p)$ est donnée par une équation polynomiale $\Phi_p(X, Y) = 0$ dans $X_0(1) \times X_0(1)$. Il s'agit exactement de la définition du polynôme modulaire Φ_p.

Maintenant, si on regarde du côté des thêta null points, on va construire une correspondance modulaire ainsi : soit $n \geqslant 4$ un nombre pair et ℓ un nombre premier à n. Si $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ est la variété abélienne marquée de niveau ℓn correspondant à un thêta null point dans $\mathcal{M}_{\overline{\ell n}}(k)$, on a en particulier une décomposition de la ℓn torsion de A_k : $A_k[\ell n] = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$. On en déduit une décomposition de la ℓ torsion de A_k : $A_k[\ell] = K_1(\mathcal{L})[\ell] \oplus K_2(\mathcal{L})[\ell]$, et par la section 3.6, il existe un unique marquage sur $B_k \coloneqq A_k/K_2(\mathcal{L})[\ell]$ et sur $C_k \coloneqq A_k/K_1(\mathcal{L})[\ell]$ compatible avec la thêta structure de A_k. On a donc une correspondance modulaire

$$\phi_{\ell n} : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}, (A_k, \mathcal{L}, G(\mathcal{L})) \mapsto (B_k, C_k).$$

Dans la section 6.2, on étudie cette correspondance modulaire, et les isogénies que l'on obtient ainsi (voir le théorème 6.2.7). Par exemple, si ℓ est premier à n, les points modulaires dans $\phi_1^{-1}((b_i)_{i \in Z(\overline{n})})$ (où $(b_i)_{i \in Z(\overline{n})}$ est le thêta null point associé à B_k, et ϕ_1 est la projection de ϕ sur le premier facteur $\mathcal{M}_{\overline{n}}$) correspondent à des noyaux isotropes (maximaux) de $B_k[\ell]$. Les équations explicites de la correspondance modulaire sont définies sur la variété $\overline{\mathcal{M}}_{\overline{\ell n}}$, ce qui veut dire qu'il nous faut un critère pour identifier quand un point solution $(a_i)_{i \in Z(\overline{\ell n})} \in \overline{\mathcal{M}}_{\overline{\ell n}}$ est dégénéré (c'est-à-dire que $(a_i)_{i \in Z(\overline{\ell n})}$ n'est pas un point géométrique $\mathcal{M}_{\overline{\ell n}}$, ou encore que

$(a_i)_{i\in Z(\overline{\ell n})}$ n'est pas le thêta null point associé à une variété abélienne marquée). C'est l'objet de la section 6.3. Comme on l'a noté dans l'introduction, l'avantage de la correspondance modulaire $\phi_{\ell n}$ vient du fait que ses équations sont faciles à expliciter : elles découlent trivialement des équations de $\overline{\mathcal{M}_{\overline{\ell n}}}$. En particulier, les coefficients sont ± 1, ce qui est un grand avantage par rapport aux polynômes modulaires entre les invariants d'Igusa en genre 2. L'inconvénient est qu'un point solution correspond à choisir une ℓ-isogénie ainsi qu'une décomposition de la ℓ-torsion de la variété isogène, compatible avec l'isogénie duale (si ℓ est premier à n). En particulier, il y a beaucoup plus de solutions que de ℓ-isogénies. Dans la section 6.4, on étudie le nombre total de solutions pour le comparer au nombre d'isogénies. On verra que le système est de degré bien plus grand que ℓ^{2g}, ce qui explique pourquoi calculer des isogénies en utilisant les formules de Vélu généralisées sont plus rapides que de calculer un point modulaire solution.

Dans ce chapitre, on présente et généralise les résultats de l'article [FLR09] (où l'on étudiait la correspondance modulaire entre le niveau ℓn et le niveau n avec ℓ premier à n) au cas du niveau quelconque (c'est-à-dire que l'on étudie la correspondance modulaire entre un niveau δ et un niveau δ_0 avec $\delta_0 \mid \delta$). Si l'on reste au cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$, alors la différence peut se voir ainsi : un point modulaire correspond à une ℓ-isogénie, et à une structure de niveau ℓn compatible avec la structure de niveau n sur B_k. Si ℓ n'est pas premier à n, il ne suffit pas de choisir une décomposition de la ℓ-torsion $A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2$ telle que $A_k[\ell]_2$ soit le noyau de l'isogénie $\pi : A_k \to B_k$.

Si on se fixe une ℓ-isogénie $f : A_k \to B_k$, on peut étudier d'une part les différentes structures de niveau sur A_k au-dessus de f en utilisant les résultats de la section 3.5 (voir la proposition 6.3.5), ce qui donne de nouveaux points modulaires. D'autre part, on peut étudier les contraintes induites par les relations de Riemann sur les points modulaires solutions (voir la proposition 6.3.2 et le lemme 6.3.4). En combinant ces deux méthodes, on peut alors déterminer exactement les points modulaires solutions induisant l'isogénie f (théorème 6.3.6 et proposition 6.4.2). Par exemple, la situation est très différente suivant que ℓ est pair ou non. Si $2 \mid \ell$, les relations de symétrie dans les relations de Riemann nous donnent moins de contraintes sur les points solutions. Ceci s'explique par le fait que dans ce cas, on a plus d'automorphismes du groupe de Heisenberg donnant lieu à la même isogénie f. En effet, on peut changer la structure de niveau de A_k par une autre structure symétrique (au-dessus de la même décomposition de $K(\mathcal{L})$) sans changer f.

6.2 LA CORRESPONDANCE MODULAIRE

Le lecteur qui ne souhaite considérer que des ℓ-isogénies pourra poser $\delta_0 = \overline{n}$, $\delta' = \overline{\ell}$ et donc $\delta = \overline{\ell n}$, avec de plus $\ell \wedge n = 1$.

Soit k un corps parfait, et donnons-nous $\delta_0 \in \mathbb{Z}^g$ divisible par un nombre pair $n \geqslant 4$ et $\delta' \in \mathbb{Z}^g$. Posons $\delta = \delta_0\delta'$. Soit $D = \prod \delta_i$ le degré de δ. Pour simplifier l'exposé, on suppose de plus que k contient les racines D-ième de l'unité (ce qui permet de s'assurer que les automorphismes du groupe symplectique $K(\delta)$ sont rationnels, on en aura besoin pour l'étude de l'action des automorphismes du groupe de Heisenberg sur les points modulaires solutions).

Définition 6.2.1 (La correspondance modulaire sur $\overline{\mathcal{M}_\delta}$). On rappelle que la variété $\overline{\mathcal{M}_\delta}$ est une variété projective donnée dans $\mathbb{P}_k^{D-1}$ par les relations de Riemann et de symétrie (en reprenant les notations du théorème 4.7.2) (voir la section 4.7) :

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t) Q_{i+t} Q_{j+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) Q_{k+t} Q_{l+t}\Big) =$$
$$\Big(\sum_{t\in Z(\overline{2})} \chi(t) Q_{i'+t} Q_{j'+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) Q_{k'+t} Q_{l'+t}\Big).$$
$$Q_i = Q_{-i}.$$

On définit la correspondance modulaire $\overline{\phi} : \overline{\mathcal{M}}_\delta \to \overline{\mathcal{M}}_{\delta_0} \times \overline{\mathcal{M}}_{\delta_0}$ sur les points géométriques par

$$\phi((a_i)_{i\in Z(\delta)}) \mapsto ((a_i)_{i\in Z(\delta_0)}, (\sum_{j\in Z(\delta')} a_{i+j})_{i\in Z(\delta_0)}) \tag{6.1}$$

◇

Exemple 6.2.2. Si $\delta = \overline{\ell n}$ et $\delta' = \overline{n}$, l'inclusion canonique de $Z(\overline{n})$ (resp. $Z(\overline{\ell})$) dans $Z(\overline{\ell n})$ est donnée par $x \mapsto \ell x$ (resp. $x \mapsto nx$). On a alors :

$$\overline{\phi}((a_i)_{i\in Z(\overline{\ell n})}) \mapsto ((a_{\ell i})_{i\in Z(\overline{n})}, (\sum_{j\in Z(\overline{\ell})} a_{\ell i+nj})_{i\in Z(\overline{n})})$$

◇

Remarque 6.2.3. Soit $\overline{\phi}_1$ la projection de $\overline{\phi}$ par rapport à la première coordonnée et $\overline{\phi}_2$ la projection par rapport à la deuxième. Si $(a_i)_{i\in Z(\delta)}$ est dans $\overline{\mathcal{M}}_\delta(k)$, on note $(b_i)_{i\in Z(\delta_0)} = \overline{\phi}_1((a_i)_{i\in Z(\delta)})$ et $(c_i)_{i\in Z(\delta_0)} = \overline{\phi}_2((a_i)_{i\in Z(\delta)})$.

S'il est clair d'après l'équation de $\overline{\phi}_1$ que $(b_i)_{i\in Z(\delta_0)}$ est bien dans $\overline{\mathcal{M}}_\delta(k)$, ça l'est peut-être moins pour $(c_i)_{i\in Z(\delta_0)}$. En fait, il suffit d'appliquer la même stratégie que dans la section 4.5 : si $\mathfrak{I}_\delta((a_i)_{i\in Z(\delta)}) \coloneqq (\sum_{j\in Z(\delta)} e_\delta(-i,j)x_j)_{i\in Z(\delta)}$, la preuve de la proposition 4.5.2 montre que $\mathfrak{I}_\delta((a_i)_{i\in Z(\delta)}) \in \overline{\mathcal{M}}_\delta(k)$. Or $\overline{\phi}_2 = \mathfrak{I}_{\delta_0} \circ \overline{\phi}_1 \circ \mathfrak{I}_\delta$, ce qui montre que $(c_i)_{i\in Z(\delta_0)} \in \overline{\mathcal{M}}_\delta(k)$. ◇

Proposition 6.2.4. *L'application $\overline{\phi} : \overline{\mathcal{M}}_\delta \to \overline{\mathcal{M}}_{\delta_0} \times \overline{\mathcal{M}}_{\delta_0}$ se restreint en une application $\phi : \mathcal{M}_\delta \to \mathcal{M}_{\delta_0} \times \mathcal{M}_{\delta_0}$.*

Soit $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$, on pose

$$\phi((a_i)_{i\in Z(\delta)}) = ((b_i)_{i\in Z(\delta_0)}, (c_i)_{i\in Z(\delta_0)}).$$

Si $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta(k)$ correspond à une variété marquée $(A_k, \mathcal{L}, \Theta_\mathcal{L})$, $(b_i)_{i\in Z(\delta_0)}$ correspond à une variété marquée $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ et $(c_i)_{i\in Z(\delta_0)}$ correspond à $(C_k, \mathcal{L}'_0, \Theta_{\mathcal{L}'_0})$ alors $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ est (l'unique variété marquée) $\hat{Z}(\delta')$-compatible avec $(A_k, \mathcal{L}, \Theta_\mathcal{L})$. De même, $(C_k, \mathcal{L}'_0, \Theta_{\mathcal{L}'_0})$ est (l'unique variété marquée) $Z(\delta')$-compatible avec $(A_k, \mathcal{L}, \Theta_\mathcal{L})$ (on peut consulter l'exemple 3.6.5 pour ces notions).

En particulier, si $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ est la décomposition de $K(\mathcal{L})$ induite par la théta structure $\Theta_\mathcal{L}$, alors $B_k = A_k/K_2(\mathcal{L})[\delta']$ et $C_k = A_k/K_1(\mathcal{L})[\delta']$ (où on note $K_2(\mathcal{L})[\delta'] \coloneqq \overline{\Theta}_\mathcal{L}(\hat{Z}(\delta'))$ et $K_1(\mathcal{L})[\delta'] \coloneqq \overline{\Theta}_\mathcal{L}(Z(\delta'))$). L'isogénie $\pi_1 : A_k \to B_k$ est donnée sur les points géométriques de A_k par

$$\pi_1((x_i)_{i\in Z(\delta)}) = (x_i)_{i\in Z(\delta_0)} \tag{6.2}$$

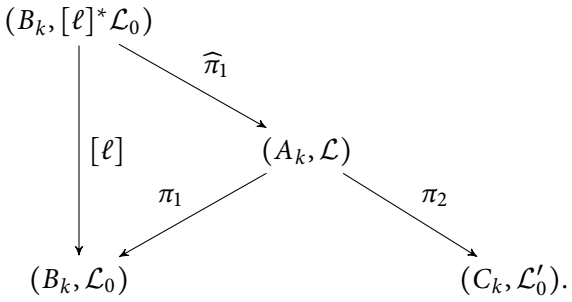
et $\pi_2 : A_k \to C_k$ est donnée sur les points géométriques par

$$\pi_2((x_i)_{i\in Z(\delta)}) = (\sum_{j\in Z(\delta')} x_{i+j})_{i\in Z(\delta_0)}. \tag{6.3}$$

Démonstration : On a vu dans l'exemple 3.6.5 que l'isogénie π_1 de type $\hat{Z}(\delta')$ était donnée sur les points géométriques par l'équation (6.2). Soit $D_k \coloneqq A_k/K_2(\mathcal{L})[\delta']$, et $\mathcal{M}$ la descente de $\mathcal{L}$ associée au groupe de niveau $s_{K(\mathcal{L})}(K_2(\mathcal{L})[\delta'])$ induit par $\Theta_\mathcal{L}$, et $\Theta_\mathcal{M}$ l'unique théta structure π_1-compatible avec $\Theta_\mathcal{L}$. Alors le théta null point de $(D_k, \mathcal{M}, \Theta_\mathcal{M})$ est donné par $\pi_1((a_i)_{i\in Z(\delta)}) = (b_i)_{i\in Z(\delta_0)}$, donc comme les théta null points déterminent le marquage, $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0}) = (D_k, \mathcal{M}, \Theta_\mathcal{M})$.

Le même raisonnement s'applique à π_2 et la variété abélienne marquée $(C_k, \mathcal{L}'_0, \Theta_{\mathcal{L}'_0})$. ■

Soit $\ell = \vee_{i=1}^{g} \delta_i'$, et $\delta'' \in \mathbb{N}^g$ le vecteur tel que $\overline{\ell} = \delta'\delta''$. L'isogénie contragrédiente $\widehat{\pi}_1 : B_k \to A_k$ a pour noyau $\pi_1(A_k[\ell])$, qui est de type $Z(\overline{\ell}) \times Z(\delta'')$. La correspondance modulaire ϕ correspond au diagramme commutatif suivant :



On constate une différence importante avec la correspondance modulaire $\phi : X_0(pN) \to X_0(N) \times X_0(N)$. Lorsqu'on part d'une courbe elliptique E représentée par un point x_E de $X_0(N)$, un relevé $y_E \in \phi_1^{-1}(x_E) \subset X_0(pN)$ représente toujours la même courbe elliptique, et $\phi_2(y_E)$ donne une courbe elliptique p-isogène à E. Ici, avec la correspondance modulaire $\phi : \mathcal{M}_\delta \to \mathcal{M}_{\delta_0} \times \mathcal{M}_{\delta_0}$, un relevé $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ correspond déjà à une variété $(\delta_1'', \dots, \delta_g'', \ell, \dots, \ell)$ isogène à B_k, et redescendre en niveau δ_0 via ϕ_2 nous donne une isogénie $\pi_2 \circ \widehat{\pi}_1$ de type $(\delta_1'', \dots, \delta_g'', \delta_1'\ell, \dots, \delta_g'\ell)$. La situation se simplifie considérablement si l'on a $\delta = \overline{\ell n}$, $\delta_0 = \overline{n}$: dans ce cas, $\widehat{\pi}_1$ est une ℓ-isogénie, et $\pi_2 \circ \widehat{\pi}_1$ une ℓ^2-isogénie. Dans la suite du chapitre, on étudie essentiellement le morphisme ϕ_1 et la relation entre B_k et A_k. Bien entendu la situation est symétrique pour C_k et ϕ_2, on peut passer d'une situation à l'autre en appliquant l'automorphisme $\mathfrak{I}$ comme dans la remarque 6.2.3.

On va commencer par déterminer les fibres de ϕ_1.

PROPOSITION 6.2.5. *Soit $(b_i)_{i\in Z(\delta_0)} \in \mathcal{M}_{\delta_0}(k)$, correspondant à la variété abélienne marquée $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$, et $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta(\overline{k})$ correspondant à $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$. Soit $K(\mathcal{L}_0^2) = K_1(\mathcal{L}_0^2) \oplus K_2(\mathcal{L}_0^2)$ la décomposition symplectique induisant le thêta null point $(b_i)_{i\in Z(\delta_0)}$, et $K(\mathcal{L}^2) = K_1(\mathcal{L}^2) \oplus K_2(\mathcal{L}^2)$ celle induisant le thêta null point $(a_i)_{i\in Z(\delta)}$. Soit $K = K_2(\mathcal{L})[\delta']$. Alors $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ si et seulement si $A_k/K \simeq B_k$, et si $\pi : A_k \to B_k$ est l'isogénie associée, on a de plus $\pi(K_1(\mathcal{L}^2)[2\delta_0]) = K_1(\mathcal{L}_0^2)$ et $\pi(K_2(\mathcal{L}^2) = K_2(\mathcal{L}_0^2)$ (et la numérotation de $K_1(\mathcal{L})$ est compatible avec la numérotation de $K_1(\mathcal{L}_0)$).*

DÉMONSTRATION : C'est une conséquence immédiate de la section 3.6 et de la proposition 4.3.1. ∎

Ainsi, si $\pi : (A_k, \mathcal{L}) \to (B_k, \mathcal{L}_0)$ est une isogénie dont le noyau est isomorphe à $Z(\delta')$, il existe une thêta structure symétrique sur $(A_k, \mathcal{L})$ telle que le thêta null point correspondant soit un point géométrique dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$. Pour simplifier l'étude des points géométriques dans la fibre, on adopte la convention suivante : si $(a_i)_{i\in Z(\delta)}$ est un point dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})(\overline{k})$, par la proposition 6.2.5 il existe une extension finie k_0 de k telle que $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})(k_0)$. Si $(a_i)_{i\in Z(\delta)}$ correspond à la variété abélienne marquée $(A_{k_0}, \mathcal{L}_{k_0}, \Theta_{\mathcal{L}_{k_0}})$, il existe alors une isogénie $\pi : (A_{k_0}, \mathcal{L}_{k_0}) \to (B_{k_0}, \mathcal{L}_{0,k_0})$ de type $Z(\delta')$, où $(B_{k_0}, \mathcal{L}_{0,k_0})$ est l'extension des scalaires de $(B_k, \mathcal{L}_{0,k})$. Pour alléger les notations, on suppose systématiquement que l'on a fait cette extension, et on pose $k = k_0$.

On peut alors se demander quelles sont les isogénies $\widehat{\pi}$ correspondant à des points géométriques dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$? Avant d'étudier ce cas dans le théorème 6.2.7, on a besoin d'étudier les sous-groupes isotropes d'un espace symplectique fini. Soit donc $K(\delta)$ le groupe

symplectique de type δ, on appelle un sous-groupe isotrope maximal un sous-groupe K de $K(\delta)$ isotrope et isomorphe à $Z(\delta)$. Il existe alors un (et même plusieurs) sous-groupe isotrope maximal K' supplémentaire de K, ce supplémentaire donne donc une décomposition symplectique de $K(\delta)$ donnée par $K(\delta) = K \oplus K'$. Enfin, on appelle un sous-groupe isotrope K de $K(\delta)$ totalement isotrope s'il est inclus dans un groupe isotrope maximal. Il existe des sous-groupes isotropes, maximaux au sens de l'inclusion, qui ne sont pas isomorphes à $Z(\delta)$ (par exemple, le groupe $K(\overline{n}) \subset K(\overline{2n})$ est isotrope pour $e_{\overline{2n}}$), ce qui nous donne des exemples de groupes isotropes qui ne sont pas totalement isotropes. Pour donner un critère caractérisant les groupes totalement isotropes, on va donner un algorithme qui permet de calculer une base symplectique. On étudiera ensuite à quelle condition on peut appliquer cet algorithme pour construire un groupe totalement isotrope contenant un sous groupe donné.

ALGORITHME 6.2.6 (CONSTRUCTION D'UNE BASE SYMPLECTIQUE) :
Entrées $x_1, \dots, x_{2g}$ une base de $K(\delta)$, ainsi que les pairings $e_\delta(x_i, x_j)$ pour $i, j \in [1..2g]$.
Sortie Une base symplectique de $K(\delta)$.

- ➔ Soit $d = \vee_{i=1}^{g} \delta_i$, $\zeta \in k$ une racine primitive d-ième de l'unité, et $n_{i,j} \in \mathbb{N}$ tel que $e_\delta(x_i, x_j) = \zeta^{n_{i,j}}$ $(i, j \in [1..2g])$. (Le calcul des $n_{i,j}$ se fait en temps sous-exponentiel en d.)
- ➔ Soit i_0 tel que $e_\delta(x_1, x_{i_0}) \neq 1$. Un tel i_0 existe car e_δ n'est pas dégénérée, on peut supposer $i_0 = g + 1$. Soit $x'_{g+1} = x_{g+1}/e_\delta(x_1, x_{g+1})$.
- ➔ Pour tout $j \in [1..2g]\backslash\{1, g\}$
  - $x'_i = x_i - n_{g+1,i}x_1 - n_{1,i}x_{g+1}$.
- ➔ Appliquer l'algorithme récursivement à $\{x'_i \mid i \in [1..2g]\backslash\{1, g+1\}\}$ pour obtenir une base symplectique $(y_2, \dots, y_g, y'_2, \dots, y'_g)$.
- ➔ Retourner $(x_1, y_2, \dots, y_g, x'_{g+1}, y'_2, \dots, y'_g)$. ◊

En étudiant l'algorithme 6.2.6, on constate que si K est un sous-groupe de $K(\delta)$, soit $\delta_1 \in \mathbb{N}^g$ tel que $\delta \mid \delta_1$, alors K est un sous-groupe totalement isotrope de $K(\delta)$ si et seulement s'il est un sous-groupe totalement isotrope de $K(\delta_1)$ (où l'on plonge K via le plongement canonique $K(\delta) \to K(\delta_1)$). Autrement dit, il s'agit d'une notion intrinsèque, à la différence de la notion de groupe isotrope, et pour montrer que $K \subset A_k[\ell]$, il suffit de montrer que K est inclus dans un sous groupe isotrope maximal de $A_k[m\ell]$, pour m quelconque.

THÉORÈME 6.2.7. *Soit $(b_i)_{i\in Z(\delta_0)} \in \mathcal{M}_{\delta_0}(k)$, correspondant à la variété abélienne marquée $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$, et $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ correspondant à $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$, et $\pi := \pi_1 : A_k \to B_k$ l'isogénie correspondante entre A_k et B_k. On note $\mathfrak{K}((a_i)_{i\in Z(\delta)})$ le sous-groupe de B_k donné par $\mathfrak{K}((a_i)_{i\in Z(\delta)}) := \pi(K_1(\mathcal{L}))$.*

L'ensemble $\{\mathfrak{K}((a_i)_{i\in Z(\delta)}) \mid (a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})\}$ est égal à l'ensemble des sous-groupes totalement isotropes $\mathfrak{K}$ de type δ de $K(\mathcal{L}_0^\ell)$. (C'est donc l'ensemble des groupes $\mathfrak{K}$ de type δ inclus dans un sous-groupe isotrope maximal de $K(\mathcal{L}_0^\ell)$, pour le commutator pairing étendu $e_{\mathcal{L}_0^\ell}$).

Enfin, soit $K(\mathcal{L}_0^\ell) = K_1(\mathcal{L}_0^\ell) \oplus K_2(\mathcal{L}_0^\ell)$ une décomposition de $K(\mathcal{L}_0^\ell)$ telle que $K \subset K_1(\mathcal{L}_0^\ell)$, alors l'isogénie contragrédiente $\widehat{\pi} := \widehat{\pi_1} : B_k \to A_k$ a pour noyau $K_1(\mathcal{L}_0^\ell)[\ell] \oplus (\mathfrak{K}^\perp[\ell] \cap K_2(\mathcal{L}_0^\ell))$ (où l'orthogonal est encore pris par rapport à $e_{\mathcal{L}_0^\ell}$).

En particulier, si $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$, avec n premier à ℓ, les variétés A_k au-dessus de B_k par ϕ_1 correspondent aux quotients de B_k par un sous-groupe isotrope maximal de $B_k[\ell]$.

DÉMONSTRATION : Soit $(a_i)_{i\in Z(\delta)} \in \phi^{-1}((b_i)_{i\in Z(\delta_0)})$, un point modulaire correspondant à la variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$. On se fixe une décomposition $K(\mathcal{L}^\ell) = K_1(\mathcal{L}^\ell) \oplus$

$K_2(\mathcal{L}^\ell)$ au-dessus de celle de $K(\mathcal{L})$, et une base symplectique qui respecte cette décomposition. On pousse cette décomposition par π pour obtenir une décomposition $K(\mathcal{L}_0^\ell) = \pi(K_1(\mathcal{L}^\ell)[\ell\delta_0]) \oplus \pi(K_2(\mathcal{L}^\ell))$. Cette décomposition de $K(\mathcal{L}_0^\ell)$ est compatible avec celle de $K(\mathcal{L}_0)$ car par hypothèse, comme $(a_i)_{i\in Z(\delta)} \in \phi^{-1}((b_i)_{i\in Z(\delta_0)})$, la décomposition de $K(\mathcal{L}_0)$ est induite de celle de $K(\mathcal{L})$ par π. Comme $K_1(\mathcal{L}) \subset K_1(\mathcal{L}^\ell)[\ell\delta_0]$, on a $\mathfrak{K} \coloneqq \pi(K_1(\mathcal{L})) \subset K_1(\mathcal{L}_0^\ell)$, donc $\mathfrak{K}$ est bien un groupe isotrope maximal de $K(\mathcal{L}_0^\ell)$. De plus, $\mathfrak{K}$ est de type $Z(\delta)$, donc son orthogonal dans $K(\mathcal{L}_0^\ell)$ est de type $Z(\ell\delta_0) \oplus \hat{Z}(\delta'')$. Or l'isogénie contragrédiente $\widehat{\pi}$ a pour noyau $\pi(A[\ell])$ qui est de type $Z(\overline{\ell}) \times \hat{Z}(\delta'')$. Le noyau de $\widehat{\pi}$ est donc bien égal à $K_1(\mathcal{L}_0^\ell)[\ell] \oplus (\mathfrak{K}^\perp[\ell] \bigcap K_2(\mathcal{L}_0^\ell))$.

> Plus généralement, soit K un sous-groupe de $K(\mathcal{L}^\ell)$ inclus dans $\pi^{-1}(K(\mathcal{L}_0^\ell))$, $x \in \pi(K)$, et y un point géométrique dans $\pi^{-1}1(K(\mathcal{L}_0^\ell))$. Si x' est un point géométrique de B_k tel que $x = [\ell]x'$, on a $e_{\mathcal{L}_0^\ell}(x, y) = e_{[\ell]^*\mathcal{L}_0}(x', \pi(y)) = e_{\mathcal{L}}(\widehat{\pi}(x'), \widehat{\pi}\circ\pi(y)) = e_{\mathcal{L}}(\widehat{\pi}(x'), [\ell]y)$. Or $\widehat{\pi}(x')$ est un antécédent de x pour π, donc l'orthogonal de K dans $K(\mathcal{L}_0^\ell)$ est égal à
>
> $$\pi\left(([\ell]^{-1}(K^\perp)) \bigcap \pi^{-1}(K(\mathcal{L}_0^\ell))\right),$$
>
> où l'orthogonal est pris dans $K(\mathcal{L}^\ell)$ dans la formule précédente. Si l'on applique cela à $K = K_1(\mathcal{L})$; $K^\perp$ est de type $Z(\ell\delta) \times \hat{Z}(\ell)$, donc son intersection avec $\pi^{-1}(K(\mathcal{L}_0^\ell))$, qui est de type $Z(\ell\delta_0) \times \hat{Z}(\ell\delta)$, est de type $Z(\ell\delta_0) \times \hat{Z}(\ell)$. On retrouve que $\pi(K)^\perp$ est de type $Z(\ell\delta_0) \times \hat{Z}(\delta'')$.

Réciproquement, soit $K(\mathcal{L}_0^\ell) = K_1(\mathcal{L}_0^\ell) \oplus K_2(\mathcal{L}_0^\ell)$ une décomposition de $K(\mathcal{L}_0^\ell)$, et $\mathfrak{K}$ le sous-groupe de type $Z(\delta)$ de $K_1(\mathcal{L}_0^\ell)$. On choisit une décomposition de $K([\ell]^*\mathcal{L}_0)$ compatible avec celle de $K(\mathcal{L}_0^\ell)$, le groupe $\mathfrak{K}_2 \coloneqq K_1(\mathcal{L}_0^\ell)[\ell] \oplus (\mathfrak{K}^\perp[\ell] \bigcap K_2(\mathcal{L}_0^\ell))$ est isotrope et de type $Z(\overline{\ell}) \times \hat{Z}(\delta'')$ dans la décomposition de $K([\ell]^*\mathcal{L}_0)$. Le théorème 3.6.4 nous donne alors l'existence d'un fibré $\mathcal{L}$ et d'une thêta structure sur $A_k \coloneqq B_k/K_2$, avec si $\widehat{\pi} : B_k \to A_k$ est l'isogénie canonique, $\widehat{\pi}^*\mathcal{L} = [\ell]^*\mathcal{L}_0$. De plus, l'image de $B_k[\ell]$ dans A_k est de type $\hat{Z}(\delta')$, donc l'isogénie contragrédiente $(A_k, \mathcal{L}) \to (B_k, \mathcal{L}_0)$ est bien de type $\hat{Z}(\delta')$. On pousse la décomposition de $K([\ell]^*\mathcal{L}_0)$ via $\widehat{\pi}$ pour obtenir une décomposition de $K(\mathcal{L})$ qui est π-compatible avec celle de $K(\mathcal{L}_0)$. Il suffit ensuite de choisir une thêta structure symétrique au-dessus de cette décomposition, qui soit compatible avec la thêta structure de $(B_k, \mathcal{L}_0)$.

Enfin, si $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$, le noyau de $\widehat{\pi}$ est donné par $\pi(K_1(\mathcal{L})[\ell])$. Réciproquement, si K est un groupe de type $Z(\overline{\ell})$ isotrope pour $e_{\mathcal{L}_0^\ell}$, et si n est premier avec ℓ, l'orthogonal de K contient un groupe isotrope maximal. (En général, si K est un groupe de type $Z(\overline{\ell})$ quelconque, il est isotrope pour $e_{[\ell]^*\mathcal{L}_0}$, par contre il n'est contenu dans un groupe isotrope maximal, et donc on ne peut appliquer la construction précédente, que si K est de plus isotrope pour $e_{\mathcal{L}_0^\ell}$). ∎

On peut alors préciser la proposition 6.2.5, pour simplifier on se restreint au cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$.

Corollaire 6.2.8. *Soit $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ une variété abélienne marquée de niveau n, et $K(\mathcal{L}_0^2) = K_1(\mathcal{L}_0^2) \oplus K_2(\mathcal{L}_0^2)$ la décomposition symplectique associée. Soit K un sous-groupe isomorphe à $Z(\overline{\ell})$ et totalement isotrope pour $e_{\mathcal{L}_0^\ell}$. Soit $A_k = B_k/K$, $\pi : A_k \to B_k$ l'isogénie contragrédiente et $\mathcal{L} = \pi^*\mathcal{L}_0$.*

Alors se donner une thêta structure symétrique sur $(A_k, \mathcal{L})$ telle que le thêta null point associé $(a_i)_{i\in Z(\overline{\ell n})}$ soit dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ revient à se donner un supplémentaire isotrope $\mathfrak{K}_0$ de $\pi^{-1}(K_2(\mathcal{L}_0^2))$ pour $e_{\mathcal{L}^2}$ tel que $\pi(\mathfrak{K}_0[2n]) = K_1(\mathcal{L}_0^2)$ (et une numérotation de $K_1(\mathcal{L})$ compatible avec celle de $K_1(\mathcal{L}_0)$). Si ℓ est impair, il suffit de se donner un supplémentaire isotrope $\mathfrak{K}$ de $\pi^{-1}(K_2(\mathcal{L}_0))$ dans $A_k[n\ell]$ tel que $\pi(\mathfrak{K}[\ell]) = K_1(\mathcal{L}_0)$, et une numérotation de $\mathfrak{K}$ compatible

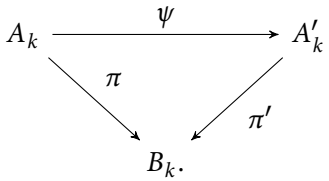
avec celle de $K_1(\mathcal{L}_0)$. Si de plus ℓ est premier à n, il suffit de se donner un supplémentaire $\mathfrak{K}'$ de $\pi^{-1}(K_2(\mathcal{L}_0))[\ell] = \widehat{\pi}(B_k[\ell])$ dans $A_k[\ell]$ (et une numérotation quelconque de $\mathfrak{K}'$).

DÉMONSTRATION : Si K est totalement isotrope pour $e_{\mathcal{L}_0^\ell}$, le théorème 6.2.7 montre qu'il existe une théta structure symétrique sur $(A_k, \mathcal{L})$ telle que $(a_i)_{i\in Z(\delta)}$ soit dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$. De plus par la proposition 6.2.5, si $K(\mathcal{L}^2) = K_1(\mathcal{L}^2) \oplus K_2(\mathcal{L}^2)$ est la décomposition symplectique associé, alors $K_2(\mathcal{L}^2) = \pi^{-1}(K_2(\mathcal{L}_0^2)$. Le groupe $K_2(\mathcal{L}^2)$ est donc entièrement fixé. De plus, un supplémentaire isotrope $\mathfrak{K}_0$ de $K_2(\mathcal{L}^2)$ compatible avec $K_1(\mathcal{L}_0^2)$ est tel que $\ell\mathfrak{K}_0 = \widehat{\pi}(K_1(\mathcal{L}_0^2))$. Ainsi, si ℓ est impair, et $\mathfrak{K}$ est un supplémentaire de $K_2(\mathcal{L})$ dans $A_k[n\ell]$, alors la seule possibilité pour avoir un supplémentaire de $K_2(\mathcal{L}^2)$ compatible avec $K_1(\mathcal{L}_0^2)$ et contenant $\mathfrak{K}$ est de prendre $\mathfrak{K}_0 = \mathfrak{K} + \pi(K_1(\mathcal{L}_0^2))$. Le cas ℓ premier à n se traite de la même manière. ■

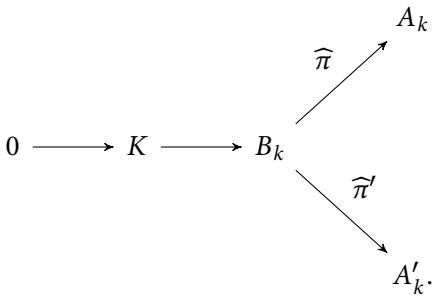
6.3 LES FIBRES DE LA CORRESPONDANCE MODULAIRE

Soit $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ une variété abélienne marquée de niveau δ_0 représentée par son théta null point $(b_i)_{i\in Z(\delta_0)} \in \mathcal{M}_{\delta_0}$. Le but de cette section est d'étudier quand deux points géométriques de la fibre $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ représentent la même variété abélienne (avec des marquages différents). Les points géométriques de $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ correspondent aux théta null points non dégénérés dans $\overline{\phi}_1^{-1}((b_i)_{i\in Z(\delta_0)})$.

Si $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ et $(A'_k, \mathcal{L}', \Theta_{\mathcal{L}'})$ sont deux points dans la fibre de $(b_i)_{i\in Z(\delta_0)}$, on cherche à déterminer s'il existe un isomorphisme $\psi : A_k \to A'_k$ qui rend commutatif le diagramme suivant :



Comme $\mathcal{L} = \pi^*\mathcal{L}_0$ et $\mathcal{L}' = \pi'^*\mathcal{L}_0$, on a $\mathcal{L} = \psi^*\mathcal{L}_0$. De plus si on passe aux isogénies contragrédientes, on voit que $\widehat{\pi}$ et $\widehat{\pi}'$ ont le même noyau K, d'où le diagramme commutatif suivant :



Autrement dit, l'ensemble précédent correspond à la classe $\mathscr{I}_K$ des isogénies de noyau K. De plus, le théorème 6.2.7 nous dit que $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ est l'union des $\mathscr{I}_K$ pour K parcourant les sous-groupes totalement isotropes de type $Z(\overline{\ell}) \times \hat{Z}(\delta'')$. Enfin le corollaire 6.2.8 montre que l'ensemble des $\mathscr{I}_K$ correspond aux choix de théta structures symétriques sur B_k/K compatibles avec $\Theta_{\mathcal{L}_0}$.

Si $(a_i)_{i\in Z(\delta)}$ et $(a'_i)_{i\in Z(\delta)}$ sont deux points géométriques de $\mathcal{M}_\delta$, on sait qu'ils correspondent à la même variété abélienne polarisée si et seulement s'ils différent par un automorphisme du

groupe de Heisenberg $\mathcal{H}(\delta)$. Soit $\alpha_{\hat{Z}(\delta')} : \rho^{-1}(\hat{Z}(\delta')) \to \mathcal{H}(\delta_0)$ l'isomorphisme canonique, où $\rho : \mathcal{H}(\delta) \to K(\delta)$ est la projection canonique. On note $\mathfrak{H}$ l'ensemble des automorphismes symétriques $\psi \in \mathrm{Aut}^0(\mathcal{H}(\delta))$, tels que $\alpha_{\hat{Z}(\delta')} \circ \psi = \alpha_{\hat{Z}(\delta')}$ sur $\rho^{-1}(\hat{Z}(\delta'))$.

Lemme 6.3.1. *Soit $\psi \in \mathrm{Aut}^0(\mathcal{H}(\delta))$ un automorphisme symétrique du groupe de Heisenberg. Alors les conditions suivantes sont équivalentes :*

i) Il existe un point géométrique $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$ tel que $\phi_1((a_i)_{i\in Z(\delta)}) = \phi_1(\psi.(a_i)_{i\in Z(\delta)})$.

ii) Pour tout point géométrique $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$, on a $\phi_1((a_i)_{i\in Z(\delta)}) = \phi_1(\psi.(a_i)_{i\in Z(\delta)})$.

iii) $\psi \in \mathfrak{H}$.

Par définition, le groupe $\mathfrak{H}$ est égal à l'ensemble des automorphismes symétriques $\psi \in \mathrm{Aut}^0 \mathcal{H}(\delta)$ tels que pour tout $x \in \mathcal{Z}(\hat{Z}(\delta'))$, on ait $\psi(x).x^{-1} \in \hat{Z}(\delta')$ (ici on plonge $\hat{Z}(\delta')$ dans $\mathcal{H}(\delta)$ via les plongements canoniques $\hat{Z}(\delta') \to \hat{Z}(\delta) \to \mathcal{H}(\delta)$). On a la suite exacte :

$$0 \longrightarrow K(\delta)[2] \cap \hat{Z}(\delta') \longrightarrow \mathfrak{H} \longrightarrow \overline{\mathfrak{H}} \longrightarrow 0,$$

où $\overline{\mathfrak{H}}$ est l'ensemble des automorphismes symplectiques $\overline{\psi} : K(\delta) \to K(\delta)$ telles que pour tout $x \in \mathcal{Z}(\hat{Z}(\delta'))$, $\overline{\psi}(x) - x \in \hat{Z}(\delta')$.

Démonstration : On a vu que le groupe $\mathrm{Aut}^0(\mathcal{H}(\delta))$ des automorphismes symétriques de $\mathcal{H}(\delta)$ était une extension de $\mathrm{Sp}(K(\delta))$ par $K(\delta)[2]$:

$$0 \longrightarrow K(\delta)[2] \longrightarrow \mathrm{Aut}^0(H(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 0.$$

Il est facile de voir que si $\psi \in \mathfrak{H}$, alors $\overline{\psi} \in \overline{\mathfrak{H}}$. Inversement, si $\overline{\psi}$ satisfait la condition que pour tout $x \in \mathcal{Z}(\hat{Z}(\delta'))$, $\overline{\psi}(x) - x \in \hat{Z}(\delta')$, on relève ψ en un automorphisme de $\mathrm{Aut}^0(\mathcal{H}(\delta))$. Alors on vérifie facilement que quitte à corriger ψ par un automorphisme $\mathtt{conj}_c$, on a $\psi \in \mathfrak{H}$. (Voir la remarque 3.5.2. On pourra consulter la proposition 6.3.5 pour des exemples explicites de tels automorphismes ψ.) Donc la flèche $\mathfrak{H} \to \overline{\mathfrak{H}}$ est bien surjective.

Enfin le noyau est donné par les $\mathtt{conj}_c$ qui sont dans $\mathfrak{H}$. Déjà, un tel c est dans $K(\delta)[2]$ car il faut que $\mathtt{conj}_c$ soit symétrique. De plus, on a vu qu'un tel automorphisme $\mathtt{conj}_c$ était compatible avec $\alpha_{\hat{Z}(\delta')}$ si et seulement si $c \in \hat{Z}(\delta')$, ce qui donne la description de $\mathfrak{H}$.

Enfin, soit $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$ un thêta null point correspondant à la variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$. Alors $(b_i)_{i\in Z(\delta_0)} = \phi_1((a_i)_{i\in Z(\delta)})$, correspond à une variété abélienne marquée $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$, où $\Theta_{\mathcal{L}_0}$ est $\hat{Z}(\delta')$-compatible avec $\Theta_{\mathcal{L}}$ par la proposition 6.2.4. Si $\psi \in \mathrm{Aut}^0(\mathcal{H}(\delta))$ est tel que $\phi_1(\psi.(a_i)_{i\in Z(\delta)}) = (b_i)_{i\in Z(\delta_0)}$, alors $\psi.(a_i)_{i\in Z(\delta)}$ correspond à une variété abélienne marquée $(A'_k, \mathcal{L}', \Theta'_{\mathcal{L}})$, $\Theta'_{\mathcal{L}}$ étant $\hat{Z}(\delta')$-compatible avec $\Theta_{\mathcal{L}_0}$. Mais $\Theta'_{\mathcal{L}}$ est la thêta structure issue de $\Theta_{\mathcal{L}}$ via l'action de ψ, et demander que $\Theta'_{\mathcal{L}}$ soit $\hat{Z}(\delta')$-compatible à $\Theta_{\mathcal{L}_0}$ revient exactement à demander que ψ soit dans $\mathfrak{H}$.

Enfin, si ψ est dans $\mathfrak{H}$, il est clair que par ce qui précède que ψ stabilise les fibres de ϕ_1. ■

Pour mieux étudier les points géométriques de $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$, on va utiliser les concepts de la section 4.4. Pour tout $j \in Z(\delta)$, on note $\widetilde{\pi}_j$ le morphisme

$$\widetilde{\pi}_j : \mathbb{A}_k^{Z(\delta)} \to \mathbb{A}_k^{Z(\delta_0)}, (x_i)_{i\in Z(\delta)} \to (x_{i+j})_{i\in Z(\delta_0)},$$

et $\pi_j : \mathbb{P}_k^{Z(\delta)} \to \mathbb{P}_k^{Z(\delta_0)}$ le morphisme projectif (rationnel) induit par $\widetilde{\pi}_j$. Si $(a_u)_{u\in Z(\delta)} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$ correspond à la variété marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$, que l'on visualise comme

étant une variété projective de $\mathbb{P}^{Z(\delta)}$ via le plongement canonique donné par les coordonnées thêta, alors les $\widetilde{\pi}_j|_{A_k} : A_k \to B_k$ correspondent exactement aux morphismes de la section 4.6. En particulier, π_0 se restreint en l'isogénie π sur A_k.

De plus, un point géométrique $(a_u)_{u\in Z(\delta)}$ est dans $\mathcal{M}_\delta$ si et seulement s'il satisfait les relations de Riemann du théorème 4.4.6 (ainsi que les relations de symétrie). On se fixe une fois pour toute un relevé affine $(b_u)_{u\in Z(\delta_0)}$ ce qui me permet si $(a_u)_{u\in Z(\delta)} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$ de le relever canoniquement en l'unique point affine $(a_u)_{u\in Z(\delta)}$ tel que $\widetilde{\pi}_0((a_u)_{u\in Z(\delta)}) = (b_u)_{u\in Z(\delta_0)}$. Comme $2 \mid \delta_0$, et que les relations de Riemann sont obtenues en sommant sur les points de 2-torsion de $Z(\delta)$, les relations de Riemann de niveau δ sur $(a_u)_{u\in Z(\delta)}$ sont exactement données par les relations de Riemann de niveau δ_0 sur

$$(\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_j((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_k((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_l((a_u)_{u\in Z(\delta)});$$
$$\widetilde{\pi}_{i'}((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_{j'}((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_{k'}((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_{l'}((a_u)_{u\in Z(\delta)}))$$

pour tous $i, j, k, l \in Z(\delta)$ tels que $i + j + k + l = 2m$ avec $i' = m - i$, $j' = m - j$, $k' = m - k$, $l' = m - l$. En particulier, en prenant $k = l = 0$, on va retrouver des relations d'additions sur les $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)})$:

Proposition 6.3.2. *Soit $(a_u)_{u\in Z(\delta)} \in \overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$. Alors l'ensemble $S \coloneqq \{i \in Z(\delta) \mid \pi_i((a_u)_{u\in Z(\delta)})$ est bien défini$\}$ est un sous-groupe de $Z(\delta)$ qui contient $Z(\delta_0)$. De plus, si $i \in S$ est d'ordre n, $\pi_i((a_u)_{u\in Z(\delta)})$ est un point de n-torsion de B_k.*

Démonstration : En effet, si $(a_u)_{u\in Z(\delta)}$ est un point géométrique quelconque de l'espace projectif $\mathbb{P}_k^{Z(\delta)}$, $(a_u)_{u\in Z(\delta)} \in \overline{\mathcal{M}}_\delta$ si et seulement s'il satisfait les formules d'addition (et de symétrie, voir la section 4.7) :

$$(a_u)_{u\in Z(\delta)} = \texttt{chain\_add}((a_u)_{u\in Z(\delta)}, (a_u)_{u\in Z(\delta)}, (a_u)_{u\in Z(\delta)}, (a_u)_{u\in Z(\delta)}).$$

Par la proposition 4.6.3, comme $\widetilde{\pi}_0((a_u)_{u\in Z(\delta)}) = (b_u)_{u\in Z(\delta_0)}$, on obtient que pour tous $i, j \in Z(\delta)$, puisque $\widetilde{\pi}_0((a_u)_{u\in Z(\delta)}) = (b_u)_{u\in Z(\delta_0)}$:

$$\widetilde{\pi}_{i+j}((a_u)_{u\in Z(\delta)}) =$$
$$\texttt{chain\_add}(\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_j((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_{i-j}((a_u)_{u\in Z(\delta)}), (b_u)_{u\in Z(\delta_0)}). \quad (6.4)$$

Donc si $\pi_i((a_u)_{u\in Z(\delta)})$ est bien défini, en appliquant l'équation (6.4) avec $j = 0$, on voit que $\pi_i((a_u)_{u\in Z(\delta)})$ est un point géométrique de B_k par le théorème 4.7.1. De plus, si $i \in Z(\delta_0)$, on a $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}) = (1, i, 0).(b_u)_{u\in Z(\delta_0)}$, donc S contient $Z(\delta_0)$.

Enfin, si $\pi_i((a_u)_{u\in Z(\delta)})$ est bien défini, $-\pi_i((a_u)_{u\in Z(\delta)}) = \pi_{-i}((a_u)_{u\in Z(\delta)})$ est bien défini, et si $\pi_j((a_u)_{u\in Z(\delta)})$ est bien défini, $\pi_i((a_u)_{u\in Z(\delta)}) + \pi_j((a_u)_{u\in Z(\delta)}) = \pi_{i+j}((a_u)_{u\in Z(\delta)})$ par l'équation (6.4) est bien défini. Donc l'ensemble S est bien un groupe, et si $i \in S$ est d'ordre n, on a $n.\pi_i((a_u)_{u\in Z(\delta)}) = \pi_{ni}((a_u)_{u\in Z(\delta)}) = \pi((a_u)_{u\in Z(\delta)}) = (b_u)_{u\in Z(\delta_0)}$, donc $\pi_i((a_u)_{u\in Z(\delta)})$ est bien un point de n-torsion. ∎

Corollaire 6.3.3. *La fibre $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$ est de dimension 0.*

Démonstration : En effet, si $(a_u)_{u\in Z(\delta)}$ est un point géométrique de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$, et $i \in Z(\delta)$, soit $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}) = (0, \dots, 0)$, soit $\pi_i((a_u)_{u\in Z(\delta)})$ est un point de N-torsion de B_k où N est l'exposant de $Z(\delta)$. Dans ce cas, soit $\widetilde{x}$ un relevé affine de $\pi_i((a_u)_{u\in Z(\delta)})$ qui vérifie $N.\widetilde{x} = (b_u)_{u\in Z(\delta_0)}$. Il existe λ_i tel que $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}) = \lambda_i\widetilde{x}$, et on a en utilisant le

lemme 4.5.3 et l'équation (6.4) : $(b_u)_{u\in Z(\delta_0)} = N.\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}) = \lambda_i^{N^2} N.\widetilde{x} = \lambda_i^{N^2}(b_u)_{u\in Z(\delta_0)}$, d'où $\lambda_i^{N^2} = 1$. Au final, on a un nombre fini de possibilités pour chaque $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)})$, et comme $(a_u)_{u\in Z(\delta)}$ est entièrement déterminé par les $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)})$, il n'y a qu'un nombre fini de points géométriques dans la variété $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$. ∎

Le reste de cette section est consacré à donner un critère pour reconnaître les points non dégénérés de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$. Déjà, il est clair que si $(a_u)_{u\in Z(\delta)}$ est un point géométrique de $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$ (donc est non dégénéré), alors $\pi_i((a_u)_{u\in Z(\delta)})$ est bien défini pour tout $i \in Z(\delta)$. On va montrer que la réciproque est vraie. Pour simplifier l'exposé, on se restreint au cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$. La stratégie est la suivante : soit $(a_u)_{u\in Z(\delta)}$ un point géométrique de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$ tel que $\pi_i((a_u)_{u\in Z(\delta)})$ soit bien défini pour tout $i \in Z(\overline{\ell n})$. Soit $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété abélienne marquée telle que $\pi_i(0_{A_k}) = \pi_i((a_u)_{u\in Z(\delta)})$ pour tout $i \in Z(\overline{\ell n})$ (on verra qu'une telle variété existe dans le théorème 6.2.7). Alors pour tout $i \in Z(\overline{\ell n})$, il existe $\lambda_i \in \overline{k}$ tel que $\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}) = \lambda_i \widetilde{\pi}_i(\widetilde{0}_{A_k})$. Premièrement, on va étudier les valeurs possibles des λ_i données par les relations de Riemann. Ensuite, on verra que toutes ces valeurs possibles sont obtenues en considérant l'action d'éléments de $\mathfrak{H}$ sur le thêta null point de $(A_k, \Theta_{\mathcal{L}}, \mathcal{L})$.

Lemme 6.3.4. *Avec les notations précédentes, soit $(e_1, \dots, e_g)$ une base de $Z(\overline{\ell n})$. Pour tout $m \in \mathbb{N}$ et $i \in Z(\overline{\ell n})$, on a $\lambda_{mi} = \lambda_i^{m^2}$ et $\lambda_{-m} = \lambda_m$. De plus, si $j \in Z(\overline{n}) \subset Z(\overline{\ell n})$, on a $\lambda_{i+j} = \lambda_i$.*
Pour tout $i, j, k \in Z(\overline{\ell n})$ on a :

$$\begin{aligned} \lambda_{i+j+k} &= \frac{\lambda_{i+j}\lambda_{i+k}\lambda_{j+k}}{\lambda_i\lambda_j\lambda_k} \\ \lambda_{i+j}\lambda_{i-j} &= \lambda_i^2\lambda_j^2 \end{aligned} \tag{6.5}$$

En combinant ces identités, il suffit de déterminer les λ_{e_i} et $\lambda_{e_i+e_j}$ pour $i, j \in [1..g]$. On a si $i, j \in [1..g]$:

$$\begin{aligned} \lambda_{e_i+e_j}^{\ell} &= \lambda_{e_i}^{\ell}\lambda_{e_j}^{\ell} \\ \lambda_{e_i}^{(2\wedge\ell)\ell} &= 1 \end{aligned} \tag{6.6}$$

Démonstration : On a $\lambda_0 = 1$ par définition des relevés affines canoniques. La relation $\lambda_{-i} = \lambda_i$ vient des relations de symétrie. Par définition de $\widetilde{\pi}_i$, on a trivialement $\lambda_{i+j} = \lambda_i$ si $j \in Z(\overline{n})$. Les formules d'addition (6.4) nous donnent $\lambda_{i+j}\lambda_{i-j} = \lambda_i^2\lambda_j^2$, on en déduit que $\lambda_{mi} = \lambda_i^{m^2}$ comme dans le lemme 4.5.3. Enfin, le reste de l'équation (6.5) vient en appliquant les relations de Riemann à $(i+j+k, i, j, k; 0, j+k, i+k, i+j)$ (on sait que ces relations donnent des équations non triviales via le théorème 4.4.4).

Si ℓ est impair, soit $\ell' \in \mathbb{N}$ tel que $\ell = 2\ell' + 1$. Si $i \in Z(\delta)$, on a $\lambda_{\ell' i} = \lambda_{-\ell' i} = \lambda_{[(n-1)\ell+\ell'+1]i} = \lambda_{(\ell'+1)i}$ puisque $(n-1)\ell i \in Z(\overline{n})$. Par le lemme 4.5.3, on obtient alors $\lambda_i^{\ell',2} = \lambda_i^{(\ell'+1)^2}$, soit $\lambda_i^{\ell} = 1$. Si ℓ est pair, on écrit $\ell = 2\ell'$, et en faisant le même raisonnement on obtient $\lambda_i^{(\ell'-1)^2} = \lambda_i^{(\ell'+1)^2}$, soit $\lambda_i^{2\ell} = 1$.

Enfin, si $i, j \in Z(\delta)$, on a $\lambda_{i+\ell j} = \lambda_i$ puisque $\ell j \in Z(\overline{n}) \subset Z(\overline{\ell n})$. Or le lemme 4.5.3 nous donne :

$$\lambda_{i+\ell j} = \frac{\lambda_{i+j}^{\ell}\lambda_j^{\ell(\ell-1)}}{\lambda_i^{\ell-1}}$$

Soit : $\lambda_{i+j}^{\ell} = \lambda_i^{\ell}\lambda_j^{\ell(1-\ell)} = \lambda_i^{\ell}\lambda_j^{\ell}$ comme $\lambda_j^{\ell^2} = 1$. ∎

Soit $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ une variété marquée $\hat{Z}(\overline{\ell})$-compatible avec $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$, de thêta null point $(a_u)_{u\in Z(\overline{\ell n})}$. On va s'intéresser aux automorphismes $\psi \in \mathfrak{H}$ qui vérifient de plus $\pi_i(\psi.(a_u)_{u\in Z(\overline{\ell n})}) = \pi_i((a_u)_{u\in Z(\overline{\ell n})})$ pour tout $i \in Z(\overline{\ell n})$. Soit $K = K_2(\mathcal{L})[\ell]$ le noyau de l'isogénie $\pi : A_k \to B_k$, et $\widetilde{K}$ son relevé canonique induit par la thêta structure. Si $\overline{\psi}$ est l'automorphisme symplectique de $K(\mathcal{L})$ induit par ψ, $\psi \in \mathfrak{H}$ si et seulement si $\psi(g)g^{-1} \in \widetilde{K}$ pour tout $g \in G(\mathcal{L})$ au-dessus d'un point de $\pi^{-1}(K(\mathcal{L}_0))$, et donc $\overline{\psi}(x) - x \in K$ pour tout $x \in \pi^{-1}(K(\mathcal{L}_0)) = K_1(\mathcal{L})[n] \oplus K_2(\mathcal{L})$. Pour que de plus $\pi_i(\psi.(a_u)_{u\in Z(\overline{\ell n})}) = \pi_i((a_u)_{u\in Z(\overline{\ell n})})$ pour tout $i \in Z(\overline{\ell n})$, il faut et il suffit que $\overline{\psi}(x) - x \in K$ pour tout $x \in K(\mathcal{L})$. Si on regarde la matrice de $\overline{\psi}$ dans la base symplectique canonique de $K(\mathcal{L})$ associée à la thêta structure $\Theta_{\mathcal{L}}$, on voit qu'elle est de la forme :

$$\overline{\psi} = \begin{pmatrix} \mathrm{Id} & 0 \\ C & \mathrm{Id} \end{pmatrix}$$

où C est une matrice symétrique à coefficients dans $Z(\overline{\ell})$.

Soit $\psi_0 : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell n})[\ell]$ un morphisme de groupe symétrique (c'est-à-dire que la matrice de ψ_0 dans la base canonique est symétrique), et $\overline{\psi}$ l'automorphisme symplectique de $K(\overline{\ell n})$ donné par $(i, j) \mapsto (i, \psi_0(i) + j)$. Soit ζ une racine primitive $2\ell n$-ième de l'unité, ζ^2 est une racine primitive ℓn-ième de l'unité donc induit un isomorphisme $f : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell n})$, de sorte que si $x, y \in Z(\overline{\ell n})$, on ait $\langle x, f(y)\rangle = \zeta^{2\sum_{i=1}^{g} x_i y_i}$. On définit alors $\frac{\langle x, f(y)\rangle}{2} \coloneqq \zeta^{\sum_{i=1}^{g} x_i y_i}$. Un relevé possible de $\overline{\psi}$ en un automorphisme ψ de $\mathcal{H}(\overline{\ell n})$ est alors donné par $\psi(\alpha, i, j) = (\alpha \frac{\langle i, \psi_0(i)\rangle}{2}, i, \psi_0(i) + j)$. On calcule alors si $i \in Z(\overline{\ell n})$:

$$\psi.\vartheta_i = \psi(1, i, 0).\vartheta_0 = (\frac{\langle i, \psi_0(i)\rangle}{2}, i, \psi_0(i)).\vartheta_0 = \frac{\langle i, \psi_0(i)\rangle}{2}\langle i, -\psi_0(i)\rangle\vartheta_i = \frac{\langle i, -\psi_0(i)\rangle}{2}\vartheta_i.$$

On en déduit :

Proposition 6.3.5. *Soit $\psi_0 : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell n})[\ell]$ un morphisme symétrique de groupe et ζ une racine primitive $2\ell n$-ième de l'unité. Soit ψ l'automorphisme du groupe de Heisenberg $\mathcal{H}(\overline{\ell n})$ donné par $\psi(\alpha, i, j) = (\alpha \frac{\langle i, \psi_0(i)\rangle}{2}, i, \psi_0(i) + j)$. Soit $(a_u)_{u\in Z(\delta)} \in \mathcal{M}_{\overline{\ell n}}$ un point géométrique, alors le point géométrique*

On note $(\cdot|\cdot)$ le produit scalaire canonique sur $Z(\overline{\ell n})$.

$$\psi.(a_u)_{u\in Z(\delta)} = (\zeta^{(i|-\psi_0(i))} a_i)_{i\in Z(\overline{\ell n})}$$

est dans $\mathcal{M}_{\overline{\ell n}}$.

De plus, si $(a_u)_{u\in Z(\delta)} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$, alors, quitte à composer ψ par un automorphisme $\mathtt{conj}_c$ où $c \in K(\overline{\ell n})[2]$, $\psi.(a_u)_{u\in Z(\delta)} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$. Enfin, si $(e_1, \ldots, e_g)$ est une base de $Z(\overline{\ell n})$, $\gamma_{e_i} \in Z((2 \wedge \ell)\ell))$ et $\gamma_{e_i+e_j} \in Z(\overline{\ell})$ pour $i, j \in [1..g]$, on peut toujours exhiber ψ_0 et $c \in K(\overline{\ell n})[2]$ tels que l'action de $\mathtt{conj}_c \circ \psi$ vérifie, si $(a'_i)_{i\in Z(\overline{\ell n})} = \mathtt{conj}_c \circ \psi.(a_u)_{u\in Z(\overline{\ell n})}$:

$$\widetilde{\pi}_{e_i}((a'_i)_{i\in Z(\overline{\ell n})}) = \zeta^{\gamma_{e_i}} \widetilde{\pi}_{e_i}((a_u)_{u\in Z(\overline{\ell n})})$$
$$\widetilde{\pi}_{e_i+e_j}((a'_i)_{i\in Z(\overline{\ell n})}) = \zeta^{\gamma_{e_i}+\gamma_{e_j}+\gamma_{e_i+e_j}} \widetilde{\pi}_{e_i+e_j}((a'_i)_{i\in Z(\overline{\ell n})})$$

Démonstration : Soit $(a_u)_{u\in Z(\delta)}$ un point géométrique dans $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$ correspondant à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$. Soit $(e'_1, \ldots, e'_g)$ la base duale de $(e_1, \ldots, e_g)$ dans $\hat{Z}(\overline{\ell n})$. Comme n est pair, on peut écrire $n = 2n'$, et on note $T_i \coloneqq \ell n' e'_i$ pour

$i \in [1..g]$. Le point T_i est un point de 2-torsion, et est dans le noyau K de l'isogénie duale $\widehat{\pi} : B_k \to A_k$ si ℓ est pair.

Soit $i \in [1..g]$, $\gamma_{e_i} \in \mathbb{N}$ et $\psi_0 : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell n})$ tel que $\psi_0(e_i) = n\gamma_{e_i} e_i'$ et $\psi_0(e_k) = 0$ si $k \neq i$. Alors $(\mathtt{conj}_{(2\wedge\gamma_i)T_i} \circ \psi).\vartheta_k = \zeta^{-n\gamma_{e_i}(e_i|k)}(-1)^{(2\wedge\gamma_i)(e_i|k)}$. Soit $(a_i')_{i\in Z(\overline{\ell n})} = (\mathtt{conj}_{(2\wedge\gamma_i)T_i} \circ \psi).(a_u)_{u\in Z(\overline{\ell n})}$, le choix de $\mathtt{conj}_{(2\wedge\gamma_i)T_i}$ est tel qu'on ait $\widetilde{\pi}_0((a_i')_{i\in Z(\overline{\ell n})}) = (b_u)_{u\in Z(\overline{n})}$, donc $(a_i')_{i\in Z(\overline{\ell n})}$ est dans $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$.

On a $\widetilde{\pi}_{e_i}((a_i')_{i\in Z(\overline{\ell n})}) = (-1)^{(2\wedge\gamma_i)}\zeta^{-n\gamma_{e_i}}\widetilde{\pi}_{e_i}((a_u)_{u\in Z(\overline{\ell n})})$. Si ℓ est impair, $(-1)^{(2\wedge\gamma_i)}\zeta^{-n\gamma_{e_i}}$ parcourt l'ensemble des racines ℓ-ièmes de l'unité quand γ_{e_i} parcourt $[1..\ell]$. Si ℓ est pair, $(-1)^{(2\wedge\gamma_i)}\zeta^{-n\gamma_{e_i}}$ parcourt la moitié des racines 2ℓ-ièmes de l'unité quand γ_{e_i} parcourt $[1..\ell]$. Cependant dans ce cas $T_i \in K$, donc $\mathtt{conj}_{T_i}.(a_i')_{i\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$. En faisant agir $\mathtt{conj}_{T_i}$ sur les points précédents, on retrouve le reste des racines 2ℓ-ièmes de l'unité.

Enfin, si $i, j \in [1..g]$ et $\gamma_{e_i+e_j} \in \mathbb{N}$, soit $\psi_0 : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell n})$ tel que $\psi_0(e_i) = n\gamma_{e_i+e_j}e_j'$, $\psi_0(e_j) = n\gamma_{e_i+e_j}e_i'$, et $\psi_0(e_k) = 0$ si $k \neq i, j$. Alors $\psi.\vartheta_k = \zeta^{-n\gamma_{e_i+e_j}2(e_i|k)(e_j|k)}$. Ainsi si $(a_i')_{i\in Z(\overline{\ell n})} = \psi.(a_u)_{u\in Z(\overline{\ell n})}$, le point géométrique $(a_i')_{i\in Z(\overline{\ell n})}$ est dans $\phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$, et $\widetilde{\pi}_{e_i+e_j}((a_i')_{i\in Z(\overline{\ell n})}) = \zeta^{-2n\gamma_{e_i+e_j}}\widetilde{\pi}_{e_i+e_j}((a_u)_{u\in Z(\overline{\ell n})})$, et $\zeta^{-2n\gamma_{e_i+e_j}}$ parcourt les racines ℓ-ièmes de l'unité lorsque $\gamma_{e_i+e_j}$ parcourt $[1..\ell]$.

Enfin, les morphismes symétriques $\psi_0 : Z(\overline{\ell n}) \to \hat{Z}(\overline{n})$ sont engendrés par les morphismes précédents, ce qui conclut la preuve. ∎

THÉORÈME 6.3.6. *Soit $(a_u)_{u\in Z(\overline{\ell n})}$ un point géométrique de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$. Alors $(a_u)_{u\in Z(\overline{\ell n})}$ est un point modulaire non dégénéré, ou autrement dit $(a_u)_{u\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$, si et seulement si le groupe $\{\pi_i((a_u)_{u\in Z(\overline{\ell n})}) \mid i \in Z(\overline{\ell n})$ et $\pi_i((a_u)_{u\in Z(\overline{\ell n})})$ est bien défini$\}$ est de cardinal $\#Z(\overline{\ell n})$.*

DÉMONSTRATION : Très clairement, si $(a_u)_{u\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_u)_{u\in Z(\delta_0)})$, les $\pi_i((a_u)_{u\in Z(\overline{\ell n})})$ sont bien définis, et on a vu qu'ils engendraient un sous-groupe isotrope maximal dans $K(\mathcal{L}_0^\ell)$.

Inversement, si $\mathcal{K} \coloneqq \{\pi_i((a_u)_{u\in Z(\overline{\ell n})}) \mid i \in Z(\overline{\ell n})$ et $\pi_i((a_u)_{u\in Z(\overline{\ell n})})$ est bien défini$\}$ est un sous-groupe de $K(\mathcal{L}_0^\ell)$, alors $\mathcal{K}$ est totalement isotrope. En effet, si on applique le théorème 5.4.1 pour calculer $e_{\mathcal{L}_0^\ell}(\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}), \widetilde{\pi}_j((a_u)_{u\in Z(\overline{\ell n})}))$, on remarque que

$$\mathtt{chain\_multadd}(\ell, \widetilde{\pi}_i((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_{i+j}((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_j((a_u)_{u\in Z(\delta)})) = \widetilde{\pi}_{\ell i+j}((a_u)_{u\in Z(\delta)})$$

par l'équation (6.4), ce qui donne $e_{\mathcal{L}_0^\ell}(\widetilde{\pi}_i((a_u)_{u\in Z(\delta)}), \widetilde{\pi}_j((a_u)_{u\in Z(\delta)})) = 1$.

Comme de plus $K_1(\mathcal{L}_0) \subset \mathcal{K}$ étant donné que $\pi((a_u)_{u\in Z(\overline{\ell n})}) = (b_u)_{u\in Z(\overline{n})}$, il existe donc une décomposition symplectique $K([\ell]^*\mathcal{L}_0) = K_1([\ell]^*\mathcal{L}_0) \oplus K_2([\ell]^*\mathcal{L}_0)$ avec $K_1([\ell]^*\mathcal{L}_0)[n\ell] = \mathcal{K}$ et $K_2(\mathcal{L}_0) \subset K_2([\ell]^*\mathcal{L}_0)$. Soit $K = \mathcal{K}[\ell]$, $A_k = B_k/K$ et $\widehat{\pi} : B_k \to A_k$ l'isogénie correspondante. Soit $\pi : A_k \to B_k$ l'isogénie contragrédiente de $\widehat{\pi}$, le noyau de π est $\widehat{\pi}(K_2([\ell]^*\mathcal{L}_0)[\ell])$. Soit $\mathcal{L} = \pi^*\mathcal{L}_0$, on se fixe la décomposition symplectique $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ donnée par $K_1(\mathcal{L}) = \pi(K_1([\ell]^*\mathcal{L}_0))$ et $K_2(\mathcal{L}) = \pi(K_2([\ell]^*\mathcal{L}_0)[n\ell]$, on a donc $\pi(K_1(\mathcal{L})) = \mathcal{K}$. On se fixe de plus un isomorphisme $\phi : Z(\overline{\ell n}) \to K_1(\mathcal{L})$ tel que $\pi(\phi(i)) = \pi_i((a_u)_{u\in Z(\delta)})$ pour tout $i \in Z(\overline{\ell n})$. Soit $\Theta_{\mathcal{L}}$ une thêta structure symétrique au-dessus de la décomposition de $K(\mathcal{L})$, compatible avec la numérotation ϕ et compatible avec $\Theta_{\mathcal{L}_0}$ (il suffit de prendre une thêta structure symétrique compatible avec la décomposition de $K(\mathcal{L})$ et de renuméroter les éléments de $K_1(\mathcal{L})$ pour que la numérotation soit donnée par ϕ).

Si $(a_i')_{i\in Z(\overline{\ell n})}$ est le thêta null point de la variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$, la construction précédente est telle que $\pi_i((a_i')_{i\in Z(\overline{\ell n})}) = \pi_i((b_u)_{u\in Z(\overline{n})})$ pour tout $i \in Z(\overline{\ell n})$. En combinant le lemme 4.5.3 et la proposition 6.3.5, on voit que $(a_u)_{u\in Z(\overline{\ell n})}$ et $(a_i')_{i\in Z(\overline{\ell n})}$ diffèrent

d'un automorphisme $\psi \in \mathfrak{H}$, ce qui montre que $(a_u)_{u\in Z(\overline{\ell n})}$ est bien un thêta null point non dégénéré. ■

6.4 DEGRÉ DES FIBRES

La variété $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est un schéma affine, dont on peut décrire l'idéal ainsi : soit I l'idéal homogène de $\overline{\mathcal{M}}_\delta$ dans $k[x_i \mid i \in Z(\delta)]$ donné par les relations de Riemann et de symétrie (voir le théorème 4.7.2). Soit $i_0 \in Z(\delta_0)$ tel que $b_{i_0} \neq 0$, et $\phi : k[x_i \mid i \in Z(\delta)] \to k[x_i \mid i \in Z(\delta), i \neq i_0]$ le morphisme donné par

$$x_i \mapsto \begin{cases} \dfrac{b_i}{b_{i_0}} & \text{si } i \in Z(\delta_0) \\ x_i & \text{sinon} \end{cases}$$

alors $\phi(I)$ est l'idéal définissant le schéma $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$.

Nous ne nous étendrons pas sur les détails d'implémentation de la génération de ces équations : il suffit de faire attention à utiliser toute la symétrie des relations de Riemann et de ne pas générer de relations triviales afin d'éviter d'obtenir des relations redondantes.

Le but de cette section est d'étudier le degré de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$, ce qui est important pour estimer le temps mis pour trouver un point solution $(a_u)_{u\in Z(\delta)} \in \overline{\phi}_1^{-1}((b_u)_{u\in Z(\delta_0)})$ via une base de Gröbner. On se restreint ici au cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$, avec ℓ impair. On verra que même dans ce cas, le degré de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est trop grand, ce qui nous conduit à user d'autres stratégies qu'employer une base de Gröbner pour trouver un point solution dans la section 7.3. (Dans [FLR09], on présente un algorithme de base de Gröbner modifié pour prendre en compte du fait qu'un point modulaire solution $(a_u)_{u\in Z(\overline{\ell n})}$ a la propriété qu'un sous-ensemble de ses coordonnées (les $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})})$) satisfont des relations de petit degré. Cet algorithme est bien mieux adapté au système considéré, mais est bien entendu moins efficace que l'algorithme 7.3.2 qui travaille directement sur les $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})})$ sans passer par une base de Gröbner).

On va procéder en trois étapes. Premièrement, on montre que $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est réduite, donc est une variété, et son degré est donné par le cardinal de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})(\overline{k})$. Ensuite, on sait que $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})(\overline{k})/\mathfrak{H}$ est l'espace des ℓ-isogénies de noyaux isotropes sur B_k pour $e_{\mathcal{L}_0^\ell}$; on peut donc calculer le cardinal de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})(\overline{k})$ si on connait celui de $\mathfrak{H}$. Enfin on étudie comment apparaissent les points de torsions dégénérés.

PROPOSITION 6.4.1. *La variété affine $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est réduite.*

DÉMONSTRATION : Soit $(a_u)_{u\in Z(\overline{\ell n})}$ un point géométrique de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$. On va montrer que $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}) \in \mathbb{A}_k^{Z(\overline{n})}(\overline{k})$ est un point réduit, ce qui montrera que $(a_u)_{u\in Z(\overline{\ell n})}$ est un point réduit de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$.

Si $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})})$ n'est pas le point d'origine $(0,\dots,0)$, alors on sait que sa projection $\pi_i((a_u)_{u\in Z(\overline{\ell n})})$ est un point de ℓ-torsion de B_k par la proposition 6.3.2. Si L est la droite reliant le point d'origine à $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})})$, le lemme 6.3.4 nous dit que l'intersection de $\widetilde{\pi}_i(\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})}))$ avec L est isomorphe au schéma $\mathrm{Spec}(k[x]/(x^\ell - 1))$. Comme ℓ est

premier à la caractéristique de k, ce schéma est réduit, ce qui implique que $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})})$ est réduit dans $\mathbb{A}_k^{Z(\overline{n})}$.

Le cas $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}) = (0,\dots,0)$ (ce qui implique que $(a_u)_{u\in Z(\overline{\ell n})}$ soit dégénéré) est plus intéressant. Soit $\mathfrak{P}$ l'idéal maximal correspondant à $(0,\dots,0)$ et J l'idéal correspondant à $\widetilde{\pi}_i(\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})}))$ localisé en $\mathfrak{P}$. Soit r_i le plus petit entier tel que $\mathfrak{P}^{r_i}\subset J$. On veut prouver que $r_i = 1$. Supposons que ce ne soit pas le cas, et soit $r_i' \geqslant r_i$ le plus petit entier plus grand que r_i et divisible par 4.

Si on utilise le changement de variable $U^{\mathcal{L}}$ de la section 4.3, comme $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est une sous-variété de $\mathcal{M}_{\overline{\ell n}}$, les coordonnées $U^{\mathcal{L}}$ satisfont les relations de Riemann et on trouve (voir l'équation (4.13)) :

$$U_i^{\mathcal{L}}U_j^{\mathcal{L}}U_k^{\mathcal{L}}U_l^{\mathcal{L}} = \frac{1}{2^{2g}}\sum_{\substack{\xi\in\hat{Z}(\overline{2})\times Z(\delta)\\ 2\xi\in Z(\overline{2})\times 0}}(m_2+\xi_2)(2\xi_1)U^{\mathcal{L}}_{i-m+\xi}U^{\mathcal{L}}_{m-j+\xi}U^{\mathcal{L}}_{m-k+\xi}U^{\mathcal{L}}_{m-l+\xi}. \tag{6.7}$$

Soit M un monôme de degré $r_i'/4$ en les $U_j^{\mathcal{L}}$, où j est dans $\hat{Z}(\overline{2})\times(2i+Z(\overline{n}))$. Alors, quitte à multiplier M par des éléments dans $U_l^{\mathcal{L}}$, où $l\in\hat{Z}(\overline{2})\times Z(\overline{n})$, on peut appliquer l'équation (6.7). De plus, $U_l^{\mathcal{L}} = U_l^{\mathcal{L}_0}((b_u)_{u\in Z(\overline{n})})$ si $l\in\hat{Z}(\overline{2})\times Z(\overline{n})$ car les $U^{\mathcal{L}}$ sont des coordonnées de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$, donc changer M comme précédemment revient à le multiplier par une constante dans $\overline{k}$, que l'on peut supposer non nulle par le théorème 4.4.4 (voir aussi la remarque 4.4.8). L'équation (6.7) montre alors (en utilisant de plus les relations de symétrie $U_j^{\mathcal{L}} = U_{-j}^{\mathcal{L}}$ si $j\in\hat{Z}(\overline{2})\times Z(\overline{\ell n})$) que M est égal à un produit M' de $r_i'/4$ polynômes de degré 4 en les $U_j^{\mathcal{L}}$ où j est dans $\hat{Z}(\overline{2})\times(i+Z(\overline{n}))$. Ainsi $M'\in\mathfrak{P}^{r_i'}\subset J$. Comme ceci est valable pour tout tel monôme M, on en déduit que $r_{2i}\leqslant r_i'/4$. Si n_0 est le plus petit entier tel que $2^{n_0}i - i\in Z(\overline{n})$, on obtient $r_i = r_{2^{n_0}i} < r_i$, ce qui nous donne la contradiction recherchée. ■

On s'intéresse maintenant au calcul du cardinal de $\mathfrak{H}$, ou plus exactement à la description de l'action de $\mathfrak{H}$ sur $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$:

Proposition 6.4.2. *L'action de $\mathfrak{H}$ sur $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est engendrée par les deux actions suivantes :*

1. *Une action de « permutation » :*

$$(a_u)_{u\in Z(\overline{\ell n})}\mapsto(a_{\psi(i)})_{i\in Z(\overline{\ell n})} \tag{6.8}$$

où l'automorphisme $\psi : Z(\overline{\ell n})\to Z(\overline{\ell n})$ fixe $Z(\overline{n})$.
Si ℓ est premier à n, $Z(\overline{\ell n})\simeq Z(\overline{n})\times Z(\overline{\ell})$ et ψ provient d'un automorphisme $\psi_1 : Z(\overline{\ell})\to Z(\overline{\ell})$. De plus, $(a_u)_{u\in Z(\overline{\ell n})}$ est entièrement déterminé par les $(\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}))_{i\in Z(\overline{\ell})}$ (voir la proposition 4.6.2), et dans ce cas cette action s'écrit plus simplement

$$(\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}))_{i\in Z(\overline{\ell})}\mapsto(\widetilde{\pi}_{\psi_1(i)}((a_u)_{u\in Z(\overline{\ell n})}))_{i\in Z(\overline{\ell})}.$$

2. *L'autre action est une action « diagonale » :*

$$(a_u)_{u\in Z(\overline{\ell n})}\mapsto(e_{\overline{\ell n}}(\psi(i),i)a_i)_{i\in Z(\overline{\ell n})} \tag{6.9}$$

où ψ est un morphisme symétrique $Z(\overline{\ell n})\to\hat{Z}(\overline{\ell})$. (Si ℓ est premier à n, ψ provient d'un morphisme symétrique $\psi_2 : Z(\overline{\ell})\to\hat{Z}(\overline{\ell})$.)

On peut voir cette action comme donnée si $(m_1, \dots, m_g) \in Z(\overline{\ell n})$ *par*

$$\widetilde{\pi}_{(m_1,\dots,m_g)}((a_u)_{u\in Z(\overline{\ell n})}) \mapsto \zeta^{\sum_{i,j\in[1..g]} c_{i,j}m_i m_j}\widetilde{\pi}_{(m_1,\dots,m_g)}((a_u)_{u\in Z(\overline{\ell n})})$$

où ζ *est une racine* ℓ*-ième de l'unité et* $(c_{i,j})_{i,j\in[1..g]} \in \mathrm{M}_g(Z(\overline{\ell}))$ *sont les coefficients de la matrice associée à* ψ*.*

Démonstration : Comme ℓ est impair, si $\psi \in \mathfrak{H}$ et $\overline{\psi}$ est l'automorphisme symplectique de $K(\overline{\ell n})$ induit par ψ, ψ est l'unique automorphisme de $\mathfrak{H}$ au-dessus de $\overline{\psi}$ comme $\hat{Z}(\overline{\ell}) \cap K(\overline{\ell n})[2] = \varnothing$. La matrice de $\overline{\psi}$ dans la base canonique de $K(\overline{\ell n})$ (donnée par le choix d'une racine ℓn-ième de l'unité) est

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

De plus, comme $\psi \in \mathfrak{H}$, on a $\overline{\psi}(i) - i \in \hat{Z}(\overline{\ell})$ lorsque $i \in Z(\overline{n}) \times \hat{Z}(\overline{\ell n})$, ce qui impose $B = 0$. De tels automorphismes symplectiques sont engendrés par les matrices de la forme $\begin{pmatrix} \mathrm{Id} & 0 \\ C & \mathrm{Id} \end{pmatrix}$, avec C symétrique à valeurs dans $Z(\overline{\ell})$, que l'on a déjà traité dans la proposition 6.3.5 et qui donnent l'action 6.9 ; et des matrices de la forme $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ où A fixe $Z(\overline{n})$. On vérifie facilement que $\psi(\alpha, i, j) = (\alpha, \overline{\psi}(i), \overline{\psi}(j))$ est un relevé symétrique de $\overline{\psi}$ qui est dans $\mathfrak{H}$. On obtient alors l'action 6.8. ■

Remarque 6.4.3. Géométriquement, les actions 6.8 et 6.9 sont très différentes. Supposons n premier avec ℓ pour simplifier la discussion. Soit $\mathfrak{H}_1$ le groupe des automorphismes symplectiques de $K(\overline{\ell})$ provenant d'un automorphisme de $Z(\overline{\ell})$, et $\mathfrak{H}_2$ celui des automorphismes symplectiques de $K(\overline{\ell})$ provenant d'un morphisme $Z(\overline{\ell}) \to \hat{Z}(\overline{\ell})$. Le groupe $\mathfrak{H}_1$ agit sur $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ par l'action 6.8, tandis que $\mathfrak{H}_2$ par l'action 6.9.

On a alors la situation suivante : choisir un point géométrique de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ revient à choisir un sous-groupe isotrope maximal K de $B_k[\ell]$ et, si $A_k = B_k/K$ et $\widehat{\pi} : B_k \to A_k$ est l'isogénie associée, un supplémentaire $\mathfrak{K}$ de $\widehat{\pi}(B_k[\ell])$ dans $A_k[\ell]$ tel que $\pi(\mathfrak{K}[n]) = K_1(\mathcal{L}_0)$ par le corollaire 6.2.8, ainsi qu'une numérotation de $\mathfrak{K}$. L'action de $\mathfrak{H}_1$ revient juste à changer la numérotation de $\mathfrak{K}$, tandis que l'action de $\mathfrak{H}_2$ revient à additionner à $\mathfrak{K}$ des éléments de $\widehat{\pi}(B_k[\ell])$ pour obtenir un nouveau supplémentaire. Si $(a_u)_{u\in Z(\overline{\ell n})} \in Z(\overline{\ell n})$ est le point géométrique de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ associé à $\mathfrak{K}$, soit $(c_u)_{u\in Z(\overline{n})} = \widetilde{\pi}_2((a_u)_{u\in Z(\overline{\ell n})})$. Si C_k est la variété abélienne correspondant à $(c_u)_{u\in Z(\overline{n})}$, alors $C_k = A_k/\mathfrak{K}$ et la figure 7.1 montre que $\pi_2 \circ \widehat{\pi}_1$ est une ℓ^2-isogénie. Les éléments de $\mathfrak{H}_1$ laissent invariants $(c_u)_{u\in Z(\overline{n})}$, tandis qu'aucun élément de $\mathfrak{H}_2$ ne stabilise $(c_u)_{u\in Z(\overline{n})}$. On montrera à la proposition 7.7.1 qu'il y a bijection entre l'orbite de $(c_u)_{u\in Z(\overline{n})}$ et les ℓ^2-isogénies de source B_k dont le noyau contient $\mathrm{Ker}\,\widehat{\pi}_1$.

Ainsi, choisir un point géométrique de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})/\mathfrak{H}_1$ revient à choisir un sous-groupe isotrope maximal de $B_k[\ell^2]$, et donc une ℓ^2-isogénie $B_k \to C_k$ par ce qui précède. Enfin, choisir un point géométrique de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})/\mathfrak{H}$ revient à choisir un sous-groupe isotrope maximal K de $B_k[\ell]$. ◇

Il nous reste à étudier les points dégénérés. Si $(a_u)_{u\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est un point géométrique non dégénéré, il existe deux manières de construire un point dégénéré à partir de $(a_u)_{u\in Z(\overline{\ell n})}$. Soit $S \subset Z(\overline{\ell n})$ un sous-groupe contenant $Z(\overline{n})$, on définit un nouveau point $(a'_i)_{i\in Z(\overline{\ell n})}$ par si $i \in Z(\overline{\ell n})$:

$$a'_i = \begin{cases} a_i & \text{si } i \in S \\ 0 & \text{sinon.} \end{cases}$$

On vérifie immédiatement que $(a'_i)_{i\in Z(\overline{\ell n})}$ vérifie les relations de Riemann, donc $(a'_i)_{i\in Z(\overline{\ell n})}$ est un point dégénéré (car si $i \notin S$, $\widetilde{\pi}_i((a'_i)_{i\in Z(\overline{\ell n})}) = (0,\dots,0)$) dans $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$. Une autre méthode consiste à prendre un morphisme $\psi : Z(\overline{\ell n}) \to Z(\overline{\ell n})$ fixant $Z(\overline{n})$, et de considérer le point $(a'_i)_{i\in Z(\overline{\ell n})}$ donné par, si $i \in Z(\overline{\ell n})$, $a'_i = a_{\psi(i)}$. Si ψ est inversible, on retrouve l'action 6.8. Dans le cas général, on vérifie facilement que $(a'_i)_{i\in Z(\overline{\ell n})}$ vérifie toujours les relations de Riemann (car ψ fixe $Z(\overline{n})$, donc la 2-torsion comme $2 \mid n$), et donc $(a'_i)_{i\in Z(\overline{\ell n})}$ est un point dégénéré (car si $\psi(i) = \psi(j)$, $\pi_i((a'_i)_{i\in Z(\overline{\ell n})}) = \pi_j((a'_i)_{i\in Z(\overline{\ell n})})$) de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$.

Or tous les points dégénérés de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ s'obtiennent ainsi : si le point géométrique $(a'_i)_{i\in Z(\overline{\ell n})} \in \overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est dégénéré, soit

$$S \coloneqq \{i \in Z(\overline{\ell n}) \mid \pi_i((a_u)_{u\in Z(\overline{\ell n})}) \text{ est bien défini}\}$$

le sous-groupe de la proposition 6.3.2. La preuve de la proposition 6.3.2 montre que l'application $\psi : i \in S \mapsto \pi_i((a'_i)_{i\in Z(\overline{\ell n})})$ est un morphisme de groupe (qui n'est pas forcément un isomorphisme comme les $\pi_i((a'_i)_{i\in Z(\overline{\ell n})})$ pour $i \in S$ ne sont pas forcément distincts). Le sous-groupe $\psi(S)$ de $B_k[\ell n]$ est totalement isotrope pour $e_{\mathcal{L}_0^\ell}$. En effet, on peut appliquer le même raisonnement que pour le théorème 6.3.6. Si $\mathcal{K}$ est un groupe isotrope maximal de $B_k[\ell n]$ pour $e_{\mathcal{L}_0^\ell}$ qui contient $\psi(S)$, soit $\psi_0 : Z(\overline{\ell n}) \to \mathcal{K}$ un isomorphisme. Le théorème 6.3.6 nous donne un point géométrique non dégénéré $(a_u)_{u\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ tel que $\pi_i((a_u)_{u\in Z(\overline{\ell n})}) = \psi_0(i)$. Soit $\psi_1 : Z(\overline{\ell n}) \to Z(\overline{\ell n})$ donné par la composée $\psi_1 = \psi_0^{-1} \circ \psi$. Soit $(a''_i)_{i\in Z(\overline{\ell n})}$ donné par si $i \in Z(\overline{\ell n})$:

$$a''_i = \begin{cases} a_{\psi_1}(i) & \text{si } i \in S \\ 0 & \text{sinon.} \end{cases}$$

Alors par construction, si $i \in S$, $\pi_i((a''_i)_{i\in Z(\overline{\ell n})}) = \pi_i((a'_i)_{i\in Z(\overline{\ell n})})$, et si $i \notin S$, $\widetilde{\pi}_i(a''_i)_{i\in Z(\overline{\ell n})}) = \widetilde{\pi}_i((a'_i)_{i\in Z(\overline{\ell n})}) = (0,\dots,0)$. Mais là encore, on voit comme dans la preuve du théorème 6.3.6 qu'en combinant le lemme 4.5.3 et la proposition 6.3.5, quitte à agir sur $(a''_i)_{i\in Z(\overline{\ell n})}$ par une action « diagonale » (6.9), on a $(a''_i)_{i\in Z(\overline{\ell n})} = (a'_i)_{i\in Z(\overline{\ell n})}$.

On remarque que les points dégénérés sont exactement là où l'action de $\mathfrak{H}$ n'est pas libre. Par exemple, si $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}) = (0,\dots,0)$, alors un sous-groupe de l'action 6.9 agit trivialement sur $(a_u)_{u\in Z(\overline{\ell n})}$, tandis que si $\pi_i((a_u)_{u\in Z(\overline{\ell n})}) = \pi_j((a_u)_{u\in Z(\overline{\ell n})})$ pour $i \neq j$, alors il existe une action « de permutation » (6.8) ψ_1 telle que $\pi_i((a_u)_{u\in Z(\overline{\ell n})}) = \pi_i(\psi_1.(a_u)_{u\in Z(\overline{\ell n})})$ pour tout $i \in Z(\overline{\ell n})$, et en corrigeant par une action « diagonale » ψ_2 on a $\widetilde{\pi}_i((a_u)_{u\in Z(\overline{\ell n})}) = \widetilde{\pi}_i((\psi_2 \circ \psi_1).(a_u)_{u\in Z(\overline{\ell n})})$.

Exemple 6.4.4 (Solutions modulaires en genre 1). Soit $g = 1$, $n = 4$ et $\ell = 3$. Si

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) \in \phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$$

est un point géométrique solution correspondant à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$, les autres points géométriques de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ donnant la même variété polarisée $(A_k, \mathcal{L})$ sont

$$(a_0, \zeta a_1, \zeta^{2^2} a_2, a_3, \zeta a_4, \zeta^{2^2} a_5, a_6, \zeta a_7, \zeta^{2^2} a_8, a_9, \zeta a_{10}, \zeta^{2^2} a_{11})$$
$$(a_0, \zeta a_5, \zeta^{2^2} a_{10}, a_3, \zeta a_8, \zeta^{2^2} a_1, a_6, \zeta a_{11}, \zeta^{2^2} a_4, a_9, \zeta a_2, \zeta^{2^2} a_7)$$

où ζ est une racine 3-ième de l'unité.

Les points dégénérés de $\overline{\phi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$ sont donnés par

$$(a_0, \zeta a_9, \zeta^{2^2} a_6, a_3, \zeta a_0, \zeta^{2^2} a_9, a_6, \zeta a_3, \zeta^{2^2} a_0, a_9, \zeta a_6, \zeta^{2^2} a_3)$$
$$(a_0, 0, 0, a_3, 0, 0, a_6, 0, 0, a_9, 0, 0)$$

Ainsi par exemple si $k = \mathbb{F}_{79}$, et E_k est la courbe elliptique donnée par l'équation de Weierstrass $y^2 = x^3 + 11.x + 47$, les formules de Thomae donnent un théta null point de niveau 4 associé à E_k : $(b_u)_{u\in Z(\overline{n})} = (1 : 1 : 12 : 1)$. Les quatre sous-groupes de rang 1 de 3-torsion de E_k (qui sont forcément isotropes) sont donnés par :

$$K_1 = \{(1 : 1 : 12 : 1), (37 : 54 : 46 : 1), (8 : 60 : 74 : 1)\}$$
$$K_2 = \{(1 : 1 : 12 : 1), (67 : 10 : 68 : 1), (62 : 8 : 70 : 1)\}$$
$$K_3 = \{(1 : 1 : 12 : 1), (42 : 5 : 15 : 1), (40 : 16 : 3 : 1)\}$$
$$K_4 = \{(1 : 1 : 12 : 1), (72 : 56 : 31 : 1), (69 : 24 : 33 : 1)\}$$

Tous les points géométriques de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ sont définis sur $\mathbb{F}_{79}(v)$ où v est une racine (primitive) du polynôme irréductible $X^3 + 9.X + 76$. Pour chacun des 4 sous-groupes K_i, il y a 6 points géométriques de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ correspondant à la courbe elliptique E/K_i par ce qui précède. On donne un représentant de chaque classe :

$Q_1 = (16v^2 + 19v + 17 : 1 : 46 : 16v^2 + 19v + 17 : 37 : 54 : 34v^2 + 70v + 46 : 54 : 37 : 16v^2 + 19v + 17 : 46 : 1)$ correspond à K_1.

$Q_2 = (64v^2 + 67v + 68 : 1 : 68 : 64v^2 + 67v + 68 : 67 : 10 : 57v^2 + 14v + 26 : 10 : 67 : 64v^2 + 67v + 68 : 68 : 1)$ correspond à K_2.

$Q_3 = (8v^2+49v+48 : 1 : 3 : 8v^2+49v+48 : 40 : 16 : 17v^2+35v+23 : 16 : 40 : 8v^2+49v+48 : 3 : 1)$ correspond à K_3.

$Q_4 = (32v^2 + 73v + 34 : 1 : 33 : 32v^2 + 73v + 34 : 69 : 24 : 68v^2 + 7v + 13 : 24 : 69 : 32v^2 + 73v + 34 : 33 : 1)$ correspond à K_4.

Les points dégénérés de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ sont $\{(55 : 1 : 12 : 55 : 1 : 1 : 28 : 1 : 1 : 55 : 12 : 1), (1 : 1 : 12 : 1 : 1 : 1 : 12 : 1 : 1 : 1 : 12 : 1), (23 : 1 : 12 : 23 : 1 : 1 : 39 : 1 : 1 : 23 : 12 : 1)\}$ dont les projections π_i pour $i \in Z(\overline{\ell})$ sont le point neutre : $\{(1 : 1 : 12 : 1), (1 : 1 : 12 : 1), (1 : 1 : 12 : 1)\}$. Pour ces points, l'action 6.8 est triviale, ce qui explique qu'il y ait seulement 3 points dans cette classe (des orbites sous $\mathfrak{H}$). Enfin on a un dernier point dégénéré donné par $(1 : 0 : 0 : 1 : 0 : 0 : 12 : 0 : 0 : 1 : 0 : 0)$, sur lequel l'action de $\mathfrak{H}$ est triviale. ◇

Exemple 6.4.5. Si $g = 2$, et ℓ est un nombre premier qui ne divise pas n, on peut calculer le cardinal de $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})(\overline{k})$ ainsi : le nombre de classes sous l'action de $\mathfrak{H}$ est égal par le théorème 6.2.7 au nombre de points géométriques de la grassmannienne $\mathrm{Gr}(2, 4)(\mathbb{F}_\ell)$ correspondant à des plans isotropes. Il y en a $(\ell^2 + 1)(\ell + 1)$. Le nombre d'actions de la forme (6.8) est donné par le nombre de matrices inversibles de dimension 2 à coefficients dans $\mathbb{F}_\ell$, soit par $(\ell^2 - 1)(\ell^2 - \ell)$. Enfin le nombre d'actions de la forme (6.9) est donné par le nombre de matrices de dimension 2 symétriques à coefficients dans $\mathbb{F}_\ell$, soit par ℓ^3. Au total, on a

$$\ell^{10} - \ell^8 - \ell^6 + \ell^4$$

théta null points valides dans $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})(\overline{k})$. Par exemple, si $\ell = 3$, on trouve 51840 théta null points valides, à comparer aux 40 $(3, 3)$isogénies de noyau isotropes possibles. Le cardinal de $\mathfrak{H}$ est 1296.

Plus généralement, si $g \in \mathbb{N}$, et ℓ est toujours un nombre premier ne divisant pas n, le nombre de points géométriques de $\mathrm{Gr}(g, 2g)(\mathbb{F}_\ell)$ correspondant à des espaces isotropes est $O(\ell^{g(g+1)/2})$ (lorsque $\ell \to \infty$, en raisonnant à g fixé), tandis que le nombre d'actions de

type (6.8) $O(\ell^{g^2})$, et le nombre d'actions de type (6.9) un $O(\ell^{g(g+1)/2})$. Au total, le nombre de points géométriques dans $\phi_1^{-1}((b_u)_{u\in Z(\overline{n})})$ est un $O(\ell^{2g^2+g})$. On voit ici l'inconvénient de considérer la correspondance modulaire $\Phi : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$: en ajoutant de la structure, on arrive aisément à donner des équations pour cette correspondance, mais de ce fait de nombreux points solutions correspondent à la même isogénie. Si l'on compare le nombre de points solutions au nombre ℓ^{2g} de points (géométriques) de ℓ-torsion dans B_k, on voit tout l'intérêt de trouver un algorithme qui permettrait d'exhiber un point solution étant donné les points d'un groupe isotrope de $B_k[\ell]$. C'est l'objet de la section 7.3. ◊

7 CALCUL D'ISOGÉNIES

MATIÈRES

7.1 INTRODUCTION

Le but de ce chapitre est le calcul explicite d'isogénies (séparables) entre variétés abéliennes. Le calcul effectif d'isogénies se décompose en plusieurs problèmes algorithmiques suivant les entrées et sorties attendues :

- Étant donnés une variété abélienne A_k sur un corps k, et un groupe abélien fini abstrait K, calculer toutes les isogénies $A_k \to B_k$ dont le noyau est isomorphe à K, et donner des expressions rationnelles pour les isogénies correspondantes.
- Étant donnés une variété abélienne A_k et un sous-groupe fini K de A_k, déterminer le quotient $B_k = A_k/K$ ainsi que l'expression rationnelle de l'isogénie $A_k \to B_k$.
- Étant données deux variétés abéliennes isogènes, A_k et B_k, calculer l'expression rationnelle de l'isogénie $A_k \to B_k$.

Dans ce chapitre, nous nous consacrons à l'étude des deux premiers problèmes. Si A_k est une courbe elliptique, on connaît des algorithmes efficaces pour résoudre chacun de ces trois problèmes [Ler97], basés essentiellement sur la formule de Vélu [Vel71].

En dimension supérieure, jusqu'aux résultats de [LR10a], on avait beaucoup moins d'outils à disposition. Les formules de Richelot [Ric36 ; Ric37] permettent de calculer des $(2, 2)$-isogénies entre des variétés abéliennes de dimension 2. Plus récemment, [Smi09] a donné une méthode pour calculer des $(2, 2, 2)$ isogénies sur des Jacobiennes de courbes hyperelliptiques de genre 3. Dans ce chapitre, nous donnons un algorithme pour le calcul (entre autres) de ℓ-isogénies entre variétés abéliennes de dimension g sur un corps k de caractéristique p différente de 2, avec ℓ premier à p.

Le théorème de l'isogénie (théorème 3.6.4) permet de décrire des isogénies explicitement, mais a l'inconvénient de prendre en entrée un thêta null point de niveau supérieur au degré de l'isogénie à calculer (autrement dit le théorème de l'isogénie ne permet que de descendre de niveau). Or quand on manipule des variétés abéliennes via les coordonnées thêta, on préfère les

prendre de niveau minimum pour réduire le nombre de coordonnées et le prix des additions, donc prendre du niveau 4, voire 2 s'il est possible de travailler sur la variété de Kummer. De plus, si la variété abélienne est donnée comme la Jacobienne d'une courbe hyperelliptique, les formules de Thomae ne permettent de retrouver les thêta constantes qu'en niveau 4 (ou 2). Le théorème de l'isogénie est alors inutilisable dans ces cas-là.

Soit $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ une variété marquée de niveau n, n étant pair. Si $\ell \in \mathbb{N}$, on a vu dans le chapitre 6 une correspondance modulaire qui induisait un morphisme $\phi_1 : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}}$. Si $(b_i)_{i\in Z(\delta_0)}$ est le thêta null point de B_k par rapport à la thêta structure $\Theta_{\mathcal{L}_0}$, tout thêta null point $(a_i)_{i\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_i)_{i\in Z(\overline{n})})$ correspond à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ ℓ-isogène à B_k. De plus, le théorème de l'isogénie nous donne explicitement l'isogénie correspondante (de type $\hat{Z}(\overline{\ell})$) $\pi_1 : A_k \to B_k$, ainsi qu'une isogénie de type $Z(\overline{\ell})$ $\pi_2 : A_k \to C_k$, où C_k est une variété abélienne marquée de niveau n. Enfin, si $\widehat{\pi}_1$ est l'isogénie contragrédiente de π_1, on a vu dans la section 6.2 que l'on avait le diagramme donné par la figure 7.1 où $\pi_2 \circ \widehat{\pi}_1$ est une ℓ^2-isogénie.

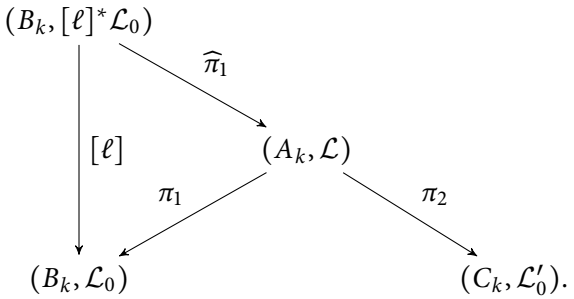


FIGURE 7.1 – Le diagramme d'isogénie associé à la correspondance modulaire

Plus généralement, si $\delta = \delta_0\delta'$, alors la figure 7.1 associée à la correspondance modulaire $\phi : \mathcal{M}_\delta \to \mathcal{M}_{\delta_0}$ de la section 6.2 donne lieu aux isogénies suivantes : π_1 est une $\hat{Z}(\delta)$ isogénie, π_2 une $Z(\delta)$ isogénie, et donc l'isogénie contragrédiente $\widehat{\pi}_1$ est une $(\ell, \dots, \ell, \ell/\delta_1, \dots, \ell/\delta_g)$ isogénie, et $\pi_2 \circ \widehat{\pi}_1$ une $(\ell\delta_1, \dots, \ell\delta_g, \ell/\delta_1, \dots, \ell/\delta_g)$-isogénie. Tous les algorithmes de ce chapitre s'étendent trivialement à ce cas-là (en utilisant les résultats du chapitre 6), cependant l'isogénie de type $\widehat{\pi}_1$ n'étant pas très intéressante en pratique (d'ailleurs une telle isogénie est rarement rationnelle), on se concentre sur le cas $\delta = \overline{\ell n}$ et $\delta_0 = \overline{n}$. Nous suivons essentiellement le plan de l'article [LR10a], en rajoutant des exemples et en détaillant un peu certaines situations (voir la remarque 7.2.6 et la proposition 7.7.1).

Dans la section 7.2, nous expliquons comment calculer explicitement $\widehat{\pi}_1$ (autrement dit comment monter de niveau) uniquement avec les formules d'addition du chapitre 4 sur B_k, à partir de la connaissance de $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$. Dans la section 7.3, nous expliquons comment calculer $(a_i)_{i\in Z(\delta)}$ à partir du noyau de $\widehat{\pi}_1$ (lorsque ℓ est premier à n), là encore uniquement avec les formules d'addition dans B_k (et des calculs de racines ℓ-ièmes). On a donc un équivalent des formules de Vélu en dimension supérieure. Pour cela on a besoin de la notion d'excellent point de ℓ-torsion, notion qui est étudiée à la section 7.4. On utilise les résultats de cette section pour expliquer comment minimiser les calculs de racines ℓ-ième lorsqu'on veut calculer toutes les ℓ-isogénies dans la section 7.6. En particulier, l'algorithme 7.5.1 est bien plus efficace que l'algorithme 7.3.2 appliqué au noyau de chaque isogénie. Dans la section 7.7, nous expliquons comment appliquer la méthode précédente pour construire des graphes d'isogénies. Pour construire un tel graphe, il faut se ramener à des points modulaires de même niveau (pour pouvoir les comparer) : on utilise pour cela toute la correspondance modulaire

du chapitre 6. Le graphe ainsi construit est un graphe de ℓ^2-isogénies. Dans cette section, nous étudions aussi la différence de nature géométrique entre les actions 6.8 et 6.9 : alors que l'action 6.8 n'agit pas sur le graphe d'isogénie, l'action 6.9 permet d'obtenir toutes les ℓ^2-isogénies qui se factorisent par la même ℓ-isogénie. Enfin nous terminons ce chapitre par la section 7.8, où nous expliquons des résultats plus récents obtenus en collaboration avec Romain Cosset, sur comment utiliser les formules d'addition du théorème 4.3.5 pour travailler tout au long en niveau n. Ceci a deux avantages : d'une part on peut calculer des graphes de ℓ-isogénie, plutôt que de se restreindre à des graphes de ℓ^2-isogénies ; d'autre part puisque l'on reste en même niveau, on obtient des formules qui sont rationnelles (si le noyau de l'isogénie l'est).

7.2 CALCUL DE L'ISOGÉNIE CONTRAGRÉDIENTE

Soit $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ une variété abélienne marquée de type δ_0, telle que δ_0 soit divisible par un nombre pair $n \geqslant 4$, et $(b_i)_{i\in Z(\delta_0)}$ son thêta null point. Soit δ' un vecteur dans $\mathbb{N}^g$, et $\delta = \delta_0\delta'$. Soit $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta(k)$ un thêta null point d'une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ tel que $(b_i)_{i\in Z(\delta_0)} = (a_i)_{i\in Z(\delta_0)}$, il existe alors une isogénie $\pi : A_k \to B_k$ de type $\hat{Z}(\delta')$ donnée par $\pi((x_i)_{i\in Z(\delta)}) = (x_i)_{i\in Z(\delta_0)}$. Soit $\widetilde{A}_k$ et $\widetilde{B}_k$ les cônes affines de A_k et B_k associés aux coordonnées thêta induites par $\Theta_{\mathcal{L}}$ et $\Theta_{\mathcal{L}_0}$, $\widetilde{\pi}$ l'extension canonique de π aux cônes affines, et si $\widetilde{0}_{B_k} \in \widetilde{B}_k$ est un relevé du thêta null point $0_{B_k} \in B_k$, on prend pour $\widetilde{0}_{A_k} \in \widetilde{A}_k$ l'unique relevé de $0_{A_k} \in A_k$ tel que $\widetilde{\pi}(\widetilde{0}_{A_k}) = \widetilde{0}_{B_k}$. Si ℓ est le plus petit commun multiple des éléments du vecteur δ', l'isogénie contragrédiente $\widehat{\pi}$ est donnée par le diagramme suivant :

$$\begin{array}{ccc} x \in A_k(\overline{k}) & \xrightarrow{[\ell]} & z \in A_k(\overline{k}). \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\widehat{\pi}} & \\ & y \in B_k(\overline{k}) & \end{array}$$

Comme on connaît π (qui relie x et y) et $[\ell]$ (qui relie x et z) par les formules d'addition, pour calculer $\widehat{\pi}$ il suffit de faire une élimination de la variable x, en utilisant des bases de Gröbner. Une telle élimination étant très coûteuse, nous donnons une méthode qui utilise uniquement les formules d'addition.

Soit $\widetilde{y}$ un point géométrique de $\widetilde{B}_k$, et $\widetilde{x}$ un point quelconque de $\widetilde{\pi}^{-1}(\widetilde{y})$. On veut calculer $\widetilde{\widehat{\pi}}(\widetilde{y}) = \ell.\widetilde{x}$. Mais les résultats de la section 4.6 montrent que $\ell.\widetilde{x}$ est entièrement déterminé par les $\widetilde{\pi}_i(\ell.\widetilde{x})$, où i parcourt $Z(\delta)$ (ou même $\mathcal{S}$, ou même une base de décompression $\mathfrak{S}$ par rapport à $Z(\delta_0)$ en reprenant les notations de la section 4.6). On rappelle que l'on a $\widetilde{\pi}_i(\widetilde{x}) \coloneqq \widetilde{\pi}((1, i, 0).\widetilde{x})$ et d'après la proposition 4.6.3,

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \widetilde{\pi}_i((1, j, 0).\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_{A_k}), \widetilde{\pi}_{i-j}(\widetilde{x})). \tag{7.1}$$

Si $i \in Z(\delta)$, on note $\widetilde{R}_i \coloneqq \widetilde{\pi}_i(\widetilde{0}_{A_k})$, $R_i \coloneqq \pi_i(0_{A_k})$. On a $\pi_i(x) = \pi(x) + R_i$, on choisit donc un point quelconque affine $\pi_i^a(x)$ au-dessus de $\pi_i(x)$. Il existe donc $\lambda_i \in \overline{k}$ tels que $\pi_i^a(x) = \lambda_i\pi_i(\widetilde{x})$. Si $\widetilde{x}'$ est un autre antécédent de $\widetilde{y}$, alors $\widetilde{\pi}_i(\widetilde{x}') = \lambda_i'\pi_i^a(x)$, avec $\lambda' = \zeta\lambda_i$, et ζ une racine ℓ-ième de l'unité par la proposition 4.6.2. On ne peut donc déterminer λ qu'à une racine ℓ-ième de l'unité près, mais cette information est suffisante pour calculer $\widetilde{\pi}_i(\ell.\widetilde{x})$:

Théorème 7.2.1. *Soit $\widetilde{y} \in \widetilde{B}_k(\overline{k})$ et $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ tel que $\widetilde{\pi}(\widetilde{x}) = \widetilde{y}$. Pour tout $i \in Z(\delta)$, on a :*

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \lambda_i^\ell\, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, \widetilde{R}_i), \tag{7.2}$$

et de plus λ_i^ℓ est déterminé par :

$$(1, \ell i, 0).\widetilde{y} = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}). \tag{7.3}$$

DÉMONSTRATION : En combinant la proposition 4.5.4 et le lemme 4.5.3, on trouve :

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \texttt{chain\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}(\widetilde{x}), \widetilde{\pi}_i(\widetilde{0}_{A_k})) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, \widetilde{R}_i).$$

Pour déterminer λ_i^ℓ lorsque $i \in Z(\delta)$, en utilisant à nouveau la proposition 4.5.4 et une récursion triviale, comme $\ell.i \in Z(\delta_0)$, on a

$$\begin{aligned}(1, \ell i, 0).\widetilde{y} = \widetilde{\pi}((1, \ell i, 0).\widetilde{x}) &= \texttt{chain\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_i, \widetilde{y}) \\ &= \lambda_i^\ell . \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}).\end{aligned}$$

(Le couple $(\ell i, 0)$ est dans $Z(\delta_0) \subset Z(\delta)$ par définition de ℓ, on peut donc bien calculer $(1, \ell i, 0).\widetilde{y}$.) ■

REMARQUE 7.2.2 (CALCUL DE LA FIBRE DE L'ISOGÉNIE). Si $4 \mid \delta_0$, on peut prendre pour base de décompression $\mathfrak{S} = \{0, e_1, \ldots, e_g\}$ par le théorème 4.6.12. Une adaptation triviale du théorème 7.2.1 permet de retrouver la valeur de chaque $\lambda_{e_i}^{\delta_i}$, pour $i \in [1..g]$ (il suffit de remplacer ℓ par δ_i). Chaque choix de λ_{e_i} correspond alors à un point de la fibre $\widetilde{\pi}^{-1}(\widetilde{y})$. On peut donc appliquer le théorème 7.2.1 pour calculer les fibres de $\widetilde{\pi}$ en plus de l'isogénie contragrédiente $\widehat{\pi}$. ♢

REMARQUE 7.2.3. Si δ' est premier à δ_0, alors on peut prendre $\mathcal{S} = Z(\delta')$, donc $\widetilde{x}$ est entièrement déterminé par $(\widetilde{\pi}_i(\widetilde{x}))_{i \in Z(\delta')}$. L'équation (7.2) devient pour $i \in Z(\delta')$:

$$\widetilde{y} = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}).$$

Enfin, $\widetilde{0}_{A_k}$ est entièrement déterminé par les $(\widetilde{R}_i)_{i \in Z(\delta')}$ et si de plus on a $\delta' = \overline{\ell}$ (avec ℓ premier à δ), alors le noyau de $\widehat{\pi}$ est exactement l'ensemble $\{R_i \mid i \in Z(\overline{\ell}) \subset Z(\delta)\}$. ♢

Pour simplifier l'exposé de l'algorithme qui calcule $\widehat{\pi}$, on se restreint au cas $\delta_0 = \overline{n}$, $\delta = \overline{\ell n}$ avec ℓ premier à n (et $4 \mid n$) puisque c'est le plus utile en pratique, son extension au cas général étant trivial. Soit $\{e_1, \ldots, e_g\}$ la base canonique de $Z(\overline{\ell n})$, et $\{d_1, \ldots, d_g\}$ celle de $Z(\overline{\ell}) \subset Z(\overline{\ell n})$ donnée par $d_i = n e_i$. Soit $\mathfrak{S} = \{d_1, \ldots, d_g, \}$une base de décompression de $Z(\overline{\ell})$ (voir la section 4.6). On a donc l'algorithme suivant pour calculer les coordonnées compressées de $\widehat{\pi}$:

ALGORITHME 7.2.4 (IMAGE D'UN POINT PAR L'ISOGÉNIE) :
Input $y \in B_k(\overline{k})$.
Output Les coordonnées compressées de $\widehat{\pi}(y) \in A_k(\overline{k})$.

➔ Pour tout $i \in \mathfrak{S}$

- Calculer $y + R_i$ et choisir un relevé affine y_i de $y + R_i$.
- Calculer $\texttt{ylR}_i := \texttt{chain\_multadd}(\ell, y_i, \widetilde{R}_i, y_0)$
  Soit λ_i tel que $y_0 = \kappa_i \texttt{ylR}_i$.
- Retourner $\kappa_i \, \texttt{chain\_multadd}(\ell, y_i, y_0, \widetilde{R}_i))$. ♢

ANALYSE DE COMPLEXITÉ 7.2.5. Pour calculer $\widetilde{\pi}_i(\widetilde{\widehat{\pi}}(\widetilde{y}))$, on a besoin de deux multiplications

de longueur ℓ. On obtient les coordonnées compressées après $\#\mathfrak{S} = (1+g)$ telles opérations, ce qui nécessite au final $O((1+g)\log(\ell))$ pseudo-additions dans B_k (ainsi que $(1+g)n^g$ divisions dans k).

On peut ensuite facilement retrouver toutes les coordonnées de $\widehat{\pi}(y)$ en faisant une décompression des coordonnées grâce à l'algorithme 4.6.8. (Même si on veut toutes les coordonnées, il est bien plus efficace de n'appliquer l'algorithme que pour $i \in \mathfrak{S}$ et de faire une décompression que de l'appliquer pour tout $i \in Z(\overline{\ell})$ pour retrouver directement toutes les coordonnées).

Enfin, on peut appliquer le théorème 7.2.1 pour trouver l'équation rationnelle de $\widehat{\pi}$ en prenant pour y le point générique de B_k. ◇

Remarque 7.2.6 (Compression composée des coordonnées). Si $n = 4m$, au lieu de faire les calculs en niveau n, on peut les effectuer en niveau 4. En effet, si $f : \mathbb{A}_k^{Z(\overline{n})} \to \mathbb{A}_k^{Z(\overline{4})}$ est défini sur les points géométriques par $f : (x_i)_{i\in Z(\overline{n})} \mapsto (x_i)_{i\in Z(\overline{4})}$, alors f induit une m-isogénie sur B_k, et la composée $f \circ \pi$ est exactement la ℓm-isogénie de A_k de type $\hat{Z}(\overline{\ell m})$. En particulier, si $i \in Z(\overline{\ell n})$, alors$(\widetilde{f} \circ \widetilde{\pi})_i = \widetilde{f} \circ \widetilde{\pi}_i$. Si on reprend les notations du théorème 7.2.1, il suffit pour calculer $\widehat{\pi}(y)$ de calculer les $(\widetilde{f} \circ \widetilde{\pi})_{e_i}(\ell\widetilde{x})$, pour $i \in [1..g]$. Or on a si $i \in Z(\overline{\ell n})$:

$$(\widetilde{f} \circ \widetilde{\pi})_i(\ell\widetilde{x}) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \widetilde{f}(\pi_i^a(x)), \widetilde{f}(\widetilde{y}), \widetilde{f}(\widetilde{R}_i))$$

et on peut retrouver λ_i^ℓ par :

$$\widetilde{f}((1, \ell i, 0).\widetilde{y}) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \widetilde{f}(\pi_i^a(x)), \widetilde{R}_i, \widetilde{y}).$$

De plus, on peut prendre pour $\widetilde{f}(\pi_i^a(x))$ un relevé quelconque de $f(y) + f(R_i)$. Donc on peut effectuer tous les calculs en niveau 4. En fait, on peut même faire tous les calculs en niveau 2 (en faisant le calcul de $y + R_i$ en niveau 4 avant de projeter le résultat en niveau 2). ◇

Exemple 7.2.7 (Image d'un point par l'isogénie). Soit B_k la courbe elliptique $y^2 = x^3 + 23x + 3$ définie sur $k = \mathbb{F}_{31}$. Les formules de Thomae [Mum84, p. 120-121] donnent qu'un thêta null point de niveau 4 correspondant à B_k (et à la puissance 4-ième du fibré principal représenté par le diviseur 0_{B_k}) est $(3:1:18:1) \in \mathcal{M}_4(\mathbb{F}_{31})$. Soit $K = \{(3:1:18:1), (22:15:4:1), (22:1:4:15)\}$ un sous-groupe de la 3-torsion. Un thêta null point correspondant à K est donné par $(3, \eta^{14233}, \eta^{2317}, 1, \eta^{1324}, \eta^{5296}, 18, \eta^{5296}, \eta^{1324}, 1, \eta^{2317}, \eta^{14233})$ où η est un élément primitif de $\mathbb{F}_{31^3}$ défini par $\eta^3 + \eta + 28 = 0$. (Voir l'algorithme 7.3.2 pour un algorithme permettant de calculer un tel thêta null point, on constate que même si les points de K sont rationnels, il faut prendre une extension de degré 3 pour avoir une solution $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$).

Prenons $y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$, y est un point de 3-torsion qui n'est pas dans le noyau. On veut calculer $\widehat{\pi}(y)$. Soit $x \in \pi^{-1}(y)$. On calcule les points suivants dans l'algorithme 7.2.4, où $R_1 = \widetilde{\pi}_1((a_i)_{i\in Z(\delta)})$:

$$\begin{array}{ccccc} & & y & & \\ R_1 & & y+R_1 & y+2R_1 & y+3R_1 = y \\ & & 2y+R_1 & & \\ & & 3y+R_1. & & \end{array}$$

La courbe elliptique B_k est ordinaire. Si l'on considère l'extension des scalaires complexe de

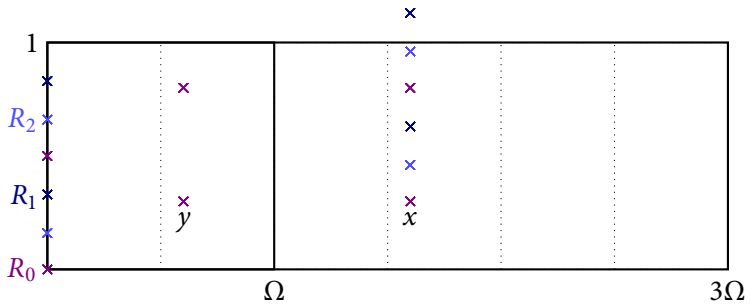


FIGURE 7.2 – Calcul de $\widehat{\pi}(y)$

son relevé canonique, on obtient la situation de la figure 7.2. Si on calcule explicitement, on obtient :

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$
$$y + R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$
$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$
$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032}$$

On a donc $\lambda_1^3 = \eta^{28758}$.

$$2y + R_1 = \lambda_1^2(\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$
$$3y + R_1 = \lambda_1^3(\eta^{7096}, \eta^{11068}, \eta^{8089,}\eta^{20005}) = \lambda_1^3\eta^{5772}R_1.$$

On en déduit :

$$\widehat{\pi}(y) = (3, \eta^{21037}, \eta^{15925}, 1, \eta^{8128}, \eta^{18904}, 18, \eta^{12100}, \eta^{14932}, 1, \eta^{9121}, \eta^{27841}).$$

De plus, on a $\texttt{chain\_mult}(3, y) = \eta^{26664}0_{B_k}$ et $\texttt{chain\_mult}(3, R_1) = 0_{B_k}$. On en déduit que

$$e_{\mathcal{L}_0^3}(y, R_1) = \frac{t^{28758}t^{26664}}{t^{5772}} = 5.$$

♢

7.2.1 *Le noyau de l'isogénie*

Soit y un point de ℓ-torsion de B_k. On cherche à déterminer quand $y \in K$, le noyau de $\widehat{\pi}$. On prend un relevé affine $\widetilde{y}$ de y tel que $\ell.\widetilde{y} = \widetilde{0}_{B_k}$. Alors y est dans K si et seulement si pour tout $i \in Z(\delta)$, on a $\widetilde{\pi}_i(\widetilde{\widehat{\pi}}(\widetilde{y})) = \widetilde{R}_i$. Si on prend un relevé affine quelconque $\widetilde{y + R_i}$ de $y + R_i$, comme y est de ℓ-torsion, il existe α_i et $\beta_i \in \overline{k}$ tels que $\texttt{chain\_multadd}(\ell, \widetilde{y + R_i}, \widetilde{y}, \widetilde{R}_i)) = \alpha_i\widetilde{R}_i$ et $\texttt{chain\_multadd}(\ell, \widetilde{y + R_i}, \widetilde{R}_i, \widetilde{y}) = \beta_i(1, \ell i, 0).\widetilde{y}$. Le théorème 7.2.1 nous dit alors que $\widetilde{\pi}_i(\widetilde{\widehat{\pi}}(\widetilde{y})) = \frac{\alpha_i}{\beta_i}\widetilde{R}_i$. Mais le théorème 5.4.1 nous donne $\frac{\alpha_i}{\beta_i} = e_{\mathcal{L}_0^\ell}(y_i, R_i)$. On retrouve que le noyau est formé des points de ℓ-torsion dans l'orthogonal des $\{R_i \mid i \in Z(\delta)\}$ (voir le théorème 6.2.7).

7.2.2 *Isogénies sur les variétés de Kummer*

Si B_k est représentée par une thêta structure de niveau 2, de telle sorte que l'on travaille sur la variété de Kummer $B_k/\pm 1$, supposons que les thêta null points pairs ne s'annulent

pas. On peut alors toujours calculer les pseudo-additions (voir la section 4.8). Si $\ell \geqslant 2$, A_k est représenté par une thêta structure de niveau 2ℓ, qui donne un plongement projectif de A_k (et non pas de la variété de Kummer associée à A_k). En particulier, à partir de $\pm\widetilde{R}_i$ et $\pm\widetilde{R}_j$ pour $i, j \in Z(2\ell)$, on peut retrouver explicitement $\pm(\widetilde{R}_i + \widetilde{R}_j) = \pm(\widetilde{R}_{i+j})$.

Si $\pm y \in B_k/\pm 1$, on veut calculer l'ensemble $\{\widehat{\pi}(y), \widehat{\pi}(-y)\}$. On peut appliquer exactement l'algorithme 7.2.4, sauf la première étape qui consiste à calculer $y + R_i$. Dans ce cas-là, on se fixe un $i_0 \in Z(\overline{\ell})$, on calcule l'ensemble $\{\pm(y + R_{i_0}), \pm(y - R_{i_0})\}$ en faisant une addition normale (qui sur la variété de Kummer nécessite une racine carrée). On choisit un point $\pm(y+R_{i_0})$ dans cet ensemble, et on calcule les $\pm(y + R_i)$ en faisant une addition compatible avec $\pm(y + R_{i_0})$ et $\pm(R_i + R_{i_0})$.

Analyse de complexité 7.2.8. Pour résumer, on a besoin de calculer g additions normales, $g(g-1)/2$ additions compatibles, et $O(\frac{1}{2}g(g+1)\log(\ell))$ pseudo-additions de niveau 2 dans la variété de Kummer $B_k/\pm 1$. ◇

7.3 FORMULES DE VÉLU EN DIMENSION SUPÉRIEURE

L'algorithme 7.2.4 prend en entrée le thêta null point $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$ (en fait si on a besoin seulement des coordonnées compressées, il suffit de lui donner en entrée les coordonnées compressées $(\widetilde{R}_i)_{i\in\mathfrak{S}}$ de $(a_i)_{i\in Z(\delta)}$). Ce thêta null point peut être calculé grâce aux méthodes du chapitre 6, mais ceci nécessite une base de Gröbner coûteuse. Dans cette section, on donne un algorithme qui reconstitue $(a_i)_{i\in Z(\delta)}$ à partir des $(R_i)_{i\in Z(\delta)}$. On peut voir cet algorithme comme une généralisation des formules de Vélu en dimension supérieure. L'idée est la suivante : on a $(a_i)_{i\in Z(\delta)} = \widehat{\pi}((b_i)_{i\in Z(\delta_0)})$, on peut donc essayer d'appliquer l'esprit de l'algorithme 7.2.4 pour retrouver $(a_i)_{i\in Z(\delta)}$.

Soit K_0 un sous-groupe de type $Z(\delta)$ isotrope maximal de B_k (c'est-à-dire qu'il existe une base symplectique de $K(\mathcal{L}_0^\ell)$ compatible avec la base symplectique de $K(\mathcal{L}_0)$ tel que K_0 soit de type $Z(\delta)$ pour cette base symplectique, où $\ell = \vee_{i=1}^g \delta_i'$). Soit $\{f_{e_1}, \dots, f_{e_g}, f'_{e_1}, \dots, f'_{e_g}\}$ la base symplectique canonique de $K(\mathcal{L}_0)$ induite par la thêta structure $\Theta_{\mathcal{L}_0}$; on se fixe une numérotation $Z(\delta) \to K_0, i \mapsto T_i$ telle que la base $\{T_{e_1}, \dots, T_{e_g}\}$ de K vérifie $\delta_i' T_{e_i} = f_{e_i}$.

Soit $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ un thêta null point correspondant à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ telle que $K_0 = \pi(K_1(\mathcal{L}))$ où $\pi : A_k \to B_k$ est l'isogénie canonique de type $\hat{Z}(\delta')$. Les résultats de la section 6.3 montrent qu'on peut supposer que $(a_i)_{i\in Z(\delta)}$ est tel que $R_{e_i} = T_{e_i}$ pour tout $i \in [1..g]$. On se fixe des relevés affines quelconques $\widetilde{T}_i$ pour tout $i \in Z(\delta)$, on a alors $\widetilde{R}_i = \lambda_i \widetilde{T}_i$. Pour retrouver $(a_i)_{i\in Z(\delta)}$, il suffit de retrouver λ_i pour tout $i \in Z(\delta)$ (on peut même se restreindre à $i \in \mathfrak{S}$ une base différentielle de $Z(\delta)$ relativement à $Z(\delta_0)$: voir la section 4.6 pour cette notion). On peut procéder comme dans la section 7.2, on sait d'après l'équation (7.1) que $\widetilde{R}_{i+j} = \texttt{chain\_add}(\widetilde{R}_i, \widetilde{R}_j, \widetilde{R}_{i-j})$ pour tous $i, j \in Z(\delta)$.

D'après la proposition 4.5.4 et le lemme 4.5.3, on obtient alors $(1, \ell i, 0).\widetilde{0}_{B_k} = \ell.\widetilde{R}_i = \lambda_i^{\ell^2}\widetilde{T}_i$. On retrouve donc la valeur de chaque $\lambda_i^{\ell^2}$, il suffit alors d'essayer toutes les combinaisons possibles jusqu'à tomber sur un point $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$.

On peut faire mieux en utilisant la symétrie : si $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_\delta$, on a $R_i = -R_{-i}$. Supposons pour simplifier que $\delta_0 = \overline{n}$ et $\delta = \overline{\ell n}$ et que ℓ soit impair et écrivons $\ell = 2\ell' + 1$. On a alors, comme R_i est un point de ℓn-torsion :

$$\begin{aligned}[\ell'+1].\widetilde{R}_i = \widetilde{\pi}((1, (\ell'+1)i, 0).\widetilde{0}_{A_k}) &= \widetilde{\pi}(-(1, (\ell n - \ell' - 1)i, 0).\widetilde{0}_{A_k}) \\ &= \widetilde{\pi}(-(1, (\ell n - \ell)i, 0).[\ell'](1, i, 0).\widetilde{0}_{A_k}) = -(1, \ell(n-1)i, 0)[\ell']\widetilde{R}_i\end{aligned}$$

ce qui donne via le lemme 4.5.3 :

$$\lambda_i^{\ell}[\ell'+1]\widetilde{T}_i = -(1, \ell(n-1)i, 0).[\ell']\widetilde{T}_i. \tag{7.4}$$

car $(\ell'+1)^2 - (\ell')^2 = 2\ell'+1 = \ell$. On peut donc retrouver λ_i^{ℓ} pour chaque $i \in \mathfrak{S}$, et le chapitre 6 montre que chaque choix de λ_i correspond à un point modulaire $(a_i)_{i\in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}$.

Remarque 7.3.1. On peut interpréter les choix des racines λ_i ainsi : se donner un thêta null point $(a_i)_{i\in Z(\overline{\ell n})}$ de niveau ℓn sur $(A_k, \mathcal{L})$ revient à se donner une base symplectique sur $A_k[\ell n]$, et une décomposition compatible de $A_k[2\ell n]$. De plus, on cherche $(a_i)_{i\in Z(\overline{\ell n})}$ π-compatible avec le thêta null point $(b_i)_{i\in Z(\overline{n})}$ sur $(B_k, \mathcal{L}_0)$, de telle sorte que $K_2(\mathcal{L})$ est forcément donné par $\pi^{-1}(K_2(\mathcal{L}_0))$. Comme ℓ est impair, la décomposition symplectique de $A_k[2\ell n]$ au-dessus de $A_k[\ell n]$ est déterminée par celle de $B_k[2n]$ au-dessus de $B_k[n]$, donc le choix de $(a_i)_{i\in Z(\overline{\ell n})}$ revient à déterminer un supplémentaire (isotrope) à $K_2(\mathcal{L})$ dans $A_k[\ell n]$ (voir le corollaire 6.2.8).

Étant donné le sous-groupe isotrope maximal $K_0 \subset B_k[\ell n]$, on va chercher $K_1(\mathcal{L})$ comme un sous groupe de $\pi^{-1}(K_0)$. Le groupe $K_1(\mathcal{L})$ est alors uniquement déterminé modulo translations par $K_2(\mathcal{L})[\ell]$, et les choix des λ_i revient à fixer un représentant, par l'action 6.9 de la proposition 6.4.2. ((Par exemple, soit ζ une racine ℓn-ième de l'unité, et $(f_1, \dots, f_g)$ est une base de $K_2(\mathcal{L})$. On va chercher le dual e_i de f_i par rapport à ζ de telle sorte que $\pi(e_i) \in K_0$ et qu'il soit non orthogonal à $\pi(f_i)$ pour $e_{\mathcal{L}_0^{\ell}}$. Le point e_i est alors uniquement déterminé modulo le noyau $K = K_2(\mathcal{L})[\ell]$ de π.))Enfin, le choix d'une numérotation de K_0 détermine une numérotation de $K_1(\mathcal{L})[\ell]$, et donne l'action 6.8.

On revient plus en détail sur l'influence du choix des racines λ_i dans la proposition 7.7.1.◇

Si $\ell = 2\ell'$ est pair, pour obtenir une équation non triviale sur λ_i on peut écrire :

$$\lambda_i^{2\ell}[\ell'+1]\widetilde{T}_i = -(1, \ell(n-1)i, 0).[\ell']\widetilde{T}_i$$

ce qui fait qu'on connaît la valeur de $\lambda^{2\ell}$. Il est normal que l'on ait plus de choix que dans le cas où ℓ est impair, car si $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_{\delta}$ est un point dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$, et $\pi : A_k \to B_k$ l'isogénie associée, alors si $c \in \operatorname{Ker}\pi[2]$, l'automorphisme symétrique de conjugaison $\mathtt{conj}_c$ stabilise $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$.

Si ℓ est premier à n, ℓ est impair, et il suffit de déterminer λ_i pour $i \in Z(\overline{\ell})$. L'équation (7.4) se simplifie alors en

$$\lambda_i^{\ell}(\ell'+1).\widetilde{T}_i = -\ell'\widetilde{T}_i. \tag{7.5}$$

De plus, l'ensemble $\{R_i \mid i \in Z(\overline{\ell})\}$ est le noyau de $\widehat{\pi}$, donc dans ce cas-là on peut reconstituer le thêta null point $(a_i)_{i\in Z(\delta)} \in \mathcal{M}_{\overline{\ell n}}$ uniquement en connaissant le noyau de $\widehat{\pi}$. Ceci est cohérent avec le fait que si ℓ est premier à n, à partir d'un sous-groupe isotrope maximal de la ℓ-torsion et du groupe isotrope maximal $K_1(\mathcal{L}_0)$, le groupe $K_0 = K \oplus K_1(\mathcal{L})$ est un sous-groupe isotrope maximal de $B_k[\ell n]$ pour $e_{\mathcal{L}_0^{\ell}}$.

Comme dans l'algorithme 7.2.4, pour simplifier on donne l'algorithme pour ℓ premier à n, même si l'extension à des δ et δ_0 généraux est facile. Si $\{d_1, \dots, d_g\}$ est la base précédente de $Z(\overline{\ell}) \subset Z(\overline{\ell n})$, on a alors $\mathfrak{S} = \{d_1, \dots, d_g, d_1+d_2, \dots, d_{g-1}+d_g\}$, et les formules de Vélu s'expriment :

Algorithme 7.3.2 (Formules de Vélu) :
Entrées $T_{d_1}, \cdots T_{d_g}$ une base du noyau de $\widehat{\pi}$.
Sortie Les coordonnées compressées de $\widetilde{0}_{A_k}$, un thêta null point de niveau ℓn correspondant à $\widehat{\pi}$.

➔ Soit ℓ' tel que $\ell = 2\ell' + 1$.
➔ Pour tous $i, j \in [1..g]$, $i \neq j$, calculer les points $T_{d_i} + T_{d_j}$. Si $I = i + j \in \mathfrak{S}$, on pose $T_I = T_{d_i} + T_{d_j}$.
➔ Pour tout $i \in \mathfrak{S}$,
- Choisir un relevé affine $\widetilde{T}_i$ de T_i, et calculer

$$(\beta^i_j)_{j\in Z(\overline{n})} := \texttt{chain\_mult}(\ell', \widetilde{T}_i)$$
$$(\gamma^i_j)_{j\in Z(\overline{n})} := \texttt{chain\_mult}(\ell'+1, \widetilde{T}_i)$$

- Trouver $\alpha_i \in k$ tel que $(\gamma^i_j)_{j\in Z(\overline{n})} = \alpha_i(\beta^i_{-j})_{j\in Z(\overline{n})}$.
- Retourner $\widetilde{R}_i := (\alpha_i)^{\frac{1}{\ell}} \cdot \widetilde{T}_i$. ◇

ANALYSE DE COMPLEXITÉ 7.3.3. Pour calculer $\widetilde{R}_i$ lorsque $i \in \mathfrak{S}$, un des ℓ relevés affines de T_i tel que : $\texttt{chain\_mult}(\ell'+1, \widetilde{R}_i) = -\texttt{chain\_mult}(\ell', \widetilde{R}_i)$, on calcule deux multiplications (par un scalaire) de longueurs $\ell/2$, et une racine ℓ-ième de l'unité. Après $g(g+1)/2 = \#\mathfrak{S} - 1$ telles opérations, on retrouve les coordonnées compressées de $\widetilde{0}_{A_k}$, et on peut utiliser l'algorithme 4.6.8 pour retrouver $\widetilde{0}_{A_k}$ en entier (ce qui n'est pas nécessaire si on a besoin uniquement des coordonnées compressées de $\widetilde{\pi}$).

Il convient de noter que le point $(a_i)_{i\in Z(\delta)}$ est dans $\mathcal{M}_{\overline{\ell n}}(\overline{k})$ à cause des racines ℓ-ièmes. Si $k = \mathbb{F}_q$ est un corps fini tel que $\ell \mid q-1$ (donc k contient les racines de l'unité), comme le groupe de Galois absolu de $\mathbb{F}_q$ est abélien, $(a_i)_{i\in Z(\delta)}$ est dans $\mathcal{M}_{\overline{\ell n}}(\mathbb{F}_{q^\ell})$. ◇

7.3.1 *Formules de Vélu sur les variétés de Kummer*

Si B_k est donné par un thêta null point $(b_i)_{i\in Z(\overline{2})}$ de niveau 2 (et tel que les thêta null points pairs ne s'annulent pas), comme dans la section 7.2.2, l'algorithme 7.3.2 s'adapte tel quel sauf pour les additions normales $T_{e_i} + T_{e_j}$. Ici, on calcule les $T_{e_1} \pm T_{e_j}$ et on choisit un représentant pour chaque $j \in [2..g]$. Ensuite, pour les additions $T_{e_i} + T_{e_j}$, on effectue une addition compatible avec le choix déjà effectué $T_{e_1} + T_{e_i}$ et $T_{e_1} + T_{e_j}$.

7.4 EXCELLENTS POINTS DE ℓ-TORSION

Pour le reste du chapitre, on se concentre sur le cas $\delta_0 = \overline{n}$, $\delta = \overline{\ell n}$, avec ℓ premier à n. On cherche à déterminer toutes les ℓ-isogénies (de noyau isotrope) de B_k. Supposons que l'on ait calculé une base symplectique de la ℓ-torsion de B_k, alors pour chaque sous-groupe isotrope maximal $K \subset B_k[\ell]$, on peut appliquer l'algorithme 7.3.2. Pour cela, il faut déterminer des relevés affines $\widetilde{T}$ de certains points $T \in K$ tels que

$$[\ell'+1].\widetilde{T} = -[\ell']\widetilde{T}.$$

où $\ell = 2\ell' + 1$.

DÉFINITION 7.4.1. Un excellent point de ℓ-torsion est un point géométrique $\widetilde{T} \in \widetilde{B}_k(\overline{k})$ qui vérifie

$$[\ell'+1].\widetilde{T} = -[\ell']\widetilde{T}.$$ ◇

Calculer un excellent point de ℓ-torsion au-dessus de tout point de ℓ-torsion dans B_k est coûteux, ceci nécessitant ℓ^g multiplications de longueur $\ell/2$. On va montrer que si $\widetilde{T}_1$, $\widetilde{T}_2$ et

$\widetilde{T_1 - T_2}$ sont d'excellents points de ℓ-torsion, alors $\widetilde{T_1 + T_2} = \texttt{chain\_add}(\widetilde{T_1}, \widetilde{T_2}, \widetilde{T_1 - T_2})$ l'est également. On verra alors qu'il suffit de calculer un excellent point de ℓ-torsion au-dessus de chaque point d'une base différentielle de $B_k[\ell]$.

LEMME 7.4.2. *Si le point géométrique $\widetilde{T} \in \widetilde{B}_k(\overline{k})$ est un excellent point de ℓ-torsion, alors $T := p_{B_k}(\widetilde{T})$ est un point de ℓ-torsion, et si $\lambda \in \overline{k}$, $\lambda\widetilde{T}$ est un excellent point de ℓ-torsion si et seulement si $\lambda^\ell = 1$. Il y a donc exactement ℓ excellents points de ℓ-torsion au-dessus de T.*

DÉMONSTRATION : On a en projetant sur B_k : $[\ell' + 1]T = -[\ell']T$ donc T est un point de ℓ-torsion. Le reste découle trivialement du lemme 4.5.3 et du fait que ℓ est premier à la caractéristique de k. ■

Pour caractériser les points excellents de ℓ-torsion, on va utiliser encore une fois l'isogénie $[\ell]$. On se donne une thêta structure sur $(B_k, [\ell]^*\mathcal{L}_0)$ compatible avec $\Theta_{\mathcal{L}_0}$, on se fixe un système de coordonnées thêta affine sur $(B_k, [\ell]^*\mathcal{L}_0)$, et on note $\widetilde{[\ell]}$ le relevé affine de $[\ell]$ par rapport à ces coordonnées, et $\widetilde{0}_{B_k,\ell}$ le relevé canonique du thêta null point de $(B_k, [\ell]^*\mathcal{L}_0)$.

PROPOSITION 7.4.3. *Soit $y \in B_k[\ell]$, $\widetilde{y} \in p_{B_k}^{-1}(y)$ et $\widetilde{x} \in \widetilde{[\ell]}^{-1}(\widetilde{y})$. Il existe $(\alpha, ni, nj) \in k^{*\ell} \times Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$ tels que $\widetilde{x} = (\alpha, ni, nj).\widetilde{0}_{B_k,\ell}$. Alors $\widetilde{y}$ est un excellent point de ℓ-torsion si et seulement si $\alpha = \lambda_{i,j}\mu$ où μ est une racine ℓ-ième de l'unité et $\lambda_{i,j} = \langle i, j\rangle^{\ell' n(\ell-1)}$.*

((On peut remarquer que les autres points géométriques $\widetilde{x}' \in \widetilde{B_k}'(\overline{k})$ de la fibre $\widetilde{[\ell]}^{-1}(\widetilde{y})$ sont de la forme $\widetilde{x}' = (1, \ell ni', \ell nj').\widetilde{x}$ où $(i', j') \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$) (voir l'exemple 7.5.2), donc la classe de $\alpha \in \overline{k}^*/\overline{k}^{*\ell}$ ne dépend que de $\widetilde{y}$.))

DÉMONSTRATION : Comme $p_{\widetilde{B_k}'}(\widetilde{x}) \in B_k[\ell^2]$, il existe $h \in \mathcal{H}(\overline{\ell^2 n})$ tel que $\widetilde{x} = h.\widetilde{0}_{B_k,\ell}$, avec $h = (\alpha, ni, nj)$. Par le lemme 7.4.2, il suffit de vérifier que $\widetilde{[\ell]}((\lambda_{i,j}, ni, nj).\widetilde{0}_{B_k,\ell})$ est un excellent point de ℓ-torsion. Si $m \in \mathbb{Z}$, soit $\widetilde{x}_m = \texttt{chain\_mult}(m, \widetilde{x})$ et $\widetilde{y}_m = \texttt{chain\_mult}(m, \widetilde{y})$. La proposition 4.5.4 nous donne $\widetilde{x}_m = (\lambda_{i,j}^{m^2}, m \cdot i, m \cdot j).\widetilde{0}_{B_k,\ell}$, et en appliquant la proposition 4.5.5 on obtient : $\widetilde{y}_m = \widetilde{[\ell]}(\lambda_{i,j}^{m^2}, m \cdot i, m \cdot j).\widetilde{0}_{B_k,\ell}$. On vérifie alors en utilisant le lemme 4.5.1 que l'on a bien :

$$\begin{aligned}
\widetilde{y}_{\ell'} &= \widetilde{[\ell]}(\lambda_{i,j}^{\ell'^2}, \ell' \cdot i, \ell' \cdot j).\widetilde{0}_{B_k,\ell} = \widetilde{[\ell]}(1, \ell n(\ell-1)i, \ell n(\ell-1)j)(\lambda_{i,j}^{\ell'^2}, \ell' i, \ell' j).\widetilde{0}_{B_k,\ell} \\
&= \langle \ell' i, \ell n(\ell-1)j\rangle \widetilde{[\ell]}(\lambda_{i,j}^{\ell'^2}, (\ell' + \ell n(\ell-1)) \cdot i, (\ell' + \ell n(\ell-1)) \cdot j).\widetilde{0}_{B_k,\ell} \\
&= \lambda_{i,j}^{\ell} \widetilde{[\ell]}(\lambda_{i,j}^{(\ell'+1)^2}/\lambda_{i,j}^{\ell}, -(\ell'+1) \cdot i, -(\ell'+1) \cdot j).\widetilde{0}_{B_k,\ell} \\
&= \widetilde{[\ell]}(-\widetilde{x}_{\ell'+1}) = -\widetilde{y}_{\ell'+1}.
\end{aligned}$$

■

REMARQUE 7.4.4. Si $i, j \in Z(\overline{2})$, on a vu dans la section 4.2 que (α, i, j) est symétrique si et seulement si $\alpha = \pm\langle i, j\rangle^{1/2}$. On peut voir la forme $(\mu\lambda_{i,j}, i, j)$ où μ est une ℓ-ième racine de l'unité comme une extension naturelle de ce concept. ◇

COROLLAIRE 7.4.5. *Soit $\widetilde{y}_1, \widetilde{y}_2$ et $\widetilde{y_1 - y_2} \in \widetilde{B}_k(\overline{k})$ des excellents points de ℓ-torsion. Alors $\widetilde{y_1 + y_2} := \texttt{chain\_add}(\widetilde{y}_1, \widetilde{y}_2, \widetilde{y_1 - y_2})$ est également un excellent point de ℓ-torsion.*

DÉMONSTRATION : Soit $(\alpha_1, i_1, j_1) \in \mathcal{H}(\overline{\ell^2 n})$, $(\alpha_2, i_2, j_2) \in \mathcal{H}(\overline{\ell^2 n})$, $(\alpha_3, i_3, j_3) \in \mathcal{H}(\overline{\ell^2 n})$, tels que

$$\widetilde{[\ell]}(\alpha_1, i_1, j_1).\widetilde{0}_{B_k,\ell} = \widetilde{y}_1, \quad \widetilde{[\ell]}(\alpha_2, i_2, j_2).\widetilde{0}_{B_k,\ell} = \widetilde{y}_2, \quad \widetilde{[\ell]}(\alpha_3, i_3, j_3).\widetilde{0}_{B_k,\ell} = \widetilde{y_1 - y_2}$$

Comme la classe de $\alpha_3 \in \overline{k}/\overline{k}^{*,\ell}$ ne dépend que de $\widetilde{y_1 - y_2}$, on peut supposer que $i_3 = i_1 - i_2$, $j_3 = j_1 - j_2$ et par le lemme 7.4.2 que $\alpha_1 = \lambda_{i_1,j_1}$, $\alpha_2 = \lambda_{i_2,j_2}$ et $\alpha_3 = \lambda_{i_1-i_2,j_1-j_2}$.

La proposition 4.5.4 et le lemme 4.5.3 nous donnent alors

$$\widetilde{y_1 + y_2} = \frac{\lambda_{i_1,j_1}^2 \lambda_{i_2,j_2}^2}{\lambda_{i_1-i_2,j_1-j_2}} (1, i_1 + i_2, j_1 + j_2).\widetilde{0}_{B_k,\ell} = (\lambda_{i_1+i_2,j_1+j_2}, i_1 + i_2, j_1 + j_2).\widetilde{0}_{B_k,\ell},$$

ce qui montre que $\widetilde{y_1 + y_2}$ est effectivement un excellent point de ℓ-torsion par la proposition 7.4.3. ■

7.5 CALCUL DE TOUTES LES ℓ-ISOGÉNIES

Le but de cette section est d'expliquer comment calculer toutes les ℓ-isogénies lorsqu'on a calculé toute la ℓ-torsion $B_k[\ell]$, en utilisant les résultats de la section 7.4 pour éviter d'avoir recours à l'algorithme 7.2.4 pour chaque sous-groupe isotrope maximal de $B_k[\ell]$.

ALGORITHME 7.5.1 (CALCUL DE TOUS LES POINTS MODULAIRES) :
Entrée $T'_1, \cdots, T'_{2g}$ une base de la ℓ-torsion de B_k.
Sorties Toutes les ℓ-isogenies de noyau isotrope.

On donne juste les grandes lignes de l'algorithme car on verra un exemple détaillé dans l'exemple 7.5.2.

- ➔ Calculer une base symplectique $T_{e_1}, \ldots, T_{e_{2g}}$ de $B_k[\ell]$ grâce à l'algorithme 6.2.6.
- ➔ Calculer des relevés affines qui soient des excellents points de ℓ-torsion $\widetilde{T}_{e_1}, \cdots, \widetilde{T}_{e_{2g}}$, $\widetilde{T_{e_1} + T_{e_2}}, \cdots, \widetilde{T_{e_{g-1}} + T_{e_g}}$.
- ➔ Utiliser des pseudo-additions à partir des points précédents pour obtenir des relevés affines $\widetilde{T}$ au-dessus de chaque point géométrique $T \in B_k[\ell]$ (ces points seront d'excellents points de ℓ-torsion par le corollaire 7.4.5).
- ➔ Pour tout sous-groupe isotrope maximal $K \subset B_k[\ell]$, prendre les relevés correspondants pour obtenir le thêta null point associé comme dans l'algorithme 7.3.2. ◇

EXEMPLE 7.5.2 (FORMULES DE VÉLU). Soit $\Theta_{\mathcal{L}}(B_k, \mathcal{L}_0^{\ell})$ une thêta structure sur $(B_k, [\ell]^*\mathcal{L}_0)$ telle que la base symplectique de la ℓ-torsion soit de la forme :

$$\begin{aligned}
\widetilde{T_1} &= \widetilde{[\ell]}(1, (n, 0, \cdots, 0), 0).\widetilde{0}_{B_k,\ell} \\
\widetilde{T_2} &= \widetilde{[\ell]}(1, (0, n, \cdots, 0), 0).\widetilde{0}_{B_k,\ell}, \ldots \\
\widetilde{T_{g+1}} &= \widetilde{[\ell]}(1, 0, (n, 0, \cdots, 0)).\widetilde{0}_{B_k,\ell} \\
\widetilde{T_{g+2}} &= \widetilde{[\ell]}(1, 0, (0, n, \cdots, 0)).\widetilde{0}_{B_k,\ell}, \ldots \\
\widetilde{T_1 + T_{g+2}} &= \widetilde{[\ell]}(1, (n, 0, \cdots, 0), (0, n, 0, \cdots, 0)).\widetilde{0}_{B_k,\ell}, \ldots
\end{aligned}$$

où $\widetilde{0}_{B_k,\ell}$ est le (relevé canonique) du thêta null point associé à $\Theta_{\mathcal{L}}(B_k, \mathcal{L}_0^{\ell})$.

Dans l'algorithme 7.5.1, on calcule alors d'après la proposition 4.5.4 les relevés suivants des points de ℓ-torsion :

$$\{\widetilde{[\ell]}(1, in, jn).\widetilde{0}_{B_k,\ell} : i, j \in \{0, 1, \cdots, \ell - 1\}^g \subset Z(\ell^2 n)\}. \tag{7.6}$$

Soit maintenant $K \subset B_k[\ell]$ un sous-groupe isotrope maximal. Dans la phase de reconstruc-

tion de l'algorithme 7.3.2, on a besoin d'avoir calculé les points de la forme $\widetilde{[\ell]}(1, in, jn).\widetilde{0}_{B_k,\ell}$ pour $i, j \in Z(\ell^2 n)$. On calcule :

$$\begin{aligned}\widetilde{[\ell]}(1, in, jn).\widetilde{0}_{B_k,\ell} &= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1, \ell\alpha n, \ell\beta n).(1, (i-\ell\alpha)n, (j-\ell\beta)n).\widetilde{0}_{B_k,\ell} \\ &= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1, (i-\ell\alpha)n, (j-\ell\beta)n).\widetilde{0}_{B_k,\ell},\end{aligned}$$

où $\alpha, \beta \in Z(\ell^2 n)$, et ζ est une racine $(\ell^2 n)$-ième de l'unité. Ainsi on est ramené à un point déjà calculé dans l'équation (7.6) à une racine ℓ-ième de l'unité près.

Pour donner un exemple plus explicite, on prend $g = 1, \ell = 3, n = 4$. Soit donc B_k une courbe elliptique munie d'une thêta structure Θ_{B_k} de niveau 4. Soit T_1, T_2 une base symplectique de $B_k[\ell]$, on choisit des excellents points de ℓ-torsion $\widetilde{T}_1, \widetilde{T}_2, \widetilde{T_1 + T_2}$. Soit $\Theta_{\mathcal{L}}(B_k, \mathcal{L}_0^{\ell})$ une thêta structure de niveau $\ell^2 n$ sur B_k compatible avec Θ_{B_k}, telle que si $\widetilde{0}_{B_k,\ell} = (b_i)_{i\in Z(\delta_0)}$ est le thêta null point correspondant, on ait $\widetilde{T}_1 = \widetilde{[\ell]}(1, n, 0).\widetilde{0}_{B_k,\ell}$, $\widetilde{T}_2 = \widetilde{[\ell]}(1, 0, n).\widetilde{0}_{B_k,\ell}$, et $\widetilde{T_1 + T_2} = \widetilde{[\ell]}(1, n, n).\widetilde{0}_{B_k,\ell}$.

On a vu dans l'équation (7.6) que l'on calculait les points suivants en utilisant l'algorithme 7.5.1 : $\widetilde{[\ell]}(1, in, jn).\widetilde{0}_{B_k,\ell}$ avec $i, j \in 0, 1, \cdots, \ell - 1 \subset \mathbb{Z}/\ell^2 n\mathbb{Z}$.

Maintenant, soit $T = p_{B_k}(\widetilde{[\ell]}(1, 2n, n).\widetilde{0}_{B_k,\ell})$, le groupe $K =< p_{B_k}(T) >$ engendré par T est un sous-groupe isotrope maximal de $B_k[\ell]$ (voir la figure 7.3). Soit $A_k = B_k/K$, et Θ_{A_k} une thêta structure sur A_k telle que le thêta null point $\widetilde{0}_{A_k}$ correspondant vérifie $a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$.

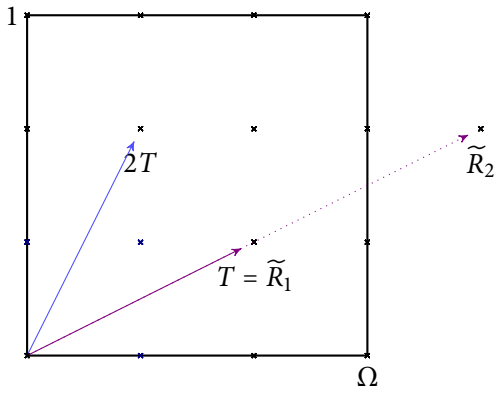


FIGURE 7.3 – Le sous-groupe engendré par T dans la 3-torsion

Si on note $\widetilde{R}_i$ le point $\widetilde{\pi}_i(\widetilde{0}_{A_k})$ lorsque $i \in \mathbb{Z}/\ell Z \subset \mathbb{Z}/\ell n\mathbb{Z}$, on peut supposer (quitte à permuter les coefficients de $(a_i)_{i\in Z(\delta)}$) qu'on a $\widetilde{R}_1 = \widetilde{[\ell]}(1, 2n, n).\widetilde{0}_{B_k,\ell}$. Explicitement, on a :

$$\begin{aligned}\widetilde{0}_{A_k} &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) \\ \widetilde{\pi}(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) &= (x_0, x_3, x_6, x_9) \\ \widetilde{R}_0 &= (a_0, a_3, a_6, a_9) = \widetilde{0}_{B_k} \\ \widetilde{R}_1 &= (a_4, a_7, a_{10}, a_1) \\ \widetilde{R}_2 &= (a_8, a_{11}, a_2, a_5).\end{aligned}$$

De plus, on sait par le corollaire 4.6.6 que $\widetilde{0}_{A_k}$ est entièrement déterminé par $\widetilde{R}_1$ (et $\widetilde{0}_{B_k}$). En effet, on a : $\widetilde{R}_2 = \texttt{chain\_add}(R_1, R_1, \widetilde{0}_{B_k})$. De plus, la proposition 4.5.4 montre :

$$\widetilde{R}_2 = \widetilde{[\ell]}(1, 4n, 2n).\widetilde{0}_{B_k,\ell} = \widetilde{[\ell]}\zeta^{-2n\cdot 3n}(1, 3n, 0).(1, n, 2n).\widetilde{0}_{B_k,\ell} = \zeta^{-2n\cdot 3n}\widetilde{[\ell]}(1, n, 2n).\widetilde{0}_{B_k,\ell},$$

où ζ est une racine $(\ell^2 n)$-ième de l'unité.

Autrement dit, pour reconstituer le thêta null point correspondant à K, on multiplie le point $\widetilde{[\ell]}(1, 2n, n).\widetilde{0}_{B_k,\ell}$ que l'on a déjà calculé par la racine ℓ-ième de l'unité $\zeta^{2n\cdot\ell n}$. ◇

ANALYSE DE COMPLEXITÉ 7.5.3. Pour calculer un relevé affine $\widetilde{T_i}$ qui soit un excellent point de ℓ-torsion, on a besoin de calculer une racine ℓ-ième de l'unité (ainsi que des pseudo-additions, mais on peut les réutiliser pour l'étape suivante). Une fois qu'on a calculé $\ell(2\ell+1)$ telles racines, on calcule (les relevés affines de) toute la ℓ-torsion en utilisant $O(\ell^{2g})$ pseudo-additions. On peut alors calculer les $e(T_i, T_j)$ avec une seule division, puisqu'on a déjà les chaînes d'addition nécessaires à l'algorithme 5.4.2. En utilisant ces pairings, on peut calculer une base symplectique de $B_k[\ell]$. (Ceci nécessite de prendre les logarithme discret des pairings, ce qui peut se faire en $O(\ell)$ opérations dans $\overline{k}$). À partir de cette base symplectique, on peut énumérer tous les sous-groupes isotropes maximaux $K \subset B_k[\ell]$, et reconstituer le thêta null point correspondant via $O(\ell^g)$ (ou seulement $O(n^g g(g+1)/2)$ si on a besoin uniquement des coordonnées compressées) multiplications par une racine ℓ-ième de l'unité. ◇

L'extension aux variétés de Kummer se fait exactement comme dans la section 7.3.1 : on calcule les $T_{e_1} + T_{e_i}$ pour $i \in [2..2g]$, puis on calcule les $T_{e_i} + T_{e_j}$ en faisant des additions compatibles.

7.6 CALCUL DE LA ℓ-TORSION

Dans cette section, si $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ est une variété abélienne marquée de niveau δ_0, on étudie quelques méthodes pour calculer la ℓ-torsion sur B_k en coordonnées thêta, ce qui nous permet d'appliquer l'algorithme 7.5.1.

La première idée est d'utiliser la correspondance modulaire ϕ du chapitre 6 avec $\delta = (\delta_{0,1}, \delta_{0,2}, \dots, \ell\delta_{0,g})$. Si $(b_i)_{i\in Z(\delta_0)}$ est le thêta null point de B_k, et $(a_i)_{i\in Z(\delta)} \in \phi_1^{-1}((a_i)_{i\in Z(\delta)})$, alors $(a_i)_{i\in Z(\delta)}$ correspond à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$ et une isogénie $\pi : A_k \to B_k$. Alors le point $\widetilde{T} = \widetilde{\pi}((0, 0, \cdots, \delta_{0,g}).\widetilde{0}_{A_k})$ est un excellent point de ℓ-torsion (primitif).

En réalité, on a uniquement les équations de la variété affine $\overline{\phi}_1^{-1}((b_i)_{i\in Z(\delta_0)})$, mais les points dégénérés de la fibre nous donnent des points T soit non définis projectivement, soit de ℓ-torsion (et non primitifs).

De plus, si ℓ est premier avec δ_0, $\widetilde{T}$ détermine uniquement $(a_i)_{i\in Z(\delta)}$ (car $\widetilde{\pi}_i((a_i)_{i\in Z(\delta)}) = i_0.\widetilde{T}$), et on obtient tous les excellents points de ℓ-torsion ainsi (car les points de ℓ-torsion sont orthogonaux à $K(\mathcal{L}_0)$ dans $K(\mathcal{L}_0^\ell)$). La fibre $\overline{\phi}_1^{-1}((b_i)_{i\in Z(\delta_0)})$ est donc de degré ℓ^{2g+1}, avec $\ell\#Z(\delta_0)$ inconnues (mais il suffit d'exprimer les relations d'addition par rapport à une séquence de Lucas, on peut donc prendre un sous-ensemble du système avec $\log(\ell)\#Z(\delta_0)$ inconnues qui donne les mêmes solutions).

Une autre méthode est d'utiliser directement les relations d'addition de l'algorithme 4.4.10 au point générique de B_k. Cette fois on obtient un système d'équations de degré ℓ^{2g} avec $\#Z(\delta_0)$ inconnues. On peut par exemple résoudre ce système via une base de Gröbner. L'avantage du système précédent est qu'il nous donne directement des excellents points de ℓ-torsion. Cependant il est plus rapide de résoudre directement le système donné par les relations d'addition comme il est de plus petit degré, puis de calculer d'excellent points de ℓ-torsion au-dessus des points solutions (d'autant plus que dans l'algorithme 7.5.1, on n'a besoin de calculer d'excellents points de ℓ-torsion que pour une base différentielle de $B_k[\ell]$, les pseudo-additions donnant ensuite d'autres excellents points de ℓ-torsion par la section 7.4).

On voit l'avantage ici de travailler en niveau 2 : on calcule alors les points de ℓ-torsion de la variété de Kummer, ce qui fait qu'on a à résoudre un système de degré $(\ell^{2g}+1)/2$. Il s'avère que calculer toute la ℓ-torsion est l'aspect le plus coûteux de tout l'algorithme de calcul d'isogénies, et la réduction par 2 du degré du système fait tout l'intérêt de travailler en niveau 2 (plus que d'avoir une représentation 2^g fois plus compacte qu'en niveau 4 et des pseudo-additions plus rapides). De plus, en genre 2, GAUDRY et SCHOST [GS08] ont un algorithme pour calculer la ℓ-torsion sur une surface de Kummer (sur un corps fini) en utilisant des résultants plutôt qu'une base de Gröbner. (Les points sont donnés en coordonnées de Mumford, mais on peut utiliser les résultats de WAMELEN [Wam99] pour les convertir en coordonnées thêta de niveau 2). Cet algorithme est en $\widetilde{O}(\ell^6)$. À titre de comparaison, le calcul des excellents points de ℓ-torsion de l'algorithme 7.5.1 est en $\widetilde{O}(\ell^4)$, et chacune des $O(\ell^3)$ ℓ-isogénies nécessite ensuite $O(\ell^2)$ multiplications par une racine ℓ-ième de l'unité. Au final on voit que l'on peut calculer des ℓ-isogénies en $\widetilde{O}(\ell^6)$ en genre 2.

La notation $\widetilde{O}$ signifie que l'on ne prend pas en compte les facteurs logarithmiques.

De manière plus générale, soit B_k une variété abélienne de dimension g sur un corps fini k. Le système d'équations décrivant l'idéal associé à $B_k[\ell]$ est de degré total ℓ^{2g}, et utilise $N = \#Z(\delta_0)$ variables. D'après [Laz81], calculer une base de Gröbner pour l'ordre lexicographique s'effectue en temps $\ell^{2gO(N)}$. On peut ensuite résoudre ce système (si la base de Gröbner est trigonale) en utilisant l'algorithme de Cantor–Zassenhaus [CZ81] pour calculer les points géométriques de ℓ-torsion de B_k. Ceci donne un algorithme polynomial en ℓ (en le nombre d'opérations sur le corps fini k, et à B_k fixé) pour calculer les points de ℓ-torsion de B_k, et donc grâce à l'algorithme 7.5.1 pour calculer des ℓ-isogénies. (En pratique, plutôt que de calculer un polyrésultant comme dans [Laz81], on va plutôt calculer une base de Gröbner pour l'ordre Grevlex [Fau99 ; Fau02], qui donne des polynômes de plus petit degrés [Laz83], et utiliser l'algorithme [FGLM93] pour calculer une base de Gröbner pour l'ordre Lex. Voir aussi [Laz92 ; Bar04].)

Enfin, une dernière méthode, lorsque k est un corps fini et que l'on connaît déjà la fonction zeta de B_k (par exemple si B_k est construite via la méthode CM, ou en appliquant l'algorithme de Schoof étendu aux variétés abéliennes [Pil90 ; AH96]), est de l'utiliser pour calculer la ℓ-torsion de B_k. On cherche la plus petite extension k_1 de k, telle que tous les points de ℓ-torsion de B_k soient définis sur k_1. Soit d le cardinal de $B_k(k_1)$, que l'on décompose en $d = d_0\ell^i$, avec d_0 premier à ℓ. Alors si P est un point aléatoire de B_k, il existe $j \leqslant i$ tel que $[\ell^j d_0].P$ soit un point de ℓ-torsion (non forcément primitif). En tirant suffisamment de points au hasard dans B_k, on finit par retrouver une base de $B_k[\ell]$.

Si B_k est la Jacobienne d'une courbe hyperelliptique H de genre g sur un corps fini k, on a ainsi un autre algorithme (probabiliste) polynomial en ℓ (et en le nombre d'opérations sur le corps k) pour calculer des ℓ-isogénies. Tout d'abord on calcule la fonction zeta associée à H, ce qui peut se faire en temps polynomial grâce à l'algorithme de Schoof (l'adaptation pour passer du comptage de points au calcul de toute la fonction zeta est facile puisque l'algorithme de Schoof calcule le polynôme caractéristique du Frobenius). On calcule ensuite dans quelle extension vivent les points géométriques de ℓ-torsion. Comme $B_k[\ell]$ est un groupe rationnel de degré ℓ^{2g}, on travaille dans une extension de degré polynomial en ℓ. Comme H est une courbe hyperelliptique, on peut prendre des points géométriques aléatoires sur H au prix d'une racine carrée, donc en temps polynomial, et en tirant g points on obtient un point sur la Jacobienne B_k en coordonnées de Mumford. Une fois tiré assez de points (un nombre polynomial en ℓ), on peut reconstituer une base (en coordonnées de Mumford) de la ℓ-torsion de B_k. Il suffit ensuite de la transformer en coordonnées thêta, et d'appliquer les algorithmes de ce chapitre, qui sont en temps polynomial. Cette méthode est plus efficace que la précédente lorsque ℓ est grand, ou que l'on peut disposer de la fonction zeta de B_k facilement (parce que B_k est généré par la méthode CM, ou parce que k est de petite caractéristique).

7.7 GRAPHES D'ISOGÉNIES

Une application possible des algorithmes présentés dans ce chapitre est le calcul de graphes d'isogénies. Pour cela il nous faut calculer des isogénies représentées par des thêta null points qui vivent dans le même espace modulaire $\mathcal{M}_{\overline{n}}$. On a vu jusqu'à présent comment calculer des ℓ-isogénies en passant d'un thêta null point dans $\mathcal{M}_{\overline{n}}(\overline{k})$ à un thêta null point dans $\mathcal{M}_{\overline{\ell n}}(\overline{k})$. Le théorème de l'isogénie quant à lui permet de calculer explicitement une isogénie en passant d'un thêta null point dans $\mathcal{M}_{\overline{\ell n}}(\overline{k})$ à un thêta null point dans $\mathcal{M}_{\overline{n}}(\overline{k})$. En combinant les deux techniques, on peut ainsi calculer des ℓ^2-isogénies tout en restant dans l'espace modulaire $\mathcal{M}_{\overline{n}}$ (voir la figure 7.1). On peut ainsi construire des graphes de ℓ^2-isogénies.

Si l'on reprend l'algorithme 7.3.2 dans ce cadre, en combinant le corollaire 6.2.8 et les remarques 6.4.3 et 7.3.1, on peut faire l'observation suivante :

PROPOSITION 7.7.1. *Soit K un sous-groupe isotrope maximal de $B_k[\ell]$, et $\{T_{e_1}, \dots, T_{e_g}\}$ une base de K. Alors il y a bijection entre les choix d'excellents points de ℓ-torsion au-dessus de $\{T_{e_i}, T_{e_i} + T_{e_j} \mid i, j \in [1..g]\}$ effectués dans l'algorithme 7.3.2 et les ℓ^2-isogénies de noyau isotrope (pour $e_{\mathcal{L}_0^{\ell^2}}$) contenant K.*

DÉMONSTRATION : Soit $A_k := B_k/K$, et $\widehat{\pi} : B_k \to A_k$ l'isogénie correspondante. Une ℓ^2 isogénie $B_k \to C_k$ dont le noyau contient K se factorise par A_k. Soit $\pi : A_k \to B_k$ l'isogénie contragrédiente de $\widehat{\pi}$. Alors il y a bijection entre les ℓ^2 isogénies $B_k \to C_k$ de noyau isotrope et les isogénies $A_k \to C_k$ dont le noyau est un supplémentaire isotrope de $\operatorname{Ker}\pi$ dans $A_k[\ell]$.

Maintenant, soit $\Theta_{\mathcal{L}}$ une thêta structure sur $(A_k, \pi^*\mathcal{L}_0)$ telle que le thêta null point $(a_i)_{i\in Z(\delta)}$ associé soit dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$. Alors la décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ induite par la thêta structure est de la forme sur la ℓ-torsion de A_k : $K(\mathcal{L})[\ell] = K_1(\mathcal{L})[\ell] \oplus \operatorname{Ker}\pi$. La section 6.3 montre que les autres thêta null points dans $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ qui correspondent à $(A_k, \mathcal{L})$ sont issus de l'action des automorphismes compatibles de $\mathcal{H}(\overline{\ell n})$ donnés par le lemme 6.3.1. Soit $\psi \in \mathfrak{H}$ un tel automorphisme, qui stabilise les $\pi_i((a_i)_{i\in Z(\delta)})$. Alors $\overline{\psi}$ change la décomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ en une décomposition $K(\mathcal{L}) = K_1(\mathcal{L})' \oplus K_2(\mathcal{L})$, et comme la décomposition de $K(\mathcal{L})[n]$ est fixée puisqu'elle doit s'envoyer via π sur la décomposition de $K(\mathcal{L}_0)$ donnée par $(b_i)_{i\in Z(\delta_0)}$, on voit que les actions de tels ψ sont en bijection avec les sous-groupes isotropes supplémentaire à $K_2(\mathcal{L})[\ell]$ dans $A_k[\ell]$.

Or ψ agit sur les $\widetilde{\pi}_i((a_i)_{i\in Z(\delta)})$ en les multipliant par des racines ℓ-ièmes de l'unité, et il y a bijection entre ces actions et le choix des excellents points de ℓ-torsion effectués dans l'algorithme 7.3.2, ce qui conclut. ■

REMARQUE 7.7.2. Lorsqu'on construit des graphes d'isogénies, on se restreint en général à des isogénies rationnelles, ou, ce qui revient au même, aux isogénies dont le noyau est rationnel. Soit $K \subset B_k[\overline{k}]$ le noyau d'une isogénie, on suppose qu'il existe $i_0 \in \delta_0$ telle que $\vartheta_{i_0}(x) \neq 0$ pour tout $x \in K$. En normalisant cette coordonnée à 1 (ce qui est possible car B_k est une variété projective), on construit ensuite les polynômes $P_i = \prod_{x\in K}(X - \vartheta_i(x))$ pour $i \in Z(\delta)\backslash\{i_0\}$. Alors K est rationnel si et seulement si les P_i le sont.

Cependant, il peut arriver que pour construire les coordonnées thêta d'une variété B_k définie sur k, on doive prendre une extension finie k_1 de k (voir la section 3.7). La méthode précédente permet de déterminer uniquement les noyaux k_1-rationnels. On peut contourner cette situation par deux méthodes différentes. Si on est en genre 2 (ou 1), et que l'on a une isogénie $\pi : B_{k_1} \to C_{k_1}$ entre variétés abéliennes marquées de niveau 2 ou 4, alors on peut calculer les invariants de C_{k_1} et regarder s'ils sont k_1-rationnels. Plus généralement, si B_k est la jacobienne d'une courbe hyperelliptique, on peut calculer les équations du noyau K en

coordonnées de Mumford (qui sont k-rationnelles), et utiliser les formules de [Wam99] pour passer des coordonnées de Mumford en coordonnées thêta (k_1-rationnelles) de niveau 2 ou 4.◊

On peut noter deux avantages à passer par l'étape intermédiaire A_k lors du calcul d'une ℓ^2-isogénie $B_k \to C_k$ faisant partie du graphe de ℓ^2-isogénies. Comme A_k est donné par un thêta null point de niveau ℓn, on connaît toute la ℓ-torsion de A_k. En la projetant sur C_k via π_2 (avec les notations de la figure 7.1), on retrouve le noyau de l'isogénie contragrédiente $\widehat{\pi}_2$ de π_2 (la situation est exactement symétrique via l'automorphisme $\mathfrak{I}$ de l'isogénie $\pi : A_k \to B_k$). Ceci nous permet lorsqu'on construit une nouvelle ℓ^2-isogénie partant de C_k, de choisir uniquement des isogénies dont le noyau est d'intersection vide avec $\operatorname{Ker}\widehat{\pi}_2$. On peut s'assurer que la composée de ces deux isogénies est bien une ℓ^4-isogénie, et pas par exemple en genre 2 une $(1, \ell^2, \ell^2, \ell^4)$-isogénie.

De plus, la connaissance de $\operatorname{Ker}\widehat{\pi}_2$ permet d'accélérer le calcul de la ℓ-torsion de C_k. En effet, si $(G_1, \cdots, G_g)$ en est une base, et $\mathcal{L}'_0$ est le fibré sur C_k induit par la thêta structure de niveau n, alors le système donné par l'idéal de ℓ-torsion de C_k et des relations $e_{\mathcal{L}'_0}(G_i, \cdot) = 1$ pour $i \in [2..g]$, est de degré ℓ^{g+1}. De plus, ce système peut être écrit explicitement grâce aux algorithmes 4.4.10 et 5.4.2. Soit H_1 un point solution non multiple de G_1 (il suffit de tester que $e_{\mathcal{L}'_0}(G_1, H_1) \neq 1$). On peut alors construire un système de degré ℓ^g donné toujours par l'idéal de ℓ-torsion sur C_k, et des relations $e_{\mathcal{L}'_0}(G_i, \cdot) = 1$ pour $i \in [1..g] \setminus \{2\}$, ainsi que de la relation $e_{\mathcal{L}'_0}(H_1, \cdot) = 1$, et chercher une solution non multiple de G_2. En continuant ce procédé, on peut construire une base $H_1, \cdots, H_g$ d'un supplémentaire isotrope de $\operatorname{Ker}\pi_2$ en résolvant des systèmes de degrés ℓ^{g+1}, ℓ^g, …, ℓ^2. Il est plus rapide de procéder ainsi que de résoudre directement l'idéal de ℓ-torsion sur C_k de degré ℓ^{2g} (si $g > 1$).

EXEMPLE 7.7.3 (GRAPHE DE $(9,9)$ D'ISOGÉNIES EN GENRE 2). Soit $k = \mathbb{F}_{17}$ et C la courbe hyperelliptique associée au polynôme[1]

$$10x^6 + 15x^5 + 6x^4 + 11x^3 + 11x^2 + 14x + 16$$

L'anneau d'endomorphisme de la Jacobienne J de C est l'ordre maximal, on s'attend donc à ce qu'il y ait deux $(3,3)$-isogénies partant de J. Si on calcule le graphe de $(9,9)$-isogénie, on constate qu'effectivement on obtient un cycle (d'ordre 3) de Jacobiennes dont les invariants d'Igusa sont

$$\{(13,12,11), (6,7,2), (5,1,7)\}.$$ ◊

EXEMPLE 7.7.4 (GRAPHE DE $(25,25)$ ISOGÉNIES EN GENRE 2). Soit $k = \mathbb{F}_{3^6}$, et t une racine du polynôme (primitif) $X^6 + 2X^4 + X^2 + 2X + 2$ sur $\mathbb{F}_3$. Soit C la courbe hyperelliptique associée au polynôme[2]

$$f = t^{693}x^6 + t^{421}x^5 + t^{657}x^4 + t^{610}x^3 + t^{31}x^2 + t^{67}x + t^{29}.$$

L'anneau d'endomorphisme de la Jacobienne J de C a pour indice $(\mathbb{Z}/5\mathbb{Z})^2$ dans l'ordre maximal. On s'attend donc à ce qu'il y ait beaucoup de $(5,5)$-isogénies rationnelles. En traçant le graphe de $(25,25)$-isogénies, on constate effectivement qu'il y en a 175. On trouvera dans la figure 7.4 la liste des invariants d'Igusa correspondant à des Jacobiennes de courbes $(25,25)$-isogènes à J. ◊

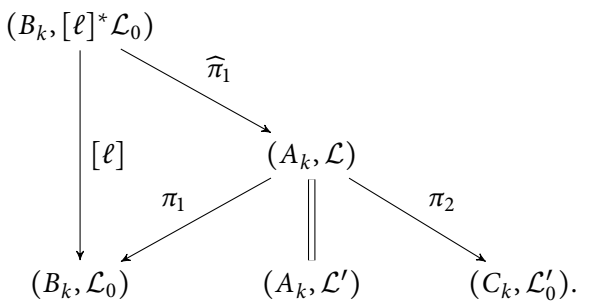
1. Cet exemple m'a été fourni par Gaëtan BISSON. 2. Cet exemple m'a été fourni par David KOHEL.

$$(t^{137}, t^{603}, t^{696}), (t^{527}, t^{476}, t^{20}), (t^{329}, t^{676}, t^{579}), (t^{551}, t^{564}, t^{491}), (t^{157}, t^{224}, t^{450}), (t^{145}, t^{476}, t^{585}), (t^{115}, t^{495}, t^{34}), (t^{713}, t^{68}, t^{453}),$$
$$(t^{337}, t^{646}, t^{87}), (t^{367}, t^{239}, t^{353}), (t^{693}, t^{649}, t^{179}), (t^{409}, t^{501}, t^{406}), (t^{59}, t^{603}, t^{64}), (t^{679}, t^{83}, t^{579}), (t^{377}, t^{291}, t^{368}), (t^{581}, t^{74}, t^{404}),$$
$$(t^{651}, t^{309}, t^{654}), (t^{221}, t^{614}, t^{552}), (t^{121}, t^{25}, t^{429}), (t^{523}, t^{373}, t^{331}), (t^{585}, t^{566}, t^{639}), (t^{681}, t^{299}, t^{681}), (t^{185}, t^{427}, t^{629}), (t^{587}, t^{334}, t^{415}),$$
$$(t^{89}, t^{41}, t^{122}), (t^{159}, t^{465}, t^{667}), (t^{639}, t^{708}, t^{598}), (t^{259}, t^{152}, t^{10}), (t^{543}, t^{668}, t^{685}), (t^{417}, t^{639}, t^{314}), (t^{689}, t^{590}, t^{120}), (t^{227}, t^{401}, t^{169}),$$
$$(t^{571}, t^{577}, t^{331}), (t^{675}, t^{472}, t^{551}), (t^{3}, t^{707}, t^{339}), (t^{77}, t^{255}, t^{612}), (t^{617}, t^{719}, t^{496}), (t^{459}, t^{416}, t^{70}), (t^{553}, t^{552}, t^{245}), (t^{267}, t^{585}, t^{62}),$$
$$(t^{455}, t^{143}, t^{516}), (t^{717}, t^{213}, t^{716}), (t^{3}, t^{535}, t^{31}), (t^{503}, t^{439}, t^{209}), (t^{689}, t^{683}, t^{573}), (t^{233}, t^{362}, t^{684}), (t^{213}, t^{16}, t^{273}), (t^{281}, 2, t^{322}),$$
$$(t^{715}, t^{330}, t^{86}), (t^{415}, t^{215}, t^{71}), (t^{295}, t^{480}, t^{485}), (t^{63}, t^{627}, t^{560}), (t^{305}, t^{90}, t^{595}), (t^{173}, t^{134}, t^{386}), (t^{271}, t^{32}, t^{143}), (t^{501}, t^{465}, t^{502}),$$
$$(t^{523}, t^{526}, t^{540}), (t^{443}, t^{327}, t^{510}), (t^{359}, t^{341}, t^{407}), (t^{399}, t^{470}, t^{355}), (t^{13}, t^{690}, t^{265}), (t^{449}, t^{149}, t^{371}), (t^{463}, t^{586}, t^{724}), (t^{477}, t^{547}, t^{96}),$$
$$(t^{31}, t^{664}, t^{557}), (t^{185}, t^{248}, t^{402}), (t^{505}, t^{553}, t^{496}), (t^{69}, t^{84}, t^{23}), (t^{675}, t^{421}, t^{118}), (t^{113}, t^{218}, t^{642}), (t^{609}, t^{36}, t^{74}), (t^{235}, t^{568}, t^{536}),$$
$$(t^{277}, t^{613}, t^{623}), (t^{243}, t^{668}, t^{235}), (t^{705}, t^{571}, t^{541}), (t^{617}, t^{75}, t^{29}), (t^{609}, t^{496}, t^{82}), (t^{161}, t^{693}, t^{673}), (t^{281}, t^{704}, t^{648}), (t^{37}, t^{338}, t^{29}),$$
$$(t^{209}, t^{546}, t^{100}), (t^{339}, t^{518}, t^{459}), (t^{227}, t^{653}, t^{494}), (t^{397}, t^{539}, t^{693}), (t^{635}, t^{393}, t^{82}), (t^{649}, t^{400}, t^{581}), (t^{197}, t^{171}, t^{102}), (t^{543}, t^{384}, t^{576}),$$
$$(t^{543}, t^{141}, t^{371}), (t^{135}, t^{117}, t^{432}), (t^{217}, t^{522}, t^{560}), (t^{103}, t^{499}, t^{490}), (t^{437}, t^{504}, t^{698}), (t^{599}, t^{543}, t^{692}), (t^{379}, t^{365}, t^{582}), (t^{193}, t^{310}, t^{488}),$$
$$(t^{685}, t^{90}, t^{508}), (t^{145}, t^{144}, t^{677}), (t^{473}, t^{178}, t^{447}), (t^{255}, t^{144}, t^{323}), (t^{131}, t^{400}, t^{255}), (t^{3}, t^{400}, t^{418}), (t^{181}, t^{486}, t^{7}), (t^{63}, t^{424}, t^{481}),$$
$$(t^{463}, t^{489}, t^{103}), (t^{533}, t^{420}, t^{60}), (t^{315}, t^{337}, t^{566}), (t^{341}, t^{675}, t^{202}), (t^{303}, t^{402}, t^{490}), (t^{607}, t^{721}, t^{712}), (t^{163}, t^{315}, t^{317}), (t^{503}, t^{674}, t^{243}),$$
$$(t^{679}, t^{604}, t^{312}), (t^{707}, t^{558}, t^{66}), (t^{329}, t^{626}, t^{173}), (t^{687}, t^{644}, t^{362}), (t^{5}, t^{148}, t^{262}), (t^{613}, t^{478}, t^{334}), (t^{483}, t^{695}, t^{165}), (t^{643}, t^{278}, t^{414}),$$
$$(t^{511}, t^{466}, t^{670}), (t^{343}, t^{208}, t^{83}), (t^{417}, t^{625}, t^{475}), (t^{605}, t^{228}, t^{95}), (t^{523}, t^{180}, t^{522}), (t^{539}, t^{481}, t^{473}), (t^{469}, t^{379}, t^{147}), (t^{593}, t^{724}, t^{389}),$$
$$(t^{405}, t^{648}, t^{91}), (t^{163}, t^{505}, t^{185}), (t^{297}, t^{649}, t^{421}), (t^{169}, t^{411}, t^{632}), (t^{147}, t^{288}, t^{308}), (t^{615}, t^{453}, t^{494}), (t^{187}, t^{117}, t^{251}), (t^{331}, t^{654}, t^{283}),$$
$$(t^{441}, t^{301}, t^{74}), (t^{337}, t^{264}, t^{707}), (t^{185}, t^{106}, t^{713}), (t^{127}, t^{172}, t^{72}), (t^{221}, t^{110}, t^{623}), (t^{299}, t^{594}, t^{457}), (t^{175}, t^{274}, t^{410}), (t^{217}, t^{646}, t^{122}),$$
$$(t^{155}, t^{59}, t^{578}), (t^{25}, t^{699}, t^{416}), (t^{77}, t^{127}, t^{480}), (t^{559}, t^{176}, t^{215}), (t^{545}, t^{679}, t^{598}), (t^{53}, t^{37}, t^{344}), (t^{183}, t^{712}, t^{465}), (t^{241}, t^{643}, t^{42}),$$
$$(t^{3}, t^{165}, t^{370}), (t^{483}, t^{80}, t^{526}), (t^{343}, t^{354}, t^{116}), (t^{111}, t^{585}, t^{206}), (t^{427}, t^{363}, t^{413}), (t^{147}, t^{630}, t^{244}), (t^{261}, t^{441}, t^{8}), (t^{341}, t^{17}, t^{467}),$$
$$(t^{599}, t^{365}, t^{83}), (t^{133}, t^{449}, t^{172}), (t^{111}, t^{247}, t^{701}), (t^{497}, t^{107}, t^{537}), (t^{533}, t^{585}, t^{497}), (t^{129}, t^{683}, t^{533}), (t^{247}, t^{154}, t^{53}), (t^{205}, t^{607}, t^{537}),$$
$$(t^{421}, t^{560}, t^{464}), (t^{467}, t^{37}, t^{396}), (t^{395}, t^{207}, t^{477}), (t^{503}, t^{72}, t^{144}), (t^{571}, t^{191}, t^{661}), (t^{185}, t^{184}, t^{10}), (t^{603}, t^{543}, t^{183})$$

FIGURE 7.4 – Invariants des courbes hyperelliptiques $(25, 25)$-isogènes à C

7.8 FORMULES DE CHANGEMENT DE NIVEAU

On a vu dans la section 7.7, que si on voulait représenter les variétés abéliennes par des points modulaires de même niveau, on était restreint à calculer des ℓ^2-isogénies. Si l'on reprend les notations de la figure 7.1, B_k et C_k sont représentées par un point modulaire de niveau $\overline{n}$, et A_k par un point modulaire de niveau $\overline{\ell n}$. Regardons plus en détail le cas $\ell = 2$: si on revient aux formules de duplication du corollaire 4.3.7, on constate qu'elles donnent des relations entre les fonctions thêta de niveau $\overline{n}$ et celles de niveau $2\overline{n}$. On peut donc calculer des 2-isogénies ainsi : on part du thêta null point $(b_i)_{i\in Z(\delta_0)}$ associé à B_k, et on utilise les formules de duplication pour le relever en un thêta null point $(b'_i)_{i\in Z(2\overline{n})} \in \mathcal{M}_{2\overline{n}}$. À partir de $(b'_i)_{i\in Z(2\overline{n})} \in \mathcal{M}_{2\overline{n}}$, on peut facilement calculer une 2-isogénie $B_k \to A_k$, où A_k est représenté par un point modulaire de niveau $\overline{n}$, en utilisant le théorème 3.6.4 et l'exemple 3.6.5. Cela donne la méthode de l'AGM [Meso1]. L'autre solution est de calculer le point modulaire $(a_i)_{i\in Z(2\overline{n})} \in \mathcal{M}_{2\overline{n}}$ représentant A_k, et de le descendre en un point modulaire via les formules de duplication (dans le diagramme suivant $\mathcal{L}'$ est l'unique fibré totalement symétrique sur A_k tel que $\mathcal{L}'^2 = \mathcal{L}$) :



Pour généraliser cette situation, il nous faut trouver des formules de ℓ-duplication, c'est-à-dire des formules reliant les thêta null points de niveau δ d'une variété abélienne $(A_k, \mathcal{L})$ aux thêta null points de niveau $\ell\delta$ de la variété abélienne polarisée $(A_k, \mathcal{L}^\ell)$. Pour cela on va appliquer le théorème 4.3.5. Pour simplifier, on se restreint au cas où $\delta = \overline{n}$. Il nous faut trouver une matrice F telle que ${}^tFF = \ell\,\mathrm{Id}$, on a alors ${}^tF(n\,\mathrm{Id})F = \ell n\,\mathrm{Id}$. Si $\ell = a^2 + b^2$, on peut prendre

$$F = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

Le cas $\ell = 2, a = b = 1$ redonne alors les formules de duplication du corollaire 4.3.7. Plus généralement, si on a $\ell = a^2 + b^2 + c^2 + d^2$ on peut prendre la matrice issue des quaternions :

$$F = \begin{pmatrix} a & b & c & d \\ d & -c & b & -a \\ c & d & -a & -b \\ b & -a & -d & c \end{pmatrix}.$$

THÉORÈME 7.8.1. *Soit $(b_i)_{i\in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}$ un point géométrique correspondant à la variété abélienne marquée de niveau n, $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$. Soit $(a_i)_{i\in Z(\overline{\ell n})} \in \phi_1^{-1}((b_i)_{i\in Z(\overline{n})})$ correspondant à la variété abélienne marquée de niveau ℓn, $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$; il existe donc un sous-groupe isotrope maximal $K \subset B_k[\ell]$ tel que $A_k = B_k/K$. Alors il existe un fibré $\mathcal{L}'$ sur A_k tel que $\mathcal{L} = \mathcal{L}'^{\ell}$ et une thêta structure symétrique $\Theta_{\mathcal{L}'}$ sur $G(\mathcal{L}')$ uniquement déterminés par $\Theta_{\mathcal{L}}$. Soit $(a'_i)_{i\in Z(\overline{n})}$ le thêta null point associé à $\Theta_{\mathcal{L}'}$, alors si $F \in \mathrm{M}_r(\mathbb{Z})$ satisfait ${}^tF.F = \ell.\,\mathrm{Id}$, on a :*

$$a'_{i_1} \dots a'_{i_r} = \sum_{\substack{j_1,\dots,j_r \in Z(\overline{\ell n}) \\ F(j_1,\dots,j_r)=(i_1,\dots,i_r)}} a_{j_1} \dots a_{j_r}. \tag{7.7}$$

De plus, si ℓ est impair, alors l'équation (7.7) est invariante sous l'action du groupe $\mathfrak{H}$ des automorphismes symétriques compatibles de $\mathcal{H}(\overline{\ell n})$ (voir la section 6.3). Donc $(a'_i)_{i\in Z(\overline{n})}$ est uniquement déterminé par $(b_i)_{i\in Z(\overline{n})}$ et $K_0 = \pi(K_1(\mathcal{L}))$.

DÉMONSTRATION : La thêta structure $\Theta_{\mathcal{L}}$ est entièrement déterminée par une base symplectique de $A_k[\ell n]$ et une décomposition symplectique (compatible) de $A_k[2\ell n]$ par la proposition 4.3.1. Comme $A_k[\ell] \subset K(\mathcal{L})$, il existe un fibré $\mathcal{M}$ sur A_k tel que $\mathcal{L} = \mathcal{M}^\ell$. On prend pour $\mathcal{L}'$ l'unique fibré totalement symétrique dans la classe d'équivalence de $\mathcal{M}$, et pour $\Theta_{\mathcal{L}'}$ la thêta structure symétrique induite par la décomposition de $A_k[2n]$ et la base symplectique compatible de $A_k[n]$ issues des décompositions précédentes.

Par définition de $\Theta_{\mathcal{L}'}$ on peut appliquer les formules d'addition du théorème 4.3.5 à l'isogénie $f : A_k^r \to A_k^r$ issue de la matrice F. On obtient alors l'équation (7.7), à un facteur projectif près, mais comme d'habitude, on a supposé que l'on prenait un relevé affine du thêta null point tel que ce facteur projectif soit égal à 1. Comme f est une isogénie, tout élément de $Z(\overline{n})^r$ est l'image par F d'un élément de $Z(\overline{\ell n})^r$ (ce que l'on peut voir directement on constatant que $\ell : Z(\overline{\ell n}) \to Z(\overline{n})$ est surjectif, et que par définition ${}^tF.F = \ell\,\mathrm{Id}$). L'équation (7.7) nous donne donc des formules explicites de changement de niveau : par exemple, il suffit de l'appliquer avec $i_1 = i \in Z(\overline{n})$ et $i_2, \dots, i_r = 0$.

Il reste à vérifier que l'équation (7.7) est invariante par l'action de $\mathfrak{H}$ lorsque ℓ est impair. Si on revient à la définition de $\mathfrak{H}$ donnée dans la section 6.3, il faut montrer que $(a'_i)_{i\in Z(\overline{n})}$ est entièrement déterminé par le choix d'un sous-groupe isotrope maximal K_0 de $B_k[\ell n]$ tel que $K_0[\ell] = K$ et $K_0[n] = K_1(\mathcal{L}_0)$ (voir le théorème 6.2.7 et la remarque 7.3.1). Cela peut se faire purement formellement, et c'est l'approche que nous suivrons dans le corollaire 7.8.2

pour traiter également le cas ℓ pair. Cependant, pour une implémentation effective calculant directement $(a'_i)_{i\in Z(\overline{n})}$ sans passer par le point intermédiaire $(a_i)_{i\in Z(\overline{\ell n})}$, il est intéressant de le vérifier directement sur l'équation (7.7).

Ici ψ agit diagonalement sur le r-uplet J.

Si $\psi \in \mathfrak{H}$ donne une action de permutation (6.8), et provient d'un automorphisme ψ_0 de $Z(\overline{\ell n})$ fixant $Z(\overline{n})$, soit $I = (i_1, \dots, i_r)$ et $J = (j_1, \dots, j_r)$, tels que $A.J = I$. On a clairement $A.\psi(J) = \psi(I) = I$, donc l'action de ψ permute les éléments de la somme dans l'équation (7.7). Si $\psi \in \mathfrak{H}$ provient d'une action diagonale (6.9), alors ψ laisse invariant chaque monôme apparaissant dans la somme de l'équation (7.7). En effet, l'action de ψ sur $(a_i)_{i\in Z(\overline{\ell n})}$ est de la forme $\psi.a_i = \lambda_i a_i$. Soit $(e_1, \dots, e_g)$ la base canonique de $Z(\overline{\ell n})$. Les actions (6.9) sont engendrées par $\lambda_{\sum m_u e_u} = \zeta^{m_{u_1} m_{u_2}}$ où $u_1, u_2 \in \{1..g\}$ et ζ est une racine ℓ-ième de l'unité (voir la proposition 6.4.2). Si $A.J = I$, on pose $\lambda_J \coloneqq \lambda_{j_1} \times \dots \times \lambda_{j_r}$. Il nous faut montrer que $\lambda_J = 1$. Si $u_1 = u_2$, on peut par linéarité se ramener au cas où $g = 1, u_1 = 1$, on a alors $J = (j_1)$ et $I = (i_1)$ et $\lambda_J = \zeta^{{}^t j_1 . j_1}$. Comme $A.j_1 = i_1$, on a ${}^t i_1 . i_1 = {}^t j_1 {}^t A A j_1 = \ell {}^t j_1 j_1$. Mais de plus comme $i_1 \in Z(\overline{n})^r$, il existe $i' \in Z(\overline{\ell n})^r$ tel que $i_1 = \ell i'$. Donc ${}^t i_1 . i_1 = \ell^2 {}^t i' . i'$, et on en tire ${}^t j_1 j_1 = \ell {}^t j' . j'$. On en déduit bien que $\lambda_J = 1$. Si $u_1 \neq u_2$, on peut se ramener au cas $g = 2, u_1 = 1, u_2 = 2$, on a alors $\lambda_J = \zeta^{{}^t j_1 . j_2}$, et on peut refaire les mêmes calculs que précédemment.

Enfin, si l'on revient aux formules de Vélu de la section 7.3, on sait que le point $(a_i)_{i\in Z(\overline{\ell n})}$ est entièrement déterminé par le groupe K_0, ainsi qu'un choix de numérotation de K_0 et des éléments λ_i. Mais ces deux derniers choix découlent d'une action de $\mathfrak{H}$, donc n'affectent pas $(a'_i)_{i\in Z(\overline{n})}$ par ce qui précède. Ainsi $(a'_i)_{i\in Z(\overline{n})}$ dépend uniquement de K_0. ■

COROLLAIRE 7.8.2. *Supposons que le corps k soit parfait (de caractéristique différente de n). Soit $B_k[2n] = K_1(\mathcal{L}_0^2) \oplus K_2(\mathcal{L}_0^2)$ la décomposition symplectique donnant le thêta null point symétrique de niveau n, $(b_i)_{i\in Z(\overline{n})}$ sur $(B_k, \mathcal{L}_0)$. Alors le point $(a'_i)_{i\in Z(\overline{n})}$ est uniquement déterminé par le choix d'un sous-groupe isotrope maximal $\mathfrak{K}$ de $B_k[2\ell n]$ tel que $\mathfrak{K}[\ell] = K$ et $\mathfrak{K}[2n] = K_1(\mathcal{L}_0^2)$ (en reprenant les notations du théorème 7.8.1), et si ℓ est impair $(a'_i)_{i\in Z(\overline{n})}$ est même uniquement déterminé par $\mathfrak{K}[\ell n]$. Ainsi si $\mathfrak{K}$ est rationnel, le point $(a'_i)_{i\in Z(\overline{n})}$ est également rationnel. Si de plus ℓ est premier à n, $(a'_i)_{i\in Z(\overline{n})}$ est uniquement déterminé par le noyau K de $\widehat{\pi}$, et est rationnel si K est rationnel.*

DÉMONSTRATION : Si k est parfait, soit $\mathfrak{K}$ un sous-groupe isotrope maximal satisfaisant les conditions du corollaire 7.8.2. Si $\mathfrak{K}$ est rationnel, le noyau $K = \mathfrak{K}[\ell]$ l'est également, ainsi que l'isogénie associée $\widehat{\pi} : B_k \to A_k$. En transportant $\mathfrak{K}$ et $K_2(\mathcal{L}_0^2)$ par $\widehat{\pi}$, on obtient une décomposition symplectique rationnelle de $K(\mathcal{L}'^2)$, qui induit une décomposition de $K(\mathcal{L}')$. De même, en transportant le morphisme $\hat{Z}(\overline{n}) \to K_2(\mathcal{L}_0)$ induit par la thêta structure $\Theta_{\mathcal{L}_0}$, on obtient un morphisme $\hat{Z}(\overline{n}) \to K_2(\mathcal{L}')$, rationnel puisque le point $(b_i)_{i\in Z(\overline{n})}$ et $\widehat{\pi}$ le sont. On en déduit que le morphisme dual $Z(\overline{n}) \to K_1(\mathcal{L}')$ est rationnel (voir la section 3.7). Au final, le point $(a'_i)_{i\in Z(\overline{n})}$ induit par ces structures est rationnel par la proposition 4.7.6, et est entièrement déterminé par $\mathfrak{K}$. De plus, si ℓ est impair, $\mathfrak{K}$ est uniquement déterminé par $\mathfrak{K}[\ell n]$ et le groupe isotrope maximal $K_1(\mathcal{L}_0^2)$ de $B_k[2n]$ (en effet le produit fibré $Z(\overline{\ell n}) \times_{Z(\overline{n})} Z(\overline{2n})$ est isomorphe à $Z(\overline{2\ell n})$). Comme ce dernier groupe est rationnel si $(b_i)_{i\in Z(\overline{n})}$ l'est, $\mathfrak{K}$ est rationnel si $\mathfrak{K}[\ell n]$ l'est.

Si ℓ est premier à n, alors $\mathfrak{K}$ est entièrement déterminé par $K_1(\mathcal{L}_0^2)$ et par le noyau K, donc $(a'_i)_{i\in Z(\overline{n})}$ est entièrement déterminé par K (et par le thêta null point $(b_i)_{i\in Z(\overline{n})}$). ■

À titre de comparaison, en reprenant la même preuve, on constate que le point $(a_i)_{i\in Z(\overline{\ell n})}$ est lui déterminé par le choix d'une base symplectique de $B_k[\ell n]$ et d'un sous-groupe isotrope maximal $\mathfrak{K}$ de $B_k[2\ell^2 n]$ tel que $\mathfrak{K}[\ell] = K$, choix compatible avec la base symplectique de

$B_k[n]$ et la décomposition symplectique de $B_k[2n]$ induites par la thêta structure symétrique $\Theta_{\mathcal{L}_0}$.

ALGORITHME 7.8.3 (FORMULES DE VÉLU EN NIVEAU CONSTANT) :
Soit $(B_k, \mathcal{L}_0, \Theta_{\mathcal{L}}(\overline{n}))$ une variété abélienne marquée de niveau n et ℓ un nombre premier à n. Soit K un sous-groupe isotrope maximal de $B_k[\ell]$, et $\widehat{\pi} : B_k \to A_k$ l'isogénie associée.

Entrées $T_{d_1}, \cdots T_{d_g}$ une base du noyau K.
Sortie Les coordonnées $(a'_i)_{i\in Z(\overline{n})}$, un thêta null point de niveau n correspondant à A_k.

- ➔ Appliquer l'algorithme 7.3.2 pour calculer (les coordonnées compressées) du thêta null point de niveau ℓn : $(a_i)_{i\in Z(\overline{\ell n})}$. Cependant à la dernière étape de cet algorithme (en reprenant les notations), on ne calcule pas explicitement une racine ℓ-ième $\alpha_i^{\frac{1}{\ell}}$, mais on travaille dans l'algèbre $\mathscr{A} = \overline{k}[\alpha_i^{\frac{1}{\ell}}]_{i\in\mathfrak{S}}$.
- ➔ Décompresser le point $(a_i)_{i\in Z(\overline{\ell n})}$ en utilisant l'algorithme 4.6.8.
- ➔ Soit $F \in \mathrm{M}_r(\mathbb{Z})$ une matrice telle que ${}^tF.F = \ell\,\mathrm{Id}$. Pour tout $i \in Z(\overline{n})$, retourner

$$a'_i = a'^{1-r}_0 \sum_{\substack{j_1,\ldots,j_r \in Z(\overline{\ell n}) \\ F(j_1,\ldots,j_r)=(i,0,\ldots,0)}} a_{j_1} \ldots a_{j_r}.$$

(Le calcul du membre de droite se fait dans $\mathscr{A}$, mais le théorème 7.8.1 et le corollaire 7.8.2 montrent que le résultat est dans k si K est k-rationnel.) ♢

ANALYSE DE COMPLEXITÉ 7.8.4. Le calcul des coordonnées non compressées $(a_i)_{i\in Z(\overline{\ell n})}$ nécessite $O(\ell^g)$ chaînes d'addition dans B_k. Comme $F : Z(\overline{\ell n}) \to Z(\overline{n})$ est surjective, chaque indice $i \in Z(\overline{n})$ a ℓ^g antécédents, donc le calcul de $(a'_i)_{i\in Z(\overline{n})}$ à partir de $(a_i)_{i\in Z(\overline{\ell n})}$ nécessite $(n\ell)^g \times r$ multiplications dans le corps k_0 de définition des points géométriques de K. (Dans la description de l'algorithme 7.8.3, le calcul se fait dans l'algèbre $\mathscr{A}$, mais il est facile en pratique de se ramener à des opérations dans k_0.) ♢

On sait que le point $(a'_i)_{i\in Z(\overline{n})}$ donné par l'algorithme 7.8.3 ne dépend pas de la base choisie pour K, et est rationnel si K l'est. Ceci montre qu'il devrait être possible d'améliorer cet algorithme pour travailler dans k, et uniquement à partir d'une base de Gröbner de l'idéal d'annulation de K, c'est-à-dire sans avoir à calculer les points géométriques de K. Une possibilité est de procéder ainsi : soit I l'idéal associé à K dans l'algèbre $k[\vartheta_i]_{i\in Z(\overline{n})}$. Soit G une base de Gröbner pour l'idéal I par rapport à l'ordre lexicographique. On suppose que la base G est trigonale. (Si i_0 est la variable de poids le plus fort, cela impose que ϑ_{i_0} sépare les points géométriques de K. Si l'on procède à un changement de variable linéaire aléatoire sur les coordonnées $(\vartheta_i)_{i\in Z(\overline{n})}$, la base G sera bien trigonale « génériquement ».) Soit $P_1(x_1) \in G$ le polynôme univarié en la coordonnée ϑ_{i_0}. Soit T_1 le point « générique » de K tel que $\vartheta_{i_0}(T_1) = x_1$. On calcule formellement dans le corps $k(x_1)$ les points $T_1, 2.T_1, \ldots, (\ell-1).T_1$, et l'on forme le polynôme $R = \prod_{j\in\{1..\ell\}}(x_1 - \vartheta_{i_0}(j.T_1))$. On calcule alors le polynôme $P_2(x_2)$ tel que $P_2.R = P_1$ dans l'extension $k(x_1)$. Soit T_2 le point « générique » de K tel que $\vartheta_{i_0}(T_2) = x_2$. On calcule formellement dans le corps $k(x_1, x_2)$ les points $j_1T_1 + j_2T_2$ pour $j_1, j_2 \in \{1..\ell\}$, et on procède par récurrence ainsi jusqu'à avoir une base formelle $T_1, \ldots, T_g$. En fait, cette méthode revient à calculer un corps de décomposition du polynôme P_1, en utilisant la loi d'addition sur B_k (et le fait que K soit un groupe) pour accélérer les calculs.

Il faut de plus noter que si l'on se fixe une variété abélienne principalement polarisée B_k, un thêta null point de niveau n associé $(b_i)_{i\in Z(\overline{n})}$ n'est pas forcément rationnel. On peut appliquer la même stratégie que dans la remarque 7.7.2 pour calculer des isogénies k-rationnelles.

REMARQUE 7.8.5. L'isogénie $\widehat{\pi} : B_k \to A_k$ s'exprime également facilement dans la base des fonctions thêta de A_k induite par le thêta null point $(a'_i)_{i\in Z(\overline{n})}$. En effet, en reprenant les notations de la formule de changement de niveau du théorème 7.8.1, on a si $F.X = Z$:

$$\vartheta_{i_1}^{\mathcal{L}'}(z_1)\dots\vartheta_{i_r}^{\mathcal{L}'}(z_r) = \sum_{\substack{j_1,\dots,j_r\in Z(\overline{\ell n})\\ F(j_1,\dots,j_r)=(i_1,\dots,i_r)}} \vartheta_{j_1}^{\mathcal{L}}(x_1)\dots\vartheta_{j_r}^{\mathcal{L}}(x_r), \tag{7.8}$$

où $X = (x_1,\dots,x_r)$ et $Z = (z_1,\dots,z_r)$ sont des points géométriques de A_k^r.

Soit $y \in \widetilde{B}_k$ un point géométrique, et x un antécédent de y par $\widetilde{\pi}$. On veut calculer $(\vartheta_i^{\mathcal{L}_0}(z))_{i\in Z(\overline{n})}$ pour $z = \ell.x$. Dans l'équation (7.8), on pose $Z = (z, 0, \dots, 0)$, et on prend $X = {}^tF.(x, 0, \dots, 0)$. On a bien $F.X = Z$, et on peut appliquer l'équation (7.8). De plus, on sait déterminer x à une action près des racines ℓ-ièmes de l'unité par le théorème 7.2.1, mais comme ${}^tF.F = \ell\,\mathrm{Id}$, on vérifie immédiatement que le membre de droite est invariant par cette action, en faisant le même raisonnement que dans le théorème 7.8.1.

Par exemple, si $\ell = a^2 + b^2$, et $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, on a alors $X = (ax, -bx)$. On peut se ramener à $g = 1$, et si $x = (x_i)_{i\in Z(\overline{\ell n})}$ un autre point antécédent $x' = (x'_i)_{i\in Z(\overline{\ell n})}$ de y est de la forme $x'_i = \zeta^i x_i$ où ζ est une racine ℓ-ième de l'unité ($i \in Z(\overline{\ell n})$). Mais si $(i_1, i_2) = F(j_1, j_2)$, avec $i_1, i_2 \in Z(\overline{n})$, on a :

$$\begin{aligned}\vartheta_{j_1}^{\mathcal{L}}(ax')\vartheta_{j_2}^{\mathcal{L}}(bx') &= \zeta^{aj_1-bj_2}\vartheta_{j_1}^{\mathcal{L}}(ax)\vartheta_{j_2}^{\mathcal{L}}(bx)\\ &= \zeta^{i_1}\vartheta_{j_1}^{\mathcal{L}}(ax)\vartheta_{j_2}^{\mathcal{L}}(bx)\\ &= \vartheta_{j_1}^{\mathcal{L}}(ax)\vartheta_{j_2}^{\mathcal{L}}(bx)\end{aligned}$$

comme $i_1 \in Z(\overline{n})$. Donc l'équation (7.7) ne dépend pas du point x choisi.

On peut facilement adapter l'algorithme 7.2.4 pour calculer l'isogénie $\widehat{\pi}$ explicitement en niveau n. Il suffit de généraliser la méthode utilisée pour passer de l'algorithme 7.3.2 à l'algorithme 7.8.3. ◇

EXEMPLE 7.8.6 (CHANGEMENT DE NIVEAU EN GENRE 1). Soit E la courbe elliptique d'équation $y^2 = x^3 + 12x + 43$ sur le corps $\mathbb{F}_{59}$. Un thêta null point de niveau 4 associé à E est donné par $(51 : 1 : 21 : 1)$. On a $E(\mathbb{F}_{59}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$. En effet, le thêta null point est rationnel, mais les racines primitives quatrièmes de l'unité ne vivent pas dans $\mathbb{F}_{59}$. La rationalité du thêta null point implique alors uniquement la rationalité de tous les points de 2-torsion, ainsi que des points d'un sous-groupe isotrope maximal de la 4-torsion.

On construit $\mathbb{F}_{59^4} = \mathbb{F}_{59}[t]/(t^4 + 43t^3 + 20t^2 + 20t + 38)$. Soit $P = (20t^3 + 13t^2 + t + 10, 19t^3 + 36t^2 + 4t + 26, 17t^3 + 23t + 35, 1)$. P est un point de 5-torsion, correspondant au point $(18t^3 + 19t^2 + 23t + 27, 43t^3 + 47t^2 + 27t + 41)$ sur E en coordonnées de Weierstrass. Le Frobenius envoie P sur $2.P$, donc le noyau K engendré par P est rationnel. Ainsi, si un thêta null point de niveau 20 correspondant à P va vivre dans l'extension $\mathbb{F}_{59^{4\times5}}$, en appliquant le théorème 7.8.1 pour descendre de niveau, on obtient qu'un thêta null point de niveau 4 correspondant à E/K est donné par $(17 : 1 : 22 : 1)$. Une équation de Weierstrass (associée à ce thêta null point par les formules de Thomae inverses) pour la courbe elliptique E/K est

$$y^2 = x^3 + 58x + 6.$$ ◇

EXEMPLE 7.8.7 (GRAPHE DE $(7,7)$-ISOGÉNIES EN GENRE 2). On construit $\mathbb{F}_{3^6} = \mathbb{F}_3[t]/(t^6 -$

$t^4 + t^2 - t - 1$). Soit H la courbe hyperelliptique d'équation[1]

$$y^2 = t^{254} \cdot x^6 + t^{223} \cdot x^5 + t^{255} \cdot x^4 + t^{318} \cdot x^3 + t^{668} \cdot x^2 + t^{543} \cdot x + t^{538}.$$

En se servant de la fonction zeta de la courbe H pour calculer la 7-torsion en coordonnées de Mumford sur la Jacobienne J associée, on constate qu'il y a un seul sous-groupe isotrope maximal rationnel. En convertissant ce sous-groupe en coordonnées thêta, et en appliquant l'algorithme 7.8.3, on obtient que la variété abélienne isogène et la Jacobienne de la courbe

$$y^2 = t^{395} \cdot x^6 + t^{257} \cdot x^5 + t^{327} \cdot x^4 + t^{140} \cdot x^3 + t^{554} \cdot x^2 + t^{268} \cdot x + t^{326}. \qquad \diamond$$

7.8.1 *Changement de niveau et espaces modulaires*

On a vu comment utiliser les formules d'addition pour « descendre de niveau » : si $(B_k, \mathcal{L}_0)$ est une variété abélienne polarisée et $\mathcal{L}_0$ un fibré totalement symétrique de niveau n, alors étant donné un thêta null point associé à une thêta structure sur $\mathcal{L}_0^\ell$, on sait exprimer grâce au théorème 7.8.1 un thêta null point associé à une thêta structure (induite par la précédente) sur $\mathcal{L}_0$. On a également vu comment descendre de niveau en prenant une isogénie dans la section 3.6, et monter de niveau en prenant une isogénie dans la section 7.3.

Pour conclure, on peut se demander s'il est possible de « monter de niveau », tout en restant sur la même variété, à la différence de l'approche du chapitre 6. Soit $(b_i)_{i\in Z(\overline{n})}$ le thêta null point associé à une thêta structure symétrique sur $\mathcal{L}_0$, si l'on suppose que ℓ est premier à n et que l'on a calculé toutes les coordonnées (en niveau n) des points de $B_k[\ell]$, alors il suffit d'écrire toutes les équations de la forme (7.8) faisant intervenir des points de ℓ-torsion dans le membre de gauche, puis de résoudre le système. En fait, il est plus simple de réutiliser les résultats de la section 7.3. Si l'on part d'un thêta null point $(b_i)_{i\in Z(\overline{n})}$ associé à une variété abélienne $(B_k, \mathcal{L}_0)$, on peut appliquer deux fois les formules de Vélu. La première fois pour calculer un thêta null point $(a_i)_{i\in Z(\overline{\ell n})}$ correspondant à $(A_k, \mathcal{L})$ à partir de $(b_i)_{i\in Z(\overline{n})}$, de telle sorte que le morphisme $\pi : A_k \to B_k$ associé soit de type $\hat{Z}(\overline{\ell})$. La seconde fois, on applique à nouveau les formules de Vélu au point $(a_i)_{i\in Z(\overline{\ell n})}$, pour obtenir un thêta null point correspondant à $(B_k, [\ell]\mathcal{L}_0)$ (voir la figure 7.1). En effet, l'isogénie contragrédiente $\widehat{\pi}$ est de type $Z(\overline{\ell})$. Le thêta null point correspondant à $(B_k, [\ell]\mathcal{L}_0)$ est de niveau $\ell^2 n$, il suffit alors d'appliquer les formules de changement de niveau pour retrouver le thêta null point de niveau ℓn correspondant à $(B_k, \mathcal{L}_0^\ell)$. On peut faire mieux en évitant le calcul intermédiaire d'un thêta null point de niveau $\ell^2 n$: à partir de $(a_i)_{i\in Z(\overline{\ell n})}$, on calcule le point de niveau n associé $(a'_i)_{i\in Z(\overline{n})}$ comme dans le théorème 7.8.1, et on applique les formules de Vélu à ce point-là pour obtenir directement le thêta null point associé à $(B_k, \mathcal{L}_0^\ell)$. (Les résultats de la section 7.3 expliquent comment calculer un thêta null point correspondant à une $\hat{Z}(\overline{\ell})$ isogénie, mais comme d'habitude il suffit d'appliquer l'action de permutation $\mathfrak{I}$ pour obtenir les résultats correspondants pour la $Z(\overline{\ell})$-isogénie $\widehat{\pi}$). La situation est résumée dans la figure 7.5.

On peut interpréter cette figure dans le cadre des espaces modulaires ainsi. Dans la remarque 6.4.3, on a montré que si ℓ est premier à n, alors prendre un point de $\mathcal{M}_{\overline{\ell n}}(\overline{k})/\mathfrak{H}_1$ revenait à choisir une variété abélienne A_k, une thêta structure symétrique de niveau n sur A_k, et une décomposition symplectique de la ℓ-torsion $A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2$. On peut alors considérer les thêtas structures de niveau n induites sur $A_k/A_k[\ell]_2$ et $A_k/A_k[\ell]_1$, on obtient alors la correspondance modulaire ϕ_1 et ϕ_2 respectivement. Prendre un point de

1. Cet exemple m'a été fourni par David Kohel.

$\mathcal{M}_{\overline{\ell n}}(\overline{k})/\mathfrak{H}$ revient à choisir un sous groupe isotrope maximal K de $A_k[\ell]$. En effet, l'action de $\mathfrak{H}_2$ donne les groupes isotropes supplémentaires de K. Ainsi ϕ_1 se factorise par $\mathcal{M}_{\overline{\ell n}}(\overline{k})/\mathfrak{H}$, et cet espace est isomorphe à $\mathcal{M}_{\overline{n}}(\overline{k})(\ell)$, l'espace modulaire des variétés abéliennes marquées munies d'un sous groupe isotrope maximal de la ℓ-torsion. On a un autre morphisme de $\mathcal{M}_{\overline{n}}(\overline{k})(\ell) \to \mathcal{M}_{\overline{n}}$ qui est simplement le morphisme d'oubli et est donné par le théorème 7.8.1. On a donc une correspondance modulaire $\mathcal{M}_{\overline{n}}(\ell) \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ qui généralise la correspondance $X_0(\ell n) \to X_0(n) \times X_0(n)$ introduite dans la section 6.1. On voit qu'à l'instar des formules de Vélu, on obtient une généralisation complète de la correspondance modulaire sur les courbes elliptiques en considérant les formules de changement de niveau. Malheureusement, on ne dispose pas des équations de l'espace $\mathcal{M}_{\overline{n}}(\ell) = \mathcal{M}_{\overline{\ell n}}/\mathfrak{H}$, ce qui nous empêche de l'utiliser en pratique (il faut revenir à la correspondance $\phi : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$). On peut consulter la figure 7.6 pour un résumé.

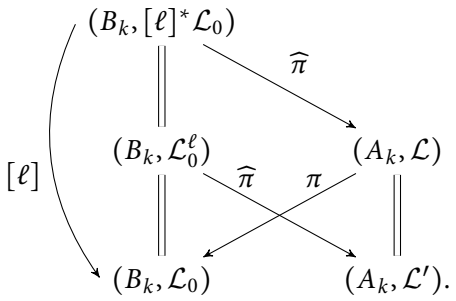


FIGURE 7.5 – Changement de niveau et isogénies

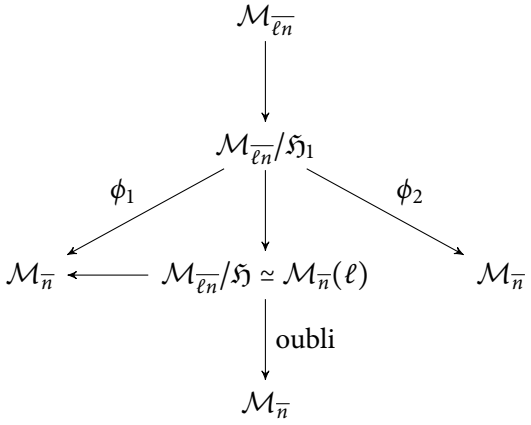


FIGURE 7.6 – Changement de niveau et espaces modulaires

8 PERSPECTIVES

MATIÈRES

8.1 INTRODUCTION

Le but de ce chapitre est de discuter de quelques perspectives des résultats obtenus dans cette thèse, ainsi que des suggestions d'améliorations possibles. On a déjà vu quelques perspectives possibles, par exemple concernant l'amélioration de l'arithmétique des courbes, regarder si la formule de triplication permet d'obtenir des formules d'addition efficaces[1] sur les fonctions thêta de niveau 3, et notamment de voir s'il est possible d'être plus rapide en genre 2 que l'arithmétique basée sur les coordonnées de Mumford, sans se restreindre aux surfaces de Kummer[2]. Une autre approche serait de regarder si des quotients de fonction thêta permettent de généraliser les coordonnées d'Edwards en genre 2. On peut également se poser la question d'améliorer l'évaluation des pairings, on s'est demandé dans le chapitre 5 s'il était possible d'étendre l'algorithme 5.4.2 pour calculer des pairings optimaux.

Dans la section 8.2 nous donnons des perspectives concernant le calcul d'isogénie. La section 8.2.1 présentent des idées pour calculer la correspondance modulaire décrite dans la section 7.8.1 et la figure 7.6. La section 8.2.2 donne des perspectives pour rendre encore plus efficace l'emploi du niveau 2, et la section 8.2.3 donne quelques perspectives offertes par le calcul explicite d'isogénies. Enfin dans la section 8.3, on rappelle les travaux de Carls [Car03] qui font suite à une idée de Mestre [Mes01] pour calculer le relevé canonique d'une variété abélienne ordinaire grâce aux relations entre fonctions thêtas. Ceci permet de compléter le panorama des outils offerts par les fonctions thêta. En effet, le calcul du relevé canonique peut être utilisé pour calculer les polynômes de classe ou faire du comptage de points (si la caractéristique est petite). On peut alors se demander s'il est possible d'utiliser les résultats du chapitre 7 pour améliorer le calcul du relevé p-adique du thêta null point. Si le Frobenius n'est pas une isogénie séparable, en revanche le Verschiebung l'est (puisque la variété est supposée ordinaire), et on peut lui appliquer les techniques du chapitre 7.

1. Il est facile d'obtenir des formules d'addition en niveau 3 en utilisant plusieurs fois la formule de triplication, exactement comme on obtient les relations de Riemann à partir de la formule de duplication. Mais ces formules ne sont pas efficaces algorithmiquement.
2. Dans cet optique, nous avons récemment travaillé sur des formules d'addition en niveau $(2,4)$, ce qui permet d'être plus rapide que le niveau 4, tout en gardant un plongement de la variété abélienne lorsque le fibré est sans point base.

8.2 AMÉLIORATIONS DU CALCUL D'ISOGÉNIE

8.2.1 *Polynômes modulaires*

La correspondance modulaire du chapitre 6 $\phi : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ est facile à exprimer parce que les espaces modulaires considérés marquent les variétés abéliennes avec beaucoup de structure, mais en conséquence, si $(b_i)_{i\in Z(\overline{n})}$ est un point géométrique de $\mathcal{M}_{\overline{n}}$ correspondant à une variété B_k, les points géométriques de la fibre $\phi_1^{-1}((b_i)_{i\in Z(\delta_0)})$ correspondent à des variétés A_k ℓ-isogènes à B_k *et* (lorsque ℓ est premier à n). à au choix d'une base symplectique de la ℓ-torsion $A_k[\ell]$ compatible avec l'isogénie, dans le sens du corollaire 6.2.8.

Ainsi, comme on l'a remarqué dans le chapitre 6, les fibres de la correspondance modulaire sont de degré bien plus grand que le nombre d'isogénies. Ceci explique pourquoi l'algorithme le plus efficace pour calculer des isogénies est donné dans le chapitre 7 par des formules à la Vélu, qui nécessitent de calculer toute la ℓ-torsion. Mais si l'on a déjà calculé la ℓ-torsion, on peut directement calculer la trace du Frobenius dessus, autrement dit les résultats du chapitre 7 ne sont pas suffisants pour améliorer l'algorithme de Schoof en genre supérieur pour le comptage de points.

Cependant, on a vu dans la section 7.8 comment combiner les formules de Vélu généralisées et les formules de changement de niveau pour calculer des ℓ-isogénies tout en restant en niveau n. On aimerait alors exprimer directement une correspondance modulaire en niveau n. Si l'on reprend les notations de la section 7.8, il suffit formellement d'exprimer les relations d'isogénie entre $(a_i)_{i\in Z(\overline{\ell n})}$ et $(b_i)_{i\in Z(\overline{n})}$, ainsi que les relations de changement de niveau entre $(a_i)_{i\in Z(\overline{\ell n})}$ et $(a'_i)_{i\in Z(\overline{\ell n})}$ (où ici ces variables sont vues de manière formelle), et d'éliminer les variables intermédiaires $(a_i)_{i\in Z(\overline{\ell n})}$. Cependant, cela passe par une base de Gröbner très coûteuse, et on aimerait trouver une méthode plus efficace.

Par exemple, on pourrait adopter les mêmes idées que [Suto9] qui calcule les polynômes modulaires en genre 1 par la méthode des restes chinois : on pourrait construire des graphes de ℓ-isogénies sur plusieurs corps finis $\mathbb{F}_p$. Ensuite, on pourrait faire de l'interpolation multivariée pour reconstituer les équations d'une telle correspondance modulaire modulo p, puis utiliser le théorème des restes chinois pour reconstituer des équations sur $\mathbb{Z}$. Pour cela, il nous faudrait analyser le degré des polynômes de cette correspondance modulaire, et surtout la hauteur de leurs coefficients. On pourrait aussi utiliser l'approche analytique comme dans [Engo9], en calculant les relations entre les fonctions modulaires (sur le demi-espace de Siegel) $\vartheta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega/n)$ et $\vartheta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](0,\Omega/\ell n)$. Là encore, cette approche passe par une borne sur la hauteur des coefficients entre les polynômes modulaires sur ces invariants, pour savoir jusqu'à quelle précision il faut pousser le développement de Fourier.

Enfin, on peut essayer de construire directement la variété quotient $\mathcal{M}_{\overline{\ell n}}/\mathfrak{H}$, en cherchant des variables invariantes par l'action de $\mathfrak{H}$, mais qui permettent de garder trace de l'application $\mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}}$ (voir la figure 7.6).

8.2.2 *Équations pour l'espace modulaire et les variétés de Kummer en niveau* 2

On a vu dans le chapitre 4 et la seconde partie tout l'intérêt de travailler avec des points modulaires de niveau 2. Une autre raison de travailler en niveau 2 est de minimiser le problème de rationalité (voir la section 3.7). En effet, même si on arrive à écrire directement les polynômes modulaires en niveau n, cela restreint les applications aux variétés abéliennes telles qu'un thêta null point de niveau n associé soit rationnel (voir la discussion à la fin de la section 7.8).

Si $4 \mid \delta$, l'espace modulaire $\mathcal{M}_\delta/\operatorname{Aut}(\mathcal{H}(\delta))$ représente les variétés abéliennes sur k munies d'une polarisation de type δ. D'où l'intérêt de trouver des équations pour $\mathcal{M}_{\bar{2}}$, que l'on

peut voir par exemple en genre 2 comme l'espace modulaire lié aux thêta structures le plus proche de l'espace modulaire donné par les invariants d'Igusa. En particulier, il serait très utile d'avoir une correspondance modulaire sur $\mathcal{M}_{\overline{2}}$ pour le calcul d'isogénies. De plus, on pourrait chercher des invariants modulaires sur $\mathcal{M}_{\overline{2}}$ stables par l'action de $\mathrm{Aut}(\mathcal{H}(\overline{2}))$, donnant donc des invariants équivalents à ceux d'Igusa en genre 2. Même en genre 2 de tels invariants seraient intéressants, s'ils permettent de réduire la taille des coefficient des polynômes modulaires associés, par rapport à ceux liés aux invariants d'Igusa.

Cependant, les théorèmes 4.7.1 et 4.7.2 ne sont plus valides dans ce cas, les relations de l'équation (4.30) étant triviales en niveau 2. Par conséquent, pour obtenir[1] un thêta null point de niveau 2, il faut choisir un thêta null point de niveau 4, puis le projeter en niveau 2 (ou utiliser les formules de duplication du théorème 4.4.3 pour rester sur la même variété abélienne). Si on suppose que ce thêta null point correspond à une variété abélienne marquée $(A_k, \mathcal{L}, \Theta_{\mathcal{L}})$, avec $\mathcal{L}$ le carré d'un fibré irréductible sur A_k, on peut se demander s'il est possible de retrouver les équations de la variété de Kummer associée à A_k (voir la section 4.8) à partir de ce thêta null point. Les équations de Riemann (4.30) provenant des formules d'addition ($x = \texttt{chain\_add}(x, 0, x)$), on peut chercher de telles formules pour déterminer ces équations. Par exemple, en dimension 2, la formule d'addition

$$2x = \texttt{chain\_add}(x, x, 0)$$

semble convenir expérimentalement.

Une autre application serait la suivante : la variété projective $\overline{\mathcal{M}}_\delta$ contient des points géométriques dégénérés. On a vu dans le théorème 6.3.6 que si l'on a un critère pour reconnaître les points modulaires dégénérés de niveau δ_0, avec δ_0 divisible par un entier pair $n \geqslant 4$, alors on a un critère pour reconnaître les points modulaires dégénérés de niveau δ avec $\delta_0 \mid \delta$. Il serait intéressant d'étendre ce théorème au cas du niveau 2. Pour cela, il suffit de généraliser la proposition 6.3.2 au cas du niveau 2. Mais si les relations d'additions $2x = \texttt{chain\_add}(x, x, 0)$ suffisent à caractériser les points sur la variété de KUMMER, on peut reprendre la preuve de la proposition 6.3.2 *mutatis mutandis* (il faut supposer de plus que les coordonnées de tous les points de ℓ-torsion de B_k sont non nuls pour que les pseudo-additions ne donnent pas des relations triviales).

8.2.3 *Applications du calcul d'isogénies*

Maintenant que l'on a un algorithme effectif de calcul d'isogénies, on peut essayer de généraliser en dimension supérieure les algorithmes utilisant des isogénies sur une courbe elliptique :

1. Calcul de l'anneau d'endomorphisme d'une variété abélienne.
2. Calcul du polynôme de classe de Hilbert par la méthode du reste chinois (plutôt qu'en prenant un relevé canonique comme dans la section 8.3).

Pour ces applications, la seule difficulté consiste à comprendre le graphe d'isogénies associé à une variété abélienne X, qui peut être plus compliqué qu'en genre 1 où l'on a un beau volcan d'isogénies [FM02]. Par exemple dans [BGL09], les auteurs utilisent des graphes de $(3,3)$-isogénies en genre 2 pour la méthode de la multiplication complexe en genre 2. Dans cet article, le graphe de $(3,3)$-isogénies est calculé en cherchant des relations sur les coefficients de Fourier des fonctions thêta de niveau 4 analytiques : $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, \Omega)$ et $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, 3\Omega)$.

1. Bien sûr, si on a une courbe hyperelliptique, on peut aussi utiliser les formules de Thomae de l'algorithme 4.7.5.

Une autre application est le transfert de logarithme discret. Par exemple, si C est une courbe hyperelliptique de genre 3, et que l'on prend une isogénie « au hasard » $f : \mathrm{Jac}(C) \to A$, alors il y a de grandes chances que la variété abélienne A soit la Jacobienne d'une courbe non hyperelliptique (en genre 3, toute variété abélienne principalement polarisée est une Jacobienne, mais à la différence du genre 2, *génériquement* une courbe de genre 3 n'est pas hyperelliptique). Or on a des algorithmes plus efficaces pour calculer le logarithme discret de la Jacobienne d'une telle courbe. [Smi09] utilise cette idée en calculant des courbes C' telles qu'il existe une $(2,2,2)$-isogénies entre $\mathrm{Jac}(C)$ et $\mathrm{Jac}(C')$. Cependant, comme il est restreint à des $(2,2,2)$-isogénies, il n'est pas sûr de pouvoir tomber sur une courbe non hyperelliptique. En augmentant le degré des isogénies, on pourrait augmenter cette probabilité. Malheureusement les algorithmes du chapitre 7 calculent des isogénies directement sur les variétés abéliennes. Or on n'a pas d'équivalents pratiques de la formule de Thomae de l'exemple 4.7.4 pour une courbe non hyperelliptique. Il nous faudrait une méthode s'appliquant dans le cas où on a une Jacobienne d'une courbe C donnée par ses thêta null points pour reconstituer C lorsqu'elle n'est pas hyperelliptique. Or dans l'article [Sheo8], l'auteur donne des formules à la Thomae pour des courbes non hyperelliptiques. Il serait intéressant de regarder si d'une il est possible de les implémenter efficacement, et d'autre part s'il est possible d'inverser ces formules pour retrouver la courbe à partir d'un thêta null point.

8.3 RELEVÉ CANONIQUE D'UNE VARIÉTÉ ABÉLIENNE

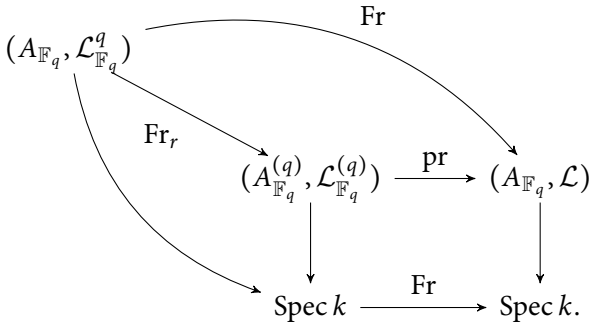
Satoh a introduit dans [Satoo] l'idée de compter des points sur une courbe elliptique en calculant son relevé canonique. L'idée d'utiliser les formules de duplication pour calculer ce relevé canonique en caractéristique 2 vient de Mestre [Meso1 ; Meso2]. Très sommairement, l'idée générale est la suivante : on part d'une variété abélienne $A_{\mathbb{F}_{2^n}}$ ordinaire définie sur le corps fini $\mathbb{F}_{2^n}$. Soit $\mathbb{Z}_{2^n}$ l'anneau 2-adique des vecteurs de Witt de $\mathbb{F}_{2^n}$, et σ un relevé à $\mathbb{Z}_{2^n}$ du (petit) Frobenius sur $\mathbb{F}_{2^n}$. Alors si on prend un relevé quelconque $A^0_{\mathbb{Z}_{2^n}}$ de $A_{\mathbb{F}_{2^n}}$ sur $\mathbb{Z}_{2^n}$, et que l'on considère la suite d'isogénies $\sigma_i : A^i_{\mathbb{Z}_{2^n}} \to A^{i+1}_{\mathbb{Z}_{2^n}}$ qui relèvent le Frobenius $\mathrm{Fr}_2 : A^i_{\mathbb{F}_{2^n}} \to A^{i+1}_{\mathbb{F}_{2^n}}$, (les j-invariants de) la suite $A^i_{\mathbb{Z}_{2^n}}$ convergent vers le relevé canonique $A^c_{\mathbb{Z}_{2^n}}$ de $A_{\mathbb{F}_{2^n}}$ [LST64]. Une fois calculé $A^c_{\mathbb{Z}_{2^n}}$ (disons avec suffisamment de précision), on peut calculer un relevé du (grand) Frobenius $\mathrm{Fr}_{2^n} : A_{\mathbb{F}_{2^n}} \to A_{\mathbb{F}_{2^n}}$ à $A^c_{\mathbb{Z}_{2^n}} \to A^c_{\mathbb{Z}_{2^n}}$, comme composé du relevé de n petits Frobenius.

Or on peut calculer ces relevés du Frobenius (on général on prend plutôt le Verschiebung qui est plus pratique car séparable) grâce aux formules de duplication. En genre 1 on retrouve la moyenne arithmético-géométrique [BM88], et en genre 2 les suites de Borchardt [Dupo6].

En pratique on procède un peu différemment, par exemple en genre 1, si R représente l'ensemble des formules de duplication, on cherche à relever le j-invariant de $A_{\mathbb{F}_{2^n}}$ en un élément j_c de $\mathbb{Z}_{2^n}$ qui vérifie $R(j_c^\sigma, j_c) = 0$. Ce j-invariant correspond alors au relevé canonique de $A_{\mathbb{F}_{2^n}}$. L'avantage de cette méthode est que l'on peut calculer le relevé de ce j-invariant via un algorithme de Newton multivarié, qui a une convergence quadratique, alors que la convergence donnée par la suite d'isogénie précédente est seulement linéaire. De plus une fois que l'on a calculé le relevé canonique $A^c_{\mathbb{Z}_{2^n}}$, il suffit de regarder l'action du relevé du petit Frobenius sur l'espace tangent. En effet, si cette action est la multiplication par λ, l'action donnée par le Frobenius Fr_2^i est donnée par $\sigma^i\lambda$. On peut donc retrouver la trace du Frobenius comme la norme de λ. Pour plus de détails, on peut consulter par exemple [LLo3 ; LLo6].

On a vu que l'algorithme de Mestre venait de la formule de duplication sur les fonctions thêta. Plus généralement, Carls a montré dans [Caro3 ; Caro7 ; Caro5] les faits suivants qui servent à calculer le relevé canonique d'une variété abélienne $(A_{\mathbb{F}_q}, \mathcal{L}_{\mathbb{F}_q})$ définie sur un corps

fini $\mathbb{F}_q$ (de caractéristique $p > 2$), en calculant un relevé *canonique* des thêta null points associés à $(A_{\mathbb{F}_q}, \mathcal{L}_{\mathbb{F}_q})$. Soit $(A^c_{\mathbb{Z}_q}, \mathcal{L})$ le relevé canonique d'une variété abélienne ordinaire $(A_{\mathbb{F}_q}, \mathcal{L}_{\mathbb{F}_q})$, où $\mathcal{L}_{\mathbb{F}_q}$ est un fibré de type $Z(\overline{n})$, avec n premier à p. Soit Fr_r le Frobenius relatif donné par le diagramme :



Il existe un unique fibré $\mathcal{L}^{(q)}$ sur $A^{(q)}_{\mathbb{Z}_q}$ tel que $\mathrm{Fr}^*\,\mathcal{L}^{(q)} = \mathcal{L}^q$ et $\mathcal{L}^{(q)_{\mathbb{F}_q}} = \mathrm{pr}^*\mathcal{L}_{\mathbb{F}_q}$ [Caro7, Théorème 5.1]. Soit $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ un relevé du Frobenius $\mathrm{Fr} : \mathbb{F}_q \to \mathbb{F}_q$. Si $\Theta_{\mathcal{L}}(\overline{n})$ est une thêta structure sur $(A^c_{\mathbb{Z}_q}, \mathcal{L})$, elle induit une thêta structure $\Theta_{\mathcal{L}}(\overline{n})^\sigma$ sur $(\sigma(A^c_{\mathbb{Z}_q}), \sigma(\mathcal{L}))$, ainsi qu'une thêta structure $\Theta_{\mathcal{L}}(\overline{n})^{(q)}$ sur $(A^{(q)}_{\mathbb{Z}_q}), \mathcal{L}^{(q)})$. On a alors : $\Theta_{\mathcal{L}}(\overline{n})^{(q)} = \Theta_{\mathcal{L}}(\overline{n})^\sigma$ ([CKLo8, Théorème 2.4]). De même, si $\mathcal{L}$ est principal, et que l'on se fixe un isomorphisme $Z(q) \to A[q]^{\mathrm{etale}}$, on a alors une thêta structure canonique Θ sur $(A^c_{\mathbb{Z}_q}, \mathcal{L}^q)$ par [Caro7, Corollaire 2.2] qui induit donc des thêta structures $\Theta^\sigma : (\sigma(A^c_{\mathbb{Z}_q}), \sigma(\mathcal{L})^q)$, et (en descendant par le Frobenius) : $\Theta^{(q)}$ sur $(A^{(q)}_{\mathbb{Z}_q}, (\mathcal{L}^{(q)})^q)$. On a encore : $\Theta_{\mathcal{L}}(\overline{n})^{(q)} = \Theta_{\mathcal{L}}(\overline{n})^\sigma$ ([Caro5, Théorème 1.1]). On peut combiner les deux approches (voir [CKLo8, Section 3.2]), pour obtenir si $m \in \mathbb{N}$ est premier à q, et $i \in Z(m)$:

$$\vartheta_i^{\mathcal{L}^{qm}}(0) = \sigma(\vartheta_i^{\mathcal{L}^m}(0))$$

(voir par exemple [CKLo8, Théorème 2.1 ; CLo8, Théorème 2.2]). Par exemple, si on a des relations R de changement de niveau q, alors le thêta null point $(a_i)_{i\in Z(\overline{\ell n})}$ du relevé canonique satisfait $R((a_i)_{i\in Z(\overline{\ell n})}, (\sigma(a_i)_{i\in Z(\overline{n})}) = 0$.

Cette idée a été utilisée dans [CKLo8] pour calculer le polynôme de classe de Hilbert (dont on se sert pour la méthode de multiplication complexe) d'un corps CM K de degré 4 (tel que 3 soit totalement décomposé dans K) en prenant le relevé canonique d'une variété abélienne ordinaire de dimension 2 définie sur un corps fini de caractéristique 3, dont l'anneau des endomorphismes est de type CM K. Dans cet article, les auteurs utilisent les formules de changement de niveau données par la matrice

$$F = \begin{pmatrix} 1 & -2 & 0 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \text{on a :} \quad {}^tFF = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

pour obtenir des relations entre les thêta null points de niveau 4, $(a_i)_{i\in Z(\delta)}$ et $\sigma((a_i)_{i\in Z(\overline{4})})$, où $(a_i)_{i\in Z(\overline{4})}$ est le thêta null point associé au relevé canonique. (Bien sûr, si 2 est totalement décomposé dans K, il est plus simple de considérer un relevé d'une variété abélienne définie sur un corps fini de caractéristique 2 pour utiliser les formules de duplication ; voir par exemple [GHK+o6].)

Kempf étudie dans [Kem89, p. 76-77], le cas des relations d'addition données par la matrice

$$F = \begin{pmatrix} 1 & m \\ 1 & n \end{pmatrix}, \quad \text{on a :} \quad {}^tF \begin{pmatrix} i & 0 \\ 0 & j \end{pmatrix} F = \begin{pmatrix} i+j & 0 \\ 0 & im^2 + jn^2 \end{pmatrix}$$

avec $im + jn = 0$. Dans [CLo08], les auteurs appliquent ces formules avec $i = j = 1, m = -n = p$ pour trouver des relations de degré p^2 entre les thêta null points $(a_i)_{i\in Z(\overline{4p})}$ et $\sigma^2(a_i)_{i\in Z(\overline{4p})}$ où $(a_i)_{i\in Z(\overline{4p})}$ est le thêta null point de niveau $\overline{4p}$ du relevé canonique d'une variété abélienne ordinaire sur un corps fini de caractéristique p. La raison pour laquelle les auteurs prennent un thêta null point de niveau $\overline{4p}$ est qu'un tel thêta null point permet facilement de calculer les valeurs propres du Frobenius (voir [CLo08, Théorème 2.8]). L'algorithme de comptage de points obtenu ainsi dans [CLo08] est quasi-quadratique (en le degré du corps fini) et est optimal asymptotiquement par rapport aux autres algorithmes de comptage de points p-adiques. Il serait intéressant de regarder si les formules de changement de niveau de la section 7.8 qui donnent des relations de degré p plutôt que p^2 permettent d'améliorer la constante de cet algorithme. De plus, si on veut utiliser le relevé canonique pour un comptage de points (plutôt que, par exemple, le calcul du polynôme de classe de Hilbert), il faut partir d'un thêta null point de niveau $\overline{4p}$. Dans [CLo08], les auteurs utilisent la correspondance modulaire $\phi : \mathcal{M}_{\overline{4p}} \to \mathcal{M}_{\overline{4}}$ du chapitre 6 pour passer d'un point de niveau $\overline{4}$ en un point de niveau $\overline{4p}$ (qui correspond à une variété isogène, ce qui ne change pas le comptage de points), en calculant directement les points géométriques de la fibre de ϕ. Cette phase d'initialisation est coûteuse, ce qui ne permet de l'appliquer que pour p très petit ($p = 3, 5$), en utilisant les améliorations de [FLR09]. Il pourrait être intéressant d'y appliquer les résultats du chapitre 7 (si A_k est une variété abélienne ordinaire de dimension g sur un corps fini de caractéristique p, alors $A_k[p]$ est de cardinal p^g, ce qui permettrait bien d'appliquer la section 7.3).

BIBLIOGRAPHIE

[AD93] L. Adleman et J. DeMarrais. « A subexponential algorithm for discrete logarithms over all finite fields ». Dans : *Advances in Cryptology—CRYPTO'93*. Springer. 1993, p. 147–158. (Cf. p. 3).

[ADH94] L. Adleman, J. DeMarrais et M. Huang. « A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields ». Dans : *Algorithmic number theory* (1994), p. 28–40. (Cf. p. 7).

[AH96] L. Adleman et M. Huang. « Counting rational points on curves and abelian varieties over finite fields ». Dans : *Algorithmic Number Theory* (1996), p. 1–16. (Cf. p. 162).

[ALNR09] C. Arene, T. Lange, M. Naehrig et C. Ritzenthaler. « Faster computation of Tate pairings ». Dans : *Preprint* (2009). arXiv : 0904.0854. (Cf. p. 105, 126).

[AGV72] M. Artin, A. Grothendieck et J. Verdier. *Théorie des topos et cohomologie étale des schémas. (SGA4)*. 1972. (Cf. p. 10).

[Atk88] A. Atkin. « The number of points on an elliptic curve modulo a prime ». Dans : *manuscript, Chicago IL* (1988). (Cf. p. 12).

[BBC+09] J. Balakrishnan, J. Belding, S. Chisholm, K. Eisentraeger, K. STANGE et E. Teske. « Pairings on hyperelliptic curves ». Dans : *Imprint* (2009). (Cf. p. 9).

[Bar04] M. Bardet. « Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie ». Thèse de doct. 2004. (Cf. p. 162).

[BKLS02] P. Barreto, H. Kim, B. Lynn et M. Scott. « Efficient algorithms for pairing-based cryptosystems ». Dans : *Lecture Notes in Computer Science* (2002), p. 354–368. (Cf. p. 9, 102).

[BN06] P. Barreto et M. Naehrig. « Pairing-friendly elliptic curves of prime order ». Dans : *Selected areas in cryptography*. Springer. 2006, p. 319–331. (Cf. p. 8).

[BGÓS07] P. Barreto, S. Galbraith, C. Ó hÉigeartaigh et M. Scott. « Efficient pairing computation on supersingular abelian varieties ». Dans : *Designs, Codes and Cryptography* 42.3 (2007), p. 239–271. (Cf. p. 125).

[BBJ+08] D. Bernstein, P. Birkner, M. Joye, T. Lange et C. Peters. « Twisted edwards curves ». Dans : *Progress in Cryptology–AFRICACRYPT 2008* (2008), p. 389–405. (Cf. p. 1).

[Ber06] D. Bernstein. « Elliptic vs. hyperelliptic, part 1 ». Dans : *Talk at ECC* (2006). url : http://cr.yp.to/talks/2007.04.25/slides.pdf. (Cf. p. 4, 15, 105).

[BL07a] D. Bernstein et T. Lange. « Elliptic vs. hyperelliptic, part 2 ». Dans : *Talk at ECC* (2007). url : http://cr.yp.to/talks/2007.09.07/slides.pdf. (Cf. p. 4, 15).

[BL07b] D. Bernstein et T. Lange. *Explicit-formulas database*. 2007. url : http://hyperelliptic.org/EFD. (Cf. p. 105).

[BL04] C. Birkenhake et H. Lange. *Complex abelian varieties*. Second. T. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin : Springer-Verlag, 2004, p. xii+635. ISBN : 3-540-20488-1. (Cf. p. 5, 13, 19–21, 25, 27, 29, 31, 33–35, 39, 64, 76, 115, 118).

[BS09] G. Bisson et A. Sutherland. « Computing the endomorphism ring of an ordinary elliptic curve over a finite field ». Dans : *Journal of Number Theory* (2009). (Cf. p. 12).

[BF03] D. Boneh et M. Franklin. « Identity-based encryption from the Weil pairing ». Dans : *SIAM Journal on Computing* 32.3 (2003), p. 586–615. (Cf. p. 7).

[BLS04] D. Boneh, B. Lynn et H. Shacham. « Short signatures from the Weil pairing ». Dans : *Journal of Cryptology* 17.4 (2004), p. 297–319. (Cf. p. 7).

[BCP97] W. Bosma, J. Cannon et C. Playoust. « The Magma algebra system I : The user language ». Dans : *J. Symb. Comput.* 24.3/4 (1997), p. 235–265. (Cf. p. 12, 14).

[BM88] J. Bost et J. Mestre. « Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2 ». Dans : *Gaz. Math* 38 (1988), p. 36–64. (Cf. p. 176).

[BLS09] R. Bröker, K. Lauter et A. Sutherland. « Modular polynomials via isogeny volcanoes ». Dans : *Preprint* (2009). arXiv : 1001.0402. (Cf. p. 12).

[BS09] R. Bröker et A. Sutherland. « An explicit height bound for the classical modular polynomial ». Dans : *The Ramanujan Journal* (2009), p. 1–21. (Cf. p. 12).

[BGL09] R. Bröker, D. Gruenewald et K. Lauter. *Explicit CM-theory in dimension 2*. Oct. 2009. arXiv : 0910.1848. (Cf. p. 175).

[Bro06] R. Bröker. « Constructing elliptic curves of prescribed order ». Dans : (2006). (Cf. p. 13).

[Bru09] P. Bruin. « The Tate pairing for Abelian varieties over finite fields ». Dans : (2009). URL : http://www.math.leidenuniv.nl/~astolk/monday/notes/bruin-tate-pairing.pdf. (Cf. p. 115).

[BLP93] J. Buhler, H. Lenstra et C. Pomerance. « Factoring integers with the number field sieve ». Dans : *The development of the number field sieve* (1993), p. 50–94. (Cf. p. 3).

[Can87] D. Cantor. « Computing in the Jacobian of a hyperelliptic curve ». Dans : *Mathematics of Computation* 48.177 (1987), p. 95–101. (Cf. p. 6).

[CZ81] D. Cantor et H. Zassenhaus. « A new algorithm for factoring polynomials over finite fields ». Dans : *Mathematics of Computation* 36.154 (1981), p. 587–592. (Cf. p. 162).

[Car05] R. Carls. « Galois theory of the canonical theta structure ». Dans : *Preprint* (2005). arXiv : math.NT/0509092. (Cf. p. 176, 177).

[Car07] R. Carls. « Canonical coordinates on the canonical lift ». Dans : *J. Ramanujan Math. Soc.* 22.1 (2007), p. 1–14. (Cf. p. 176, 177).

[CL08] R. Carls et D. Lubicz. « A p-adic quasi-quadratic time and quadratic space point counting algorithm ». Dans : *International Mathematics Research Notices* (2008). (Cf. p. 177, 178).

[Car03] R. Carls. « Generalized AGM sequences and approximation of canonical lifts ». Thèse de doct. Avr. 2003. URL : http://www.math.leidenuniv.nl/carls. (Cf. p. 173, 176).

[CKL08] R. Carls, D. Kohel et D. Lubicz. « Higher-dimensional 3-adic CM construction ». Dans : *J. Algebra* 319.3 (2008), p. 971–1006. ISSN : 0021-8693. DOI : 10.1016/j.jalgebra.2007.11.016. (Cf. p. 12, 177).

[CDL+00] S. Cavallar, B. Dodson, A. Lenstra, W. Lioen, P. Montgomery, B. Murphy, H. Te Riele, K. Aardal, J. Gilchrist, G. Guillerm et al. « Factorization of a 512-bit RSA modulus ». Dans : *Advances in Cryptology—EUROCRYPT 2000*. Springer. 2000, p. 1–18. (Cf. p. 1).

[CSB04] S. Chatterjee, P. Sarkar et R. Barua. « Efficient computation of Tate pairing in projective coordinate over general characteristic fields ». Dans : *Information Security and Cryptology (ICISC'04), Lecture Notes in Computer Science* (2004), p. 168–181. (Cf. p. 9, 126).

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Springer Verlag, 1993. (Cf. p. 102).

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen et F. Vercauteren, éds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, p. xxxiv+808. ISBN : 978-1-58488-518-4 ; 1-58488-518-1. (Cf. p. 6, 115, 116).

[Coh08] P. Cohen. « On the coefficients of the transformation polynomials for the elliptic modular function ». Dans : *Mathematical Proceedings of the Cambridge Philosophical Society*. T. 95. 03. Cambridge University Press. 2008, p. 389–402. (Cf. p. 12).

[Del69] P. Deligne. « Variétés abéliennes ordinaires sur un corps fini ». Dans : *Inventiones Mathematicae* 8.3 (1969), p. 238–243. (Cf. p. 111).

[DG70] M. Demazure et P. Gabriel. *Groupes algébriques*. Masson et Cie, 1970. (Cf. p. 58).

[Die06] C. Diem. « An index calculus algorithm for plane curves of small degree ». Dans : *Algorithmic number theory* (2006), p. 543–557. (Cf. p. 7).

[DT08] C. Diem et E. Thomé. « Index calculus in class groups of non-hyperelliptic curves of genus three ». Dans : *Journal of Cryptology* 21.4 (2008), p. 593–611. (Cf. p. 7).

[DH76] W. Diffie et M. Hellman. « New directions in cryptography ». Dans : *IEEE Transactions on information Theory* 22.6 (1976), p. 644–654. (Cf. p. 1).

[Dup06] R. Dupont. « Moyenne arithmetico-geometrique, suites de Borchardt et applications ». Dans : *These de doctorat, Ecole polytechnique, Palaiseau* (2006). (Cf. p. 12, 176).

[Elk92] N. Elkies. « Explicit isogenies ». Dans : *manuscript, Boston MA* (1992). (Cf. p. 12).

[Eng09] A. Enge. « The complexity of class polynomial computation via floating point approximations ». Dans : *Mathematics of Computation* 78.266 (2009), p. 1089–1107. (Cf. p. 12, 174).

[EG02] A. Enge et P. Gaudry. « A general framework for subexponential discrete logarithm algorithms ». Dans : *Acta Arith* (2002). (Cf. p. 3).

[EGT09] A. Enge, P. Gaudry et E. Thomé. « An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves ». Dans : *Imprint* (2009). (Cf. p. 7).

[FGJ09] X. Fan, G. Gong et D. Jao. « Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates ». Dans : *Selected Areas in Cryptography*. Springer. 2009, p. 34. (Cf. p. 125).

[Fau99] J. Faugère. « A new efficient algorithm for computing Gröbner basis (F4) ». Dans : *Journal of Pure Applied Algebra* 139 (1999), p. 61–88. (Cf. p. 162).

[Fau02] J. Faugère. « A new efficient algorithm for computing Gröbner bases without reduction to zero (F 5) ». Dans : *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*. ACM. 2002, p. 83. (Cf. p. 162).

[FGLM93] J. Faugère, P. Gianni, D. Lazard et T. Mora. « Efficient computation of zero-dimensional Gröbner bases by change of ordering ». Dans : *Journal of Symbolic Computation* 16.4 (1993), p. 329–344. (Cf. p. 162).

[FLR09] J.-C. Faugère, D. Lubicz et D. Robert. *Computing modular correspondences for abelian varieties*. Mai 2009. arXiv : 0910.4668. (Cf. p. viii, 14, 132, 143, 178).

[FM02] M. Fouquet et F. Morain. « Isogeny volcanoes and the SEA algorithm ». Dans : *Algorithmic number theory (Sydney, 2002)*. T. 2369. Lecture Notes in Comput. Sci. Berlin : Springer, 2002, p. 276–291. doi : 10.1007/3-540-45455-1_23. (Cf. p. 12, 175).

[GHV07] S. Galbraith, F. Hess et F. Vercauteren. « Hyperelliptic pairings ». Dans : *Lecture Notes in Computer Science* 4575 (2007), p. 108. (Cf. p. 9).

[GL08] S. Galbraith et X. Lin. « Computing Pairings Using x-Coordinates Only ». Dans : *Designs, Codes and Cryptography* (2008). to appear. (Cf. p. 127).

[Gau04] P. Gaudry. « Algorithmes de comptage de points d'une courbe définie sur un corps fini ». 2004. url : http://www.loria.fr/~gaudry/publis/pano.pdf. (Cf. p. 10).

[Gau07] P. Gaudry. « Fast genus 2 arithmetic based on Theta functions ». Dans : *Journal of Mathematical Cryptology* 1.3 (2007), p. 243–265. (Cf. p. xv, 1, 2, 4, 13, 15, 62, 103, 105).

[Gau08] P. Gaudry. « Algorithmique des courbes algébriques pour la cryptologie ». HDR. Oct. 2008. url : http://www.loria.fr/~gaudry/publis/hdr.pdf. (Cf. p. 4, 6).

[Gau09] P. Gaudry. « Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem ». Dans : *Journal of Symbolic Computation* 44.12 (2009), p. 1690–1702. (Cf. p. 6).

[GG03] P. Gaudry et N. Gurel. « Counting points in medium characteristic using Kedlaya's algorithm ». Dans : *Experimental Mathematics* 12.4 (2003), p. 395–402. (Cf. p. 10).

[GHS02] P. Gaudry, F. Hess et N. Smart. « Constructive and destructive facets of Weil descent on elliptic curves ». Dans : *Journal of Cryptology* 15.1 (2002), p. 19–46. (Cf. p. 6).

[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 ». Dans : *Advances in cryptology—ASIACRYPT 2006*. T. 4284. Lecture Notes in Comput. Sci. Berlin : Springer, 2006, p. 114–129. doi : 10.1007/11935230_8. (Cf. p. 12, 177).

[GL09] P. Gaudry et D. Lubicz. « The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines ». Dans : *Finite Fields and Their Applications* 15.2 (2009), p. 246–260. (Cf. p. xv, 13, 62, 103, 105).

[GS08] P. Gaudry et E. Schost. *Hyperelliptic curve point counting record : 254 bit Jacobian*. Juin 2008. url : http://webloria.loria.fr/~gaudry/record127/. (Cf. p. 162).

[GTTD07] P. Gaudry, E. Thomé, N. Thériault et C. Diem. « A double large prime variation for small genus hyperelliptic index calculus ». Dans : *Mathematics of Computation* 76.257 (2007), p. 475–492. (Cf. p. 7).

[GM07] G. Geer et B. Moonen. « Abelian varieties ». Dans : *Book in preparation* (2007). (Cf. p. 41, 112, 113).

[Gor93] D. Gordon. « Discrete Logarithms in GF(P) Using the Number Field Sieve ». Dans : *SIAM Journal on Discrete Mathematics* 6.1 (1993), p. 124–138. (Cf. p. 3).

[GPSW06] V. Goyal, O. Pandey, A. Sahai et B. Waters. « Attribute-based encryption for fine-grained access control of encrypted data ». Dans : *Proceedings of the 13th ACM conference on Computer and communications security*. ACM. 2006, p. 98. (Cf. p. 7).

[GHO+07] R. Granger, F. Hess, R. Oyono, N. Theriault et F. Vercauteren. « Ate pairing on hyperelliptic curves ». Dans : *Lecture Notes in Computer Science* 4515 (2007), p. 430–447. (Cf. p. 125).

[GD64] A. Grothendieck et J. Dieudonné. « Eléments de géométrie algébrique ». Dans : *Publ. math. IHES* 20.24 (1964), p. 1965. (Cf. p. 27).

[Har00] R. Hartshorne. *Algebraic geometry*. Springer, 2000. (Cf. p. 4, 6, 10, 27, 76).

[Har07] D. Harvey. « Kedlaya's algorithm in larger characteristic ». Dans : *Int. Math. Res. Notices* (2007). (Cf. p. 10).

[Hes08] F. Hess. « Pairing lattices ». Dans : *Pairing-Based Cryptography–Pairing* 5209 (2008), p. 18–38. (Cf. p. 125).

[HSV06] F. Hess, N. Smart et F. Vercauteren. « The Eta pairing revisited ». Dans : *IEEE Transactions on Information Theory* 52.10 (2006), p. 4595–4602. (Cf. p. 125).

[Hoy63] W. Hoyt. « On products and algebraic families of Jacobian varieties ». Dans : *Annals of Mathematics* (1963), p. 415–423. (Cf. p. 7).

[Igu72] J.-i. Igusa. *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. New York : Springer-Verlag, 1972, p. x+232. (Cf. p. 13, 79).

[Jou04] A. Joux. « A one round protocol for tripartite Diffie–Hellman ». Dans : *Journal of Cryptology* 17.4 (2004), p. 263–276. (Cf. p. 7).

[Ked01] K. Kedlaya. « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology ». Dans : *Preprint* (2001). arXiv : math/0105031. (Cf. p. 10).

[Kem88] G. Kempf. « Multiplication over abelian varieties ». Dans : *American Journal of Mathematics* 110.4 (1988), p. 765–773. (Cf. p. 76, 100).

[Kem89] G. Kempf. « Linear systems on abelian varieties ». Dans : *American Journal of Mathematics* 111.1 (1989), p. 65–94. (Cf. p. 13, 62, 68, 71, 95, 98, 100, 177).

[Kem92] G. Kempf. « Equations of Kümmer Varieties ». Dans : *American Journal of Mathematics* 114.1 (1992), p. 229–232. (Cf. p. 98).

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik et al. « Factorization of a 768-bit RSA modulus ». Dans : (2010). (Cf. p. 1).

[Kob87] N. Koblitz. « Elliptic curve cryptosystems ». Dans : *Mathematics of computation* 48.177 (1987), p. 203–209. (Cf. p. 3).

[Kob89] N. Koblitz. « Hyperelliptic cryptosystems ». Dans : *Journal of cryptology* 1.3 (1989), p. 139–150. (Cf. p. 3).

[Koh96] D. Kohel. « Endomorphism rings of elliptic curves over finite fields ». Thèse de doct. University of California, 1996. (Cf. p. 12).

[Koh03] D. Kohel. « The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting ». Dans : *Advances in cryptology—ASIACRYPT 2003*. T. 2894. Lecture Notes in Comput. Sci. Berlin : Springer, 2003, p. 124–136. (Cf. p. 131).

[Koi76] S. Koizumi. « Theta relations and projective normality of abelian varieties ». Dans : *American Journal of Mathematics* (1976), p. 865–889. (Cf. p. 62, 71, 76, 100).

[Lan58] S. Lang. « Reciprocity and Correspondences ». Dans : *American Journal of Mathematics* 80.2 (1958), p. 431–440. (Cf. p. 114–116).

[Lan05] T. Lange. « Formulae for arithmetic on genus 2 hyperelliptic curves ». Dans : *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), p. 295–328. (Cf. p. 1, 105).

[Lan06] T. Lange. « Elliptic vs. hyperelliptic, part 2 ». Dans : *Talk at ECC* (2006). URL : http://www.hyperelliptic.org/tanja/vortraege/talk_07.ps. (Cf. p. 4, 15).

[Laz81] D. Lazard. « Resolution des systemes d'equations algebriques ». Dans : *THEORET. COMP. SCI.* 15.1 (1981), p. 77–110. (Cf. p. 162).

[Laz83] D. Lazard. « Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations ». Dans : *Computer Algebra* (1983), p. 146–156. (Cf. p. 162).

[Laz92] D. Lazard. « Solving zero-dimensional algebraic systems ». Dans : *Journal of symbolic computation* 13.2 (1992), p. 117–131. (Cf. p. 162).

[LLMP93] A. Lenstra, H. Lenstra, M. Manasse et J. Pollard. « The number field sieve ». Dans : *The development of the number field sieve* (1993), p. 11–42. (Cf. p. 3).

[Ler97] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis. These, LIX–CNRS, juin 1997*. 1997. URL : http://cat.inist.fr/?cpsidt=183634. (Cf. p. 149).

[LL03] R. Lercier et D. Lubicz. « Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time ». Dans : *Advances in Cryptology—EUROCRYPT '2003*. Sous la dir. d'E. Biham. Lecture Notes in Computer Science. Springer-Verlag, mai 2003. (Cf. p. 176).

[LL06] R. Lercier et D. Lubicz. « A quasi-quadratic time algorithm for hyperelliptic curve point counting ». Dans : *Ramanujan J.* 12.3 (2006), p. 399–423. (Cf. p. 176).

[Lic69] S. Lichtenbaum. « Duality theorems for curves over p-adic fields ». Dans : *Inventiones mathematicae* 7.2 (1969), p. 120–136. (Cf. p. 115).

[LS08] D. Lubicz et T. Sirvent. « Attribute-based broadcast encryption scheme made efficient ». Dans : *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*. Springer-Verlag. 2008, p. 325–342. (Cf. p. 7).

[LR10a] D. Lubicz et D. Robert. *Computing isogenies between abelian varieties*. Jan. 2010. arXiv : 1001.2016. (Cf. p. viii, 14, 111, 149, 150).

[LR10b] D. Lubicz et D. Robert. *Efficient pairing computation with theta functions*. Sous la dir. de G. Hanrot, F. Morain et E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Jan. 2010. url : http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. (Cf. p. viii, 14, 111).

[LST64] J. Lubin, J.-P. Serre et J. Tate. *Elliptic Curves and formal groups*. 1964. url : http://ma.utexas.edu/users/voloch/lst.html. (Cf. p. 176).

[MW99] U. Maurer et S. Wolf. « The Relationship Between Breaking the Diffie–Hellman Protocol and Computing Discrete Logarithms ». Dans : *SIAM Journal on Computing* 28 (1999), p. 1689. (Cf. p. 3).

[Men07] A. Menezes. « Supersingular Elliptic Curves in Cryptography ». Dans : *Pairing-Based Cryptography–Pairing 2007* (2007), p. 293–293. (Cf. p. 5).

[MOV91] A. Menezes, T. Okamoto et S. Vanstone. « Reducing elliptic curve logarithms to logarithms in a finite field ». Dans : *Proceedings of the twenty-third annual ACM symposium on Theory of computing*. ACM. 1991, p. 89. (Cf. p. 5, 6, 8).

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley*. 2001. url : http://www.math.jussieu.fr/mestre. (Cf. p. 12, 165, 173, 176).

[Mes02] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. url : http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps. (Cf. p. 176).

[Mil04] V. S. Miller. « The Weil Pairing, and Its Efficient Calculation ». Dans : *J. Cryptology* 17.4 (2004), p. 235–261. doi : 10.1007/s00145-004-0315-8. (Cf. p. 5, 9).

[Mil85] J. Milne. « Jacobian varieties ». Dans : *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1985), p. 167–212. (Cf. p. 41).

[Mil86] J. Milne. « Abelian varieties ». Dans : *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1986), p. 103–150. (Cf. p. 41).

[Mil91] J. Milne. *Abelian varieties*. 1991. url : http://www.jmilne.org/math/CourseNotes/av.html. (Cf. p. 10, 41).

[MNT01] A. Miyaji, M. Nakabayashi et S. Takano. « New explicit conditions of elliptic curve traces for FR-reduction ». Dans : *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 84.5 (2001), p. 1234–1243. (Cf. p. 8).

[Mor95] F. Morain. « Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques ». Dans : *J. Théor. Nombres Bordeaux* 7 (1995), p. 255–282. (Cf. p. 12).

[Mor85] L. Moret-Bailly. *Pinceaux de variétés abéliennes*. Société mathématique de France, 1985. (Cf. p. 13).

[Mum66] D. MUMFORD. « On the equations defining abelian varieties. I ». Dans : *Invent. Math.* 1 (1966), p. 287–354. (Cf. p. 13, 16, 20, 41, 43, 44, 49, 51, 56, 61, 62, 64, 66, 68, 69, 71, 76, 78, 92, 94, 95, 97, 98).

[Mum67a] D. MUMFORD. « On the equations defining abelian varieties. II ». Dans : *Invent. Math.* 3 (1967), p. 75–135. (Cf. p. 13, 61, 62, 94–96).

[Mum67b] D. MUMFORD. « On the equations defining abelian varieties. III ». Dans : *Invent. Math.* 3 (1967), p. 215–244. (Cf. p. 13, 61).

[Mum69] D. MUMFORD. « Varieties defined by quadratic equations ». Dans : *Questions on Algebraic Varieties (CIME, III Ciclo, Varenna, 1969)* (1969), p. 29–100. (Cf. p. 76, 94, 100).

[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, p. viii+242. (Cf. p. 5, 19, 20, 23, 25, 27, 31, 41, 42, 63, 111, 113, 114).

[Mum83] D. MUMFORD. *Tata lectures on theta I*. T. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA : Birkhäuser Boston Inc., 1983, p. xiii+235. ISBN : 3-7643-3109-7. (Cf. p. 13, 34–37, 71, 79, 99, 100).

[Mum84] D. MUMFORD. *Tata lectures on theta II*. T. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA : Birkhäuser Boston Inc., 1984, p. xiv+272. ISBN : 0-8176-3110-0. (Cf. p. 6, 13, 95, 153).

[Mum91] D. MUMFORD. *Tata lectures on theta III*. T. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA : Birkhäuser Boston Inc., 1991, p. viii+202. ISBN : 0-8176-3440-1. (Cf. p. 13).

[Mum99] D. MUMFORD. *The red book of varieties and schemes*. T. 1358. Lecture Notes in Mathematics. Second, expanded edition. Includes the Michigan lectures (1974) on curves and their Jacobians. With contributions by Enrico Arbarello. Springer, 1999. (Cf. p. 13).

[NSA09] NSA. *Suite B Cryptography*. Fact Sheet, National Security Agency Central Security Service http://www.nsa.gov/business/programs/elliptic_curve.shtml. 2009. URL : http://www.nsa.gov/ia/programs/suiteb_cryptography/. (Cf. p. 4).

[ÓS07] C. Ó HÉIGEARTAIGH et M. SCOTT. « Pairing calculation on supersingular genus 2 curves ». Dans : *Selected Areas in Cryptography : 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006, Revised Selected Papers*. Springer-Verlag New York Inc. 2007, p. 302. (Cf. p. 9).

[OU73] F. OORT et K. UENO. « Principally polarized abelian varieties of dimension two or three are Jacobian varieties ». Dans : *Journal of the Faculty of Science, the University of Tokyo : Tōkyō Daigaku Rigakubu kiyō. Dai 1-rui, Sūgaku. Mathematics* (1973), p. 377. (Cf. p. 7).

[PSV06] D. PAGE, N. SMART et F. VERCAUTEREN. « A comparison of MNT curves and supersingular curves ». Dans : *Applicable Algebra in Engineering, Communication and Computing* 17.5 (2006), p. 379–392. (Cf. p. 5).

[Pil90] J. PILA. « Frobenius maps of abelian varieties and finding roots of unity in finite fields ». Dans : *Mathematics of Computation* 55.192 (1990), p. 745–763. (Cf. p. 162).

[PH78] S. Pohlig et M. Hellman. « An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.) » Dans : *IEEE Transactions on information Theory* 24.1 (1978), p. 106–110. (Cf. p. 3).

[Pom87] C. Pomerance. « Fast, rigorous factorization and discrete logarithm algorithms ». Dans : *Discrete algorithms and complexity : proceedings of the Japan-US Joint Seminar, June 4-6, 1986, Kyoto, Japan*. Academic Pr. 1987, p. 119–143. (Cf. p. 3).

[Ric36] F. Richelot. « Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes ». Dans : *C. R. Acad. Sci. Paris* 2 (1836), p. 622–627. (Cf. p. 12, 149).

[Ric37] F. Richelot. « De transformatione Integralium Abelianorum primiordinis commentation ». Dans : *J. reine angew. Math.* 16 (1837), p. 221–341. (Cf. p. 12, 149).

[RSA78] R. Rivest, A. Shamir et L. Adleman. « A method for obtaining digital signatures and public-key cryptosystems ». Dans : *Communications of the ACM* 21.2 (1978), p. 120–26. (Cf. p. 1).

[RS09] K. Rubin et A. Silverberg. « Using abelian varieties to improve pairing-based cryptography ». Dans : *Journal of Cryptology* 22.3 (2009), p. 330–364. (Cf. p. 4, 5, 112).

[SW05] A. Sahai et B. Waters. « Fuzzy identity-based encryption ». Dans : *Advances in Cryptology–EUROCRYPT 2005* (2005), p. 457–473. (Cf. p. 7).

[Sat00] T. Satoh. « The canonical lift of an ordinary elliptic curve over a finite field and its point counting ». Dans : *J. Ramanujan Math. Soc.* 15.4 (2000), p. 247–270. (Cf. p. 10, 12, 176).

[Sch85] R. Schoof. « Elliptic curves over finite fields and the computation of square roots mod p ». Dans : *Mathematics of computation* 44.170 (1985), p. 483–494. (Cf. p. 12, 102).

[Sch95] R. Schoof. « Counting points on elliptic curves over finite fields ». Dans : *J. Théor. Nombres Bordeaux* 7.1 (1995), p. 219–254. (Cf. p. 12).

[Ser56] J. Serre. « Géométrie algébrique et géométrie analytique ». Dans : *Ann. Inst. Fourier* 6 (1956), p. 1–42. (Cf. p. 19).

[Ser68] J. Serre. *Corps locaux*. Hermann Paris, 1968. (Cf. p. 115).

[She08] N. Shepherd-Barron. « Thomae's formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves ». Dans : (2008). (Cf. p. 176).

[Sho97] V. Shoup. « Lower bounds for discrete logarithms and related problems ». Dans : *Advances in Cryptology—EUROCRYPT'97*. Springer. 1997, p. 256–266. (Cf. p. 2).

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*. T. 106. Graduate Texts in Mathematics. Corrected reprint of the 1986 original. New York : Springer-Verlag, 1986, p. xii+400. ISBN : 0-387-96203-4. (Cf. p. 114).

[Sma09] « ECRYPT2 yearly report on algorithms and keysizes (2008-2009) ». Dans : *ECRYPT European Network of Excellence in Cryptology, Tech. Rep* (2009). Sous la dir. de N. Smart. (Cf. p. 4).

[Smi09] B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Fév. 2009. arXiv : 0806.2995. (Cf. p. 12, 149, 176).

[Sut09] A. Sutherland. « Computing Hilbert class polynomials with the Chinese remainder theorem ». Dans : *Mathematics of Computation* (2009). (Cf. p. 12, 174).

[Vel71] J. Vélu. « Isogénies entre courbes elliptiques ». Dans : *C. R. Acad. Sci. Paris Sér. A-B* 273 (1971), A238–A241. (Cf. p. 11, 149).

[Ver10] F. Vercauteren. « Optimal pairings ». Dans : *IEEE Transactions on Information Theory* 56.1 (2010), p. 455–461. (Cf. p. 15, 125).

[Ver01] E. Verheul. « Self-blindable credential certificates from the Weil pairing ». Dans : *Advances in Cryptology—ASIACRYPT 2001* (2001), p. 533–551. (Cf. p. 7).

[Wam99] P. Wamelen. « Equations for the Jacobian of a hyperelliptic curve ». Dans : *AMS* 350.8 (août 1999), p. 3083–3106. (Cf. p. 13, 95, 162, 164).

[WNM05] F. Wang, Y. Nogami et Y. Morikawa. « A High-Speed Square Root Computation in Finite Fields with Application to Elliptic Curve Cryptosystem ». Dans : *Mem Fac Eng Okayama Univ (CD-ROM)* 39 (2005), p. 82–92. (Cf. p. 102).

[Wei48] A. Weil. *Sur les courbes algébriques et les variétés qui s' en déduisent*. Hermann et Cie., 1948. (Cf. p. 4).

[Wei49] A. Weil. « Numbers of solutions of equations in finite fields ». Dans : *Bull. Amer. Math. Soc* 55.5 (1949), p. 497–508. (Cf. p. 4).

[Wei57] A. Weil. « Zum Beweis des Torellischen Satzes ». Dans : *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa* (1957), p. 33–53. (Cf. p. 7).

RÉSUMÉ

Le logarithme discret sur les courbes elliptiques fournit la panoplie standard de la cryptographie à clé publique : chiffrement asymétrique, signature, authentification. Son extension à des courbes hyperelliptiques de genre supérieur se heurte à la difficulté de construire de telles courbes qui soient sécurisées.

Dans cette thèse nous utilisons la théorie des fonctions thêta développée par MUMFORD pour construire des algorithmes efficaces pour manipuler les variétés abéliennes. En particulier nous donnons une généralisation complète des formules de Vélu sur les courbes elliptiques pour le calcul d'isogénie sur des variétés abéliennes. Nous donnons également un nouvel algorithme pour le calcul efficace de couplage sur les variétés abéliennes en utilisant les coordonnées thêta. Enfin, nous présentons une méthode de compression des coordonnées pour améliorer l'arithmétique sur les coordonnées thêta de grand niveau. Ces applications découlent d'une analyse fine des formules d'addition sur les fonctions thêta.

Si les résultats de cette thèse sont valables pour toute variété abélienne, pour les applications nous nous concentrons surtout sur les Jacobiennes de courbes hyperelliptiques de genre 2, qui est le cas le plus significatif cryptographiquement.

ABSTRACT

The discrete logarithm on elliptic curves gives the standard protocols in public key cryptography: asymmetric encryption, signatures, zero-knowledge authentification. To extend the discrete logarithm to hyperelliptic curves of higher genus we need efficient methods to generate secure curves.

The aim of this thesis is to give new algorithms to compute with abelian varieties. For this we use the theory of algebraic theta functions in the framework of MUMFORD. In particular, we give a full generalization of Vélu's formulas for the computation of isogenies on abelian varieties. We also give a new algorithm for the computation of pairings using theta coordinates. Finally we present a point compression method to manipulate more efficiently theta coordinates of high level. These applications follow from the analysis of Riemann relations on theta functions for the addition law.

Whereas the results of this thesis are valid for any abelian variety, for the applications a special emphasis is given to Jacobians of hyperelliptic genus 2 curves, since they are the most significantly relevant case in cryptography.

Mots clefs : Cryptographie, courbes hyperelliptiques, variétés abéliennes, isogénies, couplage, fonctions thêta

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