Calcul de polynômes modulaires en dimension 2

Enea Milio

université de BORDEAUX

Université de Bordeaux

THÈSE PRÉSENTÉE POUR OBTENIR LE GRADE DE

DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX

École Doctorale : **Mathématiques et Informatique**
Spécialité : **Mathématiques Pures**

Calcul de polynômes modulaires en dimension 2

par **Enea Milio**

Date de soutenance : **03/12/2015**

Sous la direction de : **Andreas Enge**
Co-encadrant : **Damien Robert**

Composition du jury :

Andreas Enge	Directeur
Pierrick Gaudry	Rapporteur
David Kohel	Examinateur
Kristin Lauter	Rapporteure
Reynald Lercier	Examinateur
Damien Robert	Co-encadrant

Calcul des polynômes modulaires en dimension 2

Enea Milio [1]

1. Thèse effectuée à l'institut de mathématiques de Bordeaux (IMB) de l'université de Bordeaux et financée par l'ERC ANTICS.

Résumé

Les polynômes modulaires sont utilisés dans le calcul de graphes d'isogénies, le calcul des polynômes de classes ou le comptage du nombre de points d'une courbe elliptique, et sont donc fondamentaux pour la cryptographie basée sur les courbes elliptiques.

Des polynômes analogues sur les surfaces abéliennes principalement polarisées ont été introduits par Régis Dupont en 2006, qui a également proposé un algorithme pour les calculer, et des résultats théoriques sur ces polynômes ont été donnés dans un article de Bröker–Lauter, en 2009. Mais les polynômes sont très gros et ils n'ont pu être calculés que pour l'exemple minimal $p = 2$.

Dans cette thèse, nous poursuivons les travaux de Dupont et Bröker–Lauter en permettant de calculer des polynômes modulaires pour des invariants basés sur les thêta constantes, avec lesquels nous avons pu calculer les polynômes jusqu'à $p = 7$, tout en démontrant des propriétés de ces polynômes. Mais des exemples plus grands ne semblent pas envisageables.

Ainsi, nous proposons une nouvelle définition des polynômes modulaires dans laquelle l'on se restreint aux surfaces abéliennes principalement polarisées qui ont multiplication réelle par l'ordre maximal d'un corps quadratique réel afin d'obtenir des polynômes plus petits. Nous présentons alors de nombreux exemples de polynômes et des résultats théoriques.

Mots-clés : Cryptographie, isogénies, variétés abéliennes, polynômes modulaires.

Title **:** Computing modular polynomials in dimension 2

Abstract

Modular polynomials on elliptic curves are a fundamental tool used for the computation of graph of isogenies, class polynomials or for point counting. Thus, they are fundamental for the elliptic curve cryptography.

A generalization of these polynomials for principally polarized abelian surfaces has been introduced by Régis Dupont in 2006, who has also described an algorithm to compute them, while theoretical results can been found in an article of Bröker–Lauter of 2009. But these polynomials being really big, they have been computed only in the minimal case $p = 2$.

In this thesis, we continue the work of Dupont and Bröker–Lauter by defining and giving theoretical results on modular polynomials with new invariants, based on theta constants. Using these invariants, we have been able to compute the polynomials until $p = 7$ but bigger examples look intractable. Thus we define a new kind of modular polynomials where we restrict on the surfaces having real multiplication by the maximal order of a real quadratic field. We present many examples and theoretical results.

Keywords : Cryptography, isogenies, abelian varieties, modular polynomials.

Remerciements

Il est bien connu que dans une thèse, les remerciements constituent la partie la plus délicate à écrire. C'est un exercice difficile pour un scientifique en mal d'inspiration littéraire ! D'autant plus que c'est la partie qui non seulement sera la plus lue de cette thèse, mais aussi celle où je serais le plus jugé : que l'on me pardonne l'oubli d'un nom qui mériterait à être cité. Mais que puis-je y faire ? Il est parfois difficile de se souvenir... Que l'on me permette donc de dire :

O Muse, O alto Ingegno, or m'aiutate
O Mente che scrivesti cio ch'io vidi
qui si parrà la tua nobilitade !

Dante, Inferno II

Faire un doctorat est une expérience enrichissante sous plusieurs points de vue. Ainsi, j'aimerais commencer par remercier celui qui m'a lancé dans cette aventure à Bordeaux. Je veux parler bien sûr de Laurent Imbert, avec qui j'ai fait mon mémoire de master, et qui m'a permis de rencontrer Andreas et Damien, mes directeurs de thèse préférés, que je ne saurais assez remercier pour tout ce qu'ils m'ont apportés. D'Andreas, et de son côté terre-à-terre, rigoureux (il est Allemand), je lui dois surtout de m'avoir appris à bien structurer mon travail. Il a eu le courage, il faut le dire, de relire mon premier article de nombreuses fois et à chacune de ses lectures, il a su me pousser à l'améliorer à travers ses nombreuses remarques pertinentes. D'autre part, ses conseils précieux lors des différentes répétitions de mon exposé pour ECC m'ont permis de bien comprendre comment présenter des travaux de recherche. Je le remercie énormément pour cet apport indispensable. Quant à Damien, je lui dois tout le reste ! C'est à travers lui que j'ai appris toutes les mathématiques que l'on retrouve dans ce document ; et plus généralement, sa manière de faire des mathématiques est, véritablement, une source d'inspiration pour moi. Je le remercie d'avoir répondu à toutes les questions que j'ai pu lui poser durant ces années, et d'y avoir répondu avec la patience et la gentillesse qui le caractérisent. Et de la patience il en a fallut ! Car de nombreuses fois j'ai eu à répéter des questions jusqu'à ce que je comprenne vraiment ses réponses (le soleil se contente de briller avec la lumière qui est la sienne !). Merci enfin pour tous les résultats de cette thèse, qui n'auraient pas vu le jour sans eux. Pour toutes ces raisons (et bien d'autres aussi), je m'estime vraiment heureux de m'être retrouvé en leur compagnie. Et que puis-je dire si ce n'est :

La soif m'attira vers l'eau
et je bus le reflet de la lune.

Rûmi, Mathnawî

La présente thèse a également été possible grâce au travail de nombreuses personnes. Je remercie les deux ingénieurs Bill et Laurent, ainsi que toute l'équipe

plafrim, sans qui je n'aurais pas pu utiliser GP sur plafrim et faire tous les calculs de polynômes ! Je remercie aussi toutes celles qui travaillent dans le service administratif : Catherine, Ida, Christine, Ingrid (avec qui j'ai de bons souvenirs de ECC)... et surtout Anne-Laure, entre autres pour sa disponibilité et son efficacité. Il me faut également ajouter des remerciements aux bibliothécaires, qui permettent d'avoir encore accès à des livres, à l'ère du numérique.

Mais faire une thèse, c'est également faire des rencontres ! Il y a avant tout tous ceux qui sont ou qui ont été membres de l'équipe LFANT : Aurel, Barinder, Chloe, Cyril, Fredrik, Gregor, Guilhem, Hamish, Ilaria, Jean-Marc, Jean-Paul, Karim, Nicolas, Pierre, Sorina, ... avec qui j'ai partagé tant de choses, dont de nombreux séminaires, indispensables dans la vie d'un laboratoire, et les gâteaux de Bill ! Il y a tous les membres du laboratoire, que je croise ou ai croisé quotidiennement (je les laisse se reconnaître), dont les membres du « péril Italien » : Giovanni, Daniele, Dajano, tous les Nicola, ... et tous ceux avec qui j'ai partagé tant de repas au Haut-Carré : Alain, Arnaud, etc. Il y a aussi tous les gens qui m'ont accueilli pour que je fasse des séminaires chez eux : les équipes de Rennes, Nancy et de Montpellier, il y a tous les membres de l'ANR PEACE et tous les gens avec qui je me suis lié d'amitié dans les différentes conférences auquelles j'ai pu participer : Laurent, Philippe, Pierfranceso, ... (et la liste est longue). J'ai d'ailleurs une pensée particulière pour Pierre Chrétien, avec qui je garde un bon souvenir de nos balades autour de Oberwolfach, lorsque j'étais au tout début de ma thèse. Enfin, comment ne pas mentionner aussi mes camarades du master maths-info à Montpellier : Bastien, Guillaume et Manu (bonne chance pour votre fin de thèse !) mais aussi Niihau et André.

Il me faut également remercier Pierrick Gaudry et Kristin Lauter pour avoir accepter d'être mes rapporteurs. Je suis redevable envers Pierrick pour sa lecture très attentive de ma thèse et pour ses nombreuses corrections, et l'en remercie énormément. Merci aussi à Reynald Lercier et à David Kohel d'avoir accepté de me faire l'honneur de faire partie du jury.

Ce manuscrit est le fruit de tant de rencontres. Il contient sans aucun doute des erreurs qui sont de mon fait : je m'en excuse par avance !

Meraveill me cum vostre cors s'orgoilla,
amics, vas me, per qui'ai razon queu.m doilla ;
non es ges dreitz c'autr' amors vos mi toilla,
per nuilla ren que.us diga ni acoilla.
E membre vos cals fo.l comensamens
de nostr'amor ! Ja Dompnedeus non voilla
qu'en ma colpa sia.l departimens.

Beatriz de Dia

Et comment ne pas mentioner mes deux frères qui ont su corriger des erreurs complexes, pour ne pas dire imaginaires, dans mon premier article ? Je leur en suis gré. Enfin et plus généralement, j'ai une pensée toute particulière pour toute ma famille.

Table des matières

Liste des Algorithmes

Introduction

Contexte

C'est un fait constatable par tous que l'informatique est de nos jours partout dans notre quotidien. Nous l'utilisons lorsque, par exemple, nous payons par carte bancaire, nous prélevons de l'argent dans un distributeur de billets, nous jouons avec nos téléphones, nous surfons sur le web ou lorsque nous faisons du commerce électronique. Tout ceci est devenu tellement naturel que nous n'avons pas conscience de cette omniprésence et de tous ces flux de données qui transitent chaque jour, flux sans lesquels notre société "virtuelle" ne pourrait exister, et qu'il faut donc sécuriser. Cette protection se fait à l'aide de la cryptographie.

Le protocole de cryptage asymétrique le plus utilisé est RSA [73]. Mais le fait que les attaques connus contre RSA sont sous-exponentielles et que les puissances de calcul des ordinateurs sont sans cesse croissantes font que la taille des clés doit beaucoup augmenter pour préserver la sécurité, ce qui rend ce protocole de moins en moins utilisable avec le temps. Ceci justifie que l'on s'intéresse à d'autres méthodes de cryptage. Or, parmis celles-ci, celle qui paraît être la meilleure alternative (les attaques sont exponentielles) est la cryptographie basée sur les courbes elliptiques, qui sont les variétés abéliennes de dimension 1, et les courbes hyperelliptiques de genre 2 (voir [64, 51, 52]), dont les Jacobiennes sont les variétés abéliennes de dimension 2 (par le théorème 2.7.6).

Alors que la sécurité de RSA repose sur la difficulté de résoudre le problème de la factorisation d'entiers, les protocoles basés sur les courbes elliptiques reposent sur la difficulté de résoudre le problème du logarithme discret dans un groupe. Plus précisément, on cherche à trouver des groupes mathématiques dans lesquels ce problème du logarithme discret est difficile tandis que l'exponentiation, qui est le problème inverse, est facile à calculer. À l'heure actuelle, les meilleurs groupes proviennent des courbes elliptiques et des Jacobiennes de courbes hyperelliptiques de genre 2 et afin que le problème mentionné plus haut soit suffisamment complexe, il nous faut des variétés abéliennes, sur un corps fini, dont le cardinal est divisible par un grand nombre premier. Pour ce faire, une approche consiste à utiliser la théorie de la multiplication complexe pour construire des variétés avec un nombre de points fixé. On pourrait également prendre des courbes au hasard et compter leurs nombres de points jusqu'en trouver une dont le nombre de points nous convienne.

Une isogénie est un morphisme entre deux variétés abéliennes qui est surjectif et de noyau fini. C'est une notion fondamentale dans l'étude théorique des variétés abéliennes, mais aussi pour les applications cryptographiques, car un tel morphisme peut permettre de transférer le problème du logarithme discret d'une variété, où ce problème est compliqué, à une autre, où il est plus facile.

Calculer une isogénie veut dire plusieurs choses : calculer une variété isogène une fois donné un sous-groupe isotrope maximal de la torsion, calculer l'image d'un point par une isogénie vérifier si deux variétés abéliennes sont isogènes et si c'est le cas, expliciter une isogénie (voir [86, 24, 23, 53] en dimension 1 et [14, 58, 59, 15] en dimension 2). Mais ce qui nous intéresse c'est le calcul de toutes les variétés isogènes, d'un degré fixé, à une variété abélienne donnée et ceci peut être fait en calculant des polynômes modulaires (voir [25, 10] en dimension 1 et [19, 9, 63] en dimension 2). De plus, ces polynômes ont de nombreuses applications. En dimension 1, ils sont la clé pour l'algorithme de Schoof-Elkies-Atkin (SEA) qui améliore l'algorithme de Schoof pour le comptage de points d'une courbe elliptique [23, 77], pour construire des courbes elliptiques avec un nombre de points fixé par la méthode de la multiplication complexe [3, 28, 81] et pour le calcul de l'anneau d'endomorphismes d'une courbe elliptique [6]. En dimension 2, ces polynômes peuvent jouer le même rôle mais sont plus compliqués à calculer. Ils permettent également d'accélérer l'algorithme CRT de calcul de corps de classes d'un corps CM de degré 4 ([22]), ce qui produit des algorithmes plus rapides pour le calcul de Jacobiennes de courbes hyperelliptiques avec une sécurité cryptographique plus importante.

En dimension 1, les polynômes modulaires peuvent être calculés en temps quasi-linéaire en la taille de l'objet calculé ([10, 25]). La technique de calcul de ces polynômes qui nous intéresse est celle qui procède par évaluation/interpolation : c'est celle qui a été généralisée par Dupont en dimension 2 ([19]). Pour pouvoir utiliser cette technique, il faut être capable d'évaluer des fonctions modulaires efficacement en suffisamment de points pour pouvoir ensuite procéder à une phase d'interpolation de polynômes univariés. La fonction modulaire qui est principalement calculée est la fonction j appelée le j-invariant (voir définition 1.1.2), qui a la propriété que deux courbes elliptiques isomorphes ont la même évaluation sur $\overline{k}$, où k est un corps, en cette fonction j. Plus généralement, on s'intéresse aux thêta constantes car la plupart des fonctions qu'on étudie s'écrivent à partir de celles-ci.

Dans sa thèse [19], Dupont présente un algorithme d'évaluation rapide des thêta constantes en dimensions 1. Ce dernier allie la moyenne arithmético-géométrique (AGM) et les itérations de Newton, deux algorithmes convergeant quadratiquement, et est alors quasi-linéaire en la précision. En généralisant ses résultats, Dupont a introduit un algorithme pour le calcul des polynômes modulaires en dimension 2. Notons que le fossé entre ces deux dimensions est particulièrement important. En dimension 1, les variétés abéliennes sont représentées comme un point du demi-plan complexe supérieur, appelé demi-plan de Poincaré, tandis qu'en dimension 2 elles le sont par des matrices 2×2 symétriques de partie imaginaire définie positive. De plus, l'équivalent du j-invariant sont les invariants d'Igusa (voir définition 3.3.1), au nombre de trois, ce qui fait que dans l'étape d'interpolation, on ne doive plus interpoler des polynômes univariés mais plutôt des fractions rationnelles trivariées. Ceci ajoute une difficulté supplémentaire car on ne peut plus choisir des points aléatoirement dans l'évaluation : on verra qu'il nous faudra être capable d'inverser les invariants d'Igusa. La généralisation de l'AGM est ce qu'on appelle les suites de Borchardt. Nous verrons comment la conjecture 3.6.2 nous permet à la fois d'inverser les invariants d'Igusa et d'évaluer rapidement les thêta constantes, et par suite les invariants d'Igusa, ce qui a permis à Dupont d'introduire un algorithme quasi-linéaire pour le calcul des polynômes

modulaires en dimension 2. En l'utilisant, il a pu calculer les polynômes paramétrisant les 2-isogénies, mais ces polynômes étant déjà très gros, il n'a pu calculer que les dénominateurs et les degrés des invariants dans les numérateurs pour les 3-isogénies.

Résultats

Nous présentons dans cette thèse une généralisation de l'algorithme de Dupont pour le calcul des polynômes modulaires en dimension 2 qui permet d'utiliser des fonctions modulaires f_1, f_2, f_3, dérivées des thêta constantes, pour un sous-groupe de congruence Γ du groupe symplectique Γ_2 et engendrant le corps des fonctions modulaires invariantes par ce sous-groupe. Nous utiliserons plus particulièrement les invariants de Streng (voir définition 3.3.2) et des quotients de thêta constantes.

Pour la phase d'évaluation, il nous faut inverser les f_i, c'est-à-dire être capable de déduire $\Omega \in \mathcal{H}_2$ modulo Γ_2 à partir de $f_1(\Omega)$, $f_2(\Omega)$ et $f_3(\Omega)$. Pour cela, il nous faut d'abord déduire des $f_i(\Omega)$ les invariants d'Igusa $j_1(\Omega)$, $j_2(\Omega)$ et $j_3(\Omega)$ pour pouvoir ensuite utiliser l'algorithme de Mestre pour obtenir une courbe hyperelliptique de genre 2 ayant les bons invariants. En utilisant les formules de Thomae, l'intégration numérique et les suites de Borchardt, il est possible de trouver Ω modulo Γ_2, sous la conjecture 3.6.2. Une fois que l'on a Ω modulo Γ_2, il nous faut trouver Ω modulo Γ. Ceci peut être fait grâce à l'équation fonctionnelle des fonctions thêta (proposition 2.6.4). Il ne reste qu'à utiliser la définition 4.2.10 des polynômes modulaires pour terminer l'étape d'évaluation.

Tous les calculs sont fait en multiprécision flottante. Des bornes explicites sur la taille des coefficients des polynômes modulaires ne sont pas connues en dimension 2 (c'est déjà un problème difficile en dimension 1). Ainsi, notre algorithme est heuristique. De plus, sous des heuristiques et la conjecture 3.6.2, il est quasi-linéaire en la taille de la sortie (théorème 4.2.15). En pratique, on augmente la précision jusqu'à en trouver une qui soit suffisante. Nous insistons sur le fait que les précisions sont grandes (nous avons fait des calculs avec une précision de plusieurs milliers de chiffres décimaux) et qu'il est donc fondamental de calculer les thêta constantes rapidement.

Cet algorithme généralisé sera appliqué tout d'abord sur les invariants de Streng, qui sont équivalents aux invariants d'Igusa dans le sens où ils décrivent le même espace de modules à équivalence birationnelle près (et en effet, il existe des formules pour passer des premiers invariants aux seconds : voir les équations (3.4) et (3.5)). Nous avons pu calculer les polynômes paramétrisant les 2- et les 3-isogénies, ces invariants produisant des polynômes plus petits en termes de degrés et tailles des coefficients par rapport aux polynômes avec les invariants d'Igusa, ce qui permet à la précision des calculs d'être plus petite, comme déjà remarqué par Streng pour le calcul des polynômes de classes ([80, Annexe 3]). Par exemple, pour $p = 2$, les polynômes avec les invariants de Streng occupent $2,1$ Mo contre 57 Mo avec les invariants d'Igusa.

Nous avons ensuite appliqué notre algorithme sur les fonctions $\mathfrak{b}_i = \frac{\theta_i(\Omega/2)}{\theta_0(\Omega/2)}$ pour $i = 1, 2, 3$, qui sont des fonctions modulaires pour le groupe $\Gamma_2(2, 4)$, et calculé les polynômes avec ces invariants pour $p = 3$, 5 et 7. Comme ces polynômes occupent respectivement 175 Ko, 200 Mo et 29 Go, nous n'avons pas essayé de les obtenir pour de plus grand nombres premiers. En outre, les polynômes trouvés sont bien plus petits que ceux avec les invariants de Streng et d'Igusa. Par exemple, pour $p = 3$ les polynômes modulaires avec les $\mathfrak{b}_i$ prennent 175 Mo contre 890 Mo avec les invariants de Streng. Cette différence se justifie par la présence de symétries (theorème 4.4.9) dans les polynômes avec les $\mathfrak{b}_i$ et par le fait qu'ils sont creux (théorème 4.4.10). Nous avons également obtenu une formule pour le degré total des dénominateurs des polynômes modulaires avec ces invariants

(corollaire 4.4.4) et, en nous basant sur [9], nous avons également donné un sens à ces dénominateurs (proposition 4.4.5).

Dans le dernier chapitre, on introduit des polynômes modulaires sur les surfaces abéliennes principalement polarisées qui ont multiplication réelle maximale par un corps de nombres quadratique $K = \mathbb{Q}(\sqrt{D})$. Si on note $\mathcal{H}_1$ le demi-plan de Poincaré, alors la surface modulaire de Hilbert $\mathcal{H}_1^2/\operatorname{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ est un espace de modules pour de telles surfaces abéliennes. Afin de distinguer les différents types de polynômes modulaires, on appelera les premiers *polynômes modulaires de Siegel* et ces derniers *polynômes modulaires de Hilbert* et puisque les premiers sont associés à des p-isogénies tandis que les seconds à des β-isogénies, on parlera aussi de p-polynômes modulaires et de β-polynômes modulaires. Des invariants rationnels qui jouent le même rôle que le j-invariant ne sont connus que pour $D = 5$ et sont dûs aux travaux de Gundlach. Nous appelons donc ces invariants les invariants de Gundlach et nous introduirons des invariants rationnels pour $D = 2$ (voir théorèmes 5.1.6 et 5.1.8). En outre, il existe un revêtement de degré 2 de la surface de Hilbert $\mathcal{H}_1^2/\operatorname{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ vers une surface de $\mathcal{H}_2/\Gamma_2$ appelée surface de Humbert. Ce revêtement nous permettra de transférer tous nos problèmes sur la surface de Hilbert vers l'espace de Siegel. En particulier, nous donnerons des formules pour exprimer les invariants de Gundlach pour $D = 2$ et $D = 5$ en fonction des tirés en arrière des invariants d'Igusa (théorèmes 5.1.11 et 5.1.13), ce qui permet d'évaluer les invariants de Gundlach avec la même complexité que les invariants d'Igusa (théorème 5.4.2). Ceci a pour application d'accélérer l'algorithme de [56] qui génère des courbes de genre 2 sur un corps fini avec un nombre de points donné sur la Jacobienne de la courbe (voir aussi [31, 21, 8, 55] à ce sujet). On donnera également une méthode pour inverser ces invariants (voir théorème 5.4.1). Enfin, nous définirons des invariants grâce aux tirés en arrière des thêta constantes pour tout D et donnerons un algorithme quasi-linéaire, à D fixé, pour calculer les polynômes modulaires de Hilbert avec ces différents invariants (théorème 5.4.4).

Plan de la thèse

Cette thèse est décomposée en deux parties. Dans la première, nous nous concentrerons sur l'aspect théorique des variétés abéliennes de dimension $g \geq 1$. Cette partie est divisée en deux chapitres. Dans le chapitre 1, nous traiterons des courbes elliptiques ($g = 1$), principalement sur $\mathbb{C}$. Nous montrerons que ces courbes elliptiques sont des tores complexes de dimension 1 et vice versa, nous décrirons l'espace de modules $\mathcal{H}_1/\Gamma_1$ qui paramétrise tous ces tores à isomorphisme près où nous y définirons des fonctions, appelées fonctions modulaires. Nous introduirons les thêta constantes et expliquerons un algorithme pour le calcul des polynômes modulaires. Enfin, nous conclurons avec plusieurs exemples de polynômes avec différents invariants. Dans le chapitre 2, nous nous concentrerons sur l'aspect théorique des variétés abéliennes complexes de dimension g. Nous verrons leur lien avec les tores complexes de dimension g et avec les Jacobiennes de courbes hyperelliptiques de genre g. Nous verrons la notion de polarisation et introduirons l'espace de module $\mathcal{H}_g/\Gamma_g$ des variétés abéliennes principalement polarisées de dimension g. En outre, nous définirons les fonctions thêta et donnerons une équation fonctionnelle décrivant le comportement d'une telle fonction par l'action d'une matrice de Γ_g.

Dans la deuxième partie, nous nous focaliserons sur la dimension $g = 2$. Cette partie est divisée en trois chapitres. Dans le chapitre 3, nous décrirons de nombreux algorithmes permettant de manipuler les différentes représentations des surfaces abéliennes complexes (comme matrice de $\mathcal{H}_2$, comme Jacobienne d'une courbe hyperelliptique de genre 2, comme triplet de nombres complexes à travers les invariants d'Igusa, ou alors à travers d'autres invariants si on ajoute de la structure) et passer de l'une à l'autre. Nous y verrons également un algorithme pour évaluer rapidement les thêta constantes. Dans les chapitres 4 et 5, nous parlerons des polynômes modulaires sur les espace de Siegel et de Hilbert et décrirons les résultats expliqués dans la section précédente.

Notations

Nous donnons quelques précisions quant à des notations qui seront utilisées tout le long de cette thèse.

- Les classes du quotient Γ_1/Γ_2 de deux groupes Γ_1 et Γ_2 seront toujours à droite. Cela signifie que les classes sont de la forme $\Gamma_2\gamma$ pour $\gamma \in \Gamma_1$ et deux classes $\Gamma_2\gamma$ et $\Gamma_2\gamma'$ sont équivalentes si et seulement si $\gamma\gamma'^{-1}$ est dans Γ_2 ;
- L'action d'un groupe G sur un ensemble H, notée H/G, est toujours une action à gauche : on a alors pour tous g, g' dans G que $g \cdot (g' \cdot h) = (gg' \cdot h)$, où $h \in H$;
- Pour tout nombre complexe z, on note $\Re(z)$ et $\Im(z)$ ses parties réelle et imaginaire. On utilise également ces symboles pour des matrices complexes. L'unité imaginaire est notée par $\imath$;
- La matrice identité de taille n est I_n ;
- Pour une matrice carré M donnée, on désigne par M_0 le vecteur composé des éléments diagonaux de M ;
- Le symbole de Kronecker $\delta_{i,j}$ vaut 1 lorsque $i = j$ et 0 sinon ;
- Soit une matrice Ω de l'espace de Siegel. La plus petite valeur propre de $\Im(\Omega)$ est $\lambda(\Omega)$;
- L'ensemble $\mathcal{P}$ vaut toujours $\{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$;
- La complexité pour multiplier deux polynômes de degrés au plus d avec des coefficients de N bits est $\mathcal{M}_N(d)$ tandis que celle pour multiplier deux entiers de N bits est $\mathcal{M}'(N)$.

Première partie

Théorie générale des variétés abéliennes complexes

Chapitre 1

Courbes elliptiques

Dans ce chapitre, nous parlerons des courbes elliptiques car ce sont, d'après le théorème 2.7.6, les variétés abéliennes de dimension 1. Par courbe, nous entendons une variété projective géométriquement connexe de dimension 1. Nous commencerons par donner des résultats généraux sur les courbes elliptiques pour tout corps parfait, puis nous nous concentrerons sur le corps $\mathbb{C}$, où nous verrons que toute courbe elliptique est un tore complexe de dimension 1 (proposition 1.2.12 et corollaire 1.2.16). Cette représentation des variétés abéliennes de dimension 1 comme tores complexes de dimension 1 nous fournira une nouvelle représentation de ces variétés : comme point du demi-plan de Poincaré $\mathcal{H}_1$. Une classe d'isomorphisme de courbes elliptiques sera alors une classe d'équivalence de points modulo l'action de $\mathrm{SL}_2(\mathbb{Z})$ et nous donnerons un domaine fondamental pour une telle action. Nous étudierons des fonctions sur $\mathcal{H}_1/\mathrm{SL}_2(\mathbb{Z})$, en particulier les fonctions thêta. Enfin, nous définirons les polynômes modulaires et donnerons un algorithme pour les calculer.

Le contenu de ce chapitre est tiré essentiellement des références suivantes : [79, 19, 68, 75, 61, 89, 25]. On note par K un corps parfait et par $\overline{K}$ sa clôture algébrique.

1.1 Généralités sur les courbes elliptiques

1.1.1 Équation de Weierstrass

Rappelons que l'espace projectif $\mathbb{P}^n(\overline{K})$ est l'ensemble des $(n+1)$-uplets d'éléments non tous nuls de $\overline{K}$, que l'on écrit sous la forme $[x_0 : x_1 : \cdots : x_n]$, muni de la relation d'équivalence :

$$[x_0 : \cdots : x_n] \sim [y_0 : \cdots : y_n]$$

si et seulement s'il existe un scalaire $\lambda \in \overline{K}^*$ tel que pour tout i de 0 à n on ait $x_i = \lambda y_i$.

On dit d'un point P d'une variété affine donnée par une équation polynomiale $F(X_1, \ldots, X_n)$ qu'il est *singulier* si on a

$$\frac{\partial F}{\partial X_1}(P) = \cdots = \frac{\partial F}{\partial X_n}(P) = 0. \tag{1.1}$$

Dans le cas contraire, on dit que ce point est *lisse*. Pour une variété projective, on dit d'un point qu'il est lisse s'il l'est dans une des cartes affines. Enfin, une courbe est dite lisse si elle l'est en tous ses points.

Définition 1.1.1. *Une* courbe elliptique *est une paire (E, O) où E est une courbe lisse de genre 1 sur $\overline{K}$ et $O \in E$.*

Le point particulier O, qu'on appelle *origine*, nous sert à établir une loi de groupe sur la courbe. Nous y reviendrons. D'après [79, Proposition III.3.1 (a)], il existe des fonctions x, y dans le corps de fonctions de E, appelées *fonctions de coordonnées de Weierstrass*. telles que l'application $[x : y : 1]$ de E vers $\mathbb{P}^2$ avec $O \mapsto [0 : 1 : 0]$ donne un isomorphisme entre E et une *équation de Weierstrass*, c'est-à-dire une équation de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.2}$$

où les coefficients $a_1, \ldots, a_6$ sont dans $\overline{K}$. Ils ne sont pas déterminés de manière unique par la courbe. Dans le cas où les coefficients a_i peuvent être choisis dans K, on dit que la courbe elliptique E est *définie sur* K, ce que l'on note par E/K. Si on déhomogénise l'équation, on obtient l'équation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1.3}$$

qu'on l'on appellera dans la suite *équation de Weierstrass affine*, plus un unique point à l'infini $[0 : 1 : 0]$. C'est ce point qu'on prend pour origine : $O = [0 : 1 : 0]$. Inversement ([79, Proposition III.3.1 (c)]), toute courbe cubique lisse C donnée par une équation de Weierstrass affine est une courbe elliptique d'origine $[0 : 1 : 0]$.

En outre, ([79, Proposition III.3.1 (b)]), deux équations de Weierstrass pour E/K sont reliées par une changement linéaire de variables de la forme

$$X = u^2X' + r \qquad \text{et} \qquad Y = u^3Y' + su^2X' + t,$$

où $u, r, s, t \in K$ et $u \neq 0$. Deux courbes elliptiques dont les équations de Weierstrass sont reliées par un changement de variables sur K sont dites *isomorphes* sur K. Dans le cas où la caractéristique de K n'est ni 2, ni 3, on peut alors montrer qu'à l'aide de changements de variables on peut ne considérer que les équations de la forme :

$$Y^2 = X^3 + AX + B \quad \text{avec} \quad 4A^3 + 27B^2 \neq 0. \tag{1.4}$$

Notons que A et B sont dans K lorsque la courbe E est définie sur K.

Une autre forme qui est parfois utile est la suivante. Une équation de Weierstrass est dite sous forme de *Legendre* si elle est de la forme $Y^2 = X(X-1)(X-\lambda)$, avec $\lambda \notin \{0, 1\}$.

Définition 1.1.2. *Pour une équation de Weierstrass comme dans (1.4), on pose $\Delta = -16(4A^3 + 27B^2)$ et $j = -1728\frac{(4A)^3}{\Delta}$. Ces quantités sont appelées respectivement le* discriminant *et le* j-invariant *de la courbe.*

Proposition 1.1.3. *Pour un corps K de caractéristique différente de 2, une courbe elliptique E/K est isomorphe sur $\overline{K}$ à une courbe elliptique E_λ sous forme de Legendre, avec $\lambda \in \overline{K}\backslash\{0, 1\}$. Le j-invariant est $j(E_\lambda) = 2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.*

Démonstration. Voir [79, Proposition III.1.7]. □

Bien entendu, il existe des formules ([79, Page 46]) pour définir ces quantités pour toute équation de la forme (1.2), mais dans la suite nous nous placerons sur $K = \mathbb{C}$ qui est de caractéristique nulle et donc nous supposons dorénavant que $\mathrm{char}(K) \neq 2, 3$. Nous renvoyons le lecteur intéressé à [79, Chapitre III].

Proposition 1.1.4. *1. Une courbe donnée par une équation de Weierstrass est lisse si et seulement si $\Delta \neq 0$;*

2. Deux courbes elliptiques sont isomorphes sur $\overline{K}$ si et seulement si elles ont le même j-invariant.

Démonstration. Voir [79, Proposition III.1.4]. □

La condition $4A^3 + 27B^2 \neq 0$ dans l'équation (1.4), ou, autrement dit, $\Delta \neq 0$, traduit le fait que la courbe doit être lisse. Remarquons que si l'on se place sur $K = \mathbb{R}$, alors le signe de Δ nous donne le nombre de zéros réels de l'équation $X^3 + AX + B$: 1 si Δ est négatif et 3 sinon. Ainsi, dans le premier cas, le graphe de la courbe admet deux composantes connexes tandis que dans le second cas, elle n'en a qu'une. D'autre part, j est un invariant de la classe d'isomorphisme de la courbe et ne dépend pas de l'équation particulière choisie. Nous verrons par la suite le rôle fondamental que joue cette fonction.

Notons $K(E)$ le corps de fraction de $K[E] = K[X, Y]/(F(X, Y))$, où F est l'équation de E.

Proposition 1.1.5. *Soit E/K une courbe elliptique avec x, y comme coordonnées de Weierstrass. On a $K(E) = K(x, y)$ et $[K(E) : K(x)] = 2$.*

Démonstration. Voir [79, Corollaire III.3.1.1]. □

1.1.2 Loi de groupe

Une courbe elliptique peut être munie d'une loi de groupe. Si on considère une droite dans $\mathbb{P}^2(\overline{K})$, elle intersecte la courbe elliptique en exactement 3 points (puisque celle-ci a une équation de degré 3) qui ne sont pas forcément distincts car la droite peut être tangente à la courbe. L'addition de deux points P et Q se fait ainsi : on considère R le troisième point d'intersection entre la droite passant par P et Q et la courbe, puis on considère R' le troisième point d'intersection de la droite passant par O et R et la courbe. On pose alors : $P + Q = R'$.

Ce procédé nous fournit bien une loi de groupe ([79, Proposition III.2.2]), où O est l'élément neutre. Cette loi a en plus la propriété d'être commutative et si on prend E définie sur K, alors $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{O\}$ est un sous-groupe de E.

On peut donner des équations explicites pour cette addition. Avant tout, on a que $O + P = P + O = P$ pour tout $P \in E$. Ensuite, pour toute paire d'éléments non nuls $P = (x_1 : y_1 : 1)$ et $Q = (x_2 : y_2 : 1)$, on a $P + Q = O$ si et seulement si $x_1 = x_2$ et $y_1 = -y_2$. Sinon, soit $\lambda \in K$ tel que

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si} \quad P \neq Q, \\ \\ \frac{3x_1^2 + A}{2y_1} & \text{si} \quad P = Q. \end{cases}$$

On pose $\mu = y_1 - \lambda x_1$ et on a alors $R = P + Q = (x_3 : y_3 : 1)$, où $x_3 = \lambda^2 - x_1 - x_2$ et $y_3 = -\lambda x_3 - \mu$. On notera que $-(x : y : z) = (x : -y : z)$.

Cette loi de groupe peut paraître étonnante. Pour en comprendre son origine, il faut s'intéresser au groupe de Picard de la courbe. Nous renvoyons à [79, Chapitre II] pour plus de détails dans ce qui suit.

Le *groupe des diviseurs* d'une courbe elliptique E, noté $\mathrm{Div}(E)$, est le groupe abélien libre engendré par les points de E. Un diviseur $D \in \mathrm{Div}(E)$ est donc

une somme formelle $D = \sum_{P \in E} n_P(P)$ avec $n_P \in \mathbb{Z}$ et $n_P = 0$ pour tous sauf un nombre fini de points $P \in E$. Le *degré* d'un tel diviseur D est $\sum_{P \in E} n_P$ et l'ensemble noté $\mathrm{Div}^0(E)$ des diviseurs qui sont de degré 0 forme un sous-groupe de $\mathrm{Div}(E)$.

Si on prend un élément $f \in \overline{K}(E)^*$, alors on peut lui associer un diviseur $\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$, où $\mathrm{ord}_P(f)$ désigne l'ordre de f en P. Un tel diviseur a alors des propriétés particulières : d'une part $\mathrm{div}(f) = 0$ si et seulement si $f \in \overline{K}^*$ et d'autre part $\deg(\mathrm{div}(f)) = 0$. On dit alors qu'un diviseur est *principal* s'il est de la forme $D = \mathrm{div}(f)$ pour un certain $f \in \overline{K}(E)^*$. On a que $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. Ceci nous permet d'établir une relation d'équivalence où deux diviseurs D_1 et D_2 sont dits *linéairement équivalents*, ce que l'on note par $D_1 \sim D_2$, si $D_1 - D_2$ est principal. D'après [79, Corollaire III.3.5], un diviseur $D = \sum_{P \in E} n_P(P)$ est principal si et seulement si $\sum n_P = 0$ et $\sum [n_P](P) = O$, où $[n_P](P) = P + P + \ldots + P$, n_P fois. Le *groupe de classes des diviseurs* ou *groupe de Picard*, noté $\mathrm{Pic}(E)$, de la courbe elliptique E est alors le quotient de $\mathrm{Div}(E)$ par le sous-groupe des diviseurs principaux et on note $\mathrm{Pic}^0(E)$ le quotient de $\mathrm{Div}^0(E)$ par le sous-groupe des diviseurs principaux.

Proposition 1.1.6. *Soit (E, O) une courbe elliptique :*

1. *Pour chaque diviseur $D \in \mathrm{Div}^0(E)$, il existe un unique point $P \in E$ tel que $D \sim (P) - (O)$. Soit alors $\sigma : \mathrm{Div}^0(E) \to E$ l'application donnée par cette association ;*
2. *L'application σ est surjective ;*
3. *Soient deux diviseurs D_1, D_2 dans $\mathrm{Div}^0(E)$. Alors $\sigma(D_1) = \sigma(D_2)$ si et seulement si $D_1 \sim D_2$. Ainsi, σ induit une bijection $\mathrm{Pic}^0(E) \simeq E$;*
4. *L'application inverse de σ est $\kappa : E \tilde{\to} \mathrm{Pic}^0(E)$, $P \mapsto$ classe de $(P) - (O)$.*

Démonstration. Voir [79, Proposition III.3.4]. □

On peut alors montrer que $\kappa(P + Q) = \kappa(P) + \kappa(Q)$, où la première addition est dans E et la deuxième dans $\mathrm{Pic}^0(E)$.

Théorème 1.1.7. *Soit E/K une courbe elliptique. Alors les équations explicites donnant la loi de groupe définissent des morphismes :*

$$+ : \begin{array}{ccc} E \times E & \longrightarrow & E \\ (P, Q) & \longmapsto & P + Q \end{array} \qquad \text{et} \qquad - : \begin{array}{ccc} E & \longrightarrow & E \\ P & \longmapsto & -P \end{array}$$

Démonstration. Voir [79, Théorème III.3.6]. □

1.1.3 Applications entre courbes elliptiques

Nous nous intéressons maintenant aux applications entre courbes elliptiques. Étant donné qu'on met en valeur un point de la courbe, l'origine, il apparaît naturel de considérer les applications qui envoient l'origine de la première courbe elliptique vers celle de la seconde.

Définition 1.1.8. *Soient E_1/K et E_2/K deux courbes elliptiques. Une* isogénie *entre E_1 et E_2 est un morphisme $\phi : E_1/\overline{K} \to E_2/\overline{K}$ tel que $\phi(O_{E_1}) = O_{E_2}$. On dit que ces courbes sont* isogènes *si l'isogénie vérifie $\phi(E_1) \neq \{O_{E_2}\}$.*

On peut montrer d'une part qu'une isogénie est soit constante, soit surjective. Dans ce dernier cas, l'isogénie est une application finie entre les courbes et ainsi on a une injection entre les corps de fonctions $\phi^* : f \in \overline{K}(E_2) \hookrightarrow f \circ \phi \in \overline{K}(E_1)$. On définit alors le *degré* de l'isogénie comme étant le degré de l'extension finie $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ (et par convention, le degré de l'isogénie constante est 0).

D'autre part, une isogénie est un morphisme de groupe ([79, Théorème III.4.8]). Posons $\mathrm{Hom}(E_1, E_2)$ l'ensemble contenant les isogénies entre E_1 et E_2. Alors d'après le théorème 1.1.7, c'est un groupe où l'addition est $(\phi + \psi)(P) = \phi(P) + \psi(P)$. Si de plus $E = E_1 = E_2$, on pose $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. C'est un anneau appelé *anneau d'endomorphismes de* E si on ajoute la loi de multiplication suivante : $(\phi\psi)(P) = \phi(\psi(P))$. L'ensemble des éléments inversibles $\mathrm{Aut}(E)$ de $\mathrm{End}(E)$ est appelé *groupe des automorphismes de* E.

Théorème 1.1.9. *Soit E/K une courbe elliptique. Alors son groupe des automorphismes* $\mathrm{Aut}(E)$ *est fini et d'ordre divisant* 24. *Plus précisément, cet ordre est :*

$$\begin{array}{rrcl} 2 & \textit{si } j(E) & \neq & 0 \textit{ ou } 1728; \\ 4 & \textit{si } j(E) & = & 1728 \textit{ et } \mathrm{char}(K) \neq 2, 3; \\ 6 & \textit{si } j(E) & = & 0 \textit{ et } \mathrm{char}(K) \neq 2, 3; \\ 12 & \textit{si } j(E) & = & 0 = 1728 \textit{ et } \mathrm{char}(K) = 3; \\ 24 & \textit{si } j(E) & = & 0 = 1728 \textit{ et } \mathrm{char}(K) = 2. \end{array}$$

Démonstration. Voir [79, Théorème III.10.1]. □

Un exemple important d'isogénie est l'application $[m] : E \to E$ de *multiplication par* m, pour $m \in \mathbb{Z}$. Si $m > 0$, alors $[m](P) = P + \cdots + P$, m fois et si $m < 0$, on la définit par $[m](P) = [-m](-P)$. De plus, on pose que $[0](P) = O$. Cette application est bien dans $\mathrm{End}(E)$ d'après le Théorème 1.1.7. Elle n'est pas constante lorsque $m \neq 0$ et on peut alors montrer que l'anneau $\mathrm{End}(E)$ est un anneau de caractéristique nulle sans diviseurs de zéro ([79, Proposition III.4.2]).

Dans le cas où $\mathrm{char}(K) = 0$, l'application $[\,\cdot\,] : \mathbb{Z} \to \mathrm{End}(E)$ est en général un isomorphisme. Si ce n'est pas le cas, c'est-à-dire si $\mathrm{End}(E)$ contient d'autres éléments que les applications du type multiplication par m, on dit que la courbe elliptique E a *multiplication complexe*. C'est systématiquement le cas lorsque K est un corps fini (il faut alors étudier l'application Frobenius).

Proposition 1.1.10. *L'anneau d'endomorphismes* $\mathrm{End}(E)$ *d'une courbe elliptique est soit $\mathbb{Z}$, soit un ordre d'un corps quadratique imaginaire ou sinon un ordre dans une algèbre de quaternions. Notons que ce dernier cas n'arrive jamais si* $\mathrm{char}(K) = 0$.

Démonstration. Voir [79, Corollaire III.9.4] □

Considérons une isogénie non constante $\phi : E_1 \to E_2$. D'après [79, Corollaire III.4.9], son noyau est un sous-groupe d'indice fini. Si de plus ϕ est séparable, c'est-à-dire si l'extension $K(E_1)/\phi^*(K(E_2))$ est séparable, alors, par [79, Théorème III.4.10], le cardinal de ce noyau est le degré de l'isogénie et l'extension $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ est galoisienne. Or, lorsque $m \in \mathbb{Z}^*$ et $\mathrm{char}(K) = 0$ (ou alors lorsque m est premier avec $\mathrm{char}(K)$), alors [79, Corollaire III.5.4] affirme que l'application multiplication par m est un endomorphisme de E fini et séparable. Ceci conduit à s'intéresser au groupe suivant : le *sous-groupe de m-torsion* d'une

courbe elliptique E, pour $m \neq 0$, est l'ensemble $E[m]$ des points d'ordre divisant m : $E[m] = \{P \in E : [m](P) = O\}$.

Inversement, on a

Proposition 1.1.11. *Soit E une courbe elliptique et soit G un sous-groupe d'indice fini de E. Il existe une unique courbe elliptique E' et une isogénie séparable $\phi : E \to E'$ tels que* $\ker \phi = G$.

Démonstration. Voir [79, Proposition III.4.12]. □

On introduit maintenant la notion d'isogénie duale qui permet entre autre d'étudier l'application multiplication par m. Soit $\phi : E_1 \to E_2$ une isogénie non constante de degré d. Par [79, Théorèmes III.6.1 et III.6.2], il existe une unique isogénie $\hat{\phi} : E_2 \to E_1$, qu'on appelle *isogénie duale*, et qui vérifie $\hat{\phi} \circ \phi = [d]$ et $\phi \circ \hat{\phi} = [d]$. De plus, si $\chi : E_2 \to E_3$ et $\psi : E_1 \to E_2$, alors $\widehat{\chi \circ \phi} = \hat{\phi} \circ \hat{\chi}$ et $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$. Pour tout $m \in \mathbb{Z}$, on a $\widehat{[m]} = [m]$ et par suite

$$\deg([m]) = m^2.$$

Enfin, $\deg(\hat{\phi}) = \deg(\phi)$ et $\hat{\hat{\phi}} = \phi$. Si $\mathrm{char}(K) = 0$, on a alors que

$$E[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),$$

d'après [79, Corollaire III.6.4].

1.2 Lien avec les tores complexes

1.2.1 Fonctions elliptiques

Par *réseau* nous entendrons dans la suite un sous-groupe discret de $\mathbb{C}$ de rang 2. Ainsi, un réseau est engendré par deux nombres $\mathbb{R}$-linéairement indépendants ω_1 et ω_2, que l'on appelle *périodes*, et est donc de la forme $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Il nous arrivera de noter ceci : $\Lambda = [\omega_1, \omega_2]$. Le quotient $\mathbb{C}/\Lambda$ est ce que l'on appelle un *tore complexe*.

Définition 1.2.1. *Un* parallélogramme fondamental *pour un réseau Λ est un ensemble de la forme*

$$\mathcal{F}_\omega = \{\omega + x_1\omega_1 + x_2\omega_2 : 0 \leq x_1, x_2 < 1\},$$

où $\omega \in \mathbb{C}$ et ω_1, ω_2 est une base de Λ. C'est un ensemble de représentants des classes de $\mathbb{C}/\Lambda$.

Définition 1.2.2 (Fonction elliptique)**.** *Soit Λ un réseau. Une* fonction elliptique *sur Λ est une fonction méromorphe $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ qui vérifie pour tous $\omega \in \Lambda$ et $z \in \mathbb{C}$:*

$$f(z + \omega) = f(z). \tag{1.5}$$

Une telle fonction est uniquement déterminée par ses valeurs dans un parallélogramme fondamental. On note $\mathbb{C}(\Lambda)$ l'ensemble de toutes les fonctions elliptiques sur le réseau Λ. C'est un corps.

Proposition 1.2.3. *Une fonction elliptique sans pôles ou sans zéros est constante.*

Démonstration. Voir [79, Proposition VI.2.1] ou [75, Théorème 1.1.4]. □

Soit f une fonction elliptique et soit $\omega \in \mathbb{C}$. On note $\mathrm{ord}_\omega(f)$ et $\mathrm{res}_\omega(f)$ respectivement l'ordre et le résidu de f au point $\omega \in \mathbb{C}$. On remarquera que dans notre cadre, les fonctions sont elliptiques et donc l'ordre et le résidu d'une fonction en un point ω restent inchangés si on remplace ω par $\omega+\omega'$ pour un ω' quelconque dans Λ.

Ceci nous induit à utiliser la convention suivante. Par $\sum_{\omega\in\mathbb{C}/\Lambda}$ on entend une somme sur tous les éléments d'un parallélogramme fondamental du réseau Λ.

Théorème 1.2.4. *Soit $f \in \mathbb{C}(\Lambda)$.*

1. $\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{ord}_\omega(f) = 0$;
2. $\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{res}_\omega(f) = 0$;
3. $\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{ord}_\omega(f)\omega \in \Lambda$.

Démonstration. Voir [79, Théorème VI.2.2] ou [75, Théorème 1.1.3]. □

Pour toute fonction elliptique, on dira que son *ordre* est son nombre de pôles compté avec multiplicité dans un quelconque parallélogramme fondamental.

Corollaire 1.2.5. *Une fonction elliptique non constante a un ordre supérieur ou égal à 2.*

Démonstration. Voir [79, Corollaire VI.2.3] ou [75, Théorème 1.1.4]. Si une fonction elliptique f a un seul pôle, alors par le théorème 1.2.4, le résidu en ce pôle vaut 0 et donc f est holomorphe. On conclut avec la proposition 1.2.3. □

Le *groupe des diviseurs* $\mathrm{Div}(\mathbb{C}/\Lambda)$ du tore est le groupe des sommes formelles de la forme $\sum_{\omega\in\mathbb{C}/\Lambda} n_\omega(\omega)$ avec $n_\omega \in \mathbb{Z}$ et $n_\omega \neq 0$ seulement pour un nombre fini de valeurs. On définit une application de *sommation*

$$\mathrm{som} : D = \sum n_\omega(\omega) \in \mathrm{Div}(\mathbb{C}/\Lambda) \longmapsto \sum n_\omega\omega \in \mathbb{C}/\Lambda$$

et une application *degré*

$$\deg : D = \sum n_\omega(\omega) \in \mathrm{Div}(\mathbb{C}/\Lambda) \longmapsto \sum n_\omega \in \mathbb{Z}.$$

Le noyau de cette dernière application est le sous-groupe $\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) : \deg(D) = 0\}$ de $\mathrm{Div}(\mathbb{C}/\Lambda)$ des diviseurs de degré zéro.

Pour chaque fonction elliptique $f \in \mathbb{C}(\Lambda)^*$, on peut définir le diviseur $\mathrm{div}(f) \in \mathrm{Div}^0(\mathbb{C}/\Lambda)$ par $\mathrm{div}(f) = \sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{ord}_\omega(f)(\omega)$ (on est bien dans le groupe des diviseurs de degré zéro d'après le théorème 1.2.4). L'application $\mathrm{div} : \mathbb{C}(\Lambda)^* \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ est un homomorphisme.

Théorème 1.2.6. *La suite suivante est exacte :*

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\Lambda)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\mathrm{som}} \mathbb{C}/\Lambda \longrightarrow 0$$

Démonstration. Voir [79, Théorème VI.2.4]. □

Le quotient $\mathrm{Jac}(\mathbb{C}/\Lambda) := \mathrm{Div}^0(\mathbb{C}/\Lambda)/\,\mathrm{div}(\mathbb{C}(\Lambda)^*)$ est appelé la *Jacobienne* de $\mathbb{C}/\Lambda$. Le théorème précédent affirme que le tore $\mathbb{C}/\Lambda$ est isomorphe à sa Jacobienne.

1.2.2 Construction de fonctions elliptiques

La fonction σ de Weierstrass relativement à un réseau Λ est :

$$\sigma_\Lambda(z) = z \prod_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right). \tag{1.6}$$

Le produit infini σ_Λ définit une fonction holomorphe sur tout $\mathbb{C}$ et converge absolument ([75, Lemme 1.2.1]). Il a un zéro de multiplicité 1 en chaque point ω du réseau Λ et seulement en ces points-là. Cette fonction n'est pas elliptique. Par contre, nous allons voir comment on peut construire toutes les fonctions elliptiques à partir d'elle.

En prenant la dérivée logarithmique de σ_Λ, on obtient la *fonction zêta de Weierstrass* qui elle non plus n'est pas elliptique :

$$\zeta_\Lambda(z) = (\log(\sigma_\Lambda(z)))' = \frac{\sigma'_\Lambda(z)}{\sigma_\Lambda(z)} = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right) \tag{1.7}$$

et en dérivant encore une fois, on obtient la *fonction $\wp_\Lambda$ de Weierstrass* :

$$\wp_\Lambda(z) = -\zeta'_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \tag{1.8}$$

et par suite sa dérivée :

$$\wp'_\Lambda = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}\,. \tag{1.9}$$

Cette dernière fonction est méromorphe et sa série converge absolument sur tout compact de $\mathbb{C}-\Lambda$. C'est clairement une fonction elliptique. C'est aussi une fonction impaire d'ordre 3 et a trois zéros simples aux *demi-périodes* de $\Lambda = [\omega_1, \omega_2]$: $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$. En effet, soit ω une de ces trois demi-périodes. On a alors $2\omega \in \Lambda$ et puisque $\wp'_\Lambda$ est elliptique, $\wp'_\Lambda(\omega) = \wp'_\Lambda(\omega - 2\omega) = \wp'_\Lambda(-\omega)$. Le fait que cette fonction soit impaire nous dit alors que $\wp'_\Lambda(\omega) = -\wp'_\Lambda(\omega)$ et donc que $\wp'_\Lambda(\omega) = 0$.

La fonction de Weierstrass $\wp_\Lambda$ est définie par une série qui converge absolument et uniformément sur tout compact de $\mathbb{C} - \Lambda$. Cette fonction est méromorphe sur $\mathbb{C}$ et a un double pôle de résidu 0 en chaque point du réseau et pas d'autres pôles ([79, Théorème VI.3.1]). Du fait que $\wp'_\Lambda$ est elliptique, on déduit pour tous $z \in \mathbb{C}$ et $\omega \in \Lambda$ que $\wp_\Lambda(z+\omega) = \wp_\Lambda(z) + c$ où c est une constante. Si on pose alors $z = -\frac{\omega}{2}$, on obtient que $\wp_\Lambda(\frac{\omega}{2}) = \wp_\Lambda(-\frac{\omega}{2}) + c$. En remarquant que la fonction $\wp_\Lambda$ de Weierstrass est paire, on trouve $c = 0$ et on conclut que $\wp_\Lambda$ est également une fonction elliptique.

Proposition 1.2.7 (Abel-Jacobi)**.** *Soient $n_1,\ldots,n_r \in \mathbb{Z}$ et $z_1,\ldots,z_r \in \mathbb{C}$ satisfaisant $\sum_{i=1}^r n_i = 0$ et $\sum_{i=1}^r n_i z_i \in \Lambda$. Alors il existe une fonction elliptique $f \in \mathbb{C}(\Lambda)$ avec la propriété que $\mathrm{div}(f) = \sum_{i=1}^r n_i(z_i)$. Plus précisément, si on normalise de telle sorte que $\sum_{i=1}^r n_i z_i = 0$, alors on peut prendre $f(z) = \prod_{i=1}^r \sigma_\Lambda(z-z_i)^{n_i}$.*

Démonstration. Voir [79, Proposition VI.3.4] ou [75, Théorème 1.3.1]. □

Exemple 1.2.8. *À titre d'exemple, on peut considérer la fonction $\wp_\Lambda(z) - \wp_\Lambda(a)$ pour un certain $a \in \mathbb{C}/\Lambda$. Elle a deux zéros d'ordre 1 aux points a et $-a$ et un*

pôle d'ordre -2 *au point* 0. *Le théorème d'Abel-Jacobi nous dit alors que* $\wp_\Lambda(z) - \wp_\Lambda(a) = c \cdot \frac{\sigma_\Lambda(z+a)\sigma_\Lambda(z-a)}{\sigma_\Lambda(z)^2}$ *pour une certaine constante* c. *On la détermine en multipliant les deux côtés par* $\sigma_\Lambda(z)^2$ *et en prenant la limite pour* $z \to 0$. *On trouve alors* $c = \frac{-1}{\sigma_\Lambda(a)^2}$.

Notons que ceci nous permet d'avoir une autre caractérisation de $\wp'_\Lambda$. *En effet, en partant de l'égalité que l'on vient de montrer :* $\wp_\Lambda(z) - \wp_\Lambda(a) = -\frac{\sigma_\Lambda(z+a)\sigma_\Lambda(z-a)}{\sigma_\Lambda(z)^2\sigma_\Lambda(a)^2}$, *en divisant les deux membres par* $(z-a)$ *et en faisant tendre* a *vers* z, *on trouve que* $\wp'_\Lambda(z) = -\frac{\sigma_\Lambda(2z)}{\sigma_\Lambda(z)^4}$.

Le résultat suivant est fondamental car il dit que toute fonction elliptique s'exprime en fonction de la fonction $\wp_\Lambda$ et de sa dérivée.

Théorème 1.2.9. *Les fonctions elliptiques sont des fractions rationnelles en* $\wp_\Lambda$ *et* $\wp'_\Lambda$ *à coefficients complexes :*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda).$$

Démonstration. Voir [79, Théorème VI.3.2] ou [75, Théorème 1.3.3]. □

1.2.3 Courbes elliptiques et tores complexes

Intéressons nous maintenant au lien entre les fonctions elliptiques et les courbes elliptiques. La *série d'Eisenstein* de poids $2k$ pour Λ est la série :

$$E_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2k}}. \tag{1.10}$$

Une telle série est absolument convergente quelque soit $k > 1$ ([79, Théorème VI.3.1] ou [75, Lemme 1.2.1]). On peut exprimer la fonction $\wp_\Lambda$ de Weierstrass en fonction des séries d'Eisenstein.

Proposition 1.2.10. *La série de Laurent de* $\wp_\Lambda$ *au point* $z = 0$ *est donnée par :*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) E_{2k+2}(\Lambda) z^{2k};$$

Démonstration. Voir [75, Lemme 1.4.2] ou [79, Théorème 3.5]. On écrit dans l'équation (1.8)

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})^2} - 1\right) = \sum_{n=2}^{\infty} n \frac{z^{n-1}}{\omega^{n+1}}.$$

Ensuite, par la convergence absolue, on peut intervertir la somme en ω et la somme en n. De plus, on remarquant que $\sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^k} = 0$ pour tout entier impair $k \geq 3$, on obtient la série de Laurent voulue. □

Notons

$$g_2 := g_2(\Lambda) := 60 E_4(\Lambda),$$

$$g_3 := g_3(\Lambda) := 140 E_6(\Lambda).$$

Théorème 1.2.11. *Les fonctions $\wp_\Lambda$ et $\wp'_\Lambda$ sont reliées algébriquement par la relation :*

$$(\wp'_\Lambda)^2 = 4\wp_\Lambda^3 - g_2\wp_\Lambda - g_3.$$

Le polynôme $4X^3 - g_2X - g_3$ a trois racines distinctes qui sont $e_i = \wp_\Lambda(w_i)$ où les w_i sont les demi-périodes du réseau Λ. On pose que son discriminant est $\Delta(\Lambda) = g_2^3 - 27g_3^2 = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0$ et son j-invariant est $j(\Lambda) = 1728g_2(\Lambda)^3/\Delta(\Lambda)$.

Démonstration. Voir [79, Théorème VI.3.5 et Proposition VI.3.6] et [75, Théorème 1.4.1]. □

Proposition 1.2.12. *Soient un réseau Λ, les valeurs associées g_2, g_3 et $E/\mathbb{C}$ la courbe elliptique $Y^2 = 4X^3 - g_2X - g_3$. Alors l'application :*

$$\begin{array}{rcl} \phi : \mathbb{C}/\Lambda & \longrightarrow & E \subseteq \mathbb{P}^2(\mathbb{C}) \\ z & \longmapsto & [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \\ 0 & \longmapsto & [0 : 1 : 0] \end{array}$$

est un isomorphisme complexe et analytique de groupes de Lie complexes (en d'autres termes, c'est un isomorphisme de surfaces de Riemann qui est aussi un homomorphisme de groupes).

Démonstration. Voir [79, Proposition VI.3.6]. □

Ainsi, à un tore complexe de dimension 1, on peut associer une courbe elliptique complexe. Nous voulons étudier la réciproque, mais avant cela, regardons les morphismes entre différents tores.

Soient Λ_1 et Λ_2 deux réseaux. Si $\alpha \in \mathbb{C}$ vérifie $\alpha\Lambda_1 \subseteq \Lambda_2$, alors l'application holomorphe *multiplication par α*

$$\phi_\alpha : \quad \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2, \quad \phi_\alpha(z) \equiv \alpha z \bmod \Lambda_2$$

est un homomorphisme.

Théorème 1.2.13.

1. *L'application $\alpha \in \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\} \mapsto \phi_\alpha \in \{$applications holomorphes $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ avec $\phi(0) = 0\}$ est une bijection.*
2. *Soient E_1 et E_2 deux courbes elliptiques qui correspondent aux réseaux Λ_1 et Λ_2 (comme dans la proposition 1.2.12). Alors l'inclusion naturelle $\{$isogénies $\phi : E_1 \to E_2\} \to \{$applications holomorphes $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ avec $\phi(0) = 0\}$ est une bijection.*

Démonstration. Voir [79, Théorème VI.4.1]. □

Ainsi, on peut faire correspondre les isogénies entre deux courbes elliptiques $E_1 \simeq \mathbb{C}/\Lambda_1$ et $E_2 \simeq \mathbb{C}/\Lambda_2$ avec les nombres complexes $\alpha \in \mathbb{C}$ tels que $\alpha\Lambda_1 \subseteq \Lambda_2$. Rappelons que l'égalité dénote le fait que les courbes sont isomorphes. Le degré de l'isogénie est alors l'indice $[\Lambda_2 : \alpha\Lambda_1]$ (par convention, cet indice est 0 lorsque $\alpha = 0$).

Le corollaire suivant dit que la notion d'isomorphisme entre courbes elliptiques se traduit en termes d'homothétie dans les réseaux.

Corollaire 1.2.14. *Soient $E_1/\mathbb{C}$ et $E_2/\mathbb{C}$ deux courbes elliptiques correspondant aux réseaux Λ_1 et Λ_2. Alors E_1 et E_2 sont isomorphes sur $\mathbb{C}$ si et seulement si Λ_1 et Λ_2 sont homothétiques, c'est-à-dire si et seulement si $\Lambda_1 = \alpha\Lambda_2$ pour un certain $\alpha \in \mathbb{C}^*$.*

Théorème 1.2.15 (Théorème d'uniformisation)**.** *Soient $A, B \in \mathbb{C}$ tels que $A^3 - 27B^2 \neq 0$. Alors il existe un unique réseau Λ vérifiant $g_2(\Lambda) = A$ et $g_3(\Lambda) = B$.*

Démonstration. Voir [79, Théorème VI.5.1]. □

Corollaire 1.2.16. *Soit $E/\mathbb{C}$ une courbe elliptique. Alors il existe un réseau Λ unique à homothétie près et un isomorphisme analytique complexe :*

$$\begin{array}{rccl} \phi : \mathbb{C}/\Lambda & \to & E \subseteq \mathbb{P}^2(\mathbb{C}) \\ z & \mapsto & [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \\ 0 & \longmapsto & [0:1:0] \end{array}$$

de groupes de Lie complexes.

Démonstration. Voir [79, Corollaire VI.5.1.1]. L'existence provient des théorèmes d'uniformisation et 1.2.12, tandis que l'unicité provient du corollaire 1.2.14. □

Nous avons donc montré l'équivalence entre les notions de tores complexes et de courbes elliptiques sur $\mathbb{C}$. On pourrait d'ailleurs se demander quelle est la fonction inverse de l'application ϕ du corollaire 1.2.16. Le résultat suivant nous fournit la réponse à cette question.

Proposition 1.2.17. *Soit $E/\mathbb{C}$ une courbe elliptique avec x et y comme coordonnées de Weierstrass.*

1. *Soient α et β deux lacets de $E(\mathbb{C})$ formant une base de $H_1(E, \mathbb{Z})$. Alors les périodes*
$$\omega_1 = \int_\alpha dx/y \qquad et \qquad \omega_2 = \int_\beta dx/y$$
sont $\mathbb{R}$-linéairement indépendantes ;
2. *Soit Λ le réseau engendré par ω_1 et ω_2. Alors l'application*
$$F : E(\mathbb{C}) \longrightarrow \mathbb{C}/\Lambda, \qquad F(P) = \int_O^P dx/y \bmod \Lambda$$
est un isomorphisme analytique complexe de groupes de Lie. C'est l'application inverse de celle du corollaire 1.2.16.

Démonstration. Voir [79, Proposition VI.5.2]. □

Soit $E/\mathbb{C}$ une courbe elliptique. On a vu que l'on peut écrire $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. L'anneau d'endomorphismes s'écrit alors $\mathrm{End}(E) \simeq \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$. Puisque le réseau est unique à homothétie près, cet anneau ce dépend pas du réseau.

Théorème 1.2.18. *Soit $E/\mathbb{C}$ une courbe elliptique et soient ω_1 et ω_2 des générateurs pour le réseau Λ associé à E. Alors soit $\mathrm{End}(E) = \mathbb{Z}$, sinon $\mathbb{Q}(\omega_1/\omega_2)$ est une extension quadratique imaginaire de $\mathbb{Q}$ et $\mathrm{End}(E)$ est isomorphe à un ordre de $\mathbb{Q}(\omega_1/\omega_2)$.*

Démonstration. Voir [79, Théorème VI.5.5]. On peut rapprocher ce résultat avec celui de la proposition 1.1.10. □

Rappelons enfin qu'une courbe elliptique est un groupe et donc sa loi de groupe doit pouvoir s'exprimer en fonction de $\wp_\Lambda$. On a en effet le résultat suivant :

Théorème 1.2.19 (Formule d'addition pour la fonction $\wp_\Lambda$)**.** *Soient $z, z' \in \mathbb{C}-\Lambda$. On a alors :*

$$\wp_\Lambda(z+z') = -\wp_\Lambda(z) - \wp_\Lambda(z') + \frac{1}{4}\left(\frac{\wp'_\Lambda(z)-\wp'_\Lambda(z')}{\wp_\Lambda(z)-\wp_\Lambda(z')}\right)^2 \quad si\ z \not\equiv \pm z' \bmod \Lambda$$

$$et \qquad \wp_\Lambda(2z) = -2\wp_\Lambda(z) + \frac{1}{4}\left(\frac{\wp''_\Lambda(z)}{\wp'_\Lambda(z)}\right)^2 \quad si\ 2z \not\equiv 0 \bmod \Lambda.$$

Démonstration. Voir [75, Théorème 1.4.4]. □

1.3 Espace de Modules

1.3.1 Demi-plan de Poincaré

Une autre description des courbes elliptiques est possible en utilisant le fait qu'étudier un tore c'est essentiellement étudier un réseau et que dans notre cadre, on considère les réseaux à homothétie près (rappelons le corollaire 1.2.14).

Soit donc un réseau $\Lambda = [\omega_1, \omega_2]$. Quitte à échanger ω_1 et ω_2, on peut supposer que le quotient $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$ a une partie imaginaire positive.

Définition 1.3.1. *On appelle* demi-plan de Poincaré*, que l'on note $\mathcal{H}_1$, le demi-plan complexe supérieur :*

$$\mathcal{H}_1 = \{z \in \mathbb{C} : \Im(z) > 0\}.$$

On l'étend parfois on considérant les pointes :

$$\mathcal{H}_1^* = \mathcal{H}_1 \cup \mathbb{Q} \cup \{\infty\}.$$

Tout réseau est homothétique à un réseau de la forme $[1, \tau]$ pour un certain $\tau \in \mathcal{H}_1$. De plus, deux réseaux $[1, \tau_1]$ et $[1, \tau_2]$ de cette forme sont homothétiques si et seulement si $\tau_2 = \frac{a\tau_1+b}{c\tau_1+d}$ pour une certaine matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Un simple calcul montre que l'on a

$$\Im\left(\frac{a\tau+b}{c\tau+d}\right) = (ad-bc)\frac{\Im(\tau)}{|c\tau+d|^2} \tag{1.11}$$

et en particulier, les matrices de $\mathrm{SL}_2(\mathbb{Z})$ envoient $\mathcal{H}_1$ dans lui-même.

Définition 1.3.2. *On appelle* groupe modulaire*, noté Γ_1, le groupe $\mathrm{SL}_2(\mathbb{Z})$:*

$$\Gamma_1 := \mathrm{SL}_2(\mathbb{Z}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, \det(M) = 1 \right\}.$$

Par ce qui précède, le groupe modulaire agit sur le demi-plan de Poincaré : on a l'action de groupe

$$\Gamma_1 \times \mathcal{H}_1 \longrightarrow \mathcal{H}_1, \quad (\gamma, \tau) \longmapsto \gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Remarquons que la matrice $-I_2$ agit trivialement sur $\mathcal{H}_1$. C'est pourquoi certains auteurs préfèrent considérer le groupe $\mathrm{PSL}_2(\mathbb{Z})$ plutôt que $\mathrm{SL}_2(\mathbb{Z})$. L'action du groupe modulaire sur le demi-plan de Poincaré est proprement discontinue ([4, Proposition 8.2.5]), c'est-à-dire que tout $\tau \in \mathcal{H}_1$ a un voisinage V tel que

$$\forall \gamma \in \Gamma_1, \quad \gamma V \cap V \neq \emptyset \implies \gamma \cdot \tau = \tau.$$

On en déduit que le quotient $\mathcal{H}_1/\Gamma_1$ hérite de $\mathcal{H}_1$ une topologie de Hausdorff. On peut aller plus loin et montrer que ce quotient est une surface de Riemann, qui n'est compacte que lorsque l'on ajoute les pointes.

Cette action de groupe se prolonge facilement en une action sur $\mathcal{H}_1^*$. Il suffit de poser pour $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ et $\frac{p}{q} \in \mathbb{Q}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \begin{cases} \frac{a}{c} & \text{si } c \neq 0, \\ \infty & \text{si } c = 0 \end{cases}$$

et

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{p}{q} = \begin{cases} \frac{ap+bq}{cp+dq} & \text{si } cp + dq \neq 0, \\ \infty & \text{si } cp + dq = 0. \end{cases}$$

Ainsi, $\mathbb{Q} \cup \{\infty\}$ est l'orbite de ∞ sous cette action. Posons

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{1.12}$$

Proposition 1.3.3. *Le groupe modulaire Γ_1 est engendré par S et T.*

Démonstration. Voir [19, Proposition 2.1]. Soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$. Montrons le résultat par récurrence sur $|a| + |c|$. Supposons que $|a| + |c| = 1$. Alors, quitte à multiplier à gauche par S, on a $|a| = 1$ et $|c| = 0$, et, par suite, quitte à multiplier par $S^2 = -I_2$, la matrice γ est de la forme $\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right) = T^c$.

Supposons maintenant qu'il existe $n \geq 1$ tel que la propriété à montrer soit vraie pour toute matrice $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ de Γ_1 avec $|a'|+|c'| \leq n$. Si γ vérifie $|a|+|c| = n+1$, alors en multipliant éventuellement γ à gauche par S, on peut supposer $|a| \geq |c|$. On écrit la division euclidienne de a par c : $a = qc + r$, avec $0 \leq r < |c|$. On a donc $T^{-q}\gamma = \left(\begin{smallmatrix} r & b-qd \\ c & d \end{smallmatrix}\right)$ qui est, par hypothèse de récurrence, engendré par S et T. Ceci conclut la démonstration. □

Posons maintenant

$$\mathcal{F}_1 = \{\tau \in \mathcal{H}_1 : |\tau| \geq 1, |\Re(\tau)| \leq \frac{1}{2}\}$$

et

$$\mathcal{F} = \mathcal{F}_1 \backslash (\delta\mathcal{F}_1 \cap \{\tau \in \mathcal{H}_1 : \Re(\tau) > 0\})$$

Définition 1.3.4 (Domaine fondamental, ensemble fondamental)**.** *Soit G un groupe agissant sur un ensemble X muni d'une topologie. Un ensemble $Y \subseteq X$ connexe est un* domaine fondamental *pour l'action de G sur X si :*

— *Pour tout $x \in X$, il existe $g \in G$ et $y \in Y$ tels que $y = g \cdot x$;*
— *Pour tous $y_1, y_2 \in Y$ et $g \in G \backslash \{1\}$ tels que $y_1 = g \cdot y_2$, on a $y_1 \in \delta(Y)$ et $y_2 \in \delta(Y)$.*

Un ensemble $Y \subseteq X$ est un ensemble fondamental *pour l'action de G sur X si, pour tout $x \in X$, il existe un unique $y \in Y$ qui soit dans l'orbite de x sous l'action de G.*

Un ensemble fondamental est donc toujours un domaine fondamental mais la réciproque n'est pas forcément vraie.

Proposition 1.3.5. *La région $\mathcal{F}$ est un ensemble fondamental pour l'action de $\Gamma_1/\langle \pm I_2 \rangle$ sur $\mathcal{H}_1$ et donc $\mathcal{F}_1$ est un domaine fondamental pour cette action. De plus, on a*

$$\mathrm{card}(\{\gamma \in \Gamma_1/\langle \pm I_2 \rangle : \tau_0 = \gamma \cdot \tau_0\}) = \begin{cases} 2 & \text{si } \tau_0 = \imath, \\ 3 & \text{si } \tau_0 = \exp\left(\frac{2\imath\pi}{3}\right), \\ 1 & \text{sinon.} \end{cases}$$

Démonstration. Voir [19, Proposition 2.2]. □

1.3.2 Sous-groupes du groupe modulaire

Nous allons étudier dans cette section différents sous-groupes de Γ_1. Tout d'abord, notons que l'on est également capable de construire un domaine fondamental pour tout sous-groupe du groupe modulaire.

Théorème 1.3.6. *Soient $\Gamma < \Gamma_1$ et γ_j un système de représentants des classes (à droite) de $\Gamma_1/(\Gamma \cup (-\Gamma))$. Alors*

$$\mathcal{F}_\Gamma = \bigcup_j \gamma_j(\mathcal{F}_1)$$

est un domaine fondamental pour Γ.

Démonstration. Voir [75, Théorème 2.1.4] ou [19, Proposition 2.3]. □

Ce théorème conduit à l'algorithme 1.3.1. Nous ne l'étudierons pas en détail mais renvoyons le lecteur à [19, Pages 46-48].

Continuons avec un lemme qui joue un rôle fondamental dans ce qui va suivre. Soit N un entier positif. On a alors :

Lemme 1.3.7. *L'homomorphisme de groupe $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ est surjectif.*

Démonstration. Soit $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ un représentant de cette classe dans $M_2(\mathbb{Z})$.

— On a tout d'abord que $\gcd(c, d, N) = 1$ car $ad - bc \equiv 1 \bmod N$;
— Maintenant si $c \neq 0$, alors on pose $t = \prod_{\substack{p \mid c \\ p \nmid d}} p$ et $d' = d + tN$. On a que $\gcd(c, d') = 1$. En effet, soit un premier p qui divise c. Si $p \nmid d$, alors $p \mid t$ et alors $p \nmid d'$. Sinon si $p \mid d$, alors $p \nmid t$, $p \mid \gcd(c, d)$ et puisque $\gcd(c, d, N) = 1$, alors $p \nmid N$ et donc $p \nmid d'$;

Algorithme 1.3.1 : Domaine fondamental et générateurs d'un sous-groupe d'indice fini de Γ_1

Entrée : Pour un sous-groupe Γ de Γ_1 d'indice fini, une fonction qui décide si un élément de Γ_1 est dans Γ ou pas, plus un ensemble de générateurs $V = \{\gamma_j\}_{j\in\{1,\dots,n\}}$ de Γ_1.

Sortie : Un ensemble S de représentants des classes Γ_1/Γ et un ensemble fini G de générateurs de Γ.

```
1  S = {I_2};
2  D = {I_2};
3  G = ∅;
4  tant que V ≠ ∅ faire
5  |  choisir γ ∈ V;
6  |  t = vrai;
7  |  pour γ' ∈ S faire
8  |  |  si γ'γ^{-1} ∈ Γ alors
9  |  |  |  t = faux;
10 |  |  |  G = G ∪ {γ'γ^{-1}};
   |  |  fin
   |  fin
11 |  si t = vrai alors
12 |  |  S = S ∪ {γ};
13 |  |  V = V ∪ ({γγ_j : j ∈ {1,...,n}}\D);
   |  fin
14 |  V = V\{γ};
15 |  D = D ∪ {γ};
   fin
16 retourner (S, G);
```

— Toujours si $c \neq 0$, il existe donc $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha c - \beta d' = 1$. On a aussi que $ad' - bc \equiv 1 \bmod N$ ce qui implique qu'il existe $k \in \mathbb{Z}$ tel que $ad'-bc = 1+kN$ et alors on a $ad'-bc = 1+kN = 1+(\alpha kc-\beta kd')N$ et donc $(a+\beta kN)d' - (b+\alpha kN)c = 1$ et la matrice $\begin{pmatrix} a+\beta kN & b+\alpha kN \\ c & d' \end{pmatrix} \in \Gamma_1$ est dans la même classe que γ ;

— Dans le cas où $c = 0$, on déduit de $\mathrm{pgcd}(c, d, N) = 1$ que $\mathrm{pgcd}(d, N) = 1$ et par suite que $d \equiv 1 \bmod N$. De $ad \equiv 1 \bmod N$ on déduit que $a \equiv 1 \bmod N$ et alors la matrice $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1$ est dans la même classe que γ.

□

On appelle *sous-groupe principal de congruence et de niveau N* le sous-groupe

$$\Gamma_1(N) = \{\gamma \in \Gamma_1 : \gamma \equiv I_2 \bmod N\}. \tag{1.13}$$

Un tel sous-groupe est le noyau de l'application de réduction $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et est d'indice fini : $[\Gamma_1 : \Gamma_1(N)] = N^3 \prod_{p|N}(1 - \frac{1}{p^2})$. Ainsi, $\Gamma_1(N)$ est un sous-groupe normal de Γ_1 et on a

$$\Gamma_1/\Gamma_1(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}). \tag{1.14}$$

Tout groupe Γ vérifiant $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_1$ pour un certain $N \in \mathbb{N}$ est dit un *sous-groupe de congruence modulo N*. Ces groupes sont d'indice fini dans Γ_1. Soit

$$\mathbb{P}_r = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = r,\ \text{pgcd}(a, b, c, d) = 1 \right\}$$

l'ensemble des matrices primitives de déterminant $r \in \mathbb{N}$. Ce n'est pas un groupe.

Proposition 1.3.8. *Pour tout $R_0 \in \mathbb{P}_r$, on a $\mathbb{P}_r = \Gamma_1 R_0 \Gamma_1$.*

Démonstration. Voir [75, Proposition 2.2.1]. □

Pour une matrice $R \in \mathbb{P}_r$, on considère maintenant le sous-groupe de Γ_1 :

$$\Gamma_R = \Gamma_1 \cap R^{-1}\Gamma_1 R.$$

(Pour être plus cohérent, il faudrait noter ce groupe $\Gamma_{1,R}$. Nous ne le ferons pas dans un souci d'allégement des notations). Les cas qui nous intéressent le plus sont lorsque l'on prend les matrices $\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right)$, où l'on obtient les deux groupes suivants

$$\begin{aligned} \Gamma_0(r) &:= \Gamma_{\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1 : c \equiv 0 \bmod r \right\}, \\ \Gamma^0(r) &:= \Gamma_{\left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right)} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1 : b \equiv 0 \bmod r \right\}. \end{aligned} \tag{1.15}$$

De manière générale, on a

Théorème 1.3.9. *Soit $R \in \mathbb{P}_r$. Le sous-groupe Γ_R est un sous-groupe de congruence modulo r.*

Démonstration. Voir [75, Théorème 2.2.2]. Soit $R \in \mathbb{P}_r$. D'après la proposition 1.3.8, il existe deux matrices M_1 et M_2 dans Γ_1 telles que l'on ait l'égalité $R = M_1 \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) M_2$. Il en découle que $\Gamma_R = \Gamma_{M_1\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)M_2}$. Or, $\Gamma_{M_1\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)M_2} = \Gamma_1 \cap (M_1 \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) M_2)^{-1}\Gamma_1(M_1 \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) M_2) = \Gamma_1 \cap (\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) M_2)^{-1}\Gamma_1(\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) M_2) = \Gamma_{\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)M_2}$. Par le théorème 1.3.10, on a que $\Gamma_R = M_2^{-1}\Gamma_{\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)}M_2$, et en utilisant, le fait que $\Gamma_1(r)$ est un sous-groupe normal de Γ_1, on en déduit l'inclusion $\Gamma_1(r) = M_2^{-1}\Gamma_1(r)M_2 \subseteq M_2^{-1}\Gamma_{\left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right)}M_2 = \Gamma_R$. □

Théorème 1.3.10. *Pour $R, R' \in \mathbb{P}_r$ et $M, M' \in \Gamma_1$, on a :*

1. $\Gamma_1 R = \Gamma_1 R' \implies \Gamma_R = \Gamma_{R'}$;
2. $M^{-1}\Gamma_R M = \Gamma_{RM}$;
3. $\Gamma_R M = \Gamma_R M' \iff \Gamma_1 RM = \Gamma_1 RM'$.

Démonstration. Voir [75, Théorème 2.2.3]. □

En appliquant la troisième propriété de ce théorème, on obtient une description des classes à droite de Γ_1/Γ_R, qui nous induit à définir sur $\mathbb{P}_r$ la relation d'équivalence

$$R \sim R' \iff \Gamma_1 R = \Gamma_1 R'.$$

Théorème 1.3.11. *Le nombre de classes d'équivalences modulo $\sim$ est fini. Un système de représentants est donné par les matrices triangulaires :*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ a > 0,\ ad = r,\ \text{pgcd}\,(a, b, d) = 1,\ b \in \{0, \ldots, d-1\}.$$

Démonstration. Voir [75, Théorème 2.2.4]. □

Les résultats qui précèdent permettent de démontrer le théorème suivant.

Théorème 1.3.12. *Soient $R_1, \ldots, R_{\psi(r)}$ un système de représentants de $\mathbb{P}_r$ modulo $\sim$ et R une matrice arbitraire dans $\mathbb{P}_r$. Alors il existe des matrices unimodulaires γ_i avec $\Gamma_1 R_i = \Gamma_1 R \gamma_i$ pour $i = 1, \ldots, \psi(r)$. On en déduit que*

$$\Gamma_1 = \bigsqcup_{i=1}^{\psi(r)} \Gamma_R \gamma_i$$

et en particulier $[\Gamma_1 : \Gamma_R] = \psi(r) = r \prod_{p|r}(1 + \frac{1}{p})$.

Démonstration. On a d'une part que

$$\Gamma_R \gamma_i = (\Gamma_1 \cap R^{-1}\Gamma_1 R)\gamma_i = \Gamma_1 \cap R^{-1}\Gamma_1 R\gamma_i = \Gamma_1 \cap R^{-1}\Gamma_1 R_i.$$

Ceci nous permet d'écrire

$$\bigsqcup \Gamma_R \gamma_i = \Gamma_1 \cap R^{-1} \left(\bigsqcup \Gamma_1 R_i \right) = \Gamma_1 \cap R^{-1}\mathbb{P}_r = \Gamma_1,$$

car $\Gamma_1 \subseteq R^{-1}\mathbb{P}_r$. En effet, pour $\gamma \in \Gamma_1$, on a $\gamma = R^{-1}R\gamma$ et $R\gamma \in \mathbb{P}_r$ car $R\gamma = I_2 R\gamma \in \Gamma_1 R \Gamma_1 = \mathbb{P}_r$, par la proposition 1.3.8. L'indice provient du théorème 1.3.11. Voir aussi [75, Théorème 2.2.5]. □

Appliquons ce théorème sur la matrice $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ où p est un nombre premier. On peut prendre, d'après le théorème 1.3.11, $R_1 = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $R_2 = R$, $R_3 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & p \end{smallmatrix}\right)$, $R_4 = \left(\begin{smallmatrix} 1 & 2 \\ 0 & p \end{smallmatrix}\right)$, …, $R_{p+1} = \left(\begin{smallmatrix} 1 & p-1 \\ 0 & p \end{smallmatrix}\right)$. On montre facilement que l'on a les relations suivantes : $R_1 = S^{-1}RS$, $R_2 = R$, $R_3 = RT$, …, $R_{p+1} = RT^{p-1}$. Ainsi, on prend $\gamma_1 = S$ et $\gamma_k = T^{k-2}$ pour k allant de 2 à $p+1$. Ces matrices γ_i sont alors les représentants des classes à droite du quotient Γ_1/Γ_R.

1.4 Formes et fonctions modulaires

Nous allons introduire dans cette partie les notions de formes et fonctions modulaires et présenter des propriétés importantes de ces dernières. L'idée sous-jacente à ces notions est de considérer des fonctions sur la courbe modulaire $\mathcal{H}_1/\Gamma_1$: on veut en particulier des fonctions qui donnent la même valeur pour des points qui soient équivalents et ceci modulo Γ_1 ou modulo un de ses sous-groupes. On veut aussi que ces fonctions aient un bon comportement "à l'infini". Pour cela, nous allons commencer par parler des formes modulaires, qui nous permettront par la suite de définir les fonctions modulaires.

1.4.1 Formes modulaires

Définition 1.4.1. *Soit Γ un sous-groupe de Γ_1 d'indice fini. On dit qu'une fonction $f : \mathcal{H}_1 \to \mathbb{C}$ vérifie la* condition de modularité *sur Γ et pour un certain poids $k \in \mathbb{N}$ si l'on a pour tous $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ et $\tau \in \mathcal{H}_1$*

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau). \tag{1.16}$$

On peut s'étonner de la présence de ce facteur $(c\tau+d)^k$ mais il s'explique très bien quand on revient à la description des courbes elliptiques complexes avec les réseaux : on veut une fonction f qui vérifie pour $\alpha \in \mathbb{C}^*$: $f(\alpha\Lambda) = \alpha^{-k} f(\Lambda)$. On a donc pour $\gamma \in \Gamma$,

$$f(\gamma\cdot\tau) = f\left(\left[\frac{a\tau+b}{c\tau+d}, 1\right]\right) = f((c\tau+d)^{-1}[a\tau+b, c\tau+d]) =$$

$$(c\tau+d)^k f([a\tau+b, c\tau+d]) = (c\tau+d)^k f([\tau,1]) = (c\tau+d)^k f(\tau).$$

Soit un sous-groupe Γ de Γ_1 d'indice fini. Remarquons que puisqu'il est d'indice fini, il existe nécessairement un $r \in \mathbb{N}^*$ tel que $T^r \in \Gamma$ (où T est la matrice de l'équation 1.12). Soit alors une fonction $f : \mathcal{H}_1 \to \mathbb{C}$ holomorphe et vérifiant la condition de modularité pour un poids k sur Γ. Si on applique cette dernière propriété sur T^r, on obtient : $f(\tau+r) = f(T^r\tau) = (0\tau+1)^k f(\tau) = f(\tau)$ et ainsi la fonction f est périodique de période r. Elle admet donc un développement de Fourier de la forme :

$$f(\tau) = \sum_{n\in\mathbb{Z}} f_n \exp(2\imath\pi\tau n/r) = \sum_{n\in\mathbb{Z}} f_n q^{\frac{n}{r}}, \quad q = \exp(2\imath\pi\tau).$$

La fonction f est dite *holomorphe à l'infini* si $f_n = 0$ pour $n < 0$. Pour un point $\frac{a}{c} \in \mathbb{Q}$, on sait qu'il existe $\gamma \in \Gamma_1$ tel que $\frac{a}{c} = \gamma\cdot\infty$. La fonction $f_\gamma : \tau \in \mathcal{H}_1 \mapsto (c\tau+d)^{-k} f(\gamma\cdot\tau) \in \mathbb{C}$ est holomorphe et vérifie la condition de modularité pour le poids k et sur le groupe $\gamma^{-1}\Gamma\gamma$. On dit alors que f est *holomorphe en* $\frac{a}{c}$ si la fonction f_γ est holomorphe à l'infini.

Définition 1.4.2 (Forme modulaire)**.** *Une* forme modulaire *de poids k pour un sous-groupe Γ d'indice fini de Γ_1 est une fonction $f : \mathcal{H}_1 \to \mathbb{C}$ qui :*

1. *Est holomorphe sur $\mathcal{H}_1$;*
2. *Est holomorphe aux pointes ;*
3. *Vérifie la condition de modularité pour k et Γ.*

Si de plus on a que, pour tout $\gamma \in \Gamma_1$, le coefficient de degré 0 du développement en série de Fourier de f_γ est nul, alors on dit que la forme est parabolique*.*

Remarquons tout de suite que si $-I_2 \in \Gamma$, alors il n'y a pas de formes modulaires de poids impair (hormis la fonction nulle). En effet, on remarque que $-\gamma \in \Gamma$ pour tout $\gamma \in \Gamma$, que $(-\gamma)\cdot\tau = \gamma\cdot\tau$ et qu'on a alors

$$f(\gamma\cdot\tau) = f((-\gamma)\cdot\tau) = (-c\tau-d)^k f(\tau) = -(c\tau+d)^k f(\tau) = -f(\gamma\cdot\tau).$$

Par contre, pour les sous-groupes qui ne contiennent pas $-I_2$, les formes modulaires de poids 1 prennent une place importante mais on ne sait pas grand chose de la dimension de l'espace qu'elles constituent ([61, Remarque 7]). Notons par ailleurs qui si on avait posé $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})/\langle\pm 1\rangle$, alors les formes modulaires de poids impairs seraient toutes nulles. Dans la suite, on considèrera toujours des sous-groupes qui contiennent $-I_2$ car c'est le cas des sous-groupes qui nous intéressent.

On note M_k le $\mathbb{C}$-espace vectoriel des formes modulaires de poids k sur tout Γ_1 et S_k le sous-espace vectoriel des formes paraboliques de poids k sur Γ_1. Les espaces vectoriels des formes modulaires de même niveau sont en somme directe ([61, Lemme 13]). Nous allons étudier la dimension de ces espaces.

Pour cela, rappelons tout d'abord que l'on a défini la série d'Eisenstein pour $k > 1$ par : $E_{2k}(\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^{2k}}$. C'est une forme modulaire de poids $2k$ sur Γ_1. Rappelons que la condition $k > 1$ est nécessaire pour garantir la convergence absolue de la série. De plus, notons qu'on veut $2k$ car pour k impair, la série E_k est nulle car les termes (m, n) et $(-m, -n)$ s'annulent.

Théorème 1.4.3. *Pour $k > 1$ on a :*

$$E_{2k}(\tau) = \frac{2(2\imath\pi)^{2k}}{(2k-1)!}\left(-\frac{B_{2k}}{4k} + \sum_{m=1}^{\infty} \sigma_{2k-1}(m)q^m\right) \tag{1.17}$$

où $q = \exp(2\imath\pi\tau)$, B_m désigne le m-ième nombre de Bernoulli et $\sigma_k(n) = \sum_{0<d|n} d^k$ est la fonction somme des puissances k-ièmes des diviseurs de l'entier n.

Démonstration. Voir [75, Théorème 1.8.4]. □

Pour plus de commodité, on va considérer dans la suite les fonctions

$$G_k = \frac{(k-1)!}{2(2\imath\pi)^k} E_k, \tag{1.18}$$

pour k pair supérieur ou égal à 4. Notons que le membre de droite de (1.17) a un sens pour $2k = 2$ ce qui nous permet de définir une fonction $G_2(\tau)$. Ce n'est pas une forme modulaire. Par contre, on peut définir la fonction non holomorphe $G_2^*(\tau) = G_2(\tau) + \frac{1}{8\pi\Im(\tau)}$ qui vérifie la condition de modularité pour $k = 2$ sur Γ_1. Un simple calcul montre alors que l'on a pour $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$:

$$G_2\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 G_2(\tau) - \frac{c(c\tau+d)}{4\imath\pi}. \tag{1.19}$$

Définissons aussi la fonction *discriminant* Δ qui va nous permettre de comprendre l'espace des formes modulaires :

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24}, \tag{1.20}$$

où $q = \exp(2\imath\pi\tau)$. C'est une forme parabolique de poids 12 pour Γ_1. C'est d'ailleurs le plus petit poids pour lequel il existe une forme parabolique (voir la proposition 1.4.6).

Soit f une fonction méromorphe sur $\mathcal{H}_1$ et soit $z_0 \in \mathcal{H}_1$. On note $\mathrm{ord}_{z_0}(f)$ l'ordre de f au point z_0 : c'est le plus grand entier n tel que $f(z)/(z-z_0)^n$ est holomorphe. Remarquons que si f vérifie la condition de modularité pour le poids k sur Γ_1, [75, Proposition 2.5.2] dit que cet ordre ne dépend que de la classe de $z_0 \bmod \Gamma_1$. Cette proposition dit aussi que pour les pointes, il suffit de regarder ce qu'il se passe au point ∞. On note $\mathrm{ord}_\infty(f)$ l'indice du premier coefficient non nul de la série de Fourier de f.

Théorème 1.4.4. *Soit $k \geq 2$ un entier et f une fonction méromorphe distincte de la fonction nulle vérifiant la condition de modularité de poids k sur Γ_1. On a :*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_\imath(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{\tau\in\mathcal{F}_1\setminus\{\imath,\rho,-\overline{\rho}\}} \mathrm{ord}_\tau(f) = \frac{k}{12},$$

où $\rho = \exp(2\imath\pi/3)$.

Démonstration. Voir [75, Théorème 2.5.3] ou [61, Lemme 22]. □

Exemple 1.4.5. *La fonction G_4 n'a qu'un seul zéro : il est au point ρ et est simple. De même, G_6 n'a qu'un seul zéro qui est au point $\imath$ et qui est simple.*

Ce théorème a de nombreuses conséquences importantes. Il permet de montrer que la seule forme modulaire de poids négatif sur Γ_1 est la fonction constante nulle. Ensuite, la seule forme parabolique de poids 0 est 0 car une telle fonction vérifie $\mathrm{ord}_\infty > 0$. Enfin, si f est une forme modulaire de poids 0, on peut construire une forme parabolique de poids 0 en retranchant à f sa limite à l'infini : ainsi, il n'y a pas de forme modulaire non constante de poids 0.

Proposition 1.4.6. *1. Si $k = 2$, alors $M_2 = S_2 = \{0\}$;*

2. Si $k \geq 4$, alors $M_k = S_k + \mathbb{C}G_k$;

3. Si $k \in \{4, 6, 8, 10, 14\}$, alors $S_k = \{0\}$ et $M_k = \mathbb{C}G_k$;

4. L'espace S_{12} est engendré par Δ ;

5. Si $k \geq 16$, alors $S_k = \Delta M_{k-12}$.

Démonstration. Voir [61, Proposition 25]. □

Il s'ensuit que M_k est de dimension finie donnée par :

k	< 0	0	2	4	6	8	10	12	14	16	18	...	k	...	$k+12$	...
$\dim M_k$	0	1	0	1	1	1	1	2	1	2	2	...	d	...	$d+1$	...

Exemple 1.4.7. *Les formes $120G_4^2$ et G_8 sont de poids 8. Or l'espace des formes modulaires de poids 8 est de dimension 1. Étant donné que ces formes ont le même terme constant, elles sont égales. On peut en déduire l'égalité suivante :*

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Exemple 1.4.8. *Les espaces M_{10} et M_{14} sont de dimension 1, ce qui implique que G_4G_6 et G_{10} sont proportionnels et que G_4G_{10}, G_6G_8 et G_{14} le sont aussi. On peut en déduire des formules arithmétiques reliant les différentes fonctions σ_i.*

Exemple 1.4.9. *En utilisant le fait que $\dim(S_{12}) = 1$, on peut montrer l'égalité $\Delta = (2\pi)^{12} \frac{(240G_4)^3 - (504G_6)^2}{1728}$ (voir [61, Équation (18)]).*

Ces exemples illustrent également le fait que l'anneau gradué des formes modulaires sur $\mathrm{SL}_2(\mathbb{Z})$ est engendré par G_4 et G_6 ([61, Corollaire 28]).

D'autre part, on peut montrer que pour tout $f \in M_k$, la fonction $f'(\tau) + 4\imath\pi k G_2(\tau) f(\tau)$ appartient à M_{k+2}. Ceci se montre facilement à partir de (1.19) et de l'égalité :

$$f'(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^{k+2} f'(\tau) + kc(c\tau + d)^{k+1} f(\tau)$$

pour une forme modulaire de poids k sur Γ_1. On trouve alors pour les formes G_4 et G_6 (voir [89, Page 15])

$$\frac{1}{2\imath\pi} G_4'(\tau) = \frac{7}{10} G_6(\tau) - 8G_2(\tau)G_4(\tau)$$

et

$$\frac{1}{2\imath\pi}G_6'(\tau) = \frac{10}{21}G_8(\tau) - 12G_2(\tau)G_6(\tau).$$

On peut également montrer que $G_2'(\tau) + 4\imath\pi G_2(\tau)^2$ est dans M_4 et déduire l'égalité suivante, que nous réutiliserons pour montrer un résultat sur le degré de certaines composantes de Humbert (corollaire 4.4.4) :

$$\frac{1}{2\imath\pi}G_2'(\tau) = \frac{5}{6}G_4(\tau) - 2G_2(\tau)^2. \tag{1.21}$$

Ces trois dernières égalités impliquent que l'extension $\mathbb{C}[G_2, G_4, G_6]$ de l'anneau gradué $\mathbb{C}[G_4, G_6]$ des formes modulaires est fermé par différentiation. Une conséquence est que si f appartient à cet anneau, alors c'est aussi le cas de f', f'' et f''' et puisque cet anneau n'a que trois générateurs, ces quatres fonctions sont reliées algébriquement. Par exemple, on a que $\frac{\imath}{\pi}G_2''' - 48G_2G_2'' + 72G_2'^2 = 0$ (voir [89]).

Des résultats plus généraux sur les dimensions des espaces de formes modulaires pour des sous-groupes du groupe modulaire existent. Nous ne les énoncerons pas ici mais renvoyons le lecteur à [61]. Il existe également des généralisations de la notion de forme modulaire pour inclure des poids rationnels, par exemple.

Citons tout de même un exemple de forme modulaire de poids 1. La *fonction η de Dedekind* est la fonction :

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n). \tag{1.22}$$

On a la relation $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ ([75, Théorème 1.9.2]) et on dispose d'une formule de transformation de la fonction η de Dedekind (voir [75, Théorème 1.10.1] :

$$\eta(\gamma\cdot\tau) = \epsilon(\gamma)\sqrt{(c\tau+d)}\eta(\tau)$$

où $\Re(\sqrt{c\tau+d}) > 0$ et $\epsilon(\gamma)$ est une racine 24-ième de l'unité. On peut être plus précis. Soit une matrice $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ dans Γ_1 avec $c \geq 0$ et $d > 0$ si $c = 0$. Une telle matrice est dite normalisé. Soient aussi c_1 et $\lambda \in \mathbb{Z}$ vérifiant $c = c_1 2^\lambda$ avec $c_1 \equiv 1 \bmod 2$ si $c \neq 0$ et $c_1 = \lambda = 1$ si $c = 0$. On a alors :

$$\epsilon(\gamma) = \left(\frac{a}{c_1}\right)\zeta_{24}^{ab+c(d(1-a^2)-a)+3(a-1)c_1+\frac{3}{2}\lambda(a^2-1)}$$

où $(\frac{a}{c_1})$ désigne le symbole de Legendre.

Ainsi, on vérifie facilement que la forme $\sqrt[12]{\Delta(\tau)} := 2\pi\eta(\tau)^2$ est de poids 1 pour le groupe $\Gamma_1(12)$. Remarquons que si $\gamma \in \Gamma_1(12)$ n'est pas normalisée, alors $\gamma\cdot\tau = (-\gamma)\cdot\tau$ et on regarde alors comment se transforme $\eta((-\gamma)\cdot\tau)$. Il est important de noter ici que si $\gamma \in \Gamma_1(12)$, alors $-\gamma \notin \Gamma_1(12)$ car $-I_2 \notin \Gamma_1(12)$ ce qui rend possible l'existence de formes modulaires de poids impair pour ce groupe.

1.4.2 Fonctions modulaires

On veut maintenant des fonctions (non constantes) qui soient en quelque sorte des formes modulaires de poids 0. Pour cela, on considère des quotients de formes modulaires de même poids pour un même groupe.

Définition 1.4.10 (Fonction modulaire)**.** *Une* fonction modulaire *pour un sous-groupe Γ de Γ_1 d'indice fini est une fonction $f : \mathcal{H}_1 \to \mathbb{C}$ qui est :*

1. *Méromorphe ;*
2. *Méromorphe aux pointes ;*
3. *Invariante sous l'action de* Γ *:* $\forall \gamma \in \Gamma$ *et* $\forall \tau \in \mathcal{H}_1$, $f(\gamma \cdot \tau) = f(\tau)$.

La notion de méromorphie aux pointes et similaire à celle d'holomorphie aux pointes. Soit f une fonction méromorphe et invariante par Γ et soit $r > 0$ tel que $T^r \in \Gamma$. La fonction est périodique de période r et admet donc un développement en série de Fourier de la forme :

$$f(\tau) = \sum_{n \in \mathbb{Z}} f_n q^{\frac{n}{r}}.$$

On dit que la fonction est *méromorphe à l'infini* s'il existe $n_0 \in \mathbb{Z}$ tel que $f_n = 0$ pour tout $n < n_0$. On définit pour $\gamma \in \Gamma_1$ la fonction $f_\gamma : \tau \in \mathcal{H}_1 \mapsto f(\gamma \cdot \tau) \in \mathbb{C}$. Elle est méromorphe et invariante sous l'action du groupe $\gamma^{-1}\Gamma\gamma$. Si la fonction f_γ est méromorphe à l'infini, on dira que f est *méromorphe en* $\frac{a}{c}$.

La fonction modulaire la plus importante est le j-invariant

$$j(\tau) = 1728 \frac{(60E_4(\tau))^3}{\Delta(\tau)}$$

qui est d'ailleurs appelé *l'invariant modulaire*. Cette fonction est holomorphe sur $\mathcal{H}_1$, a un pôle au point ∞ et est invariante pour tout Γ_1. À partir des équations (1.17) et (1.20), on peut voir que j a un développement de Fourier à coefficients entiers. Les premiers termes sont :

$$\begin{aligned} j(\tau) = \quad & q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \\ & 20245856256q^4 + 333202640600q^5 + 4252023300096q^6 + \ldots \end{aligned} \tag{1.23}$$

Appelons $\mathbb{C}_{\Gamma_1}$ le corps des fonctions modulaires pour Γ_1. C'est une extension de $\mathbb{C}$. Le résultat principal est le suivant.

Théorème 1.4.11. *Une fonction modulaire sur* Γ_1 *peut s'exprimer comme une fraction rationnelle sur* $\mathbb{C}$ *de la fonction* j *:* $\mathbb{C}_{\Gamma_1} = \mathbb{C}(j)$.

Démonstration. Voir [75, Théorème 2.5.1]. □

Corollaire 1.4.12. *L'anneau des fonctions modulaires sur* Γ_1 *qui sont holomorphes sur* $\mathcal{H}_1$ *est donné par* $\mathbb{C}[j]$.

Démonstration. Voir [75, Théorème 2.5.8]. □

Théorème 1.4.13. *On a* $j(\mathcal{H}_1) = \mathbb{C}$ *et* $j(\tau) = j(\tau') \Leftrightarrow \tau \sim \tau' \bmod \Gamma_1$ *pour tout* $\tau, \tau' \in \mathcal{H}_1$. *En particulier, pour tout* $z \in \mathbb{C}$ *il existe un* $\tau \in \mathcal{F}_1$ *tel que* $j(\tau) = z$.

Démonstration. Voir [75, Théorème 2.5.5]. □

Regardons maintenant ce qu'il se passe pour des sous-groupes de Γ_1. On note par $\mathbb{C}_\Gamma$ le corps des fonctions modulaires sur Γ pour un sous-groupe Γ de Γ_1. C'est une extension du corps $\mathbb{C}_{\Gamma_1}$.

Théorème 1.4.14. *Soit* Γ *un sous-groupe d'indice fini de* Γ_1 *avec* $-I_2 \in \Gamma$. *Alors :*

— *L'extension* $\mathbb{C}_\Gamma / \mathbb{C}_{\Gamma_1}$ *est algébrique et de degré* $[\mathbb{C}_\Gamma : \mathbb{C}_{\Gamma_1}] = [\Gamma_1 : \Gamma]$ *;*

— *Tout* $\gamma \in \Gamma_1$ *définit un isomorphisme* $\lambda_\gamma : f \in \mathbb{C}_\Gamma \mapsto f^{\lambda_\gamma}(\tau) = f(\gamma \cdot \tau) \in \mathbb{C}_{\gamma^{-1}\Gamma\gamma}$ *avec* $\lambda_\gamma|\mathbb{C}_{\Gamma_1} = \mathrm{id}_{\mathbb{C}_{\Gamma_1}}$ *qui ne dépend que des classes* $\Gamma\gamma$ *;*
— *Pour une décomposition* $\Gamma_1 = \bigsqcup_{k=1}^{n} \Gamma\gamma_k$ *en classes à droite de* Γ_1 *modulo* Γ*, on obtient par* λ_{γ_k}*,* $k = 1, \ldots, n$*, tous les différents plongements de* $\mathbb{C}_\Gamma/\mathbb{C}_{\Gamma_1}$ *vers la clôture algébrique de* $\mathbb{C}_{\Gamma_1}$ *;*
— *Soit* $f \in \mathbb{C}_\Gamma$*, le polynôme*

$$P_f(X, j) := \prod_{k=1}^{n} (X - f^{\lambda_{\gamma_k}})$$

a ses coefficients dans $\mathbb{C}_{\Gamma_1}$*. Si, de plus,* f *est holomorphe sur* $\mathcal{H}_1$*, alors* $P_f(X, j) \in \mathbb{C}[X, j]$*.*

Démonstration. Voir [75, Théorème 2.6.1]. La plus grosse difficulté dans la démonstration est de montrer que les λ_{γ_k} sont tous différents, c'est-à-dire démontrer l'existence d'une fonction dans $\mathbb{C}_\Gamma$ telle que tous les conjugués $f^{\lambda_{\gamma_k}}$ sont différents. Pour un sous-groupe donné, on peut essayer de construire une telle fonction explicitement. En général, on peut utiliser le théorème de Riemann-Roch sur la surface de Riemann compacte associée à $\mathcal{H}_1^*/\Gamma$.

Nous donnons ici une autre preuve du dernier point qui nous semble instructive. Soient $n = [\Gamma_1 : \Gamma]$, $\{\gamma_k\}_{k\in[1,n]}$ un ensemble de représentants des classes de Γ_1/Γ et f une fonction modulaire sur Γ. On peut écrire :

$$P_f(X, j) = \prod_{k=1}^{n} (X - f^{\lambda_{\gamma_k}}) = X^n + \sum_{k=0}^{n-1} c_k(\tau) X^k$$

où les c_k sont des fonctions de $\mathcal{H}_1$ vers $\mathbb{C}$ symétriques en les $\tau \mapsto f(\gamma_k \cdot \tau)$. Comme f est modulaire pour Γ et que les γ_k forment un ensemble de représentants des classes de Γ_1/Γ, les c_k sont invariantes sous l'action de Γ_1, sont méromorphes sur $\mathcal{H}_1$ et au point ∞, donc ce sont des fonctions modulaires sur Γ_1. Ainsi, par le théorème 1.4.11, ce sont des fractions rationnelles en j, ou, en d'autres termes, les c_k sont dans $\mathbb{C}_{\Gamma_1}$. Si de plus f est holomorphe sur $\mathcal{H}_1$, alors le corollaire 1.4.12 nous dit que $P_f(X, j) \in \mathbb{C}[X, j]$. □

Une conséquence du dernier point est que pour tout sous-groupe d'indice fini Γ contenant $-I_2$ de Γ_1 et pour toute fonction modulaire f de Γ, il existe un polynôme $\Phi_f(X, Y) \in \mathbb{C}[X, Y]$ de degré $[\Gamma_1 : \Gamma]$ en X tel que pour tout $\tau \in \mathcal{H}_1$ on ait $\Phi_f(f(\tau), j(\tau)) = 0$. Précisons que ce polynôme n'est pas forcément le polynôme P du théorème car on le veut dans $\mathbb{C}[X, Y]$ et non pas dans $\mathbb{C}(Y)[X]$. Pour passer de P_f à Φ_f, il suffit de multiplier le premier par le *ppcm* de tous les dénominateurs de ses coefficients en X. Ainsi, on ne demande pas au polynôme Φ_f d'être unitaire.

Définition 1.4.15 (Polynôme modulaire)**.** *Soient* Γ' *et* Γ'' *deux sous-groupes d'indices finis de* Γ_1 *contenant* $-I_2$ *et soient* f_1 *et* f_2 *deux fonctions modulaires pour respectivement* Γ' *et* Γ''*. Alors il existe un polynôme non nul* $\Phi_{f_1,f_2}(X, Y) \in \mathbb{C}[X, Y]$ *appelé* polynôme modulaire *tel que pour tout* $\tau \in \mathcal{H}_1$ *on ait*

$$\Phi_{f_1,f_2}(f_1(\tau), f_2(\tau)) = 0.$$

L'existence de ce polynôme est claire d'après ce qui précède car il suffit de considérer le résultant des deux polynômes Φ_{f_1} et Φ_{f_2} pour éliminer j.

On peut construire des fonctions modulaires pour le groupe Γ_R, où R est une matrice primitive de déterminant $r > 0$, en prenant

$$j_R(\tau) := j(R \cdot \tau) \qquad \text{ou} \qquad \phi_R(\tau) := r^{12} \frac{\Delta(R \cdot \tau)}{\Delta(\tau)},$$

où on a bien que $R \cdot \tau$ est dans $\mathcal{H}_1$ par l'équation (1.11). Pour une matrice $\gamma \in \Gamma_1$, on a $j_R(\gamma \cdot \tau) = j_{R\gamma}(\tau)$ et $\phi_R(\gamma \cdot \tau) = \phi_{R\gamma}(\tau)$ et, évidemment, ces deux fonctions ne dépendent que de la classe à droite $\Gamma_1 R$ de R, donc d'après le Théorème 1.3.11, on a $j_R = j_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)}$ et $\phi_R = \phi_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)}$ pour une certaine matrice $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ équivalente à R.

Théorème 1.4.16. *Soit g_R une des fonctions j_R et ϕ_R. Alors :*

1. $\mathbb{C}_{\Gamma_R} = \mathbb{C}(j, g_R)$;
2. *Pour un système complet de matrices non équivalentes R_i de déterminant r, les fonctions g_{R_i}, $i = 1, \ldots, \psi(r)$ sont toutes différentes et constituent un système complet de conjugués de g_R sur $\mathbb{C}_\Gamma$.*

Démonstration. Voir [75, Théorème 2.7.1]. □

Considérons les corps $\mathbb{Q}_{\Gamma_1} = \mathbb{Q}(j)$ et $\mathbb{Q}_{\Gamma_R} = \mathbb{Q}(j, j_R)$. Le polynôme minimal de j_R sur $\mathbb{C}_{\Gamma_1}$ a ses coefficients dans $\mathbb{Q}_{\Gamma_1}$.

Théorème 1.4.17. *On a $[\mathbb{Q}_{\Gamma_R} : \mathbb{Q}_{\Gamma_1}] = \psi(r)$ et les différents isomorphismes de $\mathbb{Q}_{\Gamma_R}/\mathbb{Q}_{\Gamma_1}$ sont donnés par les λ_{γ_i}, $i = 1, \ldots, \psi(r)$ si $R\gamma_i$, $\gamma_i \in \Gamma_1$, est un système de représentants des matrices primitives de déterminant r.*

Démonstration. Voir [75, Théorème 2.7.2]. □

On appelle *polynôme modulaire d'ordre r* le polynôme :

$$\Phi_r(X, j) := \prod_{i=1}^{\psi(r)} (X - j_{R_i}). \tag{1.24}$$

C'est aussi le polynôme minimal de j_R sur $\mathbb{Q}_{\Gamma_1}$. Ici, R_i est un ensemble de représentants des classes des matrices primitives de déterminant r.

Théorème 1.4.18. *On a :*

1. $\Phi_r(X, j) \in \mathbb{Z}[X, j]$;
2. $\Phi_r(X, X) \neq 0$;
3. *Le coefficient dominant de $\Phi_r(X, X)$ est ± 1 pour $r \in \mathbb{N} \backslash \mathbb{N}^2$.*

Démonstration. Voir [75, Théorème 2.7.4]. Le fait que ces polynômes soient dans $\mathbb{Z}[X, j]$ provient d'une part du corollaire 1.4.12 et d'autre part du fait que le développement de Fourier de j (voir équation (1.23)) est à coefficients entiers. □

Un des cas qui nous intéresse le plus est lorsque l'on prend $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, pour p premier. Dans ce cas là, on parle de *polynôme modulaire classique*. Nous définirons plus tard d'autres polynômes modulaires.

1.5 Fonction thêta

1.5.1 Fonction thêta et groupe de Heisenberg

On s'intéresse aux fonctions entières (définies et holomorphes sur tout $\mathbb{C}$) qui ont un comportement le plus périodique possible par rapport à un réseau $\Lambda = [1, \tau]$. Le théorème de Liouville dit qu'une fonction entière et bornée est constante et ainsi, une fonction entière ne peut être périodique de période 1 et τ à moins d'être constante.

Définition 1.5.1. *La* fonction thêta *est la fonction analytique bivariée suivante :*

$$\vartheta(z, \tau) = \sum_{n \in \mathbb{Z}} \exp(\imath\pi n^2 \tau + 2\imath\pi n z),$$

où $z \in \mathbb{C}$ *et* $\tau \in \mathcal{H}_1$.

Cette série converge absolument et uniformément sur un compact (voir [68]). Cette fonction vérifie $\vartheta(z+1, \tau) = \vartheta(z, \tau)$ et $\vartheta(z+\tau, \tau) = \exp(-\imath\pi\tau - 2\imath\pi z)\vartheta(z, \tau)$ et c'est la fonction la plus générale parmi celles qui ont deux "quasi-périodes". Nous allons introduire le groupe de Heisenberg pour rendre rigoureux ce que nous entendons par là.

Soit f une fonction holomorphe et soient $a, b \in \mathbb{R}$. On considère les transformations suivantes :

$$(S_b(f))(z) = f(z + b) \quad \text{et} \quad (T_a(f))(z) = \exp(\imath\pi a^2 \tau + 2\imath\pi a z) f(z + a\tau).$$

Un simple calcul permet de vérifier les égalités :

$$S_{b_1}(S_{b_2}(f)) = S_{b_1+b_2}(f), \quad T_{a_1}(T_{a_2}(f)) = T_{a_1+a_2}(f)$$

$$\text{et} \quad S_b \circ T_a = \exp(2\imath\pi ab) T_a \circ S_b.$$

Le *groupe de Heisenberg* $\mathscr{G}$ est le groupe engendré par ces transformations :

$$\mathscr{G} = \mathbb{C}_1^* \times \mathbb{R} \times \mathbb{R}, \quad \text{où} \quad \mathbb{C}_1^* = \{z \in \mathbb{C} : |z| = 1\}.$$

Le triplet $(\lambda, a, b) \in \mathscr{G}$ représente alors la transformation :

$$(\lambda, a, b)(f)(z) = \lambda(T_a \circ S_b)(f)(z) = \lambda \exp(\imath\pi a^2 \tau + 2\imath\pi a z) f(z + a\tau + b)$$

et la loi de groupe de $\mathscr{G}$ est donnée par

$$(\lambda, a, b)(\lambda', a', b') = (\lambda\lambda' \exp(2\imath\pi ba'), a + a', b + b').$$

Le sous-ensemble $\mathcal{G} = \{(1, a, b) \in \mathscr{G} : a, b \in \mathbb{Z}\}$ est un sous-groupe de $\mathscr{G}$. On vérifie aisément que l'on a :

$$\vartheta(z + a\tau + b, \tau) = \exp(-\imath\pi a^2 \tau - 2\imath\pi a z)\vartheta(z, \tau) \tag{1.25}$$

et donc la fonction thêta est invariante par $\mathcal{G}$. En fait, on peut même montrer que c'est l'unique fonction, à un scalaire près, invariante par $\mathcal{G}$.

Soit ℓ un entier positif. On pose $\ell\mathcal{G} = \{(1, \ell a, \ell b)\} \subseteq \mathcal{G}$ et $V_\ell = \{\text{fonctions entières invariantes sous } \ell\mathcal{G}\}$. C'est un espace vectoriel sur $\mathbb{C}$ de dimension ℓ^2

([68, Lemme 3.1]). La base standard de V_ℓ est donnée par les fonctions thêta de caractéristiques $a, b \in \frac{1}{\ell}\mathbb{Z}$:

$$\vartheta_{a,b}(z,\tau) = S_b T_a(\vartheta) = \exp(\imath\pi a^2\tau + 2\imath\pi a(z+b))\vartheta(z+a\tau+b,\tau). \tag{1.26}$$

Considérons maintenant $\ell \geq 2$, $E_\tau = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ et (a_i, b_i) un ensemble de représentants des classes de $((\frac{1}{\ell}\mathbb{Z})/\mathbb{Z})^2$. On note $\vartheta_i = \vartheta_{a_i,b_i}$ pour $0 \leq i \leq \ell^2 - 1$. L'application suivante est bien définie et est holomorphe :

$$\begin{array}{rccl} \phi_\ell : & E_\tau & \longrightarrow & \mathbb{P}^{\ell^2-1}(\mathbb{C}) \\ & z & \longmapsto & (\vartheta_0(\ell z,\tau), \ldots, \vartheta_{\ell^2-1}(\ell z,\tau)). \end{array} \tag{1.27}$$

C'est aussi un plongement et donc $\phi_\ell(E_\tau)$ est une sous-variété algébrique.

Lemme 1.5.2. *Tout $f \in V_\ell$, $f \neq 0$, a exactement ℓ^2 zéros comptés avec multiplicité dans un domaine fondamental de $\mathbb{C}/(\ell(\mathbb{Z}+\tau\mathbb{Z}))$. Les zéros de $\vartheta_{a,b}$ sont les points $(a+p+\frac{1}{2})\tau + (b+q+\frac{1}{2})$, $p, q \in \mathbb{Z}$. En particulier, ϑ_i et ϑ_j n'ont pas de zéros en commun si $i \neq j$.*

Démonstration. Voir [68, Lemme 4.1]. □

Notons $\Gamma_1(1,2)$ le sous-groupe de Γ_1 contenant les matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec ab et cd pairs.

Théorème 1.5.3 (Équation fonctionnelle)**.** *Soit $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(1,2)$. Alors il existe ζ_8 une racine 8-ième de l'unité telle que l'on ait l'équation fonctionnelle suivante :*

$$\vartheta\left(\frac{z}{c\tau+d}, \frac{a\tau+b}{c\tau+d}\right) = \zeta_8\sqrt{c\tau+d}\exp(\imath\pi c z^2/(c\tau+d))\vartheta(z,\tau). \tag{1.28}$$

Quitte à multiplier γ par $-I_2$, on peut supposer $c > 0$ ou alors $c = 0$ et $d > 0$. Ainsi, $\Im(c\tau+d) \geq 0$ et on choisit $\sqrt{c\tau+d}$ dans le premier quadrant ($\Re(...) \geq 0$ et $\Im(...) \geq 0$). De plus, on peut expliciter ζ_8 :

- *Si c est pair alors d est impair et $\zeta_8 = \imath^{\frac{1}{2}(d-1)}(\frac{c}{|d|})$;*
- *Si c est impair alors d est pair et $\zeta_8 = \exp(-\imath\pi c/4)(\frac{d}{c})$.*

Ici, $(\frac{x}{y})$ désigne le symbole de Jacobi avec pour convention $(\frac{0}{1}) = 1$.

Démonstration. Voir [68, Théorème 7.1]. □

1.5.2 Thêta constantes en caractéristique $\frac{1}{2}$

Nous nous plaçons désormais en caractéristique $\frac{1}{2}$ parce que c'est le cas qui nous intéresse le plus pour le calcul des polynômes modulaires. C'est aussi et naturellement la caractéristique la plus simple à étudier et nous allons voir qu'elle est riche en propriétés.

D'après l'équation (1.26), nous avons les quatre fonctions suivantes à considérer :

$$\vartheta_{0,0}(z,\tau) = \vartheta(z,\tau),$$

$$\vartheta_{0,\frac{1}{2}}(z,\tau) = \vartheta(z+\frac{1}{2},\tau),$$

$$\vartheta_{\frac{1}{2},0}(z,\tau) = \exp(\imath\pi\tau/4 + \imath\pi z)\vartheta(z+\frac{\tau}{2},\tau),$$

$$\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau) = \exp(\imath\pi\tau/4 + \imath\pi(z+\frac{1}{2}))\vartheta(z+\frac{\tau}{2}+\frac{1}{2},\tau).$$

Plus précisément, nous allons étudier ces fonctions par rapport à τ en $z=0$. C'est ce qu'on appelle les thêta constantes. Pour plus de simplicité, on notera dans la suite :

$$\vartheta_0(\tau) = \vartheta_{0,0}(0,\tau), \quad \vartheta_1(\tau) = \vartheta_{0,\frac{1}{2}}(0,\tau), \quad \text{et} \quad \vartheta_2(\tau) = \vartheta_{\frac{1}{2},0}(0,\tau).$$

Il est inutile de considérer $\vartheta_3(\tau) = \vartheta_{\frac{1}{2},\frac{1}{2}}(0,\tau)$ car cette fonction est identiquement nulle, d'après le lemme 1.5.2. Ce même lemme montre d'ailleurs que les trois autres thêta constantes (en caractéristique $\frac{1}{2}$) ne sont jamais nulles. La prochaine propriété confirme également ce fait.

Proposition 1.5.4. *Notons $q = \exp(\imath\pi\tau)$. Pour tout $\tau \in \mathcal{H}_1$ tel que $\Im(\tau) \geq \frac{\sqrt{3}}{2}$ (et donc en particulier pour $\tau \in \mathcal{F}_1$), on a pour $j \in \{0,1\}$:*

$$|\vartheta_j(\tau) - 1| \leq 0,141 \qquad \textit{et} \qquad \left|\frac{\vartheta_2(\tau)}{2q^{\frac{1}{4}}} - 1\right| \leq 0,005.$$

Démonstration. Nous reproduisons la preuve de [19, Proposition 2.6]. Soit $\tau \in \mathcal{H}_1$ tel que $\Im(\tau) \geq \frac{\sqrt{3}}{2}$ et soit $i \in \{0,1\}$. Alors,

$$|\theta_i(\tau) - 1| = \left|2\sum_{n\geq 1}(-1)^i q^{n^2}\right| \leq 2\sum_{n\geq 1}|q|^{n^2} \leq 2\sum_{n\geq 1}|q|^n \leq \frac{2|q|}{1-|q|},$$

et comme $|q| \leq \exp(-\pi\frac{\sqrt{3}}{2})$, un calcul numérique montre la propriété souhaitée. Par ailleurs, on a

$$\theta_2(\tau) = 2\sum_{n\geq 0} q^{(n+\frac{1}{2})^2} = 2q^{\frac{1}{4}}\left(1 + \sum_{n\geq 1} q^{n^2+n}\right),$$

donc

$$\left|\frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - 1\right| = \left|\sum_{n\geq 1} q^{n^2+n}\right| \leq \sum_{n\geq 2}|q|^n \leq \frac{|q|^2}{1-|q|},$$

et un calcul numérique montre notre proposition. □

Nous disposons d'une équation fonctionnelle qui ne découle pas directement du théorème 1.5.3 car elle ne se limite pas aux matrices de $\Gamma_1(1,2)$.

Proposition 1.5.5. *Pour tous $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_1$ et $j \in \{0,1,2\}$, il existe une racine quatrième de l'unité ζ_4 telle que pour tout $\tau \in \mathcal{H}_1$,*

$$\vartheta_j^2(\gamma\cdot\tau) = \zeta_4(c\tau+d)\vartheta^2_{\sigma(\gamma,j)}(\tau),$$

où on considère f la fonction qui à 0 associe $(0,0)$, à 1 le couple $(0,1)$, à 2 le couple $(1,0)$ et où on pose $\sigma(\gamma,j) = f^{-1}((x+cd, y+ab)\gamma \bmod 2)$ avec $(x,y) = f(j)$.

Démonstration. Voir [19, Proposition 2.5]. □

Proposition 1.5.6. *Pour tout $\tau \in \mathcal{H}_1$, on a*

$$\begin{array}{rclcrcl} \vartheta_0^2(T\tau) & = & \vartheta_1^2(\tau), & & \vartheta_0^2(S\tau) & = & -\imath\tau\vartheta_0^2(\tau), \\ \vartheta_1^2(T\tau) & = & \vartheta_0^2(\tau), & & \vartheta_1^2(S\tau) & = & -\imath\tau\vartheta_2^2(\tau), \\ \vartheta_2^2(T\tau) & = & \imath\vartheta_2^2(\tau), & & \vartheta_2^2(S\tau) & = & -\imath\tau\vartheta_1^2(\tau). \end{array}$$

Démonstration. Voir [19, Proposition 2.4]. La partie de cette proposition avec S est un corollaire du théorème 1.5.3 et de la proposition précédente car $S \in \Gamma_1(1,2)$, contrairement à T. □

Corollaire 1.5.7. *Les trois fonctions $\vartheta_0^2(\tau)$, $\vartheta_1^2(\tau)$ et $\vartheta_2^2(\tau)$ sont des formes modulaires de poids* 1 *pour le groupe $\Gamma_1(4)$.*

Démonstration. Voir [68, Proposition 9.2]. □

Signalons également cette propriété qui nous sera utile dans la suite.

Proposition 1.5.8. *Pour tout $\tau \in \mathcal{H}_1$,*

$$4\frac{d}{d\tau}\log\frac{\vartheta_2(\tau)}{\vartheta_1(\tau)} = \imath\pi\vartheta_0^4(\tau),\ 4\frac{d}{d\tau}\log\frac{\vartheta_0(\tau)}{\vartheta_1(\tau)} = \imath\pi\vartheta_2^4(\tau),\ 4\frac{d}{d\tau}\log\frac{\vartheta_2(\tau)}{\vartheta_0(\tau)} = \imath\pi\vartheta_1^4(\tau).$$

Démonstration. Voir [88, Page 82]. □

Il s'ensuit du corollaire 1.5.7 que l'application

$$\begin{array}{rccc} \psi_2 : & \mathcal{H}_1/\Gamma_1(4) & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ & \tau & \longmapsto & (\vartheta_0^2(\tau), \vartheta_1^2(\tau), \vartheta_2^2(\tau)) \end{array} \tag{1.29}$$

est holomorphe. On peut alors montrer que l'image est dans la conique $x_0^2 = x_1^2 + x_2^2$ et qu'il manque les six points $(1,0,\pm 1)$, $(1,\pm 1,0)$, et $(0,1,\pm\imath)$ dû au fait que les thêta constantes ne s'annulent pas.

Proposition 1.5.9. *Pour tout $\tau \in \mathcal{H}_1$, $\lim_{n\to\infty}\vartheta_0(2^n\tau) = \lim_{n\to\infty}\vartheta_1(2^n\tau) = 1$ et $\lim_{n\to\infty}\vartheta_2(2^n\tau) = 0$.*

Démonstration. Voir [19, Lemme 2.2]. Soit $\tau \in \mathcal{H}_1$. On a vu dans la preuve de la proposition 1.5.4 que pour $i = 0, 1$, $|\theta_i(2^n\tau) - 1| \leq \frac{2|q_n|}{1-|q_n|}$ pour $q_n = \exp(2^n\imath\pi\tau)$. Or, $\lim_{n\to+\infty}|q_n| = 0$, ce qui montre les deux premières limites. La troisième se déduit de l'égalité de Jacobi (proposition 1.5.10). □

Ainsi, on peut atteindre le point $(1,1,0)$ en prenant en compte la pointe à l'infini. On obtient les autres points manquants en considérant ensuite l'action de Γ_1 sur cette pointe (autrement dit, en considérant les autres pointes). Au final, en étendant l'application ψ_2 sur un compactifié de $\mathcal{H}_1/\Gamma_1(4)$, cette application devient un isomorphisme ([68, Théorème 10.1]). La conique nous fournit l'égalité dite de Jacobi.

Proposition 1.5.10 (Égalité de Jacobi)**.** *Pour tout $\tau \in \mathcal{H}_1$,*

$$\vartheta_0^4(\tau) = \vartheta_1^4(\tau) + \vartheta_2^4(\tau).$$

Cette égalité peut être déduite des formules de duplication.

Proposition 1.5.11 (Formules de duplication)**.** *Pour tout $\tau \in \mathcal{H}_1$, on a :*

$$\begin{array}{rclcrcl} \vartheta_0^2(2\tau) & = & \frac{\vartheta_0^2(\tau)+\vartheta_1^2(\tau)}{2}, & & \vartheta_0^2(\frac{\tau}{2}) & = & \vartheta_0^2(\tau)+\vartheta_2^2(\tau), \\ \vartheta_1^2(2\tau) & = & \vartheta_0(\tau)\vartheta_1(\tau), & & \vartheta_1^2(\frac{\tau}{2}) & = & \vartheta_0^2(\tau)-\vartheta_2^2(\tau), \\ \vartheta_2^2(2\tau) & = & \frac{\vartheta_0^2(\tau)-\vartheta_1^2(\tau)}{2}, & & \vartheta_2^2(\frac{\tau}{2}) & = & 2\vartheta_0(\tau)\vartheta_2(\tau). \end{array}$$

Démonstration. C'est un cas particulier de la proposition 2.6.12. □

Revenons à l'isomorphisme précédent. Une conséquence est :

Corollaire 1.5.12. *L'anneau des formes modulaires pour le groupe $\Gamma_1(4)$ est isomorphe à $\mathbb{C}[\vartheta_0^2, \vartheta_1^2, \vartheta_2^2]/(\vartheta_0^4 - \vartheta_1^4 - \vartheta_2^4)$.*

Démonstration. Voir [68, Corollaire 10.2]. □

Revenons à la fonction ϕ_2 définie dans l'équation (1.27). Pour tout $\tau \in \mathcal{H}_1$, $\phi_2(E_\tau)$ est une courbe C_τ de $\mathbb{P}^3(\mathbb{C})$ définie par les équations (voir [68, Pages 23 et 57]) :

$$\vartheta_0(0,\tau)^2 x_0^2 = \vartheta_1(0,\tau)^2 x_1^2 + \vartheta_2(0,\tau)^2 x_2^2,$$

$$\vartheta_0(0,\tau)^2 x_3^2 = \vartheta_2(0,\tau)^2 x_1^2 - \vartheta_1(0,\tau)^2 x_2^2.$$

On a d'ailleurs que, pour tous $\tau, \tau' \in \mathcal{H}_1$, les courbes C_τ et $C_{\tau'}$ sont soit égales, soit disjointes. En particulier, $C_\tau \cap C_{\tau'} \neq \emptyset \Leftrightarrow \psi_2(\tau) = \psi_2(\tau')$ dans $\mathbb{P}^2(\mathbb{C}) \Leftrightarrow \tau' = \gamma \cdot \tau$ pour $\gamma \in \Gamma_1(4)$ ([68, Lemme 11.3]).

Proposition 1.5.13. *Soient $\tau, \tau' \in \mathcal{H}_1$. Alors $\tau = \gamma \cdot \tau'$ pour un certain $\gamma \in \Gamma_1$ si et seulement s'il existe une application biholomorphe $f : E_\tau \to E_{\tau'}$. D'autre part, pour $n \in \mathbb{N}$, $\mathcal{H}_1/\Gamma_1(n)$ est équivalent à l'ensemble des tores complexes E_τ, modulo isomorphismes, qui préservent les automorphismes $z \mapsto z + \frac{1}{n}$ et $z \mapsto z + \frac{\tau}{n}$.*

Démonstration. Voir [68, Propositions 12.1 et 12.2]. □

Concluons cette partie avec quelques résultats dont nous n'aurons pas besoin dans la suite. On peut retrouver la fonction $\wp$ de Weierstrass à partir d'une fonction thêta :

$$\wp_{[1,\tau]}(z) = -\frac{d^2}{dz^2} \log\left(\vartheta_3(z,\tau)\right) + (\textit{constante})$$

où la constante est de telle sorte que la série de Laurent de $\wp_{[1,\tau]}(z)$ au point $z = 0$ n'a pas de terme constant ([68, Page 25]). De plus, les thêta constantes s'expriment en fonction de la fonction η de Dedekind. En effet, pour tout $\tau \in \mathcal{H}_1$, on a

$$\vartheta_0(\tau) = \exp\left(-\frac{\imath\pi\tau}{12}\right)\frac{\eta^2((\tau+1)/2)}{\eta(\tau)}, \quad \vartheta_1(\tau) = \frac{\eta^2(\tau/2)}{\eta(\tau)}, \quad \vartheta_2(\tau) = 2\frac{\eta^2(2\tau)}{\eta(\tau)}$$

$$\text{et} \quad \eta^3(\tau) = \frac{\vartheta_0(\tau)\vartheta_1(\tau)\vartheta_2(\tau)}{2},$$

d'après [88, Pages 112-116]. D'autre part, les fonctions thêta ont de nombreuses applications. Celle qui est sûrement la plus connue est la suivante ([68, Page 74] et [89, Chapitre 0]). On appelle *fonction thêta de Jacobi* la fonction $\theta(\tau) = \sum_{m\in\mathbb{Z}} q^{m^2} = 1 + 2q + 2q^4 + 2q^9 + \ldots$ pour $q = \exp(2\imath\pi\tau)$. C'est en fait $\vartheta_0(2\tau)$.

Les puissances de cette fonction thêta nous informent sur le nombre de façons de représenter un entier comme somme d'un nombre donné de carrés. Par exemple :

$$\theta(\tau)^4 = \sum_{m_1,m_2,m_3,m_4\in\mathbb{Z}} q^{m_1^2+m_2^2+m_3^2+m_4^2} = 1 + \sum_{n=1}^{\infty} r_4(n)q^n$$

où $r_4(1) = 8, r_4(2) = 24, r_4(3) = 24, \ldots$ désigne le nombre de façons de représenter 1, 2, 3, ... comme une somme de la forme $m_1^2+m_2^2+m_3^2+m_4^2$ avec $m_i \in \mathbb{Z}$. On peut montrer que $\theta(\tau)^4$ est une forme modulaire sur $\Gamma_0(4)$ de poids 2 et que l'espace vectoriel $M_2(\Gamma_0(4))$ des formes modulaires de poids 2 pour le groupe $\Gamma_0(4)$ est de dimension deux, engendré par $G_2(\tau)-2G_2(2\tau)$ et $G_2(\tau)-4G_2(4\tau)$. Donc $\theta(\tau)^4$ est une combinaison linéaire de ces deux vecteurs. En comparant les deux premiers coefficients, on trouve $\theta(\tau)^4 = 8(G_2(\tau) - 4G_2(4\tau))$ et par suite on en déduit que $r_4(n) = 8\sum_{\substack{d|n \\ d\not\equiv 0 \bmod 4}} d$ (pour $n > 0$). En particulier, $r_4(n) \geq 8$ pour tout n, donc chaque entier positif peut être écrit comme somme de quatre carrés.

1.6 Calcul des polynômes modulaires

1.6.1 Évaluation rapide des thêta constantes

Nous reprenons le contenu de [19, Chapitres 3 et 4] et y renvoyons le lecteur intéressé à avoir plus de détails. Soient les fonctions de $\mathcal{H}_1$ dans $\mathbb{C}$ suivantes :

$$k(\tau) = \frac{\vartheta_2^2(\tau)}{\vartheta_0^2(\tau)} \qquad \text{et} \qquad k'(\tau) = \frac{\vartheta_1^2(\tau)}{\vartheta_0^2(\tau)}. \tag{1.30}$$

Elles sont bien définies sur $\mathcal{H}_1$ car les trois premières thêta constantes ne s'annulent pas sur $\mathcal{H}_1$. L'égalité de Jacobi (proposition 1.5.10) nous dit que $k^2 + k'^2 = 1$. On en déduit aussi que ces deux fonctions k et k' ne s'annulent pas sur $\mathcal{H}_1$ et ne prennent pas les valeurs -1 et 1. La fonction k' est modulaire pour le groupe

$$\Gamma_{k'} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : b \equiv 0 \bmod 2 \text{ et } c \equiv 0 \bmod 4 \right\}$$

qui est engendré par les matrices T^2, ST^4S et TST^4ST. On connaît explicitement un ensemble de représentants des classes de $\Gamma_1/\Gamma_{k'}$ (voir [19, Lemme 2.4]) et un domaine fondamental

$$\begin{aligned} \mathcal{F}_{k'} = \ & \Big\{ \tau \in \mathcal{H}_1 : \ -1 \leq \Re(\tau) < 1, \ \left|\tau + \tfrac{3}{4}\right| \geq \tfrac{1}{4}, \ \left|\tau + \tfrac{1}{4}\right| > \tfrac{1}{4}, \\ & \left|\tau - \tfrac{1}{4}\right| \geq \tfrac{1}{4}, \ \left|\tau - \tfrac{3}{4}\right| > \tfrac{1}{4} \Big\} \end{aligned}$$

pour l'action de $\Gamma_{k'}/\langle \pm I_2 \rangle$ sur $\mathcal{H}_1$. Remarquons que $\mathcal{F}_1 \subseteq \mathcal{F}_{k'}$. Pour tout $x \in \mathbb{C}\backslash\{-1, 0, 1\}$, il existe un unique $\tau \in \mathcal{F}_{k'}$ tel que $k'(\tau) = x$.

Il existe une équation définissant le j-invariant en fonction de k' :

$$j(\tau) = 256\frac{(1 - k'^2(\tau) + k'^4(\tau))^3}{k'^4(\tau)(1 - k'^2(\tau))^2}. \tag{1.31}$$

On pourrait réécrire cette égalité pour exprimer j en fonction de k seulement, en utilisant l'égalité de Jacobi.

Soient a et b deux nombres réels positifs. On considère la suite $(a_n, b_n)_{n\in\mathbb{N}}$ définie par $a_0 = a$, $b_0 = b$ et pour tout $n \geq 0$:

$$a_{n+1} = \frac{a_n + b_n}{2} \qquad \text{et} \qquad b_{n+1} = \sqrt{a_n b_n}.$$

L'élément a_{n+1} est la moyenne arithmétique de a_n et b_n tandis que b_{n+1} est leur moyenne géométrique, c'est pourquoi cette suite est appelée *moyenne arithmético-géométrique* (AGM).

Supposons que $a_0 \geq b_0$. On montre facilement que $a_n \geq b_n$ pour tout n et qu'alors d'une part $a_{n+1} - a_n = \frac{b_n - a_n}{2} \leq 0$, ce qui signifie que la suite (a_n) est décroissante, et d'autre part que $b_{n+1}/b_n = \sqrt{\frac{a_n}{b_n}} \geq 1$ et donc que la suite (b_n) est croissante. On a alors pour tout n que $b_0 \leq b_n \leq a_n \leq a_0$, ce qui implique que les deux suites sont bornées et monotones, donc convergent. En considérant la suite $c_n = a_n - b_n$, on peut montrer que les suites (a_n) et (b_n) sont en réalité adjacentes. En effet,

$$c_{n+1}/c_n = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2(a_n - b_n)} = \frac{\sqrt{a_n} - \sqrt{b_n}}{2(\sqrt{a_n} + \sqrt{b_n})} \leq \frac{1}{2};$$

d'où $0 \leq c_{n+1} \leq \frac{1}{2} c_n \leq \frac{1}{2^{n+1}} c_0$ et la suite c_n tend vers 0.

Notons $\mathrm{AGM}(a, b)$ la limite commune des deux suites (a_n) et (b_n). Remarquons que $\mathrm{AGM}(a, b) = \mathrm{AGM}(b, a)$ ce qui fait qu'on n'a rien perdu à supposer $a_0 \geq b_0$.

Une autre propriété basique est que $\mathrm{AGM}(a, b) = a\,\mathrm{AGM}(1, \frac{b}{a})$ si $a \neq 0$. On peut donc se restreindre à l'étude de la fonction $M : \mathbb{R}^+ \to \mathbb{R}^+$, $M(x) = \mathrm{AGM}(1, x)$. Cette fonction est croissante et pour tout $x \in \mathbb{R}^+, M(x) \in [1, x]$. Les suites a_n et b_n convergent quadratiquement si la limite est non nulle.

Généralisons la suite AGM à des nombres complexes.

Définition 1.6.1. *Soient $a, b \in \mathbb{C}$. On dit que (a', b') est un itéré AGM de (a, b) si :*

$$a' = \frac{a + b}{2} \qquad \text{et} \qquad b'^2 = ab.$$

Notons que tout couple a deux itérés et que les itérés de (a, b) sont les mêmes que ceux de (b, a).

Définition 1.6.2. *Soient $a, b \in \mathbb{C}$. On dit que $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM associée à (a, b) si $a_0 = a$, $b_0 = b$ et si pour tout $n \in \mathbb{N}$, le couple (a_{n+1}, b_{n+1}) est un itéré AGM du couple (a_n, b_n).*

Contrairement au cadre réel, les suites AGM complexes ne sont pas déterminées uniquement par les valeurs de départ mais aussi par le choix des racines carrés tout le long des itérations.

Définition 1.6.3. *Si $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM et si $m \geq 1$, on dit que b_m est* le bon choix *de racine parmi b_m et $-b_m$ si*

$$|a_m - b_m| \leq |a_m + b_m|$$

avec de plus $\Im(\frac{b_m}{a_m}) > 0$ lorsque l'inégalité ci-dessus est une égalité. Dans le cas contraire, on parle de mauvaix choix *de racine.*

On remarque qu'une suite associée à deux réels strictement positifs ne contient que des bons choix de racines.

Si $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM, alors il existe $A \in \mathbb{C}$ tel que $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = A$ et tel que $A \neq 0$ si et seulement si le nombre de mauvais choix de la suite AGM est fini. Soit $\lambda \in \mathbb{C}^*$, alors $(\lambda a_n, \lambda b_n)$ est aussi une suite AGM et à chaque rang n, $(\lambda a_n, \lambda b_n)$ est un bon choix si et seulement si (a_n, b_n) en est un. S'il existe un rang n tel que $a_n = 0$ ou $b_n = 0$, alors $\forall m \geq n$, $b_m = 0$.

Définition 1.6.4. *On définit une fonction $M : \mathbb{C} \to \mathbb{C}$ comme suit. Pour tout $z \in \mathbb{C}\backslash\{-1, 0\}$, on prend $M(z)$ comme étant la limite de la suite AGM associée à $(1, z)$ ne comportant* que *des bons choix de racine, et avec $M(0) = M(-1) = 0$. Pour tous $a, b \in \mathbb{C}$, on définit l'ensemble $\mathcal{B}_1(a, b)$ comme étant l'ensemble de toutes les limites des suites AGM associées à (a, b).*

Notons que $\forall a, b \in \mathbb{C}, \lambda \in \mathbb{C}^*$, $\mathcal{B}_1(\lambda a, \lambda b) = \{\lambda x, x \in \mathcal{B}_1(a, b)\}$. Les deux propositions qui suivent sont des résultats fondamentaux qui vont nous permettre d'évaluer rapidement les thêta constantes.

Proposition 1.6.5. *Pour tout $\tau \in \mathcal{H}_1$, on a*

$$\mathcal{B}_1(\vartheta_0^2(\tau), \vartheta_1^2(\tau)) = \left\{ \frac{\theta_0^2(\tau)}{\theta_0^2(\gamma \cdot \tau)} : \gamma \in \Gamma_{k'} \right\} \cup \{0\}.$$

Démonstration. Voir [19, Théorème 3.1]. □

Proposition 1.6.6. *Pour tout $\tau \in \mathcal{F}_{k'}$, $M(k'(\tau)) = \frac{1}{\vartheta_0^2(\tau)}$.*

Démonstration. Voir [19, Proposition 3.2]. □

Ces deux derniers résultats ont été généralisés en dimension 2 (voir [19, Théorème 8.1] et la proposition 3.6.1). Le résultat qui suit permet de déduire un algorithme pour évaluer la fonction M à une précision donnée.

Proposition 1.6.7. *Pour tout $z \in \mathbb{C}\backslash\{0, 1\}$ ayant une partie réelle positive ou nulle, si l'on note $(a_n, b_n)_{n\in\mathbb{N}}$ la suite AGM associée au calcul de $M(z)$ et que l'on pose*

$$B(N, z) = \max\left(\lceil \log_2 |\log_2 |z|| \rceil, 1\right) + \lceil \log_2 (N + 2) \rceil + 2,$$

alors $a_{B(N,z)}$ est une approximation de $M(z)$ avec une précision relative de N bits.

Démonstration. Voir [19, Proposition 3.3]. □

On cherche un algorithme efficace qui permet d'évaluer les thêta constantes. L'algorithme naïf, qui consiste à utiliser les définitions de ces fonctions comme séries de Fourier est de complexité en $O(\mathcal{M}'(N)\sqrt{\frac{N}{\Im(\tau)}})$, d'après [19, Pages 97-100], où $\mathcal{M}'(N)$ est la complexité de la multiplication de deux entiers de N bits.

Une autre méthode consiste à utiliser l'AGM. Nous décrivons l'idée générale de l'algorithme. Une description détaillée se trouve dans [19, Section 4.2]. L'idée est la suivante. Supposons que l'on connaisse la valeur $k'(\tau)$ pour $\tau \in \mathcal{F}_1$. On a vu que $M(k'(\tau)) = \frac{1}{\vartheta_0^2(\tau)}$ pour $\tau \in \mathcal{F}_{k'}$. Mais comme $S \cdot \tau$ est aussi dans $\mathcal{F}_{k'}$, on en déduit que $M(k'(S \cdot \tau)) = \frac{1}{\vartheta_0^2(S\cdot\tau)}$, ce qui se réécrit $M(k(\tau)) = \frac{\imath}{\tau\vartheta_0^2(\tau)}$. D'où :

$$\tau = \imath \frac{M(k'(\tau))}{M(k(\tau))},$$

sachant que la valeur de $k(\tau)$ peut se déduire de celle de $k'(\tau)$ en utilisant l'égalité de Jacobi avec le fait que $\Re(k(\tau)) > 0$ (d'après [20, Proposition 7]).

Soit maintenant $\tau \in \mathcal{F}_1$ et soit la fonction

$$f_\tau : z \in \mathbb{C}^{r+} \longmapsto \imath M(z) - \tau M(\sqrt{1-z^2}) \in \mathbb{C}.$$

D'après ce qui précède, on a $f_\tau(k'(\tau)) = 0$. On peut donc penser que des itérations de Newton sur la fonction f_τ vont nous permettre d'évaluer $k'(\tau)$. C'est une fonction analytique car M l'est.

Proposition 1.6.8. *Pour tout $\tau \in \mathcal{F}_{k'}$, on a*

$$\frac{dM}{dz}(k'(\tau)) = \frac{\vartheta_0'(\tau)}{\imath\pi\vartheta_0(\tau)\vartheta_1^2(\tau)\vartheta_2^4(\tau)} \qquad et \qquad \frac{df_\tau}{dz}(k'(\tau)) = \frac{-2}{\pi\tau\vartheta_1^2(\tau)\vartheta_2^4(\tau)}.$$

Démonstration. Voir [19, Propositions 4.2 et 4.3]. □

On peut alors montrer que l'on a :

Théorème 1.6.9. *Il existe un algorithme permettant pour tous $\tau \in \mathcal{F}_1$ et $N > 0$ d'évaluer $k'(\tau)$ avec une précision relative de N bits en temps $O(\mathcal{M}'(N)\log N)$.*

Démonstration. Voir [19, Théorème 4.3]. □

Par ce qui précède, on en déduit qu'on peut également évaluer $k(\tau)$ avec la même complexité.

Nous avons vu avec l'équation (1.31) comment on peut exprimer le j-invariant en fonction de k'. Ainsi, la complexité d'évaluation de cet invariant est également en $O(\mathcal{M}'(N)\log N)$, pour tout $\tau \in \mathcal{H}_1$ (c'est bien sur $\mathcal{H}_1$ car tout τ donné est équivalent à un τ' dans le domaine fondamental $\mathcal{F}_1$, et les j-invariants de τ et τ' sont les mêmes).

La fonction η de Dedekind est souvent utilisée pour construire des fonctions modulaires. On a

$$\eta(\tau)^{12} = \frac{k^2(\tau)k'^2(\tau)\vartheta_0^2(\tau)}{16}$$

et le développement en q de η peut être utilisé pour déterminer quelle est la bonne racine douzième. On peut donc évaluer $\eta(\tau)$ en temps $O(\mathcal{M}'(N)\log N)$, indépendamment de la valeur de τ.

1.6.2 Algorithme de calcul et complexité

Soit f une fonction modulaire pour un sous-groupe Γ de Γ_1. Nous cherchons à calculer le polynôme modulaire $\Phi_{f,j}$ défini dans le théorème 1.4.14 ou la définition 1.4.15. Il existe plusieurs algorithmes pour cela ([25, 10, 11]). Mais nous allons nous concentrer sur une seule méthode : celle de l'évaluation/interpolation (voir [25]), car c'est celle que nous généraliserons pour calculer les polynômes modulaires dans le cadre de la dimension 2. Pour pouvoir utiliser cette méthode, nous supposerons que $\Phi_{f,j}$ est à coefficients entiers (d'après le théorème 1.4.18, c'est le cas pour les fonctions j_R, invariantes par le sous-groupe Γ_R) et que f est holomorphe sur $\mathcal{H}_1$.

Avec les notations du théorème 1.4.14, on a

$$\Phi_{f,j}(X,j) = \prod_{k=1}^{[\Gamma_1:\Gamma]} (X - f^{\lambda_{\gamma_k}}) = X^{[\Gamma_1:\Gamma]} + \sum_{k=0}^{[\Gamma_1:\Gamma]-1} c_k X^k,$$

où c_k est une fonction de $\mathcal{H}_1$ vers $\mathbb{C}$ qui est une expression symétrique en les conjugués $f^{\lambda\gamma_k}$ de f et qui est aussi, d'après ce théorème 1.4.14 et notre supposition de départ, un polynôme en j (corollaire 1.4.12).

Si on se donne une valeur $\tau \in \mathcal{H}_1$, que l'on évalue les $f^{\lambda\gamma_k}(\tau)$, que l'on fait le produit des $X - f^{\lambda\gamma_k}(\tau)$ et que l'on sépare les coefficients en fonction des puissances de X, alors on obtient les valeurs $c_k(\tau)$. Ainsi, un dispose d'un algorithme permettant d'évaluer les fonctions c_k en un point donné et donc si on les évalue en un nombre suffisant de valeurs, on peut procéder à une phase d'interpolation pour trouver les c_k. Rappelons qu'il faut au moins $\deg_j(\Phi_{f,j}) + 1$ valeurs pour pouvoir appliquer l'interpolation de Lagrange. Les calculs sont fait en approximation flottante et on obtient donc une approximation des c_k, mais puisque l'on sait qu'ils sont à coefficients entiers, il nous suffit d'arrondir à l'entier le plus proche. Remarquons que l'on peut appliquer la même méthode si f n'est pas holomorphe sur $\mathcal{H}_1$: dans ce cas, il faut interpoler pour avoir une fraction rationnelle et identifier les coefficients à des nombres rationnels.

Étudions la complexité de cet algorithme. Notons $E(N)$ la complexité pour évaluer la fonction f avec une précision de N bits et posons $\ell = [\Gamma_1 : \Gamma]$. Rappelons que la fonction j peut s'évaluer en temps $O(\mathcal{M}'(N) \log N)$. La phase d'évaluation comporte d'une part $\ell(\deg_j(\Phi_{f,j})+1)$ évaluations de f et $\deg_j(\Phi_{f,j})+1$ évaluations de la fonction j à un coût qui est donc en

$$O(\ell \deg_j(\Phi_{f,j})E(N) + \deg_j(\Phi_{f,j})\mathcal{M}'(N) \log N)$$

et d'autre part la reconstruction de $\deg_j(\Phi_{f,j}) + 1$ polynômes de degré ℓ à partir de leurs racines, ce qui peut se faire, en multipliant des polynômes complexes avec la FFT, en temps

$$O(\deg_j(\Phi_{f,j})\, \ell \log^2 \ell\, \mathcal{M}'(N) + \mathcal{M}'(N) \log N).$$

Ici, le terme $\mathcal{M}'(N) \log N$ représente le temps qu'il faut pour calculer une racine primitive de l'unité d'un ordre assez grand.

La phase d'interpolation consiste en ℓ interpolations de polynômes de degré $\deg_j(\Phi_{f,j})$. En utilisant des algorithmes rapides ([85, algorithme 10.11]), ceci prend

$$O(\ell \deg_j(\Phi_{f,j}) \log^2(\deg_j(\Phi_{f,j}))\mathcal{M}'(N)),$$

une fois que les racines de l'unité sont disponibles.

Dans le cas où f est une fonction qui s'exprime en fonction des thêta constantes, comme le j-invariant ou la fonction η de Dedekind, nous avons vu que $E(N) \subseteq O(\mathcal{M}'(N) \log N)$ de telle sorte que la complexité totale est

$$O((\ell \deg_j(\Phi_{f,j}) \log^2 (\max(\ell, \deg_j(\Phi_{f,j}))) + \log N)\mathcal{M}'(N)).$$

On peut enfin se demander à quelle précision il faut travailler. La *hauteur logarithmique* d'un polynôme à coefficients dans $\mathbb{Z}$ est définie comme étant le logarithme de la valeur absolue du plus grand coefficient de ce polynôme. Cette hauteur nous fournit une borne inférieure pour la précision dans laquelle nous devons faire nos calculs. Si on prend pour un nombre premier p : $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, $\Gamma = \Gamma^0(p)$ et $f(\tau) = j_R(\tau) = j(\tau/p)$, cette hauteur est connue (voir [12]) : c'est

$$6(p+1)(\log p + O(1)) \subseteq O(p \log p),$$

ce qui fait que le polynôme modulaire entre $j(\tau)$ et $j(\tau/p)$, qui est appelé *polynôme modulaire classique*, peut être calculé en temps

$$O(p^2 \log^2 p \mathcal{M}'(p \log p)),$$

en supposant pas trop de perte de précision. Cette complexité est quasi-linéaire en la taille de la sortie.

1.6.3 Exemples de polynômes modulaires

Polynômes modulaires classiques. Nous venons de voir que le polynôme modulaire reliant j et $j_p := j_R$ avec $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ s'appelle le polynôme modulaire classique de degré p. L'interprétation modulaire qu'ont ces polynômes est qu'ils paramétrisent les classes d'isomorphismes des courbes elliptiques munies d'une isogénie de degré p lorsque p est premier.

En effet, d'après le théorème 1.3.12, les matrices S et T^i, pour i de 0 à $p-1$ sont des représentants des classes à droite du quotient $\Gamma_1/\Gamma^0(p)$. Donc pour un $\tau \in \mathcal{H}_1$ donné, on s'intéresse aux points $\frac{\tau+i}{p}$ et $\frac{-1}{p\tau}$. En faisant agir par S, on remarque que le dernier point est équivalent à $p\tau$ modulo Γ_1. Or, nous avons vu dans le théorème 1.2.13 que les applications holomorphes suivantes qui envoient 0 sur 0, pour i de 0 à $p-1$,

$$\begin{array}{ccccc} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \longrightarrow & \mathbb{C}/(\mathbb{Z}+\frac{(\tau+i)}{p}\mathbb{Z}) & & \\ z & \longmapsto & z & \text{et} & \\ pz & \longleftarrow & z & & \end{array} \qquad \begin{array}{ccc} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \longrightarrow & \mathbb{C}/(\mathbb{Z}+p\tau\mathbb{Z}) \\ z & \longmapsto & pz \\ z & \longleftarrow & z \end{array}$$

correspondent aux isogénies de degré p. Ces isogénies sont bien de degré p d'après ce que nous avons dit sur les isogénies duales à la section 1.1.3.

Les points $\frac{\gamma\cdot\tau}{p}$ pour $\gamma \in \{T^i, S\}$ sont donc des représentants des classes d'isomorphismes des courbes p-isogènes à une courbe τ donnée.

Le polynôme modulaire classique d'ordre m entier pour $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)$ est le polynôme

$$\Phi_m(X, j) = \prod_{i=1}^{p+1} (X - j_m(\gamma_i \cdot \tau)),$$

pour γ_i dans $\{T^i, S\}$.

Proposition 1.6.10. *Soit $m \in \mathbb{N}$.*

1. *$\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$;*
2. *$\Phi_m(X, Y)$ est irréductible comme polynôme en X ;*
3. *Si $m > 1$, alors $\Phi_m(X, Y) = \Phi_m(Y, X)$;*
4. *Si m n'est pas un carré, alors $\Phi_m(X, Y)$ est un polynôme de degré > 1 dont le coefficient dominant est ± 1 ;*
5. *Si m est premier, alors $\Phi_m(X, Y) \equiv (X^m - Y)(X - Y^m) \bmod m\mathbb{Z}[X, Y]$.*

Démonstration. Voir [16, Théorème 11.18]. □

À titre d'exemple, on a

$$\Phi_{j,j_2}(X, Y) = X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY + 8748000000X + Y^3 - 162000Y^2 + 8748000000Y - 157464000000000;$$

$\Phi_{j,j_3}(X,Y) = X^4 - X^3Y^3 + 2232X^3Y^2 - 1069956X^3Y + 36864000X^3 + 2232X^2Y^3 + 2587918086X^2Y^2 + 8900222976000X^2Y + 452984832000000X^2 - 1069956XY^3 + 8900222976000XY^2 - 770845966336000000XY + 1855425871872000000000X + Y^4 + 36864000Y^3 + 452984832000000Y^2 + 1855425871872000000000Y;$

$\Phi_{j,j_5}(X,Y) = X^6 - X^5Y^5 + 3720X^5Y^4 - 4550940X^5Y^3 + 2028551200X^5Y^2 - 246683410950X^5Y + 1963211489280X^5 + 3720X^4Y^5 + 1665999364600X^4Y^4 + 107878928185336800X^4Y^3 + 383083609779811215375X^4Y^2 + 1285417989068288163840000X^4Y + 1284733132841424456253440X^4 - 4550940X^3Y^5 + 107878928185336800X^3Y^4 - 44120696551291483524610 0X^3Y^3 + 2689848885838073157741772 8000X^3Y^2 - 1924579346189282996551082311 68000X^3Y + 2802447778284395278043215652978688 00X^3 + 2028551200X^2Y^5 + 383083609779811215375X^2Y^4 + 2689848885838073157741772 8000X^2Y^3 + 5110941777552418083110765199360000X^2Y^2 + 3655473658394962929570647233265664000 0X^2Y + 6692500042627997708487149415015068467200X^2 - 246683410950XY^5 + 1285417989068288163840000XY^4 - 1924579346189282996551082311 68000XY^3 + 3655473658394962929570647233265664000 0XY^2 - 2640734570766205962597157902479787829493 76XY + 5327433080342442545042016027335650915123200 0X + Y^6 + 1963211489280Y^5 + 1284733132841424456253440Y^4 + 2802447778284395278043215652978688 00Y^3 + 6692500042627997708487149415015068467200Y^2 + 5327433080342442545042016027335650915123200 0Y + 1413599471547213586977534746910713627510046720 00.$

Polynômes modulaires canoniques. Les exemples qui précèdent montrent que les coefficients des polynômes croissent très rapidement. Ceci justifie qu'il est important de chercher d'autres invariants pour le groupe $\Gamma^0(p)$. Lorsque l'on prend la fonction $f_p(\tau) = \left(\frac{\eta(\tau/p)}{\eta(\tau)}\right)^{2s}$ pour $s = 12/\operatorname{pgcd}(12, p-1)$, qui est une "fonction de Weber généralisé", on obtient ce que l'on appelle le *polynôme modulaire canonique* de degré p. On trouve alors

$$\Phi_{j,f_2}(X,Y) = X^3 + 48X^2 - XY + 768X + 4096;$$

$$\Phi_{j,f_3}(X,Y) = X^4 + 36X^3 + 270X^2 - XY + 756X + 729;$$

$$\Phi_{j,f_5}(X,Y) = X^6 + 30X^5 + 315X^4 + 1300X^3 + 1575X^2 - XY + 750X + 125.$$

Polynômes modulaires avec les fonctions de Schläfli. On peut également s'intéresser à des polynômes modulaires pour d'autres groupes que $\Gamma^0(p)$. Considérons par exemple la fonction $\mathfrak{f} = \zeta_{48}^{-1}\frac{\eta((z+1)/2)}{\eta(z)} = \zeta_{48}^{-1}\mathfrak{w}_2(z+1)$ qui est modulaire pour un sous-groupe de $\Gamma_1(48)$. Soit p un premier qui ne divise pas 48, c'est-à-dire différent de 2 et 3. On pose $\mathfrak{f}_p(z) = \mathfrak{f}(z/p)$. C'est une fonction modulaire pour le groupe $\Gamma_1(48) \cap \Gamma^0(p)$. On peut montrer que le polynôme

$$\Phi_{\mathfrak{f},\mathfrak{f}_p}(X, \mathfrak{f}(\tau)) = \prod_{i=1}^{p+1}(X - \mathfrak{f}_p(\gamma_i\tau)),$$

où les γ_i sont des représentants des classes de $\Gamma_1(48)/(\Gamma_1(48) \cap \Gamma^0(p))$, est dans $\mathbb{Z}[\mathfrak{f}]$ et est unitaire. Il y a bien $p+1$ représentants car c'est le cas de $\Gamma_1/\Gamma^0(p)$ et on peut faire correspondre les classes de ces deux quotients d'après le théorème des restes Chinois (d'où l'importance de prendre p différent de 2 et 3). Un ensemble de représentants est constitué des matrices $\left(\begin{smallmatrix} 1 & 48i \\ 0 & 1 \end{smallmatrix}\right)$, pour i de 0 à $p-1$, et de la matrice $\left(\begin{smallmatrix} 1-48k & 48k \\ -48k & 1+48k \end{smallmatrix}\right)$ avec $k \equiv 48^{-1} \bmod p$ (qui correspond à S). Pour calculer ce polynôme, on peut donc utiliser l'algorithme d'évaluation/interpolation, en remplaçant j par $\mathfrak{f}$. On trouve :

$$\begin{aligned}
\Phi_{\mathfrak{f},\mathfrak{f}_5}(X,Y) &= X^6 - X^5Y^5 + 4XY + Y^6; \\
\Phi_{\mathfrak{f},\mathfrak{f}_7}(X,Y) &= X^8 - X^7Y^7 + 7X^4Y^4 - 8XY + Y^8; \\
\Phi_{\mathfrak{f},\mathfrak{f}_{11}}(X,Y) &= X^{12} - X^{11}Y^{11} + 11X^9Y^9 - 44X^7Y^7 + 88X^5Y^5 - 88X^3Y^3 + \\
&\quad 32XY + Y^{12}.
\end{aligned}$$

Weber montre dans [87, Page 266] que le fait que le monôme $c\mathfrak{f}^i\mathfrak{f}_p^k$ soit non nul implique que $pi + k \equiv p + 1 \bmod 24$, ce qui permet de diviser par 24 le nombre d'évaluations. De plus, $\Phi_{\mathfrak{f},\mathfrak{f}_p}$ est symétrique. Nous avons obtenu des résultats similaires en dimension 2 pour certains polynômes modulaires.

Polynômes modulaires avec les thêta constantes. Suivant [57], nous avons également calculé des polynômes modulaires en prenant $b(\tau) = \frac{\vartheta_1(\tau)}{\vartheta_0(\tau)}$ et $b_p(\tau) = \frac{\vartheta_1(\tau/p)}{\vartheta_0(\tau/p)}$ pour p premier.

La fonction b est modulaire pour le groupe $\Gamma_1(8)$ tandis que b_p l'est pour $\Gamma_1(8) \cap \Gamma^0(p)$, si $p \neq 2$. On se retrouve donc exactement dans le même cas que précédemment. Un ensemble de représentants est alors $\left(\begin{smallmatrix} 1 & 8i \\ 0 & 1 \end{smallmatrix}\right)$, pour i de 0 à $p-1$, plus la matrice $\left(\begin{smallmatrix} 1-8k & 8k \\ -8k & 1+8k \end{smallmatrix}\right)$ avec $k \equiv 8^{-1} \bmod p$.

$$\begin{aligned}
\Phi_{b,b_3}(X,Y) &= X^4 - 4X^3Y^3 + 6X^2Y^2 - 4XY + Y^4; \\
\Phi_{b,b_5}(X,Y) &= X^6 - 16X^5Y^5 + 10X^5Y + 15X^4Y^2 - 20X^3Y^3 + 15X^2Y^4 + \\
&\quad 10XY^5 - 16XY + Y^6; \\
\Phi_{b,b_7}(X,Y) &= X^8 - 64X^7Y^7 + 56X^7Y^3 - 112X^6Y^6 + 140X^6Y^2 - 112X^5Y^5 + \\
&\quad 56X^5Y + 70X^4Y^4 + 56X^3Y^7 - 112X^3Y^3 + 140X^2Y^6 - \\
&\quad 112X^2Y^2 + 56XY^5 - 64XY + Y^8.
\end{aligned}$$

Chapitre 2

Variétés abéliennes complexes

Le but de ce chapitre est d'étudier d'un point de vue théorique les variétés abéliennes complexes. Commençons par une définition.

Définition 2.0.11. *Une* variété abélienne *A sur un corps K parfait est un groupe algébrique, sur K, complet et géométriquement connexe.*

Sur un corps algébriquement clos, A, en tant que groupe, est commutatif ([67, Page 41]), d'où le nom d'abélien.

Lorsque l'on se place sur $K = \mathbb{C}$, l'espace complexe analytique sous-jacent d'une variété abélienne A est un groupe analytique complexe et compact. D'après [4, Lemme 1.1.1] ou [67, Chapitre I], c'est également un tore complexe, où par tore complexe nous entendons :

Définition 2.0.12. *Un tore complexe de dimension g est le quotient d'un espace vectoriel complexe V de dimension g par un* réseau Λ*, c'est-à-dire par un $\mathbb{Z}$-module discret et libre, de rang $2g$.*

Ainsi, nous allons étudier les tores complexes et nous allons voir qu'un tel tore est une variété abélienne s'il peut être muni d'une forme de Riemann définie positive, ce qui est équivalent à dire que la variété peut être plongée dans un espace projectif. Ceci conduira à la notion de polarisation d'une part et à l'étude des fonctions thêta d'autre part.

Nous verrons qu'on peut représenter une variété abélienne polarisée par une matrice dans l'espace de Siegel, et que ce dernier est un espace de modules pour les variétés abéliennes avec une polarisation fixée, ce qui constitue une généralisation de ce qui se passe en dimension 1 avec le demi-plan de Poincaré. Enfin, nous verrons le lien que ces variétés ont avec les courbes.

Nous nous sommes basé principalement sur [4, 39, 68] pour écrire ce chapitre.

2.1 Homomorphismes

Il n'existe que deux types d'applications holomorphes entre les tores complexes : les homomorphismes et les translations. Soient $X_1 = V_1/\Lambda_1$ et $X_2 = V_2/\Lambda_2$ deux tores complexes de dimensions g_1 et g_2. Par *homomorphisme*, nous entendons une application holomorphe $f : X_1 \to X_2$ qui est compatible avec la structure de groupe, tandis qu'une *translation* par un élement $x_0 \in X_1$ est l'application holomorphe $t_{x_0} : X_1 \to X_1$ qui à x associe $x + x_0$. Le fait qu'il n'y ait pas d'autres applications est justifié par la proposition qui suit.

Proposition 2.1.1. *Soit $h : X_1 \to X_2$ une application holomorphe. Il existe un unique homomorphisme $f : X_1 \to X_2$ tel que $h = t_{h(0)} \circ f$ et donc tel que $h(x) = f(x) + h(0)$ pour tout $x \in X_1$.*

Démonstration. Voir [4, Proposition 1.2.1.a]. □

L'ensemble des homomorphismes de X_1 vers X_2 forme un groupe abélien pour l'addition des applications, que l'on note $\mathrm{Hom}(X_1, X_2)$. Soit $f : X_1 \to X_2$ un homomorphisme. On peut montrer ([4, Proposition 1.2.1.b]) qu'il existe alors une unique application $\mathbb{C}$-linéaire $F : V_1 \to V_2$ telle que $F(\Lambda_1) \subseteq \Lambda_2$ induisant f. On obtient un homomorphisme injectif de groupes abéliens :

$$\begin{array}{rccc} \rho_a : & \mathrm{Hom}(X_1, X_2) & \hookrightarrow & \mathrm{Hom}_{\mathbb{C}}(V_1, V_2) \\ & f & \longmapsto & F \end{array}$$

que l'on appelle *représentation analytique* de $\mathrm{Hom}(X_1, X_2)$ (d'où le a en indice). De plus, la restriction F_{Λ_1} de F au réseau Λ_1 est $\mathbb{Z}$-linéaire et cette restriction détermine F et f. On obtient alors un autre homomorphisme injectif

$$\begin{array}{rccc} \rho_r : & \mathrm{Hom}(X_1, X_2) & \hookrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2) \\ & f & \longmapsto & F_{\Lambda_1} \end{array}$$

qui est appelé *représentation rationnelle* de $\mathrm{Hom}(X_1, X_2)$ (et, également, d'où le r en indice).

Proposition 2.1.2. $\mathrm{Hom}(X_1, X_2) \simeq \mathbb{Z}^m$ *pour un certain* $m \leq 4g_1g_2$.

Démonstration. Voir [4, Proposition 1.2.2]. On a que $\mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2) \simeq \mathbb{Z}^{4g_1g_2}$ donc ses sous-groupes sont de la forme $\mathbb{Z}^m$. On conclut avec l'injectivité de ρ_r. □

Soient $X = V/\Lambda$ un tore de dimension g, $e_1, \ldots, e_g$ une base de V et $\lambda_1, \ldots, \lambda_{2g}$ une base de Λ. On peut écrire les λ_i en termes des e_j : $\lambda_i = \sum_{j=1}^{g} \lambda_{j,i} e_j$. La matrice

$$\Pi = \begin{pmatrix} \lambda_{1,1} & \ldots & \lambda_{1,2g} \\ \vdots & & \vdots \\ \lambda_{g,1} & \ldots & \lambda_{g,2g} \end{pmatrix} \in M(g \times 2g, \mathbb{C})$$

est appelée une *matrice des périodes* de X. C'est une notion qui nous apparaît fondamentale dans la mesure où, par la suite, nous manipulerons les variétés abéliennes grâce à leur représentation en matrice des périodes. Cette matrice des périodes dépend des bases choisies bien qu'elle représente entièrement le tore. Nous verrons dans la section 2.5.1 sur les espaces de modules comment sont reliées deux matrices des périodes associées à une même variété abélienne.

Inversement, on peut se demander quelles matrices de $M(g \times 2g, \mathbb{C})$ sont des matrices des périodes d'un tore complexe. La proposition suivante nous fournit la réponse à cette question.

Proposition 2.1.3. *Une matrice $\Pi \in M(g \times 2g, \mathbb{C})$ est une matrice des périodes d'un tore complexe si et seulement si la matrice $P = \left(\frac{\Pi}{\overline{\Pi}}\right) \in M_{2g}(\mathbb{C})$ est inversible.*

Démonstration. Voir [4, Proposition 1.1.2]. La matrice Π est une matrice des périodes si et seulement si ses colonnes sont $\mathbb{R}$-linéairement indépendantes et engendrent donc une réseau de $\mathbb{C}^g$. Si ce n'est pas le cas, alors il existe $x \in \mathbb{R}^{2g}$ non

nul avec $\Pi x = 0$ et donc $Px = 0$, ce qui implique que $\det P = 0$. Réciproquement, si P n'est pas inversible, alors il existe deux vecteurs x et y de $\mathbb{R}^{2g}$, non nuls en même temps, tels que $P(x + \imath y) = 0$ et donc $\Pi(x + \imath y) = 0$ et $\overline{\Pi}(x + \imath y) = 0$. Mais $\Pi(x - \imath y) = \overline{\overline{\Pi}(x + \imath y)} = 0$ ce qui implique que $\Pi x = \Pi y = 0$ et que les colonnes de Π sont $\mathbb{R}$-linéairement dépendantes. □

Considérons respectivement deux matrices des périodes Π_1 et Π_2 pour les tores complexes $X_1 = V_1/\Lambda_1$ et $X_2 = V_2/\Lambda_2$ de dimensions g_1 et g_2. Soit $f : X_1 \to X_2$ un homomorphisme. Par rapport aux bases choisies pour les matrices des périodes, la représentation analytique (resp. rationnelle) $\rho_a(f)$ (resp. $\rho_r(f)$) est donnée par une matrice $A \in M(g_2 \times g_1, \mathbb{C})$ (resp. $R \in M(2g_2 \times 2g_1, \mathbb{Z})$). La condition $\rho_a(f)(\Lambda_1) \subseteq \Lambda_2$ se traduit matriciellement par

$$A\Pi_1 = \Pi_2 R. \tag{2.1}$$

En outre, deux matrices satisfaisant cette relation définissent un homomorphisme $X_1 \to X_2$. Lorsque $f \in \mathrm{End}(X)$, on a la relation

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

et en utilisant la proposition 2.1.3, on peut obtenir la matrice A à partir de R et vice-versa.

Proposition 2.1.4. *Soit $f : X_1 \to X_2$ un homomorphisme. Alors*
- $\mathrm{im}\,(f)$ *est un sous-tore de X_2 ;*
- $\ker(f)$ *est un sous-groupe fermé de X_1. La composante connexe* $(\ker(f))_0$ *de* $\ker(f)$ *qui contient* 0 *est un sous-tore de X_1 d'indice fini dans* $\ker(f)$.

Démonstration. Voir [4, Proposition 1.2.4]. □

Nous pouvons enfin définir la notion d'isogénie.

Définition 2.1.5. *Une* isogénie *entre X_1 et X_2 est un homomorphisme surjectif et de noyau fini. Le* degré *de l'isogénie est le cardinal du noyau.*

Si les dimensions des deux tores complexes X_1 et X_2 sont identiques, il suffit alors que f soit surjective ou de noyau fini pour être une isogénie. On peut en déduire que l'application analytique $F = \rho_a(f)$ est un isomorphisme si et seulement si f est une isogénie. Ainsi, à isomorphisme près, on peut supposer que $F = \mathrm{Id}$, $\Lambda_1 \subseteq \Lambda_2$ et que f est l'application canonique $V_1/\Lambda_1 \to V_1/\Lambda_2$. Il y a alors une bijection entre isogénies de domaine X_1 et sous-groupes finis de X_1. Le degré de l'isogénie est également l'indice $[\Lambda_2 : \rho_r(f)(\Lambda_1)]$. Si de plus f est un endomorphisme, alors $\Lambda_1 = \Lambda_2$ et $\deg f = \det \rho_r(f)$ (voir [4, Section 1.2]).

L'exemple le plus fondamental d'isogénie est la *multiplication par m*. Soit $[m] : X \to X$ l'application qui à x associe mx. Le noyau $X[m]$ de cette application est appelé le *groupe des points de m-torsion* de X. On a

$$\ker[m] = \frac{1}{m}\Lambda/\Lambda \simeq \Lambda/m\Lambda \simeq (\mathbb{Z}/m\mathbb{Z})^{2g} \tag{2.2}$$

et ainsi, la multiplication par m est une isogénie de degré m^{2g}.

Proposition 2.1.6. *Soit $f : X_1 \to X_2$ une isogénie de degré d. Il existe une unique isogénie $g : X_2 \to X_1$ telle que $f \circ g = [d]_{X_2}$ et $g \circ f = [d]_{X_1}$. Cette isogénie est appelé* l'isogénie contragrédiente *de f et est de même degré.*

Démonstration. Voir [4, Proposition 1.2.6]. □

Notons que par cette proposition, une isogénie a une isogénie inverse dans $\mathrm{Hom}_{\mathbb{Q}}(X_2, X_1) := \mathrm{Hom}(X_2, X_1) \otimes \mathbb{Q}$ qui est $(\deg f)^{-1} g$, où g est l'isogénie contragrédiente de f. Le corollaire 1.2.7 de [4] nous affirme qu'en fait un homomorphisme de $\mathrm{End}(X_1)$ est une isogénie si et seulement s'il est inversible dans $\mathrm{End}_{\mathbb{Q}}(X_1)$. Enfin, par cette même proposition, les isogénies définissent une relation d'équivalence dans l'ensemble des tores complexes. On dira que deux tores complexes sont *isogènes* s'il existe une isogénie entre eux.

2.2 Tores et variétés abéliennes complexes

Nous avons dit que toute variété abélienne est un tore complexe. La réciproque est fausse. Nous allons voir qu'un tore complexe est une variété abélienne si ce tore est muni d'une forme Hermitienne définie positive et voir que c'est équivalent à l'existence d'un diviseur ample, et donc d'un plongement dans un espace projectif.

2.2.1 Forme de Riemann

Définition 2.2.1. *Une* forme de Riemann *sur un tore complexe V/Λ est une forme hermitienne $H : V \times V \to \mathbb{C}$ telle que $\Im(H(\Lambda, \Lambda)) \subseteq \mathbb{Z}$. Nous considérons ici une forme hermitienne H sur V comme étant une application $V \times V \to \mathbb{C}$ qui est $\mathbb{C}$-linéaire en la première variable et qui vérifie $H(x, y) = \overline{H(y, x)}$ pour tous $x, y \in V$.*

Exemple 2.2.2. *Soit le réseau $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$ pour $\tau_1, \tau_2 \in \mathbb{C}$ avec, quitte à les renommer, $\Im(\tau_1/\tau_2) > 0$. Alors la forme $(x, y) \mapsto \frac{1}{\Im(\tau_1/\tau_2)} x\overline{y}$ est une forme de Riemann par rapport à Λ définie positive. Ainsi, tout tore complexe de dimension 1 est une variété abélienne de dimension 1. Les résultats du premier chapitre nous disent que c'est aussi une courbe elliptique complexe.*

Exemple 2.2.3. *Soit Ω une matrice de taille $g \times g$ qui est symétrique et dont la partie imaginaire est définie positive. Alors $H(x, y) = {}^t x \Im(\Omega)^{-1} \overline{y}$ est une forme de Riemann définie positive par rapport au réseau $\mathbb{Z}^g + \Omega\mathbb{Z}^g$. Ainsi, le tore $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ est une variété abélienne.*

Il existe une autre manière d'introduire les formes de Riemann : à travers des formes alternées.

Proposition 2.2.4. *Il y a une bijection entre l'ensemble des formes hermitiennes H de V et l'ensemble des formes alternées $E : V \times V \to \mathbb{R}$ vérifiant $E(\imath x, \imath y) = E(x, y)$. Cette bijection est donnée pour tous $x, y \in V$ par :*

$$E(x, y) = \Im(H(x, y)) \qquad \text{et} \qquad H(x, y) = E(\imath x, y) + \imath E(x, y).$$

Si, de plus, E est non dégénérée, on dit que c'est une forme symplectique.

Démonstration. Voir [4, Lemme 2.1.7]. Soit E une forme alternée vérifiant $E(\imath x, \imath y) = E(x, y)$. La forme H est hermitienne car

$$H(x, y) = E(\imath x, y) + \imath E(x, y) = -E(\imath y, -x) - \imath E(y, x) = \overline{H(y, x)}.$$

Réciproquement, soit H une forme hermitienne. La forme $E = \Im(H)$ est alternée et $E(\imath x, \imath y) = \Im(H(\imath x, \imath y)) = \Im(H(x, y)) = E(x, y)$. □

Exemple 2.2.5. *Soit le tore* $\mathbb{C}/(\mathbb{Z}+\imath\mathbb{Z})$. *Alors* $E(x+\imath x', y+\imath y') = x'y - xy'$ *et* $H(z,z') = z\overline{z}'$ *sont une paire comme dans la proposition précédente.*

Rappelons que le *symbole de Kronecker* $\delta_{i,j}$ vaut 1 lorsque $i=j$ et 0 sinon.

Lemme 2.2.6 (Frobenius)**.** *Soit* H *une forme de Riemann et* $E = \Im(H)$. *Alors il existe des entiers* $d_1, \dots, d_g \geq 0$ *avec* $d_i | d_{i+1}$ *et une base* $e_1, \dots, e_g$, $f_1, \dots, f_g$ *de* Λ *tels que*

$$E(e_i, e_j) = E(f_i, f_j) = 0 \qquad et \qquad E(e_i, f_j) = \delta_{i,j} d_i.$$

Une base qui vérifie cette propriété est dite symplectique. *Le produit* $\mathrm{Pf}(E) := d_1 \cdots d_g$, *appelé le* Pfaffien *de* E, *est la racine carrée du déterminant. Si on pose* $M = \mathrm{diag}(d_1, \dots, d_g)$, *alors la matrice* E *par rapport à cette base est* $\left(\begin{smallmatrix} 0 & M \\ -M & 0 \end{smallmatrix}\right)$.

Démonstration. Voir [39, Lemme A.5.3.1]. □

Il est clair que la forme H, et donc E, est non dégénérée si et seulement si $d_i > 0$ pour tout i de 1 à g.

2.2.2 Diviseurs et fonctions thêta

Changeons maintenant de point de vue et intéressons nous aux diviseurs sur une variété X.

Définition 2.2.7. *Un* diviseur de Cartier *sur une variété* X *est une classe d'équivalence de collections de paires* $\{(U_i, f_i)\}_{i\in I}$ *qui satisfont les conditions suivantes :*

— *Les* U_i *sont des ouverts qui forment un recouvrement de* X *;*

— *Les* f_i *sont des fonctions méromorphes non nulles sur* U_i *;*

— *Un quotient* f_i/f_j *est une fonction sans pôle et sans zéro sur* $U_i \cap U_j \neq \emptyset$ *;*

et où deux collections $\{(U_i, f_i)\}_{i\in I}$ *et* $\{(V_j, g_j)\}_{j\in J}$ *sont* équivalentes *lorsque, pour tous* $i \in I$ *et* $j \in J$, *la fonction* f_i/g_j *est sans pôle et sans zéro sur* $U_i \cap V_j$. *Deux collections équivalentes définissent alors le même diviseur.*

La *somme* de deux diviseurs de Cartier est

$$\{(U_i, f_i)\}_{i\in I} + \{(V_j, g_j)\}_{j\in J} := \{(U_i \cap V_j, f_i g_j)\}_{(i,j)\in I\times J}.$$

Muni de cette somme, l'ensemble des diviseurs de Cartier forme un groupe abélien que l'on note par $\mathrm{Div}(X)$: l'élément neutre, appelé aussi le *diviseur zéro*, étant $\{(X, 1_X)\}$ et l'inverse d'un diviseur $\{(U_i, f_i)\}_{i\in I}$ étant $\{(U_i, f_i^{-1})\}_{i\in I}$. Un diviseur D est dit *positif* ou *effectif* lorsqu'il peut être défini par une collection $\{(U_i, f_i)\}_{i\in I}$ avec des fonctions f_i qui sont holomorphes, pour tout $i \in I$. On notera ceci par $D \geq 0$. À une fonction $f \neq 0$ méromorphe sur X, on lui associe le diviseur $\mathrm{div}(f) := \{(X, f)\}$. Un tel diviseur est dit *principal* et on note par $\mathrm{Prin}(X)$ l'ensemble des diviseurs principaux. Deux diviseurs sont dit *linéairement équivalents* lorsque leur différence est un diviseur principal. Le groupe de *Picard* de X est $\mathrm{Pic}(X) := \mathrm{Div}(X)/\mathrm{Prin}(X)$, où on quotiente par la relation d'équivalence linéaire.

Définition 2.2.8. *Soit* $h : X_1 \to X_2$ *une application analytique complexe. Alors l'application*

$$\begin{array}{rccc} h^* : & \mathrm{Div}(X_2) & \longrightarrow & \mathrm{Div}(X_1) \\ & \{(U_i, f_i)\}_{i\in I} & \longmapsto & \{(h^{-1}(U_i), f_i \circ h)\}_{i\in I} \end{array}$$

est appelée le tiré en arrière *de* h.

Soit $X = V/\Lambda$ un tore complexe avec $V = \mathbb{C}^g$, $\pi : V \to X$ la projection naturelle et $t_a : x \in V \mapsto a+x \in V$ la translation par $a \in V$. Soit $D = \{(U_i, f_i)\}_{i\in I}$ un diviseur de X. Alors $D' = \pi^* D = \{(\pi^{-1}(U_i), f_i \circ \pi)\}_{i\in I}$ est un diviseur de V. Or, pour toute fonction méromorphe $f : X \to \mathbb{C}$, le tiré en arrière $\pi^* f : V \to \mathbb{C}$ vérifie $\pi^* f(v + \lambda) = \pi^* f(v)$, pour tous $\lambda \in \Lambda$ et $v \in V$. C'est donc une fonction Λ-périodique et on a alors que $t_\lambda^* D' = D'$ pour tout $\lambda \in \Lambda$. Le théorème de Cousin ([4, Lemme 2.1.1]) nous dit que D' est principal : il existe donc $f \in \mathbb{C}(V)$, l'ensemble des fonctions méromorphes sur V, tel que $D' = \mathrm{div}(f)$. L'invariance de D' par t_λ^* se traduit alors par $f(v + \lambda) = U_\lambda(v) f(v)$, pour tout $\lambda \in \Lambda$ et où U_λ est une fonction sans zéro ni pôle (d'après la notion d'équivalence des diviseurs). On appelle U_λ un *facteur d'automorphie* et on peut écrire $U_\lambda(v) = \exp(h_\lambda(v))$ pour une certaine fonction h_λ. Inversement, une fonction qui vérifie une telle équation définit un diviseur de X. Le théorème de Liouville implique que les fonctions entières périodiques pour $\lambda \in \Lambda$ sont constantes. Ceci conduit à la définition suivante qui nous permet d'étudier des fonctions assez "simples" et non constantes.

Définition 2.2.9. *Une fonction entière f sur $\mathbb{C}^g$ est une* fonction thêta *relativement au réseau Λ si elle satisfait une équation fonctionnelle du type*

$$f(z + \lambda) = \exp(g_\lambda(z)) f(z),$$

pour tout $\lambda \in \Lambda$, où $g_\lambda : \mathbb{C}^g \to \mathbb{C}$ vérifie $g_\lambda(z + z') + g_\lambda(0) = g_\lambda(z) + g_\lambda(z')$, pour tous $z, z' \in \mathbb{C}^g$. La fonction $\exp(g_\lambda(z))$ est appelée facteur d'automorphie de la fonction thêta.

Exemple 2.2.10. *Il n'est pas difficile de voir que la fonction σ_Λ de Weierstrass définie dans l'équation (1.6) est une fonction thêta. En effet, on a vu que la fonction $\wp_\Lambda$ est elliptique (c'est-à-dire Λ-périodique) et en intégrant deux fois puis en passant à l'exponentielle, on trouve que l'on a $\sigma_\Lambda(z+\lambda) = \exp(\eta(\lambda) + a(\lambda))\sigma_\Lambda(z)$, où $\eta(\lambda)$ et $a(\lambda)$ sont des constantes indépendantes de z (voir [75, Théorème 1.2.3]). Nous construirons plus tard des fonctions thêta en toute dimension.*

Théorème 2.2.11 (Poincaré)**.** *Soit D un diviseur effectif sur un tore complexe $X = V/\Lambda$. Alors il existe une fonction thêta entière par rapport à Λ qui représente ce diviseur.*

Démonstration. Voir [39, Théorème A.5.2.2]. □

Si on prend deux fonctions thêta qui représentent le même diviseur, alors il existe d'après [39, Lemme A.5.2.3] une forme quadratique Q, une forme linéaire R et une constante S telles que le quotient des deux fonctions thêta vaut $\exp(Q + R + S)$. Une fonction thêta de cette forme $\exp(Q + R + S)$ est dite une *fontion thêta triviale.*

Nous cherchons maintenant à associer à une fonction thêta une forme de Riemann. Notons pour simplifier $e(z) := \exp(2\imath\pi z)$. L'équation fonctionnelle d'une fonction thêta θ par rapport au réseau Λ peut être écrite comme

$$\theta(z + \lambda) = e(L(z, \lambda) + J(\lambda))\theta(z),$$

où $L(z, \lambda)$ est une fonction linéaire en z. À partir de cette équation et de la définition des fonctions thêta, on peut montrer que $L(z, \lambda)$ est $\mathbb{Z}$-linéaire en λ, et puisque $V = \Lambda \otimes \mathbb{R}$, on peut étendre $\mathbb{R}$-linéairement L en sa seconde variable pour obtenir une fonction $L : V \times V \to \mathbb{C}$, qui est donc $\mathbb{C}$-linéaire en sa première variable et $\mathbb{R}$-linéaire en la seconde.

Proposition 2.2.12. *Soit θ une fonction thêta par rapport à un réseau Λ, d'équation $\theta(z+\lambda) = e(L(z,\lambda) + J(\lambda))\theta(z)$. Alors en posant*

$$E(x,y) := L(x,y) - L(y,x) \qquad et \qquad H(x,y) := E(\imath x, y) + \imath E(x,y),$$

on obtient une forme de Riemann par rapport au réseau Λ. De plus, H ne dépend que du diviseur de θ, et si on note H_D la forme de Riemann associée au diviseur D, alors on a une loi d'addition $H_{D+D'} = H_D + H_{D'}$.

Démonstration. Voir [39, Proposition A.5.2.4]. □

Lemme 2.2.13. *Soit θ_0 une fonction thêta par rapport au réseau Λ et H sa forme de Riemann associée. Alors il existe une fonction thêta θ ayant les mêmes diviseur et forme de Riemann telle que*

$$\theta(z+\lambda) = \exp\left(\pi H(z,\lambda) + \frac{\pi}{2}H(\lambda,\lambda) + 2\imath\pi K(\lambda)\right)\theta(z),$$

où $K : \Lambda \to \mathbb{R}$ est une fonction qui vérifie

$$e(K(\lambda+\lambda')) = e(K(\lambda))e(K(\lambda'))e(\frac{1}{2}E(\lambda,\lambda')).$$

Démonstration. Voir [39, Proposition A.5.2.6]. □

Proposition 2.2.14. *La forme de Riemann associée à une fonction thêta est positive.*

Démonstration. Voir [39, Proposition A.5.2.5]. □

Soit θ une fonction thêta ayant pour diviseur D pour un réseau Λ dans $V = \mathbb{C}^g$. Notons $L(\theta)$ l'espace vectoriel de toutes les fonctions thêta ayant la même équation fonctionnelle. Le lemme suivant nous dit que cet espace vectoriel est de dimension finie. Notons $\ell(\theta)$ cette dimension.

Lemme 2.2.15. *Soit θ une fonction thêta et H sa forme de Riemann, que l'on suppose définie positive, par rapport au réseau $\Lambda \subseteq V = \mathbb{C}^g$. Soit $\{e_1, \ldots, e_g, f_1 \ldots, f_g\}$ une base symplectique de $E = \Im(H)$ sur Λ et $d_1, \ldots, d_g$ les entiers associés (comme dans le lemme 2.2.6).*

- *Les ensembles $\{e_1, \ldots, e_g\}$ et $\{f_1, \ldots, f_g\}$ forment des $\mathbb{C}$-bases de V ;*
- *Après multiplication par une certaine fonction thêta triviale, l'équation fonctionnelle de θ avec $z = \sum z_i e_i$ est de la forme*

$$\theta(z+e_i) = \theta(z) \qquad et \qquad \theta(z+f_i) = e(d_i z_i + c_i)\theta(z),$$

  où $c_i \in \mathbb{C}$;
- $\ell(\theta) = \mathrm{Pf}(E)$.

Démonstration. Voir [39, Lemme A.5.3.2 et Théorème A.5.3.3]. □

Soit $\theta_1, \ldots, \theta_{\ell(\theta)}$ une base de $L(\theta)$. On a l'application holomorphe :

$$\begin{array}{rccc} \phi_D : & V/\Lambda & \longrightarrow & \mathbb{P}^n(\mathbb{C}) \\ & z & \longmapsto & (\theta_1(z), \ldots, \theta_{\ell(\theta)}(z)). \end{array}$$

Définition 2.2.16. *Un diviseur D d'un tore V/Λ est dit* très ample *si l'application ϕ_D ci-dessus est un plongement. Le diviseur D est dit* ample *lorsqu'un multiple positif de D est* très ample.

Théorème 2.2.17. *Soit D un diviseur effectif d'un tore. La forme de Riemann associée à D est définie positive si et seulement si D est ample.*

Démonstration. Voir [39, Théorème A.5.2.7]. □

Le théorème de Chow nous dit que toute variété analytique complexe dans un espace projectif est algébrique. Ainsi, un tore est une variété abélienne si et seulement s'il peut être plongé dans un espace projectif, si et seulement s'il admet une forme de Riemann définie positive et si et seulement s'il contient un diviseur ample.

2.3 Diviseurs du groupe de Picard

2.3.1 Théorème d'Appell-Humbert

Soit $X = V/\Lambda$ un tore. Le groupe de Néron-Severi $\mathrm{NS}(X)$ est le groupe des formes de Riemann sur X. On pose $\mathbb{C}_1 := \{z \in \mathbb{C} : |z| = 1\}$. Un *semi-caractère* pour une forme de Riemann H est une application $\chi : \Lambda \to \mathbb{C}_1$ telle que, pour tous $\lambda, \lambda' \in \Lambda$,

$$\chi(\lambda + \lambda') = \chi(\lambda)\chi(\lambda') \exp\left(\imath\pi\Im(H(\lambda, \lambda'))\right).$$

Un caractère étant un morphisme multiplicatif, la définition de semi-caractère nous dit que les caractères sur Λ à valeur dans $\mathbb{C}_1$ sont exactement les semi-caractères pour $0 \in \mathrm{NS}(X)$. Notons maintenant $\mathcal{P}(\Lambda)$ l'ensemble des paires (H, χ) pour $H \in \mathrm{NS}(X)$ et χ un semi-caractère pour H. C'est un groupe pour l'opération

$$(H_1, \chi_1) \otimes (H_2, \chi_2) = (H_1 + H_2, \chi_1\chi_2) \tag{2.3}$$

et la suite suivante est exacte

$$1 \longrightarrow \mathrm{Hom}(\Lambda, \mathbb{C}_1) \xrightarrow{\iota} \mathcal{P}(\Lambda) \xrightarrow{p} \mathrm{NS}(X) \longrightarrow 0$$

où on a posé $\iota(\chi) = (0, \chi)$ et $p(H, \chi) = H$. Il n'y a que la surjectivité de p qui n'est pas évidente. Pour la montrer, il faut tout d'abord considérer l'application qui à un couple (H, χ) de $\mathcal{P}(\Lambda)$ associe la fonction $a_{(H,\chi)} : \Lambda \times V \to \mathbb{C}^*$ définie par

$$a_{(H,\chi)}(\lambda, v) = \chi(\lambda) \exp\left(\pi H(v, \lambda) + \frac{\pi}{2} H(\lambda, \lambda)\right).$$

On peut rapprocher une telle fonction de la fonction θ du lemme 2.2.13, où la fonction $e(K)$ est un semi-caractère. On peut montrer (voir [4, Page 30]) que la fonction $a_{(H,\chi)}$ détermine uniquement un diviseur D du groupe de Picard $\mathrm{Pic}(X)$. On écrira dans la suite $D = L(H, \chi)$ et pour un tel D, on dit de $a_D = a_{(H,\chi)}$ que c'est un *facteur d'automorphie canonique* pour D. L'application c qui à tout (H, χ) associe $L(H, \chi)$ est un morphisme de groupe. Considérons l'application $c_1 : \mathrm{Pic}(X) \to \mathrm{NS}(X)$ qui à tout diviseur D associe H tel que $D = L(H, \chi)$. On a alors $p = c_1 \circ c$.

Posons $\mathrm{Pic}^0(X)$ le noyau de c_1. À tout semi-caractère $\chi \in \mathrm{Hom}(\Lambda, \mathbb{C}_1)$, on peut associer le diviseur $L(0, \chi) \in \mathrm{Pic}^0(X)$. Cette application est un isomorphisme de groupes. Tout ces résultats se résument dans le théorème fondamental suivant :

Théorème 2.3.1 (Appell-Humbert)**.** *Soit $X = V/\Lambda$ un tore complexe. Il y a un isomorphisme canonique de suites exactes :*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(\Lambda, \mathbb{C}_1) & \longrightarrow & \mathcal{P}(\Lambda) & \longrightarrow & \mathrm{NS}(X) & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq & & \\ 1 & \longrightarrow & \mathrm{Pic}^0(X) & \longrightarrow & \mathrm{Pic}(X) & \longrightarrow & \mathrm{NS}(X) & \longrightarrow & 0 \end{array}$$

Démonstration. Voir [4, Théorème 2.2.3]. □

Soit $\widehat{V} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$ l'ensemble des formes antilinéaires de V vers $\mathbb{C}$. L'ensemble

$$\widehat{\Lambda} = \{f \in \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) : \Im(f(\Lambda)) \subseteq \mathbb{Z}\}$$

est un réseau dans $\widehat{V}$ et le quotient $\widehat{V}/\widehat{\Lambda}$ est un tore complexe de dimension g, appelé *tore complexe dual* de X. Rappelons que nous notons $e(z) := \exp(2\imath\pi z)$. L'homomorphisme $\widehat{V} \to \mathrm{Hom}(\Lambda, \mathbb{C}_1)$ qui à f associe $e(\Im(f(.)))$ induit un isomorphisme entre $\widehat{V}/\widehat{\Lambda}$ et $\mathrm{Pic}^0(X)$ ([4, Proposition 2.4.1]).

Soient $X_i = V_i/\Lambda_i$, pour $i = 1, 2, 3$, trois tores complexes et $f : X_1 \to X_2$ un homomorphisme avec représentation analytique $F : V_1 \to V_2$. L'application $F^* : G \in \widehat{V}_2 \to G \circ F \in \widehat{V}_1$ induit un homomorphisme $\widehat{f} : \widehat{X}_2 \to \widehat{X}_1$, puisque $F^*\widehat{\Lambda}_2 \subseteq \widehat{\Lambda}_1$. On a certaines propriétés évidentes comme $\widehat{\mathrm{id}_X} = \mathrm{id}_{\widehat{X}}$, $\widehat{\widehat{f}} = f$. Si $h : X_2 \to X_3$ est un autre homomorphisme, alors $\widehat{hf} = \widehat{f}\,\widehat{h}$ et si de plus la suite $0 \to X_1 \to X_2 \to X_3 \to 0$ est exacte, alors $0 \to \widehat{X}_3 \to \widehat{X}_2 \to \widehat{X}_1 \to 0$ l'est également ([4, Proposition 2.4.2]).

Proposition 2.3.2. *Si $f : X_1 \to X_2$ est une isogénie de tores complexes, alors l'application duale $\widehat{f} : \widehat{X}_2 \to \widehat{X}_1$ est aussi une isogénie et son noyau est isomorphe à* $\mathrm{Hom}(\ker(f), \mathbb{C}_1)$*. En particulier,* $\deg \widehat{f} = \deg f$*. On appelle cette isogénie* l'isogénie duale *de f.*

Démonstration. Voir [4, Proposition 2.4.3]. Supposons $X_i = V/\Lambda_i$ et que la représentation analytique de f est Id_V. Par définition, $\mathrm{Id}_{\widehat{V}}$ est la représentation analytique de $\widehat{f}$ et donc $\widehat{f}$ est une isogénie. Par l'isomorphisme $\widehat{X} \simeq \mathrm{Pic}^0(X)$, le diagramme suivant commute

$$\begin{array}{ccc} \widehat{X}_2 & \xrightarrow{\sim} & \mathrm{Pic}^0(X_2) \\ \downarrow \widehat{f} & & \downarrow f^* \\ \widehat{X}_1 & \xrightarrow{\sim} & \mathrm{Pic}^0(X_1) \end{array}$$

et si on ajoute à ceci le théorème d'Appell-Humbert, on a que

$$\ker \widehat{f} \simeq \ker(\mathrm{Hom}(\Lambda_2, \mathbb{C}_1) \to \mathrm{Hom}(\Lambda_1, \mathbb{C}_1)) \simeq \mathrm{Hom}(\Lambda_2/\Lambda_1, \mathbb{C}_1).$$

On déduit la proposition du fait que $\ker f \simeq \Lambda_2/\Lambda_1$. □

Lemme 2.3.3. *Pour chaque $D = L(H, \chi) \in \mathrm{Pic}(X)$ et $\overline{v} \in X$ avec $v \in V$ pour représentant, on a, en notant $E = \Im(H)$,*

$$t_{\overline{v}}^* L(H, \chi) = L(H, \chi e(E(v, .))).$$

Démonstration. Voir [4, Lemme 2.3.2]. □

Lemme 2.3.4. *Soit $f : X_1 \to X_2$ un homomorphisme. Pour tout $L(H,\chi) \in \mathrm{Pic}(X_2)$,*

$$f^*L(H,\chi) = L(\rho_a(f)^*H, \rho_r(f)^*\chi),$$

où $\rho_a(f)^*H$ désigne $H(\rho_a(f), \rho_a(f))$.

Démonstration. Voir [4, Lemme 2.3.4]. □

Soient $D = L(H,\chi) \in \mathrm{Pic}(X)$ et $x \in X$. Alors par le lemme 2.3.3 et l'équation (2.3), le diviseur

$$t_x^*D \otimes D^{-1} = L(H, \chi e(E(x,.))) \otimes L(-H, \chi^{-1}) = L(0, e(E(x,.)))$$

est dans $\mathrm{Pic}^0(X)$. L'application

$$\begin{array}{rccc} \phi_D : & X & \longrightarrow & \widehat{X} \simeq \mathrm{Pic}^0(X) \\ & x & \longmapsto & t_x^*D \otimes D^{-1} \end{array}$$

est un homomorphisme d'après [4, Théorème 2.3.3].

Lemme 2.3.5. *Soit $D = L(H,\chi) \in \mathrm{Pic}(X)$. L'application*

$$\begin{array}{rccc} \phi_H : & V & \longrightarrow & \widehat{V} \\ & v & \longmapsto & H(v,.) \end{array}$$

est la représentation analytique de ϕ_D.

Démonstration. Voir [4, Lemme 2.4.5]. □

Corollaire 2.3.6. *Soit $f : X_1 \to X_2$ une isogénie de tores complexes ayant représentation analytique F. Pour un diviseur $D = L(H,\chi) \in \mathrm{Pic}(X_1)$, on a l'équivalence :*

1. *$D = f^*D'$ pour un certain $D' \in \mathrm{Pic}(X_2)$;*
2. *$\Im(H(F^{-1}\Lambda_2, F^{-1}\Lambda_1)) \subseteq \mathbb{Z}$.*

Démonstration. Voir [4, Corollaire 2.4.4]. □

Corollaire 2.3.7.

1. *ϕ_D ne dépend que de H ;*
2. *$\phi_{D\otimes D'} = \phi_D + \phi_{D'}$ pour tous $D, D' \in \mathrm{Pic}(X)$;*
3. *$\widehat{\phi_D} = \phi_D$ sous l'identification naturelle $\widehat{\widehat{X}} = X$;*
4. *Pour tout homomorphisme $f : Y \to X$ de tores complexes, le diagramme suivant commute :*

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ {\scriptstyle \phi_{f^*D}}\downarrow & & \downarrow{\scriptstyle \phi_D} \\ \widehat{Y} & \xleftarrow[\widehat{f}]{} & \widehat{X} \end{array}$$

Démonstration. Voir [4, Corollaire 2.4.6]. Seule la preuve du troisième point peut poser problème. Mais puisque ϕ_H^* est la représentation analytique de $\widehat{\phi_D}$, la proposition se déduit du fait que, sous l'identification $\mathrm{Hom}_{\overline{\mathbb{C}}}(\widehat{V}, \mathbb{C}) = V$, on a $\phi_H^* = \phi_H$. □

L'homomorphisme ϕ_D associé à $D = L(H, \chi)$ est une isogénie si et seulement si H est non dégénéré (si c'est une isogénie, alors ϕ_H est un isomorphisme et donc H et non dégénérée ; et réciproquement, si H est non dégénérée, alors ϕ_H est injective ; on conclut avec le fait que V et $\widehat{V}$ sont de même dimension). On dira donc d'un diviseur du groupe de Picard qu'il est non dégénéré lorsque la forme Hermitienne lui correspondant l'est. Ainsi, un tel diviseur D est non dégénéré si et seulement si le noyau $K(D)$ de ϕ_D est fini. Le degré de ϕ_D est $\det \Im(H)$, d'après [4, Proposition 2.4.9].

On peut se demander sous quelle condition un homomorphisme d'un tore vers son dual est de la forme ϕ_D. Le théorème suivant répond à cette question.

Théorème 2.3.8. *Soit $X = V/\Lambda$ un tore complexe et $f : X \to \widehat{X}$ un homomorphisme avec pour représentation analytique $F : V \to \widehat{V}$. On a l'équivalence*

1. *$f = \phi_D$ pour $D \in \mathrm{Pic}(X)$;*
2. *La forme $F : (x, y) \in V \times V \mapsto F(x)(y) \in \mathbb{C}$ est hermitienne.*

Démonstration. Voir [4, Théorème 2.5.5]. □

2.3.2 Polarisation

Soit $X = V/\Lambda$ un tore complexe. Une *polarisation* sur X est une forme de Riemann définie positive H qui provient d'un diviseur $D = L(H, \chi) \in \mathrm{Pic}(X)$. Par abus de notation, on dira parfois que D est une polarisation. Le *type de la polarisation* est le type de H, c'est-à-dire $\mathrm{diag}(d_1, \ldots, d_g)$ comme dans le lemme 2.2.6. On définit le *degré de la polarisation* comme étant le produit $d_1 \cdots d_g$. Une polarisation est dite *principale* si elle est de type $(1, \ldots, 1)$, ce qui est équivalent à dire qu'elle est de degré 1. Puisque H est définie positive, ϕ_D est une isogénie et elle est de degré 1 si la polarisation est principale. On a alors un isomorphisme $\phi_D : X \to \widehat{X}$.

D'après le théorème 2.2.17, une variété abélienne est un tore complexe ayant une polarisation. La paire (X, H) est appelée *variété abélienne polarisée*. On notera parfois (X, D) au lieu de (X, H).

Nous avons vu qu'une polarisation D définit une isogénie $\phi_D : X \to \widehat{X}$ et qu'inversement (théorème 2.3.8), une isogénie $\phi : X \to \widehat{X}$ est de la forme ϕ_D pour une certaine polarisation D lorsque la forme provenant de la représentation analytique de ϕ est hermitienne et définie positive. Ainsi, certains auteurs préfèrent définir une polarisation comme étant une isogénie de $X \to \widehat{X}$ de la forme ϕ_D.

Définition 2.3.9. *Un homomorphisme de variétés abéliennes polarisées*

$$f : (X_1, H_1) \longrightarrow (X_2, H_2)$$

est un homomorphisme de tores complexes $f : X_1 \to X_2$ tel que $f^* H_2 = H_1$.

Notons que f est forcément de noyau fini. Inversement, si $f : X_1 \to X_2$ est un homomorphisme de tores complexes de noyau fini et que D_2 est une polarisation sur X_2, alors $D_1 := f^* D_2$ est une polarisation sur X_1, appelée *polarisation induite*. Ceci prouve que d'une part, un sous-tore d'une variété abélienne est une variété abélienne et d'autre part qu'un tore complexe isogène à une variété abélienne est une variété abélienne. En particulier, si $\widehat{X}$ est le tore dual d'une variété abélienne X, alors ce tore dual est aussi une variété abélienne, appelée *variété abélienne duale* (voir [4, Page 70]).

D'après le corollaire 2.3.7, un homomorphisme $f : X_1 \to X_2$ de tores complexes polarisés en D_1 et D_2 respecte les polarisations, c'est-à-dire que $D_1 = f^*D_2$, si et seulement si le diagramme suivant commute :

$$\begin{array}{ccc} X_1 & \xrightarrow{f} & X_2 \\ {\scriptstyle \phi_{D_1}}\downarrow & & \downarrow{\scriptstyle \phi_{D_2}} \\ \widehat{X}_1 & \xleftarrow[\widehat{f}]{} & \widehat{X}_2 \end{array}$$

Proposition 2.3.10. *Une variété abélienne polarisée est isogène à une variété abélienne principalement polarisée.*

Démonstration. Voir [4, Proposition 4.1.2]. □

Nous avons vu précédemment qu'un tore complexe est une variété abélienne lorsqu'il admet une forme de Riemann définie positive. Nous donnons une autre formulation de ce critère.

Théorème 2.3.11 (Relations de Riemann)**.** *Soit $X = \mathbb{C}^g/\Pi\mathbb{Z}^{2g}$ un tore complexe, où Π est une matrice des périodes. Alors X est une variété abélienne si et seulement s'il existe une matrice alternée et non dégénéré $A \in M_{2g}(\mathbb{Z})$ telle que :*

1. $\Pi A^{-1}\,{}^t\Pi = 0$;
2. $\imath\Pi A^{-1}\,{}^t\overline{\Pi} > 0$.

Démonstration. Voir [4, Théorème 4.2.1]. □

Ces deux relations sont appelées *relations de Riemann*. D'après [4, Lemme 4.2.2 et Lemme 4.2.3], en prenant E la forme bilinéaire alterné non dégénérée ayant pour matrice A et en posant $H(x, y) := E(\imath x, y) + \imath E(x, y)$, on a que H est une forme hermitienne si la première condition est vérifiée, et cette forme hermitienne est définie positive lorsque c'est la seconde qui l'est. De plus, si, comme dans le théorème, A est à coefficients entiers, alors on a bien que H est une forme de Riemann définie positive. C'est une polarisation pour le tore X, qui est donc bien une variété abélienne.

2.4 Endomorphismes

Soit $X = V/\Lambda$ une variété abélienne et $D = L(H, \chi)$ une polarisation. Nous avons vu que cette polarisation induit une isogénie $\phi_D : X \to \widehat{X}$. Notons d son degré. La proposition 2.1.6 nous dit qu'il existe une unique isogénie ψ_D de degré d telle que $\psi_D \circ \phi_D = [d]_X$ et $\phi_D \circ \psi_D = [d]_{\widehat{X}}$. Ainsi, $\frac{1}{d}\psi_D$ est l'inverse de ϕ_D dans $\mathrm{Hom}_{\mathbb{Q}}(\widehat{X}, X)$. D'autre part, tout $f \in \mathrm{End}_{\mathbb{Q}}(X)$ peut être écrit de la forme rh avec $h \in \mathrm{End}(X)$ et $r \in \mathbb{Q}$. Le dual d'un tel f est défini comme étant $\widehat{f} := r\widehat{h} \in \mathrm{End}_{\mathbb{Q}}(\widehat{X})$.

Définition 2.4.1. *L'application*

$$\begin{array}{rccc} {}' : & \mathrm{End}_{\mathbb{Q}}(X) & \longrightarrow & \mathrm{End}_{\mathbb{Q}}(X) \\ & f & \longmapsto & f' = \phi_D^{-1}\widehat{f}\phi_D \end{array}$$

est appelée involution de Rosati *par rapport à la polarisation D.*

C'est bien une involution car $f'' = (\phi_D^{-1}\hat{f}\phi_D)' = \phi_D^{-1}\widehat{\phi_D}f\widehat{\phi_D^{-1}}\phi_D = f$ car $\hat{\hat{f}} = f$, $\widehat{fg} = \hat{g}\hat{f}$ et $\widehat{\phi_D} = \phi_D$ (corollaire 2.3.7). On peut vérifier que l'on a de plus que $(rf + sg)' = rf' + sg'$ et $(fg)' = g'f'$ pour tous $f, g \in \mathrm{End}_{\mathbb{Q}}(X)$ et $r, s \in \mathbb{Q}$.

Proposition 2.4.2. *L'involution de Rosati est l'opérateur adjoint de la forme hermitienne H, où $D = L(H, \chi)$, et aussi de la forme alternée E associée à H. Ceci signifie que l'on a pour $f \in \mathrm{End}_{\mathbb{Q}}(X)$:*

1. *$H(\rho_a(f)(x), y) = H(x, \rho_a(f')(y))$ pour tous $x, y \in V$;*
2. *$E(\rho_r(f)(x), y) = E(x, \rho_r(f')(y))$ pour tous $x, y \in \Lambda$.*

Démonstration. Voir [4, Proposition 5.1.1]. □

Pour tout $f \in \mathrm{End}_{\mathbb{Q}}(X)$, le polynôme caractéristique P_f^r de la représentation rationnelle $\rho_r(f)$ est $P_f^r(t) = \det(t\,\mathrm{Id}_\Lambda - \rho_r(f)) = \sum_{i=0}^{2g}(-1)^i r_i t^{2g-i}$, où les r_i sont rationnels. Notons $\mathrm{Tr}_r(f)$ le coefficient r_1, appelé *trace rationnelle de f*.

Théorème 2.4.3. *L'application $(f, g) \mapsto \mathrm{Tr}_r(f'g)$ est une forme bilinéaire symétrique définie positive sur le $\mathbb{Q}$-espace vectoriel $\mathrm{End}_{\mathbb{Q}}(X)$.*

Démonstration. Voir [4, Théorème 5.1.8]. □

Corollaire 2.4.4. *Le groupe des automorphismes d'une variété abélienne polarisée est fini.*

Démonstration. Voir [4, Corollaire 5.1.9] □

D'après [4, Corollaire 5.1.10], si f est un automorphisme d'une variété abélienne polarisée (X, D) et si $n \geq 3$ est un entier, alors il suffit que la restriction de f au sous-groupe de torsion $X[n]$ soit l'identité pour que f soit la fonction identité. Ceci induit un plongement :

$$\mathrm{Aut}(X, L) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X[n]) = \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

(pour $n \geq 3$) qui donne une majoration pour l'ordre du groupe des automorphismes.

Un élément $f \in \mathrm{End}_{\mathbb{Q}}(X)$ est dit *symétrique*, par rapport à une polarisation, s'il vérifie $f' = f$. Notons $\mathrm{End}^s(X)$ (resp. $\mathrm{End}^s_{\mathbb{Q}}(X)$) le sous-ensemble de $\mathrm{End}(X)$ (resp. $\mathrm{End}\,\mathbb{Q}(X)$) contenant les éléments symétriques. $\mathrm{End}^s(X)$ est un groupe additif tandis que $\mathrm{End}^s_{\mathbb{Q}}(X)$ est un $\mathbb{Q}$-espace vectoriel isomorphe à $\mathrm{End}^s(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 2.4.5. *Soit D_0 une polarisation sur X. L'application*

$$D \in \mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{Q} \longmapsto \phi_{D_0}^{-1}\phi_D \in \mathrm{End}^s_{\mathbb{Q}}(X)$$

est un isomorphisme de $\mathbb{Q}$-espaces vectoriels. De plus, si D_0 est principale, alors cette application induit un isomorphisme de groupes entre $\mathrm{NS}(X)$ et $\mathrm{End}^s(X)$.

Démonstration. Voir [4, Proposition 5.2.1] □

Une variété abélienne est dite *simple* si elle ne contient pas d'autres variétés abéliennes si ce n'est 0 et elle-même.

Théorème 2.4.6 (Réductibilité complète de Poincaré)**.** *Pour toute variété abélienne X, il existe une isogénie*

$$X \to X_1^{n_1} \times \ldots \times X_r^{n_r},$$

où les X_i sont des variétés abéliennes simples non isogènes entre elles. Ces variétés, ainsi que les exposants n_i, sont déterminées uniquement à isogénie et permutation près.

Démonstration. Voir [4, Théorème 5.3.7] □

Corollaire 2.4.7. $\mathrm{End}_{\mathbb{Q}}(X)$ *est une $\mathbb{Q}$-algèbre semi-simple. Ceci signifie que si X est isogène à $X_1^{n_1} \times \ldots \times X_r^{n_r}$ comme dans le théorème précédent, alors*

$$\mathrm{End}_{\mathbb{Q}}(X) \simeq M_{n_1}(\mathrm{End}_{\mathbb{Q}}(X_1)) \oplus \ldots \oplus M_{n_r}(\mathrm{End}_{\mathbb{Q}}(X_r))$$

et les $\mathrm{End}_{\mathbb{Q}}(X_i)$ *sont des corps gauches de dimension finie sur $\mathbb{Q}$.*

Démonstration. Voir [4, Corollaire 5.3.8]. On peut supposer sans perte de généralité que $X = X_1^{n_1} \times \ldots \times X_r^{n_r}$. Or, puisque $\mathrm{Hom}(X_i^{n_i}, X_j^{n_j}) = 0$ pour $i \neq j$, on obtient l'égalité $\mathrm{End}_{\mathbb{Q}}(X) = \bigoplus_{i=1}^{r} \mathrm{End}_{\mathbb{Q}}(X_i^{n_i})$ et l'anneau $\mathrm{End}_{\mathbb{Q}}(X_i^{n_i})$ est égal à l'anneau des matrices $n_i \times n_i$ prenant des valeurs dans $\mathrm{End}_{\mathbb{Q}}(X_i)$. Pour une variété abélienne simple X_i, tous les endomorphismes non nuls sont des isogénies et sont donc inversibles dans $\mathrm{End}_{\mathbb{Q}}(X_i)$. Ceci prouve que $\mathrm{End}_{\mathbb{Q}}(X_i)$ est un corps gauche sur $\mathbb{Q}$. Il est de dimension finie d'après la proposition 2.1.2. □

Corollaire 2.4.8. *Pour toute variété abélienne X, le groupe de Néron-Severi* $\mathrm{NS}(X)$ *est un groupe abélien libre de rang fini.*

Démonstration. Voir [4, Corollaire 5.3.9] □

Soit (X, D) une variété abélienne simple de dimension g. On a vu que $\mathrm{End}_{\mathbb{Q}}(X)$ est un corps gauche de dimension finie sur $\mathbb{Q}$ muni d'une involution $x \mapsto x'$ qui est l'involution de Rosati par rapport à D. Soit K le centre de $\mathrm{End}_{\mathbb{Q}}(X)$. On peut montrer que son indice dans $\mathrm{End}_{\mathbb{Q}}(X)$ est toujours un carré. Soit K_0 le sous-corps de K des éléments fixés par l'involution. C'est un corps de nombres totalement réel ([4, Lemme 5.5.2]). Notons

$$[\mathrm{End}_{\mathbb{Q}}(X) : K] = d^2, \quad [K : \mathbb{Q}] = e, \quad [K_0 : \mathbb{Q}] = e_0 \quad \text{et} \quad \mathrm{rang}(\mathrm{NS}(X)) = \varrho.$$

Le couple $(\mathrm{End}_{\mathbb{Q}}, ')$ est dit du *premier type* si $K = K_0$, c'est-à-dire si l'involution est triviale sur tout K. Si ce n'est pas le cas, on dit de ce couple qu'il est du *second type*. On a alors :

Proposition 2.4.9.

$\mathrm{End}_{\mathbb{Q}}(X)$	d	e_0	ϱ	*restriction*
Corps de nombres totalement réel	1	e	e	$e \mid g$
Algèbre de quaternions totalement indéfinie	2	e	$3e$	$2e \mid g$
Algèbre de quaternions totalement définie	2	e	e	$2e \mid g$
$(\mathrm{End}_{\mathbb{Q}}, ')$ *du second type*	d	$\frac{1}{2}e$	$e_0 d^2$	$e_0 d^2 \mid g$

Démonstration. Voir [4, Proposition 5.5.7]. □

Soit X une variété abélienne. Pour tout entier N, il existe une application naturelle $X[N] \times \widehat{X}[N] \to \mu_N$, où μ_N désigne l'ensemble des racines N-ièmes de l'unité ([67, Page 183]). Une polarisation H sur X permet alors d'en déduire un couplage $e_H : X[N] \times X[N] \to \mu_N$. C'est une généralisation du couplage de Weil sur les courbes elliptiques et nous parlerons donc dans la suite de couplage de Weil associé à une polarisation.

Définition 2.4.10. *Soient (X, H_1) et (Y, H_2) deux variétés abéliennes principalement polarisées et soit $f : X \to Y$ une isogénie de degré ℓ^2, pour ℓ un nombre premier. On dit que f est une ℓ-isogénie lorsque le diagramme suivant commute :*

$$\begin{array}{ccccc} & & X & \xrightarrow{f} & Y \\ & \swarrow^{[\ell]} & \downarrow{\scriptstyle \phi_{\ell H_1}} & & \downarrow{\scriptstyle \phi_{H_2}} \\ X & \xrightarrow[\phi_{H_1}]{} & \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{Y} \end{array}$$

Dans ce cas, $\ker f \subseteq \ker \phi_{\ell H_1}$ est isotrope maximal pour le couplage de Weil issu de ℓH_1. Réciproquement, soient H une polarisation sur X et $K \subseteq \ker \phi_H$ isotrope maximal pour e_H. Alors il existe une polarisation H_2 sur X/K qui est principale et telle que $f^* H_2 = H$ (voir [66, 18]). Si ℓ est premier, alors f est une ℓ-isogénie si et seulement si $K = \ker f \subseteq X[\ell]$ est isotrope maximal pour $e_{\ell H_1}$. De plus, on a $K \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ ce qui fait que plusieurs auteurs parlent de (ℓ, ℓ)-isogénie. Nous avons choisi dans cette thèse de garder la dénomination ℓ-isogénie pour être cohérent avec la notion qui suit.

Définition 2.4.11. *Soient (X, H_1) et (Y, H_2) deux variétés abéliennes principalement polarisées de dimension 2 et soit $f : X \to Y$ une isogénie de degré ℓ, pour ℓ un nombre premier. Supposons qu'il existe $i : K_0 \to \mathrm{End}^{\mathrm{s}}_{\mathbb{Q}}(X)$, où K_0 est un corps de nombres quadratique totalement réel et que $\ell = \beta\overline{\beta}$ dans K_0 avec β totalement réel totalement positif. On dit que f est une β-isogénie lorsque le diagramme suivant commute :*

$$\begin{array}{ccccc} & & X & \xrightarrow{f} & Y \\ & \swarrow^{\beta} & \downarrow{\scriptstyle \phi_{\beta H_1}} & & \downarrow{\scriptstyle \phi_{H_2}} \\ X & \xrightarrow[\phi_{H_1}]{} & \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{Y} \end{array}$$

où $\beta H_1(x, y) := H_1(\beta x, y) = H_1(x, \beta y)$.

Dans ce cas, $\ker f \subseteq X[\beta]$ est un sous-groupe cyclique qui est alors isotrope maximal pour $e_{\beta H_1}$. Réciproquement, soient β totalement réel totalement positif de norme ℓ et K isotrope maximal dans $X[\beta]$ pour $e_{\beta H_1}$, alors il existe une polarisation principale H_2 sur X/K telle que le diagramme de la définition précédente commute (voir [18]).

2.5 Espaces de modules

Nous avons vu qu'à un tore complexe on peut associer plusieurs matrices des périodes, selon les bases que l'on choisit. Nous décrivons dans cette section un critère permettant de dire si deux matrices des périodes différentes proviennent de la même variété abélienne ou pas. D'autre part, nous allons faire la même chose avec des variétés abéliennes qui ont un certain type d'anneau d'endomorphismes.

2.5.1 Espace de Siegel et matrices symplectiques

Soit $X = V/\Lambda$ un tore complexe de dimension g et H une forme de Riemann qui définit une polarisation de type $D = \mathrm{diag}(d_1, \ldots, d_g)$. Soient $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ une base symplectique de Λ pour H. La forme alternée E qui correspond à H est donnée par la matrice $\left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)$ par rapport à cette base.

Posons maintenant $e_i = \frac{1}{d_i}\mu_i$ pour $i = 1, \ldots, g$. D'après le lemme 2.2.15, les vecteurs e_i forment une $\mathbb{C}$-base de V. Par rapport aux bases $e_1, \ldots, e_g$ et $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$, la matrice des périodes de X est de la forme $\Pi = (\Omega, D)$ pour un certain $\Omega \in M_g(\mathbb{C})$. On peut être plus précis et utiliser les relations de Riemann (théorème 2.3.11) pour trouver qu'en fait Ω est une matrice symétrique dont la partie imaginaire est définie positive et que $\Im(\Omega)^{-1}$ est la matrice de la forme hermitienne H par rapport à la base $e_1, \ldots, e_g$. Ceci conduit à la définition suivante.

Définition 2.5.1. *Le* demi-espace supérieur de Siegel $\mathcal{H}_g$ *de dimension* g *est l'ensemble*

$$\mathcal{H}_g := \{\Omega \in M_g(\mathbb{C}) : {}^t\Omega = \Omega,\ \Im(\Omega) > 0\}.$$

L'espace de Siegel est une sous-variété ouverte de dimension $\frac{1}{2}g(g+1)$ sur l'espace vectoriel des matrices symétriques de $M_g(\mathbb{C})$. On appelle *variété abélienne polarisée de type* D *avec base symplectique* un triplet de la forme

$$(X, H, \{\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g\}),$$

avec $X = V/\Lambda$ une variété abélienne, H une polarisation de type D et les λ_i et μ_i une base symplectique de Λ pour H.

Proposition 2.5.2. *Soit* D *un type. L'espace de Siegel* $\mathcal{H}_g$ *est un espace de modules (grossier) pour les variétés abéliennes polarisées de type* D *avec base symplectique.*

Démonstration. Voir [4, Section 8.1]. On a vu déjà que d'un tel triplet on peut en déduire un point $\Omega \in \mathcal{H}_g$. Réciproquement, soient D un type et $\Omega \in \mathcal{H}_g$. On pose alors $\Lambda_\Omega := (\Omega, D)\mathbb{Z}^{2g}$; c'est un réseau de $V = \mathbb{C}^g$ et $X_\Omega := V/\Lambda_\Omega$ est un tore complexe. On définit la forme hermitienne H_Ω qui s'écrit matriciellement $\Im(\Omega)^{-1}$ par rapport à la base standard de $\mathbb{C}^g$. Par définition de l'espace de Siegel, cette forme est définie positive. Considérons maintenant l'isomorphisme $\mathbb{R}$-linéaire de $\mathbb{R}^{2g}$ vers $\mathbb{C}^g$ défini par la matrice $(\Omega, D) \in M_{g\times 2g}(\mathbb{C})$. Soient $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ les images dans $\mathbb{C}^g$ des éléments de la base standard de $\mathbb{R}^{2g}$. Par définition, ces éléments forment une base de Λ_Ω. Par rapport à cette base, $\Im(H_\Omega|(\Lambda_\Omega \times \Lambda_\Omega))$ est donnée par la matrice

$$\Im({}^t(\Omega, D)(\Im(\Omega))^{-1}\overline{(\Omega, D)}) = \left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right).$$

On a donc montré que H_Ω est une polarisation de type D sur X_Ω. □

On cherche maintenant à se débarrasser de la base symplectique, c'est-à-dire à se rendre indépendant du choix de la base pour l'écriture de la matrice des périodes. En d'autres termes, à donner un critère qui permet de savoir quand deux matrices des périodes proviennent de la même variété abélienne.

Définition 2.5.3. *Soit $\mathcal{R}$ un anneau commutatif. On appelle* groupe symplectique *le groupe*

$$\mathrm{Sp}_{2g}(\mathcal{R}) := \left\{\gamma \in \mathcal{R} : \gamma \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} {}^t\gamma = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}\right\}.$$

Lemme 2.5.4. *Soit $\mathcal{R}$ un anneau commutatif.*

1. *Le groupe $\mathrm{Sp}_{2g}(\mathcal{R})$ est fermé par transposition ;*
2. *Pour une matrice $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in M_{2g}(\mathcal{R})$, on a les équivalences suivantes :*
   (a) *$\gamma \in \mathrm{Sp}_{2g}(\mathcal{R})$;*
   (b) *${}^tAC$ et ${}^tBD$ sont symétriques et ${}^tAD - {}^tCB = I_g$;*
   (c) *$A\,{}^tB$ et $C\,{}^tD$ sont symétriques et $A\,{}^tD - B\,{}^tC = I_g$.*

Démonstration. Soit $\gamma \in \mathrm{Sp}_{2g}(\mathcal{R})$. Notons que ${}^t\gamma = \left(\begin{smallmatrix} 0 & -I_g \\ I_g & 0 \end{smallmatrix}\right) \gamma^{-1} \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$. On vérifie qu'alors ${}^t\gamma \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right) \gamma = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$ et donc que le premier point est vrai. Le deuxième découle directement de la définition du groupe symplectique et du fait qu'il est fermé par transposition. Voir aussi [4, Lemme 8.2.1]. □

Le groupe $\mathrm{Sp}_{2g}(\mathbb{R})$ agit transitivement par la gauche sur $\mathcal{H}_g$ par

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \Omega := (A\Omega + B)(C\Omega + D)^{-1}.$$

De plus, tout sous-groupe discret Γ de $\mathrm{Sp}_{2g}(\mathbb{R})$ agit proprement et discontinûment sur $\mathcal{H}_g$ ([4, Proposition 8.2.5]). Ceci signifie que pour toute paire de compacts (K_1, K_2) de $\mathcal{H}_g$, l'ensemble $\{\gamma \in \Gamma : \gamma K_1 \cap K_2 \neq \emptyset\}$ est fini.

Posons $\Lambda_D := \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right) \mathbb{Z}^{2g}$ et $\Gamma_D := \{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Q}) : {}^t\gamma\Lambda_D \subseteq \Lambda_D\}$ pour un type D fixé.

Proposition 2.5.5. *Soient Ω_1, $\Omega_2 \in \mathcal{H}_g$. Les deux propositions suivantes sont équivalentes :*

1. *Les variétés abéliennes $(X_{\Omega_1}, H_{\Omega_1})$ et $(X_{\Omega_2}, H_{\Omega_2})$ de type D sont isomorphes ;*
2. *$\Omega_2 = \gamma \cdot \Omega_1$ pour un certain $\gamma \in \Gamma_D$.*

Démonstration. Voir [4, Proposition 8.1.3]. La preuve est calculatoire. Elle découle de la relation $A(\Omega_1, D) = (\Omega_2, D)R$, vue dans l'équation (2.1), où A et R sont les matrices des représentations analytique et rationnelle d'un isomorphisme $f : (X_{\Omega_1}, H_{\Omega_1}) \to (X_{\Omega_2}, H_{\Omega_2})$ par rapport à la base standard de $\mathbb{C}^g$ et des bases de Λ_{Ω_1} et Λ_{Ω_2} déterminées par Ω_1 et Ω_2. □

Puisque Γ_D est un sous-groupe discret, le [4, Théorème A.6] nous garantit que le quotient

$$\mathcal{A}_{g,D} := \mathcal{H}_g/\Gamma_D$$

est un espace analytique complexe et normal de dimension $\frac{1}{2}g(g+1)$. Avec les propositions précédentes, on en déduit :

Théorème 2.5.6. *L'espace $\mathcal{A}_{g,D}$ est un espace de modules pour les classes d'isomorphismes des variétés abéliennes polarisées de type D.*

Démonstration. Voir [4, Théorème 8.2.6]. □

Il existe une autre approche pour décrire l'espace des modules des variétés abéliennes de type D. Soit pour $\mathcal{R}$ un anneau commutatif de caractéristique nulle

$$\mathrm{Sp}_{2g}^{D}(\mathcal{R}) = \left\{\gamma \in M_{2g}(\mathcal{R}) : \gamma \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} {}^t\gamma = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}\right\}.$$

En général, ce groupe n'est pas invariant par transposition. L'application

$$\begin{array}{rccc} \sigma_D : & \mathrm{Sp}_{2g}^{D}(\mathbb{R}) & \longrightarrow & \mathrm{Sp}_{2g}(\mathbb{R}) \\ & \gamma & \longmapsto & \begin{pmatrix} I_g & 0 \\ 0 & D^{-1} \end{pmatrix} \gamma \begin{pmatrix} I_g & 0 \\ 0 & D \end{pmatrix} \end{array}$$

est un isomorphisme de groupe. L'action de $\mathrm{Sp}_{2g}(\mathbb{R})$ sur $\mathcal{H}_g$ induit une action de $\mathrm{Sp}_{2g}^{D}(\mathbb{R})$ sur $\mathcal{H}_g$ via σ_D :

$$\gamma \cdot \Omega := (A'\Omega + B'D)(D^{-1}C'\Omega + D^{-1}D'D)^{-1}$$

pour tous $\gamma = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \in \mathrm{Sp}_{2g}^{D}(\mathbb{R})$ et $\Omega \in \mathcal{H}_g$. Notons aussi que l'on a $\Gamma_D = \sigma_D(\mathrm{Sp}_{2g}^{D}(\mathbb{Z}))$. On en déduit que

$$\widetilde{\mathcal{A}}_{g,D} := \mathcal{H}_g / \mathrm{Sp}_{2g}^{D}(\mathbb{Z})$$

est un espace analytique complexe isomorphe à $\mathcal{A}_{g,D}$. D'où

Corollaire 2.5.7. *L'espace $\widetilde{\mathcal{A}}_{g,D}$ est un espace de modules pour les classes d'isomorphismes des variétés abéliennes polarisées de type D.*

Démonstration. Voir [4, Corollaire 8.2.7]. □

Dans la suite, c'est cette dernière description qui nous privilégierons.

2.5.2 Variétés abéliennes ayant multiplication réelle

Nous reprenons ici des résultats de [4, Sections 9.1 et 9.2]. Soit K un corps de nombres totalement réel de degré e sur $\mathbb{Q}$.

Définition 2.5.8. *On dit qu'une variété abélienne X a* multiplication réelle *par K lorsqu'il existe un plongement $K \hookrightarrow \mathrm{End}_{\mathbb{Q}}(X)$.*

Pour une telle variété abélienne, la proposition 2.4.9 nous dit que $g = em$ pour un certain entier $m \geq 1$.

Soit $a \in K$. Notons $a^{(i)}$ la valeur de a par le i-ème plongement de K dans $\mathbb{R}$. On pose

$$\begin{array}{rccc} \rho : & K & \longrightarrow & M_g(\mathbb{C}) \\ & a & \longmapsto & \mathrm{diag}(a^{(1)}I_m, \ldots, a^{(e)}I_m). \end{array}$$

Soit $z = (z_1, \ldots, z_e) \in \mathcal{H}_m^e$. On définit l'application

$$\begin{array}{rccc} J_z : & (K \otimes_{\mathbb{Q}} \mathbb{R})^{2m} \simeq \mathbb{R}^{2g} & \longrightarrow & \mathbb{C}^g \\ & \underline{a} & \longmapsto & \mathrm{diag}((z_1, I_m), \ldots, (z_e, I_m))\underline{a} \end{array}$$

où $\underline{a} = {}^t(\underline{a}^{(1)}, \ldots, \underline{a}^{(e)}) \in \mathbb{R}^{2g}$ avec $\underline{a}^{(i)} = {}^t(a_1^{(i)}, \ldots, a_{2m}^{(i)}) \in \mathbb{R}^{2m}$. Ainsi, $J_z(\underline{a})$ est le vecteur colonne

$$J_z(\underline{a}) = \left(z_i \, {}^t(a_1^{(i)}, \ldots, a_m^{(i)}) + {}^t(a_{m+1}^{(i)}, \ldots, a_{2m}^{(i)})\right)_{i=1,\ldots,e}.$$

Cette application est un isomorphisme de $\mathbb{R}$-espaces vectoriels. Du coup, pour tout sous-$\mathbb{Z}$-module libre $\mathcal{M}$ de K^{2m} de rang $2g$ tel que la trace $\mathrm{Tr}_{K/\mathbb{Q}}\left({}^t\underline{a}\begin{pmatrix}0 & I_m\\ -I_m & 0\end{pmatrix}\underline{b}\right)$ est dans $\mathbb{Z}$ pour tous $\underline{a},\underline{b}\in\mathcal{M}\subseteq(K\otimes_{\mathbb{Q}}\mathbb{R})^{2m}$, on a que $J_z(\mathcal{M})$ est un réseau de $\mathbb{C}^g$ et le quotient $X_z:=\mathbb{C}^g/J_z(\mathcal{M})$ est un tore complexe. Posons alors

$$H_z(x,y)={}^t x\,\mathrm{diag}(\Im(z_1),\dots,\Im(z_e))^{-1}\overline{y}.$$

C'est une forme de Riemann définie positive sur $\mathbb{C}^g$. Enfin, on a que $\rho(K)\subseteq\mathrm{End}_{\mathbb{Q}}(X_z)$ et on pose alors $\iota_z=\rho$.

Définition 2.5.9. *Fixons une représentation $\rho:K\to M_g(\mathbb{C})$. Une* variété abélienne polarisée avec $(K,\ ',\rho)$ comme structure d'endomorphismes *est un triplet (X,H,ι) tel que $X=\mathbb{C}^g/\Lambda$ est une variété abélienne, H une forme de Riemann définie positive qui est donc une polarisation sur X, et tel que l'on a un plongement $\iota:K\hookrightarrow\mathrm{End}_{\mathbb{Q}}(X)\subseteq M_g(\mathbb{C})$ (ici, on considère $\mathrm{End}_{\mathbb{Q}}(X)$ comme un sous-espace de $M_g(\mathbb{C})$ via la représentation analytique) qui vérifie :*

- *ι et ρ sont des représentations équivalentes ;*
- *l'involution de Rosati sur $\mathrm{End}_{\mathbb{Q}}(X)$ relativement à H prolonge l'involution $'$ sur K via ι.*

Proposition 2.5.10. *Pour tout $z\in\mathcal{H}_m^e$, le triplet (X_z,H_z,ι_z) est une variété abélienne polarisée avec (K,id_K,ρ) comme structure d'endomorphismes.*

Démonstration. Voir [4, Proposition 9.2.1]. □

Regardons maintenant quand est-ce que deux triplets sont isomorphes au sens suivant :

Définition 2.5.11. *Soient (X_1,H_1,ι_1) et (X_2,H_2,ι_2) deux triplets avec la même structure d'endomorphismes $(K,\ ',\rho)$. Un* isomorphisme de variétés abéliennes avec une structure d'endomorphismes $f:(X_1,H_1,\iota_1)\to(X_2,H_2,\iota_2)$ *est un isomorphisme de variétés abéliennes polarisées $f:(X_1,H_1)\to(X_2,H_2)$ tel que le diagramme suivant commute :*

$$\begin{array}{ccc} X_1 & \xrightarrow{f} & X_2 \\ {\scriptstyle\iota_1(a)}\downarrow & & \downarrow{\scriptstyle\iota_2(a)} \\ X_1 & \xrightarrow[f]{} & X_2 \end{array}$$

pour tout $a\in K$.

L'action de $\mathrm{Sp}_{2m}(\mathbb{R})$ sur $\mathcal{H}_m$ induit une action du groupe $G:=\prod_{i=1}^e\mathrm{Sp}_{2m}(\mathbb{R})$ sur $\mathcal{H}_m^e$. Cette action est, pour tous $z=(z_1,\dots,z_e)\in\mathcal{H}_m^e$ et $\gamma=(\gamma_1,\dots,\gamma_e)\in G$,

$$\gamma\cdot z:=(\gamma_1\cdot z_1,\dots,\gamma_e\cdot z_e),$$

avec $\gamma_i\cdot z_i=(A_iz_i+B_i)(C_iz_i+D_i)^{-1}$, où $\gamma_i=\begin{pmatrix}A_i & B_i\\ C_i & D_i\end{pmatrix}$ et les A_i,B_i,C_i,D_i sont des matrices $m\times m$. Pour chaque sous-module $\mathcal{M}$ sur $\mathbb{Z}$ de K^{2m} comme précédemment, on pose

$$G(\mathcal{M})=\{\gamma\in G:\mathrm{diag}({}^t\gamma_1,\dots,{}^t\gamma_e)\mathcal{M}\subseteq\mathcal{M}\}.$$

Proposition 2.5.12. *Soient z et t deux points de $\mathcal{H}_m^e$. Les variétés abéliennes polarisées (X_z, H_z, ι_z) et (X_t, H_t, ι_t) avec $(K, \, ', \rho)$ comme structure d'endomorphismes sont isomorphes si et seulement s'il existe un $\gamma \in G(\mathcal{M})$ tel que $t = \gamma \cdot z$.*

Démonstration. Voir [4, Proposition 9.2.2]. □

Ce groupe $G(\mathcal{M})$ est discret dans G. Il agit proprement et discontinûment sur $\mathcal{H}_m^e$ ([4, Proposition 8.2.5]). Donc comme dans la section précédente, on en déduit que le quotient $\mathcal{A}(\mathcal{M}) := \mathcal{H}_m^e / G(\mathcal{M})$ est un espace analytique complexe normal de dimension $\dim \mathcal{A}(\mathcal{M}) = \dim \mathcal{H}_m^e = \frac{e}{2} m(m+1)$.

Proposition 2.5.13. *$\mathcal{A}(\mathcal{M})$ est un espace de modules appelé* espace de modules pour les variétés abéliennes polarisées avec pour structure d'endomorphismes *$(K, \, ', \rho)$ associé au K-module $\mathcal{M}$.*

Démonstration. Voir [4, Page 249]. □

Notons que le choix de $\mathcal{M}$ fixe le type de polarisation et donc si on change $\mathcal{M}$, on change ce type. On obtient ainsi une multitude indéfinie d'espaces de modules associés à une même structure d'endomorphismes et chaque type de polarisation apparaît au moins une fois. Inversement, on a :

Proposition 2.5.14. *Toute variété abélienne polarisée (X, H, ι) de dimension g avec (K, id_K, ρ) comme structure d'endomorphismes est contenue dans un espace de modules de la forme $\mathcal{A}(\mathcal{M})$.*

Démonstration. Voir [4, Proposition 9.2.3]. □

Le cas qui nous intéresse le plus est lorsque l'on a que $e = g$ et $m = 1$. On prend $\mathcal{M}$ un idéal fractionnaire de K, qui est ici un corps de nombres totalement réel de degré g. On vérifie aisément que pour $z \in \mathcal{H}_1^g$, $X_z = \mathbb{C}^g / (\mathcal{M}z + \mathcal{M})$ où $\mathcal{M}z + \mathcal{M} = \{ {}^t(\lambda^{(1)} z_1 + \mu^{(1)}, \ldots, \lambda^{(g)} z_g + \mu^{(g)}) \in \mathbb{C}^g : \lambda, \mu \in \mathcal{M} \}$. L'espace de modules $\mathcal{A}(\mathcal{M})$ est appelé *variété modulaire de Hilbert*. Nous étudierons dans la section 5.1 les surfaces modulaires de Hilbert.

2.6 Fonctions thêta classiques

2.6.1 Plongements

Soit $(X_\Omega = \mathbb{C}^g / \Lambda_\Omega, H = H_\Omega)$ la variété abélienne principalement polarisée correspondant à $\Omega \in \mathcal{H}_g$. On a que $\Lambda_\Omega = \Lambda_1 \oplus \Lambda_2$ avec $\Lambda_1 = \Omega \mathbb{Z}^g$ et $\Lambda_2 = \mathbb{Z}^g$. Ceci induit la décomposition suivante $\mathbb{C}^g = V_1 \oplus V_2$ de $\mathbb{C}^g$ en deux espaces réels $V_1 = \Omega \mathbb{R}^g$ et $V_2 = \mathbb{R}^g$. La forme hermitienne H est symétrique sur V_2 car E l'est. Notons maintenant B l'extension $\mathbb{C}$-bilinéaire de la forme symétrique $H | V_2 \times V_2$. Cette extension B est également symétrique.

On a vu que $\Im(\Omega)^{-1}$ est la matrice de la forme de Riemann H et donc on a $B(x, y) = {}^t x (\Im(\Omega))^{-1} y$. On en déduit que

$$(H - B)(x, y) = {}^t x \Im(\Omega)^{-1} (\overline{y} - y) = {}^t x \Im(\Omega)^{-1} (\overline{\Omega} - \Omega) y_1 = -2\imath \, {}^t x y_1,$$

où $y = \Omega y_1 + y_2$ (voir aussi [4, Page 223]).

À partir de cette forme bilinéaire B, on définit ce que l'on appelle le *facteur d'automorphie classique*

$$a_\Omega : (\lambda, z) \in (\Lambda_\Omega, \mathbb{C}^g) \longmapsto \chi(\lambda) \exp\left(\pi(H-B)(z,\lambda) + \frac{\pi}{2}(H-B)(\lambda,\lambda)\right) \in \mathbb{C}^*.$$

Les fonctions thêta associées au facteur d'automorphie classique sont appelées *fonctions thêta classiques*. Une fonction thêta f avec un tel facteur d'automorphie doit vérifier $f(z+\lambda) = a_\Omega(\lambda, z) f(z)$ pour $\lambda \in \Lambda_\Omega$, ce qui donne pour $m \in \mathbb{Z}^g$:

$$\begin{array}{c} f(z+m) = f(z), \\ f(z+\Omega m) = \exp\left(-2\imath\pi\, {}^t z m - \imath\pi\, {}^t m \Omega m\right) f(z). \end{array} \tag{2.4}$$

Soit la fonction sur $\mathbb{C}^g \times \mathcal{H}_g$ suivante, appelée *fonction thêta classique*

$$\theta(z,\Omega) := \sum_{n\in\mathbb{Z}^g} \exp\left(\imath\pi\, {}^t n \Omega n + 2\imath\pi\, {}^t n z\right). \tag{2.5}$$

C'est une fonction holomorphe sur $\mathbb{C}^g \times \mathcal{H}_g$ ([68, Proposition II.1.1]) et elle vérifie l'équation (2.4). On peut également montrer que toute fonction f vérifiant cette même équation est de la forme $f(z) = cst \cdot \theta(z,\Omega)$ ([68, Pages 121-122]).

Définition 2.6.1. *Soit $\Omega \in \mathcal{H}_g$. Une fonction entière f sur $\mathbb{C}^g$ est Λ_Ω-quasi-périodique de poids ℓ si*

$$\begin{array}{c} f(z+m) = f(z), \\ f(z+\Omega m) = \exp\left(-2\imath\pi\ell\, {}^t z m - \imath\pi\ell\, {}^t m \Omega m\right) f(z), \end{array}$$

pour tout $m \in \mathbb{Z}^g$. Notons R_ℓ^Ω l'espace vectoriel de telles fonctions.

Pour $a, b \in \mathbb{Q}^g$, on appelle *fonction thêta classique de caractéristique* (a,b) la fonction :

$$\begin{array}{rcl} \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) & = & \sum_{n\in\mathbb{Z}^g} \exp\left(\imath\pi\, {}^t(n+a)\Omega(n+a) + 2\imath\pi\, {}^t(n+a)(z+b)\right) \\ & = & \exp\left(\imath\pi\, {}^t a \Omega a + 2\imath\pi\, {}^t a (z+b)\right) \theta(z+\Omega a + b, \Omega). \end{array} \tag{2.6}$$

Remarquons que l'on a $\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] = \theta$. La quasi-périodicité de $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ est donnée par

$$\begin{array}{rcl} \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+m,\Omega) & = & \exp\left(2\imath\pi\, {}^t a m\right) \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega); \\ \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\Omega m,\Omega) & = & \exp\left(-2\imath\pi\, {}^t b m\right) \exp\left(-\imath\pi\, {}^t m \Omega m - 2\imath\pi\, {}^t m z\right) \\ & & \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega). \end{array} \tag{2.7}$$

En outre, pour $n, m \in \mathbb{Z}^g$, on a

$$\theta\left[\begin{smallmatrix} a+n \\ b+m \end{smallmatrix}\right](z,\Omega) = \exp\left(2\imath\pi\, {}^t a m\right) \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) \tag{2.8}$$

et

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](-z,\Omega) = \theta\left[\begin{smallmatrix} -a \\ -b \end{smallmatrix}\right](z,\Omega). \tag{2.9}$$

Proposition 2.6.2. *Soit $\Omega \in \mathcal{H}_g$. On a comme bases de R_ℓ^Ω les ensembles :*

1. *$f_a(z) = \theta\left[\begin{smallmatrix} a/\ell \\ 0 \end{smallmatrix}\right](\ell z, \ell\Omega)$, pour $0 \le a < \ell$;*
2. *$g_b(z) = \theta\left[\begin{smallmatrix} 0 \\ b/\ell \end{smallmatrix}\right](\ell z, \frac{\Omega}{\ell})$, pour $0 \le b < \ell$;*
3. *Si $\ell = k^2$, une troisième base est donnée par $h_{a,b}(z) = \theta\left[\begin{smallmatrix} a/k \\ b/k \end{smallmatrix}\right](\ell z, \Omega)$, pour $0 \le a, b < k$.*

Ces bases sont reliées par

$$g_b = \sum_a \exp(2\imath\pi\ell^{-1}\,{}^t ab) f_a \qquad et \qquad h_{a,b} = \sum_{c\equiv a \bmod k} \exp(2\imath\pi k^{-1}\,{}^t cb) f_c.$$

Démonstration. Voir [68, Proposition II.1.3]. □

D'autres bases sont explicitées dans [13, Proposition 3.1.6.]. Les changements de base sont fournis dans les pages qui suivent cette proposition.

Ainsi que nous l'avons vu dans la section 2.2, les fonctions thêta permettent d'obtenir un plongement de la variété abélienne vers un espace projectif. Soit $\Lambda \subseteq \mathbb{Z}^{2g}$ d'indice s. Considérons la forme réelle antisymétrique sur $\mathbb{R}^{2g} \times \mathbb{R}^{2g}$ définie par $A(x,y) = {}^t x_1 y_2 - {}^t y_1 x_2$ où $x = (x_1, x_2)$ et $y = (y_1, y_2)$. Le *réseau perpendiculaire* à Λ est

$$\Lambda^\perp := \{x \in \mathbb{Q}^{2g} : \exp(2\imath\pi A(x,a)) = 1, \forall a \in \Lambda\}.$$

Soient $a_i, b_i \in \Lambda^\perp$ pour $1 \leq i \leq s$ un ensemble de représentants du quotient $\Lambda^\perp/\mathbb{Z}^{2g}$. Notons e_Ω l'identification de $\mathbb{R}^g \times \mathbb{R}^g$ avec $\mathbb{C}^g$ par $(x,y) \mapsto \Omega x + y$. L'ensemble des *points de base* $B_\Omega(\Lambda)$ du tore complexe $\mathbb{C}^g/e_\Omega(\Lambda)$ est l'ensemble des points de ce tore qui annulent toutes les fonctions thêta $\theta \left[\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right](z,\Omega)$:

$$B_\Omega(\Lambda) := \{z \in \mathbb{C}^g : \theta \left[\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right](z,\Omega) = 0, 1 \leq i \leq s\}/e_\Omega(\Lambda).$$

L'application holomorphe suivante est alors bien définie

$$\begin{array}{rccc} \phi_\Lambda : & (\mathbb{C}^g/e_\Omega(\Lambda)) - B_\Omega(\Lambda) & \longrightarrow & \mathbb{P}^{s-1} \\ & z & \longmapsto & (\theta \left[\begin{smallmatrix} a_1 \\ b_1 \end{smallmatrix}\right](z,\Omega), \ldots, \theta \left[\begin{smallmatrix} a_s \\ b_s \end{smallmatrix}\right](z,\Omega)). \end{array}$$

Théorème 2.6.3 (Lefschetz)**.** *Soit $\Lambda \subseteq \mathbb{Z}^{2g}$ un réseau d'indice s et supposons que $\Lambda \subseteq r\Lambda^\perp$ pour un certain $r \in \mathbb{N}$. Alors :*

1. *Si $r \geq 2$, $B_\Omega(\Lambda) = \emptyset$;*
2. *Si $r \geq 3$, ϕ_Λ est un plongement et son image est une sous-variété algébrique de $\mathbb{P}^{s-1}$;*
3. *Un tore complexe $\mathbb{C}^g/\Lambda$ peut être plongé dans un espace projectif si et seulement si $A(\Lambda) \subseteq \Omega\mathbb{Q}^g + \mathbb{Q}^g$ pour une certaine matrice A complexe $g \times g$ et un certain $\Omega \in \mathcal{H}_g$.*

Démonstration. Voir [68, Théorème II.1.3 et Corollaire page 134]. □

2.6.2 Équation fonctionnelle des fonctions thêta

Soient Ω_1 et Ω_2 dans $\mathcal{H}_g$. Nous avons vu que les tores $\mathbb{C}^g/(\mathbb{Z}^g + \Omega_i\mathbb{Z}^g)$ pour $i = 1, 2$ sont isomorphes si et seulement s'il existe une matrice $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ telle que $\gamma \cdot \Omega_1 = \Omega_2$. L'isomorphisme entre les tores est donné par :

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

D'après [68, Proposition II.5.5], le groupe $\mathrm{Sp}_{2g}(\mathbb{Z})$ agit sur $\mathbb{C}^g$ par

$$\gamma \cdot z = {}^t(C\Omega_1 + D)^{-1} z,$$

pour $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. Cette même proposition affirme que ce groupe agit également sur la caractéristique des fonctions thêta. Les trois actions de $\mathrm{Sp}_{2g}(\mathbb{Z})$ se retrouvent dans l'équation fonctionnelle sur les fonctions thêta qui suit.

Commençons par noter, pour une matrice M donnée, M_0 le vecteur colonne composé des éléments diagonaux de M.

Proposition 2.6.4 (Équation fonctionnelle)**.** *Soient $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$, $e' = \frac{1}{2}({}^tAC)_0$ et $e'' = \frac{1}{2}({}^tDB)_0$. Alors pour tous vecteurs a, b dans $\mathbb{Q}^g$, z dans $\mathbb{C}^g$ et Ω dans $\mathcal{H}_g$, on a*

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

où ζ_γ est une racine huitième de l'unité qui ne dépend que de γ.

Démonstration. Voir [48, Chapitre 5 Théorème 2] ou [13, Proposition 3.1.24]. □

Remarque 2.6.5. *La racine huitième de l'unité et la racine carré ne dépendent pas de la caractéristique. Comme dans la suite nous nous intéresserons qu'à des quotients de fonctions thêta, nous n'aurons pas besoin de connaître cette racine de l'unité ni la détermination de la racine carré.*

Similairement au cas de la dimension 1, nous notons Γ_g le groupe $\mathrm{Sp}_{2g}(\mathbb{Z})$. Définissons les groupes suivants qui sont les groupes que nous manipulerons le plus :

$$\Gamma_g(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : \ A \equiv D \equiv I_g \bmod N,\ B \equiv C \equiv 0 \bmod N\right\},$$

$$\Gamma_g(N, 2N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g(N) : \ ({}^tAC)_0 \equiv ({}^tDB)_0 \equiv 0 \bmod 2N\right\},$$

$$\Gamma_{g,0}(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : \ C \equiv 0 \bmod N\right\},$$

$$\text{et} \qquad \Gamma_g^0(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : \ B \equiv 0 \bmod N\right\}.$$

Pour ces deux derniers groupes, nous enlèverons l'indice g lorsque la dimension ambiante sera implicite.

Proposition 2.6.6. *Le groupe Γ_g est engendré par la matrice $\mathfrak{J} = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$ et les $\frac{g(g+1)}{2}$ matrices de la forme*

$$\mathfrak{M}_{i,j} = \begin{pmatrix} I_g & m_{i,j} \\ 0 & I_g \end{pmatrix},$$

où $m_{i,j}$ désigne la matrice de taille $g \times g$ dont toutes les entrées sont nulles sauf les entrées (i, j) et (j, i) qui valent 1.

Démonstration. Voir [50, Pages 41-42]. □

Les générateurs de quelques sous-groupes de Γ_g sont donnés dans l'annexe 5 de [68, Chapitre II]. Terminons avec les définitions de formes et fonctions modulaires de Siegel.

Définition 2.6.7. *Soit $g \geq 2$ et soit $\Gamma \subseteq \Gamma_g$ un sous-groupe d'indice fini. Une forme modulaire de poids k pour le groupe Γ est une fonction holomorphe f définie sur $\mathcal{H}_g$ telle que $f(\gamma \cdot \Omega) = \det(C\Omega + D)^k f(\Omega)$ pour tous $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ et $\Omega \in \mathcal{H}_g$.*

Pour $g = 1$, on a vu qu'il faut une condition supplémentaire. Le principe de Koecher [50, Section 4] nous dit que cette condition est immédiatement vérifiée lorsque $g \geq 2$. Par exemple, on a

Proposition 2.6.8. *Soit N pair. Alors pour tous a_1, a_2, b_1, $b_2 \in \frac{1}{N}\mathbb{Z}^g$, la fonction*

$$\theta\left[\begin{smallmatrix} a_1 \\ a_2 \end{smallmatrix}\right](0,\Omega) \cdot \theta\left[\begin{smallmatrix} b_1 \\ b_2 \end{smallmatrix}\right](0,\Omega)$$

est modulaire de poids 1 pour le groupe $\Gamma_g(N^2, 2N^2)$.

Démonstration. Voir [68, Corollaire II.5.11]. □

Définition 2.6.9. *Soit Γ un sous-groupe d'indice fini de Γ_g. Une fonction $f : \mathcal{H}_g \to \mathbb{C}$ est une* fonction modulaire de Siegel *lorsqu'il existe deux formes modulaires de Siegel f_1 et f_2 de même poids et pour le même groupe Γ telles que $f = \frac{f_1}{f_2}$.*

On peut prendre des quotients de fonctions comme dans la proposition précédente pour former des fonctions modulaires.

2.6.3 Thêta constantes en caractéristique $\frac{1}{2}$ et en dimension g

On va étudier maintenant les fonctions thêta au point $z = 0$ en regardant ces fonctions comme des fonctions en Ω. Dans ce cas là, on parle de *thêta constantes*. De plus, on se place en caractéristique $\frac{1}{2}$ car c'est la caractéristique la plus malléable. Soient donc $a, b \in \{0,1\}^g$, posons $\theta_{a,b}(\Omega) := \theta\left[\begin{smallmatrix} a/2 \\ b/2 \end{smallmatrix}\right](0,\Omega)$.

Les équations (2.8) et (2.9) nous disent pour $a, b \in \{0,1\}^g$ que

$$\theta\left[\begin{smallmatrix} a/2 \\ b/2 \end{smallmatrix}\right](0,\Omega) = \theta\left[\begin{smallmatrix} -a/2 \\ -b/2 \end{smallmatrix}\right](0,\Omega) = \exp(2\imath\pi(-{}^t a/2)b)\theta\left[\begin{smallmatrix} a/2 \\ b/2 \end{smallmatrix}\right](0,\Omega)$$

et donc

$$\theta_{a,b}(\Omega) = \exp(\imath\pi\, {}^t ab)\theta_{a,b}(\Omega).$$

Ceci conduit à la définition suivante.

Définition 2.6.10. *Soient $a, b \in \{0,1\}^g$. On dit que la thêta constante $\theta_{a,b}$ est* paire *lorsque ${}^t ab \equiv 0 \bmod 2$. Si ce n'est pas le cas, on dit que la thêta constante est* impaire.

Lorsque la thêta constante est impaire, on a $\theta_{a,b}(\Omega) = -\theta_{a,b}(\Omega)$ est donc cette thêta constante est identiquement nulle. On ne s'intéresse donc qu'aux thêta constantes paires. Une récurrence montre que sur les 4^g thêta constantes, il y en a $2^{g-1}(2^g + 1)$ qui sont paires et donc $2^{g-1}(2^g - 1)$ qui sont impaires.

L'équation fonctionnelle sur les carrés des thêta constantes et la définition du groupe symplectique nous donnent le résultat suivant, que nous réutiliserons.

Corollaire 2.6.11. *Pour tous* $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g(2,4)$, $a, b \in \{0,1\}^g$ *et* $\Omega \in \mathcal{H}_g$ *:*

$$\theta_{a,b}^2(\gamma \cdot \Omega) = \zeta_\gamma^2 \det(C\Omega + D)\theta_{a,b}^2(\Omega).$$

Ainsi, les quotients des carrés de fonctions thêta paires (en caractéristique $\frac{1}{2}$*) sont des fonctions modulaires pour le groupe* $\Gamma_g(2,4)$*.*

Proposition 2.6.12 (Formules de duplication)**.** *Pour tous* $a, b \in \{0,1\}^g$ *et* $\Omega \in \mathcal{H}_g$*, on a*

$$\theta_{a,b}(2\Omega) = \frac{1}{2^g} \sum_{b_1+b_2 \equiv b \bmod 2} (-1)^{{}^t a b_1} \theta_{0,b_1}(\Omega)\theta_{0,b_2}(\Omega);$$

$$\theta_{a,b}\left(\frac{\Omega}{2}\right) = \frac{1}{2^g} \sum_{a_1+a_2 \equiv a \bmod 2} (-1)^{{}^t a_1 b} \theta_{a_1,0}(\Omega)\theta_{a_2,0}(\Omega).$$

Démonstration. Voir [19, Propositions 5.5 et 5.6]. □

On note par $\lambda(\Omega)$ la plus petite valeur propre de la matrice $\Im(\Omega)$.

Lemme 2.6.13. *Pour tous* $a, b \in \{0,1\}^g$*, si* $(\Omega_n)_{n\in\mathbb{N}}$ *est une suite d'éléments de* $\mathcal{H}_g$ *telle que* $\lim_{n\to\infty} \lambda(\Omega_n) = +\infty$*, alors*

$$\lim_{n\to\infty} \theta_{a,b}(\Omega_n) = \begin{cases} 1 & \text{si } a = 0; \\ 0 & \text{si } a \neq 0. \end{cases}$$

Démonstration. Nous reprenons la preuve de [19, Lemme 5.2]. Soient $b \in \{0,1\}^g$ et $(\Omega_n)_{n\in\mathbb{N}}$. Notons $q_n = \exp(-\pi\lambda(\Omega_n))$. Alors la définition des thêta constantes montre que pour tout $n \geq 0$,

$$|\theta_{0,b}(\Omega_n) - 1| \leq \sum_{(m_1,\ldots,m_g)\in\mathbb{Z}^g\setminus\{0\}} q_n^{m_1^2+\ldots+m_g^2} \leq 2^g \Big(\sum_{m\in\mathbb{Z}\setminus\{0\}} q_n^{m^2}\Big)\Big(\sum_{m\in\mathbb{Z}} q_n^{m^2}\Big)^{2^g-1}.$$

On utilise la majoration

$$\sum_{m\geq 1} q_n^{m^2} \leq \sum_{m\geq 1} q_n^m \leq \frac{q_n}{1-q_n},$$

pour obtenir

$$|\theta_{0,b}(\Omega_n) - 1| \leq 2^g \left(1 + \frac{2q_n}{1-q_n}\right)^{2^g-1} \frac{2q_n}{1-q_n}.$$

Si $\lambda(\Omega_n)$ tend vers l'infini, alors bien sûr q_n tend vers 0 et l'inégalité ci-dessus permet de montrer le résultat puisque le côté droit tend vers zéro.

Si maintenant $a \neq 0$ et que $(\Omega_n)_{n\in\mathbb{N}}$ est une suite de $\mathcal{H}_g$ telle que $\lambda(\Omega_n)$ tend vers l'infini, alors ce qui précède montre que pour tout $b \in \{0,1\}^g$,

$$\lim_{n\to+\infty} \theta_{0,b}\left(\frac{\Omega_n}{2}\right) = 1,$$

et en exprimant les $\theta_{a,b}^2(\Omega_n)$ en fonction des $\theta_{0,b}^2(\frac{\Omega_n}{2})$ à l'aide de la formule de duplication, on voit facilement que si $a \neq 0$,

$$\lim_{n\to+\infty} \theta_{a,b}^2(\Omega_n) = 0,$$

ce qui conclut la démonstration. □

2.7 Jacobiennes de courbes

Nous avons vu dans le premier chapitre que les tores complexes de dimension 1 sont des courbes elliptiques. Nous allons voir maintenant le lien entre les courbes de genre g et les tores de dimension g.

Soit C une courbe projective lisse de genre g sur $\mathbb{C}$ de racines $e_1, \ldots, e_{2g+2}$. C'est une surface de Riemann compacte de genre g. Le groupe d'homologie $H_1(C, \mathbb{Z})$ est un groupe abélien libre de rang $2g$. Notons $A_1, \ldots, A_g, B_1, \ldots B_g$ une base et dans le cas des courbes hyperelliptiques, nous la prenons comme dans la figure 2.1. C'est une base canonique au sens où si on note $I(\sigma, \tau)$ le produit d'intersection de deux cycles σ et τ, alors

$$I(A_i, A_j) = 0, \qquad I(B_i, B_j) = 0 \qquad \text{et} \qquad I(A_i, B_j) = \delta_{i,j}.$$

Cependant, cette base n'est pas unique. En effet, le vecteur $\gamma\, {}^t(A_1, \ldots, A_g, B_1, \ldots, B_g)$ fournit une autre base canonique lorsque $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$.

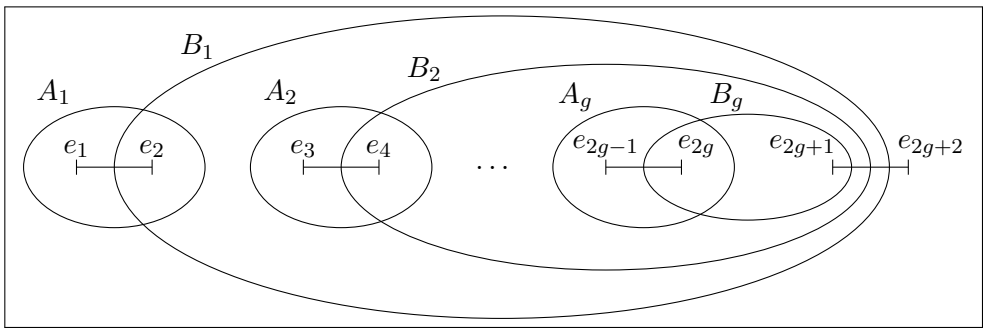

FIGURE 2.1 – Base canonique du groupe d'homologie d'une courbe hyperelliptique

Théorème 2.7.1 (Relations bilinéaires de Riemann)**.** *Soit C une surface de Riemann compacte de genre g :*

1. *Pour toutes 1-formes holomorphes ω, η :*

$$\sum_{k=1}^{g} \int_{A_k} \omega \int_{B_k} \eta - \sum_{k=1}^{g} \int_{B_k} \omega \int_{A_k} \eta = 0;$$

2. *Pour toute 1-forme holomorphe ω :*

$$\Im\left(\sum_{k=1}^{g} \overline{\int_{A_k} \omega} \int_{B_k} \omega \right) > 0.$$

Démonstration. Voir [68, Théorème II.2.1]. □

Notons par $\Gamma(C, \Omega^1)$ l'espace vectoriel de dimension g des 1-formes sur la courbe C. D'après [69, Proposition 5.2], cet espace consiste, dans le cas hyperelliptique, en les 1-formes $\omega = \frac{P(x)dx}{y}$ pour P un polynôme de degré $\leq g - 1$.

Corollaire 2.7.2. *On peut trouver une base normalisée $\omega_1, \ldots, \omega_g$ de $\Gamma(C, \Omega^1)$ telle que*

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

Soit $\Omega_{i,j} = \int_{B_i} \omega_j$. Alors $\Omega_{i,j} = \Omega_{j,i}$ et l'image de $(\Omega_{i,j})_{1 \leq i,j \leq g}$ est définie positive. On obtient ainsi une matrice de la forme $(I_g, \Omega) \in M_{g \times 2g}(\mathbb{C})$ avec $\Omega \in \mathcal{H}_g$.

Démonstration. Voir [68, Corollaire II.2.2]. Le couplage entre les $\omega \in \Gamma(C, \Omega^1)$ et les A_i est non dégénéré à cause du deuxième point des relations bilinéaires de Riemann. En appliquant le premier point à $\omega = \omega_j$ et $\eta = \omega_i$, on obtient $\int_{B_j} \omega_i - \int_{B_i} \omega_j = 0$ et donc $\Omega_{i,j} = \Omega_{j,i}$. Soient $\alpha_1, \ldots, \alpha_g$ des réels. On pose $\omega = \sum_{i=1}^g \alpha_i \omega_i$. Le point deux nous donne

$$0 < \Im\left(\sum_{k=1}^g \overline{\int_{A_k} \omega} \int_{B_k} \omega\right) = \Im\left(\sum_{k=1}^g \alpha_k \left(\sum_{i=1}^g \alpha_i \Omega_{k,i}\right)\right)$$

et donc $\Im(\Omega) > 0$. □

Une intégrale de la forme $\int_\sigma \omega$ pour $\sigma \in H_1(C, \mathbb{Z})$ et $\omega \in \Gamma(C, \Omega^1)$ est appelée une *période* de C. C'est pourquoi les matrices Ω comme dans le corollaire précédent ainsi que toute matrice de $\mathcal{H}_g$ sont appelées *matrice des périodes*.

Soit $\omega_1, \ldots, \omega_g$ la base normalisée de $\Gamma(C, \Omega^1)$. Considérons maintenant l'application

$$\begin{array}{rccc} per: & H_1(C,\mathbb{Z}) & \longrightarrow & \mathbb{C}^g \\ & \sigma & \longmapsto & (\int_\sigma \omega_1, \ldots, \int_\sigma \omega_g). \end{array}$$

Corollaire 2.7.3. *L'application per est injective et son image est le réseau $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ engendré par les vecteurs entiers et les colonnes de Ω.*

Démonstration. Voir [68, Corollaire II.2.3]. □

On peut ainsi définir un tore complexe à partir d'une surface de Riemann compacte. Ce tore est appelé la *Jacobienne* de C :

$$\mathrm{Jac}(C) := \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g).$$

Ce tore est une variété abélienne principalement polarisée. Notons H sa polarisation principale. Elle est appelée *polarisation canonique* de $\mathrm{Jac}(C)$. Tout diviseur Θ tel que le diviseur associé dans le groupe de Picard définit la polarisation canonique est dit *diviseur thêta* de la Jacobienne. On note $(\mathrm{Jac}(C), \Theta)$ la Jacobienne canoniquement polarisée.

Nous avons vu que le théorème d'Appell-Humbert nous permet de construire un isomorphisme entre $\widehat{\mathrm{Jac}(C)}$ et $\mathrm{Pic}^0(\mathrm{Jac}(C))$. De plus, la polarisation étant principale, il y a un isomorphisme entre $\mathrm{Jac}(C)$ et $\widehat{\mathrm{Jac}(C)}$. On sait donc que $\mathrm{Pic}^0(\mathrm{Jac}(C))$ est isomorphe à $\mathrm{Jac}(C)$.

Le théorème de Stokes dit qu'on peut associer canoniquement à tout élément σ de $H_1(C, \mathbb{Z})$ la forme linéaire sur l'espace vectoriel $\Gamma(C, \Omega^1)$, que l'on note également σ, suivante :

$$\sigma : \omega \in \Gamma(C, \Omega^1) \longmapsto \int_\sigma \omega \in \mathbb{C}.$$

La Jacobienne de C est canoniquement isomorphe à $\mathrm{Hom}(\Gamma(C, \Omega^1), \mathbb{C})/H_1(C, \mathbb{Z})$ (et où les éléments de groupe d'homologie sont vus comme des formes linéaires). Notons $\mathrm{Pic}^0_W(C)$ le groupe obtenu en quotientant $\mathrm{Div}^0_W(C)$, le groupe des diviseurs de Weil de degré 0, par le sous-groupe des diviseurs principaux. Chaque diviseur $D \in \mathrm{Div}^0_W(C)$ est une somme formelle finie $D = \sum_{k=1}^n (p_k) - (q_k)$ pour certains points $p_k, q_k \in C$. La classe de la forme linéaire $\omega \mapsto \sum_{k=1}^n \int_{q_k}^{p_k} \omega$ dans

$\mathrm{Hom}(\Gamma(C,\Omega^1),\mathbb{C})/H_1(C,\mathbb{Z})$ dépend certes du diviseur D, mais pas de sa représentation comme somme de différences formelles de points. Ainsi, l'application suivante, dite d'*Abel-Jacobi* est bien définie :

$$\begin{array}{ccc} \mathrm{Div}^0_W(C) & \longrightarrow & \mathrm{Jac}(C) \\ D & \longmapsto & \{\omega \mapsto \sum_{k=1}^n \int_{q_k}^{p_k} \omega\}. \end{array}$$

C'est un homomorphisme de groupes.

Les diviseurs de Weil et de Cartier sont équivalents, dans le sens où $\mathrm{Div}_W(X) = \mathrm{Div}(X)$, pour toute variété lisse X ([38, II.6.11]).

Théorème 2.7.4 (Abel-Jacobi)**.** *L'application d'Abel-Jacobi induit un isomorphisme canonique entre* $\mathrm{Pic}^0_W(C)$ *et* $\mathrm{Jac}(C)$*.*

Démonstration. Voir [4, Théorème 11.1.3]. □

Ceci montre que $\mathrm{Pic}^0(C)$ a une structure de variété abélienne principalement polarisée.

Théorème 2.7.5 (Torelli)**.** *Soient C et C' deux surfaces de Riemann compactes de genre g. Si leurs Jacobiennes $(J(C),\Theta)$ et $(J(C'),\Theta')$ sont isomorphes en tant que variétés abéliennes principalement polarisées, alors C et C' sont isomorphes.*

Démonstration. Voir [4, Théorème 11.1.7]. □

On vient de voir qu'à chaque courbe projective lisse on peut associer une variété abélienne. Réciproquement, on a le résultat suivant.

Théorème 2.7.6. *Toute variété abélienne complexe, simple et principalement polarisée de dimension $g \leq 3$ est :*

1. *Pour $g = 1$ une courbe elliptique ;*
2. *Pour $g = 2$ la Jacobienne d'une courbe lisse hyperelliptique de genre 2 ;*
3. *Pour $g = 3$ la Jacobienne d'une courbe lisse de genre 3 ;*

Démonstration. Le cas de genre 1 a été vu dans le premier chapitre. Pour les deux autres, voir [4, Corollaire 11.8.2]. □

Deuxième partie

Aspect algorithmique des variétés abéliennes principalement polarisées de dimension 2

Chapitre 3

Différentes représentations

Dans ce chapitre, nous allons nous concentrer sur les variétés abéliennes qui sont principalement polarisées et de dimension 2. Ceci ne nous empêchera pas de donner des résultats qui seront vrais en toute dimension. Le chapitre précédent nous a permis de voir que ces surfaces peuvent être représentées via des courbes hyperelliptiques de genre 2 ou des matrices des périodes dans $\mathcal{H}_2$. Une autre façon consiste à considérer des invariants appelés invariants d'Igusa qui sont la généralisation du j-invariant que l'on a vu dans le premier chapitre. Par contre, ces invariants d'Igusa sont au nombre de trois. Nous donnerons d'autres invariants que nous notons $\mathfrak{c}_i$ et $\mathfrak{b}_i$ définis à partir de quotients des carrés des thêta constantes.

Notre objectif ici est de donner différents algorithmes permettant de passer d'une représentation à l'autre. Nous allons commencer par décrire un domaine fondamental dans $\mathcal{H}_2$, ce qui permet d'avoir un représentant d'une classe d'isomorphisme de variétés abéliennes principalement polarisée, et donner un algorithme de réduction dans ce domaine (algorithme 3.1.2). L'algorithme de Mestre sert à déduire, à partir des invariants d'Igusa, l'équation d'une courbe hyperelliptique de genre 2 correspondant à la même variété. Les algorithmes 3.4.1 et 3.6.1 permettent alors de passer de cette courbe aux invariants $\mathfrak{c}_i$ et de ces invariants à une matrice des périodes de $\mathcal{H}_2$. Nous verrons le rôle fondamental que jouent les suites de Borchardt, qui sont une généralisation de l'AGM, dans ces algorithmes et comment elles peuvent être utilisées pour évaluer rapidement les thêta constantes, en généralisant l'algorithme correspondant que l'on a vu dans le premier chapitre en dimension 1.

3.1 Domaine fondamental

Nous commençons par quelques rappels pour bien fixer le cadre dans lequel nous sommes. Soit la matrice

$$\mathfrak{J} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Nous avons vu que le groupe symplectique $\mathrm{Sp}_{2g}(\mathbb{Z})$ est défini par

$$\mathrm{Sp}_{2g}(\mathbb{Z}) := \{\gamma \in M_{2g\times 2g}(\mathbb{Z}) : \gamma\mathfrak{J}\,{}^t\gamma = \mathfrak{J}\}$$

et que de façon équivalente, $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ si et seulement si

$$^tAC = {}^tCA, \qquad {}^tBD = {}^tDB, \qquad {}^tDA - {}^tBC = I_g,$$

si et seulement si

$$A\,{}^tB = B\,{}^tA, \qquad D\,{}^tC = C\,{}^tD, \qquad A\,{}^tD - B\,{}^tC = I_g.$$

Ce groupe définit une action de groupe $\gamma \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}$ sur $\mathcal{H}_g$. Remarquons que $-I_g$ agit trivialement et ainsi, plusieurs auteurs préfèrent considérer le groupe symplectique projectif $\mathrm{Sp}_{2g}(\mathbb{Z})/\langle \pm I_g \rangle$. Rappelons que nous posons

$$\Gamma_g := \mathrm{Sp}_{2g}(\mathbb{Z}).$$

La proposition 2.6.6 dit que le groupe symplectique est finiment engendré. Dans le cas de la dimension 2, les générateurs de Γ_2 sont les quatre matrices

$$\mathfrak{J}, \quad \mathfrak{M}_1 = \begin{pmatrix} I_2 & \begin{matrix}1\\0\end{matrix} & \begin{matrix}0\\0\end{matrix} \\ 0 & I_2 \end{pmatrix}, \quad \mathfrak{M}_2 = \begin{pmatrix} I_2 & \begin{matrix}0\\1\end{matrix} & \begin{matrix}1\\0\end{matrix} \\ 0 & I_2 \end{pmatrix}, \quad \mathfrak{M}_3 = \begin{pmatrix} I_2 & \begin{matrix}0\\0\end{matrix} & \begin{matrix}0\\1\end{matrix} \\ 0 & I_2 \end{pmatrix}. \tag{3.1}$$

Comme avec les courbes elliptiques (proposition 1.3.5), il existe un domaine fondamental pour l'action de $\Gamma_g/\langle \pm I_{2g} \rangle$ sur $\mathcal{H}_g$.

Définition 3.1.1 (Domaine fondamental)**.** *Définissons l'ensemble $\mathcal{F}_g$ comme étant l'ensemble des $\Omega = (\Omega_{i,j}) \in \mathcal{H}_g$ vérifiant les trois conditions suivantes :*

1. $|\Re(\Omega_{i,j})| \leq \frac{1}{2}$ *pour tous* $i, j \in \{1, \ldots, g\}$ *;*
2. *La matrice* $\Im(\Omega)$ *est réduite au sens de Minkowski ;*
3. *Pour tout* $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$, $|\det(C\Omega + D)| \geq 1$.

Cet ensemble est un fermé dans l'espace des matrices complexes symétriques ([50, Page 31]). Nous ne détaillerons pas la réduction de Minkowski. Nous donnerons seulement sa définition et renvoyons le lecteur à [50].

Une matrice réelle symétrique $A = (a_{i,j})_{1 \leq i,j \leq g}$ est *réduite au sens de Minkowski* lorsque pour tout $j \in \{1, \ldots, g\}$ et pour tout vecteur $n = (n_1, \ldots, n_g) \in \mathbb{Z}^g$ vérifiant $\mathrm{pgcd}(n_1, \ldots, n_g) = 1$, on a ${}^tnAn \geq a_{j,j}$ et lorsque pour tout $j \in \{1, \ldots, g-1\}$, on a $a_{j,j+1} \geq 0$. Par [50, Proposition 1 page 13], ceci implique pour une matrice réelle $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ que $c \geq a \geq 2b \geq 0$.

Notons que pour $g = 1$, on retrouve l'ensemble $\mathcal{F}_1$ défini dans le premier chapitre.

Proposition 3.1.2. *L'ensemble $\mathcal{F}_g$ est un domaine fondamental pour l'action de $\Gamma_g/\langle \pm I_{2g} \rangle$ sur $\mathcal{H}_g$. Ceci implique que pour tout $\Omega \in \mathcal{H}_g$, il existe $\gamma \in \Gamma_g/\langle \pm I_{2g} \rangle$ tel que $\gamma \cdot \Omega \in \mathcal{F}_g$ et cet élément γ est unique si $\gamma \cdot \Omega$ est un point intérieur de $\mathcal{F}_g$.*

Démonstration. Voir [50, Théorème 2 page 34] ou [19, Proposition 5.3]. □

Notons que la troisième condition de la définition du domaine fondamental doit être vérifiée pour toutes les matrices de Γ_g. Cependant, il est montré pour tout g qu'il suffit que cette condition soit vérifié pour un certain ensemble fini ([50, Page 30]), qui n'est connu que pour $g = 1$ et $g = 2$. Pour $g = 1$, on a vu que l'ensemble $\{S\}$ fonctionne. Pour $g = 2$, cet ensemble est constitué des 19 matrices suivantes (voir [33]) :

$$\mathfrak{N}_1 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&0\\0&1&0&0\end{pmatrix}, \quad \mathfrak{N}_2 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&1&0\\0&1&0&0\end{pmatrix}, \quad \mathfrak{N}_3 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&-1&0\\0&1&0&0\end{pmatrix},$$

$$\mathfrak{N}_4 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&0\\0&1&0&1\end{pmatrix}, \quad \mathfrak{N}_5 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&0\\0&1&0&-1\end{pmatrix}, \quad \mathfrak{N}_6 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&1&0\\0&1&0&1\end{pmatrix},$$

$$\mathfrak{N}_7 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}, \quad \mathfrak{N}_8 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&-1&0\\0&1&0&1\end{pmatrix}, \quad \mathfrak{N}_9 = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&1&0\\0&1&0&-1\end{pmatrix},$$

$$\mathfrak{N}_{10} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&1\\0&1&1&0\end{pmatrix}, \quad \mathfrak{N}_{11} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&-1\\0&1&-1&0\end{pmatrix}, \quad \mathfrak{N}_{12} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&1&1\\0&1&1&0\end{pmatrix},$$

$$\mathfrak{N}_{13} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&-1&-1\\0&1&-1&0\end{pmatrix}, \quad \mathfrak{N}_{14} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&1\\0&1&1&1\end{pmatrix}, \quad \mathfrak{N}_{15} = \begin{pmatrix} 0&0&-1&0\\0&0&0&-1\\1&0&0&-1\\0&1&-1&-1\end{pmatrix},$$

$$\mathfrak{N}_{16} = \begin{pmatrix} 1&0&-1&0\\0&1&0&-1\\1&0&0&0\\0&0&0&1\end{pmatrix}, \quad \mathfrak{N}_{17} = \begin{pmatrix} 1&0&-1&0\\0&1&0&-1\\0&0&1&0\\0&1&0&0\end{pmatrix}, \quad \mathfrak{N}_{18} = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\1&-1&1&0\\-1&1&0&1\end{pmatrix},$$

$$\mathfrak{N}_{19} = \begin{pmatrix} -1&0&0&0\\0&-1&0&0\\1&-1&-1&0\\-1&1&0&-1\end{pmatrix}.$$

On en déduit l'algorithme 3.1.1 qui permet de réduire au sens de Minkowski une matrice symétrique réelle pour $g = 2$ et l'algorithme 3.1.2 qui permet de réduire une matrice de $\mathcal{H}_2$ dans $\mathcal{F}_2$ (ce sont les algorithmes 9 et 10 de [19]).

La validité de l'algorithme de réduction dans le domaine fondamental découle de [50, Lemme 1 page 29].

Lemme 3.1.3. *Pour tout $\Omega \in \mathcal{F}_g$, si l'on note Ω_1 le premier élément diagonal de Ω, alors*

$$\Im(\Omega_1) \geq \frac{\sqrt{3}}{2}.$$

Démonstration. Voir [19, Lemme 5.2]. Soit la matrice $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$ avec

$$A = \begin{pmatrix} 0 & 0 \\ 0 & I_{g-1} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 \\ 0 & I_{g-1} \end{pmatrix}.$$

On a alors $|\det(C\Omega + D)| = |\Omega_1|$. Par définition de $\mathcal{F}_g$, on a d'une part que $|\Omega_1| \geq 1$ et d'autre part que $|\Re(\Omega_1)| \leq \frac{1}{2}$. On en déduit la proposition. □

Proposition 3.1.4. *Soit $\Omega \in \mathcal{F}_2$. Alors la plus petite valeur propre de $\Im(\Omega)$ vérifie*

$$\lambda(\Omega) \geq \frac{\sqrt{3}}{4}.$$

Démonstration. Puisque $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right)$ est dans $\mathcal{F}_2$, elle est réduite au sens de Minkowski et on a alors :

$$\Im(\Omega_3) \geq \Im(\Omega_1) \geq 2\Im(\Omega_2) \geq 0.$$

Algorithme 3.1.1 : Réduction d'une matrice symétrique réelle au sens de Minkowski

Entrée : Une matrice $\gamma = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ symétrique réelle définie positive.
Sortie : Une matrice entière unimodulaire U telle que $U\gamma\,{}^tU$ soit réduite au sens de Minkowski.

```
t = vrai;
U = I_2;
tant que t = vrai faire
    si 2|c| ≤ |a| alors
        si |a| ≤ |b| alors
            si |c| ≤ 0 alors
                γ = ( 1 0 ; 0 −1 ) γ ( 1 0 ; 0 −1 );
                U = ( 1 0 ; 0 −1 ) U;
            fin
            t = faux;
        sinon
            γ = ( 0 1 ; −1 0 ) γ ( 0 1 ; −1 0 );
            U = ( 0 1 ; −1 0 ) U;
        fin
    sinon
        q = ⌊c/a⌉;
        γ = ( 1 0 ; −q 1 ) γ ( 1 −q ; 0 1 );
        U = ( 1 0 ; −q 1 ) U;
    fin
fin
retourner U;
```

Les valeurs propres de $\Im(\Omega)$ étant les racines du polynôme $X^2 - (y_1 + y_3)X + (y_1y_3 - y_2^2)$ où $y_i = \Im(\Omega_i)$, la plus petite valeur propre $\lambda(\Omega)$ vérifie alors

$$\lambda(\Omega) = \frac{1}{2}\left(y_1 + y_3 - \sqrt{(y_3 - y_1)^2 + 4y_2^2}\right) \geq \frac{y_1}{2} \geq \frac{\sqrt{3}}{4},$$

par le lemme 3.1.3 et car $y_3 \geq \sqrt{(y_3 - y_1)^2 + 4y_2^2} \Leftrightarrow 0 \geq (y_1^2 - y_1y_3) + (4y_2^2 - y_1y_3)$, ce qui est le cas. □

3.2 Thêta constantes en caractéristique $\frac{1}{2}$ et en dimension 2

Retournons aux thêta constantes et regardons les spécificités de la dimension $g = 2$. Rappelons au lecteur que les thêta constantes sont les fonctions thêta, définies à l'équation (2.6), vues comme des fonctions sur $\mathcal{H}_2$ au point $z = 0$. En caractéristique $\frac{1}{2}$, nous avons vu à la définition 2.6.10 une notion de parité sur ces thêta constantes, qui dit que les thêta constantes impaires sont identiquement nulles. On montre aisément qu'il y a $4^g = 16$ thêta constantes, dont 10 qui sont paires et 6 qui sont impaires. Pour tous $a = {}^t(a_0, a_1)$ et $b = {}^t(b_0, b_1)$ dans $\{0, 1\}^2$,

Algorithme 3.1.2 : Réduction dans le domaine fondamental $\mathcal{F}_2$

Entrée : Une matrice des périodes $\Omega \in \mathcal{H}_2$.

Sortie : Un couple $\left(\gamma, \Omega' = \left(\begin{smallmatrix} \Omega'_1 & \Omega'_2 \\ \Omega'_2 & \Omega'_3 \end{smallmatrix}\right)\right) \in \Gamma_2 \times \mathcal{F}_2$ tel que $\Omega' = \gamma \cdot \Omega$.

$\gamma = I_4$;
$\Omega' = \Omega$;
$t = vrai$;
tant que $t = vrai$ **faire**
  $U = RéductionMinkowski(\Im(\Omega'))$;
  $\gamma = \left(\begin{smallmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{smallmatrix}\right)\gamma$;
  $\Omega' = U\Omega\,{}^tU$;
  pour $j = 1$ **à** 3 **faire**
    $a = -\lfloor \Re(\Omega'_j) \rceil$;
    $\Omega' = M_j^a \Omega'$;
    $\gamma = M_j^a \gamma$;
  fin
  $t = faux$;
  pour $j = 1$ **à** 19 **faire**
    si $|\det(C_j\Omega' + D_j)| < 1$ **alors**
      $t = vrai$;
      $\Omega' = \mathfrak{N}_j \Omega'$;
      $\gamma = \mathfrak{N}_j \gamma$;
    fin
  fin
fin
retourner (γ, Ω');

on pose

$$\theta_{b_0+2b_1+4a_0+8a_1} := \theta_{a,b}. \tag{3.2}$$

Avec cette notation, les thêta constantes impaires sont celles dont l'indice est dans $\{5, 7, 10, 11, 13, 14\}$ tandis que les paires ont un indice dans $\{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$. Notons $\mathcal{P}$ ce dernier ensemble.

Proposition 3.2.1. *Pour tous $\Omega \in \mathcal{F}_2$ et $j \in \{0, 1, 2, 3\}$,*

$$|\theta_j(\Omega) - 1| \leq 0.405.$$

Ceci reste vrai lorsqu'on remplace Ω par $\alpha\Omega$ avec $\alpha > 1$.

Démonstration. Voir [19, Proposition 6.1]. Soient $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{F}_2$ et $j \in \{0, 1, 2, 3\}$. Notons, pour $i \in \{1, 2, 3\}$,

$$q_i = |\exp(\imath\pi\Omega_i)| = \exp(-\pi\Im(\Omega_i))$$

et $Q = \exp(-\pi\frac{\sqrt{3}}{4})$. On a alors par la définition des thêta constantes :

$$|\theta_j(\Omega) - 1| \leq \sum_{(m,n)\in\mathbb{Z}^2} q_1^{m^2} q_2^{2mn} q_3^{n^2}.$$

Comme Ω est dans le domaine fondamental, on a d'une part que

$$\Im(\Omega_3) \geq \Im(\Omega_1) \geq 2\Im(\Omega_2) \geq 0$$

et d'autre part que $\Im(\Omega_1) \geq \frac{\sqrt{3}}{2}$, ce qui nous permet de déduire que

$$q_1^{m^2} q_2^{2mn} q_3^{n^2} \leq \begin{cases} Q^{2(m^2+n^2)} & \text{si } mn \geq 0; \\ Q^{2(m^2+mn+n^2)} & \text{si } mn < 0. \end{cases}$$

Nous utilisons ces majorations pour majorer une première partie de la somme :

$$\sum_{(m,n)\in[-2,2]\setminus\{(0,0)\}} q_1^{m^2} q_2^{2mn} q_3^{n^2} \leq 6Q^2 + 2Q^4 + 4Q^6 + 6Q^8 + 4Q^{10} + 2Q^{16}.$$

Pour le reste de la somme, on utilise la majoration moins fine suivante, qui provient de ce que $\lambda(\Omega) \geq \frac{\Im(\Omega_1)}{2}$:

$$q_1^{m^2} q_2^{2mn} q_3^{n^2} \leq Q^{m^2+n^2},$$

pour tous $m, n \in \mathbb{Z}$. On trouve alors :

$$\sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ |m|\geq 3 \text{ ou } |n|\geq 3}} q_1^{m^2} q_2^{2mn} q_3^{n^2} \leq 4\left(\sum_{m=0}^{2}\sum_{n\geq 3} Q^{m^2+n^2} + \sum_{m\geq 3}\sum_{n\geq 1} Q^{m^2+n^2}\right) \leq 4\frac{1+Q}{(1-Q)^2}Q^9.$$

Ces deux majorations mises ensembles nous donnent

$$|\theta_j(\Omega) - 1| \leq 6Q^2 + 2Q^4 + 4Q^6 + 6Q^8 + 4Q^{10} + 2Q^{16} + 4\frac{1+Q}{(1-Q)^2}Q^9$$

et une évaluation numérique permet de conclure la première partie de cette preuve. La dernière affirmation de la proposition vient du fait que cette preuve s'applique aisément dans le cas considéré. □

La proposition suivante contient des majorations pour d'autres thêta constantes. Les preuves sont similaires. Nous renvoyons donc le lecteur à [19, Propositions 6.2 et 6.3]

Proposition 3.2.2. *Pour tous $\Omega \in \mathcal{F}_2$, $j \in \{4, 6\}$ et $k \in \{8, 9\}$:*

$$\left|\frac{\theta_j(\Omega)}{2\exp\left(\imath\pi\frac{\Omega_1}{4}\right)} - 1\right| \leq 2\left|\exp\left(\imath\pi\frac{\Omega_1}{2}\right)\right| \quad \textit{et} \quad \left|\frac{\theta_k(\Omega)}{2\exp\left(\imath\pi\frac{\Omega_3}{4}\right)} - 1\right| \leq 2\left|\exp\left(\imath\pi\frac{\Omega_1}{2}\right)\right|.$$

Intéressons nous maintenant aux valeurs pour lesquelles les thêta constantes paires s'annulent.

Proposition 3.2.3. *Soit $\Omega \in \mathcal{H}_2$ et $\Omega' \in \mathcal{F}_2$ qui sont dans la même classe d'équivalence sous l'action de Γ_2. Alors soit la matrice Ω' est diagonale auquel cas exactement une thêta constante paire s'annule en Ω et en même temps $\theta_{15}(\Omega') = 0$, soit Ω' n'est pas diagonale et dans ce cas aucune des thêta constantes s'annule en Ω (ni en Ω' par l'équation fonctionnelle de la proposition 2.6.4).*

Démonstration. Voir [19, Proposition 6.5 et Corollaire 6.1] □

Nous concluons cette section avec un premier algorithme d'évaluation des thêta constantes. Cet algorithme est qualifié de naïf car il ne fait qu'utiliser la définition des thêta constantes comme séries de Fourier. Notons de suite qu'il suffit de savoir évaluer les thêta constantes sur le domaine fondamental, ce qui souvent permet d'avoir une meilleure convergence, car pour une matrice des périodes Ω dans $\mathcal{H}_2$, on peut calculer Ω' dans ce domaine fondamental qui lui est équivalente, évaluer les thêta constantes en Ω' et ensuite utiliser l'équation fonctionnelle des thêta constantes pour les calculer en Ω. De plus, on a

Proposition 3.2.4. *Pour tout $\Omega \in \mathcal{H}_2$, si l'on pose $(a,b,c,d) = (\theta_j^2(\Omega))_{j\in\{0,1,2,3\}}$, alors*

$$\begin{array}{rcl} (X-\theta_4^4(\Omega))(X-\theta_6^4(\Omega)) & = & X^2+(b^2+d^2-a^2-c^2)X+(ac-bd)^2, \\ (X-\theta_8^4(\Omega))(X-\theta_9^4(\Omega)) & = & X^2+(c^2+d^2-a^2-b^2)X+(ab-cd)^2, \\ \textit{et} \quad (X-\theta_{12}^4(\Omega))(X-\theta_{15}^4(\Omega)) & = & X^2+(b^2+c^2-a^2-d^2)X+(ad-bc)^2. \end{array}$$

Démonstration. Voir [19, Proposition 6.8]. □

Cette proposition nous dit qu'on peut connaître toutes les thêta constantes à une racine quatrième près à partir des quatre premières. Ces racines peuvent être déterminées en calculant des approximations à faible précision. Nous présentons donc un algorithme qui permet de calculer les quatre premières thêta constantes. Nous renvoyons à [19, Section 10.1] pour plus de détails.

Pour tous $b \in \{0,1\}^2$ et $\Omega \in \mathcal{H}_2$, on a par les équations (2.6) et (3.2) que les quatre premières thêta constantes sont

$$\theta_{0,b}(\Omega) = \sum_{n\in\mathbb{Z}^2} (-1)^{{}^t nb} \exp(\imath\pi\, {}^t n\Omega n).$$

On cherche à approcher cette somme et pour cela, on introduit les sommes partielles $S_{b,B}$ pour tous $b = {}^t(b_0,b_1) \in \{0,1\}^2$, $\Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3\end{smallmatrix}\right) \in \mathcal{H}_g$ et $B \geq 1$ par

$$S_{b,B}(\Omega) = \sum_{(m,n)\in[-B,B]^2} (-1)^{b_0m+b_1n} \exp(\imath\pi(m^2\Omega_1+n^2\Omega_3+2mn\Omega_2)).$$

En notant $q_1 = \exp(\imath\pi\Omega_1)$, $q_3 = \exp(\imath\pi\Omega_3)$, $q_2 = \exp(2\imath\pi\Omega_2)$ et en utilisant les symétries apparaissant dans $S_{b,B}$, on trouve que

$$S_{b,B} = 1+2\sum_{n=1}^{B}\left((-1)^{nb_0}q_1^{n^2}+q_3^{n^2}\left((-1)^{nb_1}+\sum_{m=1}^{B}(-1)^{mb_0+nb_1}q_1^{m^2}(q_2^{mn}+q_2^{-mn})\right)\right).$$

C'est cette expression que l'on va utiliser pour calculer $\theta_j(\Omega)$, $j \in \{0,1,2,3\}$. Pour accélérer les calculs, les $q_1^{m^2}$ sont précalculés en utilisant une chaîne d'addition adaptée. Notons que pour ces thêta constantes, les $S_{b,B}$ font intervenir les mêmes termes au signe près, ce qui fait qu'on peut les réutiliser et ainsi, la complexité de l'évaluation simultanée de ces quatre thêta constantes est la même que celle de l'évaluation d'une seule d'entre elles.

Pour tous $b \in \{0,1\}^2$, $B \geq 0$ et $\Omega \in \mathcal{F}_2$, [19, Lemme 10.1] montre que l'on a

$$|\theta_{0,b}(\Omega) - S_{b,B}(\Omega)| \leq 16\exp(-\pi\lambda(\Omega))^{(B+1)^2} \leq 16\exp(-\pi\sqrt{3}/4)^{(B+1)^2}$$

et en utilisant la proposition 3.2.1, on en déduit la majoration

$$\left|\frac{S_{b,B}(\Omega)}{\theta_{0,b}(\Omega)} - 1\right| \leq 27 \exp\left(-\pi\sqrt{3}/4\right)^{(B+1)^2}.$$

Dans ces conditions, si B vérifie

$$B \geq \sqrt{\frac{4(N + \log_2(27))}{\pi \log_2(e)\sqrt{3}}} - 1,$$

alors $S_{b,B}$ est une approximation de $\theta_{0,b}(\Omega)$ à précision N (nous avons repris ici les arguments de [19] en y apportant plusieurs corrections mineures). Tout ceci justifie l'algorithme 3.2.1 (voir [19, Algorithme 15]) qui est de complexité $O(\mathcal{M}'(N)N)$.

3.3 Fonctions modulaires pour Γ_2

Nous allons introduire dans cette section des fonctions modulaires qui sont l'analogue du j-invariant en dimension 1 et présenter des algorithmes pour obtenir ces invariants depuis une courbe hyperelliptique de genre 2 et vice-versa.

3.3.1 Invariants d'Igusa et de Streng

Commençons par définir les invariants d'Igusa et de Streng. Nous allons donner deux définitions équivalentes : une par les thêta constantes et l'autre par les séries d'Eisenstein. Nous aurons besoin des deux dans la suite.

Soient les formes modulaires de Siegel h_j, pour $j \in \{4, 6, 10, 12, 16\}$, de poids j et pour le groupe Γ_2 suivantes

$$h_4 = \sum_{j\in\mathcal{P}} \theta_j^8, \qquad h_{10} = \prod_{j\in\mathcal{P}} \theta_j^2,$$

$$\begin{aligned} h_{12} = \quad & (\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + \quad (\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4 + \quad (\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4 + \\ & (\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4 + \quad (\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + \quad (\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4 + \\ & (\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + \quad (\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4 + \quad (\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4 + \\ & (\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4 + \quad (\theta_1\theta_2\theta_3\theta_6\theta_9\theta_{15})^4 + \quad (\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4 + \\ & (\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + \quad (\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4 + \quad (\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4, \end{aligned}$$

$$\begin{aligned} h_{16} = \quad & (\theta_3^8 + \theta_6^8 + \theta_9^8 + \theta_{12}^8)(\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + \quad (\theta_3^8 + \theta_4^8 + \theta_8^8 + \theta_{15}^8)(\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4 + \\ & (\theta_2^8 + \theta_6^8 + \theta_8^8 + \theta_{12}^8)(\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4 + \quad (\theta_2^8 + \theta_4^8 + \theta_9^8 + \theta_{15}^8)(\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4 + \\ & (\theta_2^8 + \theta_3^8 + \theta_8^8 + \theta_9^8)(\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + \quad (\theta_1^8 + \theta_6^8 + \theta_8^8 + \theta_{15}^8)(\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4 + \\ & (\theta_1^8 + \theta_4^8 + \theta_9^8 + \theta_{12}^8)(\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + \quad (\theta_1^8 + \theta_3^8 + \theta_4^8 + \theta_6^8)(\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4 + \\ & (\theta_1^8 + \theta_2^8 + \theta_{12}^8 + \theta_{15}^8)(\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4 + \quad (\theta_0^8 + \theta_6^8 + \theta_9^8 + \theta_{15}^8)(\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4 + \\ & (\theta_0^8 + \theta_4^8 + \theta_8^8 + \theta_{12}^8)(\theta_1\theta_2\theta_3\theta_6\theta_9\theta_{15})^4 + \quad (\theta_0^8 + \theta_3^8 + \theta_{12}^8 + \theta_{15}^8)(\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4 + \\ & (\theta_0^8 + \theta_2^8 + \theta_4^8 + \theta_6^8)(\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + \quad (\theta_0^8 + \theta_1^8 + \theta_8^8 + \theta_9^8)(\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4 + \\ & (\theta_0^8 + \theta_1^8 + \theta_2^8 + \theta_3^8)(\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4, \end{aligned}$$

et enfin

$$h_6 = \frac{h_{12}h_4 - 3h_{16}}{2h_{10}}.$$

On pose alors

$$I_2 = \frac{h_{12}}{h_{10}}, \quad I_4 = h_4, \quad I_6 = \frac{h_{16}}{h_{10}}, \quad I_6' = h_6, \quad I_{10} = h_{10} \tag{3.3}$$

et on a la relation $I_6' = \frac{1}{2}(I_2I_4 - 3I_6)$.

Algorithme 3.2.1 : Évaluation de θ_j, $j \in \{0,1,2,3\}$, par les séries de Fourier

Entrée : $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{F}_2$, $N \geq 1$.
Sortie : $(T_j)_{j\in\{0,1,2,3\}}$ tel que pour tout $j \in \{0,1,2,3\}$, $|T_j/\theta_j(\Omega) - 1| \leq 2^{-N}$.

$B = \left\lfloor \sqrt{\frac{4(N+\log_2(27))}{\pi \log_2(e)\sqrt{3}}} \right\rfloor$;
$q_j = \exp(\imath\pi\Omega_j)$ pour $j \in \{1,3\}$ et $q_2 = \exp(2\imath\pi\Omega_2)$;
$q_4 = 1/q_2$;
$a = q_1; b = q_1^2; Q_{1,s}[1] = q_1$;
pour $m = 2$ **à** B **faire**
    $a = ab$;
    $Q_{1,s}[m] = aQ_{1,s}[m-1]$;
fin
$S_j = 0$ pour $j \in \{0,1,2,3\}$;
$Q_3 = 1; a_2 = 1; a_4 = 1; b_3 = q_3; c_3 = q_3^2$;
pour $n = 1$ **à** B **faire**
    $a_2 = a_2q_2; a_4 = a_4q_4$;
    $Q_3 = Q_3b_3; b_3 = b_3c_3$;
    $S_0 = S_0 + Q_{1,s}[n]$;
    $S_1 = S_1 + (-1)^n Q_{1,s}[n]$;
    $S_2 = S_2 + Q_{1,s}[n]$;
    $S_3 = S_3 + (-1)^n Q_{1,s}[n]$;
    $Q_2 = 1; Q_4 = 1$;
    $A_0 = 1; A_1 = 1; A_2 = (-1)^n; A_3 = (-1)^n$;
    pour $m = 1$ **à** B **faire**
        $Q_2 = Q_2a_2; Q_4 = Q_4a_4$;
        $s = Q_{1,s}[m](Q_2 + Q_4)$;
        $A_0 = A_0 + s; A_1 = A_1 + (-1)^m s; A_2 = A_2 + (-1)^n s; A_3 = A_3 + (-1)^{m+n} s$;
        $S_j = S_j + Q_3A_j$ pour $j \in \{0,1,2,3\}$;
    fin
fin
retourner $(1 + 2S_j)_{j\in\{0,1,2,3\}}$;

Définition 3.3.1. *On appelle* invariants d'Igusa *les fonctions* $\mathfrak{j}_1$, $\mathfrak{j}_2$ *et* $\mathfrak{j}_3$ *définies par*

$$\mathfrak{j}_1 = \frac{I_2^5}{I_{10}} = \frac{h_{12}^5}{h_{10}^6}, \qquad \mathfrak{j}_2 = \frac{I_4 I_2^3}{I_{10}} = \frac{h_4 h_{12}^3}{h_{10}^4} \qquad et \qquad \mathfrak{j}_3 = \frac{I_6 I_2^2}{I_{10}} = \frac{h_{16} h_{12}^2}{h_{10}^4}.$$

Définition 3.3.2. *On appelle* invariants de Streng *les fonctions* $\mathfrak{i}_1$, $\mathfrak{i}_2$ *et* $\mathfrak{i}_3$ *définies par*

$$\mathfrak{i}_1 = \frac{I_4 I_6'}{I_{10}} = \frac{h_4 h_6}{h_{10}}, \qquad \mathfrak{i}_2 = \frac{I_4^2 I_2}{I_{10}} = \frac{h_4^2 h_{12}}{h_{10}^2} \qquad et \qquad \mathfrak{i}_3 = \frac{I_4^5}{I_{10}^2} = \frac{h_4^5}{h_{10}^2}.$$

Ces invariants sont reliés par les relations suivantes

$$\mathfrak{i}_1 = \frac{\mathfrak{j}_2(\mathfrak{j}_2 - 3\mathfrak{j}_3)}{2\mathfrak{j}_1}, \quad \mathfrak{i}_2 = \frac{\mathfrak{j}_2^2}{\mathfrak{j}_1}, \quad \mathfrak{i}_3 = \frac{\mathfrak{j}_2^5}{\mathfrak{j}_1^3} \tag{3.4}$$

et

$$\mathfrak{j}_1 = \frac{\mathfrak{i}_2^5}{\mathfrak{i}_3^2}, \quad \mathfrak{j}_2 = \frac{\mathfrak{i}_2^3}{\mathfrak{i}_3}, \quad \mathfrak{j}_3 = \frac{\mathfrak{i}_2^2(\mathfrak{i}_2 - 2\mathfrak{i}_1)}{3\mathfrak{i}_3}. \tag{3.5}$$

Historiquement, les invariants d'Igusa ont été introduits par Igusa dans [45] tandis que les autres invariants l'ont été par Streng cinquante ans plus tard dans [80]. Ce dernier, dans sa thèse, les a définis afin d'obtenir des polynômes de classes plus petits que ceux que l'ont obtient avec les invariants d'Igusa ([80, Annexe 3]). Les invariants de Streng sont construits afin d'avoir une puissance minimale de h_{10} dans les dénominateurs. Nous parlerons parfois de *j-invariants* en analogie avec le j-invariant de la dimension 1 et le contexte rendra clair si nous parlons des invariants d'Igusa ou ceux de Streng. Les résultats fondamentaux d'Igusa (voir [45, 46]) sont les théorèmes :

Théorème 3.3.3. *Le corps* $\mathbb{C}_{\Gamma_2}$ *des fonctions modulaires de Siegel en dimension* 2 *est* $\mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3) = \mathbb{C}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$.

Théorème 3.3.4. *Génériquement, deux surfaces abéliennes principalement polarisées sont isomorphes si et seulement si elles ont les mêmes invariants d'Igusa, ou, de manière équivalente, de Streng.*

Redéfinissons ces invariants à travers des séries. On définit la série d'Eisenstein ψ_k de poids pair $k \geq 4$ par

$$\psi_k(\Omega) = \sum_{C,D} \det(C\Omega + D)^{-k}, \tag{3.6}$$

où la somme est prise sur l'ensemble des matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ de $\mathrm{Sp}_4(\mathbb{Z})$ à multiplication à gauche près par $\mathrm{SL}_2(\mathbb{Z})$. Soient

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}53^{-1}43867(\psi_4\psi_6 - \psi_{10}) \tag{3.7}$$

et

$$\chi_{12} = 2^{-13}3^{-7}5^{-3}7^{-2}337^{-1}131 \cdot 593(3^2 7^2 \psi_4^3 + 2 \cdot 5^3 \psi_6^2 - 691\psi_{12}) \tag{3.8}$$

deux formes modulaires paraboliques de Siegel de poids 10 et 12 respectivement. Par forme parabolique de poids k sur $\mathcal{H}_g$, on entend une forme modulaire de poids k sur $\mathcal{H}_g$ telle que sa série de fourier est de la forme

$$f(\Omega) = \sum_{t>0} a(t) \exp(2\imath\pi \mathrm{Tr}(t\Omega)),$$

où t parcourt l'ensemble des matrices semi-entières positives ([50, Proposition 2 page 56]). Ces séries peuvent être écrites en terme des thêta constantes. En effet, on a $\psi_4 = 2^{-2}h_4$, $\psi_6 = 2^{-2}h_6$, $\chi_{10} = -2^{-14}h_{10}$ et $\chi_{12} = 2^{-17}3^{-1}h_{12}$ (voir [46, 47]). L'anneau gradué des formes modulaires holomorphes de Siegel pour $\mathrm{Sp}_4(\mathbb{Z})$ est l'anneau engendré par les polynômes ψ_4, ψ_6, χ_{10} et χ_{12} (voir [46]). Ainsi, les invariants d'Igusa s'écrivent

$$\mathrm{j}_1 = 2\cdot 3^5\frac{\chi_{12}^5}{\chi_{10}^6},\quad \mathrm{j}_2 = 2^{-3}3^3\frac{\psi_4\chi_{12}^3}{\chi_{10}^4}\quad\text{et}\quad \mathrm{j}_3 = 2^{-5}3\left(\frac{\psi_6\chi_{12}^2}{\chi_{10}^3}+2^2 3\frac{\psi_4\chi_{12}^3}{\chi_{10}^4}\right) \tag{3.9}$$

et on peut aussi en déduire l'expression des invariants de Streng en fonction de ces formes modulaires, ce dont on n'aura pas besoin dans la suite.

3.3.2 Courbes hyperelliptiques de genre 2 et invariants d'Igusa

Nous allons parler ici du passage d'une courbe hyperelliptique aux invariants d'Igusa et vice-versa. Supposons donc que l'on ait l'équation $Y^2 = f(X)$ d'une courbe hyperelliptique de genre 2 avec f de degré 6 (on peut toujours se ramener à ce cas). Alors, en notant $\alpha_1,\ldots,\alpha_6$ les six racines distinctes, a_6 le coefficient dominant et (ij) la différence $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$, on a les relations

$$\begin{aligned} I_2 &= a_6^2\textstyle\sum_{15}(12)^2(34)^2(56)^2,\\ I_4 &= a_6^4\textstyle\sum_{10}(12)^2(23)^2(31)^2(45)^2(56)^2(64)^2,\\ I_6 &= a_6^6\textstyle\sum_{60}(12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2,\\ \text{et}\qquad I_{10} &= a_6^{10}\textstyle\prod_{i<j}(\alpha_i-\alpha_j)^2, \end{aligned} \tag{3.10}$$

où les indices des sommes représentent le nombre de combinaisons possibles. On obtient ainsi les invariants d'Igusa à partir d'une courbe hyperelliptique de genre 2 (voir [46]).

Il existe un algorithme appelé *Algorithme de Mestre* pour résoudre le problème inverse. Dans son article [62], Mestre étudie les invariants associés à une forme sextique. Ces invariants sont construits à partir d'une opération sur les formes appelée "Ueberschiebung".

Il est alors montré qu'à partir d'un modèle C d'équation $Y^2 = F(X)$, avec F de degré 6, et d'involution w, on peut construire une conique non dégénérée L, une cubique M et un isomorphisme $C/w \to L$ dont les images des 6 points de Weierstrass de C, c'est-à-dire des 6 racines de F, sont les points d'intersection de L et de M. Ces conique et cubique sont définies à partir des invariants trouvés par des "Ueberschiebung" et peuvent être construits directement à partir des invariants d'Igusa de la variété qui nous intéresse. L'exposition succincte qui suit de cet algorithme provient de [56] et correspond au cas général où la courbe a un groupe d'automorphisme trivial. On est sur $\mathbb{C}$ et on pose

$$x = \frac{8}{225}\left(1+20\frac{\mathrm{j}_2}{\mathrm{j}_1}\right),\quad y = \frac{16}{3375}\left(1+80\frac{\mathrm{j}_2}{\mathrm{j}_1}-600\frac{\mathrm{j}_3}{\mathrm{j}_1}\right)\quad\text{et}$$

$$z = \frac{-64}{253125}\left(-10800000/\mathrm{j}_1 - 9 - 700\frac{\mathrm{j}_2}{\mathrm{j}_1} - 3600\frac{\mathrm{j}_3}{\mathrm{j}_1} + 12400\left(\frac{\mathrm{j}_2}{\mathrm{j}_1}\right)^2 - 48000\frac{\mathrm{j}_2\mathrm{j}_3}{\mathrm{j}_1^2}\right).$$

La conique de Mestre est donnée par l'équation ${}^t vLv = 0$ pour $v = {}^t(v_1, v_2, v_3)$ et

$$L = \begin{pmatrix} x+6y & 6x^2+2y & 2z \\ 6x^2+2y & 2z & 9x^3+4xy+6y^2 \\ 2z & 9x^3+4xy+6y^2 & 6x^2y+2y^2+3xz \end{pmatrix},$$

tandis que l'équation $\sum c_{ijk} v_i v_j v_k = 0$, où les c_{ijk} sont définis plus bas, nous donne la cubique de Mestre M dans $\mathbb{P}^2$:

$$\begin{aligned}
c_{111} &= 36xy - 2y - 12z; \\
c_{112} &= -18x^3 - 12xy - 36y^2 - 2z; \\
c_{113} &= -9x^3 - 36x^2y - 4xy - 6xz - 18y^2; \\
c_{122} &= c_{113}; \\
c_{123} &= -27x^4 - 18x^2y - 18xy^2 - 3xz - 2y^2 - 12yz; \\
c_{133} &= -27/2x^4 - 72x^3y - 6x^2y - 9x^2z - 39xy^2 - 36y^3 - 2yz; \\
c_{222} &= -81x^4 - 54x^2y - 18xy^2 - 8y^2 + 6yz; \\
c_{223} &= 9x^3y - 27x^2z + 6xy^2 + 18y^3 - 8yz; \\
c_{233} &= -81/2x^5 - 27x^3y - 9x^2y^2 - 4xy^2 + 3xyz - 6z^2; \\
c_{333} &= 81/2x^4y - 81/2x^3z + 27x^2y^2 + 9xy^3 - 18xyz + 4y^3 - 30y^2z.
\end{aligned}$$

En prenant un point rationnel quelconque de L, on peut réécrire la conique comme une fonction paramétrique $v_i = f_i(X)$ pour un polynôme quadratique en X, ce qui donne d'ailleurs un isomorphisme entre L et $\mathbb{P}^1$ sur $\mathbb{C}$. En mettant ces équations dans M, on obtient une équation polynomiale f en X de degré 6. Une courbe hyperelliptique de genre 2 correspondant aux invariants d'Igusa de départ est alors $Y^2 = f(X)$. Nous renvoyons donc à l'article de Mestre pour plus de détails. Une implantation de cet algorithme est disponible dans [29].

3.4 Invariants avec les thêta constantes

En plus des invariants d'Igusa, nous allons nous intéresser à des invariants sur des sous-groupes du groupe Γ_2, afin d'obtenir des polynômes modulaires pour ces invariants plus petits que ceux avec les invariants d'Igusa ou de Streng, ainsi qu'il est fait en dimension 1.

3.4.1 Formules de Thomae

Les formules de Thomae sont des formules qui permettent d'obtenir les puissances quatrième des thêta constantes en dimension g à partir de l'équation d'une courbe hyperelliptique de genre g. Elles dépendent d'un choix de la base du groupe d'homologie. Nous les donnons avec la base canonique vue dans la figure 2.1 de la section 2.7. Soit donc

$$C : Y^2 = \prod_{j=1}^{2g+2} (x - e_j)$$

une telle courbe. On note $E = \{e_1, \ldots, e_{2g+2}\}$, $U = \{1, 3, 5, \ldots 2g+1\}$ et pour tout $j \in \{1, \ldots, g\}$, on pose

— η_{2j-1} le vecteur composé du vecteur de $\{0,1\}^g$ ayant que des entrées nulles si ce n'est la j-ième puis du vecteur de $\{0,1\}^g$ ayant que des entrées nulles si ce n'est les $j-1$ premières ;

— η_{2j} le vecteur composé du vecteur de $\{0,1\}^g$ ayant que des entrées nulles si ce n'est la j-ième puis du vecteur de $\{0,1\}^g$ ayant que des entrées nulles si ce n'est les j premières ;
— $\eta_{2g+1} = ((0,\dots,0),(1,\dots,1))$;
— $\eta_{2g+2} = ((0,\dots,0),(0,\dots,0))$.

Ceci nous permet de définir pour tout ensemble $S \subseteq E$ le vecteur η_S comme étant la somme $\sum_{e_j \in S} \eta_j$ modulo 2. Rappelons que la différence symétrique de deux ensembles S et T est

$$S\Delta T = (S \cup T) \backslash (S \cap T).$$

On peut enfin donner une version des formules de Thomae

Théorème 3.4.1 (Formules de Thomae)**.** *Pour tout ensemble de points de Weierstrass $E = \{e_1,\dots,e_{2g+2}\}$, il existe une constante c telle que pour tout sous-ensemble S de E de cardinal pair, on ait*

$$\theta^4_{\eta_S}(\Omega) = \begin{cases} 0 & \text{si } \#S\Delta U \neq g+1, \\ (-1)^{\#S\cap U} c \prod_{\substack{x\in S\Delta U \\ y\notin S\Delta U}} \frac{1}{x-y} & \text{si } \#S\Delta U = g+1. \end{cases}$$

Démonstration. Voir [83] ou [69, Section III.8]. □

Notons qu'il existe des formes plus générales pour ce théorème, en particulier on peut prendre un des points de Weierstrass comme étant le point à l'infini.

La matrice Ω qui apparaît dans ce théorème est une matrice de $\mathcal{H}_g$ qui correspond à la même variété abélienne principalement polarisée que la courbe hyperelliptique de départ. Cette matrice est déterminée par un choix dans l'ordre des racines de E. Un autre choix donne une matrice équivalente dans $\mathcal{H}_g/\Gamma_g$. Notons que les puissances quatrièmes des thêta constantes ne sont pas des fonctions modulaires (ce sont des formes modulaires) et donc si Ω' est équivalente à Ω dans $\mathcal{H}_g/\Gamma_g$, on a que, en général, $\theta^4_{a,b}(\Omega') \neq \theta^4_{a,b}(\Omega)$. Par contre, les quotients $\theta^4_{a,b}/\theta^4_{c,d}$ sont des fonctions modulaires mais seulement pour le groupe $\Gamma_g(2)$.

Considérons $\mathcal{H}^{(2)}_g$ l'ensemble des paires (C,σ), où C est une courbe hyperelliptique et $\sigma : \{1,\dots,2g+2\} \to E$ une bijection vers $E \subseteq C$ qui est l'ensemble des points de ramification de $\pi : C \to \mathbb{P}^1$, modulo isomorphismes de courbes. Puisque les points de branchement dans $\mathbb{P}^1$ déterminent la courbe, on a, d'après [69, Section III.8], que

$$\mathcal{H}^{(2)}_g \simeq \left\{ \begin{array}{l} \text{séquences de points distincts} \\ P_1,\dots,P_{2g+2} \text{ de } \mathbb{P}^1 \end{array} \right\} \Big/ \begin{array}{c} \text{modulo équivalence} \\ \text{projective } \mathrm{PGL}(2,\mathbb{C}) \end{array}$$

et puisque l'on peut normaliser P_{2g+2} comme étant le point à l'infini, on a aussi

$$\mathcal{H}^{(2)}_g \simeq \left\{ \begin{array}{l} \text{séquences de points complexes} \\ \text{distincts } e_1,\dots,e_{2g+1} \end{array} \right\} \Big/ \begin{array}{c} \text{modulo équivalence} \\ \text{affine } e_i \mapsto \lambda e_i + \mu \end{array}$$

et en normalisant encore en posant $e_1 = 0$ et $e_2 = 1$, on obtient

$$\mathcal{H}^{(2)}_g \simeq \left\{ \begin{array}{l} \text{sous-ensemble ouvert de } \mathbb{C}^{2g-1} \text{ de points} \\ (e_3,\dots,e_{2g+1}) \text{ tel que } e_i \neq e_j, e_i \neq 0,1 \end{array} \right\}.$$

Ainsi, $\mathcal{H}_g^{(2)}$ est une variété affine, car c'est l'intersection de deux ouverts fondamentaux. En terme de sa seconde description, si t est la coordonnée de $\mathbb{P}^1$, alors l'anneau de coordonnées affine de $\mathcal{H}_g^{(2)}$ est engendré par les fonctions de la forme

$$\frac{t(P_i)-t(P_k)}{t(P_j)-t(P_k)}\cdot\frac{t(P_j)-t(P_\ell)}{t(P_i)-t(P_\ell)}.$$

En terme de la troisième description, cet anneau est engendré par les fonctions de la forme

$$\frac{a_i-a_k}{a_j-a_k}.$$

Les formules de Thomae impliquent alors

Proposition 3.4.2. *L'anneau de coordonnées affine de $\mathcal{H}_g^{(2)}$ est engendré par les fonctions*

$$\left(\frac{\theta_{a,b}}{\theta_{0,0}}\right)^{\pm 4}.$$

Démonstration. Voir [69, Corollaire 8.13]. □

Le lemme 8.12 de [69] nous dit alors que $\mathcal{H}_g^{(2)}$ peut être envoyé dans $\mathcal{H}_g/\Gamma_g(2)$. Or, lorsque $g=2$, le théorème suivant nous dit qu'il y a un morphisme birationnel entre les deux.

Théorème 3.4.3. *Le corps des fonctions modulaires invariantes par $\Gamma_g(2)$ est $\mathbb{C}(\theta_{a,b}^4/\theta_{0,0}^4)$.*

Démonstration. Voir [60, Théorème 2]. □

3.4.2 Invariants pour $\Gamma_2(2)$ et $\Gamma_2(2,4)$

Tout courbe hyperelliptique de genre 2 est isomorphe via des transformations linéaires fractionnaires à une courbe de la forme :

$$C: Y^2 = X(X-1)(X-\mathfrak{r}_1)(X-\mathfrak{r}_2)(X-\mathfrak{r}_3), \tag{3.11}$$

où les $\mathfrak{r}_i$ sont appelés *invariants de Rosenhain* de C. On peut prendre

$$\mathfrak{r}_1=\frac{\theta_0^2\theta_1^2}{\theta_3^2\theta_2^2},\qquad \mathfrak{r}_2=\frac{\theta_1^2\theta_{12}^2}{\theta_2^2\theta_{15}^2},\qquad \text{et}\qquad \mathfrak{r}_3=\frac{\theta_0^2\theta_{12}^2}{\theta_3^2\theta_{15}^2}.$$

Ces invariants sont des fonctions modulaires pour $\Gamma_2(2)$. Notons qu'une courbe comme dans l'équation (3.11) est équivalente à la courbe

$$C': Y^2 = X(X-1)(X-2)\left(X-\frac{2\,\mathfrak{r}_1}{\mathfrak{r}_1+1}\right)\left(X-\frac{2\,\mathfrak{r}_2}{\mathfrak{r}_2+1}\right)\left(X-\frac{2\,\mathfrak{r}_3}{\mathfrak{r}_3+1}\right), \tag{3.12}$$

courbe que l'on obtient en envoyant le point à l'infini vers 2. On peut donc facilement obtenir les quotients des thêta constantes à la puissance 4 à partir des invariants de Rosenhain en appliquant les formules de Thomae que nous avons données sur cette dernière courbe. On en déduit le corollaire suivant du théorème 3.4.3.

Corollaire 3.4.4. *Le corps des fonctions modulaires invariantes par $\Gamma_2(2)$ est engendré par les invariants de Rosenhain.*

Rappelons que le groupe $\Gamma_2(2,4)$ est défini dans la section 2.6.2. Cette définition est équivalente à la suivante, qui est plus malléable :

$$\Gamma_2(2,4) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2(2) : B_0 \equiv C_0 \equiv 0 \bmod 4 \right\}.$$

C'est un sous-groupe normal de Γ_2 d'indice 11520. Notons pour $i \in \mathcal{P}$ et $j = 1, 2, 3$,

$$\mathfrak{c}_i(\Omega) := \frac{\theta_i^2(\Omega)}{\theta_0^2(\Omega)} \qquad \text{et} \qquad \mathfrak{b}_j(\Omega) = \frac{\theta_j(\Omega/2)}{\theta_0(\Omega/2)}. \tag{3.13}$$

Les formules de duplication de la proposition 2.6.12 permettent d'écrire les fonctions $\mathfrak{c}_i$ en fonction des $\mathfrak{b}_j$. Inversement, on a les relations

$$\begin{array}{rcl} \mathfrak{b}_1 & = & (\mathfrak{c}_1 + \mathfrak{c}_9)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}, \\ \mathfrak{b}_2 & = & (\mathfrak{c}_2 + \mathfrak{c}_6)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}, \\ \mathfrak{b}_3 & = & (\mathfrak{c}_3 + \mathfrak{c}_{15})(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}. \end{array} \tag{3.14}$$

L'équation fonctionnelle des fonctions thêta montre que les fonctions $\mathfrak{b}_j$ et $\mathfrak{c}_i$ sont invariantes par le groupe $\Gamma_2(2,4)$. On a de plus

Théorème 3.4.5. *Le corps des fonctions modulaires invariantes par* $\Gamma_2(2,4)$ *est* $\mathbb{C}(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \mathbb{C}(\mathfrak{c}_1, \ldots, \mathfrak{c}_{15})$.

Démonstration. Voir [60, Théorème 1]. □

3.4.3 Utilisation de l'intégration numérique

Nous avons vu comment en appliquant les formules de Thomae on pouvait calculer les valeurs $\mathfrak{c}_j^2(\Omega) = \frac{\theta_j^4(\Omega)}{\theta_0^4(\Omega)}$ pour $j \in \mathcal{P}$ à partir d'une courbe C qui correspond à une variété abélienne principalement polarisée dont Ω est une représentation. Nous cherchons maintenant à obtenir les $\mathfrak{c}_j$ plutôt que les $\mathfrak{c}_j^2$ car nous allons voir que l'algorithme 3.6.1 nous permettra de déduire la matrice Ω des $\mathfrak{c}_j$, si Ω est dans le domaine fondamental. Bien entendu, une telle matrice peut être obtenue directement par intégration numérique, mais puisque c'est une opération coûteuse, nous cherchons à obtenir une complexité qui soit meilleure.

Rappelons qu'on peut prendre la base $A_1, \ldots, A_g$, $B_1, \ldots, B_g$ du groupe d'homologie $H_1(C, \mathbb{Z})$ comme dans la figure 2.1. Une base des 1-formes holomorphes est l'ensemble $\{\frac{x^j dx}{y}, j \in \{0, \ldots, g-1\}\}$. Si on pose

$$\Omega_0 = \left(\int_{A_j} \frac{x^{k-1} dx}{y} \right)_{j,k \in \{1,\ldots,g\}} \qquad \text{et} \qquad \Omega_1 = \left(\int_{B_j} \frac{x^{k-1} dx}{y} \right)_{j,k \in \{1,\ldots,g\}},$$

alors la matrice $\Omega_2 = \Omega_0^{-1}\Omega_1$ est dans $\mathcal{H}_g$ et correspond à la courbe C. Cette matrice Ω_2 dépend des bases choisies pour le groupe d'homologie et pour les 1-formes. Les intégrales qui apparaissent dans ces différentes matrices sont des *intégrales hyperelliptiques*. Il existe plusieurs algorithmes pour les calculer. Par exemple [17, 7, 65].

L'algorithme 3.4.1 permet d'obtenir les $\mathfrak{c}_j(\Omega)$ à partir des points de Weierstrass d'une courbe hyperelliptique de genre 2. L'idée consiste à utiliser tout de même l'intégration numérique mais à faible précision. On obtient ainsi une matrice qui va nous permettre de choisir la bonne racine carré de $\mathfrak{c}_j^2$ afin d'obtenir $\mathfrak{c}_j$.

Dans cet algorithme, seulement un nombre constant d'opérations se font à précision N. Toutes les autres, en nombre constant aussi, se font à faible précision. On en déduit une complexité en $O(\mathcal{M}'(N))$ (voir [19, Algorithme 12]).

Algorithme 3.4.1 : Évaluation des $\mathfrak{c}_j(\Omega)$ associés à une courbe

Entrée : Les racines $(e_1, \dots, e_6) \in \mathbb{C}^6$ d'une courbe hyperelliptique $C : Y^2 = \prod_{j=1}^{6}(X - e_j)$, $N \in \mathbb{N}$.

Sortie : $(\mathfrak{c}_j(\Omega))_{j\in\{1,\dots,15\}}$ à précision N, où $\Omega \in \mathcal{F}_2$ décrit la même variété que la courbe C.

1 Calculer la matrice Ω' associée à C par intégration numérique à faible précision en utilisant le même choix de base du groupe d'homologie que les formules de Thomae ;
2 Calculer γ et $\Omega \in \mathcal{F}_2$ tels que $\Omega = \gamma\Omega'$ par l'algorithme 3.1.2;
3 Calculer les $\mathfrak{c}_j^2(\Omega')$ par les formules de Thomae à précision N;
4 En déduire les $\mathfrak{c}_j^2(\Omega) = \mathfrak{c}_j^2(\gamma\Omega')$ par l'équation fonctionnelle;
5 Calculer les $\mathfrak{c}_j(\Omega)$ à faible précision à partir de la matrice Ω : on peut utiliser les définitions des thêta constantes comme séries de Fourier;
6 En déduire les $\mathfrak{c}_j(\Omega)$ à précision N en utilisant leurs approximations pour extraire la bonne racine carré de $\mathfrak{c}_j(\Omega)$;

3.5 Suites de Borchardt

3.5.1 Définition générale

On note $\mathcal{I}_g = (\mathbb{Z}/2\mathbb{Z})^g$. Soit $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$. On dit d'un 2^g-uplet $(b_v)_{v\in\mathcal{I}_g}$ de $\mathbb{C}^{2^g}$ qu'il est un *itéré de Borchardt* de $(a_v)_{v\in\mathcal{I}_g}$ s'il existe $(\alpha_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ tel que pour tout $v \in \mathcal{I}_g$:

$$\alpha_v^2 = a_v, \qquad \text{et} \qquad b_v = \frac{1}{2^g} \sum_{v_1+v_2=v} \alpha_{v_1}\alpha_{v_2}.$$

Le 2^g-uplet (α_v) est le *choix de racines* correspondant à cette itération de Borchardt. On dit de plus que c'est un *bon choix* si pour tous $v_1, v_2 \in \mathcal{I}_g$ on a

$$|\alpha_{v_1} - \alpha_{v_2}| < |\alpha_{v_1} + \alpha_{v_2}|.$$

Si ce n'est pas le cas, on parlera de *mauvais choix* de racines. Notons qu'il y a au plus 2^g choix de racines et que les choix $(\alpha_v)_{v\in\mathcal{I}_g}$ et $(-\alpha_v)_{v\in\mathcal{I}_g}$ conduisent au même itéré, ce qui fait au plus 2^{g-1} itérés possibles.

Définition 3.5.1. *Une suite $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est une* suite de Borchardt *associée à $(a_v^{(0)})_{v\in\mathcal{I}_g}$ si, pour tout $n \in \mathbb{N}$, $(a_v^{(n+1)})_{v\in\mathcal{I}_g}$ est un itéré de Borchardt de $(a_v^{(n)})_{v\in\mathcal{I}_g}$.*

Les suites AGM (vues à la section 1.6.1) correspondent au cas $g = 1$ des suites de Borchardt.

Théorème 3.5.2. *Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite Borchardt et soit $(\alpha_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de choix de racines associée. Alors il existe un unique $A \in \mathbb{C}$ tel que, pour tout $v \in \mathcal{I}_g$,*

$$\lim_{n\to\infty} a_v^{(n)} = A.$$

On appelle A la moyenne de Borchardt *de $(a_v^{(0)})_{v\in\mathcal{I}_g}$. On a que $A = 0$ si et seulement si la suite $(\alpha_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ contient une infinité de mauvaix choix de racines. Chacune des suites $(a_v^{(n)})_{n\in\mathbb{N}}$ converge quadratiquement vers sa limite A sauf si $A = 0$ auquel cas la convergence est, en général, linéaire.*

Démonstration. Voir [19, Théorème 7.1 et Page 164]. □

On dispose de quelques renseignements sur la position de A par rapport à $(a_v^{(n)})_{v\in\mathcal{I}_g}$ pour un n fixé :

$$|A| \leq \max_{v\in\mathcal{I}_g} |a_v^{(n)}|, \quad \Re(A) \geq \min_{v\in\mathcal{I}_g} (\Re(a_v^{(n)}))$$

$$\text{et} \qquad \min_{v\in\mathcal{I}_g}(\arg(a_v^{(n)})) \leq \arg(A) \leq \max_{v\in\mathcal{I}_g}(\arg(a_v^{(n)})).$$

L'archétype de ce type de suite est l'AGM associée à $a_0 = 1$ et $b_0 = 0$: on a alors $b_n = 0$ et $|a_n| = \frac{1}{2^n}$ pour tout n.

3.5.2 Une fonction associée à la moyenne de Borchardt

Soit $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$. On lui associe la suite de Borchardt $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ définie par $a_0^{(0)} = 1$, $a_v^{(0)} = z_v$ pour $v \in \mathcal{I}_g\setminus\{0\}$ et où on définit $(a_v^{(n)})_{v\in\mathcal{I}_g}$ par récurrence sur n en posant

$$a_0^{(n+1)} = \frac{1}{2^g}\sum_{v\in\mathcal{I}_g} a_v^{(n)} \quad \text{et} \quad a_v^{(n+1)} = \sum_{v_1+v_2=v} \alpha_{v_1}^{(n)}\alpha_{v_2}^{(n)},$$

où $\alpha_0^{(n)}$ est une racine carré quelconque de $a_0^{(n)}$ et pour tout $v \neq 0$, $\alpha_v^{(n)} = 0$ si $\alpha_0^{(n)} = 0$ ou si $a_v^{(n)} = 0$ et sinon c'est une racine carrée de $a_v^{(n)}$ telle que

$$|\alpha_0^{(n)} - \alpha_v^{(n)}| \leq |\alpha_0^{(n)} + \alpha_v^{(n)}|,$$

avec $\Im(\alpha_v^{(n)}/\alpha_0^{(n)}) > 0$ en cas d'égalité.

On note $B_g((z_v)_{v\in\mathcal{I}_g\setminus\{0\}})$ la limite de cette suite. Dans le cas $g = 1$, on a que B_1 est exactement la fonction M définie dans la définition 1.6.4.

Proposition 3.5.3. *Soit $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$ avec $\Re(z_v) > 0$ pour tout v. On note $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ la suite de Borchardt associée au calcul de $A = B_g((z_v)_{v\in\mathcal{I}_g\setminus\{0\}})$. Soit $N \geq 1$. On pose*

$$B(N,(z_v)) = \left\lceil \frac{\log(1-\frac{1}{2^g})}{\log\frac{m_0}{7\Delta_0}} \right\rceil + N + 1 + \left\lceil \log_2 \frac{M_0}{7m_0} \right\rceil,$$

où $\Delta_0 = \sum_{v_1,v_2\in\mathcal{I}_g} |a_{v_1}^{(0)} - a_{v_2}^{(0)}|$, $M_0 = \max_{v\in\mathcal{I}_g}(|a_v^{(0)}|)$ et $m_0 = \min_{v\in\mathcal{I}_g}\Re(a_v^{(0)})$. Alors $a_0^{B(N,(z_v))}$ est une approximation de $B_g((z_v))$ avec une précision relative de N bits.

Démonstration. Voir [19, Proposition 7.2]. □

Cette proposition justifie la validité de l'algorithme 3.5.1 ([19, Algorithme 11]) d'évaluation de B_g. On peut montrer qu'il suffit de travailler à précision $N + g\log_2(3)B(\log(N)+1,(z_v))$, ce qui implique que la complexité de cet algorithme est en

$$O(\mathcal{M}'(N + B(\log(N),(z_v)))B(\log(N),(z_v))),$$

pour g fixé. Si de plus (z_v) est fixé, alors $B(\log(N),(z_v)) = O(\log N)$. Cela reste vrai lorsque (z_v) varie mais que m_0 est minoré tandis que M_0 est majoré (ce qui permet de majorer Δ_0). Dans ces deux cas là, la complexité de l'algorithme est en

$$O(\mathcal{M}'(N)\log N).$$

Algorithme 3.5.1 : Évaluation de la moyenne de Borchardt B_g

Entrée : $N \in \mathbb{N}^*$ et $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$ tel que $\Re(z_v) > 0$ pour tout v.

Sortie : A tel que $\left|\frac{A}{B_g((z_v))} - 1\right| \leq 2^{-N}$.

$B = B(N+1, (z_v))$;
$a_0 = 1$;
pour $v \in \mathcal{I}_g\setminus\{0\}$ **faire**
    $a_v = z_v$;
fin
pour $n = 1$ **à** B **faire**
    pour $v \in \mathcal{I}_g$ **faire**
        $\alpha_v = \sqrt{a_v}$ tel que $\Re(\alpha_v) > 0$;
        $b_v = 0$;
    fin
    pour $v \in \mathcal{I}_g$ **faire**
        $b_0 = b_0 + a_v$;
        pour $v_1 \in \mathcal{I}_g$ **faire**
            $b_v = b_v + \alpha_{v_1}\alpha_{v+v_1}$;
        fin
    fin
    pour $v \in \mathcal{I}_g$ **faire**
        $a_v = b_v/2^g$;
    fin
fin
retourner a_0;

3.6 Applications de la moyenne de Borchardt

3.6.1 D'une courbe hyperelliptique de genre 2 à une matrice de $\mathcal{H}_2$

Il existe un lien étroit entre les thêta constantes et la moyenne de Borchardt. Soit $\Omega \in \mathcal{H}_2$. Considérons la suite

$$(a_n, b_n, c_n, d_n) = \left(\frac{\theta_j^2(2^n\Omega)}{\theta_0^2(\Omega)} \right)_{j\in\{0,1,2,3\}} \qquad \text{pour } n \in \mathbb{N}.$$

Elle converge vers $\frac{1}{\theta_0^2(\Omega)}$ d'après le lemme 2.6.13. Les formules de duplication (proposition 2.6.12) nous disent que c'est une suite de Borchardt. Si de plus Ω est dans le domaine fondamental alors la proposition 3.2.1 nous dit que pour tout $n \in \mathbb{N}$, $\Re(\theta_j(2^n\Omega)) > 0$ pour $j \in \{0,1,2,3\}$. Ainsi, cette suite est une suite de Borchardt où tous les choix de racines sont bons. On a donc montré

Proposition 3.6.1. *Pour tout $\Omega \in \mathcal{F}_2$, on a*

$$B_2(\mathfrak{c}_1(\Omega), \mathfrak{c}_2(\Omega), \mathfrak{c}_3(\Omega)) = \frac{1}{\theta_0^2(\Omega)}.$$

Démonstration. Voir aussi [19, Proposition 9.1]. □

On a vu dans l'algorithme 3.4.1 comment calculer les $\mathfrak{c}_j$ à partir d'une courbe hyperelliptique de genre 2. La proposition précédente nous permet d'avoir tous les carrés des thêta constantes car $\theta_j^2(\Omega) = \mathfrak{c}_j(\Omega)\theta_0^2(\Omega)$. La conjecture suivante (qui provient de [19, Conjecture 9.1]) nous permet alors de calculer Ω. Rappelons que les matrices $\mathfrak{M}_i$ sont définies dans l'équation (3.1).

Conjecture 3.6.2. *Pour tous $\Omega \in \mathcal{F}_2$ et $\gamma \in \{(\mathfrak{JM}_1)^2, (\mathfrak{JM}_2)^2, (\mathfrak{JM}_3)^2\}$,*

$$B_2(\mathfrak{c}_1(\gamma\Omega), \mathfrak{c}_2(\gamma\Omega), \mathfrak{c}_3(\gamma\Omega)) = \frac{1}{\theta_0^2(\gamma\Omega)}.$$

Cette conjecture dit que si on fait comme dans la proposition 3.6.1, alors tous les choix de racines sont bons.

On pose $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$. L'équation fonctionnelle montre que

$$(\mathfrak{c}_1((\mathfrak{JM}_1)^2\Omega), \mathfrak{c}_2((\mathfrak{JM}_1)^2\Omega), \mathfrak{c}_3((\mathfrak{JM}_1)^2\Omega)) = \left(\frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_6^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_2^2(\Omega)}{\theta_4^2(\Omega)} \right),$$

$$(\mathfrak{c}_1((\mathfrak{JM}_2)^2\Omega), \mathfrak{c}_2((\mathfrak{JM}_2)^2\Omega), \mathfrak{c}_3((\mathfrak{JM}_2)^2\Omega)) = \left(\frac{\theta_9^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_1^2(\Omega)}{\theta_8^2(\Omega)} \right),$$

$$(\mathfrak{c}_1((\mathfrak{JM}_3)^2\Omega), \mathfrak{c}_2((\mathfrak{JM}_3)^2\Omega), \mathfrak{c}_3((\mathfrak{JM}_3)^2\Omega)) = \left(\frac{\theta_8^2(\Omega)}{\theta_0^2(\Omega)}, \frac{\theta_4^2(\Omega)}{\theta_0^2(\Omega)}, \frac{\theta_{12}^2(\Omega)}{\theta_0^2(\Omega)} \right)$$

et que

$$\theta_0((\mathfrak{JM}_1)^2\Omega) = -\imath\Omega_1\theta_4^2(\Omega),$$
$$\theta_0((\mathfrak{JM}_2)^2\Omega) = -\imath\Omega_3\theta_8^2(\Omega),$$
$$\theta_0((\mathfrak{JM}_3)^2\Omega) = (\Omega_2^2 - \Omega_1\Omega_3)\theta_0^2(\Omega).$$

Algorithme 3.6.1 : Calcul de $\Omega \in \mathcal{F}_2$ à partir des $\mathfrak{c}_j(\Omega)$ ou des $\mathfrak{b}_i(\Omega)$

Entrée : $(\mathfrak{c}_j(\Omega))_{j\in\mathcal{P}} \in \mathbb{C}^{10}$ ou $(\mathfrak{b}_i(\Omega))_{i\in\{1,2,3\}} \in \mathbb{C}^3$.
Sortie : $\Omega \in \mathcal{F}_2$ tel que $\mathfrak{c}_j = \mathfrak{c}_j(\Omega)$ pour tout j et en supposant qu'une telle matrice existe.

1 Si on part des $\mathfrak{b}_i$, utiliser les formules de duplication pour en déduire les $\mathfrak{c}_j$;
2 $T_0 = B_2(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)^{-1}$;
3 **pour** $j \in \mathcal{P}$ **faire**
4 $\quad T_j = T_0\mathfrak{c}_j$;
fin
5 $\Omega_1 = \left(-\imath T_4 B_2\left(\frac{T_0}{T_4}, \frac{T_6}{T_4}, \frac{T_2}{T_4}\right)\right)^{-1}$;
6 $\Omega_3 = \left(-\imath T_8 B_2\left(\frac{T_9}{T_8}, \frac{T_0}{T_8}, \frac{T_1}{T_8}\right)\right)^{-1}$;
7 $a = \left(T_0 B_2\left(\frac{T_8}{T_0}, \frac{T_4}{T_0}, \frac{T_{12}}{T_0}\right)\right)^{-1}$;
8 $\Omega_2 = \sqrt{a + \Omega_1\Omega_3}$ tel que $\Im(\Omega_2) > 0$;
9 **retourner** $\left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right)$;

En supposant vraie la conjecture précédente, on peut déduire Ω des carrés des thêta constantes car alors :

$$\Omega_1 = \frac{\imath}{\theta_4^2(\Omega) B_2\left(\frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_6^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_2^2(\Omega)}{\theta_4^2(\Omega)}\right)}, \tag{3.15}$$

$$\Omega_3 = \frac{\imath}{\theta_8^2(\Omega) B2\left(\frac{\theta_9^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_1^2(\Omega)}{\theta_8^2(\Omega)}\right)}, \tag{3.16}$$

$$\Omega_2^2 - \Omega_1\Omega_3 = \frac{1}{\theta_0^2(\Omega) B_2\left(\frac{\theta_8^2(\Omega)}{\theta_0^2(\Omega)}, \frac{\theta_4^2(\Omega)}{\theta_0^2(\Omega)}, \frac{\theta_{12}^2(\Omega)}{\theta_0^2(\Omega)}\right)}, \tag{3.17}$$

et de plus, comme $\Omega \in \mathcal{F}_2$, la réduction de Minkowski implique que $\Im(\Omega_2) > 0$ ce qui nous permet de déterminer la bonne racine carré de Ω_2^2. On obtient ainsi la matrice Ω. On en déduit aussi la validité de l'algorithme 3.6.1, sous la conjecture 3.6.2.

La complexité de cet algorithme se ramène à la complexité de quatre moyennes de Borchardt. Elle est donc en $O(\mathcal{M}'(N)\log N)$ ([19, Algorithmes 13 et 14]).

Remarque 3.6.3. *La conjecture a été testée et vérifiée numériquement par Dupont pour plusieurs millions de matrices aléatoires. Nous soulignons le fait qu'il est facile de tester si une matrice Ω trouvée à la fin a les bons invariants d'Igusa ou pas.*

3.6.2 Deux variantes

Notons qu'il existe une variante (voir aussi [19, Pages 200-201] pour cette variante et la suivante) de l'algorithme 3.6.1 qui permet de s'affranchir de la conjecture 3.6.2, mais qui suppose l'utilisation d'une technique d'intégration numérique. Soit $\gamma \in \{(\mathfrak{JM}_1)^2, (\mathfrak{JM}_2)^2, (\mathfrak{JM}_3)^2\}$. Supposons que l'on connaisse les valeurs des $\mathfrak{c}_j(\gamma\Omega)$, $j \in \{1,2,3\}$, pour un certain $\Omega \in \mathcal{F}_2$, ainsi qu'une approximation de cet Ω

à faible précision. Les formules de duplication et la proposition 2.6.13 nous disent que la suite

$$\left(\frac{\theta_j^2(2^n\gamma\Omega)}{\theta_0^2(\gamma\Omega)}\right)_{j\in\{0,1,2,3\},n\in\mathbb{N}}$$

est une suite de Borchardt associée à $(1, \mathfrak{c}_1(\gamma\Omega), \mathfrak{c}_2(\gamma\Omega), \mathfrak{c}_3(\gamma\Omega))$ qui converge vers $\frac{1}{\theta_0^2(\gamma\Omega)}$. Pour pouvoir évaluer cette suite, on peut déterminer les choix de racines qui correspondent aux

$$\left(\frac{\theta_j(2^n\gamma\Omega)}{\theta_0(\gamma\Omega)}\right)_{j\in\{0,1,2,3\},n\in\mathbb{N}}$$

et ceci peut être fait en utilisant l'approximation de Ω qui nous permet d'évaluer les thêta constantes à faible précision. En tout, il est nécessaire d'en calculer qu'un nombre fini car les quatre suites convergent vers la même limite et donc à partir d'un moment les racines à prendre seront toutes situées dans un même quart de plan, ce qui permet d'extraire les bonnes racines. À Ω fixé, ces calculs à faible précision ne changent pas le coût asymptotique du calcul de Ω. On en déduit alors en utilisant cette variante et l'algorithme 3.2.1 qu'on peut trouver, à partir des points de Weierstrass d'une courbe hyperelliptique C de genre 2, une matrice $\Omega \in \mathcal{H}_2$ associée à C avec une précision N en temps

$$O(\mathcal{M}'(N)\log N).$$

On peut également choisir de s'affranchir dans l'algorithme 3.4.1 du calcul numérique d'intégrales hyperelliptiques mais en utilisant la conjecture 3.6.2. Supposons donc que l'on a les valeurs $\mathfrak{c}_j^2(\Omega')$ et qu'on cherche à calculer $\Omega \in \mathcal{F}_2$ qui soit équivalent à Ω'. On a vu que les $\mathfrak{c}_j^2$ sont des générateurs du corps des fonctions modulaires pour $\Gamma_2(2)$. Ainsi, l'ensemble

$$\{(\mathfrak{c}_j^2(\gamma\Omega'))_{j\in\{1,\dots,15\}} : \gamma \in \Gamma_2/\Gamma_2(2)\}$$

est calculable et de cardinal $[\Gamma_2 : \Gamma_2(2)] = 720$. Le vecteur $(\mathfrak{c}_j(\Omega))_{j\in\{1,\dots,15\}}$ est dans l'ensemble

$$\mathcal{B}(\Omega') = \{(\epsilon_j\mathfrak{c}_j(\gamma\Omega'))_{j\in\{1,\dots,15\}} : (\epsilon_j)_{j\in\{1,\dots,15\}} \in \{\pm 1\}^{15}, \gamma \in \Gamma_2/\Gamma_2(2)\}$$

qui est fini et explicitement calculable. Pour le déterminer dans cet ensemble, on peut procéder comme suit, à faible précision :

1. Poser $S = \mathcal{B}(\Omega')$;
2. Choisir un élément $(\beta_j)_{j\in\{1,\dots,15\}} \in S$;
3. Calculer un élément $t \in \mathcal{H}_g$ en utilisant l'algorithme 3.6.1 ;
4. Si $t \notin \mathcal{F}_2$, enlever (β_j) de S et retourner au point 2 ;
5. Sinon évaluer les $\mathfrak{b}_j(t)$;
6. Vérifier si les $\mathfrak{c}_j(t)$ correspondent aux β_j : si c'est le cas, alors on a bien $(\beta_j) = (\mathfrak{c}_j(t))$, sinon on enlève (β_j) de S et on retourne au point 2.

Cette variante ne change pas la complexité asymptotique du calcul de Ω, ni même du calcul des $\mathfrak{c}_j(\Omega)$ puisqu'elle ne fait intervenir qu'un nombre fini de calculs à faible précision. Notons que l'ensemble S du point 1 peut être réduit en utilisant les propositions 3.2.1 et 3.2.2.

Algorithme 3.6.2 : Évaluation des $\mathfrak{b}_j$ par la méthode des différences finies

Entrée : Une approximation flottante $y^{(n)} \in \mathbb{C}^3$ de $\Omega \in \mathcal{F}_2$ en précision $2N$ et une approximation $x^{(n)} \in \mathbb{C}^3$ de $f(\Omega)$ en précision N.

Sortie : Une approximation flottante $x^{(n+1)}$ de $f(\Omega)$ en précision $2N$.

1 Soit $\epsilon = 2^{-N} \max_j |x_j^{(n)}|$;

2 Soit (e_j) la base standard de $\mathbb{C}^3$. Calculer $F(x^{(n)})$ et $\frac{\Delta F}{\Delta x_j} = \frac{1}{\epsilon}(F(x^{(n)} + \epsilon e_j) - F(x^{(n)}))$ en utilisant l'algorithme 3.6.1;

3 Soit $J = (J_{i,j})_{i,j=1,2,3}$ avec $J_{i,j} = \frac{\Delta F_i}{\Delta x_j}$;

4 Soit $x^{(n+1)} = x^{(n)} - (F(x^{(n)}) - y^{(n)})J^{-1}$ où l'on voit les vecteurs comme des vecteurs ligne;

3.6.3 Algorithme rapide d'évaluation des thêta constantes

Une application importante des suites de Borchardt est qu'elles permettent d'obtenir un algorithme rapide pour le calcul des thêta constantes. Notons par

$$\begin{array}{rccc} F: & \mathbb{C}^3 & \longrightarrow & \mathbb{C}^3 \\ & (\mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega)) & \longmapsto & \Omega \end{array}$$

la fonction calculée par l'algorithme 3.6.1 et par

$$\begin{array}{rccc} f: & \mathcal{F}_2 & \longrightarrow & \mathbb{C}^3 \\ & \Omega & \longmapsto & (\mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega)) \end{array}$$

son inverse dans $\mathcal{F}_2$, où $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right)$ est interprétée comme un vecteur de $\mathbb{C}^3$.

On utilise la méthode des différences finies sur F pour calculer f, ce qui conduit à l'algorithme 3.6.2 qui provient de [29]. On peut trouver dans [19, Pages 212-216] le calcul de f par des itérations de Newton utilisant la matrice Jacobienne de F. Cette méthode est plus technique et d'après [29], elle est également plus lente que la première.

Une première approximation de $f(\Omega)$ peut être calculée en utilisant la définition des fonctions thêta en terme de série de Fourier : c'est l'algorithme 3.2.1. Les calculs sont faits à précision $2N$ bits. Bien entendu, aussi bien le calcul de la matrice Jacobienne par différences finies que la méthode de Newton elle-même engendrent des pertes de précisions.

Théorème 3.6.4 (Sous la conjecture 3.6.2)**.** *Soient $\Omega \in \mathcal{F}_2$ telle que $\theta_0(\Omega/2) \neq 0$, $x = f(\Omega)$ et $x^{(0)}$ une première approximation flottante de x. Sans prendre en compte les pertes de précision, il existe deux réels $\epsilon_0 > 0$ et $\delta > 0$, qui dépendent de x, tels que pour $||x^{(0)} - x|| < \epsilon_0$, la suite $x^{(n)}$ définies par des applications successives de l'algorithme 3.6.2 converge vers x avec une précision qui augmente à chaque pas de N à $2N - \delta$. Pour atteindre une précision N donnée, la complexité totale est dominée par la complexité de la dernière étape qui est*

$$O(\mathcal{M}'(N) \log N).$$

Démonstration. Voir [29, Théorème 12]. □

Chapitre 4

Polynômes modulaires de Siegel

Ce chapitre a pour but de définir les polynômes modulaires sur l'espace de Siegel et de décrire un algorithme de type évaluation/interpolation pour les calculer. Nous commençons par expliquer comment on interpole des fractions rationnelles multivariées, puis nous décrivons l'algorithme de Régis Dupont pour le calcul de ces polynômes avec les invariants d'Igusa. Cette thèse apporte une généralisation de cet algorithme à d'autres invariants, notamment les $\mathfrak{b}_i$ qui sont définis à l'équation 3.13. De plus, nous étudierons les propriétés des polynômes modulaires avec les $\mathfrak{b}_i$: nous prouverons l'existence de symétries, de relations modulo 4 entre les exposants des invariants dans les coefficients et décrirons des propriétés des dénominateurs des coefficients des polynômes. Les références pour ce chapitre sont [19, 85, 9]. En particulier, nous avons repris plusieurs preuves de [9].

4.1 Interpolation

Nous expliquons dans cette section comment interpoler des polynômes et des fractions rationnelles multivariées. En effet, on a besoin de savoir interpoler des fractions rationnelles trivariées pour calculer les différents polynômes modulaires par la méthode d'évaluation/interpolation. Le problème est le suivant : on suppose que l'on dispose d'un algorithme f qui renvoie une approximation flottante de la valeur $P(x_1, \ldots, x_n)$, pour tous $x_1, \ldots, x_n \in \mathbb{C}$, où P est une fraction rationnelle multivariée à coefficients complexes $P(X_1, \ldots, X_n)$ en n variables que l'on ne connaît pas. Le but est de calculer P.

On note $\mathcal{M}_N(d)$ la complexité de la multiplication de deux polynômes de degrés inférieurs ou égaux à d avec des coefficients de N bits. Par ailleurs, on note $\mathcal{M}'(N)$ la complexité de la multiplication de deux entiers de N bits. D'après [85, Corollaire 8.19], on a que $\mathcal{M}_N(d) \in O(d \log d \, \mathcal{M}'(N))$ si on utilise la FFT et si on suppose que $N \in \Omega(\log d)$, ce qui est nécessaire pour distinguer les différentes racines de l'unité utilisées dans la FFT. De plus, $\mathcal{M}'(N) \in O(N \log N \log\log N)$ (voir [78]).

Ce qui suit est basé sur des idées de [19]. On entre dans les détails et on fait une étude de la complexité.

4.1.1 Interpolation d'un polynôme multivarié

Le problème de l'interpolation d'un polynôme univarié P est bien connu et peut être résolu par les méthodes de Lagrange et de Newton qui nécessitent $\deg P + 1$ évaluations (appels à l'algorithme f de l'introduction de cette section). La complexité de l'interpolation rapide est en $O(\mathcal{M}_N(\deg(P))\log(\deg(P)))$ (voir [85, Corollaire 10.12]).

Dans le cas d'un polynôme bivarié $P(X,Y)$, on note qu'il peut être écrit sous les formes

$$P(X,Y) = \sum_{i=0}^{d_X} \left(\sum_{j=0}^{d_Y} c_{i,j} Y^j \right) X^i = \sum_{i=0}^{d_X} c_i(Y) X^i.$$

On peut calculer le polynôme univarié $P(X,y)$, pour y fixé, en évaluant $P(x_i,y)$ pour $i = 1,\ldots,d_X+1$ et puis en interpolant. Le ℓ-ième coefficient de ce polynôme est $c_\ell(y)$, qui est l'évaluation du polynôme univarié $c_\ell(Y)$ au point y. On a donc un algorithme pour évaluer ce polynôme et en l'appliquant sur d_Y+1 valeurs y_j, on peut en déduire les $c_\ell(Y)$ pour tout ℓ et par suite le polynôme bivarié $P(X,Y)$.

Reprenons. Pour interpoler $P(X,Y)$ on procède comme suit. Pour j de 1 à d_Y+1, on fixe une valeur y_j et on choisit d_X+1 valeurs x_i (il n'est pas gênant de prendre les mêmes x_i pour différents j), on évalue alors tous les $P(x_i,y_j)$ et on interpole pour obtenir le polynôme univarié $P(X,y_j)$. Enfin, pour $\ell = 0,\ldots,d_X$ on interpole $c_\ell(Y)$. Ainsi, pour pouvoir interpoler un polynôme bivarié, il nous faut $(d_X+1)(d_Y+1)$ évaluations et la complexité de l'interpolation est en

$$(d_Y+1)O(\mathcal{M}_N(d_X)\log(d_X)) + (d_X+1)O(\mathcal{M}_N(d_Y)\log(d_Y)) \subseteq \tilde{O}(d_X d_Y N).$$

L'interpolation d'un polynôme trivarié peut être faite de manière similaire. On écrit

$$P(X,Y,Z) = \sum_{i=0}^{d_X} \left(\sum_{j=0}^{d_Y} \left(\sum_{k=0}^{d_Z} c_{i,j,k} Z^k \right) Y^j \right) X^i$$

$$= \sum_{i=0}^{d_X} \left(\sum_{j=0}^{d_Y} c_{i,j}(Z^k) Y^j \right) X^i = \sum_{i=0}^{d_X} c_i(Y,Z) X^i.$$

Si, pour y et z fixés, on évalue $P(x_i,y,z)$ pour $i = 1,\ldots,d_X+1$ et qu'on interpole, on obtient le polynôme univarié $P(X,y,z)$ et son ℓ-ième coefficient est $c_\ell(y,z)$. Ceci nous fournit un algorithme d'évaluation du polynôme bivarié $c_\ell(Y,Z)$ en n'importe quels points. On peut donc appliquer ce qu'on a dit sur les polynomes bivariés pour calculer tous les $c_\ell(Y,Z)$ et en déduire P.

Détaillons. Pour j de 1 à d_Y+1 et pour k de 1 à d_Z+1, on évalue $P(x_i,y_j,z_k)$ pour d_X+1 valeurs x_i et puis on fait $(d_Y+1)(d_Z+1)$ interpolations pour obtenir tous les $P(X,y_j,z_k)$. Chacun des d_X+1 coefficients $c_\ell(Y,Z)$ est un polynôme bivarié et on a déjà donné la méthode et la complexité pour le calculer. En tout, on fait $(d_X+1)(d_Y+1)(d_Z+1)$ évaluations et la complexité de l'interpolation est

$$(d_Y+1)(d_Z+1)O(\mathcal{M}_N(d_X)\log(d_X)) + (d_X+1)(d_Z+1)O(\mathcal{M}_N(d_Y)\log(d_Y)) +$$

$$(d_X+1)(d_Y+1)O(\mathcal{M}_N(d_Z)\log(d_Z)) \subseteq \tilde{O}(d_X d_Y d_Z N).$$

On peut généraliser cet algorithme par récurrence sur le nombre de variables n du polynôme multivarié $P(X_1,\ldots,X_n)$. Le nombre d'évaluations est $\prod_{i=1}^{n}(d_{X_i}+1)$

et la complexité de l'interpolation d'un polynôme à n variables est

$$\sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(d_{X_j}+1)O(\mathcal{M}_N(d_{X_i})\log(d_{X_i}))\subseteq\tilde{O}(\prod_{i=1}^{n}d_{X_i}N).$$

Notons la symétrie entre les variables dans cette complexité. Elle indique que l'ordre des variables n'a pas d'importance.

4.1.2 Interpolation d'une fraction rationnelle multivariée

On commence par le cas univarié : $F(X)=\frac{A(X)}{B(X)}$, avec $A(X)=\sum_{i=0}^{d_X^A}a_iX^i\in\mathbb{C}[X]$ et $B(X)=\sum_{i=0}^{d_X^A}b_iX^i\in\mathbb{C}[X]$. On cherche la solution avec des degrés d_X^A et d_X^B minimaux. Chaque paire (A,B) est alors définie à une constante multiplicative près.

Soit $n=d_X^A+d_X^B+1$. Écrire $A(X)-F(X)B(X)=0$ induit un algorithme par algèbre linéaire : il suffit d'évaluer F en $n+1$ valeurs x_i et de trouver les coefficients a_i et b_i en résolvant le système linéaire

$$\begin{pmatrix}1 & x_1 & \dots & x_1^{d_X^A} & -F(x_1) & -F(x_1)\cdot x_1 & \dots & -F(x_1)\cdot x_1^{d_X^B}\\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & x_n & \dots & x_n^{d_X^A} & -F(x_n) & -F(x_n)\cdot x_n & \dots & -F(x_n)\cdot x_n^{d_X^B}\end{pmatrix}\cdot\begin{pmatrix}a_0\\ \vdots\\ a_{d_X^A}\\ b_0\\ \vdots\\ b_{d_X^B}\end{pmatrix}=\begin{pmatrix}0\\ \\ \vdots\\ \\ 0\end{pmatrix}.$$

Cette méthode est particulièrement facile à implanter mais elle a une mauvaise complexité. Une autre solution consiste à utiliser l'interpolation de Cauchy (voir [85, Section 5.8]) couplée avec l'algorithme d'Euclide rapide (voir [85, Section 11]), ce qui produit un algorithme de complexité $O(\mathcal{M}_N(n)\log(n))$. Le nombre d'évaluations est alors n.

Décrivons brièvement cette dernière méthode. Soient k et m tels que $\deg A<k$ et $\deg B\leq m-k$. Prenons $x_1,\dots,x_m\in\mathbb{C}$ et $y_i=F(x_i)$ pour $1\leq i\leq m$ et interpolons : on obtient un polynôme univarié f. On cherche des polynômes $r(X)$ et $t(X)$ tels que pour tout i, $r(x_i)=t(x_i)F(x_i)$; ceci implique ($r(x_i)=t(x_i)y_i=t(x_i)f(x_i)$ si et seulement si $r\equiv tf \bmod (X-x_i)$ pour tout i) et par le théorème des restes Chinois, c'est équivalent à avoir que $r\equiv tf \bmod g$, où $g=\prod_{i=1}^{m}(X-x_i)$.

On utilise alors l'algorithme d'Euclide étendu sur g et f. Soient r_j, s_j, t_j la j-ième ligne de cet algorithme où j est minimal tel que $\deg r_j<k$ (c'est-à-dire que $r_1=g, r_2=f, s_1=1, s_2=0, t_1=0, t_2=1$ et $r_\ell=gs_\ell+ft_\ell$ pour chaque ligne ℓ). Par le corollaire 5.18 de [85, Section 5.8], r_j et t_j vérifient $r_j(x_i)=t_j(x_i)y_i$ et $t_j(x_i)\neq 0$ pour tout i. Ainsi, il suffit de calculer cette ligne pour interpoler la fraction F et il est possible de ne calculer qu'une ligne par l'algorithme d'Euclide rapide (voir [85, Section 11] pour plus de détails).

On étudie maintenant le cas bivarié $F(X,Y)=\frac{A(X,Y)}{B(X,Y)}$, avec

$$A(X,Y)=\sum_{i=0}^{d_X^A}\sum_{j=0}^{d_Y^A}c_{i,j}^AX^iY^j=\sum_{i=0}^{d_X^A}c_i^A(Y)X^i\in\mathbb{C}[X,Y]$$

et similairement pour $B(X,Y)$. On pourrait bien entendu utiliser de l'algèbre linéaire, mais la complexité serait vraiment très mauvaise. On veut plutôt faire comme dans le cas des polynômes bivariés : fixer des valeurs y_j, calculer les fractions $F(X,y_j)$ et ensuite interpoler les coefficients comme des polynômes univariés en Y. Si $F(X,Y) \in \mathbb{Q}[X,Y]$, alors pour chaque fraction rationnelle trouvée, on peut forcer les numérateur et dénominateur à avoir un contenu égal à 1. Mais à cause de la constante multiplicative, cela ne va pas marcher comme le montre l'exemple suivant.

Exemple 4.1.1. *Supposons que l'on cherche* $F(X,Y) = \frac{3X^2Y^2+Y+2}{3XY+3}$ *et que l'on a trouvé* $F(X,1) = \frac{X^2+1}{X+1}$, $F(X,2) = \frac{12X^2+4}{6X+3}$, $F(X,3) = \frac{27X^2+5}{9X+3}$ *et aussi* $F(X,5) = \frac{75X^2+7}{15X+3}$. *Pour le plus grand coefficient du numérateur,* $c_2^A(Y)$, *si on interpole avec* $y_i = 2,3,5$, *ce qui nous donne* $c_2^A(y_i) = 12,27,75$, *on trouve* $3Y^2$ *ce qui est correct ; d'un autre côté, avec* $y_i = 1,2,3$ *donnant* $c_2(y_i) = 1,12,27$, *on obtient en interpolant le polynôme* $2Y^2 + 5Y - 6$, *qui est complètement faux. Cette erreur provient de la simplification entre le numérateur et le dénominateur dans le cas* $Y = 1$.

Remarque 4.1.2. *Pour quelques valeurs de* Y, *il y a une simplification par un polynôme. Par exemple,* $F(X,-5) = -5X - 1$. *Ceci est immédiatement détecté à cause du fait que les degrés en* X *se trouvent diminués. À chaque fois que cela arrive, on abandonne nos valeurs. On supposera dans la suite que cela n'arrive jamais.*

Dans l'exemple, si on avait fixé le coefficient de degré 0 du dénominateur de la fraction rationnelle univarié calculé à une certaine valeur (3 par exemple), la simplification n'aurait pas été un problème. Ce n'est pas vrai en général.

Exemple 4.1.3. *Cette fois-ci, on écrit* $F(X,1) = \frac{X^2+1}{X+1}$, $F(X,2) = \frac{3X^2+1}{\frac{3}{2}X+\frac{3}{4}}$, $F(X,3) = \frac{\frac{27}{5}X^2+1}{\frac{9}{5}X+\frac{3}{5}}$, *..., où on fixe toujours le coefficient de degré* 0 *du numérateur à* 1. *Alors on déduit par interpolation que* $c_0^A(Y) = 1$, *ce qui est faux. En effet, lorsque l'on divise par une constante pour obtenir le coefficient* 1, *c'est comme si on divisait par le polynôme* $Y + 2$.

La difficulté est donc qu'on doit normaliser tout en étant sûr que le i-ième coefficient du numérateur et du dénominateur de chaque fraction en X provient bien de l'évaluation du même polynôme en Y.

Cette normalisation est facile à obtenir dans le cas très particulier où un des coefficients $c_i^A(Y)$ ou $c_i^B(Y) \in \mathbb{C}[Y]$ non nul est connu : on doit juste multiplier la fraction trouvée par la constante qui donne la bonne évaluation pour le coefficient connu. On peut alors obtenir par l'interpolation de Cauchy la fraction avec en tout $n(d_Y + 1)$ évaluations. La complexité de l'interpolation est alors en

$$(d_Y + 1)O(\mathcal{M}_N(n)\log(n)) + (n+1)O(\mathcal{M}_N(d_Y)\log(d_Y)) \subseteq \tilde{O}(d_X d_Y N)$$

où $d_X = \max(d_X^A, d_X^B)$, $d_Y = \max(d_Y^A, d_Y^B)$ et $n = d_X^A + d_X^B + 1 \leq 2d_X + 1$.

Exemple 4.1.4. *On reprend l'exemple précédent. Supposons que l'on connaisse* $c_0^A(Y) = Y + 2$. *On a* $c_0^A(1) = 3$ *et au lieu de prendre la fraction* $\frac{X^2+1}{X+1}$ *comme précédemment, on prend plutôt* $\frac{3X^2+3}{3X+3}$. *On a aussi que* $c_0^A(2) = 4$ *et on écrit* $F(X,2) = \frac{12X^2+4}{6X+3}$, *etc.*

En général, une idée pour éviter la difficulté à laquelle on a fait allusion plus haut consiste à considérer la fraction $F'(X,Y) = F(X,YX) = \frac{A'(X,Y)}{B'(X,Y)}$ plutôt que $F(X,Y)$ car dans ce cas, on a toujours que $c_0^{B'}(Y)$ est une constante. Si elle n'est pas nulle, on peut choisir de la fixer à 1 et alors l'argument précédent (un coefficient connu) s'applique. Ensuite, en remplaçant Y par Y/X dans $F(X,YX)$ on obtient $F(X,Y)$. Puisque $d_X^{A'} = d_T^A$ et $d_X^{B'} = d_T^B$, où l'indice T désigne le degré total, la complexité est en $\tilde{O}(d_T d_Y N)$, où $d_T = \max(d_T^A, d_T^B)$.

Remarquons que dans le cas particulier où le coefficient de degré zéro de $c_0^B(Y)$ est 0, cette méthode ne fonctionne pas. Néanmoins, pour surmonter ce problème, on peut considérer $F(X+r, Y+s)$ au lieu de $F(X,Y)$ pour certaines valeurs r et s telles que ce coefficient ne soit pas nul.

On étudie maintenant le cas trivarié. On veut interpoler $F(X,Y,Z) = \frac{A(X,Y,Z)}{B(X,Y,Z)}$ avec $A(X,Y,Z)$ et $B(X,Y,Z)$ dans $\mathbb{C}[X,Y,Z]$. Notons $d_T = \max(d_T^A, d_T^B)$ et similairement pour d_X, d_Y et d_Z. Soit $n = d_T^A + d_T^B + 1$. Comme dans le cas bivarié, on calcule $F(X,XY,XZ)$ et ensuite en remplace Y par Y/X et Z par Z/X pour obtenir $F(X,Y,Z)$. Nous expliquons comment calculer $F(X,XY,XZ)$ récursivement.

1. Supposons que l'on soit capable de calculer $F(X,XY,zX)$ pour $z \in \mathbb{C}$ fixé. Alors on n'a besoin que de $d_Z + 1$ évaluations en z_i pour interpoler, comme des polynômes, chaque coefficient en Z et trouver $F(X,XY,XZ)$. Le nombre de coefficients est majoré par $(n+1)(d_Y+1)$ de telle sorte que la complexité de l'interpolation pour cette étape est en

$$(n+1)(d_Y+1)O(\mathcal{M}_N(d_Z)\log(d_Z));$$

2. Pour obtenir $F(X,XY,zX)$ pour un z fixé, il suffit d'appliquer l'algorithme d'interpolation dans le cas d'une fraction rationnelle bivariée. On applique cette étape $d_Z + 1$ fois. La complexité est alors

$$(d_Z+1)((d_Y+1)O(\mathcal{M}_N(n)\log(n)) + (n+1)O(\mathcal{M}_N(d_Y)\log(d_Y))).$$

En procédant ainsi, le nombre d'évaluations est de $n(d_Y+1)(d_Z+1)$ et la complexité totale de l'interpolation est en $\tilde{O}(d_T d_Y d_Z N)$. Dans le cas spécial où l'on connaît un des $c_i^A(Y,Z)$ ou $c_i^B(Y,Z)$, la complexité est en $\tilde{O}(d_X d_Y d_Z N)$.

Une amélioration de cet algorithme est obtenue en remarquant qu'il y a la possibilité de remplacer Y par Y/X dans la seconde étape pour trouver $F(X,Y,zX)$ et calculer $F(X,Y,XZ)$ dans la première. Ce faisant, le nombre de coefficients dans la première étape décroit et est majoré par $(n'+1)(d_Y+1)$ où n' est $\deg_X^A(F(X,Y,zX)) + \deg_X^B(F(X,Y,zX)) + 1 \leq n$, ce qui nous permet de réduire le nombre d'interpolations. La complexité est alors

$$(d_Y+1)(d_Z+1)O(\mathcal{M}_N(n)\log(n)) + (n+1)(d_Z+1)O(\mathcal{M}_N(d_Y)\log(d_Y)) +$$

$$(n'+1)(d_Y+1)O(\mathcal{M}_N(d_Z)\log(d_Z)) \subseteq \tilde{O}(d_T d_Y d_Z N).$$

On peut généraliser tout ceci récursivement pour traiter le cas des fractions rationnelles F ayant m variables $X_1, \ldots, X_m$. On trouve

$$O(\prod_{i=2}^{m}(d_{X_i}+1)\mathcal{M}_N(n)\log(n) + \sum_{j=2}^{m}\prod_{\substack{i=2\\ i\neq j}}^{m}(d_{X_i}+1)n(j)\mathcal{M}_N(d_{X_j})\log(d_{X_j}))$$

$$\subseteq \tilde{O}(d_T \prod_{i=2}^{m} d_{X_i} N),$$

où $n = d_T^A + d_T^B + 1$ et $n(j)$ est 1 plus le degré en X_1 du numérateur plus le degré en X_1 du dénominateur de $F(X_1, X_2, \ldots, X_{j-1}, X_j X_1, \ldots, X_m X_1)$.

Notons que, cette fois-ci, toutes ces formules de complexité pour les fractions rationnelles sont asymétriques. Le choix de l'ordre des variables est alors important. Les formules suggèrent qu'il est préférable de prendre X_1 comme la variable apparaissant avec le plus grand degré. Dans ce cas, on a que $n \leq 6d_{X_1} + 1$ et la complexité de l'interpolation est alors en $\tilde{O}(\prod_{i=1}^{m} d_{X_i} N)$.

4.2 Polynômes modulaires : définition et calcul

4.2.1 Polynômes modulaires avec les invariants d'Igusa

Soit Γ un sous-groupe de Γ_2 d'indice k. Notons par $\mathbb{C}_\Gamma$ le corps des fonctions modulaires de $\mathcal{H}_2$ invariantes sous l'action de Γ. C'est le corps de fonctions de $\mathcal{H}_2/\Gamma$. Cette définition est en accord avec la définition de $\mathbb{C}_{\Gamma_2}$ vue plus haut. D'après [32], $\mathbb{C}_\Gamma$ est une extension algébrique finie de degré k de $\mathbb{C}_{\Gamma_2}$.

Soit f une fonction modulaire sur Γ_2, $\gamma \in \Gamma_2$ et p un nombre premier. On définit la matrice γ_p et les fonctions f^γ, f_p et f_p^γ de $\mathcal{H}_2 \to \mathbb{C}$ par

$$f^\gamma(\Omega) = f(\gamma\Omega), \qquad f_p(\Omega) = f(p\Omega) \qquad \text{et} \qquad f_p^\gamma(\Omega) = f(p\gamma\Omega), \tag{4.1}$$

et on définit la matrice γ_p par

$$\gamma_p := \left(\begin{smallmatrix} A & pB \\ C/p & D \end{smallmatrix}\right). \tag{4.2}$$

Définition 4.2.1. *Pour tout entier $N \geq 1$, on note $\Gamma_0(N)$ le sous-groupe de Γ_2 défini par*

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2 : C \equiv 0 \bmod N \right\}.$$

Soit p un nombre premier. Pour tous $a, b, c \in \{0, \ldots, p-1\}$, on pose

$$T_1(a,b,c) = \begin{pmatrix} I_2 & 0 \\ a & b \\ b & c \end{pmatrix}, \qquad T_2(a,b,c) = \begin{pmatrix} 0 & -I_2 \\ & a \quad b \\ I_2 & b \quad c \end{pmatrix}$$

$$T_3(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & a \\ -a & 1 & 0 & 0 \end{pmatrix}, \qquad T_4 = \begin{pmatrix} -1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Proposition 4.2.2. *Pour tout nombre premier p, l'indice du sous-groupe $\Gamma_0(p)$ dans Γ_2 est*

$$[\Gamma_2 : \Gamma_0(p)] = p^3 + p^2 + p + 1.$$

De plus, un ensemble de représentants des classes (à droite) du quotient $\Gamma_2/\Gamma_0(p)$ est

$$\begin{array}{ll} & \{T_1(a,b,c) : (a,b,c) \in \{0,\ldots,p-1\}^3\} \\ \cup & \{T_2(a,b,c) : (a,b,c) \in \{0,\ldots,p-1\}^3 \text{ tels que } ac \equiv b^2 \bmod p\} \\ \cup & \{T_3(a) : a \in \{0,\ldots,p-1\}\} \\ \cup & \{T_4\}. \end{array}$$

Démonstration. Voir [19, Proposition 10.1]. □

Proposition 4.2.3. *Les trois fonctions* $\mathrm{j}_{\ell,p} := (\mathrm{j}_\ell)_p$ *(voir définition 3.3.1) sont invariantes sous l'action du groupe* $\Gamma_0(p)$.

En effet, si $\gamma \in \Gamma_0(p)$, alors $p\gamma\Omega = \gamma_p(p\Omega)$ et $\gamma_p \in \Gamma_2$, de telle sorte que $\mathrm{j}^\gamma_{\ell,p}(\Omega) = \mathrm{j}_\ell(p\gamma\Omega) = \mathrm{j}_\ell(\gamma_p(p\Omega)) = \mathrm{j}_\ell(p\Omega) = \mathrm{j}_{\ell,p}(\Omega)$. En d'autres termes, Ω est équivalent à $\gamma\Omega$ pour $\gamma \in \Gamma_2$, c'est-à-dire que Ω et $\gamma\Omega$ ont les mêmes invariants d'Igusa, mais cela ne signifie pas que $p\Omega$ soit équivalent à $p\gamma\Omega$: ce n'est le cas que lorsque γ est dans l'ensemble $\Gamma_0(p)$.

Notons C_p un ensemble de représentants des classes du quotient $\Gamma_2/\Gamma_0(p)$. Les matrices des périodes des variétés abéliennes principalement polarisées p-isogènes à une variété Ω donnée sont les $p\gamma\Omega$ pour $\gamma \in C_p$ (par [9, Théorème 3.2]).

Lemme 4.2.4. *On a une surjection entre* $\Gamma_2 = \mathrm{Sp}_4(\mathbb{Z})$ *et* $\mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z})$ *pour tout* N *entier.*

Démonstration. Voir [1, Lemme 3.2 page 123]. □

Proposition 4.2.5. *Pour un nombre premier* p, $\mathbb{C}_{\Gamma_0(p)}$ *est égal à* $\mathbb{C}_{\Gamma_2}(\mathrm{j}_{\ell,p})$ *pour* $\ell = 1, 2, 3$.

Démonstration. Nous reprenons la preuve de [9, Lemme 4.2]. On a vu que $\mathbb{C}_{\Gamma_2} = \mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ et que $\mathbb{C}_{\Gamma_0(p)}$ est une extension de $\mathbb{C}_{\Gamma_2}$ de degré $[\Gamma_2 : \Gamma_0(p)]$. les fonctions $\mathrm{j}_{\ell,p}$ sont dans $\mathbb{C}_{\Gamma_0(p)}$ par la proposition 4.2.3. Il suffit alors de montrer qu'à ℓ fixé, les fonctions $\mathrm{j}^\gamma_{\ell,p}$ pour $\gamma \in \Gamma_2/\Gamma_0(p)$ sont distinctes (tout comme pour le théorème 1.4.14). Si deux de ces fonctions sont égales, alors le stabilisateur $S \subseteq \Gamma_2$ de $\mathrm{j}_{\ell,p}$ dans Γ_2 contient strictement $\Gamma_0(p)$. Les images de S et de $\Gamma_0(p)$ sous l'application de réduction $\pi : \Gamma_2 \twoheadrightarrow \mathrm{Sp}_4(\mathbb{F}_p)$ vérifient alors $\pi(S) \supsetneq \pi(\Gamma_0(p))$. Le groupe $\pi(\Gamma_0(p))$ est le stabilisateur d'un sous-espace isotrope de $\mathrm{Sp}_4(\mathbb{F}_p)$ et est donc maximal, par [49, Théorème 4.2]. On en déduit que $\pi(S)$ est le groupe $\mathrm{Sp}_4(\mathbb{F}_p)$ et S est égal à Γ_2, ce qui est absurde. □

Notons que les fonctions j_ℓ ont des pôles en $\Omega \in \mathcal{H}_2$ tel que $h_{10}(\Omega) = 0$. Ceci arrive quand $\theta_i(\Omega) = 0$ pour un certain $i \in \mathcal{P}$. Par la proposition 3.2.3, si $\Omega' \in \mathcal{F}_2$ est équivalent à Ω, alors Ω' est diagonal. On en déduit que Ω correspond à un produit de courbes elliptiques. Ainsi, les fonctions $\mathrm{j}_{\ell,p}$ ont des pôles en les $\Omega \in \mathcal{H}_2$ correspondant aux variétés p-isogènes à un produit de courbes elliptiques.

Soit $\Phi_{1,p}(X) = \prod_{\gamma \in C_p}(X - \mathrm{j}^\gamma_{1,p})$. C'est le polynôme minimal de $\mathrm{j}_{1,p}$ sur $\mathbb{C}_{\Gamma_2}$. Comme les fonctions $\mathrm{j}_{2,p}$ et $\mathrm{j}_{3,p}$ sont contenues dans $\mathbb{C}_{\Gamma_2}(\mathrm{j}_{1,p}) = \mathbb{C}_{\Gamma_2}[\mathrm{j}_{1,p}]$ par la proposition 4.2.5, on définit $\Phi_{2,p}(X)$ et $\Phi_{3,p}(X)$ comme étant les polynômes unitaires dans $\mathbb{C}_{\Gamma_2}[X]$ ayant un degré inférieur ou égal à $\deg(\Phi_{1,p}(X))$ vérifiant $\mathrm{j}_{2,p} = \Phi_{2,p}(\mathrm{j}_{1,p})$ et $\mathrm{j}_{3,p} = \Phi_{3,p}(\mathrm{j}_{1,p})$.

De plus, on a pour $\ell = 2, 3$ que $\Phi_{\ell,p}(\mathrm{j}_{1,p}) = \Psi_{\ell,p}(\mathrm{j}_{1,p})/\Phi'_{1,p}(\mathrm{j}_{1,p})$ où

$$\Psi_{\ell,p}(X) = \sum_{\gamma \in C_p} j^\gamma_{\ell,p} \prod_{\gamma' \in C_p \setminus \{\gamma\}} (X - \mathrm{j}^{\gamma'}_{1,p}).$$

Du coup, on va plutôt considérer $\Psi_{\ell,p}(X)$ que $\Phi_{\ell,p}(X)$, car ils sont plus petits.

Définition 4.2.6. *Soit* p *un nombre premier. On appelle* $\Phi_{1,p}$, $\Psi_{2,p}$ *et* $\Psi_{3,p}$ *les* p*-polynômes modulaires pour* j_1, j_2 *et* j_3.

Proposition 4.2.7. *Pour tout nombre premier p, les p-polynômes modulaires sont dans l'anneau $\mathbb{Q}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[X]$.*

Démonstration. Voir [9, Théorème 5.2]. Rappelons que le premier polynôme modulaire est le polynôme minimal de $\mathrm{j}_{1,p}$ par rapport à l'extension $\mathbb{C}_{\Gamma_0(p)}/\mathbb{C}_{\Gamma_2} : \Phi_{1,p}$ est donc dans $\mathbb{C}(j_1, j_2, j_3)[X]$. Soit $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$. Posons $q_i = \exp(2\imath\pi\Omega_i)$. Alors d'après [9, Lemme 5.1], les invariants d'Igusa ont une série de Laurent en q_1, q_2 et q_3 avec des coefficients rationnels. Ce résultat peut être retrouvé en regardant la définition des invariants d'Igusa par les thêta constantes. On peut écrire

$$\Phi_{1,p} = \sum_{m \geq 0} \frac{\sum_{a,b,c} c_{m,a,b,c} \mathrm{j}_1^a \mathrm{j}_2^b \mathrm{j}_3^c}{\sum_{a,b,c} d_{m,a,b,c} \mathrm{j}_1^a \mathrm{j}_2^b \mathrm{j}_3^c} X^m$$

et il nous suffit de prouver que les coefficients des numérateurs et dénominateurs sont rationnels. On réécrit l'équation $\Phi_{1,p} = 0$ avec les séries de Laurent de j_1, j_2, j_3 et $\mathrm{j}_{1,p}$ et en regardant les termes de la forme $\alpha q_1^a q_2^b q_3^c$, on en déduit un système d'équations linéaires pour les coefficients $c_{m,a,b,c}$ et $d_{m,a,b,c}$. Sur les nombres complexes, ce système a une solution qui est unique. Mais comme les coeffients qui apparaissent sont rationnels, cette unique solution doit aussi être rationnelle. La preuve pour $\Psi_{2,p}$ et $\Psi_{3,p}$ est similaire. □

Pour un p-polynôme modulaire P, on notera, selon les cas, ce polynôme comme étant à une variable $P(X)$ ou à quatre $P(X, \mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$.

L'application évaluation $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3) \to \mathbb{C}$ qui envoie j_i vers $\mathrm{j}_i(\Omega)$ associe au polynôme modulaire P le polynôme $P(X, \mathrm{j}_1(\Omega), \mathrm{j}_2(\Omega), \mathrm{j}_3(\Omega))$ dans $\mathbb{C}[X]$. L'intérêt de $\Phi_{1,p}$ est que les racines de son évaluation en $\Omega \in \mathcal{H}_2$ sont les j_1-invariants des surfaces abéliennes principalement polarisées qui sont p-isogènes à la variété Ω. De plus, si x est une telle racine, alors $(x, \Phi_{2,p}(x), \Phi_{3,p}(x))$ sont les invariants d'Igusa d'une surface abélienne principalement polarisée qui est p-isogène à la variété qui a pour invariants d'Igusa ($\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$, $\mathrm{j}_3(\Omega)$).

Notons $\mathcal{L}_p$ le lieu de toutes les surfaces abéliennes principalement polarisées qui sont p-isogènes à un produit de courbes elliptiques. Ce lieu $\mathcal{L}_p$ est une sous-variété algébrique de dimension 2 de l'espace de modules tridimensionel $\mathcal{H}_2/\Gamma_2$ et peut être paramétrisé par une équation $L_p = 0$ pour un polynôme L_p dans $\mathbb{Q}[\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3]$.

Lemme 4.2.8. *Les dénominateurs des coefficients de $\Phi_{1,p}(X)$, $\Psi_{2,p}(X)$ et $\Psi_{3,p}(X)$ sont tous divisibles par le polynôme L_p.*

Démonstration. Voir [9, Lemme 6.2]. Soit $\Omega \in \mathcal{H}_2$ tel qu'il existe une p-isogénie vers un produit de courbes elliptiques et soit c un coefficient de $\Phi_{1,p}$. Pour un certain $\gamma \in \Gamma_2/\Gamma_0(p)$, la valeur $\mathrm{j}_{1,p}(\gamma\Omega)$ est infinie car les fonctions j_i ont des pôles aux produits de courbes elliptiques (proposition 3.2.3). L'évaluation de c au point Ω est une expression symétrique en les $\mathrm{j}_{1,p}(\gamma'\Omega)$ et génériquement, il n'y a pas de relation algébrique entre ces valeurs ; l'évaluation de c en Ω est donc infinie. Mais puisque $\mathrm{j}_i(\Omega)$ est fini, le numérateur de c l'est également et c'est donc son dénominateur qui s'annule en Ω. On en déduit que c est divisible par L_p. On peut faire une preuve similaire pour $\Psi_{2,p}$ et $\Psi_{3,p}$. □

Nous donnons un algorithme pour déduire d'un triplet $(x, y, z) \in \mathbb{C}^3$ les dix $\mathfrak{c}_i(\Omega)$, où $\Omega \in \mathcal{F}_2$ est tel que $(\mathrm{j}_1(\Omega), \mathrm{j}_2(\Omega), \mathrm{j}_3(\Omega)) = (x, y, z)$. Ceci peut être fait en quatre étapes.

Algorithme 4.2.1 : Calcul de Ω à partir de $(\mathfrak{j}_1(\Omega), \mathfrak{j}_2(\Omega), \mathfrak{j}_3(\Omega))$

Entrée : $(x, y, z) = (\mathfrak{j}_1(\Omega), \mathfrak{j}_2(\Omega), \mathfrak{j}_3(\Omega))$ pour un certain $\Omega \in \mathcal{F}_2$ inconnu, une précision N.

Sortie : $\Omega \in \mathcal{H}_2$.

1 Utiliser l'algorithme de Mestre pour obtenir une courbe hyperelliptique $Y^2 = f(X)$ à précision N;
2 Déduire les dix $\mathfrak{c}_i(\Omega)$ à précision N en utilisant une technique d'intégration numérique à faible precision (algorithme 3.4.1);
3 Utiliser la proposition 3.6.1 pour obtenir le carré des thêta constantes à précision N;
4 Appliquer (3.15), (3.16), (3.17) pour calculer Ω à la précision ambiante, avec quelques pertes (algorithme 3.6.1).

1. La première consiste à utiliser l'algorithme de Mestre à précision N pour trouver l'équation d'une courbe hyperelliptique $Y^2 = f(X)$ sur $\mathbb{C}$ avec f de degré 6 dont les invariants d'Igusa sont (x, y, z) ;
2. Une fois que l'on a f, il est facile de déduire l'ensemble E des racines de f à précision N et à partir de cet ensemble, on applique les formules de Thomae pour obtenir les puissances quatrièmes des thêta constantes à partir d'un ordonnancement des racines de f, ordonnancement qui correspond à un choix de la base du groupe d'homologie de la courbe hyperelliptique.

   Le problème ici est que les fonctions $\mathfrak{c}_i$ ne sont pas invariantes sous l'action du groupe symplectique Γ_2, mais sous le sous-groupe $\Gamma_2(2)$. Ceci signifie que pour deux matrices des périodes équivalentes sous l'action de Γ_2 (en d'autres termes, avec les mêmes invariants d'Igusa), l'évaluation des $\mathfrak{c}_i$ en ces matrices peut produire des résultats différents. Plus exactement, pour deux telles matrices des périodes Ω_1 et Ω_2, il existe une matrice γ dans $\Gamma_2/\Gamma_2(2)$ telle que $\mathfrak{c}_i(\Omega_1) = \mathfrak{c}_i(\gamma\Omega_2)$ pour tout $i \in \mathcal{P}$. Ainsi, les thêta constantes trouvées avec les formules de Thomae nous donnent $\mathfrak{c}_i^2(\gamma\Omega)$ pour un certain $\gamma \in \Gamma_2/\Gamma_2(2)$;
3. Utilisons maintenant une technique d'intégration numérique à petite précision N' avec le même choix de la base du groupe d'homologie que les formules de Thomae pour trouver la matrice des périodes $\gamma\Omega$ que l'on réduit dans le domaine fondamental pour obtenir Ω, à précision N', et γ. On calcule $\mathfrak{c}_i(\Omega)$ à faible précision (avec l'algorithme 3.2.1 par exemple). On pourrait utiliser l'intégration numérique à la précision ambiante N mais alors la complexité de l'algorithme empirerait ;
4. Appliquer l'équation fonctionnelle de la proposition 2.6.4 sur les $\mathfrak{c}_i^2(\gamma\Omega)$ avec la matrice γ^{-1} permet d'obtenir les $\mathfrak{c}_i^2(\Omega)$ à précision N ; et connaître $\mathfrak{c}_i(\Omega)$ à faible précision est suffisant pour déduire les bonnes racines carrés et obtenir les $\mathfrak{c}_i(\Omega)$ à précision N.

Hypothèse 4.2.9. *Notons que l'on fait l'hypothèse que l'intégration numérique fournit un $\gamma\Omega$ avec γ suffisamment petit tel que $\gamma\Omega$ peut être correctement réduit dans le domaine fondamental à faible précision.*

On obtient ainsi l'algorithme 4.2.1. La seconde étape est l'algorithme 3.4.1 et les troisième et quatrième sont l'algorithme 3.6.1. Ils ont complexité $O(\mathcal{M}'(N))$

et $O(\mathcal{M}'(N)\log(N))$ (où $\mathcal{M}'(N)$ est la complexité pour multiplier deux entiers de N bits). Au total, cet algorithme est en $\tilde{O}(N)$.

4.2.2 Définition plus générale

Dans cette section, nous donnons une définition plus générale des p-polynômes modulaires en utilisant d'autres invariants que les invariants d'Igusa. C'est l'analogue de ce qui est fait en dimension 1 (voir les travaux de Schläfli [76] et de Weber [87] et/ou [25, Section 4.2 et 4.3] ou alors la section 1.6.3).

On ne considère que les sous-groupes de congruence $\Gamma \subseteq \Gamma_2$, c'est-à-dire les groupes qui vérifient $\Gamma_2(N) = \{M \in \Gamma_2 : M \equiv I_4 \bmod N\} \subseteq \Gamma$ pour un certain entier N. Si N est minimal avec cette propriété, on dit que N est le *niveau* de Γ. Soient donc Γ un sous-groupe de congruence et f_1, f_2, f_3 trois fonctions modulaires qui sont des générateurs pour le corps de fonctions de $\mathcal{H}_2/\Gamma$. Soit p un nombre premier qui est premier avec le niveau de Γ et C_p un ensemble de représentants des classes de $\Gamma/(\Gamma \cap \Gamma_0(p))$.

Définition 4.2.10. *Les p-polynômes modulaires pour ces données sont, pour* $\ell = 2, 3$,

$$\Phi_{1,p}(X) = \prod_{\gamma \in C_p} (X - f_{1,p}^{\gamma}) \qquad \text{et} \qquad \Psi_{\ell,p}(X) = \sum_{\gamma \in C_p} f_{\ell,p}^{\gamma} \prod_{\gamma' \in C_p \setminus \{\gamma\}} (X - f_{1,p}^{\gamma'}).$$

On écrira parfois $\Phi_{1,p}(X, f_1, f_2, f_3)$ et parfois $\Phi_{1,p}(X)$ et similairement pour $\Psi_{\ell,p}(X)$. Tandis que la phase d'interpolation reste inchangée, la phase d'évaluation, elle, est légèrement différente. En effet, cette fois-ci, il nous faut trouver une matrice des périodes $\Omega \in \mathcal{H}_2$ à partir d'un triplet $(x_1, x_2, x_3) \in \mathbb{C}$ telle que $f_i(\Omega) = x_i$. Bien sûr, cette étape dépend des trois générateurs, mais nous allons tout de même donner un algorithme général. D'un autre côté, les calculs de $\Phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et de $\Psi_{\ell,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$, pour un certain Ω, ne changent pas : on peut appliquer les mêmes algorithmes et ces calculs ont donc la même complexité, excepté, éventuellement, celle qui provient de l'évaluation des fonctions f_i.

Tout comme dans le cadre de la dimension 1, on cherche des invariants qui produisent les polynômes les plus petits possibles. Ceux produits par les invariants d'Igusa étant particulièrement gros.

Les premiers invariants que nous avons essayés sont les invariants de Streng (définition 3.3.2). Ceci est justifié par le fait que dans sa thèse, Streng les a utilisés avec succès pour obtenir des polynômes de classes plus petits que ceux trouvés avec les invariants d'Igusa. Ces invariants sont définis de telle sorte que l'exposant de h_{10} dans le dénominateur soit le plus petit possible.

Notons que les équations (3.4) et (3.5) nous disent que tous les résultats de la section précédente avec les invariants d'Igusa sont également vrais avec les invariants de Streng et que donc on peut appliquer le même algorithme. L'unique différence se situe dans l'obtention d'une matrice $\Omega \in \mathcal{H}_2$ (modulo Γ_2) à partir d'un triplet $(\mathfrak{i}_1(\Omega), \mathfrak{i}_2(\Omega), \mathfrak{i}_3(\Omega))$, où il nous faut ajouter une étape : à partir d'un tel triplet, il nous faut utiliser les équations (3.5) pour en déduire le triplet $(\mathfrak{j}_1(\Omega), \mathfrak{j}_2(\Omega), \mathfrak{j}_3(\Omega))$ et ensuite on peut appliquer l'algorithme 4.2.1. D'après l'équation (3.4), le calcul de $\mathfrak{i}_\ell(\Omega)$ a la même complexité que le calcul de $\mathfrak{j}_\ell(\Omega)$. Ainsi, la complexité du calcul des polynômes modulaires avec les invariants de Streng est exactement la même que celle du calcul des polynômes avec les invariants d'Igusa.

Toutefois, on constate (voir section 4.3) que les polynômes avec les invariants de Streng sont plus petits en termes de degrés et de taille des coefficients. Les calculs sont donc faits à une précision plus petite et l'étape d'interpolation est plus rapide. Le nombre d'appels à l'algorithme 4.2.1 est diminué.

Rappelons que les invariants d'Igusa et de Streng sont définis à partir de sommes et produits de quotients de thêta constantes. Ainsi, les fonctions $\mathfrak{r}_i$ et $\mathfrak{b}_i$, pour $i = 1, 2, 3$, définies dans la section 3.4.2 produisent potentiellement des polynômes plus petits. C'est effectivement le cas. Dans la suite, nous allons nous concentrer sur les $\mathfrak{b}_i$ qui donnent les meilleurs polynômes que nous avons obtenus.

Nous avons donc trois invariants $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{b}_3$ qui engendrent le corps des fonctions modulaires invariantes par

$$\Gamma_2(2,4) = \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2 : \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv I_4 \bmod 2 \text{ et } B_0 \equiv C_0 \equiv 0 \bmod 4 \right\},$$

qui est un sous-groupe normal de Γ_2 d'indice 11520 et de niveau 4. Notons que nous utilisons les invariants $\mathfrak{b}_i$ plutôt que $\mathfrak{c}_i$ car ces derniers sont au nombre de 10 tandis que les premiers au nombre de trois.

Proposition 4.2.11. *Soit $p > 2$ un nombre premier. Les classes de $\Gamma_2(2,4)/(\Gamma_0(p) \cap \Gamma_2(2,4))$ sont en bijection avec les classes de $\Gamma_2/\Gamma_0(p)$.*

Démonstration. Considérons l'application $\phi : \Gamma_2(2,4) \to \Gamma_2/\Gamma_0(p)$ de noyau $\Gamma_0(p) \cap \Gamma_2(2,4)$. La surjectivité provient du théorème des restes Chinois et du fait que $\mathrm{Sp}_4(\mathbb{Z}) \to \mathrm{Sp}_4(\mathbb{Z}/4p\mathbb{Z})$ est surjectif. □

Pour $p = 2$, on a que $(\Gamma_0(p) \cap \Gamma_2(2,4)) = \Gamma_2(2,4)$ ce qui justifie que le nombre premier p doit être premier au niveau du sous-groupe considéré dans la définition des polynômes modulaires.

Proposition 4.2.12. *Pour un nombre premier $p > 2$, $\mathbb{C}_{\Gamma_2(2,4)\cap\Gamma_0(p)}$ est égal à $\mathbb{C}_{\Gamma_2(2,4)}(\mathfrak{b}_{i,p})$ pour tout $i = 1, 2, 3$.*

Démonstration. La preuve est similaire à celle de la proposition 4.2.5. On doit utiliser l'isomorphisme entre $\Gamma_2(2,4)/(\Gamma_2(2,4) \cap \Gamma_2(p))$ et $\Gamma_2/\Gamma_2(p)$ qui provient du theorème des restes Chinois et de la surjectivité de $\mathrm{Sp}_4(\mathbb{Z}) \to \mathrm{Sp}_4(\mathbb{Z}/4p\mathbb{Z})$. □

Proposition 4.2.13. *Les p-polynômes modulaires pour les invariants $\mathfrak{b}_1$, $\mathfrak{b}_2$ et $\mathfrak{b}_3$ sont dans l'anneau $\mathbb{Q}(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3)[X]$. Plus généralement, ceci est le cas avec tous les invariants qui sont définis à partir des thêta constantes.*

Démonstration. Cette propriété provient du fait que, pour tout $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right)$, les fonctions $\mathfrak{b}_1, \mathfrak{b}_2$ et $\mathfrak{b}_3$ ont un développement en série de Laurent en $q_i = \exp(2\imath\pi\Omega_i)$ avec des coefficients rationnels. On conclut avec une preuve similaire à celle de la proposition 4.2.7. □

On veut pouvoir déduire Ω de $(\mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega)) = (x_1, x_2, x_3)$. La première chose à faire est de déduire de (x_1, x_2, x_3) les invariants d'Igusa de Ω. Ceci peut être fait facilement en utilisant les formules de duplication de la proposition 2.6.12 pour obtenir les 10 $\mathfrak{c}_i(\Omega)$ et en utilisant la définition des invariants d'Igusa (définition 3.3.1). On utilise alors l'algorithme 4.2.1 pour déduire une matrice des périodes $\Omega' \in \mathcal{H}_2$ à partir de ces invariants d'Igusa. Notons qu'on pourrait aussi déduire les invariants de Rosenhain $\mathfrak{r}_i$ à partir des $\mathfrak{c}_i$ (ou des $\mathfrak{b}_i$), desquels on déduit l'équation d'une courbe hyperelliptique de genre 2 et de degré 6 que l'on peut utiliser dans

l'algorithme 4.2.1. Malheureusement, dans les deux cas, la matrice Ω' que l'on obtient est équivalente à Ω dans le sens où elles ont les mêmes invariants d'Igusa, mais ceci ne signifie pas que $\mathfrak{b}_i(\Omega') = x_i$ parce que les fonctions $\mathfrak{b}_i$ sont invariantes pour le groupe $\Gamma_2(2,4)$ et non pas Γ_2.

Pour pallier cette difficulté, il faut considérer les classes du quotient $\Gamma_2/\Gamma_2(2,4)$. Pour trouver la bonne matrice Ω modulo $\Gamma_2(2,4)$, on peut prendre tous les représentants γ des classes du quotient et évaluer les trois $\mathfrak{b}_i(\gamma\Omega')$ à faible précision. Le triplet le plus proche de (x_1, x_2, x_3) nous donne la bonne matrice γ et ensuite on utilise l'équation fonctionnelle des thêta constantes pour obtenir $\mathfrak{b}_i(\gamma\Omega') = \mathfrak{b}_i(\Omega)$ à la précision courante N. Le problème de cette méthode est que l'indice de $\Gamma_2(2,4)$ dans Γ_2 est 11520 ce qui est grand et par suite cette méthode est lente. Nous proposons donc une autre méthode, plus complexe, certes, mais plus efficace.

Cette solution consiste à précalculer l'action sur les thêta constantes (permutations et constantes) de l'ensemble des représentants de $\Gamma_2/\Gamma_2(2,4)$ en utilisant l'équation fonctionnelle et en comparant les trois $\mathfrak{b}_i(\Omega)$ avec les trois $\mathfrak{b}_i(\Omega')$ pour en déduire l'action et par suite le représentant γ qui correspond à cette action, ce qui nous permet d'avoir $\gamma\Omega' = \Omega$. Ici, le temps passé sur chaque représentant est négligeable.

Exemple 4.2.14. *Nous donnons un exemple de ce que l'on appelle par action. Soit la matrice*

$$\gamma = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

En utilisant l'équation fonctionnelle, on trouve que

$$\theta_0^2(\gamma\cdot\Omega) = \zeta_\gamma^2 \det(...)\theta_6^2(\Omega), \quad \textit{que} \quad \theta_2^2(\gamma\cdot\Omega) = \imath\zeta_\gamma^2 \det(...)\theta_{12}^2(\Omega),$$

ou alors que

$$\theta_{15}^2(\gamma\cdot\Omega) = -\zeta_\gamma^2 \det(...)\theta_{15}^2(\Omega).$$

En oubliant les facteurs $\zeta_\gamma^2 \det(...)$ qui disparaissent lorsqu'on passe au quotient, on peut écrire l'action de γ sous la forme de deux tableaux : $[6,2,12,8,3,9,4,0,1,15]$, *qui est une bijection de $\mathcal{P}$, et* $[1,1,\imath,\imath,\imath,-1,1,1,\imath,-1]$.

Détaillons. On connaît les trois $\mathfrak{b}_i(\Omega)$, donc aussi les dix $\mathfrak{c}_i(\Omega)$, plus Ω' à la précision N. Notre but est de trouver une matrice $\gamma \in \Gamma_2$ telle que $\gamma\Omega' = \Omega$. On calcule les dix $\mathfrak{c}_i(\Omega')$. L'équation fonctionnelle des thêta constantes nous dit que

$$\theta_k^2(\gamma\Omega') = \zeta_\gamma^2 \det(...)\imath^{\epsilon(\gamma,k)}\theta_\ell^2(\Omega'),$$

avec $\epsilon(\gamma,k) \in \{0,1,2,3\}$, et comme les $\mathfrak{c}_i$ sont des quotients de thêta constantes, on peut oublier les facteurs ζ_γ^2 et $\det(...)$. On dira ici que l'action de γ envoie l'indice k vers l'indice ℓ. Dans le cas où 0 est envoyé vers 0, alors les ensembles A des dix $\mathfrak{c}_i(\Omega) = \mathfrak{c}_i(\gamma\Omega')$ et B des dix $\mathfrak{c}_i(\Omega')$ sont égaux à permutation et à une racine quatrième de l'unité près. Il est alors facile de comparer ces ensembles pour en déduire l'action de la matrice γ. Lorsque 0 n'est pas envoyé vers 0, les choses se corsent. Dans ce cas, $\mathfrak{c}_i(\gamma\Omega')$ pour $i \in \mathcal{P}$ s'écrit comme une racine de l'unité fois un quotient de carrés de thêta constantes évaluées en Ω'. Cependant, notons qu'il existe $c \in \mathcal{P}$ tel que c est envoyé sur 0 et un $d \in \mathcal{P}$ tel que 0 est envoyé sur d. On a alors

$$\mathfrak{c}_c(\gamma\Omega') = \imath^{\epsilon(\gamma,c)-\epsilon(\gamma,0)}\, \mathfrak{c}_d(\Omega')^{-1}$$

et en comparant A et B à une racine quatrième de l'unité près, il est possible de trouver $\mathfrak{c}_d(\Omega')$. On a alors

$$\mathfrak{c}_k(\gamma\Omega') = \imath^{\epsilon(\gamma,k)-\epsilon(\gamma,0)}\frac{\theta_\ell^2(\Omega')}{\theta_n^2(\Omega')} = \imath^{\epsilon(\gamma,k)-\epsilon(\gamma,0)}\mathfrak{c}_\ell(\Omega')\mathfrak{c}_d(\Omega')^{-1}$$

et il suffit de multiplier l'ensemble A par $\mathfrak{c}_d(\Omega')^{-1}$ et comparer ce nouvel ensemble avec B pour déduire l'action de γ.

Cette méthode peut aussi être utilisée pour modifier l'étape 2 de l'algorithme 4.2.1. En effet, dans le cas où ne peut pas choisir la base du groupe d'homologie pour l'intégration numérique, on obtient une matrice Ω à faible précision, mais on ne connaît pas la matrice γ telle que $\gamma\Omega$ est la matrice des périodes provenant des formules de Thomae. Comme expliqué plus haut, en comparant $\mathfrak{c}_i(\Omega)$ à faible précision et $\mathfrak{c}_i(\gamma\Omega)$ à la précision courante N, on peut tout de même déduire $\mathfrak{c}_i(\Omega)$ à précision N.

C'est ce qu'on a fait en pratique car on a utilisé le code de Pascal Molin (voir [65]) pour l'intégration numérique et on a d'ailleurs remarqué que ce code, une fois données les six racines de la courbe hyperelliptique, renvoie une matrice des périodes de la forme $\gamma''\Omega''$, où $\Omega'' \in \mathcal{F}_2$ et γ'' semble toujours avoir $-1, 0, 1$ comme coefficients. Ainsi, nous n'avons jamais eu de problème avec la réduction dans le domaine fondamental de $\gamma''\Omega''$ (nous rappelons l'hypothèse 4.2.9).

4.2.3 Analyse de la complexité

Soient f_1, f_2, f_3 trois fonctions modulaires pour un sous-groupe de congruence Γ de Γ_2 qui génèrent le corps de fonctions de $\mathcal{H}_2/\Gamma$. Soient p un nombre premier qui est premier au niveau de Γ et C_p un ensemble de représentants de $\Gamma/(\Gamma \cap \Gamma_0(p))$. On a décrit précédemment une procédure pour trouver Ω à partir de $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ à travers l'exemple des fonctions $\mathfrak{b}_i$ et on doit ensuite évaluer les p-polynômes modulaires pour un nombre premier p en Ω, ce qui signifie que l'on doit calculer pour $\ell = 2, 3$:

$$\Phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega)) \qquad \text{et} \qquad \Psi_{\ell,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$$

(et chacun des coefficients de ces polynômes dans $\mathbb{C}[X]$ est l'évaluation en Ω d'une fonction rationnelle trivariée en f_1, f_2, f_3 que l'on doit interpoler). Pour ce faire, on doit d'abord calculer $f_{\ell,p}^{\gamma}(\Omega)$, pour tous $\gamma \in C_p$ et $\ell = 1, 2, 3$. Soit $q = p^3 + p^2 + p + 1$ le degré de $\Phi_{1,p}(X)$. L'évaluation de $\Phi_{1,p}(X)$ en Ω peut être obtenue en $O(\mathcal{M}_N(q)\log q)$ en utilisant un arbre de sous-produits (voir [85, Section 10.1]). Les deux autres polynômes quant à eux s'obtiennent avec la même complexité grâce à une interpolation rapide (voir [85, Section 10.2]).

L'algorithme 4.2.2 résume ce que l'on a déjà expliqué. La complexité de cet algorithme dépend de la complexité de l'évaluation des fonctions f_i en $\Omega \in \mathcal{H}_2$. Dans le cas des thêta constantes et des fonctions dérivées d'elles, comme les invariants d'Igusa et de Streng, les étapes 1 à 7 sont de complexité $O(\mathcal{M}'(N)\log(N))$ ([19, Théorème 9.3]), l'étape 8 est en $O(q\mathcal{M}'(N)\log(N))$ (par [29, Théorème 12] sous la conjecture 3.6.2), l'étape 9 en $O(\mathcal{M}_N(q)\log(q))$ et la 10 en $O(\mathcal{M}_N(q)\log(q))$ de telle sorte que la complexité totale de cet algorithme avec des fonctions dérivées des thêta constantes est

$$O(q\mathcal{M}'(N)\log(N) + \mathcal{M}_N(q)\log(q)) \subseteq \tilde{O}(p^3 N).$$

Algorithme 4.2.2 : Évaluation des polynômes modulaires

Entrée : $f_1(\Omega), f_2(\Omega), f_3(\Omega)$, un sous-groupe Γ de Γ_2 tel que $\mathbb{C}_\Gamma = \mathbb{C}(f_1, f_2, f_3)$, un nombre premier p qui est premier au niveau de Γ, un ensemble C_p de représentants de $\Gamma/(\Gamma \cap \Gamma_0(p))$ et un précalcul de l'action des représentants de Γ_2/Γ, une précision N.

Sortie : $\Phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et $\Psi_{\ell,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ à précision N (avec quelques pertes) pour $\ell = 2, 3$.

1 Déduire les j-invariants $\mathfrak{j}_i(\Omega)$ ou si possible les invariants de Rosenhain $\mathfrak{r}_i(\Omega)$ à partir des $f_i(\Omega)$;
2 Utiliser l'algorithme de Mestre ou les invariants de Rosenhain pour obtenir une courbe hyperelliptique $Y^2 = f(X)$ à précision N ;
3 Déduire les dix $\mathfrak{c}_i(\Omega)$ à précision N en utilisant une technique d'intégration numérique à faible précision;
4 Inverser les fonctions pour trouver Ω' avec les bons j-invariants à précision N;
5 Comparer (permutations et constantes) les trois $f_i(\Omega)$ avec les trois $f_i(\Omega')$;
6 Déduire un représentant γ de Γ_2/Γ correspondant à cette action en utilisant le précalcul;
7 Calculer $\Omega = \gamma\Omega'$;
8 Calculer les $f_{i,p}^{\gamma}(\Omega)$ à précision N pour tout $\gamma \in C_p$;
9 Calculer $\Phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ à précision N en utilisant un arbre de sous-produits ;
10 En utilisant l'interpolation rapide, calculer $\Psi_{\ell,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$;

En pratique, l'étape qui prend le plus de temps est la 8 (voir section 4.5).

Supposons que f_1 soit la variable qui apparaît avec le plus grand degré parmi tous les numérateurs et dénominateurs des coefficients des polynômes modulaires. Notons d_T^A (resp. d_T^B) le degré total maximal des numérateurs (resp. dénominateurs) des coefficients des trois polynômes modulaires et notons d_{f_1} (resp. d_{f_2}, d_{f_3}) l'exposant maximal de la variable f_1 (resp. f_2, f_3) apparaissant dans un coefficient d'un des polynômes Soit $n = d_T^A + d_T^B \leq 6d_{f_1}$. Pour calculer les p-polynômes modulaires, l'algorithme 4.2.2 est exécuté $(n+1)(d_{f_2}+1)(d_{f_3}+1)$ fois et l'on a besoin d'interpoler $3q$ fractions rationnelles. La complexité pour calculer ces polynômes est alors

$$(n+1)(d_{f_2}+1)(d_{f_3}+1)\tilde{O}(p^3N) + \tilde{O}(np^3 d_{f_2} d_{f_3} N) \subseteq \tilde{O}(d_{f_1} d_{f_2} d_{f_3} p^3 N).$$

Remarquons que l'on suppose ici que l'on connaît les degrés de toutes les fractions rationnelles trivariées pour pouvoir utiliser l'interpolation de Cauchy avec l'algorithme d'Euclide étendu. Nous verrons à la section 4.5 comment calculer ces degrés.

Comme l'on ne connaît pas de bornes explicites pour la taille des coefficients des polynômes modulaires, on suppose qu'il suffit d'utiliser une précision flottante en $O(N)$, où N est la taille du plus grand coefficient, pour faire tous les calculs avec une précision qui, une fois la phase d'interpolation finie, permet de reconnaître correctement les coefficients comme des rationnels. On supposera également l'hypothèse 4.2.9.

Théorème 4.2.15 (Sous la conjecture 3.6.2 et les heuristiques du paragraphe précédent)**.** *Soient f_1, f_2, f_3 trois fonctions modulaires dérivées des thêta constantes pour un sous-groupe de congruence Γ de Γ_2 qui engendrent le corps des fonctions modulaires invariantes par $\mathbb{C}_\Gamma$. Soit p un nombre premier qui est premier au niveau de Γ. Alors, sous les différentes hypothèses formulées, les polynômes modulaires pour ces données peuvent être calculés avec une complexité en $\tilde{O}(d_{f_1} d_{f_2} d_{f_3} p^3 N)$, où $d_{f_1} = \max(d_{f_1}, d_{f_2}, d_{f_3})$, si les degrés en f_i de tous les coefficients (numérateurs et dénominateurs) des trois polynômes modulaires sont connus. Ici, N est la taille du plus grand coefficient entier apparaissant dans ces polynômes.*

Remarque 4.2.16.
- *La conjecture est utilisée pour la complexité mais elle n'affecte pas la justesse de l'algorithme car il est facile de vérifier si la matrice des périodes obtenue est la bonne ou pas à chaque étape d'évaluation.*
- *Pour que la complexité $\tilde{O}(d_{f_1} d_{f_2} d_{f_3} p^3 N)$ soit quasi-linéaire en la taille de la sortie, on doit supposer également que la taille moyenne des coefficients des polynômes modulaires est en $\Omega(N)$.*

4.3 Résultats

On présente dans cette section les différents polynômes modulaires que nous avons calculés avec les invariants de Streng et avec les $\mathfrak{b}_i$. Les données expérimentales de cette section qui sont prouvées dans la section qui suit sont utilisées pour optimiser l'implantation du calcul des polynômes modulaires (voir section 4.5).

4.3.1 Polynômes modulaires avec les invariants de Streng

Avec l'algorithme que nous avons présenté dans la section 4.2.1, Régis Dupont [19] a calculé les polynômes modulaires avec les invariants d'Igusa pour $p = 2$. Pour $p = 3$, il n'a pu calculer que les dénominateurs et les degrés des différents coefficients, à cause de degrés en les invariants trop élevés qui apparaissent dans les coefficients. Quant à nous, nous avons pu calculer les polynômes modulaires avec les invariants de Streng pour $p = 2$ et $p = 3$.

Nous commençons avec quelques notations pour pouvoir comparer les différents résultats trouvés entre les invariants d'Igusa et ceux de Streng (voir définitions 3.3.1 et 3.3.2). Pour $p = 2$, le nombre d'isogénies est $p^3 + p^2 + p + 1 = 15$. Notons pour $\ell = 2, 3$

$$\Phi_{1,2}(X) = X^{15} + \sum_{i=0}^{14} \frac{A_{1,i}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{B_{1,i}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)} X^i \qquad \text{et} \qquad \Psi_{\ell,2}(X) = \sum_{i=0}^{14} \frac{A_{\ell,i}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{B_{\ell,i}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)} X^i.$$

On considère le quotient $A_{j,i}/B_{j,i}$ comme le i-ième coefficient du j-ième polynôme modulaire. Les numérateur et dénominateur de chaque coefficient sont des polynômes dans $\mathbb{Z}[\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3]$.

Rappelons que Dupont a trouvé que les dénominateurs des trois polynômes modulaires sont de la forme $1428\mathfrak{j}_1^\alpha D_2(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)^6$, pour un certain entier α qui varie de 5 à 21 et où D_2 est de degrés 5, 7 et 5 en respectivement $\mathfrak{j}_1$, $\mathfrak{j}_2$, et $\mathfrak{j}_3$ (voir [19, Pages 225–226] pour ces résultats et pour la définition de D_2). Avec les invariants de Streng, nous avons trouvé que les dénominateurs sont de la forme $c\mathfrak{i}_3^\alpha D_2'(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ pour $\Phi_{1,2}$ et de la forme $c\mathfrak{i}_3^\alpha (D_2'(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3))^2$ pour les autres, où c est une constante dans $\mathbb{Z}$, α varie de 0 à 3 et

$D'_2 = (24576\mathrm{i}_3\mathrm{i}_1^5+(96\mathrm{i}_2^3-4608\mathrm{i}_3\mathrm{i}_2)\mathrm{i}_1^4+(-6220800\mathrm{i}_3\mathrm{i}_2-12288\mathrm{i}_3^2)\mathrm{i}_1^3+(-23328\mathrm{i}_2^4-48\mathrm{i}_3\mathrm{i}_2^3+1088640\mathrm{i}_3\mathrm{i}_2^2+2304\mathrm{i}_3^2\mathrm{i}_2+24883200\mathrm{i}_3^2)\mathrm{i}_1^2+(93312\mathrm{i}_3\mathrm{i}_2^3+419904000\mathrm{i}_3\mathrm{i}_2^2-5909760\mathrm{i}_3^2\mathrm{i}_2+(1536\mathrm{i}_3^3-8398080000\mathrm{i}_3^2))\mathrm{i}_1+(1417176\mathrm{i}_2^5-5832\mathrm{i}_3\mathrm{i}_2^4+(6\mathrm{i}_3^2-94478400\mathrm{i}_3)\mathrm{i}_2^3+287712\mathrm{i}_3^2\mathrm{i}_2^2+(-288\mathrm{i}_3^3+1154736000\mathrm{i}_3^2)\mathrm{i}_2+(-248832\mathrm{i}_3^3+755827200000\mathrm{i}_3^2)))$

est irréductible. Il est clair que les puissances de D_2 et D'_2 sont reliées à la puissance de h_{10} dans la définition des différents j-invariants. Notons par $d_{i,j,\ell}$ le degré du numérateur du ℓ-ième coefficient du i-ième polynôme modulaire en i_j (voir définition 4.2.10) et $\alpha_{i,\ell}$ la puissance de j_3 qui apparaît dans le dénominateur du ℓ-ième coefficient du i-ième polynôme. Les degrés trouvés sont écrits dans le tableau 4.1.

ℓ	$d_{1,1,\ell}$	$d_{1,2,\ell}$	$d_{1,3,\ell}$	$\alpha_{1,\ell}$	$d_{2,1,\ell}$	$d_{2,2,\ell}$	$d_{2,3,\ell}$	$\alpha_{2,\ell}$	$d_{3,1,\ell}$	$d_{3,2,\ell}$	$d_{3,3,\ell}$	$\alpha_{3,\ell}$
0	25	11	11	3	30	17	15	3	33	17	16	3
1	23	11	11	3	28	17	15	3	31	17	16	3
2	23	11	11	3	28	17	15	3	31	17	16	3
3	21	11	11	3	26	17	15	3	29	17	16	3
4	21	11	11	3	26	17	15	3	29	17	16	3
5	20	11	10	3	25	17	14	3	28	17	15	3
6	20	11	10	3	25	17	14	3	28	17	15	3
7	18	10	9	2	23	17	14	3	26	17	15	3
8	18	10	9	2	23	16	13	2	26	16	14	2
9	16	10	8	2	21	15	12	2	24	15	13	2
10	16	8	7	1	21	15	12	2	24	15	13	2
11	15	8	7	1	20	13	11	1	23	13	12	1
12	15	7	7	1	20	13	11	1	23	13	12	1
13	11	6	5	0	16	12	10	1	20	12	11	1
14	8	5	4	0	13	11	8	0	16	11	9	0

TABLEAU 4.1 – Degrés des numérateurs des polynômes modulaires avec les invariants de Streng pour $p = 2$.

Les degrés des numérateurs des coefficients des polynômes modulaires trouvés par Dupont avec les invariants d'Igusa varient de 37 à 60 en j_1, de 50 à 75 en j_2 et de 33 à 50 en j_3 pour $\Phi_{1,2}(X)$ tandis qu'ils n'excèdent pas 25 avec les invariants de Streng. La taille des entiers dans le premier cas est majorée par 210 chiffres décimaux et par 105 dans le dernier cas. De plus, les trois polynômes calculés par Dupont (et accessibles dans sa page web) prennent 57 Mo d'espace mémoire et les autres 2.1 Mo. Les invariants de Streng fournissent donc des polynômes plus petits en termes de degrés, précision et espace mémoire.

Nous avons aussi calculé les polynômes modulaires avec les invariants de Streng pour $p = 3$. Le nombre d'isogénies est 40. Les dénominateurs ont les mêmes propriétés que celles décrites plus haut : ils sont de la forme $c\mathrm{i}_3^\alpha(D'_3(\mathrm{i}_1,\mathrm{i}_2,\mathrm{i}_3))^2$ pour $\Phi_{1,3}$ et de la forme $c\mathrm{i}_3^\alpha(D'_3(\mathrm{i}_1,\mathrm{i}_2,\mathrm{i}_3))^4$ pour les deux autres. La partie commune D'_3 est un polynôme irréductible de degrés 13, 10 et 8 en respectivement i_1, i_2 et i_3. Dupont a trouvé que les dénominateurs avec les invariants d'Igusa sont de la forme $c\mathrm{j}_1^\alpha D_3(\mathrm{j}_1,\mathrm{j}_2,\mathrm{j}_3)^{18}$, où D_3 est de degrés 14, 20 et 13 en j_1, j_2 et j_3. Nous présentons des degrés de numérateurs dans le tableau 4.2.

Les degrés sont beaucoup plus petits que ceux avec les invariants d'Igusa qui varient de 243 à 420. Nous ne connaissons pas les tailles des entiers des polynômes avec les invariants d'Igusa, mais dans le cas des invariants de Streng, nous avons

ℓ	$d_{1,1,\ell}$	$d_{1,2,\ell}$	$d_{1,3,\ell}$	$\alpha_{1,\ell}$	$d_{2,1,\ell}$	$d_{2,2,\ell}$	$d_{2,3,\ell}$	$\alpha_{2,\ell}$	$d_{3,1,\ell}$	$d_{3,2,\ell}$	$d_{3,3,\ell}$	$\alpha_{3,\ell}$
0	61	32	32	4	87	52	48	4	92	52	49	4
1	61	32	31	4	87	52	47	4	92	52	48	4
2	61	32	31	4	87	52	47	4	92	52	48	4
⋮		⋮	⋮			⋮	⋮			⋮	⋮	
37	41	22	21	1	67	43	37	1	72	43	39	1
38	36	21	19	0	62	42	36	1	67	42	37	1
39	31	20	17	0	57	41	33	0	62	41	35	0

TABLEAU 4.2 – Degrés de numérateurs des polynômes modulaires avec les invariants de Streng pour $p = 3$.

trouvé qu'ils peuvent avoir jusqu'à 550 chiffres décimaux. Les trois polynômes occupent 890 Mo d'espace mémoire.

4.3.2 Polynômes modulaires avec les $\mathfrak{b}_i$

Nous avons calculé les polynômes modulaires avec les $\mathfrak{b}_i$ pour $p = 3, 5$ et 7 (voir équation (3.13) pour leurs définitions). Rappelons que pour $p = 2$, ces polynômes n'existent pas parce que $\Gamma_2(2,4) \cap \Gamma_0(2) = \Gamma_2(2,4)$. Cette fois, il n'y a qu'un dénominateur commun D_p pour tous les coefficients des trois polynômes (il n'y a pas de constantes ni de puissances d'un des $\mathfrak{b}_i$). Par exemple, on a

$$D_3 = 1024\mathfrak{b}_3^6\mathfrak{b}_2^6\mathfrak{b}_1^{10} - ((768\mathfrak{b}_3^8 + 1536\mathfrak{b}_3^4 - 256)\mathfrak{b}_2^8 + 1536\mathfrak{b}_3^8\mathfrak{b}_2^4 - 256\mathfrak{b}_3^8)\mathfrak{b}_1^8 + (1024\mathfrak{b}_3^6\mathfrak{b}_2^{10} + (1024\mathfrak{b}_3^{10} + 2560\mathfrak{b}_3^6 - 512\mathfrak{b}_3^2)\mathfrak{b}_2^6 - (512\mathfrak{b}_3^6 - 64\mathfrak{b}_3^2)\mathfrak{b}_2^2)\mathfrak{b}_1^6 - (1536\mathfrak{b}_3^8\mathfrak{b}_2^8 + (-416\mathfrak{b}_3^4 + 32)\mathfrak{b}_2^4 + 32\mathfrak{b}_3^4)\mathfrak{b}_1^4 - ((512\mathfrak{b}_3^6 - 64\mathfrak{b}_3^2)\mathfrak{b}_2^6 - 64\mathfrak{b}_3^6\mathfrak{b}_2^2)\mathfrak{b}_1^2 + 256\mathfrak{b}_3^8\mathfrak{b}_2^8 - 32\mathfrak{b}_3^4\mathfrak{b}_2^4 + 1.$$

Pour $p = 5$ (resp. $p = 7$), le dénominateur apparaît avec puissance 70 (resp. 226) pour les trois $\mathfrak{b}_i$. Ces dénominateurs pour $p = 3, 5, 7$ ont des propriétés intéressantes. Ils sont symétriques, les puissances des $\mathfrak{b}_i$ sont toujours paires et il y a des relations modulo 2 et 4 entre les puissances de chaque monôme. Nous avons noté des propriétés similaires sur les numérateurs. En particulier, nous avons remarqué que pour $p = 3$ et 5, $\Psi_{2,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Psi_{3,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2)$ et $\Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2)$. En outre, les degrés totaux pour les dénominateurs sont 24, 120 et 336, c'est-à-dire $p^3 - p$. Nous étudierons ces propriétés dans la section suivante.

Le tableau 4.3 montre quelques degrés pour $p = 3$. Ce tableau peut être comparé avec les résultats trouvés avec les invariants de Streng (voir tableau 4.2). Les notations sont similaires à celles d'avant.

Le tableau 4.4 indique les degrés minimaux et maximaux de chacun des $\mathfrak{b}_i$ dans les différents polynômes modulaires pour $p = 5$ et 7.

Les coefficients entiers ont jusqu'à 10, 60 et 190 chiffres décimaux pour respectivement $p = 3$, 5 et 7. Les trois polynômes occupent 270 Ko pour $p = 3$ (ce qui est 3000 fois plus petit que l'espace total que prennent les polynômes modulaires avec les invariants de Streng pour $p = 3$), et 305 Mo pour $p = 5$ tandis que seulement les deux premiers prennent 29 Go pour $p = 7$ (nous n'avons pas calculé le troisième parce qu'en supposant la symétrie constatée dans les cas $p = 3$ et

ℓ	$d_{1,1,\ell}$	$d_{1,2,\ell}$	$d_{1,3,\ell}$	$d_{2,1,\ell}$	$d_{2,2,\ell}$	$d_{2,3,\ell}$
0	40	10	10	37	13	12
1	37	12	12	36	15	14
2	38	14	14	37	17	16
3	39	16	16	36	19	18
4	36	16	16	35	19	18
⋮		⋮			⋮	
35	21	16	16	22	19	18
36	20	16	16	19	19	18
37	17	16	16	16	17	16
38	14	14	14	15	15	14
39	13	12	12	12	13	12

TABLEAU 4.3 – Degrés des numérateurs des polynômes modulaires avec les $\mathfrak{b}_i$ pour $p = 3$.

min-max de	$\mathfrak{b}_1$	$\mathfrak{b}_2$	$\mathfrak{b}_3$
$\Phi_{1,5}$	75-156	70-92	70-92
$\Psi_{2,5}$	72-155	75-97	72-94
$\Phi_{1,7}$	233-400	226-272	226-272
$\Psi_{2,7}$	230-397	233-279	230-276

TABLEAU 4.4 – Degrés des numérateurs des polynômes modulaires avec les $\mathfrak{b}_i$ pour $p = 5, 7$.

5, on peut déduire ce troisième polynôme du deuxième de telle sorte qu'essayer de le calculer directement ne résulte qu'en une perte de temps). Comparé aux polynômes trouvés avec les invariants de Streng pour $p = 3$, ces invariants produisent des polynômes plus petits en termes de degrés, de taille des entiers dans les coefficients et d'espace mémoire.

4.4 Propriétés des polynômes

4.4.1 Dénominateur et surface de Humbert

Nous allons étudier dans cette section la signification des dénominateurs qui apparaissent dans les différents polynômes modulaires et leur relation aux surfaces de Humbert, que nous étudierons plus profondément dans le chapitre suivant.

Soit $\Delta \equiv 0, 1 \bmod 4$ et $\Delta > 0$. On appelle surface de Humbert H_Δ de discriminant Δ la surface irréductible des matrices des périodes qui sont équivalentes à un certain $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right)$ modulo Γ_2 qui vérifie $k\Omega_1 + \ell\Omega_2 - \Omega_3 = 0$, où k et ℓ sont déterminés uniquement par $\Delta = 4k + \ell$ et $\ell \in \{0, 1\}$. Nous renvoyons le lecteur à [35] pour le calcul de ces surfaces.

Nous avons vu dans le lemme 4.2.8 que les dénominateurs des polynômes modulaires avec les invariants d'Igusa (ou de Streng) sont divisibles par un polynôme $L_p \in \mathbb{Q}[\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3]$. La proposition qui suit nous dit que $\mathcal{L}_p = H_{p^2}$, ce qui explique l'importance de l'étude des surfaces de Humbert (rappelons que $\mathcal{L}_p$ est le lieu de toutes les surfaces abéliennes principalement polarisées qui sont p-isogènes à un produit de courbes elliptiques).

Proposition 4.4.1. *Soit m un entier positif. Alors la surface de Humbert H_{m^2} est un espace de modules pour les classes d'isomorphismes de surfaces abéliennes principalement polarisées qui sont isogènes à un produit de courbes elliptiques via une isogénie de degré m^2.*

Démonstration. Voir [70] ou [35, Proposition 2.14]. □

Pour tout discriminant Δ, il existe un polynôme irréductible $L_\Delta(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ dont l'ensemble des zéros est la surface de Humbert de discriminant Δ. Ainsi, par le lemme 4.2.8, $L_{p^2}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ divise les dénominateurs des polynômes modulaires définis avec les invariants d'Igusa. La puissance avec laquelle $L_{p^2}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ apparaît dans le dénominateur semble être un facteur de la puissance de h_{10} dans la définition des j-invariants. Une raison heuristique à l'apparition des facteurs j_1^α dans le dénominateur d'un coefficient d'un polynôme modulaire est pour compenser le cas où $h_{12}(\Omega) = 0$ (nous rappelons la définition 3.3.1). Avec les invariants de Streng, il y a un facteur $\mathfrak{i}_3^\alpha$ pour compenser les cas où $h_4(\Omega) = 0$ (voir définition 3.3.2). Notons que j_1 (resp. $\mathfrak{i}_3$) est l'invariant parmi j_1, j_2, j_3 (resp. $\mathfrak{i}_1$, $\mathfrak{i}_2$, $\mathfrak{i}_3$) avec la plus grande puissance dans h_{12} (resp. h_4) dans sa définition.

L'avantage des surfaces de Humbert est qu'on connaît des formules pour leur degré. Soit

$$a_{p^2} := 24 \sum_{\substack{x \in \mathbb{Z}, \\ 4 | (p^2 - x^2)}} \sigma_1\left(\frac{p^2 - x^2}{4}\right) + 12p^2 - 2, \tag{4.3}$$

où $\sigma_1(n) = \sum_{d|n} d$ est la fonction somme des diviseurs positifs d'un entier. On a alors

Théorème 4.4.2. *Le degré d'une surface de Humbert de discriminant p^2 peut être obtenu par la formule*

$$v(p^2)\deg(H_{p^2}) + 5 = \frac{a_{p^2}}{2} \qquad \text{où} \qquad v(p^2) = \begin{cases} 1/2 & \text{si } p = 2 \\ 1 & \text{sinon.} \end{cases}$$

Démonstration. Voir [40, Théorème 8.10] ou [35, Théorème 3.8]. □

En appliquant cette formule, on trouve $\deg(H_4) = 60$ et $\deg(H_9) = 120$. Ici, le degré d'une surface est le degré de la forme homogène de L_Δ avec poids $(4, 6, 10, 12)$ pour les fonctions $(h_4, h_6, h_{10}, h_{12})$ (voir [40, Pages 170–172]). On a donc remplacé les j-invariants du dénominateur commun pour $p = 2$ et $p = 3$ par leurs définitions en terme des h_i et multiplié par une puissance de h_{10} pour homogénéiser. Ce faisant, le degré que nous avons trouvé pour $p = 2$ est 100 (resp. 300) avec les invariants de Streng (resp. d'Igusa), mais il y a un facteur h_4^{10} (resp. h_{12}^{20}) et on a $100 - 40 = 60$ (resp. $300 - 240 = 60$). Ce facteur peut être expliqué par le fait que tous les j-invariants s'annulent lorsque $h_4 = 0$ (resp. $h_{12} = 0$). Pour $p = 3$, on a trouvé pour les invariants de Streng que le degré est 200 et qu'il existe un facteur h_4^{20}. On a alors $200 - 80 = 120$, ce qui correspond bien à la formule.

Regardons maintenant ce qu'il se passe pour les polynômes modulaires avec les $\mathfrak{b}_i$. Il existe là aussi une formule pour les degrés due aux travaux de Runge ([74], voir aussi [35]) qui a considéré des recouvrements finis de $\mathcal{H}_2/\Gamma_2$ pour l'étude des surfaces de Humbert à cause des grands degrés et coefficients qui apparaissent dans les polynômes avec les invariants d'Igusa. Définissons $\Gamma_2^*(2, 4)$ comme étant le sous-groupe normal le plus grand de $\Gamma_2(2, 4)$ qui ne contient pas la matrice

diag$(-1,1,-1,1)$. Il est d'indice 2 dans $\Gamma_2(2,4)$. La projection $\pi : \mathcal{H}_2/\Gamma_2^*(2,4) \to \mathcal{H}_2/\Gamma_2$ est une application finie. On dit que chaque composante de $\pi^{-1}(H_{p^2})$ dans $\mathcal{H}_2/\Gamma_2^*(2,4)$ est une composante de Humbert et il est possible de définir un ordre $v_i'(p^2)$ pour chaque composante irréductible de Humbert $F_{p^2,i}$. Puisque $\Gamma_2^*(2,4)$ est normal, ces composantes ont le même degré. De plus, par [74], chaque composante irréductible du recouvrement de H_{p^2} est donné par l'ensemble des zéros d'un seul polynôme irréductible.

Proposition 4.4.3. *Le degré d'une composante de Humbert $F_{p^2,i}$ dans $\mathcal{H}_2/\Gamma_2^*(2,4)$ est donné par la formule*

$$a_{p^2} = 10(1 + \deg(F_{p^2,i})).$$

Démonstration. Voir [74, Page 293]. □

Corollaire 4.4.4. *Soit $p > 2$ un nombre premier. Le degré de $F_{p^2,i}$ est $p^3 - p$.*

Démonstration. D'après la formule du degré ci-dessus et la définition de a_{p^2} dans l'équation (4.3), il suffit de prouver que

$$\sum_{x>0} \sigma_1\left(\frac{p^2-x^2}{4}\right) = \frac{5p^3-6p^2-5p+6}{24}.$$

Le membre de gauche peut être réécrit comme

$$\sum_{x>0} \sigma_1\left(\frac{p^2-x^2}{4}\right) = \frac{1}{2}\sum_{k=1}^{p} \sigma_1(k)\sigma_1(p-k).$$

En effet, $\sum_{x>0} \sigma_1\left(\frac{p^2-x^2}{4}\right) = \sum_{x>0} \sigma_1(\frac{p-x}{2}\cdot\frac{p+x}{2})$, ce qui donne, en posant $k = \frac{p-x}{2}$, $\sum_{k=1}^{(p-1)/2} \sigma_1(k(p-k))$. Or ici, pgcd$(k, p-k) = 1$ et donc $\sigma_1(k(p-k)) = \sigma_1(k)\sigma_1(p-k)$, ce qui nous permet de déduire l'égalité voulue. L'équation (1.21) et le théorème 1.4.3 nous permettent d'écrire :

$$\sum_{m=1}^{\infty} m\sigma_1(m)q^m = \frac{5}{6}\sum_{m=1}^{\infty}\sigma_3(m)q^m + \frac{1}{6}\sum_{m=1}^{\infty}\sigma_1(m)q^m - 2\left(\sum_{m=1}^{\infty}\sigma_1(m)q^m\right)^2.$$

En regardant au point $m = p$, on trouve :

$$p(p+1) = \frac{5}{6}(p^3+1) + \frac{1}{6}(p+1) - 4\left(\frac{1}{2}\sum_{k=1}^{p}\sigma_1(k)\sigma_1(p-k)\right),$$

et un simple calcul nous permet de conclure. (De plus, en utilisant le fait que σ_1 est multiplicatif, on peut montrer que pour tout $p > 2$, le degré de $F_{4p^2,i}$ est aussi $p^3 - p$, mais on n'aura pas besoin de ce résultat). □

Dans notre cas, on considère $\Gamma_2(2,4)$ et non pas $\Gamma_2^*(2,4)$, mais nous avons remarqué que le degré total trouvé pour $p = 3, 5$ et 7 est toujours $p^3 - p$. La raison à cela est que la formule du degré dépend du nombre de composantes de Humbert et de l'ordre d'un certain sous-groupe isotrope et ces nombres sont égaux pour les groupes $\Gamma_2^*(2,4)$ et $\Gamma_2(2)$ (voir [74, 35]). Ce doit donc être aussi le cas pour $\Gamma_2(2,4)$ car $\Gamma_2^*(2,4) < \Gamma_2(2,4) < \Gamma_2(2)$. Ainsi, la formule du degré d'une composante de discriminant p^2 pour le groupe $\Gamma_2(2,4)$ est la même que celle pour

le groupe $\Gamma_2^*(2,4)$, c'est-à-dire $p^3 - p$. Notons que la définition du degré ici est le degré total du polynôme parce que les $\theta_i(\tau/2)$ sont des formes modulaires de Siegel, à une racine de l'unité près, de poids 1 pour le groupe $\Gamma_2(2,4)$.

Considérons cette fois le lieu $\mathcal{L}'_p$ de toutes les surfaces abéliennes principalement polarisées modulo $\Gamma_2(2,4)$ qui sont p-isogènes à une surface abélienne principalement polarisée Ω qui est elle-même isogène à un produit de courbes elliptiques par la 2-isogénie $\Omega \to \Omega/2$ et telle que $\theta_0(\Omega/2) = 0$ (rappelons que $\mathfrak{b}_i(\Omega) := \theta_i(\Omega/2)/\theta_0(\Omega/2)$ et la proposition 3.2.3).

Proposition 4.4.5. *Les dénominateurs des polynômes modulaires pour les fonctions $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3$ sont divisibles par un polynôme L'_p dans $\mathbb{Q}[\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3]$ décrivant le lieu précédent.*

Démonstration. On adapte la preuve du lemme 4.2.8. Soit $\Omega \in \mathcal{H}_2/\Gamma_2(2,4)$ qui est p-isogène à Ω' tel que $\theta_0(\Omega'/2) = 0$. Soit c un coefficient du polynôme $\Phi_{1,p}(X)$. Pour un certain $\gamma \in \Gamma_2(2,4)/(\Gamma_2(2,4) \cap \Gamma_0(p))$, $\mathfrak{b}_{1,p}(\gamma\Omega)$ est infini. L'évaluation de c en Ω est une expression symétrique en les $\mathfrak{b}_{1,p}^{\gamma}(\Omega)$. Génériquement, il n'existe aucune relation algébrique entre ces valeurs et l'évaluation de c en Ω est donc infinie. Or comme les $\mathfrak{b}_i(\Omega)$ sont finis, le numérateur de c est fini. On conclut que le dénominateur de c doit s'annuler en Ω, ce qui signifie que c est divisible par un polynôme décrivant le lieu. La preuve pour $\Phi_{\ell,p}$, $\ell = 2, 3$, est similaire. □

Nous avons remarqué que pour $p = 3, 5$ et 7, les coefficients des trois polynômes modulaires avec les $\mathfrak{b}_i$ ont toujours L'_p comme dénominateur (contrairement aux cas avec les différents j-invariants où le dénominateur commun peut apparaître avec une puissance > 1 et où il y a parfois des facteurs $\mathfrak{j}_1$ ou $\mathfrak{i}_3$) Ceci justifie la conjecture suivante, qui sera utilisée dans les sections suivantes.

Conjecture 4.4.6. *Soit $p > 2$ un nombre premier. Le polynôme L'_p est le dénominateur de tous les coefficients des trois p-polynômes modulaires (sauf le coefficient de degré $p^3 + p^2 + p + 1$ de $\Phi_{1,p}(X)$ qui vaut 1).*

4.4.2 Symétries

Nous avons dit précédemment (section 4.3.2), que nous avons remarqué, pour $p = 3, 5$, que

$$\Psi_{2,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Psi_{3,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2)$$

et pour $p = 3, 5, 7$ que

$$\Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2).$$

Ces symétries ont la signification suivante. Pour toutes variétés $\Omega \in \mathcal{H}_2/\Gamma_2(2,4)$ et $p\Omega$ ayant pour invariants $(\mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega))$ et $(\mathfrak{b}_{1,p}(\Omega), \mathfrak{b}_{2,p}(\Omega), \mathfrak{b}_{3,p}(\Omega))$, il existe une variété avec pour invariants $(\mathfrak{b}_1(\Omega), \mathfrak{b}_3(\Omega), \mathfrak{b}_2(\Omega))$ et telle que une de ses variétés p-isogène a $(\mathfrak{b}_1(p\Omega), \mathfrak{b}_3(p\Omega), \mathfrak{b}_2(p\Omega))$ comme invariants.

On prouve l'existence de ces symétries en regardant l'action de certaines matrices. En effet, $\Phi_{1,p}$ est le polynôme minimal de $\mathfrak{b}_{1,p}$, ce qui signifie qu'il est l'unique polynôme irréductible unitaire tel que pour tout $\Omega \in \mathcal{H}_2$, $\Phi_{1,p}(x, \mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega)) = 0$ si et seulement si $x = \mathfrak{b}_{1,p}(\gamma\Omega)$ pour un certain $\gamma \in \Gamma_2(2,4)/(\Gamma_2(2,4) \cap \Gamma_0(p))$; en particulier, on a que $\Phi_{1,p}(b_{1,p}(\Omega), \mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega)) = 0$. Or cette dernière égalité est valable pour tout $\Omega \in \mathcal{H}_2$ donc aussi

pour $\gamma\Omega$ avec $\gamma \in \Gamma_2$, d'où $\Phi_{1,p}(\mathfrak{b}_{1,p}(\gamma\Omega), \mathfrak{b}_1(\gamma\Omega), \mathfrak{b}_2(\gamma\Omega), \mathfrak{b}_3(\gamma\Omega)) = 0$ pour tout $\gamma \in \Gamma_2$. On cherche alors une matrice dont l'action fixe $\mathfrak{b}_1$ et $\mathfrak{b}_{1,p}$, et remplace $\mathfrak{b}_2$ par $\mathfrak{b}_3$ et $\mathfrak{b}_{2,p}$ par $\mathfrak{b}_{3,p}$. Cette action sur $\Phi_{1,p}(X)$ produit un polynôme unitaire avec les mêmes racines et degrés que $\Phi_{1,p}(X)$. Par unicité, ils doivent donc être égaux.

Supposons maintenant qu'il y ait la symétrie pour $\Phi_{1,p}$. Alors par la définition 4.2.10, $\mathfrak{b}_{\ell,p} = \Psi_{\ell,p}(\mathfrak{b}_{1,p})/\Phi'_{1,p}(\mathfrak{b}_{1,p})$ pour $\ell = 2, 3$. L'action décrite plus haut sur cette dernière égalité avec $\ell = 2$ nous dit alors que

$$\mathfrak{b}_{3,p} = \Psi_{2,p}(\mathfrak{b}_{1,p}, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2)/\Phi'_{1,p}(\mathfrak{b}_{1,p}, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3),$$

et donc

$$\Psi_{2,p}(\mathfrak{b}_{1,p}, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2) = \mathfrak{b}_{3,p}\Phi'_{1,p}(\mathfrak{b}_{1,p}, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Psi_{3,p}(\mathfrak{b}_{1,p}, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3).$$

La recherche de la matrice qui a cette action se fait tout d'abord parmi les représentants des classes du quotient $\Gamma_2/\Gamma_2(2,4)$ parce que $\Gamma_2(2,4)$ fixe les $\mathfrak{b}_i$. Un représentant γ de l'unique classe telle que $(\mathfrak{b}_1^\gamma, \mathfrak{b}_2^\gamma, \mathfrak{b}_3^\gamma) = (\mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2)$ est

$$\gamma = \begin{pmatrix} 1 & -3 & -2 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -4 & -5 & 1 \end{pmatrix}.$$

Deuxièmement, on cherche une matrice γ' dans $\Gamma_2(2,4)$ telle que $\gamma\gamma'$ (ou $\gamma'\gamma$ car $\Gamma_2(2,4)$ est un groupe normal) soit dans $\Gamma_0(p)$. Pour $p = 3, 5$ et 7, on peut prendre pour γ' respectivement

$$\begin{pmatrix} -5 & 24 & -12 & 12 \\ -2 & 19 & -12 & 8 \\ 0 & 6 & -5 & 2 \\ -2 & 4 & 0 & 3 \end{pmatrix}, \qquad \begin{pmatrix} -7 & 6 & 4 & 2 \\ 0 & -7 & 2 & 0 \\ 0 & 10 & -3 & 0 \\ 10 & -8 & -6 & -3 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 13 & 12 & -16 & -6 \\ -10 & -3 & 10 & 4 \\ 56 & 14 & -55 & -22 \\ 30 & -40 & -12 & -7 \end{pmatrix}.$$

Nous rappelons que nous notons X_0, pour une matrice X, le vecteur composé des éléments diagonaux de X.

Lemme 4.4.7. *Soit* $M = \left(\begin{smallmatrix} A' & B' \\ C' & D' \end{smallmatrix}\right) \in \Gamma_2/\Gamma_2(2,4)$ *et* $M' \in \Gamma_2(2,4)$ *telle que* $MM' \in \Gamma_0(p)$*, pour un nombre premier* $p > 2$*. Alors* $(MM')_p$ *est dans la même classe d'équivalence que* M *pour tout* $p \equiv 1 \bmod 4$*. Pour* $p \equiv 3 \bmod 4$*, c'est le cas si on ajoute les propriétés* $(A'\,{}^tB')_0 \equiv 0 \bmod 2$ *et* $(C'\,{}^tD')_0 \equiv 0 \bmod 2$*.*

Démonstration. Soit $MM' = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. Étudions sous quelles conditions $(MM')_p M^{-1}$ $\in \Gamma_2(2,4)$ ou, de manière équivalente, $(MM')_p(MM')^{-1}$, est dans $\Gamma_2(2,4)$. On a

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

où $\left(\begin{smallmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{smallmatrix}\right)$ est l'inverse de M. Comme $p \equiv 1 \bmod 2$, ce produit est l'identité modulo 2. Maintenant pour $p \equiv 1 \bmod 4$, on a $-A\,{}^tB + pB\,{}^tA \equiv C/p\,{}^tD - D\,{}^tC \equiv 0 \bmod 4$ (souvenons nous que ce produit est dans Γ_2) de telle sorte que $(MM')_p(MM')^{-1} \in \Gamma_2(2,4)$. Pour $p \equiv 3 \bmod 4$, on a que $-A\,{}^tB + pB\,{}^tA \equiv 2A\,{}^tB \bmod 4$ et $C/p\,{}^tD - D\,{}^tC \equiv 2C\,{}^tD \bmod 4$. Donc pour être dans $\Gamma_2(2,4)$, on veut que $(A\,{}^tB)_0 \equiv (C\,{}^tD)_0 \equiv 0 \bmod 2$. Enfin, notons que $M' \equiv I_4 \bmod 2$ et on en déduit le lemme. □

Par ce lemme, on a que $(\gamma\gamma')_p$ est dans la même classe d'équivalence que γ pour tout premier $p > 2$, d'où la permutation $(\mathfrak{b}_{1,p}^{\gamma\gamma'}, \mathfrak{b}_{2,p}^{\gamma\gamma'}, \mathfrak{b}_{3,p}^{\gamma\gamma'}) = (\mathfrak{b}_{1,p}, \mathfrak{b}_{3,p}, \mathfrak{b}_{2,p})$. De plus, la surjectivité de $\mathrm{Sp}_4(\mathbb{Z}) \to \mathrm{Sp}_4(\mathbb{Z}/4p\mathbb{Z})$ et le théorème des restes Chinois prouvent que la matrice γ' existe toujours. Ainsi, il y a des symétries pour tout premier $p > 2$ (voir théorème 4.4.9).

Par ce qui précède, on a également démontré que le dénominateur est toujours symétrique en $\mathfrak{b}_2$ et $\mathfrak{b}_3$. Pour prouver que L'_p est également symétrique en $\mathfrak{b}_1$ et $\mathfrak{b}_2$ (resp. $\mathfrak{b}_1$ et $\mathfrak{b}_3$), on utilise les matrices

$$\gamma_{410} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \qquad \text{et} \qquad \gamma_{8316} = \begin{pmatrix} 1 & 0 & 0 & 2 \\ -3 & 1 & 2 & -2 \\ -4 & 0 & 1 & -5 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

qui fixent $\mathfrak{b}_3$ (resp. $\mathfrak{b}_2$) et échangent $\mathfrak{b}_1$ avec $\mathfrak{b}_2$ (resp. avec $\mathfrak{b}_3$).

L'action de γ_{410} (resp. γ_{8316}) sur L'_p nous fournit un polynôme irréductible avec les mêmes racines que L'_p, qui est toujours dans $\mathcal{L}'_p$ par le lemme qui suit. On en déduit que ce polynôme est L'_p et donc ce dernier est symétrique.

Lemme 4.4.8. *Soit $\Omega \in \mathcal{L}'_p$, $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2/\Gamma_2(2,4)$ et γ' tel que γ_p est dans la même classe d'équivalence que γ'. Supposons que l'action de γ' sur les thêta constantes envoie l'ensemble $\{0,4,8,12\}$ vers lui-même. Alors $\gamma\Omega$ est dans $\mathcal{L}'_p$.*

Démonstration. Que $\Omega \in \mathcal{H}_2/\Gamma_2(2,4)$ soit dans $\mathcal{L}'_p$ signifie qu'il existe $M \in \Gamma_2(2,4)/\left(\Gamma_2(2,4) \cap \Gamma_0(p)\right)$ qui vérifie $\theta_0(pM\Omega/2) = 0$. Soit $M' \in \Gamma_2(2,4)/(\Gamma_2(2,4) \cap \Gamma_0(p))$ tel que $(M'\gamma)M^{-1} \in \Gamma_0(p)$. Il existe alors $\gamma'' \in \Gamma_0(p)$ avec $M'\gamma = \gamma''M$. On a, en utilisant la formule de duplication, que

$$\theta_0(pM'\gamma\Omega/2) = \theta_0(p\gamma''M\Omega/2) = \theta_0(\gamma''_p(pM\Omega)/2) = \sum_{i\in\{0,4,8,12\}} \theta_i^2(\gamma''_p(pM\Omega)).$$

De plus, $\gamma''_p = (M'\gamma M^{-1})_p$ est dans la même classe d'équivalence que γ_p, c'est-à-dire que γ' par hypothèse ($\Gamma_2(2,4)$ est un sous-groupe normal). L'action de γ' envoie $\{0,4,8,12\}$ vers lui-même, et donc

$$\sum_{i\in\{0,4,8,12\}} \theta_i^2(\gamma''_p(pM\Omega)) = \zeta^2_{\gamma''_p} \det(...) \sum_{i\in\{0,4,8,12\}} \theta_i^2(pM\Omega)$$

$$= \zeta^2_{\gamma''_p} \det(...)\theta_0(pM\Omega/2) = 0.$$

□

Nous avons prouvé le théorème suivant

Théorème 4.4.9. *Soit $p > 2$ un nombre premier. Les p-polynômes modulaires pour $\mathfrak{b}_1, \mathfrak{b}_2$ et $\mathfrak{b}_3$ satisfont*

$$\Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Phi_{1,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2) \quad \textit{et} \quad \Psi_{2,p}(X, \mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \Psi_{3,p}(X, \mathfrak{b}_1, \mathfrak{b}_3, \mathfrak{b}_2).$$

De plus, le polynôme L'_p est symétrique.

4.4.3 Relations modulo 2 et 4

On étudie maintenant les différentes relations modulo 2 et 4 qui apparaissent entre les exposants des $\mathfrak{b}_i$ dans chaque coefficient des polynômes modulaires. Considérons le numérateur du ℓ-ième coefficient du m-ième polynôme modulaire pour $m = 1$ ou 2 (nous avons vu que le troisième polynôme peut être déduit du second). Leurs monômes sont de la forme $c_{ijk}\mathfrak{b}_1^i\mathfrak{b}_2^j\mathfrak{b}_3^k$. Nous avons constaté que pour $p = 3, 5$ et 7, si $c_{ijk} \neq 0$, alors

$$\begin{aligned} &i \equiv \ell + m + 1 \bmod 2 \\ &i + j \equiv -p\ell \bmod 4 \\ &j + k \equiv p(m-1) \bmod 4 \end{aligned} \tag{4.4}$$

et, avec des notation similaires, on a toujours que

$$i \equiv j \equiv k \equiv 0 \bmod 2 \qquad \text{et} \qquad i + j \equiv j + k \equiv 0 \bmod 4 \tag{4.5}$$

pour les dénominateurs. Ces égalités sont déterminées par l'existence de matrices γ avec la propriété que $\mathfrak{b}_i(\gamma\Omega) = \imath^{\alpha_i}\mathfrak{b}_i(\Omega)$ et $\mathfrak{b}_{i,p}(\gamma\Omega) = \imath^{\beta_i}\mathfrak{b}_{i,p}(\Omega)$, avec α_i et β_i dans $\{0, 1, 2, 3\}$. On notera l'action d'une telle matrice par le vecteur $(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3)$.

Avec les mêmes arguments que pour les symétries, on déduit qu'une telle action produit un polynôme avec les mêmes racines et degrés que $\Phi_{1,p}(X)$ (resp. $\Psi_{2,p}(X)$), qui est donc $\Phi_{1,p}(X)$ (resp. $\Psi_{2,p}(X)$) à une constante près. Comme $p^3 + p^2 + p + 1 \equiv 0 \bmod 4$ pour tout premier $p > 2$ et comme le coefficient dominant de $\Phi_{1,p}(X)$ est $X^{p^3+p^2+p+1}$, on en déduit que cette action ne change pas $\Phi_{1,p}(X)$. Ce n'est pas le cas de $\Psi_{2,p}(X)$, qui est de degré $p^3 + p^2 + p$ en X.

La matrice

$$\gamma_{134} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 2 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

agit par $(-1, 1, 1, -1, 1, 1)$ pour tout p d'après l'équation fonctionnelle de la proposition 2.6.4 et le lemme 4.4.7.

Le lemme 4.4.8 montre que cette matrice préserve la composante de Humbert (et $(\gamma_{134})_p$ est dans la même classe d'équivalence que γ_{134} par le lemme 4.4.7). On obtient ainsi un polynôme avec les mêmes racines et degrés que L'_p : c'est un de ses multiples. Comme ce dernier est irréductible, il contient au moins un monôme où il n'y a pas $\mathfrak{b}_1$ et donc cette matrice ne change pas ce monôme et la constante est alors 1. Comme L'_p est symétrique, on en déduit qu'il a des exposants en $\mathfrak{b}_1$, $\mathfrak{b}_2$ et $\mathfrak{b}_3$ qui sont pairs.

En supposant la conjecture 4.4.6, on a prouvé que l'action de γ_{134} sur les numérateurs ne dépend pas de l'action sur les dénominateurs. Par suite, sur les numérateurs de $\Phi_{1,p}$, l'action de γ_{134} montre que $i + \ell$ est toujours pair. Pour $\Psi_{2,p}(X)$, on doit déterminer quelle constante apparaît. Le coefficient dominant de ce polynôme est $\sum_{\gamma\in C_p} \mathfrak{b}_{2,p}^{\gamma} X^{p^3+p^2+p}$. Considérons maintenant le polynôme minimal $\prod_{\gamma\in C_p}(X - \mathfrak{b}_{2,p}^{\gamma})$ de $\mathfrak{b}_2$ et remarquons qu'il est invariant par l'action précédente, ce qui est donc le cas de $\sum_{\gamma\in C_p} \mathfrak{b}_{2,p}^{\gamma}$. On en déduit que la constante est -1, à cause de $X^{p^3+p^2+p}$, c'est-à-dire que

$$\sum_{\gamma\in C_p} \mathfrak{b}_{2,p}^{\gamma\gamma_{134}}(\mathfrak{b}_{1,p}^{\gamma_{134}})^{p^3+p^2+p} = -\sum_{\gamma\in C_p} \mathfrak{b}_{2,p}^{\gamma}(\mathfrak{b}_{1,p})^{p^3+p^2+p}.$$

On a donc démontré la première des trois égalités de (4.4).

Pour les deux autres, on doit considérer les matrices

$$\gamma_{141} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & -1 \end{pmatrix} \quad \text{et} \quad \gamma_{21} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Leurs actions pour $p \equiv 1 \bmod 4$ sont respectivement $(\imath, \imath, 1, \imath, \imath, 1)$ et $(1, \imath, \imath, 1, \imath, \imath)$, tandis que pour $p \equiv 3 \bmod 4$ c'est $(\imath, \imath, 1, -\imath, -\imath, 1)$ et $(1, \imath, \imath, 1, -\imath, -\imath)$ parce que dans ce cas $(\gamma_{141})_p$ et $(\gamma_{21})_p$ sont équivalents à

$$\gamma_{1886} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 1 & -1 & 0 \\ 1 & -1 & 0 & -1 \end{pmatrix} \quad \text{et} \quad \gamma_{155} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 3 & 0 & -1 \end{pmatrix}.$$

Sur L'_p, l'action de γ_{141} ne change pas la composante de Humbert par le lemme 4.4.8, de telle sorte que $L'_p(\imath\mathfrak{b}_1, \imath\mathfrak{b}_2, \mathfrak{b}_3)$ est un multiple de L'_p.

Comme L'_p est irréductible, il existe un monôme sans $\mathfrak{b}_1$, qui est alors de la forme $c\mathfrak{b}_2^i\mathfrak{b}_3^j$, pour une constante c. On a déjà montré que $i \equiv j \equiv 0 \bmod 2$ et donc $c(\imath\mathfrak{b}_2)^i\mathfrak{b}_3^j = \pm c\mathfrak{b}_2^i\mathfrak{b}_3^j$. Si c'est $+$, alors l'action de γ_{141} fixe L'_p. Sinon $i \equiv 2 \bmod 4$ et comme L'_p est symétrique, on a alors que les monômes $c\mathfrak{b}_1^i\mathfrak{b}_2^j$ et $c\mathfrak{b}_3^i\mathfrak{b}_2^j$ existent. Regardons ce dernier : $c\mathfrak{b}_3^i(\imath\mathfrak{b}_2)^j = \pm c\mathfrak{b}_3^i\mathfrak{b}_2^j$. Si c'est $-$, alors $j \equiv 2 \bmod 4$ et alors $c(\imath\mathfrak{b}_1)^i(\imath\mathfrak{b}_2)^j = c\mathfrak{b}_1^i\mathfrak{b}_2^j$. Dans tous les cas, l'action de γ_{141} fixe L'_p. On peut adapter cette preuve à γ_{121} et en déduire (4.5).

On applique des arguments similaires sur $\Phi_{1,p}(X)$ et $\Psi_{\ell,p}(X)$ pour prouver (4.4). On obtient alors

Théorème 4.4.10. *Soit $p > 2$ un nombre premier. Alors le polynôme L'_p satisfait (4.5). De plus, en supposant la conjecture 4.4.6, les numérateurs des deux premiers polynômes modulaires vérifient (4.4).*

4.5 Implantation

4.5.1 Logiciels externes

Dans sa thèse, Régis Dupont a présenté deux algorithmes pour calculer les fonctions thêta. Le premier utilise la définition des thêta constantes en terme de sommes d'exponentielles et calcule $\theta_i(\Omega)$ pour $i = 0, 1, 2, 3$, $\Omega \in \mathcal{F}_2$ à précision N avec une complexité de $O(\mathcal{M}'(N)N)$. Le deuxième unit l'itération de Newton avec les suites de Borchardt et est en $O(\mathcal{M}'(N)\log(N))$ sous la conjecture 3.6.2. Il calcule $\theta_i^2(\Omega)/\theta_0^2(\Omega)$, $i = 1, 2, 3$. Ces algorithmes ont été étudiés et implantés par Enge et Thomé dans [29, 30]. En utilisant la méthode des différences finies, ils prouvent que la complexité pour calculer le carré de toutes les thêta constantes est en $O(\mathcal{M}'(N)\log(N))$ sous la conjecture 3.6.2.

Nous avons utilisé la librairie cmh [30] écrite en C pour l'évaluation des carrés des thêta constantes et avons également récupéré dans cette librairie l'implantation de l'algorithme de Mestre et quelques autres fonctions écrites en GP. Nous avons également utilisé le logiciel pari-gnump [26] pour pouvoir passer des différents types du système GNU (GMP, MPFR et MPC [34, 37, 27]) aux types correspondants dans Pari/GP afin de pouvoir appeler les algorithmes de cmh depuis GP.

Il y a deux raisons pour lesquelles les différents algorithmes de calcul des thêta constantes sont définis pour Ω seulement dans le domaine fondamental.

La première est pour la convergence et la deuxième parce qu'on peut employer l'équation fonctionnelle de la proposition 2.6.4 pour déduire les thêta constantes en $\Omega \in \mathcal{H}_2$ à partir des thêta constantes en $\Omega' \in \mathcal{F}_2$. Nous avons implanté un algorithme qui calcule les dix fonctions $\mathfrak{c}_i$ pour une matrice quelconque de $\mathcal{H}_2$ avec GP [2].

Pour pouvoir appliquer l'algorithme 4.2.2, on a besoin d'une méthode pour réduire une matrice $\Omega \in \mathcal{H}_2$ dans le domaine fondamental. Nous avons donc implanté l'algorithme 3.1.2. Comme nous l'avons déjà signalé, nous avons récupéré le code de Pascal Molin [65] pour le calcul de $\Omega \in \mathcal{H}_2$ correspondant à une courbe hyperelliptique de genre 2 donnée.

De plus, on a besoin de connaître les représentants des classes des quotients $\Gamma_2(2,4)/(\Gamma_0(p) \cap \Gamma_2(2,4))$ pour un nombre premier p. Ils sont bien sûr calculés dans une phase préparatoire. Une généralisation directe de l'algorithme 1.3.1 en dimension 2 permet de calculer pour des sous-groupes $\Gamma' \subseteq \Gamma$ de Γ_2, les représentants des classes de Γ/Γ' et un ensemble de générateurs de Γ' à partir des générateurs de Γ et une fonction qui dit si une matrice est dans Γ' ou pas. On peut l'appliquer deux fois : la première sur $\Gamma = \Gamma_2$ et $\Gamma' = \Gamma_2(2,4)$, puis la deuxième sur $\Gamma = \Gamma_2(2,4)$ et $\Gamma' = \Gamma_0(p) \cap \Gamma_2(2,4)$. Une autre solution consiste à utiliser la proposition 4.2.2 qui nous donne un ensemble de représentants des classes de $\Gamma_2/\Gamma_0(p)$ pour tout $p \geq 2$. On doit multiplier chaque représentant par une matrice dans $\Gamma_0(p)$ de telle sorte que la matrice résultante soit dans $\Gamma_2(2,4)$, ce qu'on peut toujours faire d'après le théorème des restes Chinois.

4.5.2 Évaluation et interpolation

Jusqu'à présent, nous avons présenté les algorithmes sous un point de vue théorique. En pratique, on procède comme suit. Puisque nous voulons utiliser l'interpolation rapide, il est nécessaire de connaître les degrés des coefficients des polynômes modulaires en les trois variables f_1, f_2 et f_3, où on reprend les notations de la section 4.2.2. Par exemple, soit $F(f_1, f_2, f_3)$ un des coefficients que l'on veut calculer. Pour obtenir le degré total de son numérateur et de son dénominateur, il est suffisant de calculer les matrices $\Omega \in \mathcal{H}_2$, avec l'algorithme 4.2.2, qui vérifient $(f_1(\Omega),\ f_2(\Omega),\ f_3(\Omega)) = (x_i, x_i y, x_i z)$ pour un certain nombre de x_i et des valeurs y et z fixées, pour pouvoir ensuite évaluer $F(x_i, x_i y, x_i z)$ et faire une interpolation d'une fraction rationnelle trivariée. On en déduit les degrés totaux plus des majorations des degrés en f_1, f_2 et f_3. Pour connaître les degrés en f_1, on peut calculer $F(x_i, y, z)$ puis interpoler. On procède de manière similaire pour les autres degrés. Par contre, tout ceci ne donnera pas forcément la bonne réponse à chaque fois, en supposant que la précision est correcte et que l'on a assez de x_i. En effet, il peut il y a avoir des simplifications. Donc pour être certain du résultat, il est préférable d'évaluer et d'interpoler en plusieurs valeurs de y et z et idem pour $F(X + r, y + s, z + t)$ pour plusieurs valeurs de r, s et t.

Une fois que l'on possède ces informations, on a deux choix dans la manière de procéder. La première consiste à faire suffisamment d'évaluations pour calculer tous les coefficients en X des trois polynômes modulaires en interpolant des fractions rationnelles. Ici, par évaluation, on entend l'évaluation des polynômes modulaires en une matrice des périodes Ω telle que $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ soit de la forme $(x_i, x_i y_j, x_i z_k)$. L'autre manière consiste à se concentrer sur le coefficient ayant le degré total le plus bas au numérateur afin de calculer le dénominateur commun aux différents coefficients. Ensuite, on fait assez d'évaluations, cette fois

de la forme (x_i, y_j, z_k), pour calculer les autres coefficients par interpolation de polynômes multivariés (et non pas de fractions rationnelles). On peut en effet parler de polynômes car on peut multiplier les coefficients par le dénominateur commun (et, par exemple dans le cas des invariants de Streng, aussi par une puissance de $\mathfrak{i}_3$).

Dans le premier cas, le nombre d'évaluations dépendra du degré total maximal des trois polynômes, tandis que, dans le second, le degré total n'intervient que pour le coefficient avec les plus petits degrés. De plus, la précision nécessaire pour interpoler une fraction rationnelle est plus grande que celle pour un polynôme (et la complexité d'une évaluation des trois polynômes modulaires en une matrice Ω dépend de cette précision) et il est plus facile d'interpoler des polynômes plutôt que des fractions. Pour le second choix, les tables de degrés suggèrent de se focaliser sur le coefficient de degré $p^3 + p^2 + p$ en X de $\Phi_{1,p}$.

On peut choisir de chercher des matrices Ω telles que les $f_i(\Omega)$ soient entiers. Une telle matrice Ω ainsi que les invariants de ses variétés isogènes ne sont par contre pas à valeurs entières mais chaque coefficient des polynômes modulaires évalués en cet Ω sont à valeurs rationnelles, car on a vu que les polynômes sont dans $\mathbb{Q}(f_1, f_2, f_3)[X]$. Ainsi, il est possible, à chaque étape d'évaluation, de trouver ces rationnels grâce à des fractions continues, si la précision est assez élevée. L'étape d'interpolation se fait alors avec des valeurs exactes. Cependant, en procédant de cette manière, la précision requise, en pratique, augmente et donc le temps d'évaluation aussi. Il est préférable de prendre des valeurs flottantes et de retrouver les rationnels une fois que les polynômes ont été calculés à la précision ambiante pour trouver les coefficients exacts.

4.5.3 Temps de calcul

Notons que la phase d'évaluation peut être divisée en deux étapes : à partir de $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ trouver Ω et ensuite évaluer les polynômes modulaires en Ω. Cette dernière étape prend bien plus de temps que la première (à précision suffisamment grande). Par exemple, pour $p = 5$ et 7 à une précision de 1000 chiffres décimaux il faut environ 0.5 seconde pour calculer Ω à partir des $b'_i(\Omega)$ alors que le calcul des deux polynômes modulaires $\Phi_{1,p}(X, \mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega))$ et $\Psi_{2,p}(X, \mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega))$ prend 12 et 30 secondes pour respectivement $p = 5$ et $p = 7$ (cette différence est due au nombre d'isogénies : 156 pour la première et 400 pour l'autre ; notons que ce nombre est de 1464 pour $p = 11$).

Concentrons nous maintenant sur le calcul des polynômes modulaires avec les invariants de Streng. Nous employons la deuxième méthode qui n'est pas forcément la plus rapide parce qu'elle requiert deux phases d'évaluations (une pour avoir le dénominateur et une autre pour les numérateurs), mais qui a l'avantage de se concentrer sur le dénominateur qui est à l'origine de nombreuses difficultés pour calculer les polynômes. De plus, dans notre implantation, nous faisons l'interpolation d'une fraction rationnelle univariée par algèbre linéaire.

En niveau 2, le degré total du numérateur de degré 14 de $\Phi_{1,2}(X)$ est 9 et celui du dénominateur D'_2 est 7. Pour calculer le dénominateur, il suffit de faire $(9+7+2)(5+1)(4+1) = 540$ évaluations. Une fois que nous les avons faites, nous faisons $(33+1)(17+1)(16+1) = 10404$ évaluations pour calculer les numérateurs (voir le tableau 4.1). Tout ceci peut être fait à une précision de 100 chiffres décimaux. Une évaluation prend environ 1.33 secondes de telle sorte que le dénominateur peut être calculé en environ 12 minutes et tous les polynômes en 4 heures (sur un

seul processeur).

En niveau 3, les degrés totaux sont 35 pour le numérateur du coefficient de degré 39 de $\Phi_{1,3}$ et également 35 pour le dénominateur. Le dénominateur peut être calculé avec $(35+35+2)(20+1)(17+1) = 27216$ évaluations en 17 heures à précision 300 et puis tous les numérateurs avec $(92+1)(52+1)(49+1) = 246450$ évaluations (voir le tableau 4.2) en environ 30 jours à précision 1000. L'interpolation prend environ 1 heure.

Pour calculer les polynômes modulaires avec les $\mathfrak{b}_i$, on peut utiliser les résultats trouvés dans les sections 4.3.2 et 4.4. En particulier, on ne doit calculer que les deux premiers polynômes modulaires.

Pour $p = 3$, les degrés totaux sont 25 et 24 pour le numérateur et dénominateur du 39-ième coefficient. Il faut environ $(25+24+2)(12+1)(12+1)/32 \approx 270$ évaluations pour obtenir le dénominateur et environ $(40+1)(19+1)(18+1)/32 \approx 487$ pour les numérateurs (voir tableau 4.3). Nous utilisons 100 chiffres décimaux pour la précision et ensuite une évaluation prend approximativement 0.6 secondes de telle sorte que les deux (et donc trois) polynômes modulaires peuvent être obtenus en moins de 10 minutes (la phase d'interpolation est négligeable).

Pour $p = 5$, les degrés totaux sont 121 et 120 pour le numérateur et dénominateur du 155-ième coefficient. Le nombre théorique d'évaluations pour calculer le dénominateur et tous les numérateurs est $(121+120+2)(72+1)(72+1)/32 < 40500$ et $(156+1)(97+1)(94+1)/32 < 46000$ (voir tableau 4.4). Les calculs peuvent être fait à une précision de 1000 chiffres décimaux où chaque évaluation prend environ 12 secondes. Les polynômes peuvent être calculés en moins de 12 jours (sur un processeur). La phase d'interpolation peut être faite en moins de 2 heures.

Pour $p = 7$, nous n'avons eu d'autre choix que de calculer d'abord le dénominateur commun car les deux polynômes prennent 29 Go d'espace mémoire et les calculs intermédiaires beaucoup plus. De plus, nous avons constaté que le coefficient dominant du dénominateur en $\mathfrak{b}_1$ est respectivement $2^{10}\mathfrak{b}_2^6\mathfrak{b}_3^6\mathfrak{b}_1^{10}$ et $2^{70}\mathfrak{b}_2^{10}\mathfrak{b}_3^{10}\mathfrak{b}_1^{70}$ pour $p = 3$ et 5, de telle sorte que nous avons conjecturé qu'il serait similaire pour $p = 7$. Après quelques expériences, nous avons compris qu'il devait être égal à $2^{226}\mathfrak{b}_2^{38}\mathfrak{b}_3^{38}\mathfrak{b}_1^{226}$. En connaissant ce monôme, nous n'avons pas eu besoin d'utiliser le degré total pour l'interpolation, comme expliqué dans la partie de la section sur l'interpolation où l'on explique le cas spécial où un monôme de la fraction est connu. Ceci nous a permis de réduire significativement le nombre d'évaluations, car ce nombre, au lieu de dépendre du degré total, ne dépend plus que du degré de $\mathfrak{b}_1$. En effet, les degrés en $\mathfrak{b}_1$ du 399-ième coefficient sont 233 et 226, tandis que les degrés totaux sont 337 et 336. Le nombre d'évaluation pour le calcul du dénominateur est d'environ $(233+226+2)(226+1)(226+1)/32 < 727000$ et pour les numérateurs des deux premiers polynômes modulaires d'environ $(400+1)(279+1)(276+1)/32 < 972000$ (voir tableau 4.4). Pour le dénominateur, on a réussi à le calculer en moins de 700 jours à précision 2000 tandis que pour les numérateurs il nous a fallu environ 2000 jours à précision 3000. L'interpolation nous a pris autour d'une semaine ; c'est négligeable par rapport au temps d'évaluation.

Finalement, notons que chaque évaluation est indépendante des autres ce qui fait que le calcul des polynômes modulaires est parallélisable. L'interpolation d'un coefficient est indépendant de l'interpolation des autres coefficients ; donc l'interpolation est également parallélisable.

4.6 Exemples de courbes p-isogènes

L'objectif principal des polynômes modulaires est de trouver des courbes hyperelliptiques qui ont des Jacobiennes isogènes. En particulier, ces courbes peuvent être sur un corps fini car les p-polynômes modulaires que nous avons obtenus peuvent être réduits modulo un nombre premier $\ell \neq p$ tout en conservant leur interprétation, d'après un argument que l'on peut trouver dans [8, Section 6 page 511].

Nous donnons des exemples avec les différents polynômes que nous avons calculés. Notons que l'algorithme que nous avons présenté est heuristique parce que nous n'avons pas de bornes pour la perte de précision et la taille des coefficients et nous n'avons pas de preuve que nos polynômes sont corrects. On aurait pu faire tous les calculs en utilisant une arithmétique d'intervalle mais nous préférons vérifier heuristiquement la justesse des polynômes en les testant sur des matrices des périodes aléatoires qui n'ont pas servi dans l'algorithme d'évaluation/interpolation. Pour un certain $\Omega \in \mathcal{H}_2$, il faut vérifier que

$$\Phi_{1,p}(f_{1,p}(\Omega), f_1(\Omega), f_2(\Omega), f_3(\Omega)) = 0$$

et que pour $\ell = 2, 3$,

$$f_{\ell,p}(\Omega) = \Psi_{\ell,p}(f_{1,p}(\Omega), f_1(\Omega), f_2(\Omega), f_3(\Omega))/\Phi'_{1,p}(f_{1,p}(\Omega), f_1(\Omega), f_2(\Omega), f_3(\Omega)).$$

Avec un seul calcul à haute précision, on peut être virtuellement certain que le résultat est correct.

Les Jacobiennes des courbes suivantes sont des variétés 3-isogènes entre elles. Nous avons trouvé ces courbes grâce aux polynômes avec les invariants de Streng (pour $p = 3$ bien entendu). Les premières sont sur $\mathbb{F}_{5261}$:

$$\begin{aligned} Y^2 &= 272X^5 + 4278X^4 + 4297X^3 + 4063X^2 + 1069X + 2998, \\ Y^2 &= 695X^5 + 2322X^4 + 3115X^3 + 4588X^2 + 1453X + 655 \end{aligned}$$

et les autres sur $\mathbb{F}_{2534267893}$:

$$\begin{aligned} Y^2 &= 1774507961X^6 + 48872812X^5 + 2028583210X^4 + 1092030439X^3 + \\ &\quad 671225738X^2 + 2233670825X + 608155867, \\ Y^2 &= 1927466494X^6 + 2286039407X^5 + 1720123333X^4 + 87910848X^3 + \\ &\quad 2422852850X^2 + 183139891X + 825611194. \end{aligned}$$

Nous donnons également deux exemples de courbes dont les Jacobiennes sont 5-isogènes et qui ont été trouvées grâce aux polynômes avec les $\mathfrak{b}_i$. Sur $\mathbb{F}_{101}$:

$$\begin{aligned} Y^2 &= 27X^5 + 71X^4 + 91X^3 + 59X^2 + 5X + 14, \\ Y^2 &= 29X^5 + 26X^4 + 38X^3 + 20X^2 + 7X + 51 \end{aligned}$$

et sur $\mathbb{F}_{4294967311}$:

$$\begin{aligned} Y^2 &= 2420332800X^5 + 3653091983X^4 + 2536585478X^3 + 2805510580X^2 + \\ &\quad 159741347X + 2690010753, \\ Y^2 &= 4076826784X^5 + 2616936853X^4 + 3748957676X^3 + 1209100179X^2 + \\ &\quad 3172892980X + 1266950302. \end{aligned}$$

Enfin, nous donnons deux paires de courbes avec des Jacobiennes 7-isogènes, calculées en utilisant les polynômes modulaires avec les $\mathfrak{b}_i$. Sur $\mathbb{F}_{10009}$:

$$\begin{aligned} Y^2 &= 4826X^5 + 471X^4 + 2876X^3 + 5411X^2 + 7948X + 1308, \\ Y^2 &= 7218X^5 + 7699X^4 + 7011X^3 + 7103X^2 + 1845X + 4087 \end{aligned}$$

et sur $\mathbb{F}_{3452678353}$:

$$\begin{aligned} Y^2 &= 393356368X^5 + 1698662093X^4 + 471351782X^3 + 448279016X^2 + \\ &\quad 1342046779X + 3241061457, \\ Y^2 &= 2171506943X^5 + 2231412358X^4 + 2005208933X^3 + 580698082X^2 + \\ &\quad 306153493X + 474327543. \end{aligned}$$

Le lecteur motivé peut vérifier que les courbes que nous donnons ont bel et bien les propriétés que nous leurs donnons : il suffit pour cela de calculer leurs fonctions zéta et voir si elles sont identiques ou pas (voir [82]).

Chapitre 5

Polynômes modulaires d'Hilbert

Dans ce dernier chapitre, nous allons introduire une définition de polynômes modulaires pour des surfaces abéliennes principalement polarisées qui ont multiplication réelle par un corps de nombres quadratique réel $K = \mathbb{Q}(\sqrt{D})$. Au lieu d'être sur $\mathcal{H}_2/\Gamma_2$, nous allons nous placer sur la surface de Hilbert $\mathcal{H}_1^2/\operatorname{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$, qui s'envoie sur une surface de Humbert de l'espace précédent. L'équivalent des j-invariants ici sont les invariants de Gundlach, qui n'ont été définis que pour $D = 5$. Nous allons en définir pour $D = 2$ et montrerons comment réutiliser les techniques du chapitre précédent pour calculer nos nouveaux polynômes modulaires. Enfin, nous allons définir des thêta constantes sur l'espace de Hilbert et donnerons un algorithme de calcul de ces polynômes modulaires avec des invariants définis à partir de ces thêta constantes pour tout $K = \mathbb{Q}(\sqrt{D})$.

Les références principales pour ce chapitre sont [56, 54, 72, 71, 36, 42, 43, 44, 74, 35].

5.1 Espaces modulaires d'Hilbert et de Siegel

5.1.1 Espace modulaire de Hilbert

Soit D un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{D})$ un corps quadratique réel. Son discriminant Δ_K est D si $D \equiv 1 \bmod 4$ et $4D$ si $D \equiv 2, 3 \bmod 4$. Considérons $\mathcal{O}_K$ l'anneau des entiers de K. On a que $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$, où $\omega = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \bmod 4$ et $\omega = \sqrt{D}$ sinon. Notons par $\overline{a}$ le conjugué de a dans $\mathcal{O}_K$.

Rappelons que l'ensemble $\mathcal{H}_1 = \{z \in \mathbb{C} : \Im(z) > 0\}$ est le *demi-plan de Poincaré*. Le groupe $\operatorname{SL}_2(\mathcal{O}_K)$ agit par la gauche sur $\mathcal{H}_1^2$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z_1, z_2) = \left(\frac{az_1 + b}{cz_1 + d}, \frac{\overline{a}z_2 + \overline{b}}{\overline{c}z_2 + \overline{d}} \right).$$

L'espace quotient $\mathcal{H}_1^2/\operatorname{SL}_2(\mathcal{O}_K)$ est la *surface modulaire de Hilbert*, qui paramétrise les surfaces abéliennes principalement polarisées ayant multiplication réelle par l'ordre maximal $\mathcal{O}_K$ (voir section 2.5.2).

Pour $\lambda \in K$ et $z = (z_1, z_2) \in \mathcal{H}_1^2$, on note

$$\lambda z = (\lambda z_1, \overline{\lambda} z_2), \qquad \mathrm{N}(z) = z_1 z_2 \qquad \text{et} \qquad \mathrm{tr}(z) = z_1 + z_2.$$

On définit σ comme étant l'involution

$$\sigma : (z_1, z_2) \in \mathcal{H}_1^2 \longmapsto (z_2, z_1) \in \mathcal{H}_1^2.$$

Définition 5.1.1. *Soit Γ un sous-groupe de $\mathrm{SL}_2(\mathcal{O}_K)$. Une fonction holomorphe f sur $\mathcal{H}_1^2$ est appelée* une forme modulaire de Hilbert de poids k pour le sous-groupe Γ *si elle satisfait pour chaque $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ et $z = (z_1, z_2) \in \mathcal{H}_1^2$ la condition $f(\gamma z) = \mathrm{N}(cz + d)^k f(z)$. Si de plus elle vérifie $f(\sigma(z)) = f(z)$ pour tout $z \in \mathcal{H}_1^2$, alors on dit de cette forme modulaire qu'elle est* symétrique. *Une* fonction modulaire de Hilbert *est le quotient de deux formes modulaires de Hilbert de même poids pour le même groupe. On ajoute qu'elle est symétrique si les deux formes le sont.*

Théorème 5.1.2. *La surface modulaire de Hilbert $\mathcal{H}_1^2/\mathrm{SL}_2(\mathcal{O}_K)$ est rationnelle seulement pour $D = 2, 3, 5, 6, 7, 13, 15, 17, 21, 33$.*

Démonstration. Voir [41, Théorème 2] □

On ne connaît les deux générateurs de la surface modulaire symétrique de Hilbert $\mathcal{H}_1^2/(\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma)$ que pour $D = 2$ et 5. On se concentrera sur ces deux cas à présent. Soit $\epsilon > 0$ une unité dont sa norme vérifie $\epsilon\overline{\epsilon} = -1$. On peut prendre $1 + \sqrt{2}$ et $\frac{1+\sqrt{5}}{2}$ pour respectivement $D = 2$ et $D = 5$. Posons

$$q_1 = \exp\left(2\imath\pi(\epsilon z_1 - \overline{\epsilon} z_2)/\sqrt{\Delta_K}\right) \qquad \text{et} \qquad q_2 = \exp\left(2\imath\pi(z_2 - z_1)/\sqrt{\Delta_K}\right).$$

Proposition 5.1.3. *Soit g une forme modulaire de Hilbert pour $\mathrm{SL}_2(\mathcal{O}_K)$ de poids k. Alors elle a un développement de Fourier de la forme :*

$$g(z) = a_g(0) + \sum_{t = a + b\overline{\epsilon} \in \mathcal{O}_K^+} a_g(t) q_1^a q_2^b.$$

Démonstration. Voir [56, Proposition 3.2 (1)]. □

Notons $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ le $\mathbb{Z}$-module des formes modulaires symétriques de Hilbert de poids pair k ayant des coefficients de Fourier rationnels et posons $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K)) = \bigoplus A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$. Définissons la série d'Eisenstein de poids pair $k \geq 2$ par

$$G_k(z) = 1 + \sum_{t = a + b\overline{\epsilon} \in \mathcal{O}_K^+} b_k(t) q_1^a q_2^b,$$

où

$$b_k(t) = \kappa_k \sum_{t\mathcal{O}_K \subseteq \mu\mathcal{O}_K} |\mathcal{O}_K/\mu\mathcal{O}_K|^{k-1}$$

et $\kappa_k = \zeta_K(k)^{-1}(2\pi)^{2k}((k-1)!)^{-2}\Delta_K^{1/2-k}$.

Lemme 5.1.4.
— *Si $K = \mathbb{Q}(\sqrt{2})$, alors $\kappa_2 = 2^4 \cdot 3$, $\kappa_4 = 2^5 \cdot 3 \cdot 5 \cdot 11^{-1}$ et $\kappa_6 = 2^4 \cdot 3^2 \cdot 7 \cdot 19^{-2}$;*
— *Si $K = \mathbb{Q}(\sqrt{5})$, alors $\kappa_2 = 2^3 \cdot 3 \cdot 5$, $\kappa_4 = 2^4 \cdot 3 \cdot 5$, $\kappa_6 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 67^{-1}$ et $\kappa_{10} = 2^3 \cdot 3 \cdot 5^2 \cdot 11 \cdot 412751^{-1}$.*

Démonstration. Voir [71, Lemme 1.1]. □

Les séries d'Eisenstein sont des formes modulaires symétriques pour $\mathrm{SL}_2(\mathcal{O}_K)$ avec des coefficients dans $\mathbb{Q}$. De plus, on a

Théorème 5.1.5. *Dans le cas $K = \mathbb{Q}(\sqrt{2})$, on pose*

$$H_4 = 2^{-6}\cdot 3^{-2}\cdot 11(G_2^2 - G_4) \quad et \quad H_6 = \frac{-5\cdot 7^2}{2^8 3^3 13} G_2^3 + \frac{11\cdot 59}{2^8 3^2 5\cdot 13} G_2 G_4 - \frac{19^2}{2^7 3^3 5\cdot 13} G_6.$$

Alors G_2, H_4 et H_6 sont dans $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ pour respectivement $k = 2, 4, 6$. De plus, elles forment un ensemble minimal de générateurs de $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))$ sur $\mathbb{Z}$.

Démonstration. Voir [71, Théorème 1]. □

Théorème 5.1.6. *Dans le cas $K = \mathbb{Q}(\sqrt{2})$, le corps des fonctions modulaires symétriques de Hilbert pour $\mathrm{SL}_2(\mathcal{O}_K)$ sont des fonctions rationnelles en*

$$\mathfrak{J}_1 = \frac{G_2^2}{H_4} \quad et \quad \mathfrak{J}_2 = \frac{G_2 H_6}{H_4^2}.$$

On appelle $\mathfrak{J}_1$ et $\mathfrak{J}_2$ les invariants de Gundlach *pour K.*

Démonstration. Une preuve de ce théorème sera donnée à la page 149. □

Théorème 5.1.7. *Dans le cas $K = \mathbb{Q}(\sqrt{5})$, on pose*

$$H_6 = \frac{67}{2^5 3^3 5^2}(G_2^3 - G_6),$$

$$H_{10} = 2^{-10}3^{-5}5^{-5}7^{-1}(412751 G_{10} - 5\cdot 67\cdot 2293 G_2^2 G_6 + 2^2 3\cdot 7\cdot 4231 G_2^5)$$

$$et \qquad H_{12} = 2^{-2}(H_6^2 - G_2 H_{10}).$$

Les quatre formes modulaires G_2, H_6, H_{10} et H_{12} sont dans $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ pour $k = 2, 6, 10$ et 12 respectivement. De plus, elles forment un ensemble minimal de générateurs de $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))$ sur $\mathbb{Z}$.

Démonstration. Voir [36] ou [71, Théorème 2]. □

Théorème 5.1.8. *Dans le cas $K = \mathbb{Q}(\sqrt{5})$, le corps des fonctions modulaires symétriques de Hilbert pour $\mathrm{SL}_2(\mathcal{O}_K)$ sont des fonctions rationnelles en*

$$\mathfrak{J}_1 = \frac{G_2^5}{H_{10}} \quad et \quad \mathfrak{J}_2 = \frac{H_6 G_2^2}{H_{10}}.$$

On appelle $\mathfrak{J}_1$ et $\mathfrak{J}_2$ les invariants de Gundlach *pour K.*

Démonstration. Voir [36]. Notons qu'il est usuel de prendre les invariants $\frac{G_2^5}{H_{10}}$ et $\frac{H_6}{G_2^3}$. Nous avons choisi de remplacer ce dernier par le produit de ces deux afin d'avoir le même dénominateur pour les deux invariants de Gundlach. □

5.1.2 De Hilbert à Siegel

Soient $z = (z_1, z_2) \in \mathcal{H}_1^2$, $x \in K$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$. Notons

$$z^* = \left(\begin{smallmatrix} z_1 & 0 \\ 0 & z_2 \end{smallmatrix}\right), \qquad x^* = \left(\begin{smallmatrix} x & 0 \\ 0 & \overline{x} \end{smallmatrix}\right) \qquad \text{et} \qquad \gamma^* = \left(\begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix}\right).$$

Fixons e_1, e_2 une $\mathbb{Z}$-base de $\mathcal{O}_K$ et définissons les matrices

$$R = \left(\begin{smallmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{smallmatrix}\right) \qquad \text{et} \qquad S = \left(\begin{smallmatrix} {}^tR & 0 \\ 0 & R^{-1} \end{smallmatrix}\right)$$

et les applications

$$\phi_{e_1,e_2}: \begin{array}{ccc} \mathcal{H}_1^2 & \longrightarrow & \mathcal{H}_2 \\ z & \longmapsto & {}^tRz^*R \end{array} \quad \text{et} \quad \phi_{e_1,e_2}: \begin{array}{ccc} \mathrm{SL}_2(K) & \longrightarrow & \mathrm{Sp}_4(\mathbb{Q}) \\ \gamma & \longmapsto & S\gamma^*S^{-1}. \end{array}$$

Soit

$$\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K) : a, d \in \mathcal{O}_K, b \in \partial_K^{-1} \text{ et } c \in \partial_K \right\}.$$

Comme $K = \mathbb{Q}(\sqrt{D})$, on a que $\partial_K = \sqrt{\Delta_K}\mathcal{O}_K$ et $\partial_K^{-1} = \frac{1}{\sqrt{\Delta_K}}\mathcal{O}_K$. Le groupe $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ est engendré par les matrices

$$\begin{pmatrix} 1 & 1/\sqrt{\Delta_K} \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & \omega/\sqrt{\Delta_K} \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & -1/\sqrt{\Delta_K} \\ \sqrt{\Delta_K} & 0 \end{pmatrix}.$$

Proposition 5.1.9. *L'application ϕ_{e_1,e_2} satisfait :*
- *$\phi_{e_1,e_2}^{-1}(\Gamma_2) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$;*
- *$\phi_{e_1,e_2}(\gamma \cdot z) = \phi_{e_1,e_2}(\gamma) \cdot \phi_{e_1,e_2}(z)$ pour tous $\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ et $z \in \mathcal{H}_1^2$;*
- *Si f_1, f_2 est une autre $\mathbb{Z}$-base de $\mathcal{O}_K$, alors il existe un certain $\gamma \in \Gamma_2$ tel que pour tout $z \in \mathcal{H}_1^2$, $\phi_{e_1,e_2}(z) = \gamma \cdot \phi_{f_1,f_2}(z)$;*
- *Il existe un certain $\gamma \in \Gamma_2$ tel que $\phi_{e_1,e_2}(\sigma(z)) = \gamma \cdot \phi_{e_1,e_2}(z)$.*

Démonstration. La preuve est calculatoire. Nous renvoyons à [56, Proposition 3.1]. □

L'application ϕ_{e_1,e_2} fournit donc une application holomorphe de $\mathcal{H}_1^2/\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ vers $\mathcal{H}_2/\Gamma_2$ qui est indépendante du choix de la base de $\mathcal{O}_K$. Elle envoie aussi z et $\sigma(z)$ vers le même point de $\mathcal{H}_2/\Gamma_2$.

La base que nous choisissons est $e_1 = 1$ et $e_2 = \omega$. Nous noterons ϕ au lieu de $\phi_{1,\omega}$. On a alors que $\phi(z) = \begin{pmatrix} z_1+z_2 & z_1\omega+z_2\overline{\omega} \\ z_1\omega+z_2\overline{\omega} & z_1\omega^2+z_2\overline{\omega}^2 \end{pmatrix} = \begin{pmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{pmatrix} \in \mathcal{H}_2$ et cette application vérifie

$$\begin{array}{rcl} \frac{D-1}{4}\Omega_1 + \Omega_2 - \Omega_3 & = 0 & \text{si } D \equiv 1 \bmod 4; \\ D\Omega_1 - \Omega_3 & = 0 & \text{si } D \equiv 2,3 \bmod 4. \end{array} \tag{5.1}$$

De plus, posons

$$M = \begin{cases} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \text{si } D \equiv 1 \bmod 4; \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \text{si } D \equiv 2,3 \bmod 4. \end{cases} \tag{5.2}$$

La matrice M satisfait

$$\phi(\sigma(z)) = M \cdot \phi(z). \tag{5.3}$$

Considérons maintenant $\gamma = \begin{pmatrix} a+a'\omega & (b+b'\omega)/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}(c+c'\omega) & d+d'\omega \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. Alors

$$\phi(\gamma) = \begin{cases} \begin{pmatrix} a & a' & b' & b+b' \\ (\frac{D-1}{4})a' & a+a' & b+b' & b+(\frac{D+3}{4})b' \\ (\frac{D-1}{4})c'-c & c & d & (\frac{D-1}{4})d' \\ c & c' & d' & d+d' \end{pmatrix} & \text{si } D \equiv 1 \bmod 4; \\ \begin{pmatrix} a & a' & b' & b \\ Da' & a & b & Db' \\ Dc' & c & d & Dd' \\ c & c' & d' & d \end{pmatrix} & \text{si } D \equiv 2,3 \bmod 4. \end{cases} \tag{5.4}$$

Lorsque l'unité fondamentale a norme -1, il existe un isomorphisme qui permet de se placer sur $\mathrm{SL}_2(\mathcal{O}_K)$ au lieu de $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. Soient $\epsilon > 0$ une telle unité et $\alpha = \mathrm{diag}(1, \frac{\sqrt{\Delta_K}}{\epsilon})$, alors

$$\begin{array}{rccc} \phi_0 : & \mathcal{H}_1^2 & \longrightarrow & \mathcal{H}_1^2 \\ & z & \longmapsto & \frac{\epsilon}{\sqrt{\Delta_K}} z \end{array} \quad \text{et} \quad \begin{array}{rccc} \phi_0 : & \mathrm{SL}_2(\mathcal{O}_K) & \longrightarrow & \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \\ & \gamma & \longmapsto & \alpha\gamma\alpha^{-1} \end{array}$$

sont des bijections. Notons que ceci ne fonctionne que lorsque ϵ a norme -1 afin que $\frac{\epsilon}{\sqrt{\Delta_K}}$ soit totalement positif et $\phi_0(z) \in \mathcal{H}_1^2$. Soit $\phi_1 := \phi_{1,\bar{\epsilon}}$ et $\phi_\epsilon := \phi_1 \circ \phi_0$. La base $\{1, \bar{\epsilon}\}$ est la base que nous avons utilisée pour définir les formes modulaires symétriques de Hilbert de la section précédente. L'application ϕ_ϵ vérifie des propriétés similaires à celles de la proposition 5.1.9. Reconcentrons nous sur les cas $D = 2$ et $D = 5$. Notons

$$Sym_2(\mathbb{Z})^\vee = \left\{ T = \begin{pmatrix} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{pmatrix} : m_i, m \in \mathbb{Z} \right\}$$

le dual de $Sym_2(\mathbb{Z})$ (les matrices symétriques de taille 2 dans $\mathbb{Z}$) et $Sym_2(\mathbb{Z})^{\vee,+}$ le sous-ensemble de $Sym_2(\mathbb{Z})^\vee$ des matrices définies positives.

Proposition 5.1.10. *Soit*

$$f(\Omega) = a_f(0) + \sum_{T \in Sym_2(\mathbb{Z})^{\vee,+}} a_f(T) q^T$$

une forme modulaire de Siegel pour Γ_2 de poids k. Alors son tiré en arrière $g = \phi_\epsilon^* f$ est une forme modulaire symétrique de Hilbert avec le développement de Fourier suivant :

$$g(z) = f(\phi_\epsilon(z)) = a_g(0) + \sum_{t = a + b\bar{\epsilon} \in \mathcal{O}_K^+} a_g(t) q_1^a q_2^b,$$

avec $a_g(0) = a_f(0)$ et

$$a_g(t) = \sum_{\substack{T \in Sym_2(\mathbb{Z})^{\vee,+} \\ Q_T(1,\bar{\epsilon}) = t}} a_f(T).$$

Ici, $Q_T(x_1, x_2) = (x_1, x_2) T \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right)$ est la forme quadratique définie positive associée à T. Enfin, $q^T = \exp(2\imath\pi \mathrm{tr}(T\Omega))$.

Démonstration. Voir [56, Proposition 3.2]. □

Nous nous intéressons aux tirés en arrière des invariants d'Igusa. Ils sont déjà connus lorsque $D = 5$.

Théorème 5.1.11. *Pour $K = \mathbb{Q}(\sqrt{5})$, on a*

$$\begin{array}{rcl} \phi_\epsilon^* \psi_4 & = & G_2^2; \\ \phi_\epsilon^* \psi_6 & = & -\frac{42}{25} G_2^3 + \frac{67}{25} G_6 = G_2^3 - 2^5 3^3 H_6; \\ -4\phi_\epsilon^* \chi_{10} & = & H_{10}; \\ 12\phi_\epsilon^* \chi_{12} & = & 3H_6^2 - 2G_2 H_{10}. \end{array}$$

Démonstration. Voir [72, Théorème 1]. □

Corollaire 5.1.12. *On a*

$$\begin{aligned}\phi_\epsilon^*\mathfrak{j}_1 &= 8\mathfrak{J}_1(3\mathfrak{J}_2^2/\mathfrak{J}_1-2)^5;\\ \phi_\epsilon^*\mathfrak{j}_2 &= \tfrac{1}{2}\mathfrak{J}_1(3\mathfrak{J}_2^2/\mathfrak{J}_1-2)^3;\\ \phi_\epsilon^*\mathfrak{j}_3 &= 2^{-3}\mathfrak{J}_1(3\mathfrak{J}_2^2/\mathfrak{J}_1-2)^2(4\mathfrak{J}_2^2/\mathfrak{J}_1+2^5 3^2\mathfrak{J}_2/\mathfrak{J}_1-3).\end{aligned}$$

Démonstration. C'est une conséquence du théorème précédent et de la définition 3.9 des invariants d'Igusa en séries. Voir aussi [56, Proposition 4.5]. □

En utilisant la proposition 5.1.10 et en comparant les différentes séries de Fourier (comme il est fait dans [72] dans le cas $D = 5$), nous avons trouvé :

Théorème 5.1.13. *Pour $K = \mathbb{Q}(\sqrt{2})$, on a*

$$\begin{aligned}\phi_\epsilon^*\psi_4 &= G_2^2+144H_4;\\ \phi_\epsilon^*\psi_6 &= G_2^3-648H_4G_2-1728H_6;\\ \phi_\epsilon^*\chi_{10} &= -\tfrac{1}{4}H_4H_6;\\ \phi_\epsilon^*\chi_{12} &= \tfrac{1}{12}G_2H_4H_6+H_4^3+H_6^2.\end{aligned}$$

Corollaire 5.1.14. *On a*

$$\begin{aligned}\phi_\epsilon^*\mathfrak{j}_1 &= 8\mathfrak{J}_1^3/\mathfrak{J}_2(1+12/\mathfrak{J}_2+12\mathfrak{J}_2/\mathfrak{J}_1)^5;\\ \phi_\epsilon^*\mathfrak{j}_2 &= \mathfrak{J}_1^2/\mathfrak{J}_2/2(\mathfrak{J}_1+144)(1+12/\mathfrak{J}_2+12\mathfrak{J}_2/\mathfrak{J}_1)^3;\\ \phi_\epsilon^*\mathfrak{j}_3 &= \tfrac{1}{8}(1+12/\mathfrak{J}_2+12\mathfrak{J}_2/\mathfrak{J}_1)^2\cdot\\ &\quad(\mathfrak{J}_1^3/\mathfrak{J}_2+16\mathfrak{J}_1^2+16\mathfrak{J}_1^3/\mathfrak{J}_2^2+2304\mathfrak{J}_1^2/\mathfrak{J}_2^2+408\mathfrak{J}_1^2/\mathfrak{J}_2+2880\mathfrak{J}_1).\end{aligned}$$

5.2 Surfaces de Humbert

Soit $\Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right) \in \mathcal{H}_2$ et $a, b, c, d, e \in \mathbb{Z}$. On appelle une équation de la forme :

$$a\Omega_1 + b\Omega_2 + c\Omega_3 + d(\Omega_2^2 - \Omega_1\Omega_3) + e = 0 \tag{5.5}$$

une *relation singulière*. Si de plus $\operatorname{pgcd}(a, b, c, d, e) = 1$, on dit de cette relation qu'elle est *primitive*. Enfin, on définit le *discriminant* d'une relation singulière comme étant $\Delta = b^2 - 4ac - 4de$.

Proposition 5.2.1. *Soit $\Omega \in \mathcal{H}_2$ satisfaisant une relation singulière de discriminant Δ. Alors pour tout $\gamma \in \Gamma_2$, $\gamma \cdot \Omega$ satisfait aussi une relation singulière de discriminant Δ. Cette dernière relation est primitive lorsque la première l'est.*

Démonstration. Il suffit de montrer cette proposition sur les générateurs de Γ_2. Soient $\mathfrak{M}_1$, $\mathfrak{M}_2$, $\mathfrak{M}_3$ et $\mathfrak{J}$ comme dans l'équation (3.1) et soient $\Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right) \in \mathcal{H}_2$ et des entiers $a, b, c, d, e \in \mathbb{Z}$ tels qu'on ait la relation (5.5). Commençons par $\mathfrak{M}_1$. On a $\mathfrak{M}_1 \cdot \Omega = \left(\begin{smallmatrix}\Omega_1+1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right)$ et alors

$$a(\Omega_1+1) + b\Omega_2 + (c+d)\Omega_3 + d(\Omega_2^2 - (\Omega_1+1)\Omega_3) + e - a = 0$$

est une relation singulière de discriminant $b^2 - 4a(c+d) - 4d(e-a) = \Delta$. Le cas avec $\mathfrak{M}_3$ est très proche de celui avec $\mathfrak{M}_1$. Pour $\mathfrak{M}_2$, on a $\mathfrak{M}_2 \cdot \Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2+1\\ \Omega_2+1 & \Omega_3\end{smallmatrix}\right)$ et il nous faut prendre la relation

$$a\Omega_1 + (b-2d)(\Omega_2+1) + c\Omega_3 + d((\Omega_2+1)^2 - \Omega_1\Omega_3) + e - b + d = 0$$

qui est aussi de discriminant Δ. Enfin, on a $\mathfrak{J} \cdot \Omega = \frac{1}{\Omega_2^2 - \Omega_1\Omega_3} \left(\begin{smallmatrix} \Omega_3 & -\Omega_2 \\ -\Omega_2 & \Omega_1 \end{smallmatrix} \right)$. On a alors la relation singulière

$$c\frac{\Omega_3}{\Omega_2^2 - \Omega_1\Omega_3} - b\frac{-\Omega_2}{\Omega_2^2 - \Omega_1\Omega_3} + a\frac{\Omega_1}{\Omega_2^2 - \Omega_1\Omega_3} + e\frac{1}{\Omega_2^2 - \Omega_1\Omega_3} + d = 0$$

qui est bien de discriminant Δ. □

Théorème 5.2.2 (Lemme d'Humbert)**.** *Soit* $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix} \right)$ *satisfaisant la relation primitive singulière :*

$$a\Omega_1 + b\Omega_2 + c\Omega_3 + d(\Omega_2^2 - \Omega_1\Omega_3) + e = 0$$

de discriminant $\Delta = b^2 - 4ac - 4de$*. Alors il existe une matrice* $\gamma \in \Gamma_2$ *telle que* $\gamma \cdot \Omega = \left(\begin{smallmatrix} \Omega'_1 & \Omega'_2 \\ \Omega'_2 & \Omega'_3 \end{smallmatrix} \right)$ *vérifie une unique relation normalisée de la forme :*

$$k\Omega'_1 + \ell\Omega'_2 - \Omega'_3 = 0 \tag{5.6}$$

où k *et* ℓ *sont déterminés uniquement par* $\Delta = 4k + \ell$ *et* $\ell \in \{0, 1\}$*.*

Démonstration. Voir [42, 43, 44]. □

Remarque 5.2.3. *En écrivant l'équation (5.6) avec* $\Delta = \Delta_{\mathbb{Q}(\sqrt{D})}$*, on retrouve l'équation (5.1).*

Soit $\Omega \in \mathcal{H}_2$ satisfaisant une relation singulière de discriminant Δ. Un algorithme constructif pour calculer γ comme dans le lemme d'Humbert peut être trouvé dans [5, 74]. L'algorithme 5.2.1, que nous avons pris de [5], permet de calculer cette matrice γ dans un cadre général. Il fournit alors une preuve du lemme d'Humbert dans le cas où les entiers $g_0, \ldots, g_3$ qui apparaissent dans cet algorithme sont non nuls.

Proposition 5.2.4. *Pour tout* $\Delta \equiv 0$ *ou* $1 \bmod 4$*,* $\Delta > 0$*, l'ensemble* $H_\Delta := \{\Omega \in \mathcal{H}_2/\Gamma_2 : \Omega$ *satisfait une relation primitive singulière de discriminant* $\Delta\}$ *est une surface dite* surface de Humbert de discriminant Δ*.*

Démonstration. Voir [35, Proposition 2.11]. □

Proposition 5.2.5. *Soit* A_Ω *la surface abélienne principalement polarisée associée à* $\Omega \in \mathcal{H}_2$*. Soit aussi* $\Delta \neq \Delta'$ *deux discriminants qui ne sont pas des carrés. Alors :*

- *—* A_Ω *est simple si et seulement si* $\Omega \notin \bigcup_{m>0} H_{m^2}$ *;*
- *— Si* $\Omega \in H_\Delta$*, alors* $\mathrm{End}(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ *contient* $\mathbb{Q}(\sqrt{\Delta})$ *;*
- *— Si* $\Omega \in H_\Delta \cap H_{\Delta'}$*, alors soit* A_Ω *est simple et* $\mathrm{End}(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ *est une algèbre de quaternions totalement indéfinie sur* $\mathbb{Q}$*, ou* A_Ω *est isogène à* $E \times E$*, où* E *est une courbe elliptique.*

Démonstration. Voir [35, Proposition 2.15]. □

Notons désormais $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. La proposition 5.1.9 et les équations (5.1), (5.2), (5.3) disent que l'image par ϕ de $\mathcal{H}_1^2/\tilde{\Gamma}$ et de $\mathcal{H}_1^2/(\tilde{\Gamma} \cup \tilde{\Gamma}\sigma)$ sont dans la surface de Humbert de discriminant Δ_K. C'est également vrai pour ϕ_{e_1,e_2} parce que les images de z par ϕ et par ϕ_{e_1,e_2} sont équivalentes modulo l'action de Γ_2 (ce qui signifie que ces applications envoient z vers le même point de la surface de Humbert). Similairement, ϕ_ϵ envoie z vers cette même surface de Humbert, même si les images de z par ϕ_ϵ et par ϕ ne sont pas équivalentes modulo Γ_2. On a plus précisément :

Algorithme 5.2.1 : Calcul du représentant normalisé sur une surface de Humbert

Entrée : $\Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right) \in \mathcal{H}_2$ satisfaisant la relation primitive singulière (5.5) de discriminant $\Delta = b^2 - 4ac - 4de$.

Sortie : Une matrice $\gamma \in \Gamma_2$ telle que $\gamma \cdot \Omega$ satisfait l'équation (5.6).

Notons $R_0 = \left(\begin{smallmatrix} 0 & a & 0 & d\\ -c & b & -d & 0\\ 0 & e & 0 & -c\\ -e & 0 & a & b\end{smallmatrix}\right)$.

1 Choisir des entiers α et β tels que $\alpha e - \beta c = \mathrm{pgcd}(e, c) =: g_0$. Alors $M_0 = \left(\begin{smallmatrix} 1 & 0 & 1 & 0\\ 0 & \alpha & 0 & \beta\\ -1 & 0 & 0 & 0\\ 0 & c/g_0 & 0 & e/g_0\end{smallmatrix}\right)$ est dans Γ_2 et $R_1 = {}^tM_0^{-1} R_0 \, {}^tM_0$ est de la forme $\left(\begin{smallmatrix} A_1 & 0\\ C_1 & {}^tA_1\end{smallmatrix}\right)$, avec $A_1 = \left(\begin{smallmatrix} 0 & a_1\\ -c_1 & b_1\end{smallmatrix}\right)$ et $C_1 = \left(\begin{smallmatrix} 0 & e_1\\ -e_1 & 0\end{smallmatrix}\right)$;

2 Puisque $\mathrm{pgcd}(a_1, c_1, e_1) | g_1 := \mathrm{pgcd}(a_1, e_1)$, le théorème de la progression arithmétique de Dirichlet dit qu'il existe un entier n tel que $p := \frac{e_1}{g_1} + n\frac{a_1}{g_1}$ est un nombre premier avec $|c_1| < p$. Maintenant, $M_1 = \left(\begin{smallmatrix} I_2 & -n & 0\\ & 0 & 0\\ 0 & & I_2\end{smallmatrix}\right) \in \Gamma_2$ et $R_2 := {}^tM_1^{-1} R_1 \, {}^tM_1 = \left(\begin{smallmatrix} A_1 & 0\\ C_2 & {}^tA_1\end{smallmatrix}\right)$ où $C_2 = \left(\begin{smallmatrix} 0 & e_2\\ -e_2 & 0\end{smallmatrix}\right)$ avec $e_2 = e_1 + a_1 n = g_1 p$. En particulier, $\mathrm{pgcd}(c_1, e_2) | g_1$ puisque $|c_1| < g_1$ et ainsi, $\mathrm{pgcd}(c_1, e_2) | a_1$;

3 Choisir des entiers γ et δ tels que $\gamma e_2 - \delta c_1 = \mathrm{pgcd}(e_2, c_1) =: g_2$. Alors $M_2 = \left(\begin{smallmatrix} \gamma a_1/g_2 & 0 & 1 & 0\\ 0 & \gamma & 0 & \delta\\ -1 & 0 & 0 & 0\\ 0 & c_1/g_2 & 0 & e_2/g_2\end{smallmatrix}\right) \in \Gamma_2$ et $R_3 = {}^tM_2^{-1} R_2 \, {}^tM_2$ est de la forme $\left(\begin{smallmatrix} A_3 & 0\\ 0 & {}^tA_3\end{smallmatrix}\right)$ avec $A_3 = \left(\begin{smallmatrix} 0 & a_3\\ -c_3 & b_3\end{smallmatrix}\right)$;

4 Choisir des entiers ϵ et η tels que $\epsilon a_3 + \eta c_3 = \mathrm{pgcd}(a_3, c_3) =: g_3$. Alors $M_3 = \left(\begin{smallmatrix} 1 & 0 & 1 & 0\\ 0 & c_3/g_3 & 0 & -a_3/g_3\\ -\epsilon a_3/g_3 & 0 & \eta c_3/g_3 & 0\\ 0 & \epsilon & 0 & \eta\end{smallmatrix}\right) \in \Gamma_2$ et $R_4 = {}^tM_3^{-1} R_3 \, {}^tM_3$ est de la forme $\left(\begin{smallmatrix} A_4 & 0\\ 0 & {}^tA_4\end{smallmatrix}\right)$ avec $A_4 = \left(\begin{smallmatrix} 0 & a_4 c_4\\ -c_4 & b_4\end{smallmatrix}\right)$;

5 Puisque $\mathrm{pgcd}(b_4, c_4) = 1$, on peut choisir des entiers μ et ν tels que $\mu((a_4+1)c_4 + b_4) + \mu c_4 = \mathrm{pgcd}((a_4+1)c_4 + b_4, c_4) = 1$. Alors $M_4 = \left(\begin{smallmatrix} 1 & 0 & 1 & 0\\ 0 & c_4 & 0 & -(a_4+1)c_4 - b_4\\ -\mu((a_4+1)c_4+b_4) & 0 & \nu c_4 & 0\\ 0 & \mu & 0 & \nu\end{smallmatrix}\right)$ et $M_4' = \left(\begin{smallmatrix} 1 & 0 & 0 & 0\\ -1 & 1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1\end{smallmatrix}\right)$ sont dans Γ_2 et $R_5 = {}^t(M_4 M_4')^{-1} R_4 \, {}^t(M_4 M_4') + c_4 I_4$ est de la forme $\left(\begin{smallmatrix} A_5 & 0\\ 0 & {}^tA_5\end{smallmatrix}\right)$ avec $A_5 = \left(\begin{smallmatrix} 0 & a_5\\ -1 & b_5\end{smallmatrix}\right)$;

6 Soit $\tau = b_5/2$ si b_5 est pair et $\tau = (b_5 - 1)/2$ sinon. Alors $M_5 = \left(\begin{smallmatrix} 1 & 0 & 0 & 0\\ \tau & 1 & 0 & 0\\ 0 & 0 & 1 & -\tau\\ 0 & 0 & 0 & 1\end{smallmatrix}\right) \in \Gamma_2$ et $R_6 = {}^tM_5^{-1} R_5 \, {}^tM_5 - \tau I_4$ est de la forme $\left(\begin{smallmatrix} A_6 & 0\\ 0 & {}^tA_6\end{smallmatrix}\right)$ avec $A_6 = \left(\begin{smallmatrix} 0 & a'\\ -1 & b'\end{smallmatrix}\right)$ avec $b' = 0$ si b_5 est pair et $b' = 1$ si b_5 est impair;

7 $M = M_5 M_4 M_4' M_3 M_2 M_1 M_0$; si $\Delta \equiv 1 \bmod 4$, $M = NM$ avec $N = \left(\begin{smallmatrix} 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{smallmatrix}\right)$;

8 **return** (M) ;

Proposition 5.2.6. *Le diagramme suivant commute :*

$$\begin{array}{ccccc} \mathcal{H}_1^2/\tilde{\Gamma} & \longleftarrow & \mathcal{H}_1^2 & \xrightarrow{\psi} & \mathcal{H}_2 \\ & \searrow^{\pi} & \downarrow & & \downarrow \\ & & \mathcal{H}_1^2/(\tilde{\Gamma}\cup\tilde{\Gamma}\sigma) & \xrightarrow{\rho} & \mathcal{H}_2/\Gamma_2 \end{array}$$

où ψ est soit ϕ_{e_1,e_2}, soit ϕ_ϵ, π est de degré 2 et ρ est une application génériquement de degré 1 vers la surface de Humbert H_{Δ_K}.

Démonstration. Voir [84, Page 328] ou [40, Proposition 8.4]. □

L'espace quotient analytique $\mathcal{H}_1^2/(\tilde{\Gamma}\cup\tilde{\Gamma}\sigma)$ est appelé *surface modulaire symétrique de Hilbert*. L'involution σ identifie les surfaces abéliennes dont la multiplication réelle diffèrent par conjugaison.

Lemme 5.2.7. *Soient X une sous-variété de Y, toutes les deux irréductibles. Alors l'application associée (qui n'est pas définie partout) sur les corps de fonctions $k(Y)\to k(X)$ est surjective.*

Démonstration. Puisque X est une sous-variété de Y, c'est une variété fermée dans un ouvert U de Y. L'inclusion naturelle $i : X\to U$ nous fournit un épimorphisme de faisceaux $i^* : O_U\to O_X$. En regardant les germes des points génériques, on peut en déduire que l'application $k(Y)\to k(X)$ (définie pour des fonctions $f\in k(Y)$ qui sont définies sur les points génériques de X) est surjective. □

Preuve du théorème 5.1.6. La proposition 5.2.6 dit que l'application de l'espace modulaire symétrique de Hilbert vers l'espace de Siegel est birationnelle à son image (la surface de Humbert). Par le lemme 5.2.7, toute fonction modulaire symétrique de Hilbert (vue par birationnalité comme une fonction rationnelle sur la surface de Humbert) peut être relevée en une fonction modulaire de Siegel. Nous savons déjà qu'une fonction modulaire de Siegel est une fonction rationnelle avec des coefficients complexes en les invariants d'Igusa et par le corollaire 5.1.14, les tirés en arrière des invariants d'Igusa peuvent être exprimés en terme des invariants de Gundlach. Toute fonction modulaire symétrique de Hilbert peut être ainsi exprimée en terme des invariants de Gundlach. □

Comme on n'a pas d'invariants de Gundlach pour chaque D, on peut prendre $\tilde{\mathfrak{j}}_k=\phi^*\mathfrak{j}_k$, pour $k=1,2,3$, comme invariants sur la surface modulaire symétrique de Hilbert. Ces fonctions sont algébriquement dépendantes. De même, on considère les fonctions $\tilde{\mathfrak{b}}_k=\phi^*\mathfrak{b}_k$ et $\tilde{\mathfrak{r}}_k=\phi^*\mathfrak{r}_k$ pour $k=1,2,3$ (ces fonctions $\mathfrak{b}_k$ et $\mathfrak{r}_k$ sont définies à la section 3.4.2) . Soit

$$\tilde{\Gamma}(n)=\left\{\begin{pmatrix} a & b/\sqrt{\Delta_K}\\ \sqrt{\Delta_K}c & d\end{pmatrix}\in \mathrm{SL}_2(\mathcal{O}_K\oplus\partial_K^{-1}) : a\equiv d\equiv 1 \bmod n,\ b\equiv c\equiv 0 \bmod n\right\}.$$

Définissons alors pour respectivement $D\equiv 1 \bmod 4$ et $D\equiv 2,3 \bmod 4$

$$\begin{aligned}\tilde{\Gamma}(2,4)&=\left\{\begin{pmatrix} a & b/\sqrt{\Delta_K}\\ \sqrt{\Delta_K}c & d\end{pmatrix}\in\tilde{\Gamma}(2) : b\equiv c\equiv 0 \bmod 4\right\},\\ \tilde{\Gamma}(2,4)&=\left\{\begin{pmatrix} a & (b+b'\omega)/\sqrt{\Delta_K}\\ \sqrt{\Delta_K}(c+c'\omega) & d\end{pmatrix}\in\tilde{\Gamma}(2) : b'\equiv c'\equiv 0 \bmod 4\right\}.\end{aligned} \tag{5.7}$$

Théorème 5.2.8. *Les fonctions $\tilde{\mathfrak{r}}_k$ et $\tilde{\mathfrak{b}}_k$ pour $k=1,2,3$ sont respectivement des générateurs pour le corps des fonctions modulaires invariantes par $\tilde{\Gamma}(2)$ et $\tilde{\Gamma}(2,4)$, si $D\equiv 1 \bmod 4$, et par $\tilde{\Gamma}(2)\cup\tilde{\Gamma}(2)\sigma$ et $\tilde{\Gamma}(2,4)\cup\tilde{\Gamma}(2,4)\sigma$, si $D\equiv 2,3 \bmod 4$.*

Démonstration. D'après l'équation (5.4), on a que $\phi^{-1}(\Gamma_2(2,4)) = \tilde{\Gamma}(2,4)$. Ainsi, les fonctions $\tilde{\mathfrak{b}}_k$ sont modulaires pour $\tilde{\Gamma}(2,4)$. De plus, si $D \equiv 2,3 \bmod 4$, alors ces fonctions sont aussi modulaires pour $\tilde{\Gamma}(2,4)\sigma$, car la matrice M de l'équation (5.2) appartient à $\Gamma_2(2,4)$. Similairement, $\phi^{-1}(\Gamma_2(2)) = \tilde{\Gamma}(2)$ et les $\tilde{\mathfrak{r}}_k$ sont modulaires pour $\tilde{\Gamma}(2)$ et aussi par $\tilde{\Gamma}(2)\sigma$ lorsque $D \equiv 2,3 \bmod 4$. On conlut en appliquant le lemme 5.2.7 et le fait que $\mathfrak{b}_i$ (resp. $\mathfrak{r}_i$) sont des générateurs pour le corps des fonctions modulaires de Siegel invariantes par $\Gamma_2(2,4)$ (resp. $\Gamma_2(2)$). □

Proposition 5.2.9. *Les sous-groupes $\tilde{\Gamma}(2)$ et $\tilde{\Gamma}(2,4)$ de $\tilde{\Gamma}$ sont d'indices*

$$\begin{cases} 36 & et \quad 576, & si\ D \equiv 1 \bmod 8; \\ 60 & et \quad 960, & si\ D \equiv 5 \bmod 8; \\ 48 & et \quad 192, & si\ D \equiv 2,3 \bmod 4. \end{cases}$$

Démonstration. On ne fait la preuve que pour $\tilde{\Gamma}(2,4)$ car l'autre cas fonctionne pareil. Notons que $\tilde{\Gamma}/\tilde{\Gamma}(4) \simeq \mathrm{SL}_2(\mathcal{O}_K/4\mathcal{O}_K)$. On a alors que $\mathcal{O}_K/4\mathcal{O}_K$ est isomorphe à

— $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, lorsque 2 est décomposé ($D \equiv 1 \bmod 8$) ;
— $\mathbb{Z}/4\mathbb{Z}[X]/(X^2+X+1)$, lorsque 2 est inerte ($D \equiv 5 \bmod 8$) ;
— $\mathbb{Z}/4\mathbb{Z}[X]/(X^2)$, lorsque 2 est ramifié ($D \equiv 2,3 \bmod 4$).

Le cardinal de $\mathrm{SL}_2(\mathcal{O}_K/4\mathcal{O}_K)$ est alors 48^2, 3840 ou 3072. De plus, l'indice du sous-groupe $\tilde{\Gamma}(4)$ de $\tilde{\Gamma}(2,4)$ est 4 lorsque $D \equiv 1 \bmod 4$ et 16 lorsque $D \equiv 2,3 \bmod 4$. Comme ces deux ensembles sont des sous-groupes normaux de $\tilde{\Gamma}$, le troisième théorème d'isomorphisme des groupes nous donne le résultat désiré. □

Considérons maintenant Γ un sous-groupe de Γ_2 d'indice fini. La projection $\pi : \mathcal{H}_2/\Gamma \to \mathcal{H}_2/\Gamma_2$ est une application finie. Soit Δ le discriminant d'un certain corps de nombres quadratique. Une composante irréductible de $\pi^{-1}(H_\Delta)$ dans $\mathcal{H}_2/\Gamma$ est appelée une *composante de la surface de Humbert*. Nous nous intéressons aux cas où $\Gamma = \Gamma_2(2)$ et $\Gamma = \Gamma_2(2,4)$.

Proposition 5.2.10. *Le nombre de composantes de la surface de Humbert pour respectivement $\Gamma_2(2)$ et $\Gamma_2(2,4)$ est*

$$\begin{cases} 10 & si\ D \equiv 1 \bmod 8, \\ 6 & si\ D \equiv 5 \bmod 8, \\ 15 & si\ D \equiv 2,3 \bmod 4 \end{cases} \quad et \quad \begin{cases} 10 & si\ D \equiv 1 \bmod 8, \\ 6 & si\ D \equiv 5 \bmod 8, \\ 60 & si\ D \equiv 2,3 \bmod 4. \end{cases}$$

Démonstration. Voir [74]. Un argument heuristique pour $\Gamma_2(2,4)$ est que si l'on note $P(\mathfrak{b}_1,\mathfrak{b}_2,\mathfrak{b}_3)$ la composante de Humbert qui est l'image de ϕ et $\Omega = \phi(z) \in \mathcal{H}_2$, alors pour tout $\gamma \in \Gamma_2/\Gamma_2(2,4)$, on a que $P(\mathfrak{b}_i(\gamma\Omega)) = 0$ seulement pour les matrices γ qui proviennent de l'image de $\phi(\tilde{\Gamma}/\tilde{\Gamma}(2,4))$ et de $\phi(\tilde{\Gamma}/\tilde{\Gamma}(2,4)\sigma)$ dans $\Gamma_2/\Gamma_2(2,4)$. Le nombre de composantes correspond au nombre

$$v(D) \cdot |\Gamma_2/\Gamma_2(2,4)|/|\tilde{\Gamma}/\tilde{\Gamma}(2,4)|,$$

où $v(D)$ est 1 si $D \equiv 2,3 \bmod 4$ et $\frac{1}{2}$ si $D \equiv 1 \bmod 4$. Cet argument fonctionne aussi pour $\Gamma_2(2)$. □

Nous donnons les équations des composantes des surfaces de Humbert qui correspondent à l'image de ϕ pour $\Gamma_2(2,4)$ et $D = 2,\ 3,\ 5$

$$\begin{gathered} \mathfrak{b}_1 - \tfrac{1}{2}(\mathfrak{b}_2^2 + \mathfrak{b}_3^2) = 0, \\ -\mathfrak{b}_1^4 - \mathfrak{b}_2^4 - 4\mathfrak{b}_3^2 - 2\mathfrak{b}_1^2\mathfrak{b}_2^2 + 4\mathfrak{b}_1\mathfrak{b}_2 + 4\mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3^2 = 0, \\ \tfrac{-1}{2}(\textstyle\sum_i \mathfrak{b}_i^4 + \sum_i \sum_{j\neq i} (\mathfrak{b}_i\mathfrak{b}_j)^4) + \mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3(1 + \textstyle\sum_i \mathfrak{b}_i^4 - \mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3) = 0 \end{gathered} \tag{5.8}$$

et similairement pour $\Gamma_2(2)$ et $D = 2$ seulement :

$$\begin{aligned}&((16\mathfrak{r}_3^2 - 16\mathfrak{r}_3)\mathfrak{r}_2^2 + (-16\mathfrak{r}_3^2 + 16\mathfrak{r}_3)\mathfrak{r}_2)\mathfrak{r}_1^4 + ((-16\mathfrak{r}_3^2 + 16\mathfrak{r}_3)\mathfrak{r}_2^3 + (-16\mathfrak{r}_3^3 + \\ &16\mathfrak{r}_3^2)\mathfrak{r}_2^2 + (16\mathfrak{r}_3^3 - 16\mathfrak{r}_3)\mathfrak{r}_2)\mathfrak{r}_1^3 + (-\mathfrak{r}_2^4 + (16\mathfrak{r}_3^3 - 16\mathfrak{r}_3 + 2)\mathfrak{r}_2^3 + (-14\mathfrak{r}_3^2 + \\ &14\mathfrak{r}_3 - 1)\mathfrak{r}_2^2 + (-16\mathfrak{r}_3^3 + 14\mathfrak{r}_3^2 + 2\mathfrak{r}_3)\mathfrak{r}_2 + (-\mathfrak{r}_3^4 + 2\mathfrak{r}_3^3 - \mathfrak{r}_3^2))\mathfrak{r}_1^2 + (2\mathfrak{r}_3\mathfrak{r}_2^4 + \\ &(-16\mathfrak{r}_3^3 + 14\mathfrak{r}_3^2 - 2\mathfrak{r}_3)\mathfrak{r}_2^3 + (14\mathfrak{r}_3^3 - 12\mathfrak{r}_3^2)\mathfrak{r}_2^2 + (2\mathfrak{r}_3^4 - 2\mathfrak{r}_3^3)\mathfrak{r}_2)\mathfrak{r}_1 + (-\mathfrak{r}_3^2\mathfrak{r}_2^4 + \\ &2\mathfrak{r}_3^3\mathfrak{r}_2^3 - \mathfrak{r}_3^4\mathfrak{r}_2^2) = 0.\end{aligned} \tag{5.9}$$

Pour $D = 3$, les équations sont trop grosses pour être reproduites ici. Le calcul des ces équations est le sujet de [35], où les équations associées à de nombreux discriminants peuvent être trouvées. Nous avons retrouvés les équations pour les petits discriminants $D = 2, 3, 5$ en évaluant les différents invariants en de nombreuses matrices des périodes et en procédant à une phase d'algèbre linéaire.

5.3 Polynômes Modulaires et multiplication réelle

5.3.1 Polynômes classiques

Notons dans cette section $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K)$ et considérons les cas où $D = 2$ ou 5. Le groupe $\tilde{\Gamma}$ est engendré par les trois matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $R = \left(\begin{smallmatrix} 1 & \omega \\ 0 & 1 \end{smallmatrix}\right)$. Notons que $T\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)T = -S$ de telle sorte que nous allons parfois considérer la matrice $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ au lieu de S.

Soit ℓ un nombre premier qui se décompose en facteur totalement positifs : $\ell = \beta\overline{\beta}$. Soit $z \in \mathcal{H}_1^2/\tilde{\Gamma}$. Les variétés β-isogènes sont $\frac{1}{\beta}\gamma \cdot z$ tandis que les $\overline{\beta}$-isogènes sont $\frac{1}{\overline{\beta}}\gamma \cdot z$, pour $\gamma \in \tilde{\Gamma}$. On veut définir des polynômes qui paramétrisent des classes d'isomorphismes de surfaces abéliennes ayant multiplication réelle par $\mathcal{O}_K$ munis d'une β-isogénie. Nous commençons avec quelques notations. Rappelons que $\mathfrak{J}_1$ et $\mathfrak{J}_2$ sont les invariants de Gundlach (voir théorèmes 5.1.6 et 5.1.8), que l'on connaît pour $K = \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{5})$.

Définissons pour $i = 1, 2$ et $\gamma \in \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$

$$\mathfrak{J}_{i,\beta} : \begin{array}{ccc} \mathcal{H}_1^2 & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \mathfrak{J}_i(\frac{1}{\beta}z) \end{array} \quad \text{et} \quad \mathfrak{J}_{i,\beta}^{\gamma} : \begin{array}{ccc} \mathcal{H}_1^2 & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \mathfrak{J}_i(\frac{1}{\beta}\gamma \cdot z). \end{array}$$

Soit $\tilde{\Gamma}^0(\beta) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \tilde{\Gamma} : \beta | b\}$.

Lemme 5.3.1. *Le sous-groupe $\tilde{\Gamma}^0(\beta)$ de $\tilde{\Gamma}$ est d'indice $\ell + 1$. L'ensemble des matrices*

$$C_\beta = \left\{S, T^i, i \in \{0, \ldots, \ell - 1\}\right\}$$

est un ensemble de représentants des classes de $\tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$.

Démonstration. Les $\ell + 1$ matrices de C_β sont clairement dans des classes différentes du quotient $\tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$. Remarquons que ${}^tT = ST^{-1}S^{-1} \in \tilde{\Gamma}^0(\beta)$ et ${}^tR = SR^{-1}S^{-1} \in \tilde{\Gamma}^0(\beta)$ de telle sorte que $\tilde{\Gamma}$ est engendré par S, ${}^tT$ et ${}^tR$. Pour tout $i \in \{0, \ldots, \ell - 1\}$, ${}^tTT^i$ et ${}^tRT^i$ sont dans la classe de T^i tandis que ${}^tTS$ et ${}^tRS$ sont dans la classe de S. De plus, ST^i est dans la classe de S et $SS = I_2$, ce qui montre qu'il ne peut pas y avoir une classe de plus que les $\ell + 1$ classes que l'on connaît déjà. □

Pour une matrice $\gamma \in \tilde{\Gamma}^0(\beta)$, nous notons $\gamma_\beta = \left(\begin{smallmatrix} a & b/\beta \\ c\beta & d \end{smallmatrix}\right) \in \tilde{\Gamma}$. On a que

$$\mathfrak{J}_{i,\beta}^{\gamma}(z) := \mathfrak{J}_i\left(\frac{1}{\beta}\gamma \cdot z\right) = \mathfrak{J}_i\left(\gamma_\beta \cdot \left(\frac{1}{\beta}z\right)\right) = \mathfrak{J}_i\left(\frac{1}{\beta}z\right) =: \mathfrak{J}_{i,\beta}(z),$$

où la seconde égalité provient du fait que $\frac{1}{\beta}\gamma \cdot z = \gamma_\beta \cdot (\frac{1}{\beta}z)$ et la troisième de la modularité de $\mathfrak{J}_i$. Ainsi les fonctions $\mathfrak{J}_{i,\beta}$ pour $i = 1, 2$ sont modulaires pour le groupe $\tilde{\Gamma}^0(\beta)$. Cependant, ces fonctions ne sont en général pas symétriques car $\mathfrak{J}_{i,\beta}^{\gamma}(\sigma(z)) = \mathfrak{J}_{i,\overline{\beta}}^{\overline{\gamma}}(z)$.

Rappelons que nous notons par ϵ l'unité fondamentale de $\mathcal{O}_K$. Soit $\epsilon' \in \mathcal{O}_K^{\times,+}$ une unité totalement positive de $\mathcal{O}_K$. S'il existe $n \in \mathbb{Z}$ tel que $\epsilon' = \epsilon^{2n}$, alors la matrice $\gamma = \left(\begin{smallmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{smallmatrix}\right)$ est dans $\tilde{\Gamma}$ et $\gamma \cdot z = \epsilon' z$. Ainsi, dans ce cas, $\mathfrak{J}_i(\epsilon' z) = \mathfrak{J}_i(z)$, et, en particulier, une β-isogénie est aussi une $\epsilon'\beta$-isogénie.

Remarque 5.3.2. — *Nous ne considérons que des unités totalement positives ϵ' pour garantir le fait que $\epsilon' z \in \mathcal{H}_1^2$;*
— *Lorsque $D = 2$ ou 5, l'unité fondamentale ϵ a norme -1 tandis que $\epsilon' \in \mathcal{O}_K^{\times,+}$ a norme 1, de telle sorte que ce dernier peut toujours être écrit comme une puissance paire de ϵ. Ainsi, le choix de la décomposition de ℓ n'importe pas.*

Proposition 5.3.3. *Soit $D = 2$ ou 5 et ℓ un nombre premier. Écrivons $\ell = \beta\overline{\beta}$ avec $\beta \in \mathcal{O}_K^+$. Si ℓ est ramifié, alors les polynômes*

$$\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \prod_{\gamma \in C_\beta} (X - \mathfrak{J}_{1,\beta}^{\gamma}) \qquad et \qquad \Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{\gamma \in C_\beta} \mathfrak{J}_{2,\beta}^{\gamma} \frac{\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{X - \mathfrak{J}_{1,\beta}^{\gamma}}$$

sont dans $\mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)[X]$. Si ℓ se décompose, alors les polynômes

$$\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \prod_{\gamma \in C_\beta} (X - \mathfrak{J}_{1,\beta}^{\gamma})(X - \mathfrak{J}_{1,\overline{\beta}}^{\gamma}) \qquad et$$

$$\Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{\gamma \in C_\beta} \mathfrak{J}_{2,\beta}^{\gamma} \frac{\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{X - \mathfrak{J}_{1,\beta}^{\gamma}} + \sum_{\gamma \in C_\beta} \mathfrak{J}_{2,\overline{\beta}}^{\gamma} \frac{\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{X - \mathfrak{J}_{1,\overline{\beta}}^{\gamma}}$$

sont dans $\mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)[X]$. Ces polynômes dépendent seulement de ℓ.

Démonstration. Nous ne donnons la preuve que pour Φ_ℓ car elle est similaire pour Ψ_ℓ, et seulement dans le cas décomposé car les mêmes arguments s'appliquent dans le cas ramifié. La preuve se fait en deux étapes.

1. Définissons les fonctions $c_i : \mathcal{H}_1^2 \to \mathbb{C}$, pour $i = 0, \ldots, 2(\ell+1) - 1$, par

$$\prod_{\gamma \in C_\beta} (X - \mathfrak{J}_{1,\beta}^{\gamma})(X - \mathfrak{J}_{1,\overline{\beta}}^{\gamma}) = X^{2(\ell+1)} + \sum_{i=0}^{2(\ell+1)-1} c_i X^i.$$

Les fonctions c_i sont modulaires pour $\tilde{\Gamma}$ parce qu'elles sont symétriques en les $\mathfrak{J}_{1,\beta}^{\gamma}$ et en les $\mathfrak{J}_{1,\overline{\beta}}^{\gamma}$, qui sont modulaires pour $\tilde{\Gamma}^0(\beta)$ et $\tilde{\Gamma}^0(\overline{\beta})$ respectivement, et parce que l'ensemble C_β est un ensemble de représentants des classes de $\tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$ et de $\tilde{\Gamma}/\tilde{\Gamma}^0(\overline{\beta})$.

De plus, les fonctions c_i sont symétriques dans le sens où $c_i(z) = c_i(\sigma(z))$ pour $z \in \mathcal{H}_1^2$ (en d'autres termes, c_i est modulaire pour $\tilde{\Gamma} \cup \tilde{\Gamma}\sigma$). Ceci

provient de la symétrie de $\mathfrak{J}_1$ et puis du fait que, pour $\gamma \in C_\beta$, $\mathfrak{J}_{1,\beta}^{\gamma}(\sigma(z)) = \mathfrak{J}_{1,\overline{\beta}}^{\gamma}(z)$. On en déduit que les fonctions c_i sont des fonctions modulaires symétriques de Hilbert et par les théorèmes 5.1.6 et 5.1.8, elles peuvent être écrite comme des fonctions rationnelles en $\mathfrak{J}_1$ et $\mathfrak{J}_2$ avec des coefficients complexes.

2. Comme $\mathfrak{J}_1$ et $\mathfrak{J}_2$ ont des coefficients de Fourier rationnels par les théorèmes 5.1.5 et 5.1.7, les mêmes arguments de la preuve de la proposition 4.2.7 montrent que $c_i \in \mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)$.

□

Définition 5.3.4. *Soit $\ell = \beta\overline{\beta}$ un nombre premier qui se décompose ou se ramifie en éléments totalement positifs dans $\mathcal{O}_K$. Les polynômes $\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$ et $\Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$ de la proposition 5.3.3 sont appelés les* β-polynômes modulaires *pour K. Ils ne dépendent que de ℓ.*

Remarque 5.3.5. *Ces polynômes dépendent seulement de ℓ car on se focalise sur $\mathbb{Q}(\sqrt{D})$ pour $D = 2$ et 5, où l'unité fondamentale a norme -1.*

Par construction, pour chaque $z \in \mathcal{H}_1^2$, les polynômes modulaires satisfont $\Phi_\ell(X, \mathfrak{J}_1(z), \mathfrak{J}_2(z)) = 0$ lorsque X est l'évaluation de $\mathfrak{J}_1$ en un point z' qui est β-isogène, ou $\overline{\beta}$-isogène dans le cas décomposé, à z. Alors $\mathfrak{J}_2(z') = \Psi_\ell(\mathfrak{J}_1(z'), \mathfrak{J}_1(z), \mathfrak{J}_2(z))/\Phi'_\ell(\mathfrak{J}_1(z'), \mathfrak{J}_1(z), \mathfrak{J}_2(z))$, où Φ'_ℓ est la dérivée de Φ_ℓ par rapport à la variable X. Ainsi, pour $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ donnés, les β-polynômes modulaires permettent de calculer tous les invariants de Gundlach des variétés isogènes à z.

Soit $\tilde{\Gamma}'$ un sous-groupe de $\tilde{\Gamma}$. Notons par $\mathbb{C}_{\tilde{\Gamma}'}$ le corps des fonctions méromorphes de $\mathcal{H}_1^2$ invariantes sous l'action de $\tilde{\Gamma}'$ (c'est le corps de fonctions de $\mathcal{H}_1^2/\tilde{\Gamma}'$).

Lemme 5.3.6. *L'extension de corps $\mathbb{C}_{\tilde{\Gamma}^0(\beta)}/\mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}$ est algébrique et son degré est $2[\tilde{\Gamma} : \tilde{\Gamma}^0(\beta)] = 2(\ell + 1)$.*

Démonstration. Soit $G = (\tilde{\Gamma} \cup \tilde{\Gamma}\sigma)/\tilde{\Gamma}(\ell)$ et $L = \mathbb{C}_{\tilde{\Gamma}(\ell)}$. Comme G est un groupe fini d'automorphismes de K, alors par un théorème d'Artin, l'extension L/L^G est Galoisienne de degré $|G|$. De plus, on peut facilement prouver que $L^G = \mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}$. Soit $H = \tilde{\Gamma}^0(\beta)/\tilde{\Gamma}(\ell)$ un sous-groupe d'indice fini de G. On a que $L^H = \mathbb{C}_{\tilde{\Gamma}^0(\beta)}$ donc par le théorème fondamental de la théorie de Galois, l'extension $\mathbb{C}_{\tilde{\Gamma}(\ell)}/\mathbb{C}_{\tilde{\Gamma}^0(\beta)}$ est Galoisienne de groupe de Galois H. À partir de ces deux extensions, on en déduit le lemme. Notons que le sous-groupe $\tilde{\Gamma}^0(\beta)$ n'est pas normal donc l'extension $\mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}/\mathbb{C}_{\tilde{\Gamma}^0(\beta)}$ n'est pas Galoisienne. L'indice $[\tilde{\Gamma} : \tilde{\Gamma}^0(\beta)]$ est donnée par le lemme 5.3.1. □

Lemme 5.3.7. *Soit N un entier. Alors l'application $\mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K/N\mathcal{O}_K)$ est surjective.*

Démonstration. C'est une application de la théorie d'approximation forte. □

Théorème 5.3.8. *Le corps des fonctions modulaires de Hilbert invariantes par $\tilde{\Gamma}^0(\beta)$ est $\mathbb{C}_{\tilde{\Gamma}^0(\beta)} = \mathbb{C}(\mathfrak{J}_{\mathrm{i},\beta}, \mathfrak{J}_1, \mathfrak{J}_2)$ pour $i = 1, 2$. Ainsi, $\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$ est le polynôme minimal de $\mathfrak{J}_{\imath,\beta}$ sur $\mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma} = \mathbb{C}(\mathfrak{J}_1, \mathfrak{J}_2)$.*

Démonstration. Nous avons vu dans la preuve du lemme 5.3.6 que l'extension $\mathbb{C}_{\tilde{\Gamma}(\ell)}/\mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}$ est Galoisienne de groupe de Galois $(\tilde{\Gamma}\cup\tilde{\Gamma}\sigma)/\tilde{\Gamma}(\ell)$. Soient $K_1 = \mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}(\mathfrak{J}_{\mathbb{1},\beta}) = \mathbb{C}(\mathfrak{J}_{\mathbb{1},\beta},\mathfrak{J}_1,\mathfrak{J}_2)$ et $K_2 = \mathbb{C}_{\tilde{\Gamma}(\ell)}^{\tilde{\Gamma}^0(\beta)/\tilde{\Gamma}(\ell)} = \mathbb{C}_{\tilde{\Gamma}^0(\beta)}$. Alors $K_1 \subseteq K_2$ et on veut prouver l'égalité. Par la théorie de Galois, les sous-corps entre K_1 et K_2 correspondent aux sous-groupes de $\tilde{\Gamma}\cup\tilde{\Gamma}\sigma$ contenant $\tilde{\Gamma}^0(\beta)$. Si on montre que le groupe $\tilde{\Gamma}^0(\beta)$ est maximal dans $\tilde{\Gamma}$, alors on en déduit que $K_1 = \mathbb{C}_{\tilde{\Gamma}\cup\tilde{\Gamma}\sigma}$, $K_1 = \mathbb{C}_{\tilde{\Gamma}}$ ou $K_1 = K_2$. Or seulement la dernière possibilité peut être vraie.

Soit $\pi : \tilde{\Gamma} \twoheadrightarrow \mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)$. Si ℓ se décompose, alors $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$ et $\pi(\tilde{\Gamma}^0(\beta)) = \{\left(\begin{smallmatrix}*&0\\*&*\end{smallmatrix}\right) \times \left(\begin{smallmatrix}*&*\\*&*\end{smallmatrix}\right)\}$. Par [49, Théorème 4.1], l'ensemble des matrices triangulaires de $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ est maximal et $\pi(\tilde{\Gamma}^0(\beta))$ est alors maximal dans $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$. Comme π est surjectif, on en déduit que $\tilde{\Gamma}^0(\beta)$ est maximal dans $\tilde{\Gamma}$. Si ℓ est ramifié, alors $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2((\mathbb{Z}/\ell\mathbb{Z})[X]/(X^2))$ et $\pi(\tilde{\Gamma}^0(\beta))$ est l'ensemble des matrices de la forme $\left(\begin{smallmatrix}*&xX\\*&*\end{smallmatrix}\right)$ pour chaque $x \in \mathbb{Z}/\ell\mathbb{Z}$. Soit G un groupe qui contient strictement $\pi(\tilde{\Gamma}^0(\beta))$. Alors il existe une matrice $\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right) \in G$, avec $B(0) \neq 0$. Si A est inversible (c'est-à-dire $A(0) \neq 0$) alors $\left(\begin{smallmatrix}1&0\\-AC&1\end{smallmatrix}\right)\left(\begin{smallmatrix}A^{-1}&0\\0&A\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&A^{-1}B\\0&1\end{smallmatrix}\right) \in G$ et $(A^{-1}B)(0) \neq 0$ de telle sorte que $A^{-1}B = x_0 + x_1X$ avec $x_0 \neq 0$. Finalement on a que $\left(\begin{smallmatrix}1&x_0+x_1X\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-x_1X\\0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&x_0\\0&1\end{smallmatrix}\right)$ à partir de quoi on déduit que $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \in G$. Comme cette dernière matrice ainsi que les matrices $\left(\begin{smallmatrix}1&0\\-1&1\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}1&X\\0&1\end{smallmatrix}\right)$ sont toutes dans G et sont des générateurs de $\mathrm{SL}_2(\mathcal{O}_K)$, on déduit que G est $\pi(\tilde{\Gamma})$, que $\pi(\tilde{\Gamma}^0(\beta))$ est maximal et ainsi par surjectivité que $\tilde{\Gamma}^0(\beta)$ est aussi maximal. Si A n'est pas inversible mais que D l'est, la preuve procède de manière similaire. Sinon, si A et D ne sont pas inversibles, alors B et C le sont. De plus, $\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}A+B&B\\C+D&D\end{smallmatrix}\right)$ et $(A+B)(0) \neq 0$, ce qui termine la preuve. □

Soit $\mathcal{L}_\ell$ le lieu des surfaces abéliennes principalement polarisées ayant multiplication réelle par $\mathcal{O}_K$ qui sont β-isogènes, ou $\overline{\beta}$-isogènes dans le cas décomposé, à un produit de courbes elliptiques.

Théorème 5.3.9. *Dans le cas où $D = 5$, les dénominateurs des polynômes modulaires Φ_ℓ et Ψ_ℓ sont divisibles par un polynôme L_ℓ dans $\mathbb{Q}[\mathfrak{J}_1,\mathfrak{J}_2]$ décrivant $\mathcal{L}_\ell$.*

Démonstration. On adapte la preuve du lemme 4.2.8 et on ne la fait que dans le cas décomposé. Soit $z \in \mathcal{H}_1^2$ qui est β- ou $\overline{\beta}$-isogène à un produit de courbes elliptiques et soit c_i un coefficient de Φ_ℓ. La forme parabolique χ_{10} (définie dans l'équation (3.7)) s'annule aux produits de courbes elliptiques et par le théorème 5.1.11, on a que $H_{10} = -4\phi_\epsilon^*\chi_{10}$ de telle sorte que H_{10} s'annule aussi aux produits de courbes elliptiques. Ainsi $\mathfrak{J}_1$ et $\mathfrak{J}_2$ ont des pôles en ces valeurs et il existe une certaine matrice $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$ telle que $\mathfrak{J}_{\mathbb{1},\beta}^\gamma(z)$ ou $\mathfrak{J}_{\mathbb{1},\overline{\beta}}^\gamma(z)$ soit infini. L'évaluation de c_i en z est une expression symétrique en les $\mathfrak{J}_{\mathbb{1},\beta}^\gamma(z)$ et en les $\mathfrak{J}_{\mathbb{1},\overline{\beta}}^\gamma(z)$. Génériquement, il n'existe pas de relations algébriques entre ces valeurs et l'évaluation de c_i en z est par suite également infinie. Puisque $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ sont finis, le numérateur de c_i est fini. Le dénominateur de c_i doit s'annuler en z ce qui signifie que c_i est divisible par L_ℓ. La preuve pour Ψ_ℓ est similaire. □

Si $D = 2$, les invariants de Gundlach $\mathfrak{J}_1$ et $\mathfrak{J}_2$ ont des pôles lorsque $H_4(z) = 0$. Puisque par le théorème 5.1.13, on a que $\phi_\epsilon^*\chi_{10} = \frac{-1}{4}H_4H_6$, l'ensemble des pôles est un sous-ensemble de produits de courbes elliptiques. On doit donc considérer le sous-ensemble $\mathcal{L}'_\ell$ de $\mathcal{L}_\ell$ des surfaces z telles que $H_4(\frac{1}{\beta}\gamma\cdot z) = 0$, ou $H_4(\frac{1}{\overline{\beta}}\gamma\cdot z) = 0$ dans le cas décomposé, pour un certain $\gamma \in C_\beta$.

Théorème 5.3.10. *Dans le cas où $D = 2$, les dénominateurs des polynômes modulaires Φ_ℓ et Ψ_ℓ sont divisibles par un polynôme L'_ℓ dans $\mathbb{Q}[\mathfrak{J}_1, \mathfrak{J}_2]$ décrivant $\mathcal{L}'_\ell$.*

5.3.2 Polynômes modulaires avec les fonctions thêta

Dans cette section, nous allons introduire des polynômes modulaires pour tout entier D sans facteur carré en utilisant les thêta constantes. Les invariants que nous utiliserons sont les tirés en arrière des générateurs pour le groupe $\Gamma_2(2,4)$ définis dans la section 3.13 : $\tilde{\mathfrak{b}}_i = \phi^* \mathfrak{b}_i$ pour $i = 1, 2, 3$, qui sont des fonctions modulaires pour le groupe $\tilde{\Gamma}(2,4)$ qui est défini dans l'équation (5.7). Rappelons que nous avons le théorème 5.2.8. Nous notons dans cette section $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ et nous ne considérons que des nombres premiers $\ell = \beta\overline{\beta}$ différents de 2.

Pour $i = 1, 2, 3$, $\beta \in \mathcal{O}_K^+$ et $\gamma \in \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$, on pose :

$$\tilde{\mathfrak{b}}_{\mathfrak{i},\beta} : \begin{array}{ccc} \mathcal{H}_1^2 & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \tilde{\mathfrak{b}}_i(\frac{1}{\beta} z) \end{array} \quad \text{et} \quad \tilde{\mathfrak{b}}^\gamma_{\mathfrak{i},\beta} : \begin{array}{ccc} \mathcal{H}_1^2 & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \tilde{\mathfrak{b}}_i(\frac{1}{\beta}\gamma \cdot z). \end{array}$$

Lemme 5.3.11. *Le sous-groupe $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$ de $\tilde{\Gamma}(2,4)$ est d'indice $\ell + 1$.*

Démonstration. Soit $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$. Il suffit de prouver qu'il existe un élément $\gamma' \in \tilde{\Gamma}^0(\beta)$ tel que $\gamma'\gamma \in \tilde{\Gamma}(2,4)$.

Regardons γ' tel que $\gamma'\gamma \equiv 0 \bmod 4$, c'est-à-dire tel que $\gamma' \equiv \gamma^{-1} \bmod 4$, et tel que $\gamma' \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \bmod \ell$. Par le théorème des restes Chinois, ces conditions modulo 4 et ℓ donnent une matrice γ'' qui doit satisfaire des conditions modulo 4ℓ et par le lemme 5.3.7, γ'' peut être relevé en une matrice dans $\tilde{\Gamma}$. □

Pour une matrice $\gamma \in \tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$, on aimerait pouvoir écrire

$$\tilde{\mathfrak{b}}^\gamma_{\mathfrak{i},\beta}(z) = \tilde{\mathfrak{b}}_i\left(\frac{1}{\beta}\gamma \cdot z\right) = \tilde{\mathfrak{b}}_i\left(\gamma_\beta \cdot \left(\frac{1}{\beta} z\right)\right) = \tilde{\mathfrak{b}}_i\left(\frac{1}{\beta} z\right) = \tilde{\mathfrak{b}}_{\mathfrak{i},\beta}(z)$$

pour pouvoir conclure que les fonctions $\tilde{\mathfrak{b}}_{\mathfrak{i},\beta}$ pour $i = 1, 2, 3$ sont modulaires pour le groupe $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$. Cependant, la troisième égalité n'est vraie que si la matrice γ_β est dans $\tilde{\Gamma}(2,4)$. Un simple calcul montre que c'est toujours le cas lorsque $D \equiv 1 \bmod 4$. Lorsque $D \equiv 2, 3 \bmod 4$, ceci n'arrive que si β est de la forme $a + b\omega$ avec b pair. Si $D \equiv 2 \bmod 4$, c'est équivalent à demander que $\ell \equiv 1 \bmod 4$ et sinon si $D \equiv 3 \bmod 4$, ℓ doit nécessairement vérifier $\ell \equiv 1 \bmod 4$. En particulier, dans ce dernier cas, 0, 1 ou 2 polynômes modulaires avec une structure sur $\tilde{\Gamma}(2,4)$ peuvent exister pour un nombre premier qui se décompose en facteurs totalement positifs donné, en fonction de l'unité fondamentale ϵ. Ainsi :

Proposition 5.3.12. *Les fonctions $\tilde{\mathfrak{b}}_{\mathfrak{i},\beta}$ pour $i = 1, 2, 3$ sont des fonctions modulaires pour $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$ lorsque*

- *$D \equiv 1 \bmod 4$;*
- *$D \equiv 2 \bmod 4$ et $\beta = a + b\omega$ avec b pair, ou, de manière équivalente, $\ell \equiv 1 \bmod 4$;*
- *$D \equiv 3 \bmod 4$ et $\beta = a + b\omega$ avec b pair ; ceci implique que $\ell \equiv 1 \bmod 4$.*

Proposition 5.3.13. *Soit ℓ un nombre premier. Écrivons $\ell = \beta\overline{\beta}$ avec $\beta \in \mathcal{O}_K^+$ et C_β un ensemble de représentants des classes de $\tilde{\Gamma}(2,4)/(\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))$. Si*

$D \equiv 1 \bmod 4$, alors les polynômes

$$\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \prod_{\gamma \in C_\beta} (X - \tilde{\mathfrak{b}}_{1,\beta}^\gamma) \quad et \quad \Psi_{k,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \sum_{\gamma \in C_\beta} \tilde{\mathfrak{b}}_{k,\beta}^\gamma \frac{\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)}{X - \tilde{\mathfrak{b}}_{1,\beta}^\gamma}$$

pour $k = 1, 2$ sont dans $\mathbb{Q}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)[X]$. Si $D \equiv 2, 3 \bmod 4$ et $\beta = a + b\omega$ avec b pair, alors

$$\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \prod_{\gamma \in C_\beta} (X - \tilde{\mathfrak{b}}_{1,\beta}^\gamma)(X - \tilde{\mathfrak{b}}_{1,\beta}^{\gamma\sigma}), \qquad et$$

$$\Psi_{k,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \sum_{\gamma \in C_\beta} \tilde{\mathfrak{b}}_{k,\beta}^\gamma \frac{\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)}{X - \tilde{\mathfrak{b}}_{1,\beta}^\gamma} + \sum_{\gamma \in C_\beta} \tilde{\mathfrak{b}}_{k,\beta}^{\gamma\sigma} \frac{\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)}{X - \tilde{\mathfrak{b}}_{1,\beta}^{\gamma\sigma}}$$

pour $k = 1, 2$ sont dans $\mathbb{Q}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)[X]$.

Démonstration. La preuve est comme celle de la proposition 5.3.3. La différence entre les cas $D \equiv 1 \bmod 4$ et $D \equiv 2, 3 \bmod 4$ réside dans les équations (5.2) et (5.3) : dans le premier cas, par la proposition 5.2.6, l'application $\mathcal{H}_1^2/\tilde{\Gamma}(2,4) \to \mathcal{H}_2/\Gamma_2$ est injective tandis que dans le second, c'est l'application $\mathcal{H}_1^2/(\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma) \to \mathcal{H}_2/\Gamma_2$ qui l'est. Les coefficients des séries de Fourier des $\tilde{\mathfrak{b}}_i$ sont dans $\mathbb{Q}$ parce que c'est le cas des séries de Fourier des thêta constantes de Hilbert (voir [54]). □

Définition 5.3.14. *Les polynômes $\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ et $\Psi_{k,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ pour $k = 2, 3$ définis dans la proposition 5.3.13 sont appelés les* β-polynômes modulaires *pour K.*

Notons qu'il existe trois polynômes pour que à $\tilde{\mathfrak{b}}_1$, $\tilde{\mathfrak{b}}_2$ et $\tilde{\mathfrak{b}}_3$ donnés, on puisse obtenir les valeurs $\tilde{\mathfrak{b}}_{1,\beta}^\gamma$, $\tilde{\mathfrak{b}}_{2,\beta}^\gamma$ et $\tilde{\mathfrak{b}}_{3,\beta}^\gamma$ pour tout $\gamma \in C_\beta$, alors que nous n'avions que deux polynômes avec les invariants de Gundlach. Néanmoins :

Remarque 5.3.15. *Lorsque $D = 2$, l'équation (5.8) dit que l'on doit considérer seulement $\tilde{\mathfrak{b}}_2$ et $\tilde{\mathfrak{b}}_3$ car $\tilde{\mathfrak{b}}_1$ est déterminé par $\tilde{\mathfrak{b}}_2$ et $\tilde{\mathfrak{b}}_3$.*

Contrairement aux polynômes modulaires avec les invariants de Gundlach, les polynômes définis avec les $\tilde{\mathfrak{b}}_i$ dépendent du choix de β. Notons tout de même que lorsque deux paires $(\beta, \overline{\beta})$ et $(\beta', \overline{\beta'})$ d'éléments totalement positifs dont le produit vaut ℓ et qui diffèrent d'un facteur pair de ϵ, où ϵ est une unité fondamentale qui peut être de norme -1 ou 1, alors $\beta' = \epsilon^{2n}\beta = \left(\begin{smallmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{smallmatrix}\right)\beta$. Ainsi pour tout $z \in \mathcal{H}_1^2$, si on calcule $\tilde{\mathfrak{b}}_{i,\beta}(z)$, pour $i = 1, 2, 3$, à partir des $\tilde{\mathfrak{b}}_i(z)$ et des β-polynômes modulaires, alors on a que $\tilde{\mathfrak{b}}_{i,\beta'}(z) = \tilde{\mathfrak{b}}_i\left(\left(\begin{smallmatrix} \epsilon^{-n} & 0 \\ 0 & \epsilon^n \end{smallmatrix}\right)\frac{1}{\beta}z\right)$ et en sachant comment la matrice $\left(\begin{smallmatrix} \epsilon^{-n} & 0 \\ 0 & \epsilon^n \end{smallmatrix}\right)$ agit sur les $\tilde{\mathfrak{b}}_{i,\beta}$, on peut calculer les $\tilde{\mathfrak{b}}_{i,\beta'}$ à partir des $\tilde{\mathfrak{b}}_{i,\beta}$. Dans ce cas-là, il est inutile de calculer les β'-polynômes modulaires.

Exemple 5.3.16. *Lorsque $D = 2$, 5 ou 13, l'unité fondamentale a norme -1.*

- *Si $D = 2$, on a que $(\tilde{\mathfrak{b}}_{1,\epsilon^2}, \tilde{\mathfrak{b}}_{2,\epsilon^2}, \tilde{\mathfrak{b}}_{3,\epsilon^2}) = (\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2)$;*
- *Si $D = 5$, on a que $(\tilde{\mathfrak{b}}_{1,\epsilon^2}, \tilde{\mathfrak{b}}_{2,\epsilon^2}, \tilde{\mathfrak{b}}_{3,\epsilon^2}) = (\tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)$;*
- *Si $D = 13$, on a que $(\tilde{\mathfrak{b}}_{1,\epsilon^2}, \tilde{\mathfrak{b}}_{2,\epsilon^2}, \tilde{\mathfrak{b}}_{3,\epsilon^2}) = (\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_1)$.*

Lorsque la norme de ϵ est 1, alors si $\ell = \beta\overline{\beta}$, on a aussi que $\ell = \beta'\overline{\beta'}$, où $\beta' = \epsilon\beta$. La multiplication par ϵ ne provient pas de l'action d'une matrice et l'argument précédent ne tient pas.

Exemple 5.3.17. *Lorsque $D = 55$, l'unité fondamentale $\epsilon = 89+12\sqrt{55}$ a norme 1 et pour $\ell = 5$, on peut choisir $\beta = 15 + 2\sqrt{55}$ et $\beta' = \epsilon\beta = 2655 + 358\sqrt{55}$. Comme 2 et 358 sont pairs, on peut définir deux triplets de polynômes modulaires "non équivalents" (par les propositions 5.3.12 et 5.3.13) .*

Théorème 5.3.18. *Si $\tilde{\mathfrak{b}}_{i,\beta}$ est une fonction modulaire pour $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$, alors le corps des fonctions modulaires de Hilbert invariantes par $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$ est $\mathbb{C}_{\tilde{\Gamma}^0(\beta)} = \mathbb{C}(\tilde{\mathfrak{b}}_{i,\beta}, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ pour $i = 1, 2, 3$. Ainsi, $\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ est le polynôme minimal de $\tilde{\mathfrak{b}}_{1,\beta}$ sur $\mathbb{C}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$.*

Démonstration. La preuve est similaire à celle du théorème 5.3.8. □

Comme Φ_β est un polynôme minimal, c'est l'unique polynôme unitaire et irréductible qui vérifie, pour tout $z \in \mathcal{H}_1^2$, $\Phi_\beta(\tilde{\mathfrak{b}}_{1,\beta}(z), \tilde{\mathfrak{b}}_1(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_3(z)) = 0$. Regardons ce qu'il se passe sur $\sigma(z)$. La matrice M de l'équation (5.2) agit comme suit : $(\mathfrak{b}_1^M, \mathfrak{b}_2^M, \mathfrak{b}_3^M) = (\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3)$ si $D \equiv 2, 3 \bmod 4$ et $(\mathfrak{b}_1^M, \mathfrak{b}_2^M, \mathfrak{b}_3^M) = (\mathfrak{b}_3, \mathfrak{b}_2, \mathfrak{b}_1)$ si $D \equiv 1 \bmod 4$. Ainsi $(\tilde{\mathfrak{b}}_1^\sigma, \tilde{\mathfrak{b}}_2^\sigma, \tilde{\mathfrak{b}}_3^\sigma) = (\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ si $D \equiv 2, 3 \bmod 4$ et $(\tilde{\mathfrak{b}}_1^\sigma, \tilde{\mathfrak{b}}_2^\sigma, \tilde{\mathfrak{b}}_3^\sigma) = (\tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_1)$ si $D \equiv 1 \bmod 4$. Le polynôme irréductible et unitaire $\Phi_\beta(\tilde{\mathfrak{b}}_{1,\beta}^\sigma, \tilde{\mathfrak{b}}_1^\sigma, \tilde{\mathfrak{b}}_2^\sigma, \tilde{\mathfrak{b}}_3^\sigma)$ a les mêmes racines que $\Phi_\beta(\tilde{\mathfrak{b}}_{1,\beta}, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ et donc, par unicité, ces polynômes doivent être égaux. Ainsi par exemple, si $D \equiv 1 \bmod 4$ (l'autre cas étant similaire), $\Phi_\beta(\tilde{\mathfrak{b}}_{3,\overline{\beta}}, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_1) = \Phi_\beta(\tilde{\mathfrak{b}}_{1,\beta}, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$ et il est possible d'obtenir la valeur $\tilde{\mathfrak{b}}_{3,\overline{\beta}}(z)$ pour tout $z \in \mathcal{H}_1^2$ en utilisant le β-polynôme modulaire. On a alors que, toujours en agissant par σ,

$$\tilde{\mathfrak{b}}_{2,\overline{\beta}}(z) = \Psi_{2,\beta}(\tilde{\mathfrak{b}}_{3,\overline{\beta}}(z), \tilde{\mathfrak{b}}_3(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_1(z))/\Phi'_\beta(\tilde{\mathfrak{b}}_{3,\overline{\beta}}(z), \tilde{\mathfrak{b}}_3(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_1(z)) \quad \text{et}$$

$$\tilde{\mathfrak{b}}_{1,\overline{\beta}}(z) = \Psi_{3,\beta}(\tilde{\mathfrak{b}}_{3,\overline{\beta}}(z), \tilde{\mathfrak{b}}_3(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_1(z))/\Phi'_\beta(\tilde{\mathfrak{b}}_{3,\overline{\beta}}(z), \tilde{\mathfrak{b}}_3(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_1(z)).$$

On conclut qu'une fois que l'on possède les β-polynômes modulaires, il est inutile de calculer les $\overline{\beta}$-polynômes modulaires.

On peut procéder de la même manière avec des matrices de $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}(2,4)$ qui ont des propriétés spéciales, comme dans le cas des p-polynômes modulaires (voir section 4.4). Si γ permute les $\tilde{\mathfrak{b}}_i$ et les $\tilde{\mathfrak{b}}_{i,\beta}$, ceci implique qu'il existe des symétries dans les polynômes modulaires. En particulier, si γ satisfait $(\tilde{\mathfrak{b}}_1^\gamma, \tilde{\mathfrak{b}}_2^\gamma, \tilde{\mathfrak{b}}_3^\gamma) = (\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2)$ et $(\tilde{\mathfrak{b}}_{1,\beta}^\gamma, \tilde{\mathfrak{b}}_{2,\beta}^\gamma, \tilde{\mathfrak{b}}_{3,\beta}^\gamma) = (\tilde{\mathfrak{b}}_{1,\beta}, \tilde{\mathfrak{b}}_{3,\beta}, \tilde{\mathfrak{b}}_{2,\beta})$, ceci signifie que

$$\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2)$$

et par conséquent que

$$\Psi_{2,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_3, \tilde{\mathfrak{b}}_2) = \Psi_{3,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$$

de telle sorte que l'on n'a besoin de calculer que les deux premiers β-polynômes modulaires, car le troisième peut être déduit du deuxième. Ceci arrive par exemple pour $D = 6$, $\ell = 73$, $\beta = 13 - 4\sqrt{6}$ et pour $D = 10$, $\ell = 41$, $\beta = 9 - 2\sqrt{10}$.

De plus, si γ satisfait $\tilde{\mathfrak{b}}_i^\gamma = \imath^{\alpha_i}\tilde{\mathfrak{b}}_i$ et $\tilde{\mathfrak{b}}_{i,\beta}^\gamma = \imath^{\beta_i}\tilde{\mathfrak{b}}_{i,\beta}$, pour $i = 1, 2, 3$ et $\alpha_i, \beta_i \in \{0, 1, 2, 3\}$, alors les puissances des $\tilde{\mathfrak{b}}_i$ dans chacun des coefficients des polynômes modulaires vérifient des relations modulo 4. Comme l'on calcule ces polynômes par évaluation/interpolation (voir section 5.4), ceci peut être utilisé pour faire décroître le nombre d'évaluations.

L'existence de ces matrices dépendent de D et de β. Elles peuvent être recherchées dans une phase de précalcul. Nous donnerons des exemples de relations dans la section 5.5 (voir équation (5.12)).

Soit $\mathcal{L}_\beta$ le lieu des surfaces abéliennes principalement polarisées z modulo $\tilde{\Gamma}(2,4)$ ayant multiplication réelle par $\mathcal{O}_K$ pour lesquelles z, ou $\sigma(z)$ dans le cas $D \equiv 2,3 \bmod 4$, est β-isogène à z' tel que $\phi(z')$ est isogène à un produit de courbes elliptiques par la 2-isogénie $\phi(z') \to \phi(z')/2$ et telle que $\theta_0(\phi(z')/2) = 0$.

Théorème 5.3.19. *Les dénominateurs des polynômes modulaires Φ_β et $\Psi_{k,\beta}$ sont divisibles par un polynôme L_β dans $\mathbb{Q}[\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3]$ décrivant $\mathcal{L}_\beta$.*

Démonstration. Soit $z \in \mathcal{L}_\beta$ et soit c un coefficient de Φ_β. Alors il existe un $\gamma \in \tilde{\Gamma}(2,4)/(\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))$ tel que $\tilde{\mathfrak{b}}_{1,\beta}^{\gamma}$, ou $\tilde{\mathfrak{b}}_{1,\beta}^{\gamma\sigma}$ si $D \equiv 2,3 \bmod 4$, est infini. En effet, rappelons nous que $\mathfrak{b}_{\mathfrak{i}} = \frac{\theta_i}{\theta_0}(\Omega/2)$ et que par la proposition 3.2.3, exactement une des thêta constantes s'annule en Ω si et seulement si Ω est isomorphe à un produit de courbes elliptiques. On conclut en utilisant les mêmes arguments que dans la preuve du théorème 5.3.9. □

La raison pour laquelle nous avons introduit des polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ est pour obtenir des polynômes plus petits que ceux avec les invariants de Gundlach ou avec les tirés en arrière des invariants d'Igusa. Par le théorème 5.3.12, les β-polynômes modulaires ne sont pas définis pour tous les ℓ qui se décomposent en facteurs totalement positifs. Nous avons deux manières de gérer ce problème. La première consiste à trouver un sous-ensemble de $\tilde{\Gamma}(2,4)$ pour lequel $\tilde{\mathfrak{b}}_{i,\beta}$ est invariant (on est dans le cas $D \equiv 2,3 \bmod 4$). Un groupe qui fait toujours l'affaire est le groupe $\tilde{\Gamma}'$ défini comme $\tilde{\Gamma}(2,4)$ dans le cas $D \equiv 1 \bmod 4$. Ce sous-groupe est d'indice 4 dans $\tilde{\Gamma}(2,4)$ et on considère le quotient $\tilde{\Gamma}(2,4)/(\tilde{\Gamma}' \cap \tilde{\Gamma}^0(\beta))$, contenant $4(\ell+1)$ classes, pour définir nos polynômes. La seconde manière consiste à prendre d'autres invariants. En particulier, les tirés en arrière des invariants de Rosenhain $\tilde{\mathfrak{r}}_i = \phi^* \mathfrak{r}_i$. Nous avons déjà dit qu'ils sont des générateurs pour le corps des fonctions modulaires de Hilbert invariantes par $\tilde{\Gamma}(2)$ (voir théorème 5.2.8) et $\tilde{\mathfrak{r}}_{i,\beta}$, pour $i = 1,2,3$, est toujours invariant par $\tilde{\Gamma}(2) \cap \tilde{\Gamma}^0(\beta)$. Tous les résultats de cette section peuvent être adaptés à ces invariants.

5.4 Algorithme

Nous décrivons maintenant un algorithme pour calculer les polynômes modulaires. Nous commençons par les β-polynômes avec les invariants de Gundlach. Nous avons vu que $\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = X^{2(\ell+1)} + \sum_{k=0}^{2(\ell+1)-1} c_k X^k \in \mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)[X]$. On procède par évaluation/interpolation pour calculer les $c_k \in \mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)$ et nous réutilisons et adaptons les techniques décrites dans le chapitre précédent pour le calcul des p-polynômes modulaires.

Rappelons brièvement la phase d'interpolation. Soit $z \in \mathcal{H}_1^2$. En calculant le produit $\prod_{\gamma \in C_\beta} (X - \mathfrak{J}_{1,\beta}^{\gamma}(z))(X - \mathfrak{J}_{1,\overline{\beta}}^{\gamma}(z))$ et en séparant les coefficients en fonction des puissances de X, on obtient les valeurs $c_k(\mathfrak{J}_1(z), \mathfrak{J}_2(z))$. C'est une procédure qui permet d'évaluer les fonctions $c_k \in \mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)$ en n'importe quel point $z \in \mathcal{H}_1$, sans connaître les c_k, qui peuvent alors être obtenus par interpolation (d'une fonction rationnelle bivariée). On écrit

$$c_k = c_k(\mathfrak{J}_1, \mathfrak{J}_2) = \frac{A(\mathfrak{J}_1, \mathfrak{J}_2)}{B(\mathfrak{J}_1, \mathfrak{J}_2)} = \frac{\sum_{m=0}^{d_{\mathfrak{J}_1}^A} \sum_{n=0}^{d_{\mathfrak{J}_2}^A} a_{m,n} \mathfrak{J}_1^m \mathfrak{J}_2^n}{\sum_{m=0}^{d_{\mathfrak{J}_1}^B} \sum_{n=0}^{d_{\mathfrak{J}_2}^B} b_{m,n} \mathfrak{J}_1^m \mathfrak{J}_2^n} = \frac{\sum_{m=0}^{d_{\mathfrak{J}_1}^A} a_m(\mathfrak{J}_2) \mathfrak{J}_1^m}{\sum_{m=0}^{d_{\mathfrak{J}_1}^B} b_m(\mathfrak{J}_2) \mathfrak{J}_1^m}.$$

Soit z_m pour $m = 1, \ldots, d_T^A + d_T^B + 2$, où T désigne le degré total, tel que $(\mathfrak{J}_1(z_m), \mathfrak{J}_2(z_m))$ soit de la forme (u_m, vu_m) pour un $v \in \mathbb{C}$ fixé. On interpole pour trouver la fraction rationnelle univariée $c_k(\mathfrak{J}_1, v\mathfrak{J}_1)$ et on écrit la fraction telle que le coefficient de degré 0 du dénominateur soit 1. Calculons de cette manière les fractions $c_k(\mathfrak{J}_1, v_n\mathfrak{J}_1)$ pour $n = 1, \ldots, \max(d_{\mathfrak{J}_2}^A, d_{\mathfrak{J}_2}^B) + 1$. Il nous reste à interpoler les polynômes a_m et b_m pour obtenir $c_k(\mathfrak{J}_1, \mathfrak{J}_1\mathfrak{J}_2)$ et à remplacer $\mathfrak{J}_2$ par $\mathfrak{J}_2/\mathfrak{J}_1$ pour en déduire $c_k(\mathfrak{J}_1, \mathfrak{J}_2)$.

Les calculs sont fait à une précision N qui doit être suffisamment élevée pour qu'on puisse à la fin reconnaître les coefficients des fractions rationnelles bivariées comme des nombres rationnels. Puisque l'on ne connaît pas de bornes pour cette précision, on l'augmente, en pratique, jusqu'à trouver une précision qui soit suffisante. La complexité de l'interpolation d'une fraction rationnelle bivariée est $\tilde{O}(d_T d_{\mathfrak{J}_2} N)$, où $d_T = \max(d_T^A, d_T^B)$ et $d_{\mathfrak{J}_2} = \max(d_{\mathfrak{J}_2}^A, d_{\mathfrak{J}_2}^B)$.

Notons que pour pouvoir utiliser cette interpolation, on doit être capable de trouver des $z_j \in \mathcal{H}_1^2$ tels que $(\mathfrak{J}_1(z_j), \mathfrak{J}_2(z_j))$ soient de la forme $(u_m, v_n u_m)$. On décrit un algorithme (algorithme 5.4.1) pour calculer $z \in \mathcal{H}_1^2$ à partir des valeurs $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$.

Algorithme 5.4.1 : Calcul de z à partir de $(\mathfrak{J}_1(z), \mathfrak{J}_2(z))$

Entrée : Les valeurs $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$, une précision N
Sortie : z modulo $\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma$

1 Calculer $\mathfrak{j}_1(\Omega)$, $\mathfrak{j}_2(\Omega)$, $\mathfrak{j}_3(\Omega)$, où $\Omega \in \mathcal{H}_2$ tel que $\Omega = \phi_\epsilon(z)$;
2 Appliquer l'algorithme 4.2.1 pour déduire une matrice des périodes Ω (modulo Γ_2) à partir des trois invariants d'Igusa;
3 Trouver un certain $\gamma \in \Gamma_2$ tel que $\phi_\epsilon(z) = \gamma\Omega$ et en déduire z;

La première étape peut être faite en utilisant le corollaire 5.1.12 ou 5.1.14. La seconde a déjà été expliquée et peut être faite en $O(\mathcal{M}'(N)\log N)$ sous la conjecture 3.6.2. Pour la troisième, remarquons que pour $D = 5$, si $z \in \mathcal{H}_1^2$, alors $\phi_\epsilon(z) = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ vérifie par définition $\Omega_1 + \Omega_2 - \Omega_3 = 0$. La seconde étape fournit un $\Omega' \in \mathcal{H}_2$ qui est plus précisément dans la surface de Humbert H_5. Ainsi, par le lemme d'Humbert, on sait qu'il existe une matrice $\gamma \in \Gamma_2$, que l'on peut calculer avec l'algorithme 5.2.1, telle que $\Omega'' = \gamma\Omega' = \left(\begin{smallmatrix} \Omega_1'' & \Omega_2'' \\ \Omega_2'' & \Omega_3'' \end{smallmatrix}\right)$ vérifie $\Omega_1'' + \Omega_2'' - \Omega_3'' = 0$. On a alors que $z^* = ((\frac{\epsilon}{\sqrt{\Delta_K}})^*)^{-1}\, {}^tR^{-1}\Omega''R^{-1}$. Pour $D = 2$, $\phi_\epsilon(z)$ satisfait $\Omega_1 + 2\Omega_2 - \Omega_3 = 0$ et on peut adapter l'algorithme 5.2.1 pour trouver la matrice γ. On a donc montré :

Théorème 5.4.1. *Soient $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$, où $\mathfrak{J}_1$ et $\mathfrak{J}_2$ sont les invariants de Gundlach pour $D = 2$ ou 5, et $z \in \mathcal{H}_1^2$. Sous la conjecture 3.6.2, on peut trouver $z \in \mathcal{H}_1^2/(\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma)$ en temps $O(\mathcal{M}'(N)\log N)$.*

On doit aussi être capable d'évaluer $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ pour tout $z \in \mathcal{H}_1^2$. On pourrait le faire en utilisant leurs définitions en série de Fourier mais la complexité serait mauvaise. On procède comme suit.

Algorithme 5.4.2 : Évaluation de $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$, pour $z \in \mathcal{H}_1^2$

Entrée : $z \in \mathcal{H}_1^2$ et une précision N
Sortie : $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$

1 Calculer $\Omega = \phi_\epsilon(z)$ à précision N;
2 Calculer $\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$ et $\mathrm{j}_3(\Omega)$;
3 Déduire $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ à partir des invariants d'Igusa;

Pour la première étape, il suffit d'utiliser la définition de ϕ_ϵ. Pour la seconde, on peut utiliser l'algorithme 3.6.2 qui calcule rapidement les thêta constantes et la définition 3.3.1 des invariants d'Igusa en terme des thêta constantes. La complexité est en $O(\mathcal{M}'(N)\log N)$, sous la conjecture 3.6.2. Pour la troisième, on doit inverser les tirés en arrière des corollaires 5.1.12 et 5.1.14. Ceci doit être fait dans une étape de précalcul et on peut utiliser des bases de Gröbner. Dans le cas $D = 5$, on a trouvé :

$$\mathfrak{J}_2/\mathfrak{J}_1 = (1/6912\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2 - 1/2304\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_3 - 1/3359232\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3 + 1/373248\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3 + 1/864\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2 - 1/124416\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^2 + 1/124416\phi^*\mathrm{j}_1\phi^*\mathrm{j}_3^3 + 1/3359232\phi^*\mathrm{j}_2^4 - 1/1119744\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3)/(\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2 + 1/1944\phi^*\mathrm{j}_2^4 - 1/648\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3);$$

$$\mathfrak{J}_1 = -(45349632\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^4 - 2584929024/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3 - 499571546112/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^3 + 11019960576/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^2 + 1410554953728/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3 - 20815481088/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^3 + 14693280768/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_3^4 - 186624\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^6 + 16236288/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3 - 12380449536/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^5 - 23514624\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^2 + 146887458048/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3 + 31972578951168/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4 + 90699264\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^3 - 651402114048/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^2 - 90275517038592/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3 - 196515072\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^4 + 1279948013568/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^3 + 226748160\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^5 - 940369969152/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^4 - 544195584/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_3^6 + 192\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^8 - 22464/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 - 18289152/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^7 + 229824/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 + 260527104/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3 + 30051689472/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6 - 1342656/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^3 - 1482541056/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^2 - 171240210432/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3 + 979776\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^4 + 4212476928/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^3 + 243799621632/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^2 - 2286144\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^5 - 5976073728/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^4 + 16656192/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^6 + 3386105856/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^5 - 13856832/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^7 + 5038848/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_3^8 - 320\phi^*\mathrm{j}_2^9 + 5568\phi^*\mathrm{j}_2^8\phi^*\mathrm{j}_3 - 155520\phi^*\mathrm{j}_2^8 - 40320\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3^2 + 4572288/5\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 + 3869835264/5\phi^*\mathrm{j}_2^7 + 155520\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^3 - 6718464/5\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 - 336960\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^4 + 388800\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^5 - 186624\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^6)/(\phi^*\mathrm{j}_2^8 - 42/5\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 - 7776/5\phi^*\mathrm{j}_2^7 + 117/5\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 - 108/5\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^3);$$

Dans le cas $D = 2$, les équations sont trop grosses pour être reproduites ici. Nous en profitons pour remercier Pierre-Jean Spaenlehauer d'avoir réussi à calculer cette base de Gröbner pour nous. On a donc montré :

Théorème 5.4.2. *On peut évaluer les invariants de Gundlach $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ pour $D = 2$ ou 5 en tout point $z \in \mathcal{H}_1^2$ avec une complexité en $O(\mathcal{M}'(N)\log N)$, sous la conjecture 3.6.2.*

Nous avons vu que la complexité pour obtenir z à partir $\mathfrak{J}_1(z)$ et $\mathfrak{J}_2(z)$ est en $\tilde{O}(N)$. Nous devons calculer $\mathfrak{J}_{1,\beta}^{\gamma}$ et $\mathfrak{J}_{1,\overline{\beta}}^{\gamma}$ pour tout $\gamma \in C_\beta$, ce qui peut être

fait avec une complexité en $\tilde{O}(\ell N)$. En utilisant un arbre de sous-produits (voir [85, Section 10.1]), $\Phi_\ell(X, \mathfrak{J}_1(z), \mathfrak{J}_2(z))$ peut être obtenu en $\tilde{O}(\ell N)$ et en utilisant l'interpolation rapide (voir [85, Section 10.2]), $\Psi_\ell(X, \mathfrak{J}_1(z), \mathfrak{J}_2(z))$ peut être calculé avec la même complexité. Tout ceci correspond à une phase d'évaluation.

Pour trouver les β-polynômes modulaires, le nombre de phases d'évaluations est en $O(d_T d_{\mathfrak{J}_2})$ et nous devons interpoler $4(\ell+1)$ fractions rationnelles bivariées. La complexité est alors

$$O(d_T d_{\mathfrak{J}_2})\tilde{O}(\ell N) + 4(\ell+1)\tilde{O}(d_T d_{\mathfrak{J}_2} N) \subseteq \tilde{O}(d_T d_{\mathfrak{J}_2} \ell N). \tag{5.10}$$

Nous considérons maintenant les β-polynômes avec pour invariants les $\tilde{\mathfrak{b}}_i$ (ou les $\tilde{\mathfrak{r}}_i$: la méthode est la même). On doit interpoler des fractions rationnelles trivariées, ce qui peut être fait en regardant des z_j avec la propriété que $(\tilde{\mathfrak{b}}_1(z_j), \tilde{\mathfrak{b}}_2(z_j), \tilde{\mathfrak{b}}_3(z_j))$ sont de la forme $(u_m, v_n u_m, w_r u_m)$, où les indices m, n et r varient de 1 au degré maximal auquel les variables $\tilde{\mathfrak{b}}_1$, $\tilde{\mathfrak{b}}_2$ et $\tilde{\mathfrak{b}}_3$ apparaissent. Le problème est que ces trois variables sont algébriquement dépendantes (rappelons les équations (5.8) et (5.9)), de telle sorte qu'à $\tilde{\mathfrak{b}}_1$ et $\tilde{\mathfrak{b}}_2$ fixés, les valeurs que $\tilde{\mathfrak{b}}_3$ peut prendre sont déterminées (de plus, elles ne seront pas de la forme $w_r u_m$ et le nombre de valeurs sera inférieur au degré en $\tilde{\mathfrak{b}}_3$). Notons par E l'équation entre les trois variables. Une solution à ce problème consiste à remarquer que $\mathbb{Q}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)/(E) = \mathbb{Q}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)[\tilde{\mathfrak{b}}_3]/(E)$. Ainsi, chaque coefficient c_k du β-polynôme modulaire peut être écrit comme $c_k(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \sum_{i=0}^{d-1} c_{k,i}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)\tilde{\mathfrak{b}}_3^i$, où d est le degré dans lequel les variables $\tilde{\mathfrak{b}}_3$ apparaissent dans E et $c_{k,i} \in \mathbb{Q}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)$.

L'interpolation est faite comme suit. Pour assez de valeurs u_m et v_n, on calcule les d racines w_r de $E(u_m, v_n u_m, x)$. Pour $r = 1, \ldots, d$, on trouve $z_r \in \mathcal{H}_1^2$ tel que $(\tilde{\mathfrak{b}}_1(z), \tilde{\mathfrak{b}}_2(z), \tilde{\mathfrak{b}}_3(z)) = (u_m, v_n u_m, w_r)$ et on évalue les β-polynômes modulaires en z_r. Ceci donne les valeurs $c_k(\tilde{\mathfrak{b}}_1(z_r), \tilde{\mathfrak{b}}_2(z_r), \tilde{\mathfrak{b}}_3(z_r))$. En faisant l'interpolation d'un polynôme univarié avec w_r et $c_k(\tilde{\mathfrak{b}}_1(z_r), \tilde{\mathfrak{b}}_2(z_r), \tilde{\mathfrak{b}}_3(z_r))$, on trouve les $c_{k,i}(\tilde{\mathfrak{b}}_1(z_r), \tilde{\mathfrak{b}}_2(z_r)) = c_{k,i}(u_m, v_n u_m)$. Nous venons juste d'expliquer une procédure pour évaluer les polynômes bivariés $c_{k,i}$ en un point donné et on a déjà vu comment interpoler une fraction rationnelle bivariée.

Comme avec les invariants de Gundlach, on a besoin de procédures pour le calcul des $\tilde{\mathfrak{b}}_i(z)$ en $z \in \mathcal{H}_1^2$ et pour trouver certains $z \in \mathcal{H}_1^2$ à partir des $\tilde{\mathfrak{b}}_i(z)$. Le premier est similaire à l'algorithme 5.4.2, la troisième étape étant triviale car $\tilde{\mathfrak{b}}_i = \phi^* \mathfrak{b}_\mathfrak{i}$, et a la même complexité. Pour la deuxième procédure, on procède comme dans l'algorithme 5.4.1, la première étape étant également triviale. Pour la seconde, il est possible de trouver Ω modulo $\Gamma_2(2,4)$ en $\tilde{O}(N)$ (voir l'algorithme 4.2.2 et la section 4.2.2). La difficulté réside dans la troisième étape. En effet, nous sommes capable de trouver γ tel que $\phi(z) = \gamma\Omega$, mais γ n'est pas nécessairement dans $\Gamma_2(2,4)$ de telle sorte que l'on ne trouve que z modulo $\tilde{\Gamma} \cup \tilde{\Gamma}\sigma$ au lieu de z modulo $\tilde{\Gamma}(2,4)$, si $D \equiv 1 \bmod 4$, et modulo $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$, si $D \equiv 2, 3 \bmod 4$. Une solution consiste à précalculer toutes les classes de $\tilde{\Gamma}/\tilde{\Gamma}(2,4)$ et de $\tilde{\Gamma}/\tilde{\Gamma}(2,4)\sigma$ et voir comment ces classes sont envoyées vers les classes de $\Gamma_2/\Gamma_2(2,4)$. Il suffit de trouver dans quelle classe de $\Gamma_2/\Gamma_2(2,4)$ γ appartient pour trouver la matrice $\tilde{\gamma}$ qui correspond dans $\tilde{\Gamma}/\tilde{\Gamma}(2,4)$ ou dans $\tilde{\Gamma}/\tilde{\Gamma}(2,4)\sigma$. On a alors $\phi(\tilde{\gamma}^{-1}z) = \phi(\tilde{\gamma}^{-1})\phi(z) = \gamma^{-1}\gamma\Omega = \Omega$. Ainsi :

Théorème 5.4.3. *Supposons la conjecture 3.6.2. On peut évaluer les trois $\tilde{\mathfrak{b}}_i(z)$ pour $z \in \mathcal{H}_1^2$ en $O(\mathcal{M}'(N)\log N)$ et on peut déduire z modulo $\tilde{\Gamma}(2,4)$ ou modulo $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$ selon les cas à partir des $\tilde{\mathfrak{b}}_i(z)$ avec cette même complexité.*

Pour calculer les β-polynômes modulaires, l'étape d'évaluation sera exécutée $O(dd_T d_{\tilde{\mathfrak{b}}_2})$ fois, où d est le degré en $\tilde{\mathfrak{b}}_3$ de E, et on doit interpoler $O(d\ell)$ fractions rationnelles bivariées et faire $O(\ell d_T d_{\tilde{\mathfrak{b}}_2})$ interpolations de polynômes univariés. La complexité est alors

$$O(dd_T d_{\tilde{\mathfrak{b}}_2})\tilde{O}(\ell N)+O(d\ell)\tilde{O}(d_T d_{\tilde{\mathfrak{b}}_2} N)+O(\ell d_T d_{\tilde{\mathfrak{b}}_2})\tilde{O}(dN) \subseteq \tilde{O}(dd_T d_{\tilde{\mathfrak{b}}_2}\ell N). \quad (5.11)$$

Théorème 5.4.4. *Sous les heuristiques du théorème 4.2.15, la complexité du calcul des β-polynômes modulaires avec les Gundlach est donnée par l'équation (5.10), tandis que la complexité pour le calcul des β-polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ est donnée par l'équation (5.11). Ces complexités sont quasi-linéaires en la taille de la sortie.*

5.5 Résultats

Nous présentons dans cette section des polynômes que nous avons calculés et nous comparons des polynômes avec des invariants différents lorsque cette comparaison a un sens.

5.5.1 Cas $D = 2$

Nous avons calculé des β-polynômes modulaires avec les Gundlach pour de nombreux nombres premiers, en particulier pour $\ell = 2, 7, 17, 23, 31$ et 41. Si on écrit dans le cas ramifié

$$\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(\mathfrak{J}_1, \mathfrak{J}_2)X^i \quad \text{et} \quad \Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{i=0}^{2\ell+1} d_i(\mathfrak{J}_1, \mathfrak{J}_2)X^i,$$

alors nous avons constaté que le dénominateur de c_i est de la forme $D(\mathfrak{J}_1, \mathfrak{J}_2)^4$ sauf pour $i = 2\ell + 1$, où c'est $D(\mathfrak{J}_1, \mathfrak{J}_2)^2$, et le dénominateur de d_i est de la forme $D(\mathfrak{J}_1, \mathfrak{J}_2)^6$, sauf pour $i = 2\ell+1$, où c'est $D(\mathfrak{J}_1, \mathfrak{J}_2)^4$. Nous avons par exemple pour $\ell = 7$

$$D(\mathfrak{J}_1, \mathfrak{J}_2) = \mathfrak{J}_1^2 - \mathfrak{J}_1\mathfrak{J}_2^2 + 2\mathfrak{J}_1\mathfrak{J}_2 - 81\mathfrak{J}_1 + 64\mathfrak{J}_2^2$$

et pour $\ell = 17$

$$\begin{aligned} D(\mathfrak{J}_1, \mathfrak{J}_2) = {} & \mathfrak{J}_1^7 - \mathfrak{J}_1^6\mathfrak{J}_2^3 - 6\mathfrak{J}_1^6\mathfrak{J}_2^2 + \mathfrak{J}_1^6\mathfrak{J}_2 - 414\mathfrak{J}_1^6 + 428\mathfrak{J}_1^5\mathfrak{J}_2^3 + 2387\mathfrak{J}_1^5\mathfrak{J}_2^2 - \\ & 17760\mathfrak{J}_1^5\mathfrak{J}_2 + 431811\mathfrak{J}_1^5 + 17728\mathfrak{J}_1^4\mathfrak{J}_2^4 - 331952\mathfrak{J}_1^4\mathfrak{J}_2^3 - 2578856\mathfrak{J}_1^4\mathfrak{J}_2^2 + \\ & 6229197\mathfrak{J}_1^4\mathfrak{J}_2 - 80515134\mathfrak{J}_1^4 - 6145536\mathfrak{J}_1^3\mathfrak{J}_2^4 + 52974272\mathfrak{J}_1^3\mathfrak{J}_2^3 + \\ & 53503704\mathfrak{J}_1^3\mathfrak{J}_2^2 + 611681641\mathfrak{J}_1^3\mathfrak{J}_2 + 3782285936\mathfrak{J}_1^3 - 91648000\mathfrak{J}_1^2\mathfrak{J}_2^5 - \\ & 650215321\mathfrak{J}_1^2\mathfrak{J}_2^4 - 7579320576\mathfrak{J}_1^2\mathfrak{J}_2^3 - 19714461177\mathfrak{J}_1^2\mathfrak{J}_2^2 - \\ & 17565696000\mathfrak{J}_1\mathfrak{J}_2^5 - 781204275\mathfrak{J}_1\mathfrak{J}_2^4 + 1105920000\mathfrak{J}_2^6. \end{aligned}$$

Le tableau 5.1 contient certaines informations au sujet de ces polynômes. La première colonne est le nombre premier ℓ, la seconde l'espace mémoire des β-polynômes modulaires, ensuite nous avons mis le degré total et les degrés en $\mathfrak{J}_1$ et en $\mathfrak{J}_2$ du polynôme bivarié $D(\mathfrak{J}_1, \mathfrak{J}_2)$, et de même pour les degrés maximaux apparaissant dans les numérateurs. La dernière colonne est le nombre de chiffres décimaux du plus grand coefficient apparaissant dans un des polynômes.

2	0.325 Ko	3	0	3	4	4	2	8
7	163 Ko	3	2	2	25	23	13	66
17	5.8 Mo	9	7	6	65	61	36	195
23	21 Mo	12	11	8	87	85	48	280
31	70 Mo	17	14	10	117	111	61	401
41	225 Mo	23	21	14	157	153	84	559

TABLEAU 5.1 – Informations sur les β-polynômes modulaires pour $D = 2$.

Nous avons obtenu des β-polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ pour $\ell = 17$ et 41 (qui sont congrus à 1 modulo 4, voir la proposition 5.3.12). Par la remarque 5.3.15, les β-polynômes modulaires sont

$$\Phi_\beta(X, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)X^i \quad \text{et} \quad \Psi_\beta(X, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \sum_{i=0}^{2\ell+1} d_i(\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)X^i.$$

Nous avons constaté que les dénominateurs de c_i et de d_i sont de la forme $D(\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)^2$ sauf pour $i = 2\ell + 1$, où c'est $D(\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3)$. Par exemple, on a pour $\ell = 17$ et $\beta = 5 + 2\sqrt{2}$:

$$D(\tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = \tilde{\mathfrak{b}}_3^6\tilde{\mathfrak{b}}_2^{18} + (6\tilde{\mathfrak{b}}_3^8 - 6\tilde{\mathfrak{b}}_3^4 + 1)\tilde{\mathfrak{b}}_2^{16} + (15\tilde{\mathfrak{b}}_3^{10} - 24\tilde{\mathfrak{b}}_3^6 + 7\tilde{\mathfrak{b}}_3^2)\tilde{\mathfrak{b}}_2^{14} + (20\tilde{\mathfrak{b}}_3^{12} - 42\tilde{\mathfrak{b}}_3^8 + 9\tilde{\mathfrak{b}}_3^4 + 2)\tilde{\mathfrak{b}}_2^{12} + (15\tilde{\mathfrak{b}}_3^{14} - 48\tilde{\mathfrak{b}}_3^{10} + 37\tilde{\mathfrak{b}}_3^6 + 4\tilde{\mathfrak{b}}_3^2)\tilde{\mathfrak{b}}_2^{10} + (6\tilde{\mathfrak{b}}_3^{16} - 42\tilde{\mathfrak{b}}_3^{12} + 68\tilde{\mathfrak{b}}_3^8 - 26\tilde{\mathfrak{b}}_3^4 + 3)\tilde{\mathfrak{b}}_2^8 + (\tilde{\mathfrak{b}}_3^{18} - 24\tilde{\mathfrak{b}}_3^{14} + 37\tilde{\mathfrak{b}}_3^{10} + 8\tilde{\mathfrak{b}}_3^6 - \tilde{\mathfrak{b}}_3^2)\tilde{\mathfrak{b}}_2^6 + (-6\tilde{\mathfrak{b}}_3^{16} + 9\tilde{\mathfrak{b}}_3^{12} - 26\tilde{\mathfrak{b}}_3^8 - 24\tilde{\mathfrak{b}}_3^4 + 2)\tilde{\mathfrak{b}}_2^4 + (7\tilde{\mathfrak{b}}_3^{14} + 4\tilde{\mathfrak{b}}_3^{10} - \tilde{\mathfrak{b}}_3^6)\tilde{\mathfrak{b}}_2^2 + (\tilde{\mathfrak{b}}_3^{16} + 2\tilde{\mathfrak{b}}_3^{12} + 3\tilde{\mathfrak{b}}_3^8 + 2\tilde{\mathfrak{b}}_3^4 + 1).$$

Pour $\ell = 17$ et 41, les degrés des coefficients c_i et d_i en les variables $\tilde{\mathfrak{b}}_2$ et $\tilde{\mathfrak{b}}_3$ sont proches des degrés en les variables $\mathfrak{J}_1$ et $\mathfrak{J}_2$. Par contre, avec les $\tilde{\mathfrak{b}}_i$, il y a certaines relations entre les exposants. Le numérateur de c_i peut être écrit comme $\sum_m \sum_n c_{i,m,n}\tilde{\mathfrak{b}}_2^m\tilde{\mathfrak{b}}_3^n$ (et similairement pour d_i). On a alors que pour $\ell = 17$ et $\beta = 5 + 2\sqrt{2}$:

$$\begin{array}{rcl} m & \equiv & 0 \bmod 2 \\ n+i & \equiv & 0 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \qquad \text{et} \qquad \begin{array}{rcl} m & \equiv & 1 \bmod 2 \\ n+i & \equiv & 1 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \tag{5.12}$$

pour respectivement c_i et d_i. Dans le cas $\ell = 41$ et $\beta = 7 + 2\sqrt{2}$, ces équations sont les mêmes sauf pour la dernière qui est $m + n \equiv -i \bmod 4$ pour c_i et d_i. Une autre différence est que pour $\ell = 17$, le plus grand $c_{i,m,n}$ ou $d_{i,m,n}$ s'écrit avec 13 chiffres décimaux, contre 195 pour les polynômes avec les invariants de Gundlach. Pour $\ell = 41$, c'est 38 contre 559. Du coup, les β-polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ sont plus petits. En terme d'espace mémoire, ils prennent respectivement 221 Ko et 7.2 Mo, ce qui est environ 26 et 31 fois plus petit que dans le cas des Gundlach.

Lorsque $\ell \equiv 3 \bmod 4$, nous avons fait comme expliqué à la fin de la section 5.3.2. D'une part, nous avons calculé les polynômes en utilisant le sous-groupe d'indice $4(\ell + 1)$ et d'autre part, nous avons calculé les polynômes en utilisant les invariants de Rosenhain. La première solution donne de meilleurs résultats en terme de degrés, les polynômes sont plus creux et ils occupent 930 Ko dans le premier cas contre 70 Mo dans le second pour $\ell = 7$. Notons que dans les deux cas, c'est bien plus que les 163 Ko avec les invariants de Gundlach.

5.5.2 Cas $D = 5$

Nous avons calculé les β-polynômes modulaires avec les Gundlach pour $\ell = 5, 11, 19, 29$ et 31. Si on écrit

$$\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(\mathfrak{J}_1, \mathfrak{J}_2)X^i \quad \text{et} \quad \Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{i=0}^{2\ell+1} d_i(\mathfrak{J}_1, \mathfrak{J}_2)X^i,$$

lorsque ℓ se décompose, alors nous avons constaté que les dénominateurs de c_i et de d_i sont de la forme $D(\mathfrak{J}_1, \mathfrak{J}_2)^4$ sauf pour $i = 2\ell + 1$, où c'est $D(\mathfrak{J}_1, \mathfrak{J}_2)^2$. Nous avons par exemple pour $\ell = 11$:

$$\begin{aligned}
&D(\mathfrak{J}_1, \mathfrak{J}_2) = 4\mathfrak{J}_1^7 + (-12\mathfrak{J}_2^2 - 19236\mathfrak{J}_2 + 119497519)\mathfrak{J}_1^6 + (12\mathfrak{J}_2^4 + 56972\mathfrak{J}_2^3 - \\
&387805052\mathfrak{J}_2^2 - 278163835056\mathfrak{J}_2 + 35953243171744)\mathfrak{J}_1^5 + (-4\mathfrak{J}_2^6 - 55980\mathfrak{J}_2^5 + \\
&4497306 98\mathfrak{J}_2^4 + 943837290960\mathfrak{J}_2^3 - 1332306926913 92\mathfrak{J}_2^2 + 6651010132099840\mathfrak{J}_2 + \\
&13001634695104256)\mathfrak{J}_1^4 + (18500\mathfrak{J}_2^7 - 215193500\mathfrak{J}_2^6 - 1170430882000\mathfrak{J}_2^5 + \\
&3883242339800000\mathfrak{J}_2^4 - 3239522671651200 0\mathfrak{J}_2^3)\mathfrak{J}_1^3 + (32609375\mathfrak{J}_2^8 + \\
&635091750000\mathfrak{J}_2^7 - 7186325130000000\mathfrak{J}_2^6 + 346206774240000 00\mathfrak{J}_2^5)\mathfrak{J}_1^2 + \\
&(-1248750000000\mathfrak{J}_2^9 + 60191100000000 00\mathfrak{J}_2^8)\mathfrak{J}_1 - 18225000000000 00\mathfrak{J}_2^{10}.
\end{aligned}$$

Nous avons obtenu les β-polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ pour $\ell = 5, 11$ et 19. Ces polynômes sont

$$\Phi_\beta(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = X^{\ell+1} + \sum_{i=0}^{\ell}(\sum_{j=0}^{4} c_{i,j}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)\tilde{\mathfrak{b}}_3^j)X^i \qquad \text{et}$$

$$\Psi_{k,\beta}(X, \tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2, \tilde{\mathfrak{b}}_3) = X^{\ell+1} + \sum_{i=0}^{\ell}(\sum_{j=0}^{4} d_{k,i,j}(\tilde{\mathfrak{b}}_1, \tilde{\mathfrak{b}}_2)\tilde{\mathfrak{b}}_3^j)X^i,$$

d'après l'équation (5.8) et ce que l'on a dit dans la section 5.4. Le tableau 5.2 contient les mêmes informations que le tableau 5.1. La partie haute concerne les polynômes avec les invariants de Gundlach tandis que la seconde ceux avec les $\tilde{\mathfrak{b}}_i$.

5	14 Ko	5	3	5	10	10	10	53
11	3.5 Mo	10	7	10	40	40	40	252
19	33 Mo	16	12	16	64	64	64	513
5	14 Ko	16	8	8	31	19	22	5
11	296 Ko	72	40	40	76	49	49	11
19	3.6 Mo	128	96	96	128	103	108	25

TABLEAU 5.2 – Informations sur les polynômes modulaires pour $D = 5$.

On peut voir qu'il y a un gain à utiliser les $\tilde{\mathfrak{b}}_i$ en terme d'espace mémoire, sauf pour $\ell = 5$, qui correspond au cas ramifié. Les degrés sont plus grand avec les $\tilde{\mathfrak{b}}_i$ mais il y a des relations modulo 4 entre les exposants.

5.6 Exemples de courbes β-isogènes

Comme pour les p-isogénies, nous donnons des exemples de courbes hyperelliptiques dont les Jacobiennes sont β-isogènes sur un corps fini.

Commençons avec des exemples de courbes trouvées en se plaçant sur $\mathbb{Q}(\sqrt{2})$ et en prenant les invariants de Gundlach. Les Jacobiennes des courbes suivantes sont $(3 + \sqrt{2})$-isogènes sur $\mathbb{F}_{2333}$:

$$\begin{aligned} Y^2 &= 356X^6 + 116X^5 + 1589X^4 + 986X^3 + 178X^2 + 1094X + 1229, \\ Y^2 &= 144X^6 + 2096X^5 + 387X^4 + 1562X^3 + 478X^2 + 486X + 1718 \end{aligned}$$

tandis que les Jacobiennes de celles qui suivent sont $(5+2\sqrt{2})$-isogènes sur $\mathbb{F}_{345267203}$:

$$\begin{aligned} Y^2 &= 288618938X^5 + 208826828X^4 + 73681500X^3 + 329580565X^2 + \\ &\quad 193693317X + 328425210, \\ Y^2 &= 229859713X^5 + 180037958X^4 + 95105703X^3 + 68631100X^2 + \\ &\quad 32660205X + 107566399 \end{aligned}$$

et les Jacobiennes des courbes ci-après sont $(7+\sqrt{2})$-isogènes sur $\mathbb{F}_{3526982779}$:

$$\begin{aligned} Y^2 &= 3476666651X^5 + 2997006123X^4 + 2343918968X^3 + 1313289865X^2 + \\ &\quad 1251164949X + 1521154595, \\ Y^2 &= 2390845907X^6 + 2649299485X^5 + 3307186776X^4 + 2143442296X^3 + \\ &\quad 1448110737X^2 + 918458873X + 1476608496. \end{aligned}$$

Nous donnons également deux exemples de paires de courbes calculées avec les polynômes modulaires avec les invariants de Gundlach sur $\mathbb{Q}(\sqrt{5})$. Premier exemple de courbes pour des $(4-(1+\sqrt{5})/2)$-isogénies sur $\mathbb{F}_{56311}$:

$$\begin{aligned} Y^2 &= 13477X^5 + 6136X^4 + 35146X^3 + 28148X^2 + 7150X + 19730, \\ Y^2 &= 2953X^5 + 26725X^4 + 14100X^3 + 6565X^2 + 22149X + 19740 \end{aligned}$$

et deuxième exemple pour des $(5+2(1+\sqrt{5})/2)$-isogénies sur $\mathbb{F}_{6728947}$:

$$\begin{aligned} Y^2 &= 3739712X^6 + 4881762X^5 + 6611129X^4 + 5775262X^3 + 521647X^2 + \\ &\quad 2066678X + 350732, \\ Y^2 &= 2707309X^6 + 1535264X^5 + 311501X^4 + 2965267X^3 + 3507011X^2 + \\ &\quad 101110X + 5795310. \end{aligned}$$

Enfin, nous donnons une paire de courbes dont les Jacobiennes sont $(7+2\sqrt{2})$-isogènes sur $\mathbb{F}_{562789}$, calculées en utilisant les polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ sur $\mathbb{Q}(\sqrt{2})$:

$$\begin{aligned} Y^2 &= 540913X^5 + 353915X^4 + 118050X^3 + 355166X^2 + 424096X + 379433, \\ Y^2 &= 231396X^5 + 474300X^4 + 200176X^3 + 335056X^2 + 345222X + 464702 \end{aligned}$$

et une paire pour des $(5-(1+\sqrt{5})/2)$-isogénies sur $\mathbb{F}_{5362789}$, calculés en utilisant les polynômes modulaires avec les $\tilde{\mathfrak{b}}_i$ sur $\mathbb{Q}(\sqrt{5})$:

$$\begin{aligned} Y^2 &= 2531476X^5 + 900554X^4 + 1248025X^3 + 440959X^2 + 912166X + \\ &\quad 4367293, \\ Y^2 &= 1772175X^5 + 3557482X^4 + 848889X^3 + 4562893X^2 + 146681X + \\ &\quad 475016. \end{aligned}$$

Ici aussi, le lecteur motivé peut vérifier l'existence d'une isogénie entre les différentes Jacobiennes de courbes en vérifiant que les fonctions zéta des courbes sont identiques.

Perspectives

Avant la présente thèse, une généralisation en dimension 2 des polynômes modulaires ne se retrouve essentiellement que dans les travaux de thèse de Régis Dupont ([19]), quant à l'aspect algorithmique des polynômes définis avec les invariants d'Igusa, et dans un article de Bröker-Lauter ([9]) donnant de nombreux résultats théoriques permettant de caractériser ces polynômes : on y montre que le premier polynôme modulaire est un polynôme minimal, que les trois polynômes modulaires sont dans $\mathbb{Q}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[X]$ et le lien entre le dénominateur commun et les surfaces qui sont p-isogènes à un produit de courbes elliptiques.

Nous avons pu généraliser ces différents résultats selon deux directions. D'une part, en introduisant des polynômes modulaires pour d'autres invariants, comme les invariants de Streng et les $\mathfrak{b}_i$, et en démontrant des propriétés de ces polynômes, analogues à celles de [9] avec en plus des symétries et des relations modulo 2 et 4 avec les invariants $\mathfrak{b}_i$, et, d'autre part, en définissant la notion de polynômes modulaires associées aux isogénies cycliques dans le cas où il y a multiplication réelle maximale, où nous avons là aussi pu démontrer des résultats au sujet de ces polynômes.

Néanmoins, il reste encore quelques zones d'ombres. Nous n'avons pas de bornes sur les coefficients entiers qui apparaissent dans les polynômes, ni sur les degrés des invariants dans les numérateurs et nous ne savons pas d'où viennent les exposants qui apparaissent dans la partie commune aux dénominateurs.

Alors que nous avons pu calculer de nombreux polynômes modulaires de Hilbert, nous avons vu que nous ne disposons de polynômes de Siegel que pour $p = 2, 3, 5$ et 7. Pour pouvoir obtenir plus de polynômes, nos travaux suggèrent de trouver des invariants qui seraient définis pour des sous-groupes dont la définition fait intervenir des congruences modulo un nombre plus grand que 4. Dans tous les cas, le nombre de p-isogénies est d'ordre p^3 ce qui nous fait penser que la taille des polynômes modulaires est en p^{15} (p^3 par invariant, p^3 pour le nombre d'isogénies et p^3 pour la taille des entiers). Mais de meilleurs invariants ne feront que diviser la complexité par une constante.

On pourrait également définir et calculer des polynômes modulaires sur la surface de Hilbert avec des p-isogénies, au lieu des β-isogénies comme on l'a présenté dans ce manuscrit. Le nombre d'isogénies est ici d'ordre p^2.

Enfin, nous comptons appliquer ces différents polynômes modulaires comme on le fait en dimension 1. En particulier dans l'exploration de graphes d'isogénies, dans le calcul de l'anneau des endomorphismes de surfaces abéliennes et dans la production d'un algorithme type CRT de calcul de polynômes de classes d'Igusa.

Bibliographie

[1] A.N. Andrianov et V.G. Zhuravlev : *Modular forms and Hecke operators*, volume 145 de *AMS Translations of mathematical monographs*. American Mathematical Society, 1995.

[2] K. Belabas et al. : Pari/gp. `http://pari.math.u-bordeaux.fr/`, October 2012. Bordeaux, 2.5.3 edition.

[3] J. Belding, R. Bröker, A. Enge et K. Lauter : Computing Hilbert class polynomials. *In Algorithmic Number Theory 8th International Symposium (ANTS VIII)*, volume 5011 de *LNCS*, pages 282–295. Springer-Verlag Berlin, 2008.

[4] C. Birkenhake et H. Lange : *Complex abelian varieties, 2nd ed*, volume 302 de *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin, 2003.

[5] C. Birkenhake et H. Wilhelm : Humbert surfaces and the Kummer plane. *Transactions of the American Mathematical society*, 355(5):1819–1841, 2003.

[6] G. Bisson et A.V. Sutherland : Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 113:815–831, 2011.

[7] J.-B. Bost et J.-F. Mestre : Moyenne arithmético-géométrique et périodes de courbes de genre 1 et 2. *Gaz. Math.*, 38:36–64, 1988.

[8] R. Bröker, D. Gruenewald et K. Lauter : Explicit CM-theory for level 2-structures on abelian surfaces. *Algebra Number Theory*, 5(4):495–528, 2011.

[9] R. Bröker et K. Lauter : Modular polynomials for genus 2. *LMS Journal of Computation and Mathematics*, 12:326–339, 2009.

[10] R. Bröker, K Lauter et A.V. Sutherland : Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81:1201–1231, 2012.

[11] D. Charles et K Lauter : Computing modular polynomials. *LMS Journal of Computation and Mathematics*, 8:195–204, 2005.

[12] P. Cohen : On the coefficients of the transformation polynomials for the elliptic modular function. *Mathematical Proceedings of the Cambridge Philosophical Society*, 95:389–402, 1984.

[13] R. Cosset : *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*. Thèse de doctorat, Université Henri Poincaré - Nancy 1, 2011.

[14] R. Cosset et D. Robert : Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. *Mathematics of Computation*, 84(294):1953–1975, 2015.

[15] J.-M. Couveignes et T. Ezome : Computing functions on Jacobians and their quotients. *LMS Journal of Computation and Mathematics*, 18(1):555–577, 2015.

[16] D. Cox : *Primes of the form $x^2 + ny^2$*. John Wiley and Sons, Inc., 1989.

[17] P. Davis et P. Rabinowitz : *Methods of Numerical Integration, 2nd ed.* Academic Press, Orlando, FL, 1984.

[18] A. Dudeanu, D. Jetchev et D. Robert : Computing cyclic isogenies in genus 2. À paraître.

[19] R. Dupont : *Moyenne arithmético-géométrique, suites de Borchardt et applications*. Thèse de doctorat, École polytechnique, 2006. `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/`.

[20] R. Dupont : Fast evaluation of modular functions using Newton iterations and the AGM. *Mathematics of Computation*, 80(275):1823–1847, 2011.

[21] K. Eisenträger et K. Lauter : A CRT algorithm for constructing genus 2 curves over finite fields. *In Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 de *Sémin. Congr.*, pages 161–176. Soc. Math. France, Paris, 2010.

[22] K. Eisenträger et K. Lauter : A CRT algorithm for constructing genus 2 curves over finite fields. *In Arithmetic, Geometry and Coding Theory (AGCT-10)*, volume 21 de *Séminaires et Congrès*, pages 161–176. Société Mathématique de France, Paris, 2009.

[23] N. Elkies : Elliptic and modular curves over finite fields and related computational issues. *In Computational perspectives on number theory : Proceedings of the conference in honor of A.O.L. Atkin*, volume 7 de *AMS/IP Studies in Advanced Mathematics, Boston*, pages 21–76. AMS, 1998.

[24] N.D. Elkies : Explicit isogenies. *manuscript, Boston MA*, 1992.

[25] A. Enge : Computing modular polynomials in quasi-linear time. *Mathematics of Computation*, 78:1809–1824, 2009.

[26] A. Enge : Pari-gnump. `http://www.multiprecision.org/index.php?prog=pari-gnump/`, February 2014. 0.0.1 edition.

[27] A. Enge, M. Gastineau, P. Théveny et P. Zimmermann : Gnu mpc - a library for multiprecision complex arithmetic with exact rounding. `http://mpc.multiprecision.org/`, September 2012. INRIA, 1.0.1 edition.

[28] A. Enge et A.V. Sutherland : Class invariants by the CRT method. *In Algorithmic Number Theory 9th International Symposium (ANTS IX)*, volume 6197 de *LNCS*, pages 142–156. Springer-Verlag Berlin, 2010.

[29] A. Enge et E. Thomé : Computing class polynomials for abelian surfaces. *Experimental Mathematics*, 23(2):129–145, 2014.

[30] A. Enge et E. Thomé : Cmh - computation of Igusa class polynomials. `http://cmh.gforge.inria.fr/`, March 2014. 1.0 edition.

[31] D. Freeman et K. Lauter : Computing endomorphism rings of Jacobians of genus 2 curves over finite fields. *In Algebraic geometry and its applications*, volume 5 de *Ser. Number Theory Appl.*, pages 29–66. World Sci. Publ., Hackensack, NJ, 2008.

[32] E. Freitag : *Siegelsche Modulfunktionen*, volume 254 de *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin, 1983.

[33] E. Gottschling : Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades. *Annals of Mathematics*, 138:103–124, 1959.

[34] T Granlund et al. : Gmp - the GNU multiple precision arithmetic library. `http://gmplib.org/`, February 2013. 5.1.1 edition.

[35] D. Gruenewald : *Explicit algorithms for Humbert surfaces*. Thèse de doctorat, University of Sydney, 2008. `http://echidna.maths.usyd.edu.au/~davidg/thesis.html`.

[36] K.-B. Gundlach : Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$. *Math. Ann.*, 152:226–256, 1963.

[37] G. Hanrot, V. Lefèvre, P. Pélissier, P. Zimmermann et al. : GNU mpfr - a library for multiple-precision floating-point computations with exact rounding. `http://www.mpfr.org/`, July 2012. 3.1.1 edition.

[38] R. Hartshorne : *Algebraic Geometry*, volume 52 de *Graduate Texts in Mathematics*. Springer-Verlag New York, 1977.

[39] M. Hindry et J.H. Silverman : *Diophantine geometry*, volume 201 de *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[40] F. Hirzebruch et G. Van der Geer : *Lectures on Hilbert modular surfaces*, volume Séminaire scientifique OTAN,77 de *Presses de l'université de Montréal, Montréal*. Séminaire de Mathématiques Supérieures, 1981.

[41] F. Hirzebruch et D. Zagier : Classification of hilbert modular surfaces. *In* W. L. Jr Baily et T. Shioda, éditeurs : *Complex Analysis and Algebraic Geometry*, pages 43–78. Cambridge University Press, 1977.

[42] G. Humbert : Sur les fonctions abéliennes singulières i. *Journal de Mathématiques Pures et Appliquées, serie 5*, V:233–350, 1899.

[43] G. Humbert : Sur les fonctions abéliennes singulières ii. *Journal de Mathématiques Pures et Appliquées, serie 5*, VI:279–386, 1900.

[44] G. Humbert : Sur les fonctions abéliennes singulières iii. *Journal de Mathématiques Pures et Appliquées, serie 5*, VII:97–124, 1901.

[45] J.I. Igusa : Arithmetic variety of moduli for genus 2. *Annals of Mathematics*, 72(3):612–649, 1960.

[46] J.I. Igusa : On Siegel modular forms of genus 2. *American Journal of Mathematics*, 84(1):175–200, 1962.

[47] J.I. Igusa : Modular forms and projective invariants. *American Journal of Mathematics*, 89(3):817–855, 1967.

[48] J.I. Igusa : *Theta functions*, volume 194 de *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1972.

[49] O.H. King : The subgroup structure of finite classical groups in terms of geometric configurations. *In* Bridget S. Webb, éditeur : *Surveys in Combinatorics*, pages 29–56. Cambridge University Press, 2005.

[50] H. Klingen : *Introductory lectures on Siegel modular forms*, volume 20 de *Cambridge studies in advanced mathematics*. Cambridge University Press, Cambridge, 1990.

[51] N. Koblitz : Elliptic curves cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[52] N. Koblitz : Hyperelliptic cryptosystems. *Journal of Cryptologie*, 1:139–150, 1989.

[53] D. Kohel : *Endomorphism rings of elliptic curves over finite fields*. Thèse de doctorat, University of California, 1996.

[54] K. Lauter, M. Naehrig et T. Yang : Hilbert theta series and invariants of genus 2 curves. *Journal of Number Theory*, 2015.

[55] K. Lauter et D. Robert : Improved CRT Algorithm for Class Polynomials in Genus 2. *In ANTS X - Algorithmic Number Theory 2012*, volume 1 de *The Open Book Series*, pages 437–461. Mathematical Sciences Publisher, 2012.

[56] K. Lauter et T.H. Yang : Computing genus 2 curves from invariants on the Hilbert moduli space. *Journal of Number Theory, Elliptic Curve Cryptography*, 131(5), 2011.

[57] I. Lovato : Computing modular polynomials with theta functions. `http://algant.eu/documents/theses/lovato.pdf`, Academic year 2011/2012. master thesis.

[58] D. Lubicz et D. Robert : Computing isogenies between Abelian Varieties. *Compositio Mathematica*, 148(05):1483–1515, 2012.

[59] D. Lubicz et D. Robert : Computing separable isogenies in quasi-optimal time. *LMS Journal of Computation and Mathematics*, 18(1):198–216, 2015.

[60] R. Manni : Modular varieties with level 2 theta structure. *American Journal of Mathematics*, 116:1489–1511, 1994.

[61] F. Martin et E. Royer : Formes modulaires et périodes. *In Formes modulaires et transcendance*, volume 12 de *Séminaires et Congrès*, pages 1–117. Société Mathématique de France, 2005.

[62] J.-F. Mestre : Construction de courbes de genre 2 à partir de leurs modules. *In Effective methods in algebraic geometry*, volume 94 de *Progress in Mathematics*, pages 313–334. Birkhäuser Boston, 1991.

[63] E. Milio : A quasi-linear time algorithm for computing modular polynomials in dimension 2. *LMS Journal of Computation and Mathematics*, 18(1):603–632, 2015.

[64] V. Miller : Use of elliptic curves in cryptography. *In Advances in Cryptology — CRYPTO '85 Proceedings*, volume 218 de *Lecture Notes in Computer Science*, pages 417–426. Springer Berlin Heidelberg, 1986.

[65] P. Molin : *Intégration numérique et calculs de fonctions L*. Thèse de doctorat, Université Bordeaux 1, 2010. `https://github.com/pascalmolin/hcperiods`.

[66] D. Mumford : On the equations defining abelian varieties. i. *Inventiones mathematicae*, 1(4):287–354, 1966.

[67] D. Mumford : *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.

[68] D. Mumford : *Tata lectures on theta I*, volume 28 de *Progress in Mathematics*. Birkhäuser Boston, 1983.

[69] D. Mumford : *Tata lectures on theta II*, volume 43 de *Progress in Mathematics*. Birkhäuser Boston, 1984.

[70] N. Murabayashi : The moduli space of curves of genus two covering elliptic curves. *Manuscripta Mathematica*, 84(1):125–133, 1994.

[71] S. Nagaoka : On the ring of hilbert modular forms over $\mathbb{Z}$. *Journal Math. Soc. Japan*, 35(4):589–608, 1983.

[72] H.L. Resnikoff : On the Graded Ring of Hilbert Modular Forms Associated with $\mathbb{Q}(\sqrt{5})$. *Math. Ann.*, 208:161–170, 1974.

[73] R. Rivest, A. Shamir et L. Adleman : A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[74] B. Runge : Endomorphism rings of abelian surfaces and projective models of their moduli spaces. *Tohoku mathematical journal*, 51(3):283–303, 1999.

[75] R. Schertz : *Complex multiplication*, volume 15 de *New mathematical monographs*. Cambridge University Press, Cambridge, 2010.

[76] L. Schläfli : Beweis der Hermiteschen Verwandlungstafeln für die elliptischen Modulfunktionen. *Journal für die reine und angewandte Mathematik*, 72:360–369, 1870.

[77] R. Schoof : Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–264, 1995.

[78] A. Schönhage et V. Strassen : Schnelle Multiplikation grosser Zahlen. *Computing*, 7(3):281–292, 1971.

[79] J.H. Silverman : *The Arithmetic of Elliptic Curves*, volume 106 de *Graduate Texts in Mathematics*. Springer-Verlag New York, 1986.

[80] M. Streng : *Complex multiplication of abelian surfaces*. Thèse de doctorat, Universiteit Leiden, 2010.

[81] A.V. Sutherland : Computing Hilbert class polynomials with the Chinese remainder theorem. *Mathematics of Computation*, 80:501–538, 2011.

[82] J. Tate : Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones mathematicae*, 2:133–144, 1966.

[83] J. Thomae : Beitrag zur Bestimmung von $\theta(0, 0, \ldots, 0)$ durch die Klassenmoduln algebraischer Funktionen. *Journal für die Reine und Angewandte Mathematik*, 70:201–222, 1870.

[84] G. Van der Geer : On the geometry of a Siegel modular threefold. *Math. Ann.*, 260(3):317–350, 1982.

[85] J. von zur Gathen et G. Jürgen : *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 1999.

[86] J. Vélu : Isogénies entre courbes ellitiques. *Compte Rendu Académie Sciences Paris Série A-B*, 273:A238–A241, 1971.

[87] H. Weber : *Elliptische Funktionen und Algebraische Zahlen*, volume 3 de *Lehrbuch der Algebra, 2nd ed.* Vieweg, Braunschweig, 1908.

[88] H. Weber : *Lehrbuch der Algebra*, volume 3. Chelsea Publishing Company, New York, 1908.

[89] Don Zagier : Modular forms of one variable. *Notes based on a course given in Utrecht*, 1991. `http://people.mpim-bonn.mpg.de/zagier/files/tex/UtrechtLectures/UtBook.pdf`.

Résumé

Les polynômes modulaires sont utilisés dans le calcul de graphes d'isogénies, le calcul des polynômes de classes ou le comptage du nombre de points d'une courbe elliptique, et sont donc fondamentaux pour la cryptographie basée sur les courbes elliptiques.

Des polynômes analogues sur les surfaces abéliennes principalement polarisées ont été introduits par Régis Dupont en 2006, qui a également proposé un algorithme pour les calculer, et des résultats théoriques sur ces polynômes ont été donnés dans un article de Bröker–Lauter, en 2009. Mais les polynômes sont très gros et ils n'ont pu être calculés que pour l'exemple minimal $p = 2$.

Dans cette thèse, nous poursuivons les travaux de Dupont et Bröker–Lauter en permettant de calculer des polynômes modulaires pour des invariants basés sur les thêta constantes, avec lesquels nous avons pu calculer les polynômes jusqu'à $p = 7$, tout en démontrant des propriétés de ces polynômes. Mais des exemples plus grands ne semblent pas envisageables.

Ainsi, nous proposons une nouvelle définition des polynômes modulaires dans laquelle l'on se restreint aux surfaces abéliennes principalement polarisées qui ont multiplication réelle par l'ordre maximal d'un corps quadratique réel afin d'obtenir des polynômes plus petits. Nous présentons alors de nombreux exemples de polynômes et des résultats théoriques.

Mots-clés : Cryptographie, isogénies, variétés abéliennes, polynômes modulaires.

Abstract

Modular polynomials on elliptic curves are a fundamental tool used for the computation of graph of isogenies, class polynomials or for point counting. Thus, they are fundamental for the elliptic curve cryptography.

A generalization of these polynomials for principally polarized abelian surfaces has been introduced by Régis Dupont in 2006, who has also described an algorithm to compute them, while theoretical results can been found in an article of Bröker–Lauter of 2009. But these polynomials being really big, they have been computed only in the minimal case $p = 2$.

In this thesis, we continue the work of Dupont and Bröker–Lauter by defining and giving theoretical results on modular polynomials with new invariants, based on theta constants. Using these invariants, we have been able to compute the polynomials until $p = 7$ but bigger examples look intractable. Thus we define a new kind of modular polynomials where we restrict on the surfaces having real multiplication by the maximal order of a real quadratic field. We present many examples and theoretical results.

Keywords : Cryptography, isogenies, abelian varieties, modular polynomials.